paloalto TECHDOCS

Aide sur l’interface Web PAN-OS

11.0

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

March 28, 2023

Table of Contents

Bases d’interface Web 17

Vue d’ensemble du pare-feu 18
Fonctionnalités et avantages 19
Heure de la dernière connexion et tentatives de connexion échouées 21
Message du jour 22
Gestionnaire de tâches 23
Langue 26
Alarmes 27
Validation des modifications 28
Enregistrement des configurations candidates 33
Annuler les modifications 38
Configurations du verrouillage 43
Recherche globale 45
Détails de la menace 46
Récapitulatif d'AutoFocus Intelligence 49
Exportation du tableau de configuration 52
Modifier le mode de démarrage 54

Tableau de bord 57

Widgets du tableau de bord 58

ACC 61

Aperçu de l’ACC 62
Onglets de l’ACC 64
Widgets de l’ACC 66
Actions de l’ACC 68
Utilisation des onglets et des widgets 68
Utilisation des filtres – Filtres locaux et filtres généraux 69

surveiller 73

Surveillance > Journaux 74
Types de journaux 74
Actions des journaux 82
Surveillance > External Logs 85
Surveillance > Moteur de corrélation automatique 86
Surveillance > Moteur de corrélation automatique > Objets de corrélation 86
Surveillance > Moteur de corrélation automatique > Événements corrélés 87
Surveillance > Capture de paquets 90
Aperçu de la capture de paquets 91

Blocs de construction d’une capture de paquets personnalisée....91
Activation de la capture de paquets de menaces....94
Surveillance > App-Scope....96
Aperçu de l’App-Scope....96
Rapport récapitulatif App-Scope....97
Rapport de surveillance des modifications App-Scope....98
Rapport de surveillance des menaces App-Scope....99
Rapport de la carte des menaces App-Scope....101
Rapport de surveillance du réseau App-Scope....102
Rapport de la carte du trafic App-Scope....104
Surveillance > Navigateur de session....106
Surveillance > Liste d’interdiction d’adresses IP....107
Entrées de la liste d’interdiction d’adresses IP....107
Afficher ou supprimer les entrées de la liste d’interdiction d’adresses IP....108
Surveillance > Botnet....110
Paramètres d'un rapport du Botnet....110
Paramètres de configuration d’un Botnet....111
Surveillance > Rapports au format PDF....113
Surveillance > Rapports au format'A0;PDF > Gérer un récapitulatif au format PDF....113
Surveillance > Rapports au format PDF > Rapport d'activité des utilisateurs....114
Surveillance > Rapports PDF > Utilisation de l'application SaaS....116
Surveillance > Rapports au format PDF > Groupes de rapports....119
Surveillance > Rapports au format PDF > Planificateur de courrier électronique....120
Surveillance > Gérer des rapports personnalisés....121
Surveillance > Rapports....123

Politiques....125

Types de politique....126
Déplacement ou clonage d’une règle de politique....127
Archive des commentaires d’audit....128
Commentaires d’audit....128
Journaux de configuration (entre les validations)....128
Changements des règles....129
Requête sur le nombre d’utilisations de la règle....130
Requête sur le nombre d’utilisations de la règle du périphérique....131
Politiques > Sécurité....133
Présentation de la politique de sécurité....133
Blocs de construction dans une règle de politique de sécurité....134
Création et gestion des politiques....147

Application d’un contrôle prioritaire ou rétablissement d’une règle de politique de sécurité 151
Applications et utilisation 154
Optimiseur de la politique de sécurité 160
Politiques > NAT 164
Onglet Général des politiques NAT 164
Onglet Paquet d’origine NAT 165
Onglet Paquet translaté NAT 166
Onglet Liaison HA Actif / Actif 170
Onglet Cible NAT 171
Politiques > QoS 172
Politiques > Transfert basé sur une politique 177
Onglet Général du transfert basé sur une politique 177
Onglet Source du transfert basé sur une politique 178
Onglet Destination / Application / Service du transfert basé sur une politique 180
Onglet Transfert du transfert basé sur une politique 180
Onglet Cible du transfert basé sur une politique 182
Politiques > Déchiffrement 183
Onglet Général du déchiffrement 183
Onglet déchiffrement de la source 184
Onglet Déchiffrement de la destination 186
Onglet Service de déchiffrement / catégorie d’URL 186
Onglet Options de Déchiffrement 187
Onglet cible de déchiffrement 189
Politiques >Broker de paquets de réseau 190
Onglet Général du Broker de paquets de réseau 190
Onglet Source du Broker de paquets réseau 191
Onglet Destination du Broker de paquets réseau 192
Onglet Application/Service/Trafic du Broker de paquets de réseau 193
Onglet Sélection du chemin d’accès du Broker de paquets de réseau 194
Utilisation de la règle d’optimisation de la politique du Broker de paquets de réseau 194
Politiques > Inspection des tunnels 196
Blocs de construction dans une politique d’inspection des tunnels 196
Politiques > Contrôle prioritaire sur l'application 204
Onglet Général d’outre-passement sur l’application 205
Onglet Source outre-passement d’une l’application 206
Onglet outrepasser Destination sur l’application 206
Onglet Application/ Protocole d’outrepasser l’application 207
Onglet cible Outrepasser l’application 207
Politiques > Authentification 209

Blocs de construction d’une règle de politique d’authentification....209
Créer et gérer la politique d’authentification....216
Politiques > Protection DoS....218
Onglet Général de protection DoS ;....218
Onglet Source de protection DoS ;....219
Onglet Destination de protection DoS ;....220
Onglet Option / Protection de protection DoS....221
Onglet cible de protection DoS....223
Politiques > SD-WAN....225
Onglet Général SD-WAN....225
Onglet Source SD-WAN....226
Onglet Destination SD-WAN....227
Onglet Application/Service SD-WAN....228
Onglet Sélection du chemin d’accès SD-WAN....230
Onglet Cible SD-WAN....230

Objets....233

Déplacement, clonage ou rétablissement des objets ou application d’un contrôle prioritaire sur ceux-ci....234
Déplacement ou clonage d’un objet....234
Contrôle prioritaire et rétablissement d’un objet....234
Objets > Adresses....236
Objets > Groupes d'adresses....239
Objets > Régions....242
Objets > Groupes d’utilisateurs dynamiques....243
Objets > Applications....246
Présentation des applications....246
Actions prises en charge sur les applications....251
Définition des applications....254
Objets > Groupes d'applications....260
Objets > Filtres d'applications....261
Objets > Services....262
Objets > Groupes de services....265
Objets > Étiquettes....266
Création d’étiquettes....266
Afficher la base de règles en tant que groupes....268
Gestion des étiquettes....272
Objets > Périphériques....275
Objets > Listes dynamiques externes....277
Objets > Objets personnalisés....284
Objets > Objets personnalisés > Modèles de données....284

Objets > Objets personnalisés > Logiciels espions / vulnérabilité....291
Objets > Objets personnalisés > Catégories d'URL....296
Objets > Profils de sécurité....298
Actions dans des profils de sécurité....298
Objets > Profils de sécurité > Antivirus....302
Objets > Profils de sécurité > Profil antispyware....306
Objets > Profils de sécurité > Protection contre les vulnérabilités....314
Objets > Profils de sécurité > URL Filtering....321
Paramètres généraux du filtrage des URL....321
Catégories de URL Filtering....322
Paramètres de URL Filtering....326
Détection des informations d'identification de l'utilisateur....327
Insertion de l'en-tête HTTP....330
Catégorisation en ligne....332
Objets > Profils de sécurité > Blocage des fichiers....333
Objets > Profils de sécurité > Analyse WildFire....335
Objets > Profils de sécurité > Filtrage des données....337
Objets > Profils de sécurité > Protection DoS....339
Objets > Profils de sécurité > Protection du réseau mobile....344
Objets > Profils de sécurité > Protection SCTP....353
Objets > Groupes de profils de sécurité....360
Objets > Transfert des journaux....361
Objets > Authentification....366
Objets > Profils de déchiffrement....369
Paramètres généraux des profils de déchiffrement....369
Paramètres de contrôle du trafic SSL déchiffré....370
Paramètres de contrôle du trafic non déchiffré....378
Paramètres de contrôle du trafic SSH déchiffré....378
Objets > Profil de broker de paquets....380
Objets > Gestion des liens SD-WAN....384
Objects > SD-WAN Link Management > Path Quality Profile (Objets > Gestion des liens SD-WAN > Profil de qualité des chemins d'accès)....384
Objects > SD-WAN Link Management > SaaS Quality Profile (Objets > Gestion des liens SD-WAN > Profil de qualité SaaS)....385
Objets > Gestion des liens SD-WAN > Profil de distribution du trafic....387
Objets > Gestion des liens SD-WAN > Profil de correction des erreurs....388
Objets > Calendriers....391

Réseau....393

Réseau > Interfaces....394
Présentation des interfaces de pare-feu....395

Composants communs des interfaces de pare-feu....395
Composants communs des interfaces de pare-feu PA-7000 Series....397
Interface Tap....398
Interface HD....399
Interface du câble virtuel....400
Sous-interface de câble virtuel....402
Interface de niveau 2 de la série PA-7000....403
Sous-interface de niveau 2 de la série PA-7000....405
Interface de niveau 3 de la série PA-7000....406
Interface de niveau 3....420
Sous-interface de couche 3....439
Interface de la carte des journaux....458
Sous-interface de la carte des journaux....459
Interface miroir de déchiffrement....460
Groupe d'interfaces Ethernet agrégées (AE)....461
Interfaces Ethernet agrégées (AE)....469
Réseau > Interfaces > VLAN....482
Réseau > Interfaces > En boucle....499
Réseau > Interfaces > De tunnel....502
Réseau > Interfaces > SD-WAN....505
Réseau > Interfaces > PoE....507
Réseau > Zones....510
Présentation des zones de sécurité....510
Étapes de configuration des zones de sécurité....510
Réseau > VLAN....514
Réseau > Câbles virtuels....515
Réseau > Routeurs virtuels....516
Paramètres généraux d'un routeur virtuel....516
Itinéraires statiques....517
Redistribution d'itinéraire....521
RIP....523
OSPF....526
OSPFv3....532
BGP....540
Multidiffusion IP....557
ECMP....562
Statistiques d'exécution supplémentaires d'un routeur virtuel....565
Statistiques d'exécution supplémentaires d'un routeur logique....576
Réseau > Routage > Routeurs logiques....582
Réseau > Routage > Routeurs logiques > Généralités....583
Réseau > Routage > Routeurs logiques > Statique....586

Réseau > Routage > Routeurs logiques > OSPF 590
Réseau > Routage > Routeurs logiques >OSPFv3 594
Réseau > Routage > Routeurs logiques > RIPv2 600
Réseau > Routage > Routeurs logiques > BGP 602
Réseau > Routage > Routeurs logiques > Multidiffusion 608
Réseau > Routage > Profiles de routage 616
Réseau > Routage > Profiles de routage > BGP 616
Réseau > Routage > Profiles de routage > BFD 624
Réseau > Routage > Profiles de routage > OSPF 626
Réseau > Routage > Profiles de routage > OSPFv3 631
Réseau > Routage > Profiles de routage > RIPv2 636
Réseau > Routage > Profiles de routage > Filtres 639
Réseau > Routage > Profiles de routage > Multidiffusion 648
Réseau > Tunnels IPSec 651
Gestion d’un tunnel VPN IPSec 651
Onglet Général Tunnel IPSec 652
Onglet ID de proxy Tunnel IPSec 655
Statut du tunnel IPSec sur le pare-feu 657
Redémarrage ou actualisation d'un tunnel IPSec 657
Réseau > Tunnels GRE 658
Tunnels GRE 658
Réseau > DHCP 661
Présentation de DHCP 661
Adressage DHCP 662
Serveur DHCP 662
Relais DHCP 666
Client DHCP 666
Réseau > Proxy DNS 668
Présentation du proxy DNS 668
Paramètres du proxy DNS 669
Actions de proxy DNS supplémentaires 672
Proxy > réseau 673
Réseau > QoS 675
Paramètres d'une interface de QoS 675
Statistique de l’interface QoS 677
Réseau > LLDP 679
Présentation de LLDP 679
Étapes de configuration de LLDP 679
Réseau > Profils réseau 683
Réseau > Profils réseau > Crypto IPSec GlobalProtect 683
Réseau > Profils réseau > Passerelles IKE 684

Réseau > Profils réseau > Crypto IPSec 692
Réseau > Profils réseau > Crypto IKE 694
Réseau > Profils réseau > Surveillance 695
Réseau > Profils réseau > Gestion de l'interface 696
Réseau > Profils réseau > Protection de zone 698
Réseau > Profils réseau > QoS 727
Réseau > Profils réseau > Profil LLDP 729
Réseau > Profils réseau > Profil BFD 731
Réseau > Profils réseau > Profil d'interface SD-WAN 734

Périphérique 739

Périphérique > Configuration 741
Périphérique > Configuration > Gestion 742
Périphérique > Configuration > Opérations 778
Activation de la surveillance SNMP 786
Périphérique > Configuration > Module de sécurité matériel 790
Paramètres du fournisseur du module matériel de sécurité 790
Authentication HSM 791
Opérations matérielles de sécurité 792
Configuration et état du fournisseur du module matériel de sécurité matériel 792
Statut du module matériel de sécurité 793
Périphérique > Configuration > Services 795
configuration des services pour les systèmes globaux et virtuels ; 795
Paramètres des services globaux 796
Prise en charge des protocoles IPv4 et IPv6 pour la configuration de l'itinéraire de service 799
Route pour le service de destination 803
Périphérique > Configuration > Interfaces 805
Périphérique > Configuration > Télémétrie 809
Périphérique > Configuration > Content-ID 810
Périphérique > Configuration > WildFire 820
Périphérique > Configuration > Session 825
Paramètres de session 825
Délais d'expiration de session 831
Paramètres TCP 833
Paramètres de décryptage : Vérification de la révocation du certificat 837
Paramètres de décryptage : Paramètres de certificat du serveur proxy de transfert 838
Paramètres de décryptage : Paramètres de décryptage SSL 840
Paramètres de session VPN 840
Appareil > Configuration > ACE 842

Périphérique > Configuration > DLP....843
Périphérique > Haute disponibilité....845
Considérations importantes pour la configuration HD....845
HA Paramètres généraux....846
Communications HA....851
Surveillance des chemins et des liens HA....856
Actif HA/Config active....859
Config. du cluster....862
Périphérique > Carte de transfert des journaux....864
Périphérique > Audit de configuration....867
Périphérique > Profils de mot de passe....868
Exigences relatives au nom d’utilisateur et au mot de passe....869
Périphérique > Administrateurs....871
Périphérique > Rôles admin....874
Périphérique > Domaine d'accès....877
Périphérique > Profil d'authentification....878
Profil d'authentification....878
Exportation des métadonnées SAML à partir d’un Profil d’authentification....888
Périphérique > Séquence d'authentification....891
Périphérique > IoT > Serveur DHCP....893
Périphérique > Redistribution des données....896
Périphérique > Redistribution des données > Agents....896
Périphérique > Redistribution des données > Clients....898
Périphérique > Redistribution des données > Paramètres du collecteur....898
Périphérique > Redistribution des données > Inclure/Exclure des réseaux....898
Périphérique > Quarantaine du périphérique....900
Périphérique > Sources d'informations de machine virtuelle....902
Paramètres pour activer les sources d’informations de machine virtuelle pour les Serveurs VMware ESXi et vCenter....904
Paramètres pour activer les sources d’informations de machine virtuelle pour AWS VPC....905
Paramètres pour activer les sources d’informations de machine virtuelle pour Google Compute Engine....907
Périphérique > Résolution des problèmes....910
Correspondance de la politique de sécurité....910
Correspondance de la politique QoS....912
Correspondance de la politique d’authentification....913
Correspondance politique SSL/déchiffrement....915
Correspondance de la politique NAT....916
Correspondance à la politique PBF (transfert basé sur une politique)....917
Correspondance de la politique DoS....919

Routage 920
Test WildFire 921
Archivage sécurisé des menaces 922
Ping 923
Trace Route 924
Connectivité du collecteur de journaux 926
Liste dynamique externe 927
Serveur de mises à jour 928
État du service de journalisation du cloud de test GP 928
État du service du cloud de test GP 929
Périphérique > Systèmes virtuels 930
Périphérique > Passerelles partagées 934
Périphérique > Gestion des certificats 935
Périphérique > Gestion des certificats > Certificats 936
Gestion des certificats du pare-feu et de Panorama 936
Gestion des autorités de certification de confiance par défaut 942
Périphérique > Gestion des certificats > Profil de certificat 944
Périphérique > Gestion des certificats > Répondeur OCSP 947
Périphérique > Gestion des certificats > Profil de service SSL/TLS 948
Périphérique > Gestion des certificats > SCEP 950
Périphérique > Gestion des certificats > Exclusion du déchiffrement SSL 954
Périphérique > Gestion des certificats > Profil de service SSL 957
Périphérique > Pages de réponse 959
Périphérique > Paramètres des journaux 963
Sélection des destinations du transfert des journaux 963
Définition des paramètres d’alarme 967
Effacer les journaux 969
Périphérique > Profils de serveur 970
Périphérique > Profils de serveur > Piège'A0;SNMP 971
Périphérique > Profils de serveur > Syslog 974
Périphérique > Profils de serveur > Messagerie 976
Périphérique > Profils de serveur > HTTP 979
Périphérique > Profils de serveur > NetFlow 983
Périphérique > Profils de serveur > RADIUS 985
Périphérique > Profils de serveur > TACACS+ 988
Périphérique > Profils de serveur > LDAP 990
Périphérique > Profils de serveur > Kerberos 993
Périphérique > Profils de serveur > Fournisseur d’identité SAML 994
Périphérique > Profils de serveur > DNS 998
Périphérique > Profils de serveur > Authentification multi-facteur 999
Périphérique > Base de données d'utilisateurs locale > Utilisateurs 1002

Périphérique > Base de données d'utilisateurs locale > Groupes d'utilisateurs....1004
Périphérique > Exportation programmée des journaux....1005
Périphérique > Logiciel....1007
Périphérique > Mises à jour dynamiques....1010
Périphérique > Licences....1015
Périphérique > Support....1017
Périphérique > Clé principale et diagnostics....1019
Déployer la clé principale....1022
Appareil > Recommandation de politique > IoT....1024
Périphérique > Politique > Recommandation SaaS....1028

Identification utilisateur....1031

Périphérique > Identification utilisateur > Mappage d'utilisateur....1032
Configuration de l'agent User-ID Palo Alto Networks....1032
Surveillance des serveurs....1042
Inclure ou exclure des sous-réseaux pour l'association d'utilisateur....1045
Périphérique > Identification utilisateur > Sécurité de la connexion....1047
Périphérique > Identification utilisateur > Agents de Terminal Server....1048
Périphérique > Identification utilisateur > Paramètres de mappage de groupe....1050
Périphérique > Identification utilisateur> Adresse source fiable....1056
Périphérique > Identification utilisateur > Paramètres du portail d'authentification....1057
Device > User Identification > Cloud Identity Engine (Périphérique > Identification de l'utilisateur > Moteur d'identification du cloud....1061

GlobalProtect....1063

Réseau > GlobalProtect > Portails....1064
Onglet Général Portails GlobalProtect....1065
Onglet de Configuration de l'Authentification des portails GlobalProtect....1068
Onglet Collecte de données du portail GlobalProtect....1070
Onglet GlobalProtect Portals Agent (Agent des portails GlobalProtect)....1071
Onglet des VPN sans client des portails GlobalProtect....1107
Onglet du satellite du portail GlobalProtect....1111
Réseau > GlobalProtect > Passerelles....1116
Onglet Général des passerelles GlobalProtect....1116
Onglet d'authentification de la passerelle GlobalProtect....1118
Onglet Agent de passerelles GlobalProtect....1120
Onglet GlobalProtect Gateway Satellite(Satellite de la passerelle GlobalProtect)....1135
Réseau > GlobalProtect > Gestionnaire de périphériques mobiles....1139
Réseau > GlobalProtect > Applications sans client....1141
Réseau > GlobalProtect > Groupes d'applications sans client....1142
Objets > GlobalProtect > Objets HIP....1143

Onglet Général des objets HIP..... 1143
Onglet Périphérique mobile des objets HIP..... 1146
Onglet Gestion des correctifs des objets HIP..... 1147
Onglet Pare-feu des objets HIP..... 1148
Onglet Anti-logiciels malveillants des objets HIP..... 1149
Onglet Sauvegarde du disque des objets HIP..... 1150
Onglet Cryptage du disque des objets HIP..... 1150
Onglet Prévention des pertes de données des objets HIP..... 1151
Onglet HIP Objects Certificate (Certificat d'objets HIP)..... 1152
Onglet Vérifications personnalisées des objets HIP..... 1152
Objets > GlobalProtect > Profils HIP..... 1154
Périphérique > Client GlobalProtect..... 1156
Gestion du logiciel de l'application GlobalProtect..... 1156
Paramétrage de l'application GlobalProtect..... 1158
Utilisation de l'application GlobalProtect..... 1158

Interface Web de Panorama..... 1161

Utilisation de l'interface Web de Panorama..... 1163
Commutateur de contexte..... 1169
Opérations de validation de Panorama..... 1170
Définition des politiques sur Panorama..... 1183
Partitions de stockage des journaux pour un appareil virtuel Panorama en Mode hérité.. 1185
Panorama > Configuration > Interfaces..... 1187
Panorama > Haute disponibilité..... 1192
Panorama > Clusters WildFire gérés..... 1196
Tâches des clusters WildFire gérés..... 1196
Tâches de l'appareil WildFire géré..... 1197
Informations WildFire gérées..... 1198
Cluster WildFire géré et administration de l'appareil..... 1203
Panorama > Clusters de pare-feu..... 1218
Vue récapitulative..... 1218
Surveillance..... 1219
Panorama > Administrateurs..... 1222
Panorama > Rôles admin..... 1226
Panorama > Domaines d'accès..... 1229
Panorama > Transmission programmée des configurations..... 1231
Planificateur de transmission programmée des configurations..... 1232
Historique d'exécution de la transmission programmée des configurations..... 1233
Panorama > Périphériques gérés > Récapitulatif..... 1235
Administration du pare-feu géré..... 1235
Informations sur les pare-feu gérés..... 1236

Mises à jour logicielles et de contenu du pare-feu....1241
Sauvegardes du pare-feu....1242
Panorama > Quarantaine du périphérique....1243
Panorama > Périphériques gérés > État....1244
État détaillé des périphériques dans Panorama....1246
Panorama > Modèles....1251
Modèles....1251
Piles de Modèles....1252
Panorama > Modèles > Variables des modèles....1254
Panorama > Groupes de périphériques....1257
Panorama > Collecteurs gérés....1260
Informations sur les collecteurs de journaux....1260
Configuration du Collecteur de journaux....1262
Mises à jour logicielles pour les collecteurs de journaux dédiés....1272
Panorama > Groupes de collecteurs....1274
Configuration du groupe de collecteurs....1274
Information sur les groupes de collecteurs....1282
Panorama > Plug-ins....1284
Panorama > SD-WAN....1286
Ajouter des Périphériques SD-WAN....1286
Clusters VPN SD-WAN....1289
Surveillance SD-WAN....1289
Rapports SD-WAN....1291
Panorama > VMware NSX....1293
Configuration d’un groupe de notification....1293
Création de définitions de services....1294
Configuration de l’accès à NSX Manager....1295
Création de règles de redirection....1297
Panorama > Profil d’ingestion des journaux....1300
Panorama > Paramètres des journaux....1301
Panorama > Profils de serveur > SCP....1304
Panorama > Exportation programmée des configurations....1305
Panorama > Logiciel....1307
Gestion des mises à jour logicielles Panorama....1307
Affichage des informations sur les mises à jour logicielles Panorama....1308
Panorama > Déploiement du périphérique....1310
Gestion des mises à jour logicielles et de contenu....1310
Affichage des informations sur les mises à jour logicielles et de contenu....1313
Planification des mises à jour de contenu dynamiques....1314
Rétablissement des versions de contenu précédentes de Panorama....1316
Gestion des licences du pare-feu....1317

Panorama > Clé d’autorisation de l’enregistrement du périphérique.....1319
Ajouter une clé d’autorisation de l’enregistrement du périphérique..... 1319

Bases d’interface Web

Les rubriques suivantes fournissent un aperçu du pare-feu et décrivent les tâches administratives de base.

- Vue d’ensemble du pare-feu
- Fonctionnalités et avantages
- Heure de la dernière connexion et tentatives de connexion échouées
- Message du jour
- Gestionnaire de tâches
- Langue
- Alarmes
- Validation des modifications
- Enregistrement des configurations candidates
- Annuler les modifications
- Configurations du verrouillage
- Recherche globale
- Détails de la menace
- Récapitulatif d'AutoFocus Intelligence
- Modifier le mode de démarrage

Vue d’ensemble du pare-feu

Les pare-feu Palo Alto Networks® de nouvelle génération inspectent l'ensemble du trafic (y compris les applications, les menaces et les contenus) et l'associent à l'utilisateur, où qu'il se trouve et quel que soit le type de périphérique. L’utilisateur, l’application et les contenus, c'est-à-dire tout ce qui fait fonctionner votre entreprise, deviennent parties intégrantes de votre politique de sécurité d'entreprise. Cela vous permet d’harmoniser votre sécurité à vos politiques d’entreprises et de rédiger des règles qui sont faciles à comprendre et à préserver.

Dans le cadre de notre plate-forme d'exploitation de la sécurité, nos pare-feu de nouvelle génération fournissent à votre organisation la possibilité de :

- Activer les applications (y compris les applications en tant que service), les utilisateurs et le contenu en toute sécurité en classant tout le trafic (peu importe le port).
- Réduire le risque d’attaque à l’aide d’un modèle d’application positif, en autorisant toutes les applications désirées et en bloquant tout le reste.
- Appliquer les politiques de sécurité afin de bloquer les exploitations de vulnérabilités connues, les virus, les rançongiciels, les spyware, les botnets et les autres logiciels malveillants inconnus, comme les menaces persistantes avancées.
- Protéger vos centres de données (y compris les centres de données virtuels) en segmentant les données et les applications, ainsi qu’en appliquant le principe de confiance zéro.
- Appliquer une sécurité cohérente dans l'ensemble de vos établissements et de vos environnements infonuagiques.
- Adopter l'informatique mobile sécurisée en étendant la plateforme d’exploitation de sécurité aux utilisateurs et aux périphériques où qu'ils se trouvent.
- Obtenir un aperçu centralisé et simplifier la sécurité du réseau, ce qui rend vos données exploitables afin de pouvoir prévenir des cyberattaques réussies.
- Identifier et empêcher les tentatives de vol d'identifiants en arrêtant l’envoi d’identifiants d’entreprise valides à des sites Web illégitimes. Elle neutralise également la capacité d'un pirate informatique à utiliser des identifiants volés pour un mouvement latéral ou une compromission du réseau en appliquant des politiques d'authentification au niveau de la couche réseau.

Fonctionnalités et avantages

Les pare-feu Palo Alto Networks de dernière génération assurent un contrôle granulaire du trafic autorisé à accéder à votre réseau. Les fonctionnalités et avantages principaux incluent'A0;:

- **Mise en œuvre d’une politique basée sur une application (App-ID™)** – Le contrôle des accès selon le type d’application est beaucoup plus efficace lorsque l’identification d’une application ne se base pas uniquement sur le protocole et le numéro de port. Le service App-ID peut bloquer des applications à haut risque, ainsi que des comportements à haut risque, tels que le partage de fichiers, et le trafic crypté avec le protocole SSL (Secure Sockets Layer) peut être décrypté et inspecté.
- **Identification de l'utilisateur (User-ID™)** - La fonction User-ID permet aux administrateurs de configurer et d'appliquer des politiques de pare-feu basées sur des utilisateurs et des groupes d'utilisateurs, à la place de ou en plus des zones et adresses réseaux. Le pare-feu peut communiquer avec de nombreux serveurs d'annuaire, comme Microsoft Active Directory, eDirectory, SunOne, OpenLDAP et la plupart des autres serveurs d'annuaire basés sur le protocole LDAP afin de fournir au pare-feu des informations concernant un utilisateur et un groupe. Vous pouvez utiliser ces informations pour la mise en œuvre sécurisée d'applications qui peut être définie par utilisateur ou par groupe. Par exemple, l'administrateur peut autoriser une seule organisation de l'entreprise à utiliser une application Web. Vous pouvez également configurer le contrôle granulaire de certains composants d’une application en fonction des utilisateurs et des groupes (voir Identification utilisateur).
- **Prévention des menaces** – Les services de prévention des menaces qui protègent le réseau des virus, des vers, des logiciels espions et d’autres trafics malveillants peuvent varier selon la source de l’application et du trafic (voir Objets > Profils de sécurité).
- **Filtrage des URL** – Les connexions sortantes peuvent être filtrées pour empêcher l’accès à des sites Web inappropriés (voir Objets > Profils de sécurité > Filtrage des URL).
- **Visibilité du trafic** - Les rapports, journaux et mécanismes de notification étendus fournissent une visibilité détaillée dans le trafic des applications réseaux et des événements de sécurité. Le Centre de commande de l’application (ACC) de l’interface Web identifie les applications dont le trafic est le plus dense et les risques de sécurité les plus élevés (voir Surveillance).
- **Adaptabilité et vitesse du réseau** - Le pare-feu Palo Alto Networks peut développer ou remplacer votre pare-feu existant et peut être installé de façon transparente dans n'importe quel réseau ou configuré de sorte à prendre en charge un environnement ayant fait l'objet d'un basculement ou d'un routage. Des vitesses pouvant atteindre plusieurs gigaoctets et une architecture à accès unique permettent de vous fournir ces services avec peu, voire aucun impact sur les délais d'attente du réseau.
- **GlobalProtect** - Le logiciel GlobalProtect™ sécurise les systèmes clients, tels que les ordinateurs portables qui sont utilisés sur le terrain, grâce à une connexion simple et sécurisée où que vous soyez.
- **Fonctionnement à sécurité intégrée** – Un support haute disponibilité (HA) assure un basculement automatique en cas de défaillance matérielle ou logicielle (voir Périphérique > Systèmes virtuels).
- **Analyse de logiciels malveillants et création de rapports** – Le service d’analyse basé sur le cloud WildFire™ fournit une analyse détaillée et crée un rapport concernant les logiciels malveillants qui traversent le pare-feu. L’intégration avec le service de renseignement sur les menaces AutoFocus™ vous permet d’évaluer le risque associé au trafic de votre réseau à l’échelle organisationnelle, industrielle et mondiale.
- **Pare-feu série VM** – Un pare-feu série VM fournit une instance virtuelle de PAN-OS® pouvant être utilisée dans un environnement de centre de données virtualisé. Il est idéal pour les environnements publics, privés et hybrides du cloud.

- **Gestion et Panorama** – Vous pouvez gérer chaque pare-feu par l’intermédiaire d’une interface Web intuitive ou une interface de ligne de commande (CLI) ou tous les pare-feu peuvent être gérés de façon centralisée via le système de gestion centralisée de Panorama™ qui dispose d’une interface Web très similaire à celle des pare-feu Palo Alto Networks.

Heure de la dernière connexion et tentatives de connexion échouées

Pour détecter l'utilisation malveillante et empêcher l'exploitation d'un compte privilégié, comme un compte administratif sur un pare-feu Palo Alto Networks ou sur Panorama, l'interface Web et l'interface de ligne de commande (CLI) affichent l'heure de la dernière connexion au compte et toute tentative de connexion échouée liée à votre nom d'utilisateur lorsque vous vous connectez. Cette information vous permet d'identifier facilement si quelqu'un utilise vos informations d'identification administratives pour lancer une attaque.

Une fois que vous êtes connecté à l’interface Web, l’heure de la dernière connexion au compte apparaît dans la portion inférieure gauche de la fenêtre. Si une ou plusieurs tentatives de connexion échouées se sont produites depuis la dernière connexion réussie, une icône de mise en garde apparaît à droite de l'information concernant la dernière connexion. Placez le curseur sur le symbole de mise en garde pour afficher le nombre de tentatives de connexion ayant échoué ou cliquez pour consulter la fenêtre **Récapitulatif des échecs de tentatives de connexion**, qui liste le nom du compte administrateur, l’adresse IP source et la raison de l’échec de connexion.

Si vous voyez plusieurs tentatives de connexion échouées dont vous n'êtes pas l'auteur, vous devez communiquer avec votre administrateur réseau pour localiser le système qui exécute l'attaque exhaustive, puis enquêtez sur l'utilisateur et l'ordinateur de l'hôte pour identifier et éradiquer toute activité malveillante. Si vous voyez que la date et l'heure de la dernière connexion au compte indiquent un compte compromis, vous devez immédiatement changer votre mot de passe, puis effectuer une vérification de la configuration pour déterminer si l'on a effectué des modifications de configuration suspectes. Si vous constatez que les journaux ont été effacés ou si vous avez des difficultés à déterminer si des modifications inappropriées ont été effectuées à l'aide de votre compte, rétablissez la configuration afin d'obtenir une bonne configuration.

Message du jour

Si un autre administrateur ou vous avez configuré un message du jour ou si Palo Alto Networks en a intégré un dans le cadre d’une nouvelle version du logiciel ou du contenu, une boîte de dialogue Message du jour s’affiche lorsque les utilisateurs se connectent à l’interface Web. Cela garantit que les utilisateurs voient l’information importante, comme un redémarrage imminent du système, qui affecte les tâches qu’ils souhaitent effectuer.

La boîte de dialogue affiche un message par page. Si la boîte de dialogue comprend l’option **Do not show again (Ne plus afficher)**, vous pouvez la sélectionner pour chaque message dont vous ne souhaitez pas que la boîte de dialogue s’affiche lors des prochaines connexions.

*Chaque fois qu'une modification est apportée au **Message of the Day (Message du jour)**, le nouveau message apparaît lors de votre prochaine connexion au compte, même si vous avez sélectionné l'option **Do not show again (Ne plus afficher)** lors d'une connexion précédente. Vous devez ensuite resélectionner cette option pour éviter de voir le message modifié lors de vos prochaines connexions.*

Pour naviguer parmi les différentes boîtes de dialogue, cliquez sur les flèches droite ( ) et gauche ( ) situées sur les côtés de la boîte de dialogue ou cliquez sur un sélecteur de page ( ) le long de la portion inférieure de la boîte de dialogue. Après avoir cliqué sur **Close (Fermer)** dans la boîte de dialogue, vous pouvez l'ouvrir à nouveau manuellement en cliquant sur les messages ( ) au bas de l'interface Web.

Pour configurer un message du jour, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les paramètres des bannières et des messages.

Gestionnaire de tâches

Cliquez sur **Tâches** en bas de l’interface Web, pour afficher les opérations que d’autres administrateurs, PAN-OS ou vous avez lancées depuis le dernier redémarrage du pare-feu (par exemple, des validations manuelles ou des rafraîchissements automatiques du nom de domaine complet [FQDN]). Pour chaque tâche, le Gestionnaire des tâches fournit les informations et les actions décrites dans le tableau ci-dessous.

*Par défaut, certaines colonnes sont masquées. Pour afficher ou masquer des colonnes spécifiques, ouvrez le menu déroulant dans n’importe quel en-tête de colonne, sélectionnez **Colonnes**, puis sélectionnez (afficher) ou effacer (masquer) les noms des colonnes.*

Champ/Bouton	Description
  	Pour filtrer les tâches, vous devez saisir une chaîne de texte basée sur une valeur dans l’une des colonnes et Appliquer le filtre (). Par exemple, saisir **`edl`** filtrera la liste pour afficher uniquement les tâches EDLFetch (récupérer les listes dynamiques externes). Pour supprimer le filtrage, cliquez sur Supprimer le filtre ().
Type	Le type de tâche, comme une demande de journaux, un rafraîchissement de la licence ou une validation. Si les informations relatives à la tâche (les avertissements par exemple) sont trop longues pour rentrer dans la colonne Messages, vous pouvez cliquer sur la valeur Type pour afficher tous les détails.
Status (État)	Indique si la tâche est en attente (comme les validations dont l’état est « File d’attente »), en cours (telles que les demandes de journaux dont l’état est « Actif »), terminée ou échouée. Pour les validations en cours, l'État indique le pourcentage d'achèvement.
ID de tâche	Un numéro qui identifie la tâche. À partir de la CLI, vous pouvez utiliser l’ID de tâche pour afficher les détails supplémentaires d’une tâche. Par exemple, vous pouvez consulter la position d’une tâche de validation dans la file d’attente de validation en saisissant : `> afficher l'identifiant de la tâche<job-id>`
Heure de début	La date et l’heure de début de la tâche. Pour les tâches de validation, l’Heure de début indique le moment où une validation a été ajoutée à la file d’attente de validation.

Champ/Bouton	Description
Messages	Affichent des détails sur la tâche. Si l’entrée indique qu’il y a trop de messages, vous pouvez cliquer sur le Type de tâche pour voir les messages. En ce qui concerne les tâches de validation, les Messages comprennent le délai avant le retrait de la file d’attente pour indiquer quand PAN-OS a commencé à procéder à la validation. Pour voir la description qu'a saisie un administrateur relativement à une validation, cliquez sur **Commit Description (Description de validation)**. Pour plus d’informations, reportez-vous à la section Validation des modifications.
Action (Action)	Cliquez sur **x** pour annuler une validation en attente initiée par un administrateur ou par PAN-OS. Ce bouton est disponible uniquement pour les administrateurs qui ont l’un des rôles prédéfinis suivants : super utilisateur, administrateur du périphérique, administrateur du système virtuel ou administrateur de Panorama.
Admin	Affiche l’administrateur qui a lancé la tâche. Pour les tâches automatiques, telles qu’une `License Refresh (actualisation de licence)`, l’administrateur est le `System (système)` (Panorama managed firewalls (Pare-feu gérés par Panorama)) Si une tâche est lancée par un administrateur Panorama, le nom de l’administrateur est ajouté à `Panorama`. Par exemple, `Panorama-<admin>`.
Heure de fin	La date et l’heure de fin de la tâche. Cette colonne est masquée par défaut.
Montrer	Sélectionnez les tâches que vous souhaitez afficher : • **Toutes les tâches** (par défaut). • **Toutes** les tâches d’un certain type (**Tâches**, **Rapports** ou **Requêtes du journal**). • Toutes les tâches **En cours d’exécution** (en cours). • Toutes les tâches **En cours d’exécution** d’un certain type (**Tâches**, **Rapports** ou **Requêtes du journal**). • (Panorama uniquement) Utilisez la deuxième liste déroulante pour afficher les tâches de **Panorama** (par défaut) ou un pare-feu géré spécifique.
Effacer la file d'attente de validation	Annule toutes les validations en attente initiées par les administrateurs ou par PAN-OS. Ce bouton est disponible uniquement pour les administrateurs qui ont l’un des rôles prédéfinis

Champ/Bouton	Description
	suivants : super utilisateur, administrateur du périphérique, administrateur du système virtuel ou administrateur de Panorama.

Langue

Par défaut, la langue qui est définie sur l'ordinateur à partir duquel vous vous connectez au pare-feu détermine la langue qui s’affiche sur l'interface de gestion Web. Pour changer manuellement la langue, cliquez sur **Language (Langue)** (dans le coin inférieur droit de l'interface Web), sélectionnez la langue souhaitée dans le menu déroulant, puis cliquez sur **OK**. L’interface Web s’actualise et s’affiche dans la langue souhaitée.

Voici certaines langues prises en charge : français, japonais, espagnole, chinois simplifié et chinois traditionnel

Alarmes

Une alarme est un message généré par le pare-feu indiquant que le nombre d’événements d’un certain type (par exemple, les erreurs de chiffrement et de déchiffrement) a dépassé le seuil configuré pour ce type d’événement (reportez-vous à la section Définitions des paramètres d’alarme). Lorsqu'il génère une alarme, le pare-feu crée un Journal des alarmes et ouvre la boîte de dialogue Alarmes du système pour afficher l'alarme en question. Après avoir fermé la boîte de dialogue, vous pouvez à tout moment la rouvrir en cliquant sur **Alarmes** () au bas de l’interface Web. Pour éviter que le pare-feu ouvre automatiquement la boîte de dialogue pour une alarme en particulier, sélectionnez Alarmes non acquittées, puis cliquez sur **Acquitter** pour ajouter les alarmes à la liste des Alarmes acquittées.

Validation des modifications

Cliquez sur **Valider** dans le coin supérieur droit de l’interface Web et indiquez une opération à appliquer pour les modifications en attente relatives à la configuration du pare-feu : commit (activer), valider ou prévisualiser. Vous pouvez filtrer les modifications en attente par l’administrateur ou l’*emplacement* et ensuite prévisualiser, valider et confirmer uniquement ces modifications. L’emplacement peut être les systèmes virtuels spécifiques, des politiques et des objets partagés ou des paramètres de périphériques et de réseau partagés.

Le pare-feu met en attente les demandes de validation afin que vous puissiez lancer une nouvelle validation lorsqu'une validation précédente est en cours. Le pare-feu exécute les validations dans l’ordre dans lequel elles sont initiées, mais donne la priorité aux validations que le pare-feu initie automatiquement, comme les actualisations du nom de domaine complet. Cependant, si la file d’attente possède déjà le nombre maximum de validations lancées par l’administrateur, vous devez attendre que le pare-feu termine le traitement d’une validation en attente avant d’en lancer une nouvelle.

Utilisez le Gestionnaire de tâches pour annuler des validations ou pour voir les détails des validations dont l’état est en attente, en cours, terminé ou échoué.

La boîte de dialogue Validation affiche les options décrites dans le tableau suivant.

Champ/Bouton	Description
Valider toutes les modifications	Confirme toutes les modifications pour lesquelles vous avez des privilèges administratifs (par défaut). Vous ne pouvez pas filtrer manuellement le périmètre des modifications de configuration que le pare-feu valide lorsque vous sélectionnez cette option. Au lieu de cela, le rôle d’administrateur affecté au compte que vous avez utilisé pour vous connecter détermine l’étendue de validation : • **Rôle du super-utilisateur** – Le pare-feu valide les modifications de tous les administrateurs. • **Rôle personnalisé** – Les privilèges du profil de Rôle administrateur affecté à votre compte déterminent l’étendue de validation (voir Périphérique > Rôles administrateur). Si le profil inclut le privilège **Valider pour d’autres administrateurs**, le pare-feu valide les modifications configurées par tous les administrateurs. Si votre profil de Rôle administrateur n’inclut pas le privilège **Valider pour les autres administrateurs**, le pare-feu ne valide que vos modifications et non celles d’autres administrateurs. Si vous avez mis en œuvre des domaines d’accès, le pare-feu applique automatiquement ces domaines pour filtrer le périmètre de validation (voir Périphérique > Domaine d’accès). Quel que soit votre rôle administrateur, le pare-feu ne valide que les modifications de configuration dans les domaines d’accès affectés à votre compte.

Champ/Bouton	Description
Valider les modifications effectuées par	Filtre le périmètre des modifications de configuration que le pare-feu valide. Le rôle administrateur affecté au compte que vous avez utilisé pour vous connecter détermine vos options de filtrage : • **Rôle du super-utilisateur** – Vous pouvez limiter l’étendue de validation aux modifications apportées par des administrateurs spécifiques et aux modifications effectuées dans des emplacements spécifiques. • **Rôle personnalisé** – Les privilèges du profil de Rôle administrateur affecté à votre compte déterminent vos options de filtrage (voir Périphérique > Rôles administrateur). Si le profil inclut le privilège **Valider pour les autres administrateurs**, vous pouvez limiter l’étendue de validation aux modifications configurées par des administrateurs spécifiques et aux modifications effectuées dans des emplacements spécifiques. Si votre profil de Rôle administrateur n’inclut pas le privilège **Commit For Other Admins (Valider pour les autres administrateurs)**, vous pouvez limiter l’étendue de validation uniquement aux modifications que vous avez effectuées dans des emplacements spécifiques. Filtre l’étendue de validation comme suit : • **Filtrer par administrateur** – Même si votre rôle vous permet de valider les modifications effectuées par les autres administrateurs, par défaut, l’étendue de validation inclut uniquement vos modifications. Pour ajouter d’autres administrateurs à la portée de la validation, cliquez sur le lien **<usernames>**, sélectionnez les administrateurs et cliquez sur **OK**. • **Filtrer par emplacement** – Sélectionnez les emplacements spécifiques pour les modifications à Inclure dans la validation. Si vous avez mis en œuvre des domaines d’accès, le pare-feu filtre automatiquement le périmètre de validation en fonction de ces domaines (voir Périphérique > Domaine d’accès). Quel que soit votre rôle administrateur et vos choix de filtrage, l’étendue de validation inclut uniquement les modifications de configuration dans les domaines d’accès affectés à votre compte.  *Après avoir chargé une configuration (*Périphérique > Configuration > Opérations*), vous devez* ***Valider toutes les modifications****.* Lorsque vous validez des modifications apportées à un système virtuel, vous devez inclure les modifications de tous les administrateurs qui ont ajouté, supprimé ou repositionné des règles pour la même base de règles dans ce système virtuel.

Champ/Bouton	Description
Étendue de la validation	Répertorie les emplacements contenant des modifications à valider. Différents facteurs déterminent si la liste inclut toutes les modifications ou un sous-ensemble de modifications, comme il est décrit dans Valider toutes les modifications et Valider les modifications effectuées par. Les emplacements peuvent être l’un des éléments suivants : • **objet partagé** – Les paramètres qui sont définis dans l’emplacement Partagé. • **Politique et objets** – Règles de politique ou objets qui sont définis sur un pare-feu qui ne dispose pas de plusieurs systèmes virtuels. • **Périphérique et réseau** – Paramètres réseau et de périphériques globaux (tels que les profils de Gestion de l’interface) et non spécifiques à un système virtuel. Cela s’applique également aux paramètres réseau et de périphériques sur un pare-feu qui ne dispose pas de plusieurs systèmes virtuels. • **<virtual-system>** – Le nom du système virtuel dans lequel les règles de politique ou les objets sont définis sur un pare-feu comportant plusieurs systèmes virtuels. Cela comprend également les paramètres réseau et de périphérique spécifiques à un système virtuel (par exemple, des zones).
Type d'emplacement	Cette colonne classe les emplacements des modifications en attente : • **Systèmes virtuels** – Les paramètres qui sont définis dans un système virtuel spécifique. • **Autres modifications** – Les paramètres qui ne sont pas spécifiques à un système virtuel (comme les objets partagés).
Inclure dans la validation (Validation partielle uniquement)	Vous permet de sélectionner les modifications que vous souhaitez valider. Par défaut, toutes les modifications de l’**Étendue de validation** sont sélectionnées. Cette colonne s’affiche uniquement après que vous avez choisi de **Valider les modifications effectuées par** des administrateurs spécifiques.  *Il peut y avoir des dépendances affectant les modifications que vous incluez dans une validation. Par exemple, si vous ajoutez un objet et qu’un autre administrateur modifie cet objet, vous ne pouvez pas valider la modification pour l’autre administrateur sans valider votre propre modification.*
Regrouper par type d’emplacement	Regroupe la liste des modifications de configuration de l’**Étendue de validation** par **Type d’emplacement**.

Champ/Bouton	Description
Prévisualiser les modifications	Vous permet de comparer les configurations que vous avez sélectionnées dans l’**Étendue de validation** de la configuration en cours d’exécution. La fenêtre de prévisualisation utilise un code couleur pour indiquer quelles modifications sont des ajouts (en vert), des modifications (en jaune) ou des suppressions (en rouge). Pour vous aider à faire correspondre les modifications aux sections de l’interface Web, vous pouvez configurer la fenêtre de prévisualisation pour afficher **Lignes de contexte** avant et après chaque modification. Ces lignes proviennent des fichiers du candidat et des configurations en cours d’exécution que vous comparez. *Étant donné que les résultats de prévisualisation s’affichent dans une nouvelle fenêtre de navigateur, votre navigateur doit autoriser les fenêtres contextuelles. Si la fenêtre de prévisualisation ne s’ouvre pas, reportez-vous à la documentation de votre navigateur pour connaître les étapes permettant d’autoriser les fenêtres contextuelles.*
Modifier le récapitulatif	Répertorie les paramètres individuels pour lesquels vous effectuez des modifications. La liste **Récapitulatif des modifications** affiche les informations suivantes pour chaque paramètre : • **Nom de l’objet** – Le nom qui identifie la politique, l’objet, le paramètre réseau ou le paramètre de périphérique. • **Type** – Le type de paramètre (comme Adresse, règle de Sécurité ou Zone). • **Type d’emplacement** – Indique si le paramètre est défini dans **Systèmes virtuels**. • **Emplacement** – Le nom du système virtuel sur lequel le paramètre est défini. La colonne affiche **Partagé** pour les paramètres qui ne sont pas spécifiques à un système virtuel. • **Opérations** – Indique chaque opération (créer, modifier ou supprimer) exécutée sur le paramètre depuis la dernière validation. • **Propriétaire** – L’administrateur qui a effectué la dernière modification du paramètre. • **Sera validé** – Indique si la validation inclut le paramètre actuellement. • **Propriétaires précédents** – Les administrateurs qui ont apporté des modifications au paramètre avant la dernière modification. Vous pouvez éventuellement **Regrouper par** Nom de colonne (comme **Type**).

Champ/Bouton	Description
	Sélectionnez un objet dans la liste des changements pour afficher la **Différence au niveau de l’objet**.
Confirmer la validation	Vérifie que la syntaxe de la configuration du pare-feu est correcte et est complète d’un point de vue sémantique. Le résultat inclut les mêmes erreurs et avertissements qu’une validation afficherait, y compris la règle l’occultation et l’application des avertissements de dépendance. Le processus de validation vous permet de trouver et de corriger les erreurs avant la validation (il ne modifie pas la configuration en cours d’exécution). Cette option est utile si vous avez une fenêtre de validation fixe et que vous souhaitez vous assurer que la validation sera une réussite exempte d’erreur.
Description	Vous permet de saisir une description (comportant jusqu’à 512 caractères) pour aider les autres administrateurs à comprendre les modifications que vous avez effectuées. *Le Journal système pour un événement de validation tronquera la description si elle dépasse 512 caractères.*
Valider	Démarre la validation ou, si d’autres validations sont en attente, l’ajoute à la file d’attente de validation.
État de la validation	Fournit la progression pendant la validation et fournit ensuite les résultats après la validation. Les résultats de la validation indiquent la réussite ou l’échec, les détails sur la validation des modifications et les avertissements de la validation. Les avertissements sont les suivants : • **Validation** – Répertorie les avertissements généraux sur la validation. • **Dépendance d’application** – Répertorie toutes les dépendances d’application requises pour les règles existantes. • **Règle Shadow** – Répertorie toutes les règles Shadow.

Enregistrement des configurations candidates

Sélectionnez **Config (Configuration)** > **Save Changes (Enregistrer les modifications)** en haut à droite du pare-feu ou de l’interface Web Panorama pour enregistrer un nouveau fichier instantané de configuration candidate ou pour écraser un fichier de configuration existant. Si le pare-feu ou Panorama redémarre avant que vous validiez vos modifications, vous pouvez rétablir la configuration candidate à l’instantané sauvegardé pour restaurer les modifications apportées après la dernière validation. Pour revenir à l’instantané, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)**et **Load named configuration snapshot (Charger l’instantané de la configuration)**. Si l’instantané n’est pas rétabli après avoir effectué un redémarrage, la configuration candidate sera la même que la dernière configuration validée (la configuration active).

Vous pouvez filtrer les modifications de la configuration à enregistrer en fonction de l’administrateur ou de l’*emplacement*. L’emplacement peut être les systèmes virtuels spécifiques, des politiques et des objets partagés ou des paramètres de périphériques et de réseau partagés.

Vous devez régulièrement enregistrer vos modifications afin de ne pas les perdre si le pare-feu ou Panorama redémarre.

L’enregistrement de vos modifications dans la configuration candidate n’active pas ces modifications ; vous devez Valider les modifications *pour les activer.*

La boîte de dialogue Enregistrer les modifications affiche les options décrites dans le tableau suivant :

Champ/Bouton	Description
Enregistrer toutes les modifications	Enregistre toutes les modifications pour lesquelles vous avez des privilèges administratifs (par défaut). Vous ne pouvez pas filtrer manuellement la portée des modifications de configuration que le pare-feu enregistre lorsque vous sélectionnez cette option. Au lieu de cela, le rôle d’administrateur affecté au compte que vous avez utilisé pour vous connecter détermine la portée de l’enregistrement : • **Rôle de super-utilisateur** – Le pare-feu enregistre les modifications de tous les administrateurs. • **Rôle personnalisé** – Les privilèges du profil de rôle administrateur affectés à votre compte déterminent la portée de l’enregistrement (voir Périphérique > Rôles administrateur). Si le profil inclut le privilège d’**Enregistrer pour les autres administrateurs**, le pare-feu enregistre les modifications configurées par tous les administrateurs. Si votre profil de rôle administrateur n’inclut pas le privilège d’**Enregistrer pour les autres administrateurs**, le pare-feu n’enregistre que vos modifications et non celles des autres administrateurs. Si vous avez implémenté des domaines d’accès, le pare-feu applique automatiquement ces domaines pour filtrer la portée de l’enregistrement (voir Périphérique > Domaine d’accès). Indépendamment de votre rôle administratif, le pare-feu n’enregistre

Champ/Bouton	Description
	que les modifications de configuration dans les domaines d’accès affectés à votre compte.
Enregistrer les modifications effectuées par	Permet de filtrer la portée des modifications de configuration que le pare-feu valide. Le rôle administrateur affecté au compte que vous avez utilisé pour vous connecter détermine vos options de filtrage : • **Rôle de super-utilisateur** – Vous pouvez limiter la portée de l’enregistrement aux modifications apportées par des administrateurs spécifiques et aux modifications dans des emplacements spécifiques. • **Rôle personnalisé** – Les privilèges du profil de Rôle administrateur affecté à votre compte déterminent vos options de filtrage (voir Périphérique > Rôles administrateur). Si le profil inclut le privilège d’**Enregistrer pour les autres administrateurs**, vous pouvez limiter la portée de l’enregistrement aux modifications configurées par des administrateurs spécifiques et aux modifications dans des emplacements spécifiques. Si votre profil de Rôle administrateur n’inclut pas le privilège d’**Enregistrer pour les autres administrateurs**, vous pouvez limiter la portée de l’enregistrement uniquement aux modifications que vous avez effectuées dans des emplacements spécifiques. Filtrez la portée de l’enregistrement comme suit : • **Filtrer par administrateur** – Même si votre rôle permet d’enregistrer les modifications d’autres administrateurs, la portée de l’enregistrement inclut uniquement vos modifications par défaut. Pour ajouter d’autres administrateurs à la portée de l’enregistrement, cliquez sur le lien **<usernames>**, sélectionnez les administrateurs et cliquez sur **OK**. • **Filtrer par emplacement** – Sélectionnez les modifications dans des emplacements spécifiques pour les Inclure dans l’enregistrement. Si vous avez implémenté des domaines d’accès, le pare-feu filtre automatiquement la portée de l’enregistrement en fonction de ces domaines (voir Périphérique > Domaine d’accès). Quels que soient votre rôle administratif et vos choix de filtrage, la portée de l’enregistrement inclut uniquement les modifications de configuration dans les domaines d’accès affectés à votre compte.
Enregistrer la portée	Énumère les emplacements contenant des modifications à enregistrer. Le fait que la liste comprenne toutes les modifications ou un sous-ensemble de modifications dépend de plusieurs facteurs, comme décrit pour les options Enregistrer toutes les modifications et Enregistrer les modifications effectuées par. Les emplacements peuvent être l’un des éléments suivants :

Champ/Bouton	Description
	• **shared-object (objet partagé)** – Les paramètres qui sont définis dans l’emplacement Partagé. • **policy-and-objects (politique et objets)** – (Pare-feu uniquement) Règles de politique ou objets définis sur un pare-feu qui ne possède pas plusieurs systèmes virtuels. • **device-and-network (périphérique et réseau)** – (Pare-feu uniquement) Paramètres réseau et périphériques qui sont globaux (tels que les profils de gestion d’interface) et non spécifiques à un système virtuel. • **<virtual-system>** – (Pare-feu uniquement) Le nom du système virtuel dans lequel les règles ou objets de stratégie sont définis sur un pare-feu doté de plusieurs systèmes virtuels. Cela comprend également les paramètres réseau et de périphérique spécifiques à un système virtuel (par exemple, des zones). • **<device-group>** – (Panorama uniquement) Le nom du groupe de périphériques dans lequel les règles de politique ou les objets sont définis. • **<template>** – (Panorama uniquement) Le nom du modèle ou de la pile de modèles dans lequel les paramètres sont définis. • **<log-collector-group>** – (Panorama uniquement) Le nom du Groupe de collecteurs dans lequel les paramètres sont définis. • **<log-collector>** – (Panorama uniquement) Le nom du Collecteur de journaux dans lequel les paramètres sont définis.
Type d'emplacement	Cette colonne classe les emplacements où les modifications ont été apportées : • **Systèmes virtuels** – (Pare-feu uniquement) Les paramètres définis dans un système virtuel spécifique. • **Groupes de périphériques** – (Panorama uniquement) Paramètres définis dans un groupe de périphériques spécifique. • **Modèles** – (Panorama uniquement) Paramètres définis dans un modèle spécifique ou une pile de modèles spécifique. • **Groupes de collecteurs** – (Panorama uniquement) Paramètres spécifiques à une configuration de Groupe de collecteurs.
Inclure dans Enregistrer (Enregistrement partiel uniquement)	Vous permet de sélectionner les modifications que vous souhaitez enregistrer. Par défaut, toutes les modifications contenues dans **Enregistrer la portée** sont sélectionnées. Cette colonne s’affiche uniquement après que vous avez choisi d’**Enregistrer les modifications effectuées par** des administrateurs spécifiques.

Champ/Bouton	Description
	Il peut y avoir des dépendances qui affectent les modifications que vous incluez dans un enregistrement. Par exemple, si vous ajoutez un objet et qu’un autre administrateur modifie cet objet, vous ne pouvez pas enregistrer la modification pour l’autre administrateur sans enregistrer votre propre modification.
Regrouper par type d’emplacement	Regroupe la liste des modifications de configuration dans le champ **Enregistrer la portée** par **Type d’emplacement**.
Prévisualiser les modifications	Vous permet de comparer les configurations que vous avez sélectionnées dans le champ **Enregistrer la portée** à la configuration en cours d’exécution. La fenêtre de prévisualisation utilise un code couleur pour indiquer quelles modifications sont des ajouts (en vert), des modifications (en jaune) ou des suppressions (en rouge). Pour vous aider à faire correspondre les modifications aux sections de l’interface Web, vous pouvez configurer la fenêtre de prévisualisation pour afficher **Lignes de contexte** avant et après chaque modification. Ces lignes proviennent des fichiers du candidat et des configurations en cours d’exécution que vous comparez. *Etant donné que les résultats de la prévisualisation s’affichent dans une nouvelle fenêtre, votre navigateur doit autoriser les fenêtres contextuelles. Si la fenêtre de prévisualisation ne s'ouvre pas, reportez-vous à la documentation de votre navigateur pour connaître les étapes permettant de débloquer l'ouverture des fenêtres contextuelles.*
Modifier le récapitulatif	Énumère les paramètres individuels pour lesquels vous enregistrez des modifications. La liste **Récapitulatif des modifications** affiche les informations suivantes pour chaque paramètre : • **Nom de l’objet** – Le nom qui identifie la politique, l’objet, le paramètre réseau ou le paramètre de périphérique. • **Type** – Le type de paramètre (comme Adresse, règle de Sécurité ou Zone). • **Type d’emplacement** – Indique si le paramètre est défini dans **Systèmes virtuels**. • **Emplacement** – Le nom du système virtuel sur lequel le paramètre est défini. La colonne affiche **Partagé** pour les paramètres qui ne sont pas spécifiques à un système virtuel. • **Opérations** – Indique chaque opération (créer, modifier ou supprimer) exécutée sur le paramètre depuis la dernière validation.

Champ/Bouton	Description
	• **Propriétaire** – L’administrateur qui a effectué la dernière modification du paramètre. • **Sera enregistré** – Indique si l’opération d’enregistrement inclura le paramètre. • **Propriétaires précédents** – Les administrateurs qui ont apporté des modifications au paramètre avant la dernière modification. Vous pouvez éventuellement **Regrouper par** Nom de colonne (comme **Type**).
Save (Enregistrer)	Enregistre les modifications sélectionnées dans un fichier instantané de configuration : • Si vous avez sélectionné **Enregistrer toutes les modifications**, le pare-feu écrase le fichier instantané de configuration par défaut (.snapshot.xml). • Si vous avez sélectionné **Enregistrer les modifications effectuées par**, spécifiez le **Nom** d’un nouveau fichier de configuration ou d’un fichier de configuration existant et cliquez sur **OK**.

Annuler les modifications

Sélectionnez **Config (Configuration)** > **Revert Changes (Annuler les modifications)** en haut à droite du pare-feu ou de l’interface Web Panorama pour annuler les modifications apportées à la configuration candidate depuis la dernière validation. L’annulation des modifications restaure les paramètres en fonction des valeurs de la configuration en cours d’exécution. Vous pouvez filtrer les modifications de la configuration à annuler en fonction de l’administrateur ou de l’*emplacement*. L’emplacement peut être les systèmes virtuels spécifiques, des politiques et des objets partagés ou des paramètres de périphériques et de réseau partagés.

Vous ne pouvez pas annuler les modifications jusqu’à ce que le pare-feu ou Panorama finisse de traiter tous les engagements en attente ou en cours. Après avoir lancé le processus d’annulation, le pare-feu ou Panorama verrouille automatiquement le candidat et exécute les configurations afin que les autres administrateurs ne puissent pas modifier les paramètres ou effectuer de modifications. Après avoir terminé le processus d’annulation, le pare-feu ou Panorama supprime automatiquement le verrouillage.

La boîte de dialogue Annuler les modifications affiche les options décrites dans le tableau suivant :

Champ/Bouton	Description
Annuler toutes les modifications	Annule toutes les modifications pour lesquelles vous avez des privilèges administratifs (par défaut). Vous ne pouvez pas filtrer manuellement la portée des modifications de configuration que le pare-feu annule lorsque vous sélectionnez cette option. Au lieu de cela, le rôle d’administrateur affecté au compte que vous avez utilisé pour vous connecter détermine la portée de l’annulation : • **Rôle de super-utilisateur** – Le pare-feu annule les modifications de tous les administrateurs. • **Rôle personnalisé** – Les privilèges du profil de rôle administrateur affectés à votre compte déterminent la portée de l’annulation (voir Périphérique > Rôles administrateur). Si le profil inclut le privilège de **Valider pour les autres administrateurs**, le pare-feu annule les modifications configurées par tous les administrateurs. Si votre profil de rôle administrateur n’inclut pas le privilège de **Valider pour les autres administrateurs**, le pare-feu n’annule que vos modifications et non celles des autres administrateurs. *Dans les profils de rôle d’administrateur, les privilèges de validation s’appliquent également à l’annulation.* Si vous avez implémenté des domaines d’accès, le pare-feu applique automatiquement ces domaines pour filtrer la portée de l’annulation (voir Périphérique > Domaine d’accès). Indépendamment de votre rôle administratif, le pare-feu n’annule que les modifications de configuration dans les domaines d’accès affectés à votre compte.

Champ/Bouton	Description
Annuler les modifications effectuées par	Permet de filtrer la portée des modifications de configuration que le pare-feu annule. Le rôle administrateur affecté au compte que vous avez utilisé pour vous connecter détermine vos options de filtrage : • **Rôle de super-utilisateur** – Vous pouvez limiter la portée de l’annulation aux modifications apportées par des administrateurs spécifiques et aux modifications dans des emplacements spécifiques. • **Rôle personnalisé** – Les privilèges du profil de Rôle administrateur affecté à votre compte déterminent vos options de filtrage (voir Périphérique > Rôles administrateur). Si le profil inclut le privilège de **Valider pour les autres administrateurs**, vous pouvez limiter la portée de l’annulation aux modifications configurées par des administrateurs spécifiques et aux modifications dans des emplacements spécifiques. Si votre profil de Rôle administrateur n’inclut pas le privilège de **Valider pour les autres administrateurs**, vous pouvez limiter la portée de l’annulation uniquement aux modifications que vous avez effectuées dans des emplacements spécifiques. Filtrez la portée de l’annulation comme suit : • **Filtrer par administrateur** – Même si votre rôle permet d’annuler les modifications d’autres administrateurs, la portée de l’annulation inclut uniquement vos modifications par défaut. Pour ajouter d’autres administrateurs à la portée de l’annulation, cliquez sur le lien **<usernames>**, sélectionnez les administrateurs et cliquez sur **OK**. • **Filtrer par emplacement** – Sélectionnez les modifications dans des emplacements spécifiques pour les Inclure dans l’annulation. Si vous avez implémenté des domaines d’accès, le pare-feu filtre automatiquement la portée de l’annulation en fonction de ces domaines (voir Périphérique > Domaine d’accès). Quels que soient votre rôle administratif et vos choix de filtrage, la portée de l’annulation inclut uniquement les modifications de configuration dans les domaines d’accès affectés à votre compte.
Portée de l’annulation	Liste les emplacements qui ont des modifications à annuler. Que la liste inclue toutes les modifications ou un sous-ensemble de modifications dépend de plusieurs facteurs, comme décrit pour les options Annuler toutes les modifications et Annuler les modifications effectuées par. Les emplacements peuvent être l’un des éléments suivants : • **shared-object (objet partagé)** – Les paramètres qui sont définis dans l’emplacement Partagé.

Champ/Bouton	Description
	• **policy-and-objects (politique et objets)** – (Pare-feu uniquement) Règles de politique ou objets définis sur un pare-feu qui ne possède pas plusieurs systèmes virtuels. • **device-and-network (périphérique et réseau)** – (Pare-feu uniquement) Paramètres réseau et périphériques qui sont globaux (tels que les profils de gestion d’interface) et non spécifiques à un système virtuel. • **<virtual-system>** – (Pare-feu uniquement) Le nom du système virtuel dans lequel les règles ou objets de stratégie sont définis sur un pare-feu doté de plusieurs systèmes virtuels. Cela comprend également les paramètres réseau et de périphérique spécifiques à un système virtuel (par exemple, des zones). • **<device-group>** – (Panorama uniquement) Le nom du groupe de périphériques dans lequel les règles de politique ou les objets sont définis. • **<template>** – (Panorama uniquement) Le nom du modèle ou de la pile de modèles dans lequel les paramètres sont définis. • **<log-collector-group>** – (Panorama uniquement) Le nom du Groupe de collecteurs dans lequel les paramètres sont définis. • **<log-collector>** – (Panorama uniquement) Le nom du Collecteur de journaux dans lequel les paramètres sont définis.
Type d'emplacement	Cette colonne classe les emplacements où les modifications ont été apportées : • **Systèmes virtuels** – (Pare-feu uniquement) Les paramètres définis dans un système virtuel spécifique. • **Groupe de périphériques** – (Panorama uniquement) Les paramètres définis dans un groupe de périphériques spécifique. • **Modèle** – (Panorama uniquement) Les paramètres définis dans un modèle ou une pile de modèles spécifiques. • **Groupe de collecteurs de journaux** – (Panorama uniquement) Les paramètres spécifiques à une configuration de Groupe de collecteurs. • **Collecteur de journaux** – (Panorama uniquement) Les paramètres spécifiques à une configuration de Collecteur de journaux. • **Autres changements** – Paramètres qui ne sont pas spécifiques à l’une des zones de configuration précédentes (telles que les objets partagés).
Inclure dans l’annulation	Permet de sélectionner les modifications que vous souhaitez annuler. Par défaut, toutes les modifications de la **Portée d’annulation** sont sélectionnées. Cette colonne s’affiche uniquement après avoir choisi

Champ/Bouton	Description
(Annulation partielle uniquement)	d’**Annuler les modifications effectuées par** des administrateurs spécifiques. *Certaines dépendances peuvent affecter les modifications que vous incluez dans une annulation. Par exemple, si vous ajoutez un objet et un autre administrateur puis que vous modifiez cet objet, vous ne pouvez pas annuler votre modification sans annuler la modification pour l’autre administrateur.*
Regrouper par type d’emplacement	Liste les modifications de configuration dans la **Portée d’annulation** par **Type d’emplacement**.
Prévisualiser les modifications	Vous permet de comparer les configurations que vous avez sélectionnées dans la **Portée d’annulation** à la configuration en cours d’exécution. La fenêtre de prévisualisation utilise un code couleur pour indiquer quelles modifications sont des ajouts (en vert), des modifications (en jaune) ou des suppressions (en rouge). Pour vous aider à faire correspondre les modifications aux sections de l’interface Web, vous pouvez configurer la fenêtre de prévisualisation pour afficher **Lignes de contexte** avant et après chaque modification. Ces lignes proviennent des fichiers du candidat et des configurations en cours d’exécution que vous comparez. *Etant donné que les résultats de la prévisualisation s’affichent dans une nouvelle fenêtre, votre navigateur doit autoriser les fenêtres contextuelles. Si la fenêtre de prévisualisation ne s'ouvre pas, reportez-vous à la documentation de votre navigateur pour connaître les étapes permettant de débloquer l'ouverture des fenêtres contextuelles.*
Modifier le récapitulatif	Liste les paramètres individuels pour lesquels vous annulez les modifications. La liste **Récapitulatif des modifications** affiche les informations suivantes pour chaque paramètre : • **Nom de l’objet** – Le nom qui identifie la politique, l’objet, le paramètre réseau ou le paramètre de périphérique. • **Type** – Le type de paramètre (comme Adresse, règle de Sécurité ou Zone). • **Type d’emplacement** – Indique si le paramètre est défini dans **Systèmes virtuels**. • **Emplacement** – Le nom du système virtuel sur lequel le paramètre est défini. La colonne affiche **Partagé** pour les paramètres qui ne sont pas spécifiques à un système virtuel.

Champ/Bouton	Description
	• **Opérations** – Indique chaque opération (créer, modifier ou supprimer) exécutée sur le paramètre depuis la dernière validation. • **Propriétaire** – L’administrateur qui a effectué la dernière modification du paramètre. • **Sera annulé** – Indique si l’opération d’annulation inclut le paramètre. • **Propriétaires précédents** – Les administrateurs qui ont apporté des modifications au paramètre avant la dernière modification. Vous pouvez éventuellement **Regrouper par** Nom de colonne (comme **Type**).
Rétablir	Annule les modifications sélectionnées.

Configurations du verrouillage

Pour vous aider à coordonner les tâches de configuration avec d’autres administrateurs de pare-feu lors de sessions de connexion simultanées, l’interface Web vous permet de verrouiller la configuration ou la validation. Ainsi, aucun autre administrateur ne peut modifier la configuration ou valider des modifications jusqu’à suppression de ce verrou.

Dans le coin supérieur droit de l'interface Web, un cadenas verrouillé ( ) indique qu'un ou plusieurs verrous ont été activés (avec le nombre de verrous entre parenthèses) et un cadenas déverrouillé ( ) indique qu'aucun verrou n'a été activé. En cliquant sur le cadenas verrouillé ou déverrouillé, la boîte de dialogue Verrous s'ouvrira et fournira par le fait même les options et les champs suivants.

*Pour configurer le pare-feu afin d’activer automatiquement un verrou de validation chaque fois qu’un administrateur modifie la configuration candidate, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)**, modifiez les Paramètres généraux, activez **Automatically Acquire Commit Lock (Appliquer automatiquement un verrou de validation)**, puis cliquez sur **OK** et **Commit (Valider)**.*

*Lorsque vous annulez les modifications (**Config (Configuration)** > **Revert Changes (Annuler les modifications)**), le pare-feu verrouille automatiquement la configuration candidate et active afin que les autres administrateurs ne puissent ni éditer les paramètres ni valider des modifications. Le pare-feu supprime automatiquement le verrou une fois l’annulation terminée.*

Champ/Bouton	Description
Admin	Le nom d'utilisateur de l'administrateur qui a activé le verrou.
Location (Emplacement)	Sur un pare-feu possédant plus d'un système virtuel (vsys), la portée du verrou peut être un vsys spécifique ou l'emplacement Partagé.
Type	Voici les différents types de verrous : • **Verrou de configuration** : empêche d'autres administrateurs de modifier la configuration candidate. Seuls un super utilisateur ou l'administrateur qui a activé le verrou peuvent le retirer. • **Verrou de validation** – Empêche d’autres administrateurs de valider des modifications apportées à la configuration candidate. La file d'attente de validations n'accepte aucune nouvelle validation jusqu'à ce que tous les verrous aient été retirés. Ce verrou empêche l'occurrence de collisions qui peuvent se produire lorsque plusieurs administrateurs apportent des changements au cours de sessions de connexion simultanées, puis qu'un administrateur termine et lance une validation avant que les autres administrateurs aient terminé. Le pare-feu retire automatiquement le verrou après avoir terminé la validation pour laquelle l'administrateur avait activé le verrou. Un super utilisateur

Champ/Bouton	Description
	ou l'administrateur qui a activé le verrou peut également le retirer manuellement.
Commentaire	Saisissez un texte allant jusqu'à 256 caractères. Cette fonction est utile pour les autres administrateurs qui veulent connaître la raison de l'activation du verrou.
Créé à	La date et l'heure où un administrateur a activé le verrou.
Connecté(s)	Indique si l'administrateur ayant activé le verrou est actuellement connecté ou non.
Poser un verrou	Pour activer un verrou, cliquez sur **Take a Lock (Poser un verrou)**, sélectionnez le **Type**, sélectionnez le **Location (Emplacement)** (pare-feu à plusieurs systèmes virtuels), saisissez des **Comments (Commentaires)** facultatifs, cliquez sur **OK** puis vous pouvez **Close (Fermer)**.
Supprimer le verrouillage	Pour retirer un verrou, sélectionnez-le, cliquez sur **Remove Lock (Retirer le verrou)**, cliquez ensuite sur **OK**, puis sur **Close (Fermer)**.

Recherche globale

La recherche globale vous permet de rechercher une chaîne particulière, telle qu'une adresse IP, un nom d'objet, un nom de politique, un ID de menace, un UUID de règle ou un nom d'application, dans la configuration candidate sur un pare-feu ou Panorama. Les résultats de la recherche sont regroupés par catégorie et fournissent des liens vers l’emplacement de la configuration dans l’interface Web, de manière à pouvoir trouver facilement tous les endroits où la chaîne existe ou a été référencée.

Pour lancer la recherche globale, cliquez sur l’icône de **Recherche**  située en haut à droite de l’interface Web. La Recherche globale est disponible à partir de toutes les pages et de tous les emplacements de l’interface Web. Voici une liste des fonctionnalités de la recherche globale qui vous permettront d'effectuer des recherches réussies :

- Si vous initiez une recherche sur un pare-feu avec plusieurs systèmes virtuels ou si les rôles administrateur sont définis, la Recherche globale renvoie uniquement les résultats pour les zones du pare-feu pour lesquelles vous disposez d’autorisations. Il en va de même pour les groupes de périphériques Panorama ; vous verrez les résultats de la recherche uniquement pour les groupes de périphériques pour lesquels vous disposez d’un accès administratif.
- Les espaces dans le texte de la recherche sont traités comme des opérations ET. Par exemple, si vous recherchez`corp policy`, à la fois **entreprise** et **politique** doivent exister dans l’élément de configuration pour qu’il soit inclus dans les résultats de la recherche.
- Pour rechercher une expression exacte, mettez-la entre guillemets.
- Pour relancer une recherche précédente, cliquez sur Recherche globale et une liste des 20 dernières recherches s’affiche. Cliquez sur un élément de la liste pour relancer cette recherche. La liste d’historique de recherche est unique pour chaque compte administrateur.

Recherche globale est disponible pour chaque champ qui peut faire l’objet d’une recherche. Par exemple, dans le cas d'une politique de sécurité, vous pouvez faire porter la recherche sur les champs suivants : Nom, Étiquettes, Zone, Adresse, Utilisateur, Profil HIP, Application, UUID et Service. Pour effectuer une recherche, cliquez sur la liste déroulante à côté de l’un de ces champs, puis sur **Recherche globale**. Par exemple, si vous cliquez sur **Recherche globale** dans une zone nommée l3-vlan-trust, la Recherche globale recherche cette zone dans l’ensemble de la configuration et les résultats pour chaque emplacement où la zone est référencée sont renvoyés. Les résultats de la recherche sont regroupés par catégorie et vous pouvez pointer chaque élément avec la souris pour en afficher les détails ou cliquer sur un élément pour accéder sa page de configuration.

La Recherche globale ne recherche pas de contenu dynamique que le pare-feu affecte aux utilisateurs (comme les journaux, les plages d’adresses ou les adresses DHCP individuelles). Dans le cas de DHCP, vous pouvez faire porter la recherche sur un attribut de serveur DHCP, tel que l'entrée NS, mais vous ne pouvez pas rechercher d'adresses émises pour les utilisateurs. Un autre exemple est les noms d’utilisateur que le pare-feu collecte lorsque vous activez la fonctionnalité User-ID ™. Dans ce cas, un nom d’utilisateur ou un groupe d’utilisateurs existant dans la base de données User-ID peut faire l’objet d’une recherche uniquement si le nom ou le groupe existe dans la configuration, comme lorsqu’un nom de groupe d’utilisateurs est défini dans une politique. En général, vous pouvez rechercher uniquement du contenu que le pare-feu écrit dans la configuration.

Vous souhaitez en savoir plus ?

En savoir plus sur l’utilisation de la Recherche globale pour rechercher la configuration du pare-feu ou de Panorama.

Détails de la menace

- Surveillance > Journaux > Menace
- ACC > Activité des menaces
- Objets > Profils de sécurité > Antispyware / Protection contre les vulnérabilités

Utilisez la boîte de dialogue Détails de la menace pour en savoir plus sur les signatures de menaces qui équipent le pare-feu et les événements qui déclenchent ces signatures. Les détails de la menace sont fournis pour :

- Les journaux de menace qui enregistrent les menaces détectées par le pare-feu (**Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menace)**)
- Les principales menaces découvertes dans votre réseau (**ACC** > **Threat Activity (Activité des menaces)**)
- Les signatures de menaces que vous souhaitez modifier ou exclure de l’exécution (**Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware/Vulnerability Protection (Protection antispyware / contre les vulnérabilités)**)

Lorsque vous trouvez une signature de menace à propos de laquelle vous souhaitez en apprendre davantage, passez la souris sur le **Threat Name (Nom de la menace)** ou l’**ID** de menace et cliquez sur **Exception** pour examiner les détails de la menace. Les détails de la menace vous permettent de vérifier facilement si une signature de menace est configurée en tant qu’exception à votre politique de sécurité et de trouver les dernières informations relatives à l’Archivage sécurisé des menaces d’une menace spécifique. La base de données d’Archivage sécurisé des menaces de Palo Alto Networks est intégrée au pare-feu, ce qui vous permet de visualiser de plus amples détails sur les signatures de menaces dans le contexte du pare-feu ou de lancer une recherche d’Archivage sécurisé des menaces dans une nouvelle fenêtre de navigateur pour une menace enregistrée.

Selon le type de menace que vous visualisez, les détails incluent tous ou certains détails de la menace décrits dans le tableau suivant.

Détails de la menace	Description
Name (Nom)	Nom de la signature de menace.
ID	ID de signature de menace unique. Sélectionnez **View in Threat Vault (Afficher dans l’Archivage sécurisé des menaces)** pour ouvrir une recherche d’Archivage sécurisé des menaces dans une nouvelle fenêtre de navigateur et rechercher les dernières informations que la base de données des menaces de Palo Alto Networks détient pour cette signature. L’entrée d’Archivage sécurisé des menaces pour la signature de la menace peut inclure des détails supplémentaires, y compris les premières et dernières versions de contenu pour inclure les mises à jour de la signature et la version PAN-OS minimale requise pour prendre en charge la signature.
Description	Informations sur la menace qui déclenche la signature.

Détails de la menace	Description
Sévérité	Le niveau de gravité de la menace : informations, faible, moyen, élevé ou critique.
CVE	Failles de sécurité connues associées à la menace. L’identifiant des Failles et vulnérabilités communes (CVE) est l’identifiant le plus utile pour trouver des informations sur les vulnérabilités uniques, car les ID spécifiques aux fournisseurs incluent généralement de multiples vulnérabilités.
ID bugtraq	L’ID Bugtraq associée à la menace.
ID constructeur	L’identifiant spécifique au fournisseur d’une vulnérabilité. Par exemple, MS16-148 est l’ID de fournisseur pour une ou plusieurs vulnérabilités Microsoft et APBSB16-39 est l’ID de fournisseur pour une ou plusieurs vulnérabilités Adobe.
Référence	Les sources de recherche que vous pouvez utiliser pour en savoir plus sur la menace.
Profils d'exemption	Les profils de sécurité qui définissent une action d’application différente pour la signature de menace que l’action de signature par défaut. L’exception de menace n’est active que lorsque des profils d’exemption sont attachés à une règle de politique de sécurité (vérifiez si l’exception est Utilisée dans la règle de sécurité actuelle).
Utilisé dans la règle de sécurité en cours	Exceptions de menace actives – Une coche dans cette colonne indique que le pare-feu applique activement l’exception de menace (les Profils d’exemption qui définissent l’exception de menace sont attachés à une règle de politique de sécurité). Si cette colonne est décochée, le pare-feu applique la menace en se basant uniquement sur l’action de signature par défaut recommandée.
Exempter les adresses IP	Adresses IP d’exemption – Vous pouvez ajouter une adresse IP sur laquelle filtrer l’exception de menace ou afficher les **Exempt IP Addresses (Adresses IP d’exemption)** existantes. Cette option n’applique une exception de menace que lorsque la session associée comporte une adresse IP source ou de destination qui correspond à l’adresse IP d’exemption. Pour toutes les autres sessions, la menace est appliquée en fonction de l’action de signature par défaut.

Si vous rencontrez des difficultés pour afficher les détails de la menace, vérifiez les conditions suivantes :

- *La licence de Prévention contre les menaces du pare-feu est active (**Device (Périphérique)** > **Licenses (Licences)**).*
- *Les dernières mises à jour de contenu des Antivirus, des Menaces et des Applications sont installées.*
- *L’accès à l’Archivage sécurisé des menaces est activé (sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifier le paramètre **Logging and Reporting (Journalisation et génération de rapports)** sur **Enable Threat Vault Access (Activer l’accès à l’archivage sécurisé des menaces)**).*
- *Les valeurs par défaut (ou personnalisées) des* profils de sécurité Antivirus, Antispyware et Contre les vulnérabilités *sont appliquées à votre politique de sécurité.*

Récapitulatif d'AutoFocus Intelligence

Vous pouvez afficher un aperçu graphique des renseignements sur les menaces qu’AutoFocus compile pour vous aider à évaluer l’omniprésence et les risques des artefacts de pare-feu suivants :

- Adresse IP
- URL
- Domaine
- agent utilisateur (trouvé dans la colonne Agent utilisateur des Journaux de filtrage des données) ;
- nom de la menace (uniquement pour les menaces des sous-types de virus et du virus détectés par WildFire) ;
- Nome de fichier
- hash SHA-256 (trouvé dans la colonne résumé de fichier des journaux des soumissions WildFire).

Pour consulter la fenêtre Récapitulative d'AutoFocus Intelligence), vous devez d’abord avoir un abonnement actif à AutoFocus et activez les renseignements de menaces AutoFocus (sélectionnez **Périphérique** > **Configuration** > **Gestion** et modifiez les paramètres AutoFocus).

Après avoir activé les renseignements AutoFocus, placez votre souris sur un artefact de journal ou de la liste dynamique externe pour ouvrir le menu déroulant ( ), puis cliquez sur **AutoFocus** :

- afficher le Trafic, les Menaces, le Filtrage des URL, les Envois WildFire, le Filtrage des données et les Journaux unifiés (**Surveillance** > **Journaux**).
- afficher les entrées de la liste dynamique externe.

Vous pouvez également lancer la recherche AutoFocus à partir du pare-feu pour étudier d’avantage les artefacts intéressants ou suspects que vous trouvez.

Champ/Bouton	Description
Rechercher l’AutoFocus pour...	Cliquez pour lancer une recherche AutoFocus pour l’artefact.
Onglet Informations d’analyse	
Sessions	Le nombre de sessions privées dans lesquelles WildFire a détecté l’artefact. Les sessions privées sont celles qui s'exécutent uniquement sur les pare-feu associés à votre compte de support. Placez le curseur sur une barre de session pour afficher le nombre de sessions par mois.
Échantillons	Organisation et échantillons globaux (fichiers et liens d’e-mail) associés à l’artefact et regroupés par verdict de WildFire (bénins, indésirables, malveillants, hameçonnage). *Global* fait référence à des échantillons provenant de tous les envois WildFire, alors que *organisation* se réfère uniquement aux échantillons soumis à WildFire par votre organisation.

Champ/Bouton	Description
	Cliquez sur un verdict de WildFire pour lancer une recherche AutoFocus pour l’artefact filtré par portée (organisation ou mondiale) et le verdict de WildFire.
Étiquettes correspondantes	Étiquette AutoFocus qui correspondent à l’artefact : • **Étiquettes privés** – Visibles uniquement pour les utilisateurs AutoFocus associés à votre compte de support. • **Étiquettes publics** – Visibles pour tous les utilisateurs AutoFocus. • **Étiquettes de l’Unité 42** – Identifient les menaces et les campagnes constituant un risque direct relatif à la sécurité. Ces tags sont créées par l’Unité 42 (l’équipe de recherche et de renseignement sur les menaces de Palo Alto Networks). • **Étiquettes informationelles** – Étiquette de l’Unité 42 qui identifient les menaces touchant les produits informatiques. Placez le curseur sur une étiquette pour afficher la description de l’étiquette et d’autres détails concernant l’étiquette. Cliquez sur une étiquette pour lancer une recherche AutoFocus pour cette étiquette. Pour afficher plus d’étiquettes correspondantes pour un artefact, cliquez sur le symbole (...) pour lancer une recherche AutoFocus pour cet artefact. La colonne étiquette dans les résultats de recherche AutoFocus affiche plus d’étiquettes correspondantes pour l’artefact.
Onglet DNS passif L’onglet DNS passif affiche l’historique du DNS passif associé à l’artefact. Cet onglet affiche uniquement des informations correspondantes si l’artefact est une adresse IP, un domaine ou une URL.	
Requête	Le domaine qui a soumis une requête DNS. Cliquez sur le domaine pour lancer une recherche AutoFocus pour ce dernier.
Type	Le type de demande DNS (par exemple : A, NS, CNAME).
Réponse	L'adresse IP ou le domaine vers lequel la requête DNS a été résolue. Cliquez sur l’adresse IP ou le domaine pour lancer une recherche AutoFocus. *La colonne Réponse n’affiche pas d’adresses IP privées.*
Nombre	Le nombre de fois que la requête a été soumise.
Première apparition	La date et l’heure auxquelles la combinaison Requête, Réponse et Type a été vue pour la première fois en fonction de l’historique DNS passif.

Champ/Bouton	Description
Vu en dernier	La date et l’heure auxquelles la combinaison Requête, Réponse et Type a été vue le plus récemment en fonction de l’historique DNS passif.
Onglet Hachages correspondants L’onglet Hachages correspondants affiche les cinq échantillons privés les plus récents dans lesquels WildFire a détecté l’artefact. Les échantillons privés sont ceux qui sont détectés uniquement sur les pare-feu associés à votre compte de support.	
Sha256	Le hash SHA-256 pour un échantillon. Cliquez sur le hachage pour lancer une recherche AutoFocus pour ce hachage.
Type de fichier	Le type de fichier de l’échantillon.
Date de création	La date et l’heure auxquelles WildFire a analysé un échantillon et lui a affecté un verdict de WildFire.
Date de la mise à jour	La date et l’heure auxquelles WildFire a mis à jour le verdict de WildFire pour un échantillon.
Verdict	Le verdict de WildFire pour un échantillon : bénin, indésirable, malveillant ou hameçonnage.

Exportation du tableau de configuration

Les utilisateurs administratifs peuvent exporter les données qui figurent dans les bases de règles de politiques, les objets, les périphériques gérés et les interfaces dans un format tabulaire, soit dans un fichier PDF, soit dans un fichier CSV. Les données exportées sont celles qui sont visibles sur l’interface Web. Dans le cas de données filtrées, seules les données correspondant au filtre sont exportées. Si vous n’appliquez aucun filtre, tous les données sont exportées.

L’exportation vers un fichier PDF ne prend en charge que les descriptions en anglais.

Toutes les données de nature délicate, comme les mots de passe, sont masquées par des symboles génériques (*).

Un journal système et un lien de téléchargement sont générés lorsque l’exportation du tableau de configuration s’effectue avec succès. Utilisez le lien de téléchargement pour enregistrement le fichier PDF ou CSV localement. Après la fermeture de la fenêtre qui contient le lien de téléchargement, le lien de téléchargement de cette exportation n’est plus disponible.

Pour exporter des données du tableau, cliquez sur **PDF/CSV** et configurez les paramètres suivants :

Paramètres d'exportation	Description
Nom du fichier	Saisissez un nom (maximum de 200 caractères) pour identifier les données exportées. Ce nom devient le nom du fichier téléchargé qui est généré lors de l’exportation.
Type de fichier	Sélectionnez le type de résultats d’exportation à générer. Vous pouvez choisir le format PDF ou CSV.
Taille de la page	Par défaut, la taille de la page est définie sur lettre (8,5 sur 11,0 pouces). Vous ne pouvez pas modifier la taille de la page. Par défaut, le PDF est généré en orientation portrait et passe à l’orientation paysage pour permettre l’intégration du nombre maximal de colonnes.
Description (PDF seulement)	Saisissez une description (maximum de 255 caractères) pour fournir le contexte et des informations supplémentaires de l’exportation.
Données du tableau	Montre les données du tableau qui seront exportées. Si vous devez effacer les paramètres de filtrage qui vous avez définis précédemment, cliquez sur **Show All Columns (Afficher toutes les colonnes)** pour afficher toutes les règles de politique qui correspondent au type de politique sélectionné. Vous pouvez ensuite ajouter ou supprimer des colonnes et appliquer des filtres, au besoin.
Montrer toutes les colonnes	Supprime tous les filtres et affiche toutes les colonnes du tableau.

Cliquez sur **Exporter** pour générer le lien de téléchargement du tableau de configuration.

Modifier le mode de démarrage

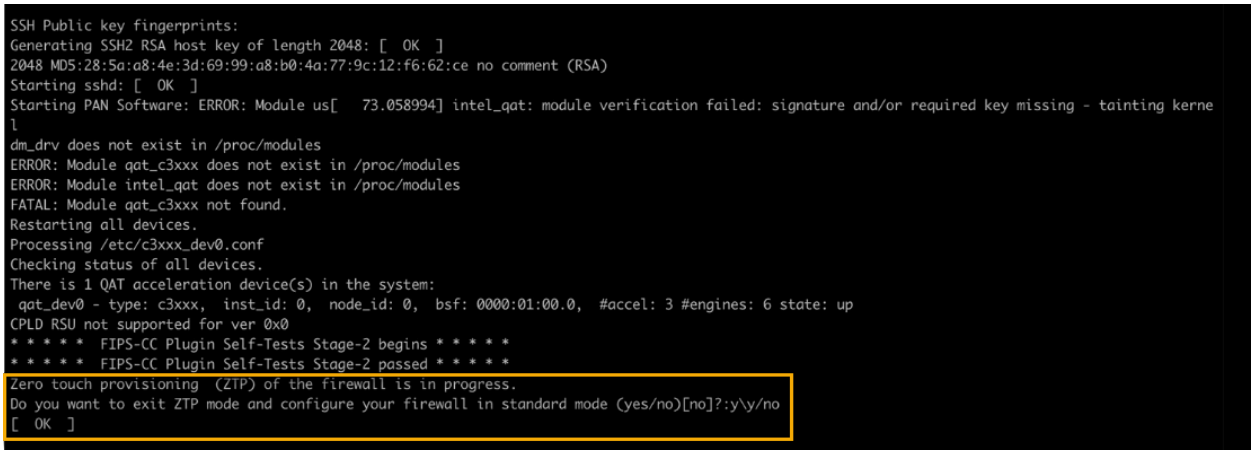
Certains pare-feu démarrent en mode Zero Touch Provisioning (ZTP) par défaut. Aucune saisie n'est requise au démarrage si vous optez pour une configuration ZTP. Si vous déployez un pare-feu non ZTP (standard), vous devez accéder à la CLI pour quitter le mode ZTP.

Vous devez avoir le plugin ZTP installé sur votre serveur de gestion Panorama pour accéder à la fonctionnalité ZTP.

STEP 1 | Après avoir allumé le pare-feu, utilisez un émulateur de terminal tel que PuTTY pour surveiller l'invite CLI suivante :

```
Voulez-vous quitter le mode ZTP et configurer votre pare-feu en
 mode standard (oui/non)[non] ?
```

Entrez **`oui`**. Le système vous demande alors de confirmer. Saisissez à nouveau **`yes (oui)`** pour démarrer le pare-feu en mode standard.



STEP 2 | (If you miss the above CLI prompt (Si vous manquez l'invite CLI ci-dessus)) Vous pouvez également modifier votre mode de démarrage à l'aide de l'interface Web. Accédez à l'écran de connexion du pare-feu à tout moment avant ou pendant le processus de démarrage. Une invite vous demande si vous souhaitez continuer à démarrer en mode ZTP ou si vous souhaitez passer en mode standard. Sélectionnez le **`Standard Mode (mode standard)`** et le pare-feu commence à redémarrer en mode standard.

STEP 3 | Configurez le pare-feu manuellement si vous utilisez le mode standard. Si vous utilisez le mode ZTP, le groupe de périphériques et la configuration du modèle définis sur le serveur de gestion Panorama sont automatiquement poussés vers le pare-feu par le service ZTP.

- (Standard Mode (Mode standard)) Remplacez l'adresse IP de votre ordinateur par une adresse du réseau 192.168.1.0/24, telle que 192.168.1.2. À partir d'un navigateur Web, accédez à https://192.168.1.1. Lorsque vous êtes invité, connectez-vous à l'appareil en utilisant le nom d'utilisateur par défaut et le mot de passe (admin / admin).
- (ZTP mode (mode ZTP)) Suivez les instructions fournies par votre administrateur Panorama pour enregistrer votre pare-feu ZTP. Vous devez saisir le numéro de série (numéro à 12 chiffres

identifié comme S/N) et la clé de réclamation (numéro à 8 chiffres). Ces numéros se trouvent sur des autocollants fixés à l'arrière de l'appareil.

Tableau de bord

Les widgets du Tableau de bord affichent les informations générales concernant le pare-feu ou Panorama™, comme la version du logiciel, l'état de chaque interface, l'utilisation des ressources et jusqu'à 10 entrées pour chaque type de journaux ; les widgets de journaux affichent les entrées depuis la dernière heure.

Le sujet Widgets du tableau de bord décrit la manière d'utiliser le Tableau de bord et décrit les widgets disponibles.

Widgets du tableau de bord

Par défaut, le **Tableau de bord** affiche les widgets dans une **Structure** à **3 colonnes**, mais vous pouvez personnaliser les **Tableaux de bord** pour afficher uniquement **2 colonnes**.

Vous pouvez également choisir les widgets à afficher ou à masquer pour visualiser uniquement ceux que vous souhaitez contrôler. Pour afficher un widget, sélectionnez une catégorie de widget à partir du menu déroulant **Widgets** et sélectionnez-en un pour l'ajouter au Tableau de bord (les noms des widgets qui apparaissent comme grisés sont déjà affichés). Vous pouvez cacher (cesser l'affichage) un widget en fermant celui-ci (✕ dans l'en-tête du widget). Les pare-feu et Panorama sauvegardent vos paramètres d'affichage des widgets au cours des connexions (connexion séparée pour chaque administrateur).

Veuillez vous référer à l'horodatage de la **Dernière mise à jour** pour déterminer quand les données du tableau de bord ont été actualisées pour la dernière fois. Vous pouvez actualiser manuellement l'ensemble du **Tableau de bord** (↻ dans le coin supérieur droit du Tableau de bord) ou vous pouvez actualiser les widgets individuels (↻ dans chaque en-tête de widget). Utilisez le menu déroulant sans référence à côté de l'option d'actualisation manuelle du Tableau de bord (↻) pour sélectionner l'intervalle d'actualisation automatique pour l'ensemble du **Tableau de bord** (en minutes) : **1 minute**, **2 minutes**, ou **5 minutes**; pour désactiver l'actualisation automatique de l'ensemble du **Tableau de bord**, sélectionnez **Actualisation manuelle**.

Widgets du tableau de bord	Description
Widgets Application	
Applications principales	Affiche les applications ayant le plus grand nombre de sessions. La taille du bloc indique le nombre relatif de sessions (passez la souris sur le bloc pour afficher le nombre correspondant) et la couleur indique les risques de sécurité ; vert pour des risques faibles et rouge pour des risques élevés. Cliquez sur une application pour afficher son profil d'application.
Applications principales à haut risque	Similaire à Principales applications, sauf que les applications présentant les risques les plus élevés avec la plupart des sessions sont affichées.
Facteur de risque de ACC	Affiche le facteur de risque moyen (entre 1 et 5) du trafic réseau traité au cours de la semaine passée. Plus la valeur est élevée, plus le risque est important.
Widgets Système	
Informations générales	Affiche le nom et le modèle du pare-feu ou de Panorama, le processeur et la mémoire vive de Panorama, le mode du système de Panorama, la version logicielle de PAN-OS® ou de Panorama, les informations de gestion IPv4 et IPv6, le numéro de série, l'ID de CPU et l'UUID, les versions des définitions des applications, du trafic, des menaces et du filtrage des URL, la date et l'heure actuelles et la période de temps depuis le dernier redémarrage.

Widgets du tableau de bord	Description
Interfaces (Pare-feu uniquement)	Indique si chaque interface est active (vert), inactive (rouge) ou si son état est inconnu (gris). Les interfaces qui prennent en charge l'alimentation par Ethernet (PoE) sont marquées d'une icône représentant un éclair. Passer le curseur de la souris sur une interface affiche la configuration de la liaison et les informations d'état. Des détails supplémentaires tels que la vitesse de liaison, le duplex de liaison et les informations PoE sont affichés en fonction du type de port.
Ressources système	Affiche la Gestion de l'utilisation du processeur, l'utilisation du Panneau de données et le Nombre de sessions (le nombre de sessions établies via le pare-feu ou Panorama).
Haute disponibilité	Si la haute disponibilité (HD) est activée, il indique l'état HD du pare-feu / Panorama local et homologue ; vert (actif), jaune (passif) ou noir (autre). Pour plus d'informations sur la HD, reportez-vous à la section Device > High Availability (Appareil > Haute disponibilité) ou Panorama > High Availability (Panorama > Haute disponibilité).
Cluster HA	Lorsque le cluster HA est activé, indique les statistiques du cluster ainsi que la valeur Keep Alive pour les liens HA4 et HA4_backup pour chaque membre du cluster.
Verrous	Montre les verrous de configuration qui ont été établis par les administrateurs.
Administrateurs connectés	Affiche l'adresse IP source, le type de session (interface Web ou CLI) et l'heure de début de session pour chaque administrateur actuellement connecté.
Budget d'alimentation PoE (Pare-feu pris en charge uniquement)	Affiche le bilan de puissance total et la puissance totale allouée des interfaces configurées lors de l'utilisation de l'alimentation par Ethernet. Le graphique en anneau confirme l'alimentation disponible sur le pare-feu et vous aide à décider quels périphériques alimentés (PD) connecter aux ports PoE.
Widgets Journaux	
Journaux des menaces	Affiche l'ID de menace, l'application, ainsi que la date et l'heure des 10 dernières entrées du journal des menaces. L'ID de menace correspond à la description ou à l'URL d'un site malveillant qui va à l'encontre du profil de filtrage des URL. Seules les entrées des 60 dernières minutes sont affichées.
Journaux de filtrage des URL	Affiche la description, ainsi que la date et l'heure des 60 dernières minutes du journal de filtrage des URL.
Journaux de filtrage des données	Affiche la description, ainsi que la date et l'heure des 60 dernières minutes du journal de filtrage des données.

Widgets du tableau de bord	Description
Journaux de configuration	Affiche le nom d'utilisateur de l'administrateur, le client (interface Web ou CLI), ainsi que la date et l'heure des 10 dernières entrées du journal de configuration. Seules les entrées des 60 dernières minutes sont affichées.
Journaux systèmes	Affiche la description, ainsi que la date et l'heure des 10 dernières entrées du journal système. *Une entrée « Configuration installée » indique que les modifications apportées à la configuration ont été correctement validées. Seules les entrées des 60 dernières minutes sont affichées.*

ACC

Le centre de commande de l’application (ACC) est un outil analytique qui fournit des renseignements exploitables concernant l’activité sur votre réseau. L’ACC utilise les journaux du pare-feu pour représenter graphiquement les tendances du trafic sur votre réseau. Cette représentation graphique vous permet d'interagir avec les données et de visualiser les relations entre les événements sur le réseau, notamment les modèles d'utilisation réseau, les modèles de trafic, les activités suspectes et les anomalies.

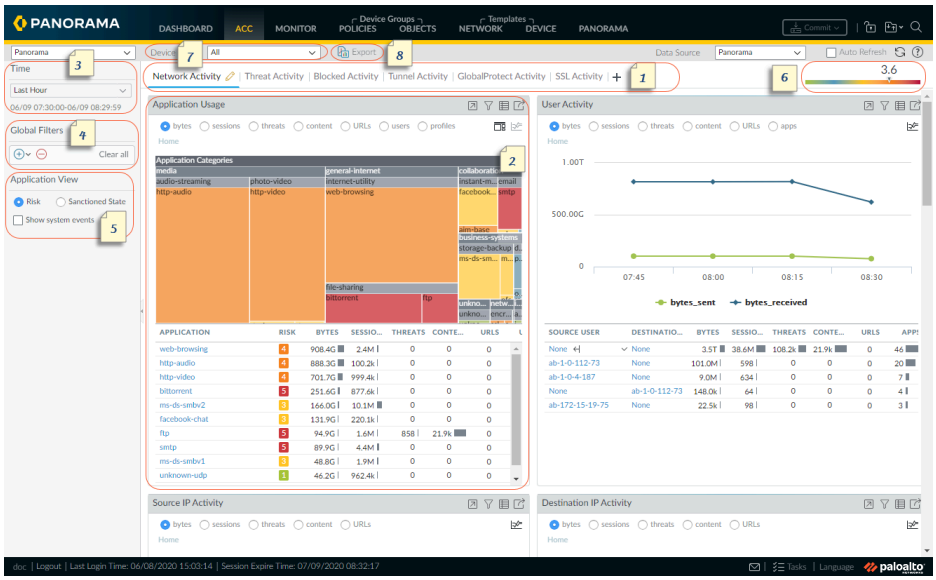
- Aperçu de l’ACC
- Onglets de l’ACC
- Widgets de l’ACC
- Actions de l’ACC
- Utilisation des onglets et des widgets
- Utilisation des filtres – Filtres locaux et filtres généraux

Vous souhaitez en savoir plus ?

Reportez-vous à la section Utilisation du centre de commande de l’application.

Aperçu de l’ACC

Le tableau suivant affiche l’onglet ACC et décrit chaque composant.

Aperçu de l’ACC


1	**Onglets**	L’ACC comprend des onglets prédéfinis qui offrent une visibilité sur le trafic réseau, l’activité des menaces, les activités bloquées, l’activité du tunnel et l’activité du réseau mobile (si la sécurité GTP est activée). Pour plus d’informations sur chaque onglet, reportez-vous à la section Onglets ACC.
2	**Widgets**	Chaque onglet inclut un ensemble de widgets par défaut qui représentent le mieux les événements et les tendances associés à l’onglet. Les widgets vous permettent d’examiner les données à l’aide des filtres suivants : nombre d’octets (entrants et sortants), sessions, contenu (fichiers et données), catégories d’URL, applications, utilisateurs, menaces (malveillantes, bénignes, indésirables, hameçonnage) et nombre. Pour plus d’informations sur chaque widget, reportez-vous à la section Widgets ACC.
3	**Période**	Les diagrammes et les graphiques de chaque widget fournissent un affichage en temps réel de l’historique. Vous pouvez choisir un intervalle personnalisé ou utiliser une période prédéfinie, allant des 15 dernières minutes aux 90 derniers jours ou aux 30 derniers jours calendaires. La période utilisée pour effectuer le rendu des données est, par défaut, la dernière heure. Les intervalles de date et d’heure sont affichés à l’écran. Par exemple : `11/11 10:30:00-01/12 11:29:59`

Aperçu de l’ACC		
4	**Filtres Globaux**	Les filtres généraux vous permettent de définir un filtre pour tous les onglets. Les diagrammes et les graphiques appliquent les filtres sélectionnés avant d’effectuer le rendu des données. Pour plus d’informations sur l’utilisation des filtres, reportez-vous à la section Actions ACC.
5	**Affichage des applications par**	L’affichage de l’application vous permet de filtrer la vue ACC soit par les applications approuvées et non approuvées utilisées sur votre réseau, soit par le niveau de risque des applications utilisées sur votre réseau. Le vert indique les applications approuvées, le bleu les applications non approuvées et le jaune indique les applications qui ont un état d’approbation différent au sein de différents systèmes virtuels ou groupes de périphériques.
6	**Échelle de risque**	L’échelle de risque allant de 1 (risque le plus faible) à 5 (risque le plus élevé) indique le risque de sécurité relatif sur votre réseau. L’échelle de risque utilise différents facteurs, tels que le type des applications vues sur le réseau et les niveaux de risque associés aux applications, l’activité des menaces et les logiciels malveillants via le nombre de menaces bloquées, ainsi que les hôtes compromis ou le trafic vers les hôtes et les domaines malveillants.
7	**Source**	Les données utilisées pour l’affichage varient entre le pare-feu et Panorama™. Les options suivantes sont à votre disposition pour sélectionner les données utilisées pour générer les vues sur l’ACC : **Système virtuel** : sur un pare-feu qui est activé pour plusieurs systèmes virtuels, vous pouvez utilisez le menu déroulant **Système virtuel** pour modifier l’affichage ACC pour inclure tous les systèmes virtuels ou seulement une sélection de systèmes virtuels. **Groupe de périphériques**: sur Panorama, vous pouvez utiliser le menu déroulant **Groupe de périphériques** pour modifier l’affichage ACC pour inclure des données provenant de tous les groupes de périphériques ou uniquement d’une sélection de groupes de périphériques. **Source de données** : sur Panorama, vous pouvez également modifier l’affichage pour utiliser **Panorama** ou les **Données du périphérique distant** (données du pare-feu géré). Lorsque la source de données est **Panorama**, vous pouvez filtrer l’affichage pour un groupe de périphériques spécifique.
8	**Exporter**	Vous pouvez exporter les widgets affichés dans l’onglet actif au format PDF.

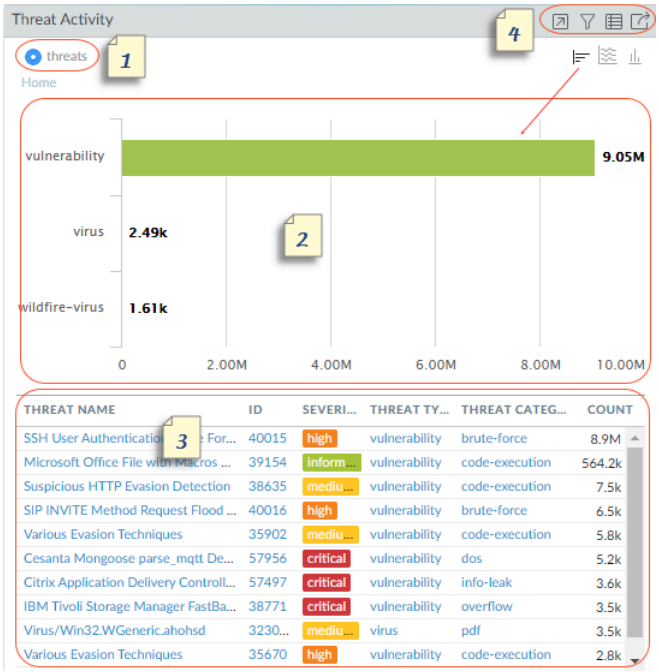
Onglets de l’ACC

- **Activité du réseau** – Affiche une vue d’ensemble du trafic et de l’activité des utilisateurs sur votre réseau. Cette vue se concentre sur les applications les plus utilisées, les principaux utilisateurs qui génèrent du trafic en examinant le nombre d'octets, le contenu, les menaces et les URL consultées par les utilisateurs, et les règles de politique de sécurité les plus utilisées auxquelles le trafic correspond. De plus, vous pouvez afficher l'activité réseau par zone source ou de destination, région, adresse IP, interface d'entrée ou de sortie et par information sur l'hôte, notamment les systèmes d'exploitation des périphériques les plus couramment utilisés sur le réseau.
- **Activité des menaces** – Affiche une vue d’ensemble des menaces sur le réseau. Il se concentre sur les principales menaces : vulnérabilités, logiciels espions, virus, hôtes visitant des domaines ou URL malveillants, principaux envois WildFire par type de fichier et application, et applications qui utilisent des ports non standard. Le widget Hôtes compromis complète la détection par de meilleures techniques de visualisation. Il utilise les informations de l’onglet Événements corrélés (Surveillance > Moteur de corrélation automatique > Événements corrélés) pour présenter une vue agrégée des hôtes compromis sur votre réseau par utilisateurs source ou adresses IP, triés par gravité.
- **Activités bloquées** – Se concentre sur le trafic dont l’entrée sur le réseau a été empêchée. Les widgets de cet onglet vous permettent d'afficher l'activité refusée par nom d'application, nom d'utilisateur, nom de menace, contenu (fichiers et données) et les principales règles de sécurité dont l'action de refus a bloqué le trafic.
- **Activité du réseau mobile** – Affiche une représentation visuelle du trafic mobile sur votre réseau à l’aide des journaux GTP générés à partir de votre configuration de la règle de politique de sécurité. Cette vue comprend des widgets interactifs et personnalisables d’Événements GTP, d’Activité de l’abonné mobile et de Causes de rejet GTP auxquels vous pouvez appliquer des Filtres de l’ACC et descendre dans la hiérarchie pour isoler les informations dont vous avez besoin. Lorsque vous activez la Sécurité SCTP, les widgets de cet onglet affiche une représentation visuelle et les détails des événements SCTP sur le pare-feu, de même que le nombre de blocs envoyés et reçus par ID d’association SCTP.
- **Activité du tunnel** – Affiche l’activité du trafic du tunnel que le pare-feu a inspecté en fonction de vos politiques d’inspection du tunnel. Les informations incluent l’utilisation du tunnel en fonction de l’ID de tunnel, de la balise de surveillance, de l’utilisateur et des protocoles de tunnel tels que l’Encapsulation générique de routage (GRE), le Protocole de tunnel de type GPRS (General Packet Radio Service) pour les Données utilisateur (GTP-U) et le protocole IPSec non crypté.
- **Activité GlobalProtect** – Affiche une vue d’ensemble de l’activité des utilisateurs de votre déploiement GlobalProtect. Les informations incluent le nombre d’utilisateurs et le nombre de fois que les utilisateurs se sont connectés, les passerelles auxquelles les utilisateurs se sont connectés, le nombre d’échecs de connexion ainsi que la raison de l’échec, un récapitulatif des méthodes d’authentification et les versions de l’application GlobalProtect utilisées, ainsi que le nombre de postes en quarantaine.
- **Activité SSL** : Affiche l’activité du trafic TLS/SSL décrypté et non décrypté sur la base des profils et des politiques de décryptage. Vous pouvez voir l’activité TLS par rapport à l’activité non TLS, la quantité de trafic déchiffré par rapport à la quantité de trafic non déchiffré, les motifs des échecs de déchiffrement et la version TLS qui a réussi et l’activité d’échange de clé. Utilisez ces informations pour identifier le trafic qui cause des problèmes de cryptage puis utilisez le Journal de déchiffrement et les modèles de rapport de déchiffrement personnalisés pour afficher les détails obtenir le contexte sur le trafic afin de pouvoir diagnostiquer et régler les problèmes correctement.

Vous pouvez également personnaliser les onglets et les widgets, comme décrit dans la rubrique Utilisation des onglets et des widgets*.*

Widgets de l’ACC

Les widgets de chaque onglet sont interactifs. Vous pouvez définir des filtres et obtenir un affichage détaillé en la personnalisant et en l’axant sur les informations dont vous avez besoin.



Chaque widget est structuré pour afficher les informations suivantes :

1	**Vue**	Vous pouvez trier les données par nombre d’octets, sessions, menaces, nombre, utilisateurs, contenu, applications, URL, caractère malveillant, bénin, indésirable, de hameçonnage, (nom de)fichiers, données, profils, objets, portails et passerelles. Les options disponibles varient selon le widget.
2	**Graphique**	Les options d'affichage graphique sont arborescence, graphique linéaire, graphique à barres horizontales, graphique à aires empilées, graphique à barres empilées, graphiques en camembert et carte. Les options disponibles varient selon le widget et l’interactivité varie selon le type de graphique. Par exemple, le widget Applications utilisant des ports non standard vous permet de choisir entre une arborescence et un graphique linéaire. Pour obtenir un affichage détaillé, cliquez sur le graphique. La zone sur laquelle vous cliquez devient un filtre et vous permet de faire un zoom avant et d’afficher des informations plus granulaires sur cette sélection.
3	**Tableau**	La vue détaillée des données utilisées pour effectuer un rendu du graphique s’affiche dans une table sous le graphique. Vous pouvez cliquer et définir un filtre local ou général pour les éléments de la table. Avec un filtre local le graphique est mis à jour et la table est triée selon ce filtre.

		Avec un filtre général, la vue de l'ACC pivote de manière à afficher uniquement les informations spécifiques à votre filtre.
4	**Actions**	Voici les actions disponibles dans la barre de titre d'un widget : • **Agrandir la vue**: permet d'agrandir le widget et de l'afficher dans un espace d'écran plus grand. Dans la vue agrandie, vous pouvez voir d'autres éléments que les dix principaux qui s'affichent dans l'écran du widget par défaut. • **Définir les filtres locaux** – Vous permet d'ajouter des filtres qui précisent l'affichage au sein du widget. Reportez-vous à Utilisation des filtres – Filtres locaux et filtres généraux. • **Accéder aux journaux** - Vous permet d'accéder directement aux journaux (**Surveillance** > **Journaux** > **<log-type>**). Les journaux sont filtrés en fonction de la période pour laquelle le graphique est rendu. Si vous définissez des filtres locaux et globaux, la requête de journal concatène la période et les filtres et affiche uniquement les journaux qui correspondent à votre jeu de filtres. • **Exporter (Export)** : permet d'exporter le graphique au format PDF.

Pour une description de chaque widget, reportez-vous aux détails de la section utilisation de l'ACC.

Actions de l’ACC

Pour personnaliser et préciser l'affichage de l'ACC, vous pouvez ajouter et supprimer des onglets et des widgets, définir des filtres locaux et généraux, et interagir avec les widgets.

- Utilisation des onglets et des widgets
- Utilisation des filtres – Filtres locaux et filtres globaux

Utilisation des onglets et des widgets

Les options suivantes décrivent comment utiliser et personnaliser les onglets et les widgets.

- Ajout d'un onglet personnalisé.
  1. Sélectionnez Ajouter (＋) dans la liste des onglets.
  2. Ajoutez un **View Name (Nom de vue)**. Ce nom sera utilisé comme nom d'onglet. Vous pouvez ajouter jusqu’à 10 onglets personnalisés.

- Modifier un onglet.

  Sélectionnez l'onglet et cliquez sur Modifier à côté du nom de l'onglet pour le modifier.

  Exemple : 

  .

- Définir l’onglet par défaut
  1. Modifier un onglet.
  2. Sélectionnez pour définir l’onglet actuel comme valeur par défaut. Chaque fois que vous vous connectez au pare-feu, cet onglet s’affiche.

- Enregistrer l’état de l’onglet
  1. Modifier un onglet.
  2. Sélectionnez pour enregistrer vos préférences dans l’onglet actuel en tant que valeurs par défaut.

     L’état de l’onglet, y compris les filtres que vous auriez pu configurer, est synchronisé entre les paires HD.

- Exporter un onglet
  1. Modifier un onglet.
  2. Sélectionnez pour exporter l’onglet actuel. L’onglet se télécharge sur votre ordinateur en tant que fichier .txt. Vous devez activer les fenêtres contextuelles pour télécharger le fichier.

- Importer un onglet
  1. Ajout d'un onglet personnalisé.
  2. Sélectionnez pour importer un onglet.
  3. Recherchez le fichier texte (.txt) et sélectionnez-le.

- Affichage des widgets inclus dans une vue.
  1. Sélectionnez la vue et cliquez sur Modifier ( ).
  2. Sélectionnez la liste déroulante **Add Widgets (Ajouter des widgets)** pour revoir les widgets sélectionnés.

- Ajout d'un widget ou d'un groupe de widgets
  1. Ajoutez un nouvel onglet ou modifiez un onglet prédéfini.
  2. Sélectionnez **Add Widget (Ajouter un widget)**, puis cochez la case correspondant au widget que vous souhaitez ajouter. Vous pouvez sélectionner un maximum de 12 widgets.
  3. (Facultatif) Pour créer un modèle à 2 colonnes, sélectionnez **Ajouter un Groupe de widgets**. Vous pouvez faire glisser et déposer des widgets dans l'affichage à deux colonnes. Lorsque vous faites glisser le widget sur le modèle, un espace réservé s'affiche et vous permet de déposer le widget.

     Vous ne pouvez pas nommer de groupe de widgets.

- Supprimer l'onglet, le widget ou le groupe de widgets.
  - Pour supprimer un onglet personnalisé, sélectionnez l'onglet et cliquez sur Supprimer (Test).

    Vous ne pouvez pas supprimer d'onglet prédéfini.

  - Pour supprimer un widget ou un groupe de widgets, modifiez l'onglet, puis cliquez sur Supprimer ([X]). Vous ne pouvez pas annuler une suppression.

- Réinitialisation de la vue par défaut

  Dans une vue prédéfinie, telle que la vue **Blocked Activity (Activité bloquée)**, vous pouvez supprimer un ou plusieurs widgets. Si vous souhaitez réinitialiser le modèle pour inclure l'ensemble de widgets par défaut de l'onglet, modifiez l'onglet et cliquez sur **Reset View (Réinitialiser la vue)**.

Utilisation des filtres – Filtres locaux et filtres généraux

Pour accéder aux détails et contrôler avec précision l'affichage de l'ACC, vous pouvez utiliser les filtres.

- **Filtres locaux** - ils sont appliqués à un widget spécifique. Un filtre local vous permet d'interagir avec le graphique et de personnaliser l'affichage de manière à pouvoir accéder aux détails et accéder aux informations que vous souhaitez surveiller sur un widget spécifique. Vous pouvez appliquer un filtre local de deux façons : en cliquant sur un attribut dans le graphique ou la table, ou en sélectionnant l'option **Définir le filtre** dans un widget. **Définir un filtre** vous permet de définir un filtre local persistant au redémarrage.
- **Filtres généraux** - ils sont appliqués à l'ensemble de l'ACC. Un filtre général vous permet de pivoter l'affichage sur les détails qui vous importent le plus et d'exclure les informations sans rapport de l'affichage actif. Par exemple, pour afficher tous les éléments relatifs à un utilisateur et une application spécifiques, vous pouvez appliquer l'adresse IP de l'utilisateur et spécifier l'application pour créer un filtre général qui affiche uniquement les informations qui se rapportent à cet utilisateur et cette

application via tous les onglets et les widgets dans l'ACC. Les filtres généraux ne sont pas persistants au cours des connexions.

Les filtres généraux peuvent être appliqués de trois façons :

- **Définir un filtre général à partir d'une table** : sélectionnez un attribut dans la table d'un widget et appliquez-le comme filtre général.
- **Ajouter un filtre widget comme filtre général** – Placez la souris sur l'attribut et cliquez sur l'icône en forme de flèche qui se trouve à droite de l'attribut. Cette option vous permet d'élever un filtre local utilisé dans un widget et d'appliquer l'attribut globalement de sorte que l'affichage de l'ensemble des onglets de l'ACC soit mis à jour.
- **Définition d'un filtre général** : définissez un filtre à l'aide du volet **Global Filters (Filtres généraux)** de l'ACC.

- Définition d'un filtre local.

  Vous pouvez également cliquer sur un attribut dans la table sous le graphique pour l'appliquer comme filtre local.

  1. Sélectionnez un widget et cliquez sur Filtre ( ).
  2. Ajoutez ( ) les filtres que vous souhaitez appliquer.
  3. Cliquez sur **Apply (Appliquer)**. Ces filtres sont persistants au redémarrage.

     Le nombre de filtres locaux appliqués à un widget est indiqué en regard de son nom.

- Définissez un filtre général à partir d'une table.

  Placez la souris sur un attribut d'un tableau et cliquez sur la flèche qui apparaît à droite de l'attribut.

- Définissez un filtre général à l'aide du volet Filtres généraux.

  Ajoutez ( ) les filtres que vous souhaitez appliquer.

- Promotion d'un filtre local comme filtre général
  1. Dans n'importe quelle table d'un widget, sélectionnez un attribut pour le définir comme filtre local.
  2. Pour promouvoir le filtre comme filtre général, placez la souris sur l'attribut et cliquez sur la flèche qui se trouve à droite de l'attribut.

- Supprimez un filtre.

  Cliquez sur Supprimer ( ) pour supprimer un filtre.

  - **Filtres généraux** - Cette option se trouve dans le volet Filtres généraux.
  - **Filtres locaux** - Cliquez sur Filtre ( ) pour faire apparaître la boîte de dialogue Définir les filtres locaux, puis sélectionnez le filtre et supprimez-le.

- Effacez tous les filtres.
  - **Filtres généraux** - **Clear all (Effacer tous)** les filtres généraux.
  - **Filtres locaux** - Sélectionnez un widget et cliquez sur Filtre ( ). Puis cliquez sur **Clear all (Effacer tous)** dans le widget Définir les filtres locaux.
- Refus de filtres.

  Sélectionnez un attribut et Refusez ( ) un filtre.
  - **Filtres généraux** - Cette option se trouve dans le volet Filtres généraux.
  - **Filtres locaux** - Cliquez sur Filtre ( ) pour faire apparaître la boîte de dialogue Définir les filtres locaux, ajoutez un filtre, puis refusez-le.
- Affichage des filtres en cours d'utilisation.
  - **Filtres généraux** - Le nombre de filtres généraux appliqués est affiché dans le volet de gauche sous Filtres généraux.
  - **Filtres locaux** - Le nombre de filtres locaux appliqués à un widget est affiché en regard de son nom. Pour afficher les filtres, cliquez sur **Définir les filtres locaux**.

surveiller

Les rubriques suivantes décrivent les journaux et les rapports du pare-feu que vous pouvez utiliser pour surveiller l’activité sur votre réseau :

- Surveillance > Journaux
- Surveillance > External Logs
- Surveillance > Moteur de corrélation automatique
- Surveillance > Capture de paquets
- Surveillance > App-Scope
- Surveillance > Navigateur de session
- Surveillance > Liste d’interdiction d’adresses IP
- Surveillance > Botnet
- Surveillance > Rapports au format PDF
- Surveillance > Gérer des rapports personnalisés
- Surveillance > Rapports

Surveillance > Journaux

Les rubriques suivantes fournissent des informations supplémentaires sur les journaux de surveillance.

Que voulez-vous savoir ?	Reportez-vous à la section :
Parlez-moi des différents types de journaux.	Types de journaux
Journaux de filtrage. Journaux d'exportation. Afficher les détails des entrées des journaux. Modifier l'affichage des journaux.	Actions des journaux
Vous souhaitez en savoir plus ?	Surveillance et gestion des journaux.

Types de journaux

- **Surveiller** > **Journaux**

Le pare-feu affiche tous les journaux afin que les autorisations d'administration basées sur les rôles soient respectées. Seules les informations que vous avez la permission de voir sont visibles, ce qui varie selon les types de journaux que vous visualisez. Pour plus d'informations sur les autorisations d'administrateur, reportez-vous à Périphérique > Rôles administrateur.

Type de journal	Description
Trafic	Affiche une entrée au début et à la fin de chaque session. Chaque entrée contient la date et l'heure, les zones source et de destination, des adresses et des ports, le nom de l'application, le nom de la règle de sécurité appliquée au flux, l'action de la règle (**allow (autoriser)**, **deny (refuser)** ou **drop (supprimer)**), l'interface d'entrée et de sortie, ainsi que le nombre d'octets et le motif de fin de session. La colonne Type indique si l'entrée correspond au début ou à la fin d'une session, ou si la session a été refusée ou supprimée. Une « suppression » indique que la règle de sécurité qui bloquait le trafic a défini « n'importe quelle » application, alors qu'un « refus » indique que la règle a identifié une application spécifique. Si le trafic est supprimé avant d'avoir identifié l'application, comme lorsqu'une règle supprime l'ensemble du trafic d'un service spécifique, l'application affiche « non applicable ».

Type de journal	Description
	Examinez les journaux du trafic pour obtenir plus de détails sur les entrées, les artefacts et ls actions individuels : • Cliquez sur Détails () pour afficher des détails supplémentaires concernant une session, à savoir si une entrée ICMP regroupe plusieurs sessions entre une même source et destination (la valeur **Count (Nombre)** sera supérieure à 1). • Sur un pare-feu doté d'une licence AutoFocus™ active, pointez à côté d'une adresse IP, d'un nom de fichier, d'une URL, d'un agent utilisateur, d'un nom de menace ou d'un hachage contenu dans une entrée de journal et cliquez sur la liste déroulante () pour ouvrir le Récapitulatif des renseignements sur les menaces AutoFocus pour l'artefact. • Pour ajouter un périphérique à la liste de quarantaine (**Device (Périphérique)** > **Device Quarantine (Quarantaine du périphérique)**), ouvrez le menu déroulant **Host ID (ID de l'hôte)** et recherchez le périphérique puis cliquez sur **Block Device (Bloquer le périphérique) (** (dans la boîte de dialogue qui apparait).
Prévention	Affiche une entrée pour chaque alarme de sécurité générée par le pare-feu. Chaque entrée inclut la date et l'heure, le nom ou l'URL d'une menace, les zones sources et de destination, des adresses et des ports, le nom d'une application, le nom de la règle de sécurité appliquée au flux ainsi que l'action de l'alarme (**allow (autoriser)** ou **block (bloquer)**) et sa gravité. La colonne Type indique le type de menace, comme « virus » ou « logiciel espion ». La colonne Nom présente la description de la menace ou l'URL. Quant à la colonne Catégorie, elle correspond à la catégorie de menace (comme « un enregistreur de frappe ») ou la catégorie d'URL. Explorez les journaux des menaces pour obtenir de plus amples détails sur chaque entrée et artefact : • Cliquez sur () pour afficher des détails supplémentaires concernant une menace, à savoir si une entrée regroupe plusieurs menaces du même type entre une même source et destination (la valeur **Count (Nombre)** sera supérieure à 1).

Type de journal	Description
	• Sur un pare-feu doté d'une licence AutoFocus active, pointez à côté d'une adresse IP, d'un nom de fichier, d'une URL, d'un agent utilisateur, d'un nom de menace ou d'un hachage contenu dans une entrée de journal et cliquez sur la liste déroulante () pour ouvrir le Récapitulatif des renseignements sur les menaces AutoFocus pour cet artefact. • Si les captures de paquets locaux sont activées, cliquez sur Télécharger () pour accéder aux paquets capturés. Pour activer les captures de paquets locaux, reportez-vous aux sous-sections dans **Objects (Objets)** > **Security Profiles (Profils de sécurité)**. • Pour afficher plus de détails à propos d'une menace ou pour configurer rapidement des exemptions de menace directement à partir des journaux de menaces, cliquez sur le nom de la menace dans la colonne **Name (Dénomination)**. La liste des Profils d'exemption affiche tous les profils personnalisés de protection Antivirus, Antispyware et Vulnérabilité. Pour configurer une exemption pour une signature de menace, cochez la case à gauche de la dénomination du profil de sécurité et enregistrez vos modifications. Pour ajouter des exemptions pour des adresses IP (jusqu'à 100 adresses IP par signature), surlignez le profil de sécurité, ajoutez la ou les adresse(s) IP dans la section Adresses IP exemptées et cliquez sur **OK** pour enregistrer. Pour afficher ou modifier l'exemption, reportez-vous au profil de sécurité associé et cliquez sur l'onglet **Exceptions**. Par exemple, si la menace relève de la catégorie vulnérabilité, sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Vulnerability Protection (Protection contre les vulnérabilités)**, cliquez sur le profil associé, puis sur l'onglet **Exceptions**. • Pour ajouter un périphérique à la liste de quarantaine (**Device (Périphérique)** > **Device Quarantine (Quarantaine du périphérique)**), ouvrez le menu déroulant **Host ID (ID de l'hôte)** et recherchez le périphérique puis cliquez sur **Block Device (Bloquer le périphérique) (** (dans la boîte de dialogue qui apparait).
Filtrage des URL	Affiche les journaux pour les filtres des URL qui contrôlent l'accès à des sites Web et qui déterminent si les utilisateurs peuvent envoyer des informations d'identification à des sites Web.

Type de journal	Description
	Sélectionnez Objets > Profils de sécurité > Filtrage des URL pour définir les paramètres de filtrage des URL, y compris les catégories d'URL à bloquer ou à autoriser et pour lesquelles vous souhaitez autoriser ou désactiver l'envoi d'informations d'identification. Vous pouvez également activer la journalisation des options d'en-tête HTTP pour l'URL. Sur un pare-feu doté d'une licence AutoFocus active, pointez à côté d'une adresse IP, d'un nom de fichier, d'une URL, d'un agent utilisateur, d'un nom de menace ou d'un hachage contenu dans une entrée de journal et cliquez sur la liste déroulante () pour ouvrir le Récapitulatif des renseignements sur les menaces AutoFocus pour cet artefact.
Envois WildFire	Affiche les journaux pour les fichiers et les liens d'e-mails que le pare-feu a transmis pour l'analyse WildFire™. Le cloud WildFire analyse l'échantillon et renvoie les résultats de l'analyse, y compris le verdict WildFire attribué à l'échantillon (bénin, malveillant, grayware ou hameçonnage). Vous pouvez confirmer si le pare-feu a autorisé ou bloqué un fichier en fonction des règles de politique de sécurité en consultant la colonne Actions. Sur un pare-feu doté d'une licence AutoFocus active, pointez à côté d'une adresse IP, d'un nom de fichier, d'une URL, d'un agent utilisateur, d'un nom de menace ou d'un hachage (dans la colonne Prétraitement des fichiers) contenu dans une entrée de journal et cliquez sur la liste déroulante () pour ouvrir le Récapitulatif des renseignements sur les menaces AutoFocus pour l'artefact.
Filtrage des données	Affiche les journaux des politiques de sécurité ainsi que les profils de filtrage des données, pour empêcher les informations sensibles, comme les numéros de carte de crédit ou de sécurité sociale, de quitter la zone protégée par le pare-feu, et les profils de blocage des fichiers, qui empêchent le chargement ou le téléchargement de certains types de fichiers. Pour configurer la protection par mot de passe pour accéder aux détails d'une entrée de journal, cliquez sur . Saisissez un mot de passe et cliquez sur **OK**. Pour obtenir des instructions sur la modification ou la suppression d'un mot de passe pour la protection des données, reportez-vous à Périphérique > Pages de réponse.

Type de journal	Description
	le système vous invite à saisir votre mot de passe une seule fois par session.
Correspondance HIP	Affiche toutes les correspondances HIP que la passerelle GlobalProtect™ identifie lors de la comparaison des données HIP brutes signalées par l'agent aux objets et aux profils HIP définis. Contrairement à d'autres journaux, une correspondance HIP est enregistrée même si elle ne correspond pas à une politique de sécurité. Pour davantage d'informations, reportez-vous à la section Réseau > GlobalProtect > Portails. Pour ajouter un périphérique à la liste de quarantaine (**Device (Périphérique)** > **Device Quarantine (Quarantaine du périphérique)**), ouvrez le menu déroulant **Host ID (ID de l'hôte)** et recherchez le périphérique puis cliquez sur **Block Device (Bloquer le périphérique) (** (dans la boîte de dialogue qui apparait).
GlobalProtect	Affiche les journaux de connexions à GlobalProtect Utilise cette information pour identifier vos utilisateurs GlobalProtect et leur version de système d'exploitation client, résoudre les problèmes de connexion et de performance, ainsi qu'identifier le portail et les passerelles auxquels les utilisateurs se connectent. Pour ajouter un périphérique à la liste de quarantaine (**Device (Périphérique)** > **Device Quarantine (Quarantaine du périphérique)**), ouvrez le menu déroulant **Host ID (ID de l'hôte)** et recherchez le périphérique puis cliquez sur **Block Device (Bloquer le périphérique) (** (dans la boîte de dialogue qui apparait).
Indicateur d'adresse IP	Affiche les informations sur la façon dont une étiquette a été appliquée à une adresse IP particulière et le moment où elle a été appliquée. Utilisez ces informations pour déterminer le moment où une adresse IP particulière a été placé dans un groupe d'adresses, et pourquoi, ainsi que pour déterminer les règles de politique qui influent sur cette adresse. Le journal comprend la réception de l'heure (la date et l'heure d'arrivée du premier et du dernier paquet de la session), le système virtuel, l'adresse IP source, l'étiquette, l'événement, le délai de temporisation, le nom de la source et le type de source.
User-ID™	Affiche des informations concernant les mappages d'adresse IP / nom d'utilisateur, comme la source des informations de mappage, la date à laquelle l'agent User-ID a effectué le mappage et le temps restant avant l'expiration des mappages. Vous pouvez utiliser ces informations pour résoudre les problèmes d'User-ID. Par exemple, si le pare-feu applique la mauvaise règle de

Type de journal	Description
	politique pour un utilisateur, vous pouvez afficher les journaux pour vérifier si cet utilisateur est mappé à la bonne adresse IP et si les associations de groupe sont correctes.
Déchiffrement	Affiche des informations sur les sessions de déchiffrement et les sessions non décryptées pour le trafic contrôlé par un profil Sans chiffrement, y compris les sessions GlobalProtect. Par défaut, les journaux affichent des informations sur les communications de déchiffrement SSL avortées. Vous pouvez activer la journalisation des communications de déchiffrement SSL réussies dans les **Options** de règles de politique de déchiffrement. Les journaux affichent une richesse d'informations qui vous permet d'identifier les protocoles faibles et les suites de cryptogrammes (échange de clé, chiffrement et algorithmes d'authentification), l'activité de chiffrement contournée, les échecs de chiffrement et leurs causes (par ex. une chaîne de certificats, une authentification du client ou des certificats joints incomplets), motifs de fin de session et plus encore. Par exemple, utilisez les informations pour déterminer si vous voulez autoriser les sites qui utilisent des protocoles et des algorithmes faibles. Il est peut-être préférable de bloquer les sites faibles auxquels vous accédez pour des besoins professionnels. Pour le trafic, le pare-feu ne décrypte pas si vous appliquez un profil Sans chiffrement, le journal affiche les sessions bloquées du fait de problèmes de vérification de certificat du serveur. La taille du journal de déchiffrement par défaut est de 32 Mo. Cependant, si vous décryptez un trafic important ou si vous activez la journalisation de communications de déchiffrement SSL réussies, vous aurez probablement besoin d'augmenter la taille du journal (**Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **Logging and Reporting Settings (Paramètres de journalisation et de création de rapports)** et de modifier les quotas de **Log Storage (Stockage de journaux)**. Si vous n'avez pas d'espace de journaux non attribué, envisagez des compromis entre la taille du journal de déchiffrement et les autres tailles de journaux. Plus vous vous connectez, plus les journaux consomment des ressources.
GTP	Affiche les journaux d'événements comprenant des informations sur la large gamme d'attributs GTP. Ces informations incluent le type d'événement GTP, le type de message d'événement GTP, APN, IMSI, IMEI, l'adresse IP de l'utilisateur final, en plus des informations TCP/IP que le pare-feu de prochaine génération identifie, telles que l'application, la source, l'adresse de destination et l'horodatage.

Type de journal	Description
Inspection des tunnels	Affiche une entrée au début et à la fin de chaque session de tunnel inspecté. Le journal comprend l'Heure de réception (date et heure d'arrivée du premier et du dernier paquet dans la session), ID du tunnel, Balise de suivi, ID de la session, Règle de sécurité appliquée au trafic du tunnel, etc. Voir Politiques > Inspection des tunnels pour davantage d'informations.
SCTP	Affiche les associations et événements SCTP selon les journaux générés par le pare-feu lors de l'inspection d'état, la validation du protocole et le filtrage du trafic SCTP. Les journaux SCTP comprennent des informations sur la large gamme d'attributs SCTP et de son protocole de charge utile, comme le type d'événement SCTP, le type de bloc, le « cause code, ID Diameter Application, Code de commande Diameter et les blocs. Ces informations SCTP sont fournis en plus des informations générales que le pare-feu identifie, comme l'adresse source et l'adresse de destination, le port source et le port de destination, la règle et l'horodatage. Reportez-vous à la section Objets > Profils de sécurité > Protection SCTP pour obtenir plus d'informations.
Configuration	Affiche une entrée pour chaque modification de la configuration. Chaque entrée inclut la date et l'heure, le nom d'utilisateur de l'administrateur, l'adresse IP correspondant à l'emplacement où la modification a été effectuée, le type de client (interface Web ou CLI), le type de commande exécutée, la réussite ou l'échec de la commande, le chemin de la configuration et les valeurs avant et après la modification.
system	Affiche une entrée pour chaque événement du système. Chaque entrée inclut la date et l'heure, la gravité de l'événement et sa description.
Alarmes	Le journal des alarmes enregistre des informations détaillées sur les alarmes qui sont générées par le système. Les informations figurant dans ce journal sont également indiquées dans Alarmes. Reportez-vous à la section Définir les paramètres d'alarme.
Authentification	Affiche des informations à propos des événements d'authentification qui se produisent lorsque les utilisateurs finaux essaient d'accéder aux ressources du réseau pour lesquelles l'accès est contrôlé par les Règles de la politique d'authentification. Vous pouvez utiliser ces informations pour résoudre les problèmes d'accès et pour adapter votre Politique d'authentification si nécessaire. En parallèle des objets de corrélation, vous pouvez également utiliser les Journaux d'authentification pour identifier les activités suspectes sur votre réseau, telles que les attaques par force brute.

Type de journal	Description
	Vous pouvez éventuellement configurer les Règles d'authentification sur Délais d'expiration d'authentification du journal. Ces délais d'expiration font référence à la période pendant laquelle un utilisateur doit s'authentifier une seule fois pour une ressource, mais qu'il peut y accéder à plusieurs reprises. Consulter les informations à propos de ces délais d'expiration vous aide à décider s'il est nécessaire de les régler, et comment le faire. *Les journaux système enregistrent les événements d'authentification liés à GlobalProtect et à l'accès administrateur à l'interface Web.*
unified	Affiches les plus récentes entrées de journal relatives au trafic, aux menaces, au filtrage des URL, aux envois WildFire et au filtrage des données en une vue unifiée. Cette vue commune des journaux vous permet d'examiner conjointement ces différents types de journaux et de les filtrer (plutôt que de chercher chaque journal séparément). Ou, vous pouvez choisir les types de journaux à afficher : cliquez sur la flèche à gauche du champ de filtrage et sélectionnez **traffic (trafic)**, **threat (menace)**, **URL**, **data (données)** et/ou **wildfire** pour afficher seulement les types de journaux sélectionnés. Sur un pare-feu doté d'une licence AutoFocus active, pointez à côté d'une adresse IP, d'un nom de fichier, d'une URL, d'un agent utilisateur, d'un nom de menace ou d'un hachage contenu dans une entrée de journal et cliquez sur la liste déroulante ( ) pour ouvrir le Récapitulatif des renseignements sur les menaces AutoFocus pour cet artefact. Le pare-feu affiche tous les journaux afin que les autorisations d'administration basées sur les rôles soient respectées. Lorsque vous affichez des journaux unifiés, seuls les journaux que vous êtes autorisés à voir sont inclus. Par exemple, un administrateur qui n'est pas autorisé à visualiser les journaux des envois WildFire ne verra pas les entrées des journaux des envois WildFire lorsqu'il visualisera les journaux unifiés. Pour plus d'informations sur les autorisations d'administrateur, reportez-vous à Périphérique > Rôles administrateur. *Vous pouvez utiliser le Jeu de journaux unifié avec le portail de renseignement de menaces AutoFocus. Pour ajouter des filtres de recherche AutoFocus directement dans le champ de filtrage des journaux Unifiés, vous devez* Définir une recherche AutoFocus.

Type de journal	Description
	Pour ajouter un périphérique à la liste de quarantaine (**Device (Périphérique)** > **Device Quarantine (Quarantaine du périphérique)**), ouvrez le menu déroulant **Host ID (ID de l'hôte)** et recherchez le périphérique puis cliquez sur **Block Device (Bloquer le périphérique) (** (dans la boîte de dialogue qui apparait).

Actions des journaux

Le tableau suivant décrit les actions de journaux.

Action (Action)	Description
Journaux de filtrage	Chaque page du journal dispose d'un champ de filtrage situé en haut de la page. Vous pouvez ajouter des artefacts au champ, comme une adresse IP ou une plage horaire, pour trouver les entrées du journal correspondantes. Les icônes qui se situent à la droite du champ vous permettent d'appliquer, d'effacer, de créer, d'enregistrer et de charger des filtres.  • Créer un filtre : • Cliquez sur un artefact d'une entrée de journal pour ajouter cet artefact au filtre. • Cliquez sur**Add (Ajouter)** () pour définir de nouveaux critères de recherche. Pour chaque critère, sélectionnez le **Connector (Connecteur)** qui définit le type de recherche (**and (et)** ou **or (ou)**), l'**Attribute (Attribut)** sur lequel se fonde la recherche, un **Operator (Opérateur)** pour définir la portée de la recherche ainsi qu'une **Value (Valeur)** pour l'évaluation par rapport aux entrées du journal. **Add (Ajoutez)** chaque critère au champ de filtrage et **Close (Fermez)** lorsque vous avez terminé. Vous pouvez ensuite appliquer (

Action (Action)	Description
	) le filtre.  *Si la chaîne **Value (Valeur)** correspond à un **Operator (Opérateur)** (tel que **has** ou **in**), entrez la chaîne entre guillemets afin d'éviter une erreur de syntaxe. Par exemple, si vous filtrez par pays de destination et que vous utilisez **IN** en tant que **Value (Valeur)** pour préciser INDE, saisissez le filtre en tant que **(dstloc eq "IN")**.*  *Le filtre des journaux **(receive_time in last-60-seconds)** entraîne l'augmentation ou la diminution du nombre d'entrées de journal (et de pages de journal) au fil du temps.* • Appliquer les filtres - Cliquez sur Appliquer les filtres () pour afficher les entrées de journal qui correspondent au filtre actuel. • Supprimer les filtres - Cliquez sur Effacer les filtres () pour effacer les valeurs inscrites dans le champ de filtrage. • Enregistrer un filtre - Cliquez sur Enregistrer un filtre (), saisissez un nom de filtre, puis cliquez sur **OK**. • Utiliser un filtre enregistré - Cliquez sur Charger un filtre () pour ajouter un filtre enregistré dans le champ de filtrage.
Journaux d'exportation	Cliquez sur Exporter vers un fichier CSV () pour exporter tous les journaux qui correspondent au filtre actuel vers un rapport au format CSV et continuer **Download file (Télécharger le fichier)**. Par défaut, le rapport comprend un maximum de 2 000 lignes de journal. Pour modifier le nombre maximum de lignes des rapports CSV générés, sélectionnez**Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **Logging and Reporting Settings (Paramètres de journalisation et de génération de rapports)** > **Log Export and Reporting (Exportation et génération de rapports de journaux)** et saisissez une nouvelle valeur **Max Rows in CSV Export (Nombre max. de lignes du rapport d'exportation CSV)**.
Mettre en surbrillance	Sélectionnez pour surligner les entrées des journaux qui correspondent à l'action. Les journaux filtrés sont surlignés dans les couleurs suivantes : • vert – autoriser ;

Action (Action)	Description
les actions de politique	• jaune – continuer ou forcer ; • rouge – refuser, abandonner, abandonner l'ICMP, réinitialiser le client, réinitialiser le serveur, réinitialiser les deux, bloquer-continuer, bloquer le forçage, bloquer l'URL, abandonner tout, entonnoir.
Modifier l'affichage des journaux	Pour personnaliser l'affichage des journaux : • Modifier l'intervalle d'actualisation automatique - Sélectionnez un intervalle dans la liste déroulante des intervalles (**60 seconds (60 secondes)**, **30 seconds (30 secondes)**, **10 seconds (10 secondes)** ou **Manual (Manuel)**). • Modifier le nombre d'entrées affichées par page ainsi que leur ordre de présentation - Les entrées de journaux sont extraites en blocs de 10 par page. • Utilisez les commandes de pagination situées en bas de la page pour naviguer dans la liste du journal. • Pour modifier le nombre d'entrées par page dans le journal, sélectionnez le nombre de lignes dans la liste déroulante Par page (**20**, **30**, **40**, **50**, **75**, ou **100**). • Pour trier les résultats par ordre croissant ou décroissant, utilisez la liste déroulante **ASC (Croissant)** ou **DESC (Décroissant)**. • Résoudre des adresses IP en noms de domaines – Sélectionnez **Resolve Hostname (Résolution du nom d'hôte)** pour commencer à résoudre des adresses IP externes en noms de domaines. • Changer l'ordre de présentation des journaux - Sélectionnez **DESC (Décroissant)** pour afficher les journaux en ordre décroissant, en commençant par les entrées de journaux ayant l'heure de réception la plus récente. Sélectionnez **ASC (Croissant)** pour afficher les journaux en ordre croissant, en commençant par les entrées de journaux ayant l'heure de réception la moins récente.
Afficher les détails des entrées des journaux.	Pour afficher des informations sur les détails des entrées des journaux : • Pour afficher des détails supplémentaires, cliquez sur Détails () d'une entrée. Si la source ou la destination a un mappage d'une adresse IP à un domaine ou à un nom d'utilisateur défini dans la page **Addresses (Adresses)**, ce nom s'affiche à la place de l'adresse IP. Pour afficher l'adresse IP associée, placez votre curseur sur le nom. • Sur un pare-feu doté d'une licence AutoFocus active, pointez à côté d'une adresse IP, d'un nom de fichier, d'une URL, d'un agent utilisateur, d'un nom de menace ou d'un hachage contenu dans une entrée de journal et cliquez sur la liste déroulante () pour ouvrir le Récapitulatif des renseignements sur les menaces AutoFocus pour l'artefact.

Surveillance > External Logs

Utilisez cette page pour consulter les journaux ingérés depuis Endpoint Security Manager (ESM) de Traps™ vers les collecteurs de journaux gérés par Panorama™. Pour afficher les journaux du Traps ESM sur Panorama, procédez comme suit :

- Sur le serveur Traps ESM, configurez Panorama en tant que serveur Syslog et sélectionnez les événements de journalisation à transférer à Panorama. Les événements peuvent inclure des événements de sécurité ainsi que tout changement apporté à la stratégie, à l'état de l'agent ou du serveur ESM, et aux paramètres de configuration.
- Sur un Panorama déployé en mode Panorama avec un ou plusieurs Collecteurs de journaux gérés, configurez un profil d'ingestion des journaux (Panorama > Profil d'ingestion des journaux) et associez-le à un Groupe de collecteurs (Panorama > Groupes de collecteurs) dans lequel stocker les journaux du Traps ESM.

Les journaux externes ne sont pas associés à un groupe de périphériques et ne sont visibles que lorsque vous sélectionnez **Groupe de périphériques** : **Tous,** car les journaux ne sont pas transférés depuis les pare-feu.

Type de journal	Description
Surveiller > **Journaux externes** > **Pièges ESM** > **Prévention**	Ces événements de menaces comprennent tous les événements de prévention, de notification, les événements provisoires et les événements de post-détection signalés par les agents Traps.
Surveiller > **Journaux externes** > **Pièges ESM** > **Système**	Les événements du système de serveur ESM incluent les modifications liées à l'état ESM, aux licences, aux fichiers de Support technique ESM et à la communication avec WildFire.
Surveiller > **Journaux externes** > **Pièges ESM** > **Politique**	Les événements de changement de politique incluent les modifications apportées aux règles, aux niveaux de protection, aux mises à jour de contenu, aux journaux de contrôle de hachage et aux verdicts.
Surveiller > **Journaux externes** > **Pièges ESM** > **Agent**	Les événements de changement d'agent se produisent au niveau du point de terminaison et incluent les modifications apportées aux mises à jour de contenu, aux licences, au logiciel, à l'état de la connexion, aux règles d'actions ponctuelles, aux processus et aux services et aux fichiers mis en quarantaine.
Surveiller > **Journaux externes** > **Pièges ESM** > **Configuration**	Les événements de modification de la configuration ESM incluent les modifications à l'échelle du système pour les licences, les utilisateurs administratifs et les rôles administrateur, les processus, les paramètres de restriction et les conditions.

Panorama peut mettre en corrélation les événements de sécurité distincts au niveau des points de terminaison avec les événements sur le réseau pour détecter toute activité suspecte ou malveillante entre les points d'extrémité et le pare-feu. Pour afficher les événements mis en corrélation identifiés par Panorama, voir Surveillance > Moteur de corrélation automatique > Événements corrélés.

Surveillance > Moteur de corrélation automatique

Le moteur de corrélation automatique suit les modèles sur votre réseau et met en corrélation les événements qui indiquent une hausse des comportements suspects ou des événements représentant une activité malveillante. Le moteur fonctionne comme votre analyste de sécurité personnel qui examine les événements isolés dans les différents ensembles de journaux sur le pare-feu, interroge les données de modèles spécifiques et fait les liens afin de vous fournir des informations exploitables.

Le moteur de corrélation utilise des objets de corrélation qui génèrent des événements corrélés. Les événements corrélés collectent les preuves vous permettant de repérer les similitudes entre des événements réseau apparemment sans rapport et constituent une base de réponse en cas d'incident.

Les modèles suivants prennent en charge le moteur de corrélation automatique :

- Panorama - appareils et appareils virtuels de la série M
- Pare-feu PA-3200 Series
- Pare-feux série PA-3400
- Pare-feu PA-5200 Series
- Pare-feu PA-5400 Series
- Pare-feu PA-7000 Series

Que voulez-vous savoir ?	Reportez-vous à la section :
Quels sont les objets de corrélation ?	Surveillance > Moteur de corrélation automatique > Objets de corrélation
Qu'est-ce qu'un événement corrélé ? Où puis-je voir la preuve de correspondance d'une correspondance de corrélation ?	Surveillance > Moteur de corrélation automatique > Événements corrélés
Comment puis-je obtenir une vue graphique des correspondances de corrélation ?	Reportez-vous au widget Hôtes compromis dans la section ACC.
Vous souhaitez en savoir plus ?	Utilisation du moteur de corrélation automatique

Surveillance > Moteur de corrélation automatique > Objets de corrélation

Pour contrer la progression des méthodes de diffusion de logiciels malveillants et d'attaques, les objets de corrélation étendent les fonctionnalités de détection des logiciels malveillants basées sur les signatures sur le pare-feu. Ils fournissent des renseignements permettant l'identification de modèles de comportement suspect dans les différents ensembles de journaux et rassemblent les preuves requises pour l'examen et répondre rapidement à un événement.

Un objet de corrélation est un fichier de définition qui spécifie les modèles de correspondance, les sources de données à utiliser pour les recherches et la période de recherche de ces modèles. Un modèle est une structure booléenne de conditions qui interrogent les sources de données. Chaque modèle se voit affecté un niveau de gravité et un seuil, qui est le nombre de fois qu'une correspondance au modèle se produit dans un délai imparti. Lorsqu'une correspondance au modèle survient, un événement de corrélation est consigné dans le journal.

Les sources de données utilisées pour effectuer des recherches peuvent inclure les journaux suivant : statistiques d'application, trafic, récapitulatif du trafic, récapitulatif des menaces, menaces, filtrage des données et filtrage des URL. Par exemple, la définition d'un objet de corrélation peut inclure un ensemble de modèles qui recherchent les preuves d'hôtes infectés, de modèles de logiciels malveillants ou de mouvement latéral de logiciels malveillants dans les journaux du trafic, de filtrage des URL et des menaces.

Les objets de corrélation sont définis par Palo Alto Networks® et sont fournis dans les mises à jour de contenu. Vous devez disposer d'une licence de prévention des menaces valide pour obtenir des mises à jour de contenu.

Tous les objets de corrélation sont activés par défaut. Pour désactiver un objet, sélectionnez-le et **Désactivez-le**.

Champs des objets de corrélation	Description
Nom et titre	L'étiquette indique le type d'activité que l'objet de corrélation détecte.
ID	Un nombre unique identifie l'objet de corrélation. Ce nombre se trouve dans la série 6000.
Catégorie	Un récapitulatif du type de menace ou nuisance qui pèse sur le réseau, l'utilisateur ou l'hôte.
État	L'état indique si l'objet de corrélation est activé (actif) ou désactivé (inactif).
Description	La description spécifie les conditions de correspondance pour lesquelles le pare-feu ou Panorama analysera les journaux. Elle décrit le modèle d'escalade ou le chemin de progression qui sera utilisé pour identifier toute activité malveillante ou comportement suspect de l'hôte.

Surveillance > Moteur de corrélation automatique > Événements corrélés

Les événements corrélés étendent les fonctionnalités de détection des menaces sur le pare-feu et Panorama. Ils rassemblent les preuves de comportement suspect ou inhabituel des utilisateurs ou des hôtes sur le réseau.

L'objet de corrélation permet de s'appuyer sur certains comportements ou conditions et de suivre les similitudes entre plusieurs sources de journaux. Lorsque l'ensemble des conditions spécifiées dans un

objet de corrélation est observé sur le réseau, chaque correspondance est consignée dans le journal comme événement corrélé.

L'événement corrélé comprend les détails répertoriés dans le tableau suivant.

Champ	Description
Heure de correspondance	L'heure à laquelle l'objet de corrélation a déclenché une correspondance.
Heure de mise à jour	L'horodatage auquel la correspondance a été mise à jour pour la dernière fois.
Nom de l'objet	Le nom de l'objet de corrélation qui a déclenché la correspondance.
Source Address (Adresse source)	L'adresse IP de l'utilisateur d'où provient le trafic.
Source User (Utilisateur source)	Les informations sur l'utilisateur et le groupe d'utilisateurs du serveur d'annuaire, si User-ID™ est activé.
Sévérité	Un indice qui classe le risque en fonction de l'étendue du dommage causé.
Résumé	Une description qui récapitule les preuves rassemblées sur l'événement corrélé.
ID d'hôte	L'ID de l'hôte du périphérique. Pour ajouter un périphérique à la liste de quarantaine (**Device (Périphérique)** > **Device Quarantine (Quarantaine du périphérique)**), cliquez sur la flèche vers le bas à côté de**Host ID (ID de l'hôte)** du périphérique et sélectionnez **Block Device (Bloquer le périphérique)** dans la fenêtre pop-up qui s'ouvre.

Pour afficher la vue détaillée du journal, cliquez sur Détails ( ) d'une entrée. La vue détaillée du journal inclut toutes les preuves d'une correspondance :

Onglet	Description
Informations sur la correspondance	**Détails sur l'objet** - présente des informations sur l'objet de corrélation qui a déclenché la correspondance. Pour plus d'informations sur les objets de corrélation, reportez-vous à Surveillance > Moteur de corrélation automatique > Objets de corrélation.
	Détails de la correspondance - Un récapitulatif des détails de la correspondance, notamment l'heure de correspondance, l'heure de la dernière mise à jour selon la preuve de correspondance, le niveau de gravité de l'événement et un récapitulatif des événements.

Onglet	Description
Preuve de correspondance	Cet onglet inclut toutes les preuves qui corroborent l'événement corrélé. Il affiche des informations détaillées sur les preuves collectées pour chaque session.

Consultez une présentation graphique des informations dans l’onglet **Correlated Events (Événements corrélés)**, consultez le widget Hôtes compromis dans l’onglet **ACC** > **Threat Activity (Activités des menaces)**. Dans le widget Hôtes compromis, l'affichage est agrégé par adresse IP et utilisateur source, et trié par niveau de gravité.

Pour configurer les notifications lorsqu’un événement corrélé est consigné dans le journal, accédez à **Device (Périphérique)** > **Log Settings (Paramètres du journal)** ou à l’onglet **Panorama** > **Log Settings (Paramètres du journal)**.

Surveillance > Capture de paquets

Tous les pare-feu Palo Alto Networks disposent d'une fonctionnalité intégrée de capture de paquets que vous pouvez utiliser pour capturer des paquets qui traversent les interfaces réseau sur le pare-feu. Vous pouvez ensuite utiliser les données capturées à des fins de dépannage ou pour créer des signatures d'application personnalisées.

La fonctionnalité de capture de paquets est gourmande en ressources processeur et peut réduire les performances du pare-feu. Utilisez uniquement cette fonctionnalité lorsque cela est nécessaire et assurez-vous de la désactiver après avoir collecté les paquets requis.

Que voulez-vous savoir ?	Reportez-vous à la section :
Quelles sont les différentes méthodes que le pare-feu peut utiliser pour capturer des paquets ?	Aperçu de la capture de paquets
Comment puis-je générer une capture de paquets personnalisée ?	Blocs de construction d’une capture de paquets personnalisée
Comment puis-je générer des captures de paquets lorsque le pare-feu détecte une menace ?	Activation de la capture de paquets de menaces
Comment puis-je télécharger une capture de paquets ?	Aperçu de la capture de paquets
Vous souhaitez en savoir plus ?	
• Activez la capture de paquets étendue pour les profils de sécurité.	Périphérique > Configuration > Content-ID
• Utilisez la capture de paquets pour écrire des signatures d’application personnalisées.	Voir Custom Application and Threat Signatures (Application personnalisée et signatures de menace).
• Empêcher un administrateur du pare-feu d’afficher les captures de paquets.	Définir l’accès administrateur à l’interface Web.
• Voir un exemple.	Voir Captures de paquets.

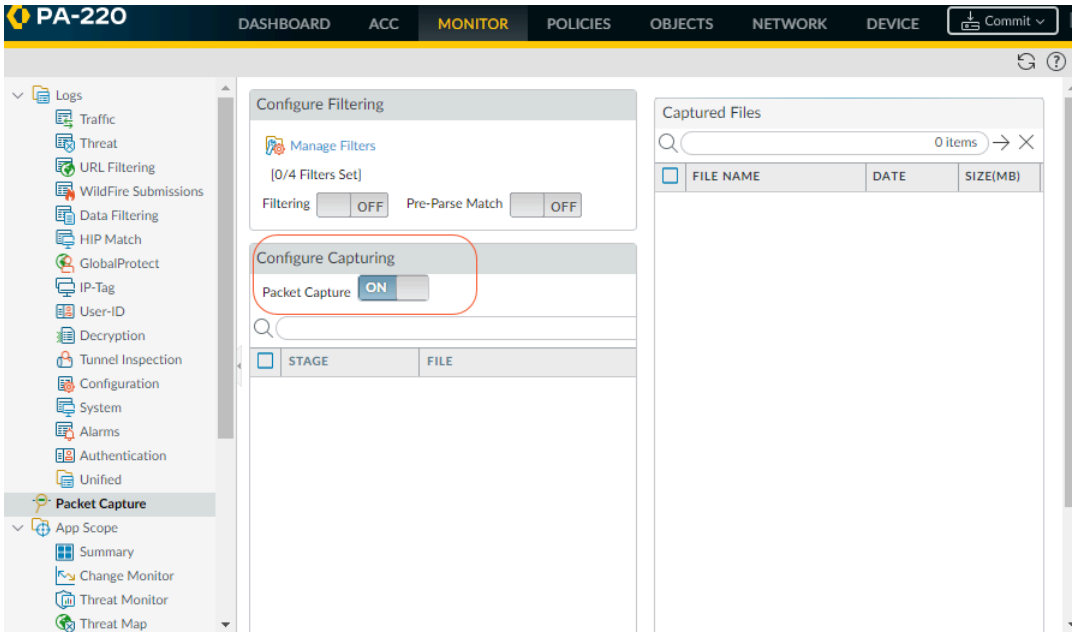
Aperçu de la capture de paquets

Vous pouvez configurer un pare-feu Palo Alto Networks pour effectuer une capture de paquets personnalisée ou une capture de paquets de menace.

- **Capture de paquets personnalisée** - Capturez des paquets pour l'ensemble du trafic ou le trafic en fonction des filtres définis. Par exemple, vous pouvez configurer le pare-feu pour capturer uniquement les paquets depuis et vers une adresse IP source et de destination ou un port spécifique. Utilisez ces captures de paquets pour résoudre les problèmes liés au trafic réseau ou pour collecter les attributs de l'application pour écrire des signatures d'applications personnalisées (**Monitor (Surveillance)** > **Packet Capture (Capture de paquets)**). Définissez le nom de fichier en fonction de l'étape (Supprimer, Pare-feu, Recevoir ou Transmettre). Une fois la capture de paquets terminée, vous pouvez la télécharger dans la section Fichiers capturés.
- **Capture de paquets de menace** - Capturez des paquets lorsque le pare-feu détecte un virus, un logiciel espion ou une vulnérabilité. Vous pouvez activer cette fonctionnalité dans les profils de sécurité Antivirus, Antispyware et Protection contre les vulnérabilités. Ces captures de paquets fournissent le contexte d'une menace qui vous permet de déterminer si une attaque est réussie ou d'en savoir plus sur les méthodes utilisées par une personne malveillante. L'action relative à la menace doit être définie sur Autoriser ou Alerter, sinon la menace est bloquée et les paquets ne peuvent pas être capturés. Vous pouvez configurer ce type de capture de paquets dans **Packet Capture (Objets)** > **Security Profiles (Profils de sécurité)**. Pour télécharger (↓) des captures de paquets, sélectionnez **Monitor (Surveillance)** > **Threat (Menaces)**.

Blocs de construction d'une capture de paquets personnalisée

Le tableau suivant décrit les composants de la page **Surveillance** > **Capture de paquets** utilisée pour configurer les captures de paquets, activer la capture de paquets et télécharger les fichiers de capture de paquets.



Blocs de construction de capture personnalisée de paquets	Configuré dans	Description
Gérer les filtres	Configuration du filtrage	Lorsque vous activez la capture de paquets personnalisée, vous pouvez définir des filtres pour capturer uniquement les paquets correspondant à ces filtres. Cela facilitera la localisation d'informations dont vous avez besoin dans les captures de paquets et réduira la puissance de traitement requise par le pare-feu pour effectuer la capture de paquets. Cliquez sur **Ajouter** pour ajouter un nouveau filtre et configurez les champs suivants : • **ID** - Saisissez ou sélectionnez un identifiant pour le filtre. • **Interface d'entrée** - Sélectionnez l'interface d'entrée sur laquelle vous souhaitez capturer le trafic. • **Source** - Spécifiez l'adresse IP source du trafic à capturer. • **Destination** - Spécifiez l'adresse IP de destination du trafic à capturer. • **Port source** - Spécifiez le port source du trafic à capturer. • **Port de destination** - Spécifiez le port de destination du trafic à capturer. • **Protocole** - Spécifiez le numéro de protocole de filtrage (1-255). Par exemple, le numéro de protocole d'ICMP est 1. • **Non IP** - Indiquez la méthode de traitement du trafic non IP (exclure tout le trafic IP, inclure tout le trafic IP, inclure uniquement le trafic IP ou n'inclure aucun filtre IP). Broadcast et AppleTalk sont des exemples de trafic non IP. • **IPv6** - Sélectionnez cette option pour inclure des paquets IPv6 dans le filtre.
Filtrage	Configuration du filtrage	Une fois les filtres définis, définissez le **Filtrage** sur **activé**. Si le filtrage est **désactivé**, l'ensemble du trafic est capturé.
Correspondance avant analyse	Configuration du filtrage	Cette option est à des fins de dépannage avancé. Lorsqu'un paquet arrive au port d'entrée, il passe par plusieurs étapes de traitement avant d'être analysé pour

Blocs de construction de capture personnalisée de paquets	Configuré dans	Description
		identifier des correspondances par rapport aux filtres préconfigurés. Il est possible qu'un paquet, en raison d'un échec, n'atteigne pas à l'étape de filtrage. Ceci peut se produire, par exemple, lors de l'échec de la recherche d'un itinéraire. Placez le paramètre **Correspondance avant analyse** sur **Activé** afin d'émuler une correspondance positive pour chaque paquet entrant dans le système. Ceci permet au pare-feu de capturer les paquets n'atteignant pas le processus de filtrage. Si un paquet peut arriver à l'étape de filtrage, il est ensuite traité en fonction de la configuration du filtre et supprimé s'il ne répond pas aux critères de filtrage.
Capture de paquets	Configuration de la capture	Cliquez sur l'interrupteur à bascule pour **ACTIVER** ou **DÉSACTIVER** la capture de paquets. Vous devez sélectionner au moins une étape de capture. Cliquez sur **Ajouter** et indiquez les éléments suivants : • **Étape** - Indique le point auquel les paquets doivent être capturés : • **Supprimer** - Lorsque le traitement d'un paquet rencontre une erreur et que ce paquet est supprimé. • **Pare-feu** - Lorsqu'un paquet dispose d'une correspondance de session ou qu'un premier paquet doté est correctement créé avec une session. • **Recevoir** - Lorsqu'un paquet est reçu sur le processeur du panneau de données. • **Transmettre** - Lorsqu'un paquet doit être transmis au processeur du panneau de données. • **Fichier** - Indiquez le nom du fichier de capture. Ce nom de fichier doit commencer par une lettre et peut inclure des lettres, des chiffres, des points, des caractères de soulignement ou des traits d'union. • **Nombre de paquets** - Indiquez le nombre maximum de paquets au-delà desquels la capture s'arrête.

Blocs de construction de capture personnalisée de paquets	Configuré dans	Description
		• **Nombre d'octets** – Indiquez le nombre maximum d'octets au-delà desquels la capture s'arrête.
Fichiers capturés	Fichiers capturés	Contient une liste de captures de paquets personnalisées précédemment générées par le pare-feu. Cliquez sur un fichier pour le télécharger sur votre ordinateur. Pour supprimer une capture de paquets, sélectionnez la capture de paquets, puis cliquez sur **Supprimer**. • **Nom de fichier** - Affiche les fichiers de capture de paquets. Les noms de fichiers sont basés sur le nom de fichier spécifié pour l'étape de capture. • **Date** - Date à laquelle le fichier a été généré. • **Taille (Mo)** - Taille du fichier de capture. Une fois la capture de paquets activée puis désactivée, vous devez cliquez sur Actualiser () pour afficher tout nouveau fichier de capture de paquets dans cette liste.
Effacer tous les paramètres	Paramètres	Cliquez sur **Effacer tous les paramètres** pour désactiver la capture de paquets et effacer tous les paramètres de capture de paquets. *Cela ne désactive pas la capture de paquets définie dans un profil de sécurité. Pour plus d'informations sur l'activation de la capture de paquets dans un profil de sécurité, reportez-vous à la section* Activation de la capture de paquets de menaces.

Activation de la capture de paquets de menaces

- Objets > Profils de sécurité

Pour permettre au pare-feu de capturer des paquets lorsqu'il détecte une menace, activez l'option de capture de paquets dans le profil de sécurité.

D'abord, sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)**, puis modifiez le profil souhaité comme décrit dans le tableau suivant :

Options de capture de paquets dans les Profils de sécurité	Location (Emplacement)
Antivirus	Sélectionnez un profil Antivirus personnalisé et, dans l'onglet **Antivirus**, sélectionnez **Packet Capture (Capture de paquets)**.
Antispyware	Sélectionnez un profil Antispyware personnalisé, cliquez sur l'onglet **DNS Signatures (Signatures DNS)** et, dans la liste déroulante **Packet Capture (Capture de paquets)**, sélectionnez **single-packet (un seul paquet)** ou **extended-capture (capture étendue)**.
Protection contre les vulnérabilités	Sélectionnez un profil Protection contre les vulnérabilités et, dans l'onglet **Rules (Règles)**, cliquez sur **Add (Ajouter)** pour ajouter une nouvelle règle ou choisissez-en une existante. Puis, cliquez sur la liste déroulante **Packet Capture (Capture de paquets)** et sélectionnez **single-packet (un seul paquet)** ou **extended-capture (capture étendue)**.

*dans les profils Antispyware et Protection contre les vulnérabilités, vous pouvez également activer la capture de paquets pour les exceptions. Cliquez sur l'onglet **Exceptions** et, dans la colonne Capture de paquets d'une signature, cliquez sur la liste déroulante et sélectionnez **single-packet (un seul paquet)** ou **extended-capture (capture étendue)**.*

(Facultatif) Pour définir la longueur d'une capture de paquets de menaces en fonction du nombre de paquets capturés (basé sur un paramètre global), sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Content-ID** et, dans la section Paramètres Content-ID™, modifiez la **Extended Packet Capture Length (packets) (Longueur de capture de paquets étendue)** (plage comprise entre 1 et 50, valeur par défaut : 5).

Une fois la capture de paquets activée dans un profil de sécurité, vous devez vérifier que celui-ci fait partie d'une règle de sécurité. Pour savoir comment ajouter un profil de sécurité à une règle de sécurité ; reportez-vous à Présentation de la politique de sécurité.

Toutes les fois qu'un pare-feu détecte une menace et que la capture des paquets est activée dans le profil de sécurité, vous pouvez télécharger (⭳) ou exporter la capture de paquets.

Surveillance > App-Scope

Les rubriques suivantes décrivent les fonctionnalités d'App Scope.

- Aperçu de l'App-Scope
- Rapport récapitulatif App-Scope
- Rapport de surveillance des modifications App-Scope
- Rapport de surveillance des menaces App-Scope
- Rapport de la carte des menaces App-Scope
- Rapport de surveillance du réseau App-Scope
- Rapport de la carte du trafic App-Scope

Aperçu de l'App-Scope

Les rapports App-Scope fournissent une visibilité graphique des aspects suivants de votre réseau :

- Modifications au niveau de l'utilisation de l'application et de l'activité des utilisateurs
- Utilisateurs et applications monopolisant la bande passante du réseau
- Menaces du réseau

Les rapports App Scope vous permettent de voir rapidement si un comportement est inhabituel ou inattendu et d'identifier un comportement problématique; chaque rapport propose une fenêtre dynamique et personnalisable par l'utilisateur dans le réseau. Ces rapports contiennent des options permettant de sélectionner les données et les plages à afficher. Sur Panorama, vous pouvez également sélectionner la **(Source de données** des informations affichées. La source de données par défaut (sur les nouvelles installations Panorama) utilise la base de données locale de Panorama, qui stocke les journaux transférés par les pare-feu gérés ; lors d'une mise à niveau, la source de données par défaut est **La données du périphérique distant** (données du pare-feu géré). Pour afficher une vue agrégée des données directement depuis les périphériques gérés, vous devez faire basculer la source de **Panorama** sur **Données du périphérique distant**.

Pointez la souris et cliquez sur les lignes ou les barres des diagrammes pour accéder à l'ACC et afficher des informations détaillées sur l'application, la catégorie d'application, l'utilisateur ou la source spécifique.

Diagrammes du centre de commande de l'application	Description
Résumé	Rapport récapitulatif App-Scope
Surveillance des modifications	Rapport de surveillance des modifications App-Scope
Utilitaire de surveillance des menaces	Rapport de surveillance des menaces App-Scope

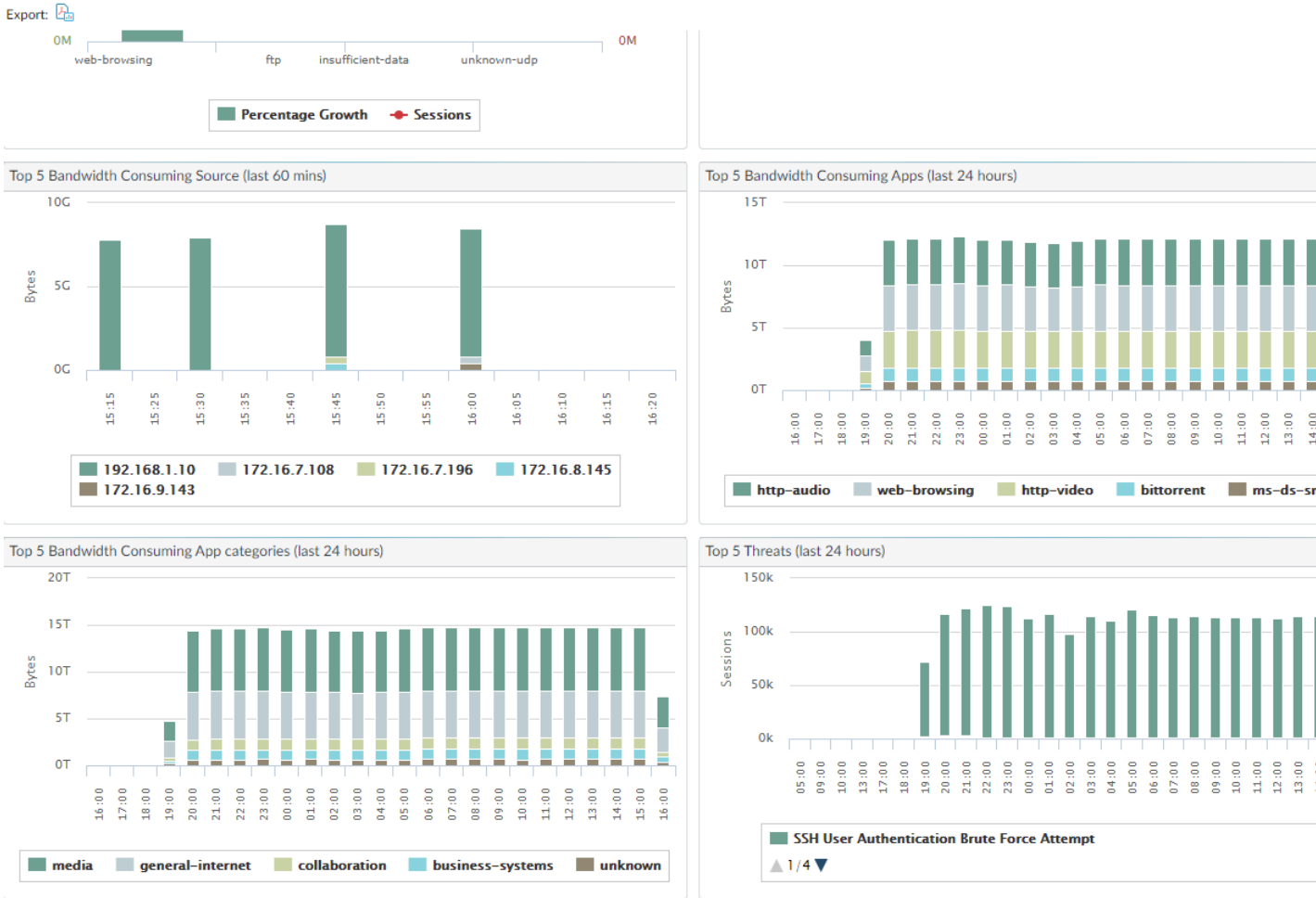
Diagrammes du centre de commande de l’application	Description
Carte des menaces	Rapport de la carte des menaces App-Scope
Surveillance réseau	Rapport de surveillance du réseau App-Scope
Carte du trafic	Rapport de la carte du trafic App-Scope

Rapport récapitulatif App-Scope

Le rapport récapitulatif affiche les diagrammes des cinq applications, catégories d’applications, utilisateurs et sources obtenant, perdant et consommant le plus de bande passante.

Pour exporter les diagrammes dans le rapport récapitulatif au format PDF, cliquez sur **Exporter** ( ). Chaque diagramme est enregistré sous forme de page du fichier'A0;PDF.

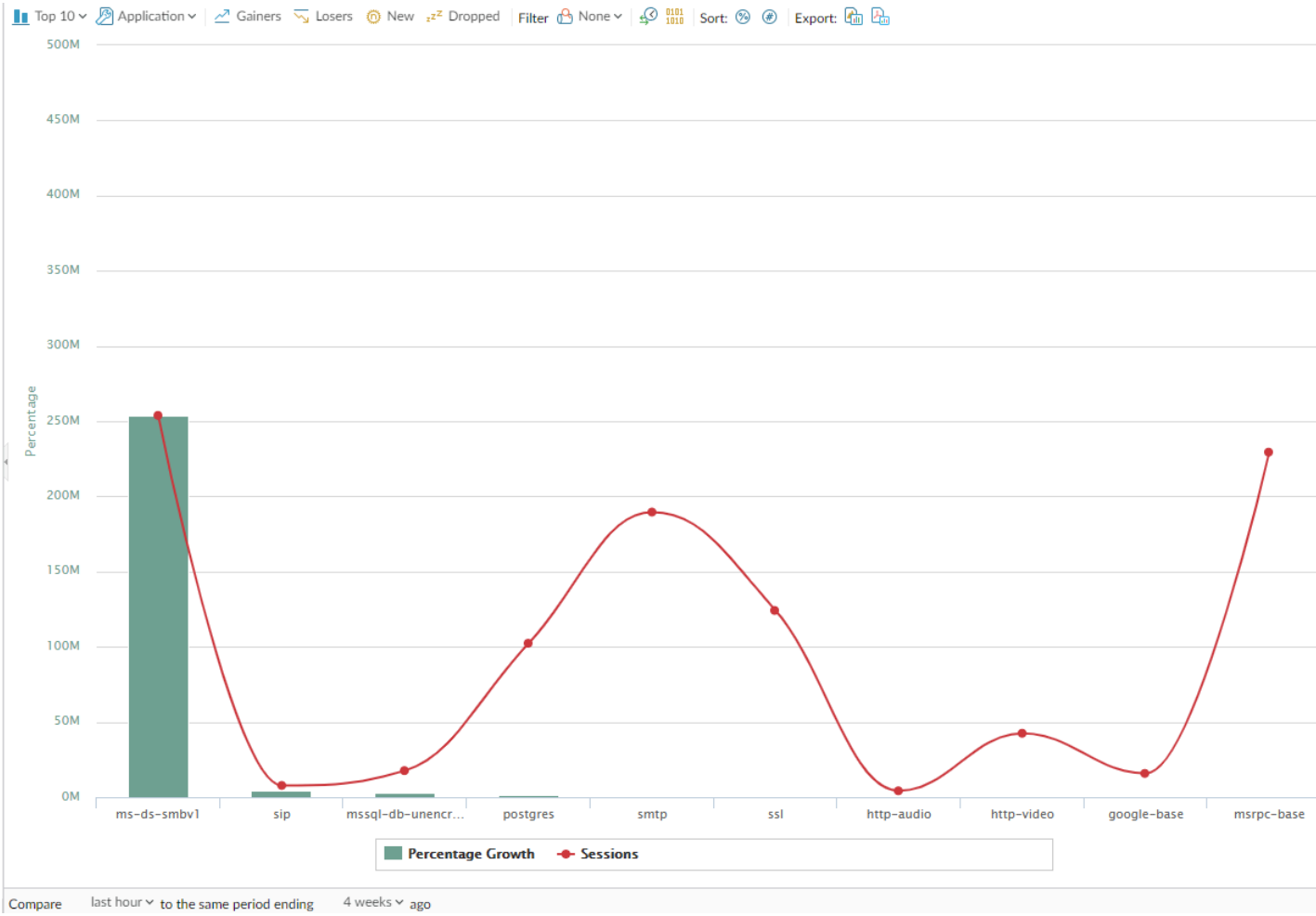
Rapport récapitulatif App-Scope



Rapport de surveillance des modifications App-Scope

Le rapport de surveillance des modifications affiche les modifications effectuées au cours d'une période définie. Par exemple, le diagramme ci-dessous affiche les applications les plus utilisées au cours de la dernière heure par rapport à la dernière période de 24 heures. Les principales applications sont définies par nombre de sessions et triées par pourcentage.

Rapport de surveillance des modifications App-Scope



Ce rapport contient les options suivantes.

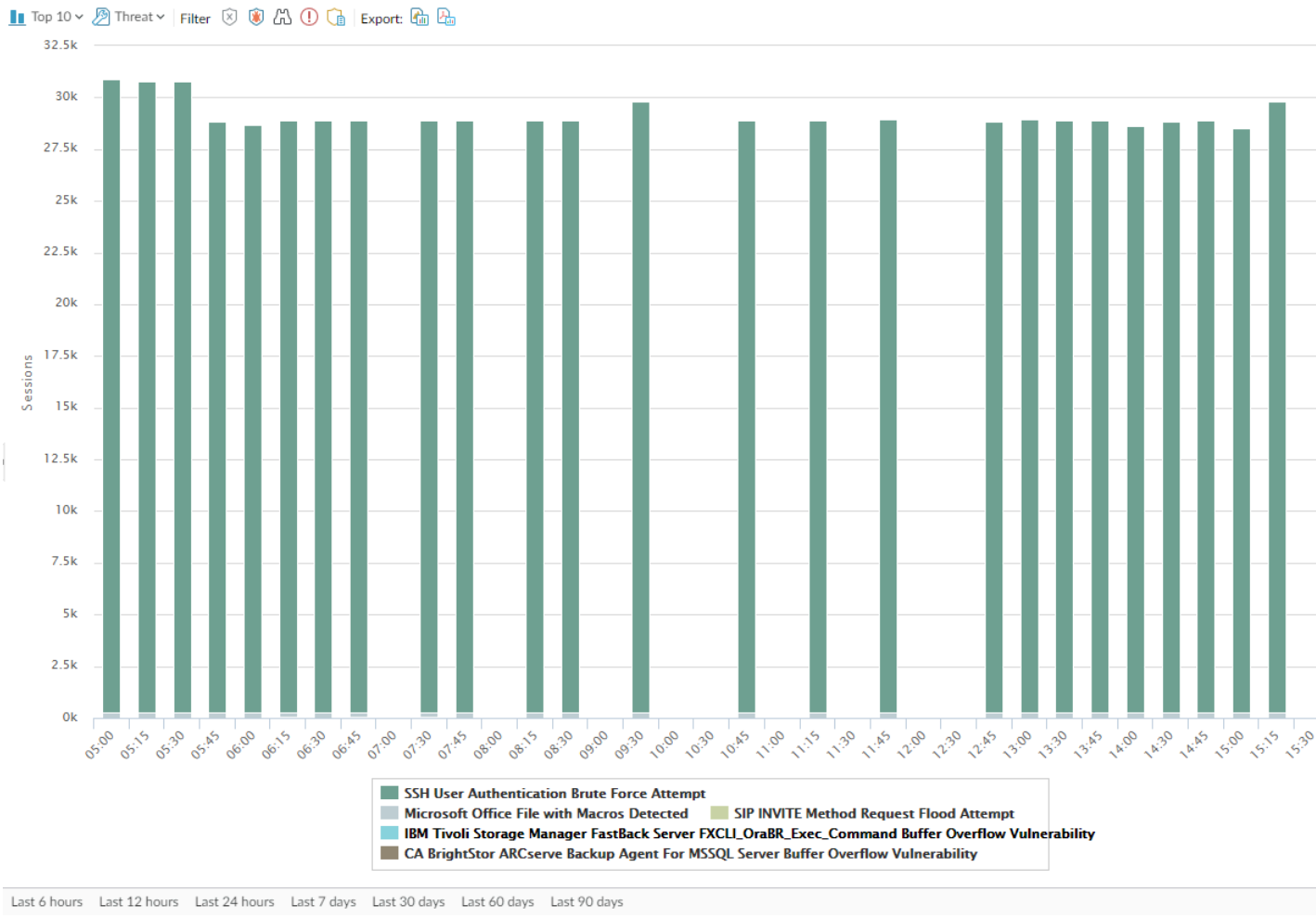
Options du rapport de surveillance des modifications	Description
Barre du haut	
Top 10	Détermine le nombre d'enregistrements dont la mesure la plus élevée est incluse dans le diagramme.
Application	Détermine le type d'élément signalé : application, catégorie d'applications, source ou destination.

Options du rapport de surveillance des modifications	Description
Gagnants	Affiche les mesures des éléments dont le nombre a augmenté au cours de la période évaluée.
Perdants	Affiche les mesures des éléments dont le nombre a baissé au cours de la période évaluée.
Nouveau	Affiche les mesures des éléments ajoutés au cours de la période évaluée.
Dropped	Affiche les mesures des éléments abandonnés au cours de la période évaluée.
Filtre	Applique un filtre afin d'afficher uniquement l'élément sélectionné. Aucun affichage dans toutes les entrées.
Compter les sessions et compter les octets	Indique si des informations de sessions ou d'octets doivent être affichées.
Trier	Indique si des entrées doivent être triées par pourcentage ou par croissance brute.
Export (Exporter)	Exporte le graphique sous forme d'image .png ou au format PDF.
Barre du bas	
Comparer (intervalle)	Indique la période au bout de laquelle les mesures des modifications apportées sont réalisées.

Rapport de surveillance des menaces App-Scope

Le rapport de surveillance des menaces affiche le nombre de menaces principales identifiées au cours de la période sélectionnée. Par exemple, la figure ci-dessous affiche les 10 types de menaces principales rencontrées au cours des 6 dernières heures.

Rapport de surveillance des menaces App-Scope



Chaque type de menace est représenté par une couleur, comme indiqué dans la légende située sous le diagramme. Ce rapport contient les options suivantes.

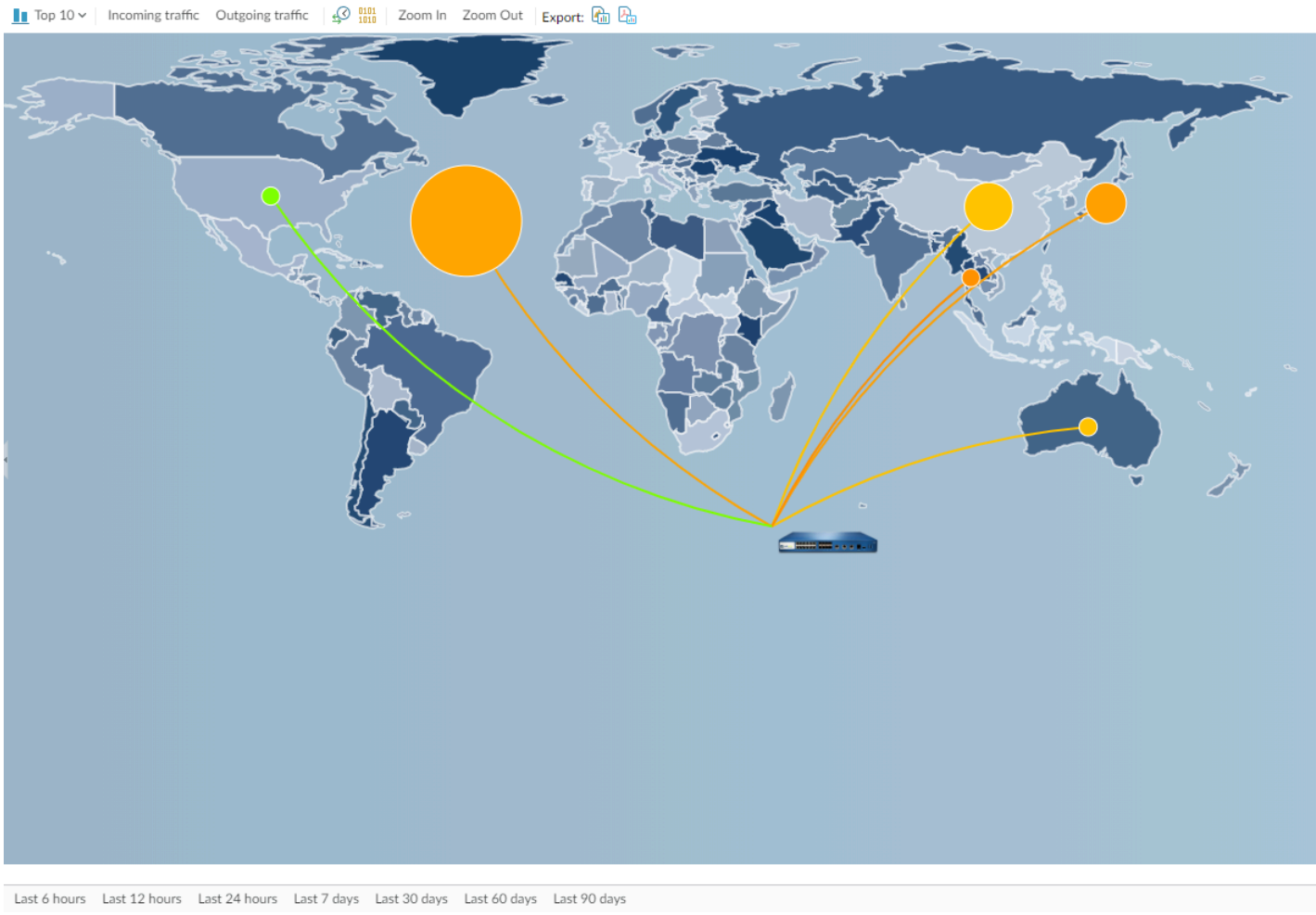
Options du rapport de surveillance des menaces	Description
Barre du haut	
Top 10	Détermine le nombre d'enregistrements dont la mesure la plus élevée est incluse dans le diagramme.
Prévention	Détermine le type d’élément mesuré : menace, catégorie de menaces, source ou destination.
Filtre	Applique un filtre afin d'afficher uniquement l'élément sélectionné.
	Indique si les informations sont présentées sous la forme d'un histogramme empilé ou d'un diagramme en aires empilées.

Options du rapport de surveillance des menaces	Description
Exporter	Exporte le graphique sous forme d'image .png ou au format PDF.
Barre du bas	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last 90 days	Indique la période au bout de laquelle des mesures sont réalisées.

Rapport de la carte des menaces App-Scope

Le rapport de la carte des menaces affiche une vue géographique des menaces, ainsi que leur gravité.

Rapport de la carte des menaces App-Scope



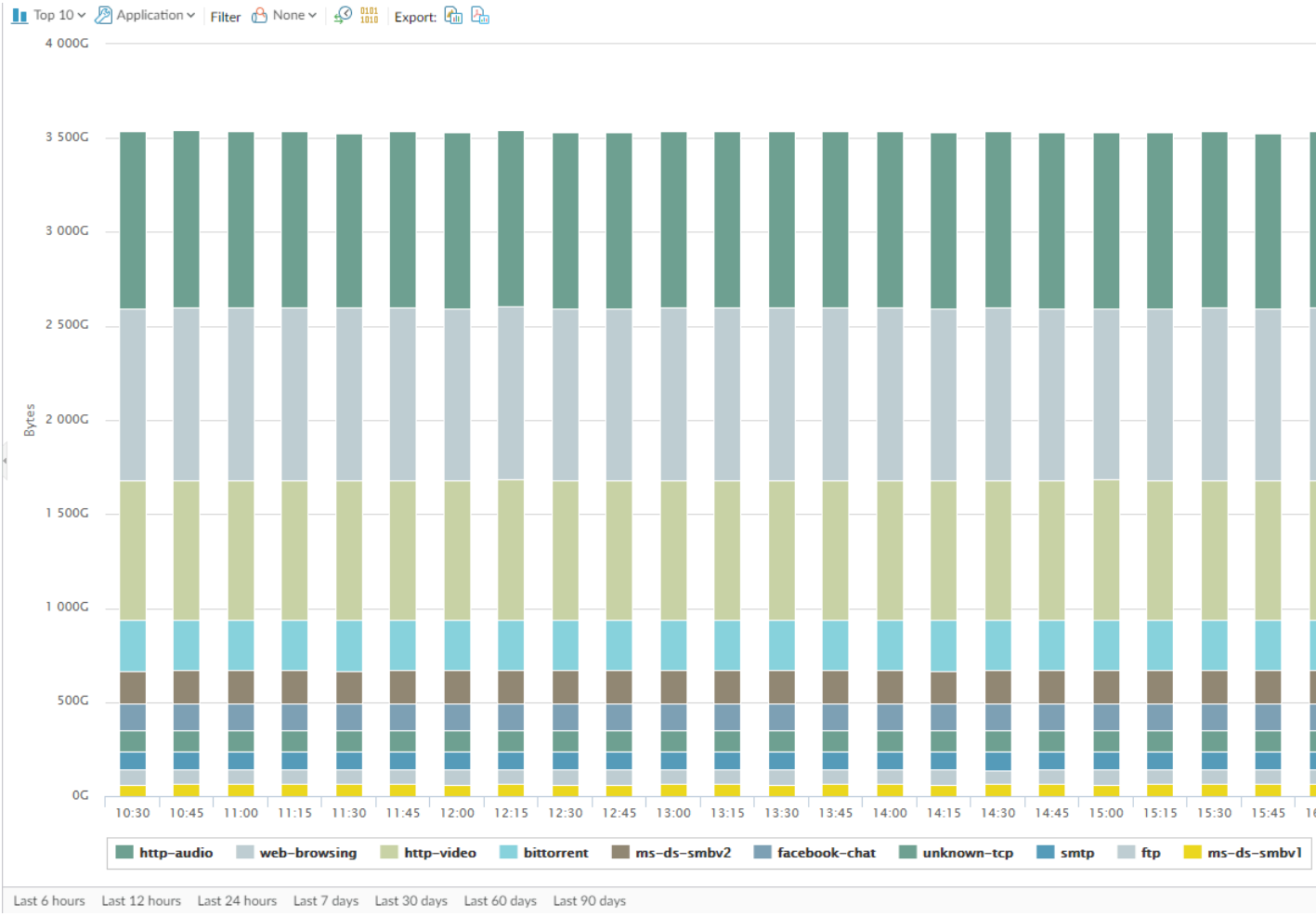
Chaque type de menace est représenté par une couleur, comme indiqué dans la légende située sous le diagramme. Cliquez sur un pays de la carte pour faire un **Zoom avant**, puis un **Zoom arrière**, au besoin. Ce rapport contient les options suivantes.

Options du rapport de la carte des menaces	Description
Barre du haut	
Top 10	Détermine le nombre d'enregistrements dont la mesure la plus élevée est incluse dans le diagramme.
Menaces entrantes	Affiche les menaces entrantes.
Menaces sortantes	Affiche les menaces sortantes.
Filtre	Applique un filtre afin d'afficher uniquement l'élément sélectionné.
Zoom avant et zoom arrière	Zoom avant et zoom arrière de la carte.
Exporter	Exporte le graphique sous forme d'image .png ou au format PDF.
Barre du bas	
Last 6 hours Last 12 hours Last 24 hours Last 7 days Last 30 days Last 60 days Last Calendar	Indique la période au bout de laquelle des mesures sont réalisées.

Rapport de surveillance du réseau App-Scope

Le rapport de surveillance du réseau affiche la bande passante dédiée aux différentes fonctions réseau au cours d'une période définie. Chacune de ces fonctions est représentée par une couleur, comme indiqué dans la légende située sous le diagramme. Par exemple, l’image ci-dessous montre la bande passante de l’application au cours des 7 derniers jours et se base sur des informations de session.

Rapport de surveillance du réseau App-Scope



Ce rapport contient les options suivantes.

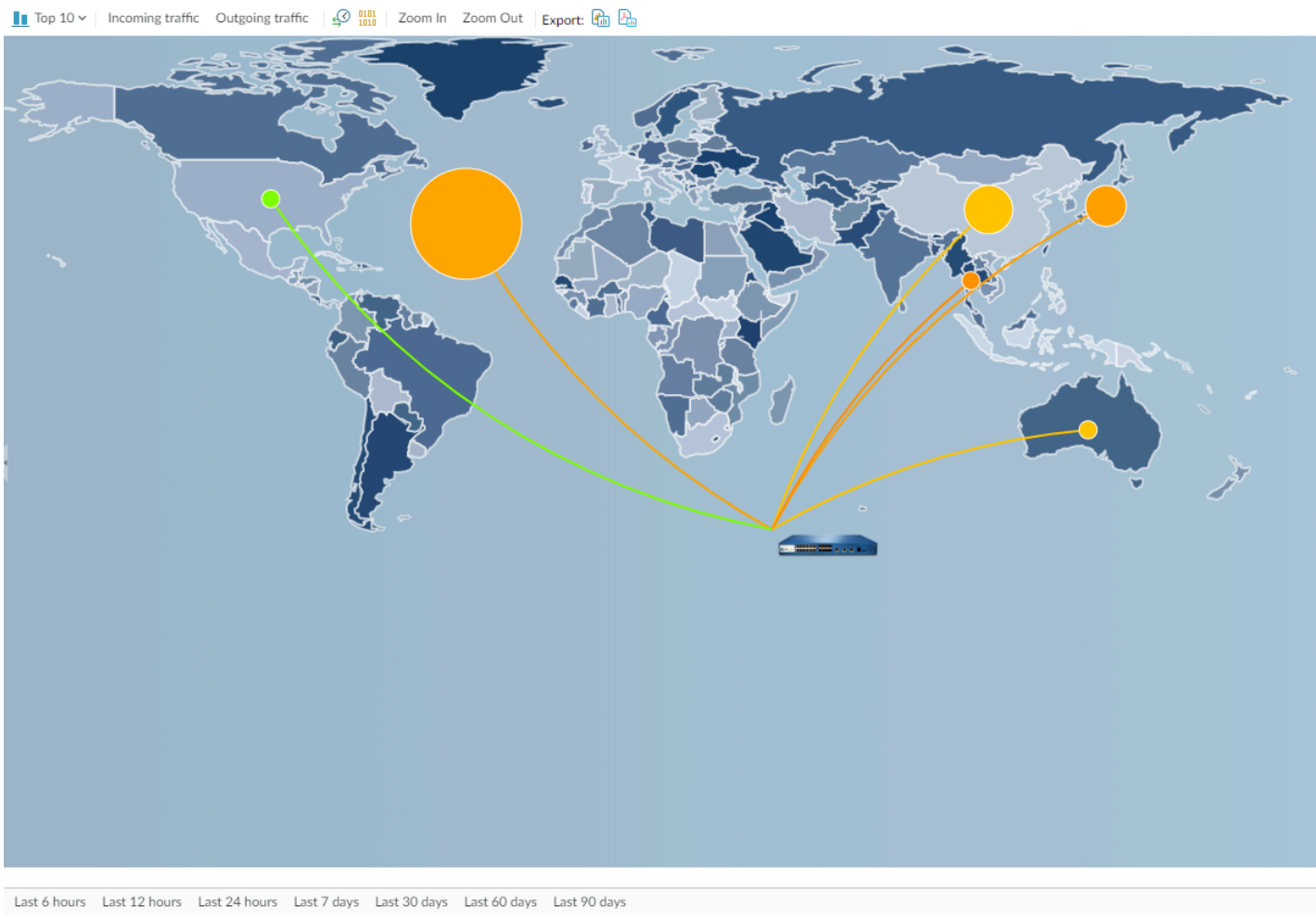
Options du rapport de surveillance du réseau	Description
Barre du haut	
Top 10	Détermine le nombre d'enregistrements dont la mesure la plus élevée est incluse dans le diagramme.
Application	Détermine le type d’élément signalé : application, catégorie d'applications, source ou destination.
Filtre	Applique un filtre afin d'afficher uniquement l'élément sélectionné. **Aucun** affiche toutes les entrées.
Compter les sessions et compter les octets	Indique si des informations de sessions ou d'octets doivent être affichées.

Options du rapport de surveillance du réseau	Description
	Indique si les informations sont présentées sous la forme d'un histogramme empilé ou d'un diagramme en aires empilées.
Exporter	Exporte le graphique sous forme d'image .png ou au format PDF.
Barre du bas	
	Indique la période au bout de laquelle les mesures des modifications apportées sont réalisées.

Rapport de la carte du trafic App-Scope

Le rapport de la carte du trafic affiche une vue géographique des flux de trafic en fonction des sessions ou des flux.

Rapport de la carte du trafic App-Scope



Chaque type de trafic est représenté par une couleur, comme indiqué dans la légende située sous le diagramme. Ce rapport contient les options suivantes.

Options du Rapport de la carte du trafic	Description
Barre du haut	
Top 10	Détermine le nombre d'enregistrements dont la mesure la plus élevée est incluse dans le diagramme.
Trafic entrant	Affiche le trafic entrant.
Trafic sortant	Affiche le trafic sortant.
Compter les sessions et compter les octets	Indique si des informations de sessions ou d'octets doivent être affichées.
Zoom avant et zoom arrière	Zoom avant et zoom arrière de la carte.
Exporter	Exporte le graphique sous forme d’image .png ou au format PDF.
Barre du bas	
	Indique la période au bout de laquelle les mesures des modifications apportées sont réalisées.

Surveillance > Navigateur de session

Sélectionnez **Monitor (Surveillance)** > **Session Browser (Navigateur de session)** pour parcourir et filtrer les sessions en cours d’exécution sur le pare-feu. Pour plus d’informations sur les options de filtrage pour cette page, reportez-vous à la section Actions des journaux.

Surveillance > Liste d’interdiction d’adresses IP

Il existe plusieurs façons de configurer le pare-feu pour placer des adresses IP sur la liste d’interdictions, y compris les méthodes suivantes :

- Configurez une règle de politique de Protection DoS avec l’action **Protéger**, puis appliquez un profil de Protection DoS classé à cette règle. Le profil comprend la durée du blocage.
- Configurez une règle de politique de sécurité avec un profil de protection contre les vulnérabilités qui utilise une règle avec l’action **Bloquer IP**, puis appliquez la règle à une zone.

La liste d’interdiction d’adresses IP est prise en charge sur les pare-feux PA-3200 Series, PA-5200 Series et PA-7000 Series.

Que voulez-vous savoir ?	Reportez-vous à la section :
Que signifient les champs Liste d’interdiction d’adresses IP ?	Entrées de la liste d’interdiction d’adresses IP
Comment puis-je filtrer, naviguer ou supprimer les entrées de la liste d’interdiction d’adresses IP ?	Afficher ou supprimer les entrées de la liste d’interdiction d’adresses IP
Vous souhaitez en savoir plus ?	Paramétrage des profils Antivirus, Antispyware et Protection contre les vulnérabilités Protection DoS contre la saturation de nouvelles sessions Surveiller les adresses IP bloquées

Entrées de la liste d’interdiction d’adresses IP

- **Surveiller** > **BlockIPList**

Le tableau suivant explique l’entrée de la liste d’interdiction pour une adresse IP source bloquée par le pare-feu.

Champ	Description
Délai de blocage	Mois/jour et heures:minutes:secondes lorsque l’adresse IP est placée dans la liste d’interdiction d’adresses IP.
Type	Type d’action de blocage : indique si le matériel (hw) ou le logiciel (sw) ont bloqué l’adresse IP. Lorsque vous configurez une politique de Protection DoS ou une politique de Sécurité qui utilise un profil de Protection contre les vulnérabilités pour bloquer les connexions à partir d’adresses sources IPv4, le pare-feu bloque automatiquement ce trafic dans le matériel avant que ces paquets n’utilisent des ressources du processeur ou de la mémoire tampon des paquets. Si le

Champ	Description
	trafic d’attaque dépasse la capacité de blocage du matériel, le pare-feu utilise un logiciel pour bloquer le trafic.
Adresse IP source	Adresse IP source du paquet bloqué par le pare-feu.
Zone d'entrée	Zone de sécurité affectée à l’interface sur laquelle le paquet traverse le pare-feu.
Temps restant	Nombre de secondes restantes pour que l’adresse IP se retrouve sur la liste d’interdiction d’adresses IP.
Bloquer la source	Nom du profil de Protection DoS classé ou nom de l’objet de Protection contre les vulnérabilités sur lesquels vous avez indiqué l’action de blocage d’adresses IP.
Nombre total d’adresses IP bloquées : x sur un total de y (z % utilisés)	Nombre d’adresses IP bloquées (x) sur le nombre d’adresses IP bloquées prises en charge par le pare-feu (y) et le pourcentage correspondant d’adresses IP bloquées utilisé (z).

Afficher ou supprimer les entrées de la liste d’interdiction d’adresses IP

Accédez aux entrées de la liste d’interdiction d’adresses IP, visualisez les informations détaillées et supprimez une entrée si vous le souhaitez.

Afficher ou supprimer les entrées de la liste d’interdiction d’adresses IP	
Rechercher des informations spécifiques concernant la liste d’interdiction d’adresses IP	Sélectionnez une valeur dans une colonne, qui entre dans un filtre dans le champ **Filtres**, puis cliquez sur la flèche de droite pour initier la recherche d’entrées avec cette valeur. Cliquez sur le « X » pour supprimer un filtre.
Afficher les entrées de la liste d’interdiction d’adresses IP au-delà de l’écran actuel	Saisissez un numéro de page dans le champ **Page** ou cliquez sur les flèches simples pour afficher la Page suivante ou la Page précédente des entrées. Cliquez sur les flèches doubles pour afficher la Dernière page ou la Première page des entrées.
Afficher des informations détaillées sur une adresse IP de la liste d’interdiction d’adresses IP	Cliquez sur une Adresse IP source d’une entrée qui relie les Solutions réseau WhoIs avec des informations concernant l’adresse.

Afficher ou supprimer les entrées de la liste d’interdiction d’adresses IP	
Supprimer les entrées de la liste d’interdiction d’adresses IP	Sélectionnez une entrée et cliquez sur **Supprimer**. *Uniquement la suppression d’entrées matérielles est prise en charge par l’interface web. Cependant, la suppression d’entrées matérielles et logicielles est prise en charge par la CLI.*
Effacer toute la liste d’interdiction d’adresses IP	Cliquez sur **Effacer tout** pour supprimer définitivement toutes les entrées, ce qui signifie que ces paquets ne sont plus bloqués. *Uniquement la suppression de la liste d’adresses IP bloquées des entrées matérielles est prise en charge par l’interface web. Cependant, la suppression de la liste d’adresses IP bloquées des entrées matérielles et logicielles est prise en charge par la CLI.*

Surveillance > Botnet

Le rapport du Botnet vous permet d'utiliser des mécanismes comportementaux pour identifier d'éventuels hôtes infectés par un Botnet dans votre réseau. Le rapport attribue à chaque hôte une note de confiance de 1 à 5 pour indiquer la probabilité d'une infection par un Botnet ; une note de 5 correspond à la plus grande probabilité. Avant de programmer l'exécution du rapport ou de l'exécuter à la demande, vous devez le configurer pour identifier les types de trafic qui sont suspects. Le Guide de l'administrateur PAN-OS® fournit des détails sur l'Interprétation du résultat du rapport du Botnet.

- Paramètres d'un rapport du Botnet
- Paramètres de configuration d'un Botnet

Paramètres d'un rapport du Botnet

- Surveillance > Botnet > Paramètre du rapport

Avant de générer le rapport du Botnet, vous devez préciser les types du trafic qui peuvent indiquer l'activité d'un Botnet (reportez-vous à la section Configuration des rapports du Botnet). Pour programmer un rapport quotidien ou pour l'exécuter sur demande, cliquez sur **Report Setting (Paramètre du rapport)** et remplissez les champs suivants. Pour exporter un rapport, sélectionnez le rapport et**Exporter au format PDF**, **Exporter vers un fichier CSV** ou **Exporter au format XML**.

Paramètres d'un rapport du Botnet	Description
Délai d'exécution du test	Sélectionnez un délai pour le rapport - **Dernière 24 heures** (par défaut) or **Dernier jour calendaire**.
Lancer l'exécution	Cliquez sur **Run Now (Lancer l'exécution)** pour générer un rapport manuellement et immédiatement. Le rapport s'affiche dans un nouvel onglet de la boîte de dialogue du rapport Botnet.
Nbre de rangées	Indiquez le nombre de lignes à afficher dans le rapport (valeur par défaut : 100).
Planifié	Sélectionnez cette option pour générer automatiquement le rapport tous les jours. Cette option est activée par défaut.
Générateur de requêtes	**(**Facultatif**) Add (Ajoutez)** des requêtes au Générateur de requêtes pour filtrer les résultats du rapport par attributs tels que les adresses IP source / de destination, les utilisateurs ou les zones. Par exemple, si vous savez que le trafic ayant été initié à partir de l'adresse IP 192.0.2.0 ne possède aucun risque d'activité d'un Botnet, vous pouvez ajouter **`not (addr.src in 192.0.2.0)`** en tant que requête pour exclure cet hôte des résultats du rapport. • **Connector (Connecteur)** - Sélectionnez un connecteur logique (**and (et)** ou **or (ou)**). Si vous avez sélectionné **Negate (Ignorer)**, le rapport exclura les hôtes indiqués dans la requête.

Paramètres d'un rapport du Botnet	Description
	• **Attribute (Attribut)** - Sélectionnez une zone, une adresse ou un utilisateur qui est associé aux hôtes que le pare-feu évalue afin de détecter une activité du Botnet. • **Operator (Opérateur)** - Sélectionnez un opérateur pour lier l'**Attribute (Attribut)** à une **Value (Valeur)**. • **Value (Valeur)** - Saisissez une valeur à faire correspondre avec la requête.

Paramètres de configuration d’un Botnet

- Surveillance > Botnet > Configuration

Pour préciser les types de trafic qui indiquent un risque d'activité d'un Botnet, cliquez sur **Configuration** du côté droit de la page **Botnet** et renseignez les champs suivants. Après avoir configuré le rapport, vous pouvez l’exécuter sur demande ou le programmer pour qu’il s’exécute quotidiennement (voir Surveillance > Rapports au format PDF > Gestion des rapports récapitulatifs au format PDF).

La configuration du rapport Botnet par défaut est optimale. Si vous croyez que les valeurs par défaut identifient des faux positifs, créez un billet d’assistance, pour que Palo Alto Networks puisse réévaluer les valeurs.

Paramètres de configuration d’un Botnet	Description
Trafic HTTP	Cliquez sur **Activer** et définissez la valeur **Nombre** de chacun des types de trafic HTTP que le rapport doit inclure. Les valeurs **Nombre** que vous saisissez représentent le nombre minimum d'événements pour chaque type de trafic qui doivent survenir pour que l'hôte qui y est associé obtienne une note de confiance plus élevée dans le rapport (plus grand risque d'infection par un Botnet). Si le nombre d’événements est inférieur au **Nombre**, le rapport indiquera la note de confiance la plus basse ou (pour certains types de trafic) n’affichera pas d’entrée pour l’hôte. • **Visite de l'URL d'un site malveillant** (intervalle compris entre 2 et 1000 ; valeur par défaut : 5) - Identifie les utilisateurs communiquant avec des URL de sites malveillants connus en fonction des catégories de filtrage des URL du Botnet et des sites malveillants. • **Utilisation d'un DNS dynamique** (intervalle compris entre 2 et1000 ; valeur par défaut : 5) - Recherche le trafic d'une requête DNS dynamique pouvant indiquer la présence d'un logiciel malveillant, de communications avec un Botnet ou de kits d'attaques. Il est généralement très risqué d'utiliser des domaines DNS dynamiques. Les logiciels malveillants se servent souvent des domaines DNS

Paramètres de configuration d’un Botnet	Description
	dynamiques pour éviter les listes de blocage d'adresses IP. Envisagez d’utiliser le Filtrage des URL pour bloquer ce type de trafic. • **Navigation dans des domaines IP** (intervalle compris entre 2 et 1000 ; valeur par défaut : 10) - Identifie les utilisateurs qui naviguent dans des domaines IP au lieu d'adresses URL. • **Browsing to recently registered domains (Navigation dans des domaines récemment enregistrés)** (intervalle compris entre 2 et 1000 ; valeur par défaut : 5) - Recherche du trafic dans les domaines ayant été enregistrés au cours des 30 derniers jours. Les pirates, les logiciels malveillants et les kits d'attaques utilisent fréquemment les domaines nouvellement enregistrés. • **Fichiers exécutables provenant de sites inconnus** (intervalle compris entre 2 et 1000 ; valeur par défaut : 5) - Identifie les fichiers exécutables téléchargés à partir d'URL inconnues. Les fichiers exécutables jouent un rôle dans de nombreuses infections et, lorsqu'ils sont combinés à d'autres types de trafic suspect, peuvent vous aider à prioriser les analyses d'hôtes à effectuer.
Applications inconnues	Définissez les seuils permettant de déterminer si le rapport englobera le trafic associé aux applications TCP inconnu et UDP inconnu qui sont suspectes. • **Sessions par heure** (intervalle compris entre 1 et 3 600 ; valeur par défaut : 10) - Le rapport présente le trafic des applications ayant un nombre de sessions par heure inférieur ou égal à la valeur précisée. • **Destinations par heure** (intervalle compris entre 1 et 3 600 ; valeur par défaut : 10) - Le rapport présente le trafic des applications ayant un nombre de destinations par heure inférieur ou égal à la valeur précisée. • **Nombre minimum d'octets** (intervalle compris entre 1 et 200 ; valeur par défaut : 50) - Le rapport présente le trafic des applications dont la charge utile est égale ou supérieure à la taille précisée. • **Nombre maximum d'octets** (intervalle compris entre 1 et 200 ; valeur par défaut : 100) - Le rapport présente le trafic des applications dont la charge utile est égale ou inférieure à la taille précisée.
IRC	Sélectionnez cette option pour inclure le trafic faisant appel aux serveurs IRC.

Surveillance > Rapports au format PDF

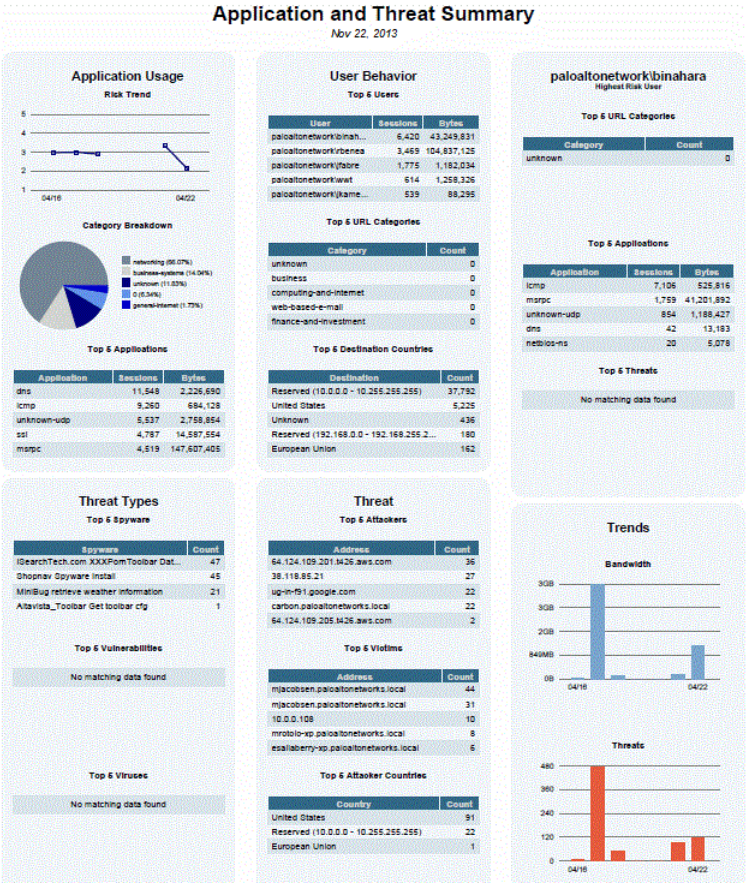
Les rubriques suivantes décrivent les rapports au format PDF.

- Surveillance > Rapports au format'A0;PDF > Gérer un récapitulatif au format PDF
- Surveillance > Rapports au format PDF > Rapport d'activité des utilisateurs
- Surveillance > Rapports PDF > Utilisation de l'application SaaS
- Surveillance > Rapports au format PDF > Groupes de rapports
- Surveillance > Rapports au format PDF > Planificateur de courrier électronique

Surveillance > Rapports au format'A0;PDF > Gérer un récapitulatif au format PDF

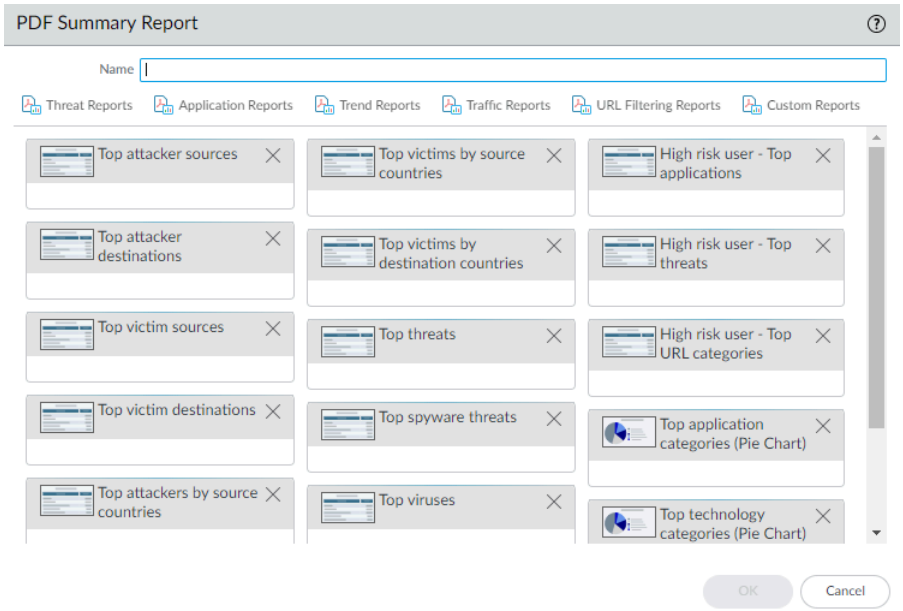
Les rapports récapitulatifs au format PDF contiennent des informations compilées à partir de rapports existants, en fonction des données figurant dans les 5 meilleurs de chaque catégorie (au lieu des 50 meilleurs). Ils contiennent également des diagrammes de tendance qui ne sont pas disponibles dans les autres rapports.

Rapport récapitulatif au format PDF



Pour créer des rapports récapitulatifs au format PDF, cliquez sur **Ajouter**. La page **PDF Summary Report (Rapport récapitulatif au format PDF)** s'ouvre pour afficher tous les éléments disponibles du rapport.

Gestion de rapports au format PDF



Utilisez une ou plusieurs de ces options pour élaborer un rapport :

- Pour supprimer un élément du rapport, cliquez sur Supprimer ([X]) ou désélectionnez l'élément de la liste déroulante pertinente.
- Sélectionnez des éléments supplémentaires dans la liste déroulante pertinente.
- Faites glisser et déposez un élément pour le déplacer vers une autre zone du rapport.

18 éléments de rapport au maximum sont autorisés. Si vous en avez déjà 18, vous devez supprimer certains éléments existants avant de pouvoir en ajouter des nouveaux.

Pour **Enregistrer** le rapport, saisissez un nom de rapport et cliquez sur **OK**.

Pour afficher les rapports PDF, sélectionnez **Monitor (Surveiller)** > **Reports (Rapports)**, cliquez sur **PDF Summary Report (Rapport récapitulatif au format PDF)** pour sélectionner un rapport et cliquez ensuite sur un jour dans le calendrier pour télécharger un rapport pour ce jour-là.

Les nouveaux rapports récapitulatifs au format PDF ne s'affichent qu'après l'exécution du rapport, ce qui se produit automatiquement toutes les 24 heures à 2 heures du matin.

Surveillance > Rapports au format PDF > Rapport d'activité des utilisateurs

Utilisez cette page pour créer des rapports qui récapitulent l'activité des utilisateurs individuels ou des groupes d'utilisateurs. Cliquez sur **Ajouter** et indiquez les informations suivantes.

Paramètres du rapport d’activité des utilisateurs / groupes	Description
Name (Nom)	Donnez un nom au rapport (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement.
Type	Pour le rapport d'activité des utilisateurs : sélectionnez **User (Utilisateur)**, puis saisissez l’**Username (Nom d'utilisateur)** ou l'**IP address (Adresse IP)** (IPv4 ou IPv6) de l'utilisateur qui sera le sujet du rapport.
	Pour le rapport d'activité des groupes : Sélectionnez un **Group (Groupe)** et saisissez le **Group Name (Nom du groupe)**.
Filtres supplémentaires	Sélectionnez **Filter Builder (Générateur de filtre)** pour créer des filtres à appliquer au rapport d’activité des utilisateurs / groupes.
Période de temps	Sélectionnez un délai pour le rapport dans la liste déroulante.
Inclure la navigation détaillée	(Facultatif) Sélectionnez cette option pour inclure pour inclure des journaux des URL détaillés dans le rapport. *les informations relatives à la navigation détaillée peuvent inclure un grand nombre de journaux (des milliers) pour l'utilisateur ou le groupe d'utilisateurs sélectionné et peuvent rendre le rapport très volumineux.*

Le rapport d'activité des groupes n'inclut pas l'option Parcourir le récapitulatif par catégorie d'URL ; toutes les autres informations sont communes aux rapports d'activité des utilisateurs et des groupes.

Pour exécuter le rapport sur demande, cliquez sur **Run Now (Lancer l'exécution)**. Pour modifier le nombre maximum de lignes affichées dans le rapport, reportez-vous à la section Paramètres de journalisation et de génération de rapports.

Pour enregistrer le rapport, cliquez sur **OK**. Vous pouvez ensuite planifier le rapport pour la distribution par courrier électronique (Surveillance > Rapports au format PDF > Planificateur de courrier électronique).

Ajouter un filtre de journal

Générez des filtres de journal à appliquer au rapport d’activité des utilisateurs ou au rapport d'activité des groupes pour personnaliser les rapports. Vous pouvez filtrer les rapports d’activité selon l’application, les caractéristiques d’application, etc. Par exemple, si vous vous intéressez à une application SaaS qui ne possèdent pas de certificats, vous pouvez générer un filtre selon cette caractéristique d’application.

Champ Ajouter un filtre de journal	Description
Zone de texte Filtre de journal	Inscrivez le filtre que vous aimeriez appliquer au journal. Vous pouvez en inscrire plus d'un.
Connecteur	Modifier le filtre pour y ajouter une option de filtrage supplémentaire. Cochez la case **Negate (Refuser)** pour ne pas appliquer un filtre de connecteur que vous avez créé.
Attribut	Sélectionnez l'attribut que vous aimeriez ajouter à partir du menu.
Opérateur	Déterminez si l'Attribut doit être égal ou non à la Valeur.
Valeur	Définissez la Valeur de l'attribut. Lorsque possible, un menu déroulant dans lequel figureront des valeurs possibles s'affichera.

Sélectionnez **Apply (Appliquer)** pour appliquer le filtre généré au Rapport d'activités de l'utilisateur ou au Rapport d'activités du groupe.

Surveillance > Rapports PDF > Utilisation de l'application SaaS

Utilisez cette page pour générer un rapport d'utilisation de l'application Saas qui résume les risques de sécurité associés aux applications SaaS qui traversent votre réseau. Ce rapport prédéfini présente une comparaison des applications autorisées et des applications non autorisées, les applications SaaS risquées qui possèdent des caractéristiques d'hébergement défavorables ainsi que l'activité, l'utilisation et la conformité des applications en indiquant les principales applications de chaque catégorie sur les pages détaillées. Vous pouvez utiliser ces informations détaillées sur les risques pour appliquer une politique relative aux applications SaaS que vous souhaitez autoriser ou bloquer sur votre réseau.

Pour générer un rapport informatif et précis, vous devez étiqueter les applications approuvées sur votre réseau (reportez-vous à la section Génération du rapport d'utilisation de l'application SaaS). Le pare-feu et Panorama considère que toute application qui n'est pas dotée d'une telle étiquette prédéfini n'est pas approuvée sur le réseau. Il importe d'être au fait des applications approuvées et des applications non approuvées qui existent sur votre réseau puisque les applications SaaS non approuvées peuvent représenter une menace pour la sécurité de l'information ; elles ne sont pas autorisées à être utilisées sur votre réseau et peuvent entraîner une exposition à des risques ainsi que la perte de données privées et de nature délicate.

Assurez-vous d'étiqueter uniformément les applications sur tous les pare-feu ou les groupes de périphériques. Si la même application est étiquetée comme étant approuvée dans un système virtuel et comme étant non approuvée dans un autre système virtuel ou sur Panorama ou encore si une application n'est pas approuvée dans un groupe de périphériques parent mais qu'elle est approuvée dans un groupe de périphériques enfants (ou l'inverse), le rapport d'utilisation de l'application Saas générera des résultats non concordants.

*Sur le ACC, définissez l'**Affichage de l'application** sur **Par état approuvé** pour identifier visuellement les applications qui ont un état approuvé différent dans les systèmes virtuels ou les groupes de périphériques. Le vert indique les applications approuvées, le bleu les applications non autorisées et le jaune indique les applications qui ont un état approuvé différent dans différents systèmes virtuels ou groupes de périphériques.*

Pour configurer le rapport, cliquez sur **Add (Ajouter)** et indiquez les informations suivantes :

Paramètres du rapport d'utilisation de l'application SaaS	Description
Name (Nom)	Donnez un nom au rapport (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Période de temps	Sélectionnez un délai pour le rapport dans la liste déroulante. Le rapport comprend les données du jour actuel (le jour où le rapport est généré).
Inclure les journaux à partir de	Dans le menu déroulant, sélectionnez si vous souhaitez générer le rapport sur un groupe d'utilisateurs sélectionné, sur une zone sélectionnée ou pour tous les groupes d'utilisateurs et zones configurés sur le pare-feu ou Panorama. • **Pour un groupe d'utilisateurs sélectionné** – Sélectionnez le **Groupe d'utilisateurs** pour lequel le pare-feu ou Panorama filtrera les journaux. • **Pour une zone sélectionnée** – Sélectionnez la **Zone** pour laquelle le pare-feu ou Panorama filtrera les journaux. • **Pour tous les groupes d'utilisateurs et zones** – Vous pouvez générer des rapports sur tous les groupes ou choisir jusqu'à 25 groupes d'utilisateurs pour lesquels vous souhaitez obtenir une visibilité. Si vous avez plus de 25 groupes, le pare-feu ou Panorama affiche les 25 principaux groupes dans le rapport et affectez tous les groupes d'utilisateurs restants au groupe Autres.
Inclure les informations sur les groupes d'utilisateurs dans le rapport	Cette option filtre les journaux pour les groupes d'utilisateurs que vous souhaitez inclure dans le rapport. Sélectionnez le lien **Groupes de gestion** ou les **Groupes de gestion pour la zone sélectionnée** pour choisir jusqu'à 25 groupes d'utilisateurs pour lesquels vous souhaitez obtenir une visibilité.

Paramètres du rapport d'utilisation de l'application SaaS	Description
(Non disponible si vous choisissez de générer le rapport sur un **Groupe d'utilisateurs sélectionné**.)	Lorsque vous générez un rapport pour des groupes d'utilisateurs spécifiques sur une zone sélectionnée, les utilisateurs qui ne sont membres d'aucun des groupes sélectionnés sont affectés à un groupe d'utilisateurs appelé Autres.
Groupe d'utilisateurs	Sélectionnez le ou les groupes d'utilisateurs pour lesquels vous souhaitez générer le rapport. Cette option s'affiche uniquement lorsque vous choisissez **Groupe d'utilisateurs sélectionné** dans le menu déroulant **Inclure les journaux à partir de**.
Employé	Sélectionnez la zone pour laquelle vous souhaitez générer le rapport. Cette option s'affiche uniquement lorsque vous choisissez **Zone sélectionnée** dans le menu déroulant **Inclure les journaux à partir de**. Vous pouvez ensuite sélectionner Inclure les informations sur les groupes d'utilisateurs dans le rapport.
Inclut des renseignements détaillés sur les catégories d'application dans le rapport	Le rapport d'utilisation de l'application SaaS au format PDF comprend deux sections. Les deux sections du rapport sont générées par défaut. La première section du rapport (dix pages) porte sur les applications SaaS utilisées sur votre réseau au cours de la période considérée. Désélectionnez cette options si vous ne voulez pas que la seconde section du rapport comprenne des renseignements détaillés sur les applications SaaS et autres que SaaS pour chacune des sous-catégories d'applications figurant à la première section du rapport. Cette seconde section du rapport englobe les noms des principales applications de chacune des sous-catégories ainsi que des informations sur les utilisateurs, les groupes d'utilisateurs, les fichiers, les octets transférés et les menaces provenant de ces applications. Sans les informations détaillées, le rapport comprend dix pages.
Nombre max. de sous-catégories dans le rapport à	Sélectionnez si vous souhaitez utiliser toutes les sous-catégories d'applications dans le rapport d'Utilisation de l'application SaaS ou si vous souhaitez limiter le nombre maximum de 10, 15, 20 ou 25 sous-catégories. Lorsque vous réduisez le nombre maximum de sous-catégories, le rapport détaillé est plus court, car vous limitez les informations d'activité de l'application SaaS et non-SaaS incluses dans le rapport.

Cliquez sur **Run Now (Exécuter maintenant)** pour générer le rapport sur demande.

Vous pouvez générer ce rapport sur demande ou vous pouvez programmer sa génération quotidienne, hebdomadaire ou mensuelle. Pour programme la génération du rapport, reportez-vous à la section Planifier des rapports pour la livraison par courrier électronique.

Sur les pare-feu PA-220 et PA-220R, le rapport d’utilisation d’application SaaS n’est pas transmis en tant que fichier PDF joint à l’e-mail. L’e-mail contient plutôt un lien qui vous permettra d’ouvrir le rapport dans un navigateur Web.

Pour plus d’informations sur le rapport, consultez la section Gestion de la génération de rapports.

Surveillance > Rapports au format PDF > Groupes de rapports

Les groupes de rapports vous permettent de créer des ensembles de rapports que le système peut compiler et envoyer sous la forme d'un rapport unique agrégé au format PDF avec une page de titre facultative et tous les rapports constitutifs inclus.

Paramètres du groupe de rapports	Description
Name (Nom)	Donnez un nom au groupe de rapports (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement.
Titre de la page	Sélectionnez cette option pour inclure une page de titre dans le rapport.
Title	Saisissez un nom qui va servir de titre au rapport.
Sélection du rapport / widgets	Pour chaque rapport à inclure dans le groupe, vous devez sélectionner le rapport dans la colonne de gauche et l’**Ajouter** à la colonne de droite. Vous pouvez sélectionner les types de rapports suivants : • Rapport prédéfini • Rapport personnalisé • Rapport récapitulatif au format PDF • Csv • Vue détaillée du journal – Chaque fois que vous créez un rapport personnalisé, le pare-feu crée automatiquement un rapport de Vue détaillée du journal portant le même nom. Le rapport Aperçu du journal affiche les journaux utilisés par le pare-feu pour générer le contenu du rapport personnalisé. Pour inclure les données de la vue détaillée du journal, lors de la création d’un groupe de rapports, ajoutez vos **Rapports personnalisés** puis ajoutez les rapports de **Vue détaillée du journal** correspondants. Le rapport agrégé généré pour le groupe de rapports affiche les données du rapport personnalisé suivies des données de journaux. Après l’enregistrement du groupe de rapports, la colonne Widgets de la page Groupes de rapports répertorie les rapports que vous avez ajoutés au groupe.

Pour utiliser le groupe de rapports, reportez-vous à Surveillance > Rapports au format PDF > Planificateur de courrier électronique.

Surveillance > Rapports au format PDF > Planificateur de courrier électronique

Utilisez le planificateur de courrier électronique pour planifier la distribution de rapports par courrier électronique. Avant d'ajouter un planning, vous devez définir des groupes de rapports et un profil de messagerie. Reportez-vous à Surveillance > Rapports au format PDF > Groupes de rapports et Périphérique > Profils de serveur > E-mail.

L'exécution des rapports planifiés commence à 2h00 et le transfert du courrier électronique s'effectue à la fin de l'exécution de tous les rapports planifiés.

Paramètres du planificateur de courrier électronique	Description
Name (Nom)	Saisissez un nom pour identifier le planning (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Groupe de rapports	Sélectionnez le groupe de rapports (Surveillance > Rapports au format PDF > Groupes de rapports) ou le rapport d'Utilisation de l'application SaaS (Surveillance > Rapports PDF > Utilisation de l'application SaaS) que vous souhaitez planifier.
Profil de messagerie	Sélectionnez le profil qui définit les paramètres de messagerie. Pour plus d'informations sur la définition des profils de messagerie, reportez-vous à Périphérique > Profils de serveur > E-mail.
Récurrence	Sélectionnez la fréquence à laquelle le rapport doit être généré et envoyé.
Contrôle prioritaire sur les adresses électroniques	Saisissez une adresse de courrier électronique facultative à utiliser à la place du destinataire défini dans le profil de messagerie.
Envoyer le courrier électronique de test	Cliquez pour envoyer un courrier électronique de test à l'adresse de messagerie définie dans le **Profil de messagerie** sélectionné.

Surveillance > Gérer des rapports personnalisés

Vous pouvez créer des rapports personnalisés à exécuter sur demande ou selon la planification (chaque nuit). Pour les rapports prédéfinis, sélectionnez **Monitor (Surveillance)** > **Reports (Rapports)**.

Une fois que le pare-feu a généré un rapport personnalisé planifié, vous risquez d'invalider les résultats antérieurs du rapport si vous modifiez sa configuration pour changer les résultats ultérieurs. Si vous devez modifier la configuration d'un rapport planifié, il est recommandé de créer un nouveau rapport.

Vous devez **Add (Ajouter)** un rapport personnalisé pour en créer un nouveau. Pour que le rapport se base sur un modèle existant, cliquez sur **Load Template (Charger un modèle)** et sélectionnez le modèle. Pour générer un rapport sur demande, au lieu de ou en plus du moment **Scheduled (Planifié)**, cliquez sur **Run Now (Exécuter maintenant)**. Indiquez les paramètres suivants pour définir un rapport.

Paramètres d'un rapport personnalisé	Description
Name (Nom)	Donnez un nom au rapport (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Description	Saisissez une description pour le rapport personnalisé.
Base de données	Sélectionnez la base de données à utiliser comme source de données pour le rapport.
Planifié	Sélectionnez cette option pour exécuter le rapport de nuit. Le rapport est rendu accessible en sélectionnant **Monitor (Surveillance)** > **Reports (Rapports)**.
Intervalle de temps	Sélectionnez un délai fixe ou choisissez **Custom (Personnalisé)** et indiquez une date et un délai.
Trier par	Sélectionnez des options de tri afin d'organiser le rapport, y compris la quantité d'informations à y inclure. Les options disponibles dépendent du choix de base de données.
Regrouper par	Sélectionnez des options de regroupement afin d'organiser le rapport, y compris la quantité d'informations à inclure dans le rapport. Les options disponibles dépendent du choix de base de données.
Colonnes	Sélectionnez les colonnes Disponible à inclure dans le rapport personnalisé et ajoutez-les (⊕) aux colonnes Sélectionné. Sélectionnez **Up (Déplacer en haut)**, **Down (Déplacer en bas)**, **Top (Monter)** et **Bottom (Descendre)** pour réorganiser les colonnes sélectionnées.

Paramètres d’un rapport personnalisé	Description
	Au besoin, vous pouvez également sélectionner et supprimer (⊖) les colonnes précédemment sélectionnées.
Générateur de requêtes	Pour générer une requête de rapport, indiquez les options suivantes et cliquez sur **Add (Ajouter)**. Répétez ces différentes étapes, le cas échéant, pour formuler une requête complète. • **Connector (Connecteur)** - Sélectionnez le connecteur (**and (et)** ou **or (ou)**) devant précéder l'expression que vous ajoutez. • **Negate (Refuser)** - Sélectionnez cette option pour interpréter la requête en tant que refus. Dans l'exemple précédent, l'option de refus fait correspondre des entrées qui ne figurent pas dans les dernières 24 heures ou qui ne proviennent pas d'une zone « non sécurisée ». • **Attribute (Attribut)** : sélectionnez un élément de donnée. Les options disponibles dépendent du choix de base de données. • **Operator (Opérateur)** : sélectionnez des critères pour déterminer si un attribut s'applique (comme =). Les options disponibles dépendent du choix de base de données. • **Value (Valeur)** : indiquez la valeur de l'attribut à faire correspondre.

Pour plus d’informations, reportez-vous à la section Génération de rapports personnalisés.

Surveillance > Rapports

Le pare-feu fournit plusieurs rapports (les 50 principaux) concernant les statistiques du trafic pour le jour précédent ou un jour sélectionné au cours de la semaine précédente.

Pour afficher un rapport, développez une catégorie de rapport (comme Rapports personnalisés) sur le côté droit de la page et sélectionnez un nom de rapport. La page répertorie les rapports dans les sections. Vous pouvez afficher des informations dans chaque rapport pour la période sélectionnée.

Par défaut, le pare-feu affiche tous les rapports pour le jour calendaire précédent. Pour afficher les rapports d'un autre jour, sélectionnez une date de génération de rapport dans le calendrier dans le coin inférieur droit de la page.

Pour afficher les rapports sur un système autre que le pare-feu, sélectionnez une option d'exportation :

- **Exporter vers un fichier PDF**
- **Exporter vers un fichier CSV**
- **Exporter vers un fichier XML**

Politiques

Les rubriques suivantes décrivent les types de stratégie de pare-feu, la manière de déplacer ou cloner des stratégies et ainsi que les paramètres de stratégie :

- Types de politique
- Déplacement ou clonage d’une règle de politique
- Archive des commentaires d’audit
- Requête sur le nombre d’utilisations de la règle
- Politiques > Sécurité
- Politiques > NAT
- Politiques > QoS
- Politiques > Transfert basé sur une politique
- Politiques > Déchiffrement
- Politiques >Broker de paquets de réseau
- Politiques > Inspection des tunnels
- Politiques > Contrôle prioritaire sur l'application
- Politiques > Authentification
- Politiques > Protection DoS
- Politiques > SD-WAN

Types de politique

Les politiques vous permettent de contrôler le fonctionnement du pare-feu en mettant des règles en application et en automatisant des actions. Le pare-feu prend en charge les types de politiques suivantes :

- Les politiques de sécurité de base visant à bloquer ou autoriser une session réseau en fonction de l'application, des zones et adresses source et de destination ou, en option, du service (port et protocole). Les zones identifient les interfaces physiques ou logiques qui envoient ou reçoivent le trafic. Voir Politiques > Sécurité.
- Politiques de traduction des adresses réseau (Network Address Translation, NAT) visant à traduire des adresses et des ports. Voir Politiques > NAT.
- Politiques de qualité du service (QoS) visant à déterminer comment le trafic est classé en vue de son traitement lorsqu'il transite par une interface sur laquelle la QoS est activée. Voir Politiques > QoS.
- Politiques de transfert basé sur une politique visant à appliquer un contrôle prioritaire sur la table de routage et à indiquer une interface de trafic sortant. Voir Politiques > Transfert basé sur une politique (PBF).
- Politiques de déchiffrement visant à déchiffrer le trafic pour les politiques de sécurité. Chaque politique peut définir les catégories d'URL pour le trafic à déchiffrer. Le déchiffrement SSH est utilisé pour identifier et contrôler la tunnellisation SSH en plus de l'accès au shell SSH. Voir Politiques > Déchiffrement.
- Les politiques d'inspection des tunnels pour imposer la sécurité, la Protection DoS et les politiques QoS sur le trafic par tunnel et pour visualiser l'activité du tunnel. Voir Politiques > Inspection des tunnels.
- Politiques de contrôle prioritaire visant à appliquer un contrôle prioritaire sur les définitions d'applications fournies par le pare-feu. Voir Politiques > Contrôle prioritaire sur l'application.
- Les politiques d'authentification pour définir l'authentification pour les utilisateurs finaux qui ont accès aux ressources du réseau. Voir Politiques > Authentification.
- Politiques de déni de service (DoS) visant à assurer une protection contre les attaques'A0;DoS et à prendre des mesures de protection en cas de correspondance des règles. Voir Politiques > Protection DoS.
- Les politiques SD-WAN déterminent la gestion des chemins des liens entre la zone source et la zone de destination lorsque l'état des chemins des liens se dégrade sous le seuil établi par les mesures d'état approuvés et configurés. Voir Politiques > SD-WAN.

Les politiques partagées envoyées depuis Panorama ™ s'affichent en orange sur l'interface Web du pare-feu. Vous pouvez modifier ces politiques partagées uniquement sur Panorama ; vous ne pouvez pas les modifier sur le pare-feu.

Afficher la base de règles en tant que groupes pour afficher tous les groupes d'étiquettes d'une base de règles. Dans les bases de règles disposant de nombreuses règles, afficher la base de règles en tant que groupe simplifie l'affichage en présentant les étiquettes, le code de couleur et le nombre de règles contenu dans chaque groupe tout en préservant la hiérarchie des règles établie.

Déplacement ou clonage d’une règle de politique

Lorsque vous déplacez ou clonez des politiques, vous pouvez définir une **Destination** (un système virtuel sur un pare-feu ou un groupe de périphériques sur Panorama) pour laquelle vous disposez d’autorisations d’accès, y compris l’emplacement partagé.

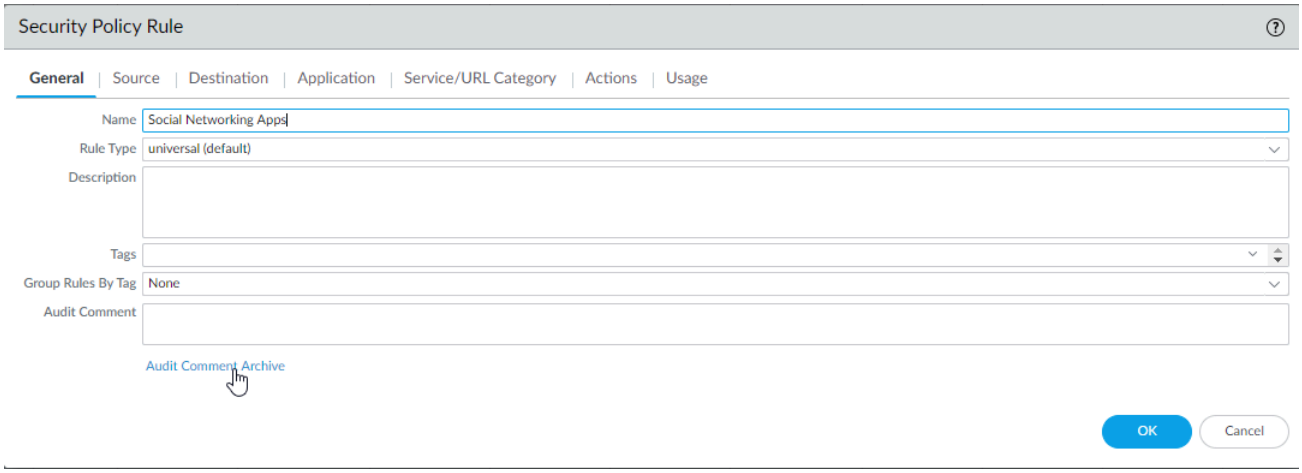
Pour déplacer une règle de politique, sélectionnez-la dans l’onglet **Policies (Politiques)**, cliquez sur **Move (Déplacer)**, sélectionnez **Move to other vsys (Passer à un autre système virtuel)** (pare-feu uniquement) ou **Move to different rulebase or device group (Passer à une autre règle de base ou un autre groupe de périphériques)** (Panorama uniquement), spécifiez les champs dans le tableau suivant et cliquez sur **OK**.

Pour cloner une règle de politique, sélectionnez-la dans l'onglet **Policies (Politiques)**, cliquez sur **Clone (Cloner)**, renseignez les champs du tableau suivant, puis cliquez sur **OK**.

Paramètres de déplacement/ clonage	Description
Règles sélectionnées	Affiche le nom et l'emplacement actuel (système virtuel ou groupe de périphériques) des règles de politique que vous avez sélectionnées pour l'opération.
Destination	Sélectionnez le nouvel emplacement de la politique ou de l'objet : un système virtuel, un groupe de périphériques ou un emplacement partagé. La valeur par défaut est le **Virtual System (Système virtuel)** ou le **Device Group (Groupe de périphériques)** que vous avez sélectionné dans l'onglet **Policies (Politiques)** ou **Objects (Objets)**.
Ordre des règles	Sélectionnez la position de la règle par rapport aux autres règles : • **Move top (Monter)** - La règle va précéder toutes les autres règles. • **Move bottom (Descendre)** - La règle va suivre toutes les autres règles. • **Before rule (Avant la règle)** - Dans la liste déroulante adjacente, sélectionnez la règle suivante. • **After rule (Après la règle)** - Dans la liste déroulante adjacente, sélectionnez la règle précédente.
Erreur sortante dès la première erreur détectée lors de la validation	Sélectionnez cette option (sélectionnée par défaut) pour que le pare-feu ou Panorama affiche la première erreur trouvée et arrête de rechercher d'autres erreurs. Par exemple, une erreur se produit si la **Destination** ne contient aucun objet référencé dans la règle de la politique que vous déplacez. Si vous désélectionnez cette option, le pare-feu ou Panorama trouvera toutes les erreurs avant de les afficher.

Archive des commentaires d’audit

Sélectionnez **Archive des commentaires d’audit** pour afficher l’historique des commentaires d’audit, les journaux de configuration et l’historique des changements apportés à une règle de politique sélectionnée.



- Commentaires d’audit
- Journaux de configuration (entre les validations)
- Changements des règles

Commentaires d’audit

Afficher l’historique des **Commentaires d’audit**applicable à une règle de politique sélectionnée. Appliquez et enregistrez les filtres pour identifier rapidement des commentaires d’audit spécifiques et pour exporter les commentaires d’audit affichés au format CSV.

Champ	Description
Moment de validation	Moment auquel le commentaire a été validé
Commentaire d’audit	Contenu du commentaire d’audit.
Administrateur	Utilisateur qui a validé le commentaire d'audit.
Version de la configuration	Version de la révision de configuration. 0 indique la première fois que la règle de politique a été créée et validée dans Panorama.

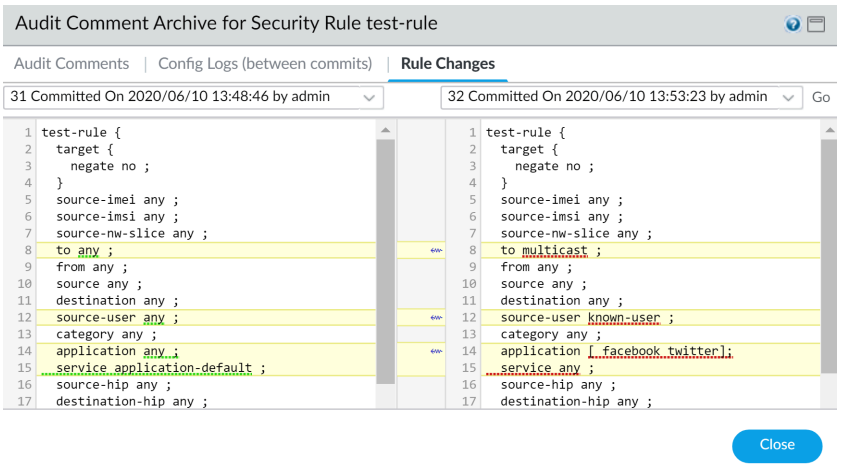
Journaux de configuration (entre les validations)

Affichez le journal de configuration généré par la règle de politique sélectionnée entre les validations. Appliquez et enregistrez les filtres pour identifier rapidement des journaux de configuration spécifiques et pour exporter les journaux de configuration affichés au format CSV.

Champ	Description
Période	Moment auquel le commentaire a été validé
Administrateur	Contenu du commentaire d’audit.
Commande	Type de commande exécuté.
Avant les modifications	Informations relatives à la règle avant le changement. Par exemple, si vous renommez une règle, l’ancien nom s’affiche.
Après modification	Informations relatives à la règle après le changement. Par exemple, si vous renommez une règle, le nouveau nom s’affiche.
Nom du périphérique	Nom du périphérique avant la modification des commentaires d’audit.

Changements des règles

Afficher et comparer la version de la configuration de la règle de politique sélectionnée pour analyser les changements qui se sont produits. Dans le menu déroulant, sélectionnez les deux versions de configuration des règles de politique que vous souhaitez comparer.



Requête sur le nombre d’utilisations de la règle

- **Politiques** > **Rule Usage (Utilisation d'une règle)**

Utilisez la requête sur le nombre d’utilisations de la règle pour filtrer la base de règle sélectionnée sur une période de temps donnée. La requête sur l’utilisation des règles vous permet de filtrer rapidement votre base de règles de politique pour identifier les règles non utilisées à des fins de suppression pour que vous puissiez réduire les points d’entrée ouverts aux pirates. Cliquez sur **PDF/CSV** pour exporter les règles filtrées au format PDF ou CSV. Pour utiliser la requête sur le nombre d’utilisations de la règle, vous devez activer le paramètre **Policy Rule Hit Count (Requête sur le nombre d’utilisation de la règle)** (Périphérique > Configuration > Gestion).

Par défaut, les colonnes **Name (Nom)**, **Location (Emplacement)**, **Created (Créé)**, **Modified (Modifié)** et **Rule Usage (Utilisation de la règle)** s'affichent lorsque vous interrogez l’utilisation de la règle dans votre base de règles de politique. Vous pouvez ajouter plus de colonnes pour afficher des renseignements supplémentaires sur les règles de politique.

Tâche	Description
Nombre de correspondances	
Délai	Indiquez le délai au cours duquel interroger la base de règles sélectionnée. Sélectionnez un délai prédéterminé ou définissez un délai **Custom (Personnalisé)**.
Usage	Sélectionnez l’utilisation de la règle à interroger : **Any (Indifférent)**, **Unused (Non utilisée)**, **Used (Utilisée)** ou **Partially Used (Partiellement utilisée)** (Panorama uniquement).
Depuis	(Délai personnalisé uniquement) Sélectionnez la date et l’heure de l’interrogation de la base de règles de politique.
Exclure la réinitialisation des règles au cours des _ derniers jours	Sélectionnez cette option pour exclure les règles qui ont été manuellement réinitialisées par un utilisateur au cours du nombre de jours indiqués.
Actions	
Supprimer	Supprimez une ou plusieurs règles de politique sélectionnées.
Activer	Activez une ou plusieurs règles de politique sélectionnées lorsque cela est désactivé.
Désactiver	Désactivez une ou plusieurs règles de politique sélectionnées.
PDF/CSV	Exportez les règles de politique filtrées actuellement affichées au format PDF ou CSV.

Tâche	Description
Réinitialiser le Compteur d’accès de la règle	Réinitialisez les données d’utilisation de la règle pour les **Selected rules (règles sélectionnées)** ou pour **All rules (toutes les règles)** qu ont été filtrées et sont actuellement affichées.
Étiquette	Appliquez une ou plusieurs étiquettes de groupe à une ou plusieurs règles de politique sélectionnées. L’étiquette de groupe doit déjà exister afin d’étiqueter la règle/les règles de politique.
Supprimer l’étiquette	Supprimez une ou plusieurs étiquettes de groupe d’une ou plusieurs règles de politique.

Requête sur le nombre d’utilisations de la règle du périphérique

Vous pouvez afficher l’utilisation de la règle du système virtuel et du périphérique lorsque vous affichez l’utilisation de la règle d’une politique de Panorama ou du serveur de gestion. **Reset Rule Hit Counter (Réinitialiser le compteur d’une règle)** pour réinitialiser le nombre de correspondances, la première correspondance et la dernière correspondance.

Cliquez sur **PDF/CSV** pour exporter les règles filtrées au format PDF ou CSV.

Champ	Description
Groupe de périphériques	Le groupe de périphériques auquel le périphérique ou le système virtuel appartient.
Nom de périphérique/ Système virtuel	Nom du groupe de périphériques ou du système virtuel.
Nombre de correspondances	Nombre total de correspondances du trafic à la règle de politique.
Dernière correspondance	Date et heure de la dernière correspondance du trafic à la règle de politique.
Première correspondance	Date et heure de la première correspondance du trafic à la règle de politique.
Dernière mise à jour reçue	Date et heure des dernières informations d'utilisation de la règle reçues du pare-feu ou du serveur de gestion Panorama.
Créé	Date et heure de création de la règle de politique.

Champ	Description
Modifié	Date et heure de la dernière modification de la règle de politique. La colonne est vide si la règle de politique n'a pas été modifiée.
État	L’état de la connexion du périphérique : `Connected` ou `Disconnected`.

Politiques > Sécurité

Les règles de politiques de sécurité référencent les zones de sécurité et vous permettent d'autoriser, de limiter et de suivre le trafic sur votre réseau en fonction des applications, des utilisateurs ou groupes d'utilisateurs et des services (port et protocole). Par défaut, le pare-feu inclut une règle de sécurité nommée *règle1* qui autorise tout trafic issu d'une zone approuvée vers une zone non approuvée.

Que voulez-vous savoir ?	Reportez-vous à la section :
Qu'est-ce qu'une politique de Sécurité ?	Présentation de la politique de sécurité Pour Panorama, reportez-vous à Déplacer ou cloner une règle de stratégie
Quels sont les champs disponibles pour créer une règle de politique de Sécurité ?	Blocs de construction dans une règle de politique de sécurité
Comment puis-je utiliser l'interface Web pour gérer des règles de politique de Sécurité ?	Création et gestion des politiques Application d'un contrôle prioritaire ou rétablissement d'une règle de politique de sécurité Applications et utilisation Optimiseur de la politique de sécurité
Vous souhaitez en savoir plus ?	Politique de Sécurité

Présentation de la politique de sécurité

Les politiques de sécurité vous permettent d'appliquer des règles et d'agir. Elles peuvent être aussi générales ou spécifiques que vous le souhaitez. Les règles des politiques sont comparées au trafic entrant dans un ordre précis, et comme la première règle qui correspond au trafic est appliquée, les règles spécifiques doivent précéder les règles plus générales. Par exemple, une règle correspondant à une application unique doit précéder une règle correspondant à l'ensemble des applications si tous les autres paramètres relatifs au trafic sont identiques.

Pour s'assurer que les utilisateurs finaux s'authentifient lorsqu'ils essaient d'accéder à vos ressources réseau, le pare-feu évalue la politique d'Authentification avant la politique de Sécurité. Pour plus d'informations, voir Politiques > Authentification.

Pour le trafic qui ne correspond à aucune règle définie par l'utilisateur, les règles par défaut s'appliquent. Les règles par défaut, qui s'affichent en bas de la base des règles de sécurité, sont prédéfinies pour autoriser l'ensemble du trafic intra-zone (au sein de la zone) et refuser le trafic inter-zone (entre les zones). Bien que ces règles fassent partie de la configuration prédéfinie et soient en lecture seule par défaut, vous pouvez appliquer un **Override (Contrôle prioritaire)** afin de modifier un nombre limité de paramètres,

notamment les étiquettes, l'action (autoriser ou refuser), les paramètres des journaux et les profils de sécurité.

L’interface contient les onglets suivants pour définir les règles de politique de Sécurité.

- **General (Général)** – Sélectionnez l’onglet **General (Général)** pour définir un nom et une description pour la règle de politique de Sécurité.
- **Source** - Sélectionnez l'onglet **Source** pour définir la zone source ou l'adresse source qui génère le trafic.
- **User (Utilisateur)** - Sélectionnez l'onglet **User (Utilisateur)** pour appliquer la politique à des utilisateurs individuels ou à un groupe d'utilisateurs. Si vous utilisez GlobalProtect™ et que l’option profil d’informations sur l’hôte (HIP) est activée, vous pouvez également baser la politique sur les informations collectées par GlobalProtect. Par exemple, le niveau d'accès de l'utilisateur peut être déterminé par un HIP qui indique au pare-feu la configuration locale de l'utilisateur. Les informations HIP peuvent être utilisées pour un contrôle d'accès granulaire basé sur les programmes de sécurité exécutés sur l'hôte, les valeurs du registre et de nombreuses autres vérifications telles que l'installation ou non du logiciel antivirus sur l'hôte.
- **Destination** - Sélectionnez l'onglet **Destination** pour définir la zone de destination ou l'adresse de destination du trafic.
- **Application** – Sélectionnez l’onglet **Application** pour définir l’action de la politique en fonction d’une application ou d’un groupe d’applications. Un administrateur peut également utiliser une signature App-ID™ existante et la personnaliser pour détecter les applications propriétaires ou certains attributs d’une application existante. Les applications personnalisées sont définies dans **Objects (Objets)** > **Applications**.
- **Service/URL Category (Catégorie de Service / URL)** – Sélectionnez l’onglet **Service/URL Category (Catégorie de Service / URL)** pour indiquer un protocole TCP et/ou un numéro de port UDP ou une catégorie d’URL spécifique comme critère de correspondance dans la politique.
- **Actions** : Sélectionnez l'onglet **Actions** pour déterminer l'action qui sera prise en fonction du trafic correspondant aux attributs de la politique définie.
- **Target (Cible)** : Sélectionnez l’onglet **Target (Cible)** pour préciser les périphériques ou les étiquettes de la règle de politique de sécurité.
- **Usage (Utilisation)** - Sélectionnez l’onglet **Usage (Utilisation)** pour afficher l’utilisation d’une règle, y compris le nombre d’applications vues sur une règle, la dernière fois que des nouvelles applications ont été vues sur la règle, les données du Compteur d’accès, le trafic des 30 derniers jours, la date de création de la règle et la date de sa dernière modification.

Blocs de construction dans une règle de politique de sécurité

- Politiques > Sécurité

La section suivante décrit chaque composant d’une règle de politique de Sécurité. Lorsque vous créez une règle de politique de Sécurité, vous pouvez configurer les options décrites ici.

Éléments de base d'une politique de sécurité	Configuré dans	Description
Numéro de règle	S. O.	Le pare-feu numérote automatiquement chaque règle, et l'ordre des règles change à mesure que les règles sont déplacées. Lorsque vous filtrez des règles pour rechercher des règles correspondant à un ou plusieurs filtres spécifiques, chaque règle s'affiche avec son numéro dans l'ensemble des règles de la base de règles et sa position dans l'ordre d'évaluation. Panorama numérote indépendamment les règles avant et les règles après. Lorsque Panorama transfère les règles à un pare-feu géré, la numérotation des règles intègre la hiérarchie dans les règles avant, les règles de pare-feu et les règles après d'une base de règles et reflète la séquence de règles et son ordre d'évaluation.
Nom	**Général**	Donnez un nom à la règle afin de l'identifier. Le nom est sensible à la casse et peut comporter jusqu'à 63 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement. Le nom doit être unique sur un pare-feu et, dans Panorama, unique au sein de son groupe de périphériques et des groupes de périphériques anciens ou descendants.
Type de règle		Indique si la règle s'applique au trafic dans une zone, entre des zones ou aux deux'A0;: • **universal (universel)** (par défaut) : applique la règle à l'ensemble du trafic inter-zone et intra-zone correspondant dans les zones source et de destination indiquées. Par exemple, si vous créez une règle universelle pour les zones source A et B et de destination A et B, la règle s'applique à l'ensemble du trafic dans la zone A, dans la zone B, ainsi que de la zone A à la zone B et de la zone B à la zone A. • **intrazone (intra-zone)** : applique la règle à l'ensemble du trafic correspondant dans les zones source indiquées (vous ne pouvez pas indiquer de zone de destination pour les règles intra-zone). Par exemple, si vous définissez la zone source sur A et B, la règle s'applique à l'ensemble du trafic dans les zones A et B, mais pas entre les zones A et B. • **interzone (inter-zone)** : applique la règle à l'ensemble du trafic correspondant entre les zones source et de destination indiquées. Par exemple, si vous définissez la zone source sur A, B et C, et la zone de destination

Éléments de base d'une politique de sécurité	Configuré dans	Description
		sur A et B, la règle s'applique à l'ensemble du trafic de la zone A à la zone B, de la zone B à la zone A, de la zone C à la zone A, de la zone C à la zone B, mais pas au trafic dans les zones A, B et C.
Description		Saisissez une description de la politique (1 024 caractères maximum).
Étiquettes		Spécifiez l'étiquette pour la politique. Une étiquette de politique est un mot-clé ou une expression qui vous permet de trier ou de filtrer les politiques. Cela est utile lorsque vous avez défini de nombreuses politiques et que vous souhaitez afficher celles qui sont identifiées par un mot-clé particulier. Par exemple, vous pouvez ajouter des étiquettes à certaines règles avec des mots spécifiques, tels que Déchiffrement et Aucun déchiffrement, ou utiliser le nom d'un centre de données spécifique pour les politiques associées à cet emplacement. Vous pouvez également ajouter des étiquettes aux règles par défaut.
Zone source	**Source**	Il faut **Ajouter** des zones source (la valeur par défaut est **tout**). Les zones doivent être du même type (couche 2, couche 3 ou câble virtuel). Pour définir de nouvelles zones, voir Réseau > Zones. Il est possible d'utiliser plusieurs zones pour simplifier la gestion. Par exemple, si vous possédez trois zones internes différentes (marketing, ventes et relations publiques) qui sont toutes reliées à la zone de destination non approuvée, vous pouvez créer une règle qui couvre tous les cas possibles.
Adresse source	**Source**	Cliquez sur **Add (Ajouter)** des adresses, des groupes d'adresses ou des régions source (la valeur par défaut est **Any [indifférent]**). Faites votre sélection dans la liste déroulante ou sélectionnez l'objet d'**Adresse**, le **Groupe d'adresses** ou les **Régions** (en bas de la liste déroulante) pour définir les paramètres. Objets>Adresses et Objets>Groupes d'adresses décrivent les types d'objets d'adresses et les groupes d'adresses, respectivement, qu'une règle de politiques de sécurité prend en charge.

Éléments de base d'une politique de sécurité	Configuré dans	Description
		Si vous sélectionnez l’option **inverse**, la règle appliquera les adresses source de la zone spécifiée, à l’exception des adresses spécifiées.
Utilisateur source	**Source**	**Ajoutez** les utilisateurs ou les groupes d'utilisateurs source soumis à la politique : • **Tout** - Inclut tout trafic, quelles que soient les données utilisateur. • **pré-ouverture de session** - Inclut les utilisateurs distants connectés au réseau à l'aide de GlobalProtect mais non connectés à leur système. Lorsque l'option Pré-ouverture de session est configurée sur le portail des terminaisons GlobalProtect, tout utilisateur non connecté à sa machine est identifié avec le nom d'utilisateur pre-logon. Vous pouvez ensuite créer des politiques pour les utilisateurs pre-logon. Bien que l'utilisateur ne soit pas directement connecté, sa machine est authentifiée sur le domaine, comme s'il était complètement connecté. • **Utilisateur connu** – Inclut tous les utilisateurs authentifiés, c’est-à-dire toute adresse IP dont les données utilisateur sont mappées. Cette option est équivalente au groupe d'utilisateurs du domaine sur un domaine. • **inconnu** - Inclut tous les utilisateurs non authentifiés, c'est-à-dire les adresses IP non mappées à un utilisateur. Par exemple, vous pouvez utiliser l’option **Inconnu** pour accéder à quelque chose au niveau invité, car les invités ont une adresse IP sur votre réseau, mais ne sont pas authentifiés sur le domaine et ne disposent d’aucune information de mappage utilisateur/adresse IP sur le pare-feu. • **Sélection** - Inclut les utilisateurs sélectionnés dans cette fenêtre. Par exemple, vous pouvez ajouter un utilisateur, une liste d'individus, certains groupes ou des utilisateurs manuellement. *Si le pare-feu collecte les informations utilisateur depuis un serveur RADIUS, TACACS+ ou le serveur du fournisseur d’identité SAML et non depuis l’agent User-ID™, la liste des utilisateurs ne s’affiche pas ; vous devez saisir les informations de l’utilisateur manuellement.*

Éléments de base d'une politique de sécurité	Configuré dans	Description
Périphérique source	**Source**	**Ajoutez** les périphériques hôtes soumis à la politique : • **Tout** : inclut n'importe quel périphérique. • **pas de hip** – Les informations HIP ne sont pas requises. Ce paramètre permet d'accéder à des périphériques tiers qui ne peuvent pas collecter ou soumettre des informations HIP. • **quarantaine**: inclut n'importe quel périphérique qui se trouve sur cette liste de quarantaine (**Périphérique** > **Quarantaine du périphérique**). • **sélectionner** : Inclut les périphériques sélectionnés comme déterminé par votre configuration. Par exemple, vous pouvez ajouter un périphérique sur la base d'un modèle, OS, famille d'OS ou fournisseur.
Profil HIP source	**Source**	**Ajouter** des profils HIP (profils d'informations sur l'hôte) vous permet de collecter des informations sur l'état de sécurité de vos hôtes, à savoir s'ils ont installé les derniers correctifs de sécurité et les dernières définitions antivirus. L'utilisation des profils d'informations sur l'hôte pour la mise en œuvre d'une stratégie active la sécurité granulaire qui garantit que les hôtes distants accédant à vos ressources vitales sont adéquatement maintenus et en conformité avec vos normes de sécurité avant de les autoriser à accéder à vos ressources réseau. Les profils HIP source suivants sont pris en charge : • **Indifférent** – Inclut tous les terminaux, quelles que soient les informations HIP. • **Sélectionner** – Inclut les profils HIP sélectionnés comme déterminé par votre configuration. Par exemple, vous pouvez ajouter un profil HIP, une liste de profils HIP ou ajouter des profils HIP manuellement. • **pas de hip** – Les informations HIP ne sont pas requises. Ce paramètre permet d'accéder à des clients tiers qui ne peuvent pas collecter ou soumettre des informations HIP.
Abonné source	**Source**	**Ajoutez** un ou plusieurs abonnés source à un réseau 5G ou 4G en utilisant les formats suivants : • **indifférent** • (5G uniquement) identifiant permanent d'abonnement 5G (SUPI) incluant le numéro IMSI • Numéro IMSI (14 ou 15 chiffres)

Éléments de base d'une politique de sécurité	Configuré dans	Description
		• La fourchette des valeurs IMSI va de 11 à 15 chiffres, séparés par un tiret • Le préfixe IMSI de six chiffres, avec une astérisque (*) en tant que caractère de remplacement après le préfixe • EDL qui spécifie les IMSI
Equipement source		**Ajoutez** une ou plusieurs ID d'équipement source à un réseau 5G ou 4G en utilisant les formats suivants : • **indifférent** • (5G uniquement) Identifiant d'équipement permanent 5G (PEI) incluant le numéro d'identité international d'équipement mobile (IMEI) • IMEI (de 11 à 16 chiffres) • Préfixe IMEI de huit chiffres pour le Code d'attribution de type (TAC) • EDL qui spécifie les IMEI
Partie du réseau	**Source**	**Ajoutez** un ou plusieurs portion du réseau sources sur la base du type de service de portion du réseau (SST) sur un réseau 5G, comme suit : • **SST normalisé (prédéfini)** • **eMBB** (enhanced Mobile Broadband - Large bande mobile améliorée) : pour des vitesses et des taux de données élevés plus rapides, comme le streaming de vidéos. • **URLLC** Communications à faible latence ultra fiables : pour les applications cruciales à une mission qui sont sensibles à la latence, comme les IoT critiques (soins de santé, paiements sans fil, contrôle du domicile, et communication des véhicules). • **MIoT** Internet massif des objets : par exemple, les mesures intelligentes, la gestion intelligente des déchets, la lutte contre les vols, la gestion des actifs et la géolocalisation. • **SST portion du réseau - Spécifique à l'opérateur** : vous nommez et indiquez la portion. Le format du nom de la tranche est un texte suivi d'une virgule (,) et un chiffre (allant de 128 à 255). Par exemple, Enterprise Oil2, 145.

Éléments de base d'une politique de sécurité	Configuré dans	Description
Zone de destination	**Destination**	Il faut **Ajouter** des zones de destination (la valeur par défaut est **(n'importe laquelle**). Les zones doivent être du même type (couche 2, couche 3 ou câble virtuel). Pour définir de nouvelles zones, voir Réseau > Zones. Il est possible d'utiliser plusieurs zones pour simplifier la gestion. Par exemple, si vous possédez trois zones internes différentes (marketing, ventes et relations publiques) qui sont toutes reliées à la zone de destination non approuvée, vous pouvez créer une règle qui couvre tous les cas possibles. *Vous ne pouvez pas définir de zone de destination pour les règles intra-zone car ces types de règle s'appliquent uniquement au trafic disposant d'une source et d'une destination dans la même zone. Pour indiquer les zones qui correspondent à une règle intra-zone, vous devez définir uniquement la zone source.*
Adresse de destination		Cliquez sur **Ajouter** des adresses, des groupes d'adresses ou des régions de destination (la valeur par défaut est **n'importe laquelle**). Faites votre sélection dans la liste déroulante ou cliquez sur l'objet d'**Adresse**, le **Groupe d'adresses** ou les **Régions** (en bas de la liste déroulante) pour définir les paramètres d'adresses. Objets>Adresses et Objets>Groupes d'adresses décrivent les types d'objets d'adresses et les groupes d'adresses, respectivement, qu'une règle de politiques de sécurité prend en charge. Si vous sélectionnez l'option **inverse**, la règle appliquera les adresses de destination de la zone spécifiée, à l'exception des adresses spécifiées.
Périphérique de destination		**Ajoutez** les périphériques hôtes soumis à la politique : • **Tout** : inclut n'importe quel périphérique. • **quarantaine**: inclut n'importe quel périphérique qui se trouve sur cette liste de quarantaine (**Périphérique** > **Quarantaine du périphérique**). • **sélectionner** : Inclut les périphériques sélectionnés comme déterminé par votre configuration. Par exemple, vous pouvez ajouter un périphérique sur la base d'un modèle, OS, famille d'OS ou fournisseur.

Éléments de base d'une politique de sécurité	Configuré dans	Description
Application	**Application**	**Ajoutez** des applications spécifiques pour la règle de politique de Sécurité. Si une application présente plusieurs fonctions, vous pouvez sélectionner l'application dans son ensemble ou des fonctions individuelles. Si vous sélectionnez l'application dans son ensemble, toutes les fonctions seront incluses et la définition de l'application sera automatiquement mise à jour lors de l'ajout de fonctions supplémentaires. Si vous utilisez des groupes d'applications, des filtres ou des conteneurs dans la règle de politique de Sécurité, vous pouvez en consulter les détails en passant la souris sur l'objet dans la colonne Application, en ouvrant la liste déroulante et en sélectionnant **Valeur**. Ainsi, vous pourrez accéder aux membres des applications directement depuis la politique, sans passer par l'onglet **Objet**. *Spécifiez toujours une ou plusieurs applications de sorte que seules les applications que vous voulez sur votre réseau sont autorisées, ce qui réduit la surface d'attaque et vous donne un plus grand contrôle du trafic réseau. Ne définissez pas l'application sur **n'importe laquelle**, ce qui autorise le trafic de n'importe quelle application et augmente la surface d'attaque.*
Service	**Catégorie de service/URL**	Sélectionnez les services que vous souhaitez limiter à des numéros de ports TCP et/ou UDP spécifiques. Choisissez l'une des options suivantes dans la liste déroulante : • **N'importe laquelle** - Les applications sélectionnées sont autorisées ou non sur n'importe quel protocole ou port. • **valeur par défaut de l'application** - Les applications sélectionnées sont autorisées ou non seulement sur leurs **ports par défaut définis par Palo Alto Networks®**. Cette option est recommandée pour les politiques d'autorisation, car elle empêche l'exécution d'applications sur des ports ou protocoles inhabituels, qui, si elle n'est pas intentionnelle, peut être un signe de comportement et d'utilisation non souhaité des applications.

Éléments de base d'une politique de sécurité	Configuré dans	Description
		Si vous utilisez cette option, le pare-feu vérifiera toujours les applications sur tous les ports, mais les applications seront autorisées uniquement sur leurs ports et protocoles par défaut. *Pour la plupart des applications, utilisez l'option **application par défaut** pour empêcher l'application d'utiliser les ports non standard ou d'afficher d'autres comportements d'évitement. Si le port par défaut de l'application change, le pare-feu met automatiquement à jour la règle en utilisant le bon port par défaut. Pour les applications qui utilisent des ports non standard, comme les applications personnalisées internes, modifiez l'application ou créez une règle qui spécifie les ports non standard et appliquez la règle uniquement au trafic qui exige l'application.* • **Sélectionnez** - **Ajoutez** un service existant ou choisissez **Service** ou **Groupe de services** pour définir une nouvelle entrée. (Ou sélectionnez Objets > Services et Objets > Groupes de services).
Catégorie d'URL		Sélectionnez des catégories d'URL pour la règle de sécurité. • Choisissez **tout** pour autoriser ou non toutes les sessions, quelle que soit la catégorie d'URL. • Pour indiquer une catégorie, **Ajoutez** une ou plusieurs catégories spécifiques (y compris des catégories personnalisées) dans la liste déroulante. Sélectionnez Objets > Listes dynamiques externes pour définir des catégories personnalisées.
Paramètres d'action	**Actions**	Sélectionnez l'**Action** que le pare-feu prend à l'égard du trafic qui correspond aux attributs définis dans une règle : • **Autoriser** : (par défaut) Autorise le trafic mis en correspondance. • **Refuser** - Bloque le trafic mis en correspondance et applique l'*action Refuser* définie par défaut pour l'application refusée. Pour afficher l'action refuser

Éléments de base d'une politique de sécurité	Configuré dans	Description
		définie par défaut pour une application, consultez les détails de l'application (**Objets** > **Applications**). Étant donné que l'action Refuser par défaut varie d'une application à une autre, le pare-feu pourrait bloquer la session et envoyer une réinitialisation à une application, pendant qu'il abandonne silencieusement la session d'une autre application. • **Abandonner** - Abandonne l'application sans aucune notification. Aucune réinitialisation TCP n'est envoyée à l'hôte ou à l'application, à moins d'avoir sélectionné **Envoyer ICMP inaccessible**. • **Réinitialiser le client** - Envoie une réinitialisation TCP au périphérique côté client. • **Reset server (Réinitialiser le serveur)** - Envoie une réinitialisation TCP au périphérique côté serveur. • **Réinitialiser le client et le serveur** - Envoie une réinitialisation TCP aux périphériques côté client et côté serveur. • **Envoyer ICMP inaccessible** – Uniquement disponible pour les interfaces de Couche 3. Lorsque vous configurez une règle de politique de Sécurité pour abandonner du trafic ou réinitialiser la connexion, le trafic n'atteint pas l'hôte de destination. Dans ces cas-là, pour tout trafic UDP et TCP abandonné, vous pouvez activer le pare-feu pour qu'il envoie une réponse ICMP inaccessible à l'adresse IP source qui génère le trafic. L'activation de ce paramètre permet à la source de fermer ou d'arrêter facilement la session, évitant ainsi le plantage des applications. Pour afficher le taux de paquets ICMP inaccessibles configuré sur le pare-feu, consultez la section Paramètres de la session (**Périphérique** > **Configuration** > **Session**). Pour appliquer un contrôle prioritaire sur l'action par défaut définie sur les règles inter-zones et intra-zones prédéfinies : reportez-vous à la section Application d'un contrôle prioritaire ou rétablissement d'une règle de politique de sécurité.
Paramètres du profil	**Actions**	Pour définir la vérification additionnelle que le pare-feu effectue sur les paquets qui correspondent à la règle de profil de Sécurité, sélectionnez les profils individuels Antivirus, Protection contre les vulnérabilités, Antispyware,

Éléments de base d'une politique de sécurité	Configuré dans	Description
		URL Filtering, Blocage des fichiers, Filtrage des données, Analyse WildFire, Protection de réseau mobile, et SCTP. Pour définir un groupe de profils plutôt que des profils individuels, sélectionnez **Type de profil** qui sera un**groupe** puis sélectionnez un **Profil de groupe**. Pour définir de nouveaux profils ou groupes de profils, cliquez sur **Nouveau** à côté du profil ou sélectionnez **New Group Profile (Nouveau profil de groupe)**). Vous pouvez également joindre des Profils de Sécurité (ou des groupes de profils) aux règles par défaut.
Paramètre des journaux et autres paramètres	**Actions**	Pour générer des entrées dans le journal du trafic local en cas de trafic correspondant à cette règle, sélectionnez les options suivantes'A0;: • **Se connecter au début de la session** (option désactivée par défaut) – Génère une entrée dans le journal du trafic pour le début d'une session. *Évitez d'activer l'option **Se connecter au début de la session** sauf à des fins de résolution de problèmes ou pour que les journaux de session de tunnel présentent les tunnels GRE actifs dans l'ACC. La journalisation à la fin de session consomme moins de ressources et identifie l'application exacte si l'application change après quelques paquets, par exemple, de facebook-base à facebook-chat.* • **Se connecter en fin de session** (option activée par défaut) – Génère une entrée dans le journal du trafic pour la fin d'une session. *Si des entrées pour le début ou la fin de la session sont journalisées, des entrées le sont également en cas d'abandon et de refus.* • **Profil de transfert des journaux** - Pour transférer des entrées du journal du trafic local et du journal des menaces vers des destinations distantes, comme des serveurs Panorama et Syslog, sélectionnez un **Profil de transfert des journaux**.

Éléments de base d'une politique de sécurité	Configuré dans	Description
		*La génération d'entrées du journal des menaces est déterminée par les Profils de Sécurité. Définissez de **nouveaux profils** de journalisation, au besoin (voir Objets > Transfert des journaux).* *Créez et activez des profils de transfert de journaux pour envoyer des journaux à des périphériques de stockage externes dédiés. Les journaux sont alors préservés, car le pare-feu dispose d'une capacité de stockage des journaux limitée et, lorsque l'espace est utilisé, le pare-feu supprime les journaux les plus vieux.* Vous pouvez également modifier les paramètres de journal dans les règles par défaut. Indiquez toute les combinaisons des options suivantes: • **Calendrier** – Pour limiter les dates et les heures auxquelles la règle est en vigueur, sélectionnez un calendrier dans la liste déroulante. Définissez de **Nouveaux** calendriers, au besoin (reportez-vous à Paramètres de contrôle du trafic SSL déchiffré). • **Marquage QoS** – Pour modifier le paramètre de qualité du service (QoS) des paquets qui correspondent à la règle, sélectionnez **IP DSCP** ou **Priorité IP** et saisissez la valeur QoS au format binaire ou sélectionnez une valeur prédéfinie dans le menu déroulant. Pour plus d'informations sur la QoS, reportez-vous à la section Qualité de service . • **Désactiver l'inspection de la réponse du serveur** – Désactive l'inspection des paquets entre le serveur et le client. L'option est désactivée par défaut. *Pour une sécurité optimale, n'activez pas **Désactiver l'inspection de la réponse du serveur**. Lorsque cette option est sélectionnée, le pare-feu n'inspecte que les flux de données client-à-serveur. Il n'inspecte pas les flux de données serveur-à-client et, par conséquent, ne peut déterminer si ces flux de trafic comportent des menaces.*

Éléments de base d'une politique de sécurité	Configuré dans	Description
De Base	**Utilisation d'une règle**	• **Règle créée** : date et heure de création de la règle. • **Dernière modification** : date et heure de la dernière modification de la règle.
Activité	**Utilisation d'une règle**	• **Nombre de correspondances** : nombre total de fois que le trafic a été mis en correspondance avec la règle. • **Première correspondance** : moment de la première correspondance. • **Dernière correspondance** : moment de la dernière correspondance.
Applications	**Utilisation d'une règle**	• **Applications vues** : le nombre d'applications que la règle autorise. • **Dernière application vue** : le nombre de jours depuis que la dernière nouvelle application (une application jamais vue jusqu'à présent) a été vue sur la règle. • **Comparer les applications et les applications vues** : Cliquez sur cette option pour comparer les applications configurées sur la règle aux applications vues dans la règle. Utilisez cette outil pour découvrir les applications qui correspondent à la règle et pour ajouter des applications à la règle.
Traffic (des 30 derniers jours)	**Utilisation d'une règle**	• **Octets** : la quantité, en octets, de trafic de la règle au cours des 30 derniers jours. *Si la période de temps dépasse 30 jours, les plus vieilles règles demeureraient au haut de la liste, car ce sont elles qui risquent d'avoir le plus important trafic cumulé. Les règles les plus récentes pourraient se retrouver sous les plus anciennes règles, même si du trafic important passe par les nouvelles règles.*
Tous (cible tous les périphériques) Panorama uniquement	**Cible**	Activez (cochez) pour valider la règle de politique de tous les pare-feux gérés du groupe de périphériques.
Périphériques		Sélectionnez un ou plusieurs pare-feux gérés associés au groupe de périphériques pour valider la règle de politique.

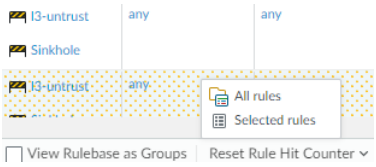
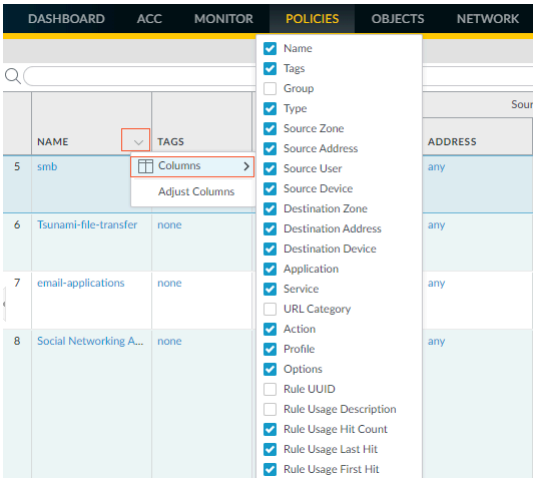
Éléments de base d'une politique de sécurité	Configuré dans	Description
Panorama uniquement		
Étiquettes Panorama uniquement		**Add (Ajoutez)** une ou plusieurs étiquettes pour valider la règle de politique des pare-feux gérés dans le groupe de périphériques ayant l'étiquette indiquée.
Cibler tous les périphériques sauf ceux spécifiés Panorama uniquement		Cochez pour valider la règle de politique pour tous les pare-feux gérés associés au groupe de périphériques sauf pour le(s) périphérique(s) et étiquette(s) sélectionnés.

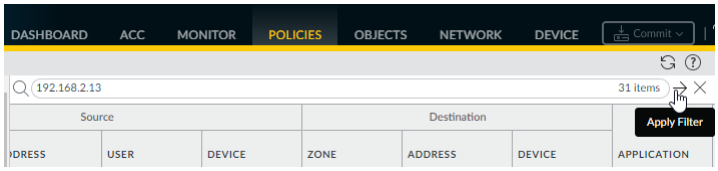
Création et gestion des politiques

Sélectionnez la page **Politiques** > **Sécurité** pour ajouter, modifier et gérer les politiques de sécurité :

Tâche	Description
Ajouter	**Ajoutez** une nouvelle règle de politique ou sélectionnez une règle sur laquelle fonder une nouvelle règle et **Dupliquez la règle**. La règle copiée « règle*n* », où *n* représente le premier nombre entier disponible qui caractérise le nom de la règle, est insérée sous la règle sélectionnée. Pour plus d'informations sur le clonage, reportez-vous à la section Déplacement ou clonage d'une règle de politique.
Modifier	Sélectionnez une règle pour en modifier les paramètres. Si la règle est transmise par Panorama, elle est en lecture seule sur le pare-feu et vous ne pouvez la modifier localement.
	Les actions **écrasez** et **Rétablir** ne concernent que les règles par défaut affichées en bas de la base des règles de Sécurité. Ces règles prédéfinies, autorisant l'ensemble du trafic intra-zone et refusant l'ensemble du trafic inter-zone, indiquent au pare-feu comment gérer le trafic qui ne correspond à aucune autre règle dans la base de règles. Comme elles font partie de la configuration prédéfinie, vous devez appliquer un **écrasez** afin de modifier les paramètres de politique sélectionnés. Si vous utilisez Panorama, vous pouvez également **écrasez** les règles par défaut et les appliquer sur les pare-feu dans un Groupe de périphériques ou un Contexte partagé. Vous pouvez également **Rétablir** les règles par défaut afin de restaurer les paramètres prédéfinis ou les paramètres transmis par Panorama. Pour plus d'informations, reportez-vous à la section Application d'un contrôle prioritaire ou rétablissement d'une règle de politique de sécurité.

Tâche	Description
Se déplacer	Les règles sont évaluées de haut en bas et telles qu'elles apparaissent dans la page **Politiques**. Pour modifier l'ordre d'évaluation des règles par rapport au trafic réseau, sélectionnez une règle et cliquez sur **Déplacer en haut**, **Déplacer en bas**, **Déplacer vers le haut**, **Déplacer vers le bas** ou **Déplacer vers une autre base de règles ou un autre groupe de périphériques.**. Pour plus d'informations, reportez-vous à la section Déplacement ou clonage d'une règle de politique.
Copiez l'UUID.	Copiez l'UUID de la règle au presse-papiers aux fins d'utilisation lors de la recherche de la configuration ou des journaux.
Supprimer	Sélectionnez et **Supprimer** une règle existante.
Activer/ désactiver	Pour désactiver une règle, sélectionnez-la et **Désactivez**-la ; pour activer une règle qui est désactivée, sélectionnez-la et **Enable (Activez)**-la.
Surveiller l'utilisation d'une règle	Pour identifier les règles qui n'ont pas été utilisées depuis le dernier redémarrage du pare-feu, sélectionnez **Mettre en évidence les règles non utilisées**. Les règles non utilisées apparaissent sur un fonds à pois. Vous pourrez ensuite décider de la **Désactiver** ou de la **Supprimer**. Les règles qui ne servent pas à l'heure actuelle s'affichent sur un fond jaune pointillé. Lorsque le compteur d'accès à une règle de politique est activé, les données du Compteur d'accès sont utilisées pour déterminer si une règle est inutilisée. *Chaque pare-feu garde un indicateur de trafic pour les règles ayant une correspondance. Comme l'indicateur est réinitialisé à l'occasion de la réinitialisation du panneau de données au moment d'un redémarrage, dans le cadre des meilleures pratiques, contrôlez cette liste régulièrement pour déterminer si la règle a eu une correspondance depuis le dernier contrôle avant de la supprimer ou de la désactiver.* 
Réinitialiser le Compteur d'accès	Le **Compteur d'accès** suit le trafic total qui correspond à la règle de politique. Ce chiffre demeure après le redémarrage, la mise à niveau et le redémarrage du panneau de données.

Tâche	Description
	Vous pouvez également **Réinitialiser le Compteur d'accès** (menu du bas). Pour effacer les statistiques du compteur d'accès, sélectionnez **All Rules (Toutes les règles)** ou sélectionnez des règles précises et réinitialiser les statistiques du compteur pour les **Règles sélectionnées** uniquement.  Consultez le **Premier accès** pour déterminer la première utilisation de la politique de sécurité. La date est indiquée au format hh:mm:ss année. Vous ne pouvez pas réinitialiser cette valeur. Consultez le **Dernier accès** pour déterminer la dernière utilisation de la politique de sécurité. La date est indiquée au format hh:mm:ss année. Vous ne pouvez pas réinitialiser cette valeur.
Afficher/ Masquer les colonnes	Montrer ou masquer les colonnes qui s'affichent sous **Politiques**. Sélectionnez le nom de la colonne pour faire basculer l'affichage. 
Appliquer des filtres	Pour appliquer un filtre à la liste, faites votre choix parmi la liste déroulante **Règles de filtrage**. Pour définir un filtre, choisissez **Filtre** dans le menu déroulant des éléments. *Les règles par défaut ne font pas partie du filtrage de la base de règles et s'affichent toujours dans la liste des règles filtrées.*
	Pour afficher les sessions réseau consignées comme correspondances par rapport à la politique, sélectionnez **Afficheur de journaux** dans le menu déroulant des noms de règles.

Tâche	Description
	Pour afficher la valeur actuelle, sélectionnez **Valeur** dans le menu déroulant des entrées. Vous pouvez également modifier, filtrer ou supprimer les éléments directement depuis le menu de la colonne. Par exemple, pour afficher les adresses incluses dans un groupe d'adresses, placez votre souris sur l'objet dans la colonne **Adresse**, puis sélectionnez **Valeur** dans la liste déroulante. Ainsi, les membres et les adresses IP correspondantes du groupe d'adresses s'affichent rapidement, sans devoir accéder à l'onglet **Objet**.
	Pour rechercher des objets qui sont utilisés dans une politique basée sur leur nom ou adresse IP, utilisez le filtre. Après avoir appliqué le filtre, vous ne verrez que les éléments qui correspondent à ce dernier. Le filtre fonctionne également avec les objets imbriqués. Par exemple, si vous filtrez 10.1.4.8, seule la politique qui contient cette adresse s'affiche : 
Prévisualiser les règles (Panorama uniquement)	Cliquez sur l'option **Prévisualiser les règles** pour afficher une liste des les règles avant de les appliquer sur les pare-feu gérés. Dans chaque base de règles, la hiérarchie des règles est marquée visuellement pour chaque groupe de périphériques (et pare-feu géré), afin de faciliter l'analyse d'un grand nombre de règles.
Exporter le tableau de configuration	Les rôles administrateur qui sont au moins dotés de l'accès en lecture seule peuvent exporter la base de règles de politique au format **PDF/CSV**. Vous pouvez appliquer des filtres pour créer des sorties du tableau de configuration plus précises, au besoin, par exemple, pour effectuer des audits. Seules les colonnes qui sont visibles dans l'interface Web seront exportées. Reportez-vous à la section Exportation du tableau de configuration.
Surligner la règle inutilisée	Surlignez une règle de politique sans correspondances de trafic dans la colonne **Utilisation d'une règle**.
Groupe	Gérez les groupes d'étiquettes lorsque la case **Afficher la base de règles en tant que groupes** est cochée. Vous pouvez effectuer les actions suivantes : • **Déplacer les règles d'un groupe vers une autre base de règles ou un autre groupe d'appareils**: déplace le groupe de balises sélectionné vers un autre groupe d'appareils. • **Modifier le groupe de toutes les règles** : déplacez les règles du groupe d'étiquettes sélectionné vers un autre groupe d'étiquettes dans la base de règles • **Supprimer toutes les règles du groupe** : supprime toutes les règles d'un groupe d'étiquettes sélectionné.

Tâche	Description
	• **Dupliquer toutes les règles du groupe** : clone toutes les règles d'un groupe d'étiquettes sélectionné vers un groupe de périphériques.
Afficher la base de règles en tant que groupes	Sélectionnez **Afficher la base de règles en tant que groupes** pour afficher la base de règles de la politique au moyen de l'étiquette utilisée dans **Règles de groupe par étiquette**. Les règles de politique visibles sont celles qui appartiennent au groupe d'étiquettes sélectionné.
Tester la correspondance de la politique	Effectuez un test des politiques de protection pour la base de règles de politique sélectionnée pour vérifier que le bon trafic est refusé et autorisé.

Application d'un contrôle prioritaire ou rétablissement d'une règle de politique de sécurité

Les règles de sécurité par défaut, inter-zone (par défaut) et intra-zone (par défaut), disposent de paramètres prédéfinis qui peuvent avoir un contrôle prioritaire sur un pare-feu ou sur Panorama. Si un pare-feu reçoit les règles par défaut d'un groupe de périphériques, vous pouvez également appliquer un contrôle prioritaire sur les paramètres du groupe de périphériques. Le pare-feu ou le système virtuel sur lequel vous appliquez un contrôle prioritaire stocke une version locale de la configuration de la règle. Les paramètres sur lesquels vous pouvez appliquer un contrôle prioritaire sont un sous-ensemble de l'ensemble complet (le tableau suivant affiche une liste du sous-ensemble des règles de sécurité). Pour plus d'informations sur les règles de sécurité par défaut, consultez la section Politiques > Sécurité.

Pour appliquer un contrôle prioritaire sur une règle, sélectionnez **Policies (Politiques)** > **Security (Sécurité)** sur un pare-feu ou **Policies (Politiques)** > **Security (Sécurité)** > **Default Rules (Règles par défaut)** sur Panorama. La colonne Nom affiche une icône représentant les éléments hérités ( ) pour les règles sur lesquelles vous pouvez appliquer un contrôle prioritaire. Sélectionnez la règle, cliquez sur **Override (Contrôle prioritaire)** et modifiez les paramètres dans le tableau suivant.

Pour rétablir les paramètres prédéfinis d'une règle ayant été forcée ou les paramètres transmis par un groupe de périphériques Panorama, sélectionnez **Policies (Politiques)** > **Security (Sécurité)** sur un pare-feu ou **Policies (Politiques)** > **Security (Sécurité)** > **Default Rules (Règles par défaut)** sur Panorama. La colonne Nom affiche une icône représentant le contrôle prioritaire ( ) pour les règles contenant des valeurs qui ont été forcées. Sélectionnez la règle, cliquez sur **Revert (Rétablir)** et cliquez sur **Yes (Oui)** pour confirmer l'opération.

Champs pour appliquer un contrôle prioritaire d'une règle de sécurité par défaut	Description
Onglet Général	
Nom	Le **Name (Nom)** indique que la règle est en lecture seule ; un contrôle prioritaire ne peut pas être appliqué.

Champs pour appliquer un contrôle prioritaire d'une règle de sécurité par défaut	Description
Rule Type (Type de règle)	Le **Rule Type (Type de règle)** est en lecture seule ; un contrôle prioritaire ne peut pas être appliqué.
Description	La **Description** est en lecture seule ; un contrôle prioritaire ne peut pas être appliqué.
Étiquette	Sélectionnez **Tags (Étiquettes)** dans la liste déroulante. Une étiquette de politique est un mot-clé ou une expression qui vous permet de trier ou de filtrer les politiques. Cela est utile lorsque vous avez défini de nombreuses politiques et que vous souhaitez afficher celles qui sont identifiées par un mot-clé particulier. Par exemple, vous pouvez ajouter l'étiquette Trafic entrant vers la zone DMZ à certaines politiques de sécurité, ajouter une étiquette avec les mots Déchiffrement et Aucun déchiffrement aux politiques de déchiffrement spécifiques ou utiliser le nom d'un centre de données spécifique pour les politiques associées à cet emplacement.
Onglet Actions	
Paramètres d'action	Sélectionnez l'**Action** appropriée pour le trafic correspondant à la règle. • **Allow (Autoriser)** - (par défaut) Autorise le trafic. • **Deny (Refuser)** - Bloque le trafic et applique l'action Refuser définie par défaut pour l'application refusée par le pare-feu. Pour afficher l'action Refuser définie par défaut pour une application, consultez les détails de l'application dans **Objects (Objets)** > **Applications**. • **Drop (Abandonner)** - Abandonne l'application sans aucune notification. Le pare-feu n'envoie aucun message de réinitialisation TCP à l'hôte ou à l'application. • **Reset client (Réinitialiser le client)** - Envoie un message de réinitialisation TCP au périphérique côté client. • **Reset server (Réinitialiser le serveur)** - Envoie un message de réinitialisation TCP au périphérique côté serveur. • **Reset both (Réinitialiser les deux)** - Envoie un message de réinitialisation TCP aux périphériques côté client et côté serveur.
Paramètres du profil	**Profile Type (Type de profil)** - Affectez des profils ou groupes de profils à la règle de sécurité : • Pour définir la vérification que les profils de sécurité effectuent par défaut, sélectionnez **Profiles (Profils)**, puis sélectionnez un ou plusieurs profils individuels **Antivirus**, **Vulnerability**

Champs pour appliquer un contrôle prioritaire d’une règle de sécurité par défaut	Description
	Protection (Protection contre les vulnérabilités), **Anti-Spyware (Antispyware)**, **URL Filtering (Filtrage des URL)**, **File Blocking (Blocage de fichiers)**, **Data Filtering (Filtrage des données)** et/ou **WildFire Analysis (Analyse WildFire)**, **SCTP Protection (Protection SCTP)**, et **Mobile Network Protection (Protection de réseau mobile)**. • Pour assigner un groupe de profils plutôt que des profils individuels, sélectionnez **Group (Groupe)**, puis sélectionnez **Group Profile (Profil de groupe)** dans la liste déroulante. • Pour définir de nouveaux profils(Objects > Security Profiles (Objets > Profils de sécurité)) ou groupes de profils, cliquez sur **New (Nouveau)** dans la liste déroulante pour le profil ou le profil de groupe correspondant.
Paramètre des journaux	Indiquez n'importe quelle combinaison des options suivantes'A0;: • **Log Forwarding (Transfert des journaux)** - Pour transférer des entrées du journal du trafic local et du journal des menaces vers des destinations distantes, comme des serveurs Panorama et Syslog, sélectionnez un profil **Log Forwarding (Transfert des journaux)** dans la liste déroulante. Les profils de sécurité déterminent la génération d'entrées dans le journal des menaces. Pour définir un nouveau profil de **Log Forwarding (Transfert des journaux)**, sélectionnez **Profile (Profil)** dans la liste déroulante (reportez-vous à la section Objets > Transfert de journaux). • Pour générer des entrées dans le journal du trafic local en cas de trafic correspondant à cette règle, sélectionnez les options suivantes'A0;: • **Log at Session Start (Se connecter au début de la session)** - Génère une entrée dans le journal du trafic pour le début d’une session (sélectionné par défaut). • **Log at Session End (Se connecter en fin de session)** - Génère une entrée dans le journal du trafic pour la fin d’une session (désactivé par défaut). *Si vous configurez le pare-feu afin qu’il inclue des entrées au début et à la fin de la session dans le journal du Trafic, il va également inclure des entrées d’abandon et de refus.*

Applications et utilisation

- **Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer (Optimiseur de politique)** > **New App (Nouvelle appli)** > **Viewer (Visionneuse),** puis cliquez sur le nombre dans **Apps seen (applications vues)** ou cliquez sur **Compare (Comparer)**.

  Vous devez disposer d'un abonnement SaaS Inline Security pour voir la nouvelle visionneuse d'applications dans l'interface. La nouvelle visionneuse d'applications inclut des applications fournies dans le cloud en plus des applications fournies par du contenu et si vous n'avez pas d'abonnement SaaS Inline Security, vous ne recevez pas d'applications fournies dans le cloud.

- **Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer (Optimiseur de politiques)** > **Rules Without App Controls (Règles sans contrôle des appli)** puis cliquez sur le nombre dans **Apps Seen (applications vues)** ou cliquez sur **Compare (Comparez)**.
- **Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer (Optimiseur de politiques)** > **Unused Apps (Applications non utilisées)** puis cliquez sur le nombre dans **Apps Seen (applications vues)** ou cliquez sur **Compare (Comparer)**.
- **Policies (Politiques)** > **Security (Sécurité)** puis cliquez sur le nombre dans **Apps Seen (applications vues)**

Avec l'onglet Usage (Utilisation) de la règle de politique de sécurité, vous pouvez aussi **Comparer les applications et les applications vues** pour accéder aux outils qui vous aident à passer de règles de politique de sécurité basées sur les ports à des règles de politique de sécurité basées sur les applications et à éliminer les applications non utilisées des règles sous **Applications et utilisation**.

Champ	Description
Délai	La période de temps pour les informations d'application : • **Tout le temps** : affiche les applications vues au cours de la durée de vie de la règle. • **7 derniers jours** : affiche uniquement les applications vues au cours des 7 derniers jours. • **15 derniers jours** : affiche uniquement les applications vues au cours des 15 derniers jours. • **30 derniers jours** : affiche uniquement les applications vues au cours des 30 derniers jours.
Applications d'une règle	Les applications configurées dans la règle ou **n'importe laquelle** si aucune application spécifique n'est configurée dans la règle. Vous pouvez **Parcourir**, **Ajouter** et **Supprimer** les applications, au besoin, et les applications sont configurées dans une règle. Le chiffre entouré d'un cercle qui figure à côté d'une application d'une règle indique le nombre d'applications. L'ajout d'applications à partir de cet emplacement revient à ajouter des applications dans la règle de politique de sécurité à l'onglet **Application**.

Champ	Description
Applications vues	Toutes les applications vues et autorisées sur le pare-feu qui correspondent à la règle. Le chiffre qui figure à côté de Applications vues indique le nombre d'applications vues dans la règle. • **Applications** : les applications vues dans la règle. Par exemple, si une règle autorise le trafic de navigation Web (comme indiqué dans Applications sur règle), vous pouvez voir de nombreuses applications dans la liste Applications vues car de nombreuses applications sont identifiées comme naviguant sur le Web. • **Sous-catégorie** : la sous-catégorie de l'application. • **Risque** : la cote de risque de l'application. • **Première apparition** : le premier jour où l'application a été vue sur le réseau. • **Dernière apparition** : la dernière journée à laquelle l'application a été vue sur le réseau. *La granularité de la mesure des options Première apparition et Dernière apparition est d'une journée. Ainsi, au cours de la journée où vous définissez une règle, les journées indiquées dans Première apparition et Dernière apparition sont identiques.* • **Trafic (30 jours)** : la quantité de trafic, en octets, vue au cours des 30 derniers jours. *Si la période de temps était plus longue, les plus vieilles règles demeureraient au haut de la liste, car ce sont elles qui risquent d'avoir le plus important trafic cumulé. Les règles les plus récentes pourraient se retrouver sous les plus anciennes règles, même si du trafic important passe par les nouvelles règles.*
Actions des applications vues	Actions que vous pouvez exécuter à l'option **Applications vues** : • **Créer une règle clonée** : clone la règle actuelle. Lors de la migration de règles basées sur les ports à et des règles basées sur les applications, clonez d'abord la règle basée sur les ports, puis modifiez la règle clonée pour créer la règle autorisant le trafic basée sur les applications. La règle clonée est insérée au-dessus de la règle basée sur les ports dans la liste de politiques. Utilisez cette méthode de migration afin de veiller à ne pas refuser par inadvertance le trafic que vous souhaitez autoriser ; si la règle clonée n'autorise pas toutes

Champ	Description
	les applications dont vous avez besoin, la règle basée sur les ports qui suit les autorise. Surveillez la règle basée sur les ports et ajustez la règle basée sur les applications (clonée), au besoin. Lorsque vous avez la certitude que la règle basée sur les applications autorise le trafic que vous souhaitez et que seul le trafic non désire passe à la règle basée sur les ports, vous pouvez supprimer cette dernière en toute sécurité. Le clonage offre des avantages similaires pour les applications vues dans la **New App Viewer (nouvelle visionneuse)** d'applications et vous permet de déplacer des applications cloud nouvellement identifiées ainsi que des applications fournies par le contenu vers des règles de stratégie de sécurité qui vous permettent de contrôler l'application et l'accès. Vous pouvez sélectionner l'ajout d'applications à une règle clonée individuellement, dans un groupe d'applications ou dans un filtre d'application. • **Add to this Rule (Ajouter à cette règle)** (non disponible pour la nouvelle visionneuse d'applications) : ajoute des applications depuis les Applications vues à la règle. L'ajout d'applications à la règle transforme une règle configurée pour qu'elle corresponde à **N'importe laquelle** application (une règle basée sur les ports) en une règle basée sur les applications qui autorise les applications que vous indiquez (la nouvelle règle basée sur les applications remplace la règle basée sur les ports). La règle interdit les applications que vous n'ajoutez pas, comme c'est le cas pour toutes les règles basées sur les applications. Veillez à identifier toutes les applications que vous souhaitez autoriser et ajoutez-les à la règle, afin d'éviter de refuser accidentellement une application. • **Ajouter à une règle existante** : ajoute des applications vues à une règle existante basée sur les applications (App-ID). Par exemple, ceci vous permet de cloner une règle basée sur App-ID à partir d'une règle basée sur un port, puis d'ajouter d'autres applications vues dans les règles sur les ports à l'application basée sur App-ID par la suite. Pour les applications vues dans la nouvelle visionneuse d'applications, vous pouvez organiser les applications basées sur le cloud et le contenu nouvellement identifiées en règles de politique de sécurité sensibles à mesure que de nouvelles applications sont découvertes. Vous pouvez sélectionner l'ajout d'applications à une règle existante individuellement, dans un groupe d'applications ou dans un filtre d'application. • **Match Usage (Correspondance d'utilisation)** (non disponible pour la nouvelle visionneuse d'applications) :

Champ	Description
	déplace toutes les applications vues dans la règle (elles sont répertoriées sous Applications sur la règle après avoir activé **Match Usage (correspondance d'utilisation**). Si vous êtes certain que la règle devrait autoriser *toutes* les applications indiquées, la **Correspondance de l'utilisation** est très pratique. Vous devez toutefois être certain que toutes les applications indiquées sont des applications que vous souhaitez autoriser sur votre réseau. Si de nombreuses applications ont été vues dans la règle (par exemple, dans une règle qui autorise la navigation Web), il vaut mieux cloner la règle et passer à une règle basée sur les applications. La **correspondance de l'utilisation** fonctionne bien pour des règles simples disposant d'applications bien connues. Par exemple, si une règle basée sur les ports associée au port 22 n'a vu que du trafic SSH (et que c'est le seul trafic qu'elle devrait voir), il est sécuritaire de **Match Usage (Mettre l'utilisation en correspondance)**. Les boîtes de dialogue **Dupliquer**, **Ajouter à la règle** et **Ajouter des applications à une règle existante** permettent de garantir que les applications ne s'interrompent pas et vous permettent de protéger la règle à l'épreuve du temps en incluant des applications individuelles pertinentes qui sont associées aux applications que vous clonez ou ajoutez à une règle.
Créer un règle clonée > Applications Ajouter à cette règle Ajouter à la règle existante > Applications	Sélectionnez des applications, puis clonez ou ajoutez des applications individuelles à une règle : • **Nom** (Boîtes de dialogue Dupliquer et Ajouter des applications seulement à une règle existante). • Dupliquer : Saisir le nom de la nouvelle règle duppliquée. • Ajouter des applications à une règle existante : Sélectionnez la règle à laquelle ajouter des applications ou entrez le nom de la règle. • **Applications** : • Ajouter une application conteneur (par défaut) : Sélectionne toutes les applications du conteneur, les applications vues sur la règle et les applications de conteneur qui n'ont pas été vues sur la règle. Les futures applications vues pour le conteneur correspondront à la règle, la pérennisant ainsi à mesure que l'application change. • Ajouter des applications spécifiques vues: Sélectionne uniquement les applications qui ont été réellement vues sur la règle. (Vous pouvez également sélectionner manuellement des applications de conteneur et des applications fonctionnelles.)

Champ	Description
	• **Application**: • Les applications sélectionnées qui ont été vues dans la règle, surlignées en vert. • Applications de containeur surlignées en gris, et les applications fonctionnelles sont indiquées ci-dessous. • Applications fonctionnelles incorporées qui ont été vues dans la règle, mais qui n'ont pas été sélectionnées dans **Applications & Usage (Application et utilisation)** (texte normal). • Applications fonctionnelles incorporées qui n'ont pas été vues dans la règle (*italicized (italiques)*). • La date à laquelle les applications ont été **Vues en dernier** dans la règle. • **Applications dépendantes** : • Applications requises pour l'exécution des applications sélectionnées. • **Depends on (Dépend de)**: les applications dépendantes dont les applications sélectionnées ont besoin pour s'exécuter. • **Required by (Requis par)** :application qui requiert l'application dépendante. (Parfois, une application dépendante a des applications dépendantes.)
Créer une règle clonée > Groupe d'applications Ajouter à la règle existante > Groupe d'applications	Sélectionnez des applications, puis clonez ou ajoutez des applications à une règle dans un groupe d'applications dans la boîte de dialogue **Create Cloned Rule (Créer une règle clonée)** ou **Add Apps to Existing Rule (Ajouter des applications à une règle existante)** : • **Cloned Rule Name (Nom de la règle clonée)** ou **Name (Nom)**: • Nom de la règle clonée : Saisir le nom de la nouvelle règle duppliquée. • Nom : Sélectionnez la règle à laquelle ajouter le groupe d'applications ou entrez le nom de la règle. • **Policy Action (Action de politique)** (règle clonée uniquement) : indiquez si vous souhaitez autoriser ou refuser le trafic dans la règle clonée. • **Add to Application Group (Ajouter au Groupe d'applications)**: sélectionnez un groupe existant ou tapez un nouveau nom pour créer un nouveau groupe d'applications.

Champ	Description
	• **Applications** : • Ajouter une application conteneur (par défaut) : Sélectionne toutes les applications du conteneur, les applications vues sur la règle et les applications de conteneur qui n'ont pas été vues sur la règle. Les futures applications vues pour le conteneur correspondront à la règle, la pérennisant ainsi à mesure que l'application change. • Ajouter des applications spécifiques vues: Sélectionne uniquement les applications qui ont été réellement vues sur la règle. (Vous pouvez également sélectionner manuellement des applications de conteneur et des applications fonctionnelles.) • **Application**: • Les applications sélectionnées qui ont été vues dans la règle, surlignées en vert. • Applications de containeur surlignées en gris, et les applications fonctionnelles sont indiquées ci-dessous. • Applications fonctionnelles incorporées qui ont été vues dans la règle, mais qui n'ont pas été sélectionnées dans **Applications & Usage (Application et utilisation)** (texte normal). • Applications fonctionnelles incorporées qui n'ont pas été vues dans la règle (*italicized (italiques)*). • La date à laquelle les applications ont été **Vues en dernier** dans la règle. • **Applications dépendantes** : • Applications requises pour l'exécution des applications sélectionnées. • **Depends on (Dépend de)**: les applications dépendantes dont les applications sélectionnées ont besoin pour s'exécuter. • **Required by (Requis par)** :application qui requiert l'application dépendante. (Parfois, une application dépendante a des applications dépendantes.)
Créer une règle clonée > Filtre d'applications Ajouter à une règle existante > Filtre d'applications	Sélectionnez des applications, puis clonez ou ajoutez des applications à une règle dans un filtre d'application dans la boîte de dialogue **Create Cloned Rule (Créer une règle clonée)** ou **Add Apps to Existing Rule (Ajouter des applications à une règle existante)** :

Champ	Description
	• **Cloned Rule Name (Nom de la règle clonée)** ou **Existing Rule Name (Nom de la règle existante)**: • Nom de la règle clonée : Saisir le nom de la nouvelle règle duppliquée. • Nom de la règle existante : Sélectionnez la règle à laquelle ajouter le filtre d'applications ou entrez le nom de la règle. • **Policy Action (Action de politique)** (règle clonée uniquement) : indiquez si vous souhaitez autoriser ou refuser le trafic dans la règle clonée. • **Application Filter Name (Nom du filtre d'applications)** : sélectionnez un filtre existant ou tapez un nouveau nom pour créer un nouveau filtre d'application. Le filtre d'application fonctionne de la même manière que les **Objects (Objets)** > **Application Filters (Filtres d'applications)** (voir Create an Application Filter (Créer un filtre d'applications)). Vous pouvez filtrer les applications basées sur le cloud (avec un abonnement SaaS Inline Security) et basées sur le contenu et les ajouter à des filtres existants ou nouveaux.

Optimiseur de la politique de sécurité

- Politiques > Sécurité > Optimiseur de politique

Policies (Politiques) > **Security (Sécurité)** > **Policy Optimizer (Optimiseur de politique)** affiche :

- **New App Viewer (Nouvelle visionneuse)**d'applications : nouvelles applications cloud téléchargées à partir du moteur de contrôle des applications si le pare-feu dispose d'un abonnement SaaS Security.
- **Rules Without App Controls (Règles sans contrôle des applications)** : règles dont l'application est définie sur **any (Indifférent)**, pour que vous puissiez identifier les règles basées sur le port pour convertir les règles basées sur l'application.
- **Applications non utilisées** : règles qui incluent les applications qui n'ont jamais été mises en correspondance avec la règle.
- **Transfert de journaux pour les services de sécurité**: attachez un profil de transfert de journaux à plusieurs règles en bloc et envoyez des journaux à des services tels que IoT Security pour l'analyse et Cortex Data Lake pour le stockage.

  Avant d'utiliser cette fonctionnalité, vous devez d'abord configurer vos règles de stratégie de sécurité *pour capturer et* transférer les journaux *et activer les* services de journalisation *avec une journalisation améliorée des applications.*

- **Rule Usage (Utilisation de la règle)** : les informations d'utilisation de la règle au cours de différentes périodes, y compris les règles non utilisées au cours de différentes périodes.

Champ	Description
Name (Nom)	Le nom de la règle de politique de sécurité.
Service (Service)	Tous les services associés avec la règle de politique de sécurité.
Traffic (octets, 30 jours)	**Traffic (30 days) (Trafic [30 jours])** : la quantité de trafic, en octets, vue au cours des 30 derniers jours. *Si la période de temps était plus longue, les plus vieilles règles demeureraient au haut de la liste, car ce sont elles qui risquent d'avoir le plus important trafic cumulé. Les règles les plus récentes pourraient se retrouver sous les plus anciennes règles, même si du trafic important passe par les nouvelles règles.*
Applications autorisées	Les applications que la règle autorise. Ouvrez la boîte de dialogue **Application** à partir de laquelle vous pouvez ajouter et supprimer des applications sur la règle.
Application	(**New App Viewer only (Nouvelle visionneuse d'applications uniquement)**) Les applications que la règle autorise.
Applications vues	Le nombre d'applications vues dans la règle. Cliquez sur le nombre pour ouvrir la boîte de dialogue **Applications & Usage (Applications et utilisation)**, qui vous permet de comparer les applications configurées sur la règle aux applications vues dans la règle et de modifier les applications.
Journée sans nouvelles applications	Le nombre de jours depuis la dernière fois que des nouvelles applications ont été vues dans la règle.
Comparer	Ouvrez la boîte de dialogue **Applications & Usage (Applications et utilisation)** pour comparer les applications configurées sur la règle aux applications vues dans la règle et modifier la règle.
Dernière correspondance (Utilisation d'une règle)	La dernière correspondance du trafic à la règle.
Première correspondance (Utilisation d'une règle)	La première correspondance du trafic à la règle.
Nombre de correspondances (Utilisation d'une règle)	Le nombre de fois où le trafic a correspondu à la règle.
Modifié	La date et l'heure de modification de la règle.

Champ	Description
Créé	La date et l'heure de création de la règle.
Délai	La durée (nombre de jours) pendant laquelle les données sont affichées.
Usage	Affiche : • **Any (indifférent)** (toutes) les règles sur le pare-feu dans le délai indiqué, quel que soit le trafic qui a correspondu aux règles (règles utilisées) ou non (règles non utilisées). • Règles **Unused (non utilisées)** auxquelles le trafic n'a pas correspondu dans le délai indiqué. • Règles **Used (utilisées)** auxquelles le trafic a correspondu dans le délai indiqué.
Exclure la réinitialisation des règles au cours des *xx* derniers jours	N'affiche pas les règles pour lesquelles vous **Reset Rule Hit Counter (Réinitialiser le Compteur d'accès de la règle)** pendant le nombre de jours indiqué (de 1 à 5 000 jours). Par exemple, cela vous permet d'examiner des règles plus anciennes qui n'ont pas correspondu au trafic pendant un délai tout en excluant les règles plus récentes qui n'ont peut-être pas eu le temps de correspondre au trafic.
Date de réinitialisation	La dernière date à laquelle le compteur de correspondance de la règle a été réinitialisé.
Profil de transfert de journal (transfert de journal pour les services de sécurité uniquement)	Affiche : • **Tous** – Règles sur le pare-feu, qu'un profil de transfert de journal leur soit attaché ou non. • **Aucun** – Règles qui n'ont pas de profil de transfert de journal attaché à eux. • **<profile-name>** – Règles auxquelles est attaché un profil de transfert de journal spécifique.
Joindre le profil de transfert de journal (transfert de journal pour les services de sécurité uniquement)	Après avoir sélectionné Règles de stratégie de sécurité, utilisez cette option en bas de l'écran pour ouvrir une boîte de dialogue et sélectionnez un profil de transfert de journal à attacher aux règles sélectionnées : • **Profil de transfert de journal (Log Forwarding Profile)** : choisissez un profil de transfert de journal à attacher aux règles sélectionnées. • **Activer la journalisation IoT améliorée** : Sélectionnez si le profil de transfert de journal choisi ne transfère pas déjà

Champ	Description
	les journaux d’application améliorés (ECL). Cela permet le transfert EAL sur le profil de transfert de journal choisi.

Politiques > NAT

Si vous définissez des interfaces de Niveau 3 sur le pare-feu, vous pouvez configurer une politique de traduction des adresses réseau (NAT pour « Network Address Translation ») pour préciser si les adresses IP et les ports source ou de destination doivent être convertis en adresses et ports publics ou privés. Par exemple, des adresses source privées peuvent être traduites en adresses publiques sur le trafic envoyé depuis une zone interne (de confiance) vers une zone publique (non approuvée). La traduction des adresses réseau est également prise en charge sur les interfaces de câble virtuel.

Les règles de traduction des adresses réseau (NAT) sont basées sur les zones source et de destination, les adresses source et de destination et le service de l'application (HTTP par exemple). Comme les politiques de sécurité, les règles des politiques NAT sont comparées au trafic entrant dans un ordre précis et la première règle qui correspond au trafic est appliquée.

En fonction de vos besoins, ajoutez des itinéraires statiques vers le routeur local afin que le trafic vers l'ensemble des adresses publiques soit acheminé au pare-feu. Il peut également être nécessaire d'ajouter des itinéraires statiques vers l'interface de réception sur le pare-feu pour réacheminer le trafic vers l'adresse privée.

Les tableaux suivants décrivent les paramètres NAT et NPTv6 (traduction de préfixe réseau entre IPv6 et IPv6) :

- Onglet Général des politiques NAT
- Onglet Paquet d'origine NAT
- Onglet Paquet translaté NAT
- Onglet Liaison HA Active / Active
- (Panorama uniquement) Onglet Cible NAT

Vous souhaitez en savoir plus ?

Voir NAT

Onglet Général des politiques NAT

- Politiques > NAT > Général

Sélectionnez l'onglet **General (Général)** pour définir un nom et une description pour la politique NAT ou NPTv6. Vous pouvez configurer une étiquette afin que vous puissiez trier ou filtrer les politiques lorsqu'il en existe un grand nombre. Sélectionnez le type de politique NAT que vous voulez créer et qui va affecter les champs disponibles sur les onglets **Original Packet (Paquet d'origine)** et **Translated Packet (Paquet translaté)**.

Règle NAT - Paramètres généraux	Description
Name (Nom)	Donnez un nom à la règle afin de l'identifier. Le nom est sensible à la casse et peut comporter jusqu'à 63 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement. Le nom doit être unique

Règle NAT - Paramètres généraux	Description
	sur un pare-feu et, dans Panorama, unique au sein de son groupe de périphériques et des groupes de périphériques anciens ou descendants.
Description	Saisissez une description de la règle (1024 caractères maximum).
Étiquette	Si vous avez voulez étiqueter la politique, cliquez sur **Ajouter** et indiquer l'étiquette. Une étiquette de politique est un mot-clé ou une expression qui vous permet de trier ou de filtrer les politiques. Cela est utile lorsque vous avez défini de nombreuses politiques et que vous souhaitez afficher celles qui sont identifiées par un mot-clé particulier.
Regrouper des règles par étiquette	Saisissez une étiquette selon laquelle regrouper des règles de politique similaires. L'étiquette de groupe vous permet d'afficher votre base de règles de politique en fonction de ces étiquettes. Vous pouvez regrouper les règles en fonction d'une **Tag (Étiquette)**.
Type NAT	Indiquez le type de traduction : • **ipv4** - traduction effectuée entre des adresses IPv4. • **nat64** - traduction effectuée entre des adresses IPv6 et IPv4. • **nptv6** - traduction effectuée entre des préfixes IPv6. Vous ne pouvez pas combiner des plages d'adresses IPv4 et IPv6 dans une même règle NAT.
Commentaire d'audit	Saisissez un commentaire pour auditer la création ou la modification d'une règle de politique. Le commentaire d'audit est sensible à la casse et peut comporter jusqu'à 256 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement.
Archive des commentaires d'audit	Afficher les **Audit Comments (Commentaires d'audit)** précédents pour la règle de politique. Vous pouvez exporter l'archive des commentaires d'audit au format CSV.

Onglet Paquet d'origine NAT

- Politiques > NAT > Paquet d'origine

Sélectionnez l'onglet **Original Packet (Paquet d'origine)** pour définir les zones de paquets source et de destination qui seront translatées par le pare-feu, ainsi que l'interface de destination et le type de service. Vous pouvez configurer plusieurs zones source et de destination de même type et vous pouvez appliquer la règle à des réseaux donnés ou à des adresses IP données.

Règle NAT - Paramètres du paquet d'origine	Description
Zone source / zone de destination	Sélectionnez une ou plusieurs zones source et de destination pour le paquet (non NAT) d'origine (valeur par défaut : **Any (indifférent)**). Les zones doivent être du même type (couche 2, couche 3 ou câble virtuel). Pour définir de nouvelles zones, voir Réseau > Zones. Pour faciliter la gestion, vous pouvez préciser de multiples zones. Par exemple, vous pouvez configurer les paramètres afin que plusieurs adresses NAT internes renvoient vers la même adresse IP externe.
Interface de destination	Indiquez l'interface de destination des paquets que traduit le pare-feu. Vous pouvez utiliser l'interface de destination pour traduire des adresses IP différemment dans le cas où le réseau est connecté à deux fournisseurs d'accès avec des pools d'adresses IP différents.
Service (Service)	Précisez le service pour lequel le pare-feu traduit l'adresse source ou de destination. Pour définir un nouveau groupe de services, sélectionnez Objets > Groupes de service.
Adresse source / adresse de destination	Indiquez une combinaison d'adresses source et de destination que doit traduire le pare-feu. Pour NPTv6, les préfixes configurés pour l'**Adresse source** et l'**Adresse de destination** doivent être au format xxxx:xxxx::/yy. L'adresse ne peut pas contenir une partie de l'identifiant d'interface (hôte) défini. La plage des longueurs de préfixe prises en charge est comprise entre /32 et /64.

Onglet Paquet translaté NAT

- Politique > NAT > Paquet translaté

Aux fins de la traduction de l'adresse source, sélectionnez l'onglet **Translated Packet (Paquet translaté)** pour déterminer le type de traduction à effectuer sur la source et l'adresse et, éventuellement, sur le port auxquels la source est traduite.

Vous pouvez également activer la Translation d'une adresse de destination pour un hôte interne afin de le rendre accessible à une adresse IP publique. Dans ce cas, définissez une adresse source publique et une adresse de destination pour un hôte interne dans l'onglet **Original Packet (Paquet d'origine)**, puis à l'onglet **Translated Packet (Paquet translaté)**, vous configurez la **Static IP (Adresse IP statique)** ou **Dynamic IP (with session distribution) (Adresse IP dynamique (avec distribution de sessions)** et saisissez la **Translated Address (Adresse traduite)**. Ensuite, lorsque l'hôte interne accède à l'adresse publique, celle-ci est translatée vers l'adresse (de destination) interne de l'hôte interne.

Règle NAT - Paramètres du paquet translaté	Description
Traduction de l'adresse source	Sélectionnez le **Translation Type (type de translation)** (pool d'adresses dynamiques ou statiques) et saisissez une adresse IP ou une plage d'adresses (adresse1-adresse2) vers laquelle l'adresse source sera translatée (**Translated Address (Adresse translatée)**). La taille de la plage d'adresses est limitée par le type de pool d'adresses : • **Dynamic IP And Port (IP et port dynamiques)** - La sélection de l'adresse est basée sur un hachage de l'adresse IP source. Pour une adresse IP source donnée, le pare-feu utilise la même adresse source translatée pour toutes les sessions. Le NAT source d'adresses IP et de ports dynamiques prend en charge environ 64 000 sessions simultanées sur chaque adresse IP du pool NAT. Certains modèles prennent en charge la sursouscription, ce qui permet à une seule adresse IP d'héberger plus de 64 000 sessions simultanées. La translation des adresses IP / ports dynamiques de Palo Alto Networks® prend en charge plus de sessions NAT que d'adresses IP et ports disponibles. Grâce à la sursouscription, le pare-feu peut utiliser les combinaisons d'adresses IP et de ports jusqu'à deux fois en simultané sur les pare-feux PA-220, PA-820, PA-850, VM-50, VM300 et VM-1000-HV, jusqu'à quatre fois en simultané sur les pare-feux PA-5220 et de la série PA-3200, et jusqu'à huit fois en simultané sur les pare-feux PA-5250, PA-5260, PA-5280, PA-7050, PA-7080, VM-500 et VM-700 lorsque les adresses IP de destination sont uniques. • **Dynamic IP (IP dynamique)** - Translate à la prochaine adresse disponible dans la plage définie, mais le numéro de port ne change pas. Jusqu'à 32 000 adresses IP consécutives sont prises en charge. Un pool d'adresses IP dynamiques peut contenir plusieurs sous-réseaux, donc vous pouvez traduire vos adresses réseau internes vers deux ou plusieurs sous-réseaux publics distincts. • **Advanced (Dynamic IP/Port Fallback) (Avancé (IP dynamique / port dynamique de secours))** - Utilisez cette option pour créer un pool de secours qui assure la translation des adresses IP et des ports si le pool principal est à court d'adresses. Vous pouvez définir des adresses pour le pool en utilisant l'option **Translated Address (Adresse traduite)** ou l'option **Interface Address (Adresse de l'interface)** ; la dernière option est réservée aux interfaces qui reçoivent une adresse IP de manière dynamique. Lors de la création d'un pool de secours, vérifiez que les adresses ne coïncident pas avec celles du pool principal.
Traduction de l'adresse source (suite)	• **Static IP (IP statique)** - La même adresse est toujours utilisée pour la translation et le port ne change pas. Par exemple, si la plage source est 192.168.0.1 - 192.168.0.10 et que la plage de translation est 10.0.0.1 - 10.0.0.10, l'adresse 192.168.0.2 est toujours translatée en 10.0.0.2. La taille de la plage d'adresses est quasi-illimitée. Vous devez utiliser une translation **Static IP (IP statique)** pour la translation de l'adresse source. Pour NPTv6, les préfixes configurés pour **Translated Address (Adresse translatée)** doivent être au format xxxx:xxxx::/yy et l'adresse ne peut

Règle NAT - Paramètres du paquet translaté	Description
	pas contenir une partie de l'identifiant d'interface (hôte) définie. La plage des longueurs de préfixe prises en charge est comprise entre /32 et /64. • **None (Aucune)** - Aucune translation n'est effectuée.
Bidirectionnel	(Facultatif) Activez la translation bidirectionnelle pour la translation d'une adresse **Static IP (IP statique)** source pour que le pare-feu puisse créer une translation correspondante (NAT ou NPTv6) dans le sens opposé de la translation que vous configurez. *Si vous activez la traduction bidirectionnelle, vous devez vous assurer d'avoir mis en place des politiques de sécurité pour contrôler le trafic dans les deux sens. En l'absence de telles politiques, la fonctionnalité de traduction bidirectionnelle autorise la traduction automatique des paquets dans les deux directions.*
Traduction de l'adresse de destination	Configure les options suivantes pour que le pare-feu exécute la règle NAT de destination. Généralement, vous utilisez le NAT de destination pour autoriser l'accès à un serveur interne, tel qu'un serveur de messagerie, depuis le réseau public.
Type de translation et adresse translatée	Sélectionnez le type de translation effectuée par le pare-feu sur l'adresse de destination : • **None (Aucune)** (par défaut) • **Static IP (IP statique)** : saisissez une **Translated Address (Adresse translatée)** comme adresse IP ou plage d'adresses IP et un numéro de **Translated Port (Port translaté)** (de 1 à 65535) pour la translation de l'adresse de destination et du numéro de port initiaux. Si le champ **Translated Port (Port translaté)** n'est pas renseigné, le port de destination n'est pas modifié. Pour NPTv6, les préfixes configurés pour le préfixe de Destination et la **Translated Address (Adresse translatée)** doivent être au format xxxx:xxxx::/yy. L'adresse ne peut pas contenir une partie de l'identifiant d'interface (hôte) défini. La plage des longueurs de préfixe prises en charge est comprise entre /32 et /64. *Le port translaté n'est pas pris en charge pour NPTv6 car NPTv6 sert strictement à la translation de préfixe. La section de l'adresse du port et de l'hôte est simplement transférée telle quelle.* *La translation d'adresses IP statiques pour IPv4 vous permet aussi de **Enable DNS Rewrite (Activer la réécriture DNS)** (tel que décrit ci-dessous)* • **Dynamic IP (with session distribution) (IP dynamique (avec distribution de sessions)** : sélectionnez ou saisissez une **Translated Address (Adresse**

Règle NAT - Paramètres du paquet translaté	Description
	translatée) qui est un FQDN, un objet d'adresse ou un groupe d'adresses à partir duquel le pare-feu sélectionne l'adresse translatée. Si le serveur DNS renvoie plus d'une adresse pour un FQDN ou si l'objet d'adresse ou le groupe d'adresses se translate en plus d'une adresse IP, le pare-feu distribue les sessions parmi ces adresses en utilisant la **Session Distribution Method (Méthode de distribution de sessions)** définie.
Méthode de Distribution de Sessions	Si vous sélectionnez de translater le NAT de destination vers **Dynamic IP (with session distribution) (Adresse IP dynamique (avec distribution de session)**, il est possible que l'adresse de destination translatée (vers un nom de domaine complet (FQDN), un objet d'adresse ou un groupe d'adresses) peut se résoudre en plus d'une adresse. Vous pouvez choisir la manière dont le pare-feu distribue (affecte) les sessions par ces adresses pour équilibrer la distribution des sessions : • **Round Robin (Pondération comparative)** : (par défaut) affecte de nouvelles sessions à des adresses IP en ordre rotatif. Sauf si votre environnement vous force à choisir l'une des autres méthodes de distribution, utilisez cette méthode. • **Source IP Hash (Hachage IP source)** : affecte de nouvelles sessions en fonction du hachage des adresses IP source. Si vous avez du trafic entrant provenant d'une seule adresse IP source, sélectionnez une autre méthode que le **Source IP Hash (Hachage IP source)**. • **IP Modulo (Modulo IP)** : Le pare-feu tient compte de l'adresse IP source et de destination du paquet entrant ; le pare-feu effectue une opération XOR et une opération modulo. Le résultat détermine à quelle adresse IP le pare-feu affecte les nouvelles sessions. • **IP Hash (Hachage IP)** : affecte de nouvelles sessions au moyen d'un hachage d'adresses IP source et de destination. • **Least Sessions (Le moins de sessions)** : affecte de nouvelles sessions à l'adresse IP qui possède le moins de sessions concurrentes. Si vous disposez de nombreuses sessions de courte durée, l'option **Least Sessions (le moins de sessions)** vous fournit une distribution plus équilibrée des sessions.
Activer la réécriture DNS :	Dans PAN-OS 9.0.2 et versions 9.0 ultérieurs, si la règle de politique NAT de destination est de type **ipv4**et que la translation de l'adresse de destination est de type **Static IP (IP statique), l'option Enable DNS Rewrite (Activer la réécriture DNS)** est disponible. Vous pouvez activer la réécriture DNS si vous utiliser un NAT de destination ainsi que les services DNS sur un côté du pare-feu pour résoudre les FQDN d'un client qui se trouve de l'autre côté du pare-feu. Lorsque la réponse DNS traverse le pare-feu, le pare-feu réécrit l'adresse IP dans la réponse DNS par rapport à l'adresse de destination originale ou à l'adresse de destination translatée qui correspond à la réponse DNS dans la règle de politique NAT. Une seule règle de politique NAT permet au pare-feu d'effectuer la NAT sur les paquets qui correspondent à la règle et d'effectuer la NAT sur les IP addresses in DNS responses that match the rule (adresses IP dans les réponses DNS qui correspondent à la règle). Vous devez spécifier la manière dont le pare-feu effectue

Règle NAT - Paramètres du paquet translaté	Description
	la NAT sur une adresse IP dans une réponse DNS relative à la règle NAT : inverse ou directe. • **reverse (inverse)** - (par défaut) Si le paquet est une réponse DNS qui correspond à l'adresse de destination translatée dans la règle, la réponse DNS est translatée en utilisant la translation inverse de la règle utilisée. Par exemple, si la règle translate 1.1.1.10 en 192.168.1.10, le pare-feu réécrit la réponse DNS 192.168.1.10 en 1.1.1.10. • **forward (directe)** - Si le paquet est une réponse DNS qui correspond à l'adresse de destination originale dans la règle, la réponse DNS est translatée en utilisant la même translation que la règle utilise. Par exemple, si la règle translate 1.1.1.10 en 192.168.1.10, le pare-feu réécrit la réponse DNS 1.1.1.10 en 192.168.1.10.

Onglet Liaison HA Actif / Actif

- Politiques > NAT > Liaison HA Actif/Actif

L'onglet Liaison HA Actif / Actif n'est disponible que si le pare-feu est dans une configuration haute disponibilité (HD) active / active. Dans cette configuration, vous devez lier chaque règle NAT source (qu'elle soit statique ou dynamique) à l'ID de périphérique 0 ou à l'ID de périphérique 1 ; vous devez lier chaque règle NAT de destination à l'ID de périphérique **0**, à l'ID de périphérique **1**, **aux deux** (ID de périphérique 0 et ID de périphérique 1) ou au pare-feu actif-**principal**.

Sélectionnez les paramètres d'une **Liaison HA Actif/Actif** pour lier une règle NAT à un pare-feu HA comme suit :

- **0** - Lie la règle NAT au pare-feu qui possède l'ID du périphérique HA 0.
- **1** - Lie la règle NAT au pare-feu qui possède l'ID du périphérique HA 1.
- **both (aux deux)** - Lie la règle NAT aux deux pare-feu qui ont l'ID du périphérique HA 0 et l'ID du périphérique HA 0. Ce paramètre ne prend pas en charge la traduction d'adresses IP dynamiques ni la traduction d'adresses IP dynamiques et de ports NAT.
- **primary (principal)** - Lie la règle NAT au pare-feu à l'état HA actif/principal. Ce paramètre ne prend pas en charge la traduction d'adresses IP dynamiques ni la traduction d'adresses IP dynamiques et de ports NAT.

Généralement, les règles NAT spécifiques au périphérique sont configurées lorsque les deux homologues HA possèdent des pools d'adresses IP NAT uniques.

Lorsque le pare-feu crée une nouvelle session, la liaison HA détermine les règles NAT qui peuvent être mises en correspondance avec la session. La liaison doit comprendre le propriétaire de la session pour la mise en correspondance de la règle. Le pare-feu configuré pour la session effectue la mise en correspondance de la règle NAT, mais la session est comparée aux règles NAT qui sont liées au propriétaire de la session et traduite selon l'une des règles. En cas de règles spécifiques au périphérique, le pare-feu ignore toutes les règles NAT qui ne sont pas associées au propriétaire de la session. Par exemple, supposons que le pare-feu ayant le périphérique 1 est le propriétaire de la session et le pare-feu configuré

pour la session. Lorsque le périphérique 1 tente de mettre en correspondance une session et une règle NAT, il ignore toutes les règles liées au périphérique ID 0.

En cas d'échec de l'un des homologues, le second homologue continue de traiter le trafic des sessions synchronisées du premier homologue, y compris les traductions NAT. Palo Alto Networks recommande la création d'une règle NAT double qui est liée à l'ID du second périphérique. Il y a ainsi deux règles NAT pour des adresses translatées source et des adresses translatées de destination identiques, soit une règle liée à chacun des ID du périphérique. Cette configuration permet à l'homologue HA de procéder aux taches de configuration d'une nouvelle session et d'effectuer la mise en correspondance de la règle NAT pour les règles NAT qui sont liées à son ID du périphérique. Sans une règle NAT double, l'homologue actif tentera d'effectuer la mise en correspondance de la politique NAT, mais la session ne correspondra pas aux règles propres au périphérique du pare-feu et le pare-feu sautera toutes les règles NAT qui ne sont pas liées à son ID du périphérique.

Vous souhaitez en savoir plus ?

Reportez-vous à la section NAT en mode HA actif/actif.

Onglet Cible NAT

- (Panorama uniquement) **Policies (Politiques)** > **NAT** > **Target (cible)**

Sélectionnez l'onglet **Target (Cible)** pour sélectionner les pare-feux gérés du groupe de périphériques auxquels appliqués la règle de politique. Vous pouvez préciser à quels pare-feux gérés appliquer en sélectionnant les pare-feux gérés ou en attribuant une étiquette. De plus, vous pouvez configurer la cible de la règle de politique à appliquer à tous les pare-feux gérés sauf ceux indiqués.

Règle NAT - Paramètres de la cible	Description
Tous (cible tous les périphériques)	Activez (cochez) pour valider la règle de politique de tous les pare-feux gérés du groupe de périphériques.
Périphériques	Sélectionnez un ou plusieurs pare-feux gérés associés au groupe de périphériques pour valider la règle de politique.
Étiquettes	**Add (Ajoutez)** une ou plusieurs étiquettes pour valider la règle de politique des pare-feux gérés dans le groupe de périphériques ayant l'étiquette indiquée.
Cibler tous les périphériques sauf ceux spécifiés	Activez (cochez) pour valider la règle de politique pour tous les pare-feux gérés associés au groupe de périphériques sauf pour le(s) périphérique(s) et étiquette(s) sélectionnés.

Politiques > QoS

Ajoutez des règles de politique QoS pour définir le trafic qui reçoit un traitement QoS spécifique et affecter une classe QoS à chaque règle de politique QoS afin de spécifier que la classe de service affectée s'applique à tous les trafics correspondants à la règle associée lorsqu'elle sort d'une interface sur laquelle la QoS est activée.

Les règles de politique de QoS transférées de Panorama vers un pare-feu s'affichent en orange et ne peuvent pas être modifiées au niveau du pare-feu.

De plus, pour permettre complètement au pare-feu d'assurer la QoS :

- Définissez des limites de bande passante pour chaque classe de service QoS (sélectionnez Réseau > Profils réseau > QoS pour ajouter ou modifier un profil QoS).
- Activez la QoS sur une interface (sélectionnez Réseau > QoS).

Référez-vous à la Qualité de service pour des flux de travail, des concepts et des cas pratiques relatifs à la QoS.

Vous devez **Ajouter** une nouvelle règle ou cloner une règle existante, puis définir les champs suivants.

Paramètres d'une règle de politique de QoS	
Onglet Général	
Name (Nom)	Saisissez un nom pour identifier la règle (63 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Description	Saisissez une description (facultatif).
Étiquette	Si vous avez besoin d'étiqueter la politique, cliquez sur **Ajouter** et indiquez l'étiquette. Une étiquette de politique est un mot-clé ou une expression qui vous permet de trier ou de filtrer les politiques. Cela est utile lorsque vous avez défini de nombreuses politiques et que vous souhaitez afficher celles qui sont identifiées par un mot-clé particulier. Par exemple, vous pouvez ajouter l'étiquette Trafic entrant vers la zone DMZ à certaines politiques de sécurité, les mots Déchiffrement et Aucun déchiffrement aux politiques de déchiffrement, ou utiliser le nom d'un centre de données spécifique pour les politiques associés à cet emplacement.
Regrouper des règles par étiquette	Saisissez une étiquette selon laquelle regrouper des règles de politique similaires. L'étiquette de groupe vous permet d'afficher votre base de règles de politique en fonction de ces étiquettes. Vous pouvez regrouper les règles en fonction d'une **Tag (Étiquette)**.
Commentaire d'audit	Saisissez un commentaire pour auditer la création ou la modification d'une règle de politique. Le commentaire d'audit est sensible à la casse et peut

Paramètres d’une règle de politique de QoS	
	comporter jusqu’à 256 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d’union et des traits de soulignement.
Archive des commentaires d’audit	Afficher les **Audit Comments (Commentaires d’audit)** précédents pour la règle de politique. Vous pouvez exporter l’archive des commentaires d’audit au format CSV.
Onglet Source	
Source Zone (Zone source)	Sélectionnez une ou plusieurs zones sources (la valeur par défaut est « **Indifférent** »). Les zones doivent être du même type (couche 2, couche 3 ou câble virtuel).
Source Address (Adresse source)	Indiquez une combinaison d'adresses IPv4 ou IPv6 sources dont l'application identifiée peut être écrasée. Pour sélectionner des adresses spécifiques, choisissez **select (sélectionner)** dans la liste déroulante et procédez de l'une des manières suivantes : • Sélectionnez cette option à côté des adresses  et/ou des groupes d’adresses  appropriés dans la colonne Disponible et cliquez sur **Ajouter** pour ajouter vos sélections à la colonne Sélectionnée. • Saisissez les premiers caractères d'un nom dans le champ Rechercher pour afficher toutes les adresses et tous les groupes d'adresses commençant par ces caractères. La sélection d'un élément dans la liste active cette option dans la colonne Disponibles. Répétez ce processus aussi souvent que nécessaire, puis cliquez sur **Add (Ajouter)**. • Saisissez une ou plusieurs adresses IP (une par ligne), avec ou sans masque réseau. Le format courant est : *<ip_address>/<mask>* • Pour supprimer des adresses, sélectionnez-les (colonne Sélectionné) et cliquez sur **Delete (Supprimer)** et cliquez sur Supprimer ou sélectionnez **any (indifférent)** pour effacer toutes les adresses et tous les groupes d'adresses. Pour ajouter de nouvelles adresses pouvant être utilisées dans cette politique ou dans d'autres politiques, cliquez sur **New Address (Nouvelle adresse)**. Pour définir de nouveaux groupes d’adresses, sélectionnez Objets > Groupes d’adresses.
Source User (Utilisateur source)	Indiquez les utilisateurs et groupes sources auxquels la politique de QoS va s'appliquer.
Inverser	Sélectionnez cette option pour que la politique s’applique en cas de non-correspondance des informations spécifiées dans cet onglet.

Paramètres d’une règle de politique de QoS	
Onglet Destination	
Destination Zone (Zone de destination)	Sélectionnez une ou plusieurs zones de destination (la valeur par défaut est **any (indifférent)**). Les zones doivent être du même type (couche 2, couche 3 ou câble virtuel).
Adresse de destination	Indiquez une combinaison d'adresses IPv4 ou IPv6 sources dont l'application identifiée peut être écrasée. Pour sélectionner des adresses spécifiques, choisissez **select (sélectionner)** dans la liste déroulante et procédez de l'une des manières suivantes : • Sélectionnez cette option à côté des adresses  et/ou des groupes d’adresses  appropriés dans la colonne Disponible et cliquez sur **Ajouter** pour ajouter vos sélections à la colonne Sélectionnée. • Saisissez les premiers caractères d'un nom dans le champ Rechercher pour afficher toutes les adresses et tous les groupes d'adresses commençant par ces caractères. La sélection d'un élément dans la liste active cette option dans la colonne Disponibles. Répétez ce processus aussi souvent que nécessaire, puis cliquez sur **Add (Ajouter)**. • Saisissez une ou plusieurs adresses IP (une par ligne), avec ou sans masque réseau. Le format courant est : <*ip_address*>/<*mask*> • Pour supprimer des adresses, sélectionnez-les (colonne Sélectionné) et cliquez sur **Delete (Supprimer)** et cliquez sur Supprimer ou sélectionnez **any (indifférent)** pour effacer toutes les adresses et tous les groupes d'adresses. Pour ajouter de nouvelles adresses pouvant être utilisées dans cette politique ou dans d'autres politiques, cliquez sur **New Address (Nouvelle adresse)**.
Inverser	Sélectionnez cette option pour que la politique s’applique en cas de non-correspondance des informations spécifiées dans cet onglet.
Onglet Application	
Application	Sélectionnez des applications spécifiques pour la règle de QoS. Pour définir de nouvelles applications ou de nouveaux groupes d’applications, sélectionnez **Objects (Objets)** > **Applications**. Si une application présente plusieurs fonctions, vous pouvez sélectionner l'application dans son ensemble ou des fonctions individuelles. Si vous sélectionnez l'application dans son ensemble, toutes les fonctions sont

Paramètres d’une règle de politique de QoS	
	incluses et la définition de l'application est automatiquement mise à jour lors de l'ajout de fonctions supplémentaires. Si vous utilisez des groupes d'applications, des filtres ou un conteneur dans la règle de QoS, vous pouvez afficher les détails de ces objets en passant la souris sur l'objet qui figure dans la colonne Application, cliquez sur la flèche vers le bas et sélectionnez **Value (Valeur)**. Ainsi, vous pouvez facilement accéder aux membres des applications directement depuis la politique sans passer par l’onglet **Objets**.
Onglet Service / Catégorie d’URL	
Service (Service)	Sélectionnez des services à limiter à des numéros de ports TCP et/ou UDP spécifiques. Choisissez l'une des options suivantes dans la liste déroulante : • **any (indifférent)** - Les applications sélectionnées sont autorisées ou non sur n'importe quel protocole ou port. • **application-default (par défaut de l’application)** - Les applications sélectionnées sont autorisées ou non seulement sur leurs **ports par défaut définis par Palo Alto Networks**. Cette option est recommandée pour les politiques d'autorisation. • **Select (Sélection)** - Cliquez sur **Add (Ajouter)**. Choisissez un service existant ou choisissez **Service** ou **Service Group (Groupe de services)** pour définir une nouvelle entrée.
URL Category (Catégorie d'URL)	Sélectionnez des catégories d'URL pour la règle de QoS. • Sélectionnez **Any (Indifférent)** pour vous assurer qu'une session peut correspondre à cette règle de QoS, quelle que soit la catégorie d'URL. • Pour indiquer une catégorie, cliquez sur **Add (Ajouter)** et sélectionnez une catégorie spécifique (y compris une catégorie personnalisée) dans la liste déroulante. Vous pouvez ajouter plusieurs catégories. Reportez-vous à Objets > Listes dynamiques externes pour des informations sur la définition des catégories personnalisées.
Onglet DSCP/TOS	
indifférent	Sélectionnez **Any (Indifférent)** (défini par défaut) pour autoriser la politique à être mise en correspondance avec le trafic, quel que soit la valeur DSCP (Differentiated Services Code Point/code d'accès aux services différenciés) ou ToS (type de service)/de priorité des adresses IP définie pour le trafic.
Points de code	Sélectionnez l'option **Codepoints (Points de code)** pour activer le trafic pour recevoir le traitement de la QoS en fonction de la valeur DSCP ou ToS définie dans l'en-tête IP d'un paquet. Les valeurs DSCP et ToS permettent d'indiquer le niveau de service demandé pour le trafic, tel que la remise au mieux. L'utilisation de points de code comme critère

Paramètres d’une règle de politique de QoS	
	de correspondance dans une politique de QoS permet à une session de recevoir le traitement de la QoS en fonction du point de code détecté au début de la session. Continuez d'**Ajouter** des points de code pour faire correspondre le trafic à la politique de QoS : • Donnez un **Name (Nom)** descriptif aux entrées de point de code. • Sélectionnez le **Type** de point de code que vous souhaitez utiliser comme critère de correspondance pour la politique de QoS, puis sélectionnez une valeur **Codepoint (Point de code)** spécifique. Vous pouvez également créer un **Custom Codepoint (Point de code personnalisé)** en saisissant un **Codepoint Name (Nom de point de code)** et une **Binary Value (Valeur binaire)**.
Onglet Autres paramètres	
class	Sélectionnez la classe de QoS à assigner à la règle et cliquez sur **OK**. Les caractéristiques d'une classe sont définies dans le profil de QoS. Reportez-vous à Réseau > Profils réseau > QoS pour des informations sur la configuration de paramètres pour les classes de QoS.
Programmer	• Sélectionnez **None (Aucun)** pour que la règle de politique soit active en tout temps. • À partir du menu déroulant, sélectionnez **Schedule (Calendrier)** (icône du calendrier) pour définir une plage horaire fixe ou récurrente pendant laquelle la règle est active.
Onglet cible (Panorama uniquement)	
Tous (cible tous les périphériques)	Activez (cochez) pour valider la règle de politique de tous les pare-feux gérés du groupe de périphériques.
Périphériques	Sélectionnez un ou plusieurs pare-feux gérés associés au groupe de périphériques pour valider la règle de politique.
Étiquettes	**Add (Ajoutez)** une ou plusieurs étiquettes pour valider la règle de politique des pare-feux gérés dans le groupe de périphériques ayant l’étiquette indiquée.
Cibler tous les périphériques sauf ceux spécifiés	Activez (cochez) pour valider la règle de politique pour tous les pare-feux gérés associés au groupe de périphériques sauf pour le(s) périphérique(s) et étiquette(s) sélectionnés.

Politiques > Transfert basé sur une politique

Normalement, lorsque le trafic entre dans le pare-feu, l’interface d’entrée du routeur virtuel dicte l’itinéraire qui détermine l’interface de sortie et la zone de sécurité de destination en se basant sur l’adresse IP de destination. En créant une règle de transfert basé sur une politique (Policy-based Forwarding, PBF), vous pouvez préciser d’autres informations pour déterminer l’interface de sortie, y compris la zone source, l’adresse source, l’utilisateur source, l’adresse de destination, l’application de destination et le service de destination. La session initiale sur une adresse IP de destination et un port donnés associés à une application ne correspondra à aucune règle spécifique à l'application et sera transférée conformément aux règles PBF subséquentes (qui ne précisent aucune application) ou à la table de transfert du routeur virtuel. Toutes les sessions subséquentes sur cette adresse IP de destination et ce port pour la même application correspondront à une règle spécifique à l'application. Pour assurer le transfert via des règles PBF, il est déconseillé d'utiliser des règles spécifiques à une application.

Si nécessaire, des règles PBF peuvent être utilisées pour forcer le passage du trafic dans un système virtuel supplémentaire à l'aide de l'action Transférer à Vsys. Dans ce cas, il est nécessaire de définir une règle PBF supplémentaire qui transférera le paquet depuis le système virtuel de destination vers une interface de sortie spécifique sur le pare-feu.

Les tableaux suivants décrivent les paramètres de transfert basé sur une politique'A0;:

- Onglet Général du transfert basé sur une politique
- Onglet Source de transmission basé sur une politique
- Onglet Destination / Application / Service de transmission basé sur une politique
- Onglet Transfert du transfert basé sur une politique
- (Panorama uniquement) Onglet Cible du transfert basé sur une politique

Vous souhaitez en savoir plus ?

Référez-vous au Transfert basé sur une politique

Onglet Général du transfert basé sur une politique

Sélectionnez l'onglet **General (Général)** pour définir un nom et une description pour la politique PBF. Une étiquette peut également être configurée et vous permettre de trier ou de filtrer les politiques lorsqu'il en existe un grand nombre.

Champ	Description
Name (Nom)	Donnez un nom à la règle afin de l'identifier. Le nom est sensible à la casse et peut comporter jusqu’à 63 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d’union et des traits de soulignement. Le nom doit être unique sur un pare-feu et, dans Panorama, unique au sein de son groupe de périphériques et des groupes de périphériques anciens ou descendants.
Description	Saisissez une description de la politique (1024 caractères maximum).

Champ	Description
Étiquette	Si vous avez besoin d'étiqueter la politique, cliquez sur **Ajouter** et indiquez l'étiquette. Une étiquette de politique est un mot-clé ou une expression qui vous permet de trier ou de filtrer les politiques. Cela est utile lorsque vous avez défini de nombreuses politiques et que vous souhaitez afficher celles qui sont identifiées par un mot-clé particulier. Par exemple, vous pouvez ajouter l'étiquette Trafic entrant vers la zone DMZ à certaines politiques de sécurité, les mots Déchiffrement et Aucun déchiffrement aux politiques de déchiffrement, ou utiliser le nom d'un centre de données spécifique pour les politiques associés à cet emplacement.
Regrouper des règles par étiquette	Saisissez une étiquette selon laquelle regrouper des règles de politique similaires. L'étiquette de groupe vous permet d'afficher votre base de règles de politique en fonction de ces étiquettes. Vous pouvez regrouper les règles en fonction d'une **Tag (Étiquette)**.
Commentaire d'audit	Saisissez un commentaire pour auditer la création ou la modification d'une règle de politique. Le commentaire d'audit est sensible à la casse et peut comporter jusqu'à 256 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement.
Archive des commentaires d'audit	Afficher les **Audit Comments (Commentaires d'audit)** précédents pour la règle de politique. Vous pouvez exporter l'archive des commentaires d'audit au format CSV.

Onglet Source du transfert basé sur une politique

L'onglet **Source** vous permet de définir la zone ou l'adresse source qui définit le trafic source entrant auquel la politique de transfert est appliquée.

Champ	Description
Source Zone (Zone source)	Pour choisir des zones source (valeur par défaut : indifférent), cliquez sur **Add (Ajouter)** et faites votre sélection dans la liste déroulante. Pour définir de nouvelles zones, voir Réseau > Zones. Il est possible d'utiliser plusieurs zones pour simplifier la gestion. Par exemple, si vous possédez trois zones internes différentes (marketing, ventes et relations publiques) qui sont toutes reliées à la zone de destination non approuvée, vous pouvez créer une règle qui couvre tous les cas possibles. *seules les zones de type Couche'A0;3 sont prises en charge pour le transfert basé sur la politique.*

Champ	Description
Source Address (Adresse source)	Cliquez sur **Add (Ajouter)** pour ajouter des adresses, des groupes d'adresses ou des régions source (valeur par défaut : indifférent). Faites votre sélection dans la liste déroulante ou cliquez sur **Address (Adresse)**, **Address Group (Groupe d'adresses)** ou **Regions (Régions)** en bas de la liste déroulante et définissez les paramètres.
Source User (Utilisateur source)	Cliquez sur **Add (Ajouter)** pour choisir les utilisateurs ou les groupes d'utilisateurs source soumis à la politique. Les types d'utilisateur source suivants sont pris en charge'A0;: • **any (indifférent)** - Inclut tout trafic, quelles que soient les données utilisateur. • **pre-logon (pré-ouverture de session)** - Inclut les utilisateurs distants connectés au réseau à l'aide de GlobalProtect™ mais non connectés à leur système. Lorsque l'option Pré-ouverture de session est configurée sur le portail des applications GlobalProtect, tout utilisateur non connecté à sa machine est identifié avec le nom d'utilisateur pre-logon. Vous pouvez ensuite créer des politiques pour les utilisateurs pre-logon. Bien que l'utilisateur ne soit pas directement connecté, sa machine est authentifiée sur le domaine, comme s'il était complètement connecté. • **known-user (utilisateur connu)** - Inclut tous les utilisateurs authentifiés, c'est-à-dire toute adresse IP dont les données utilisateur sont mappées. Cette option est équivalente au groupe « utilisateurs » du domaine sur un domaine. • **unknown (inconnu)** - Inclut tous les utilisateurs non authentifiés, c'est-à-dire les adresses IP non mappées à un utilisateur. Par exemple, vous pouvez utiliser l'option Inconnu pour accéder à quelque chose au niveau invité, car les invités ont une adresse IP sur votre réseau, mais ne sont pas authentifiés sur le domaine et ne disposent d'aucune information de mappage nom d'utilisateur/adresse IP sur le pare-feu. • **Select (Sélection)** - Inclut les utilisateurs sélectionnés dans cette fenêtre. Par exemple, vous pouvez ajouter un utilisateur, une liste d'individus, certains groupes ou des utilisateurs manuellement. *Si le pare-feu collecte les informations utilisateur depuis un serveur RADIUS, TACACS+ ou le serveur du fournisseur d'identité SAML et non depuis l'agent User-ID™, la liste des utilisateurs ne s'affiche pas ; vous devez saisir les informations de l'utilisateur manuellement.*

Onglet Destination / Application / Service du transfert basé sur une politique

Sélectionnez l'onglet **Destination/Application/Service** pour définir les paramètres de destination qui seront appliqués au trafic correspondant à la règle de transfert.

Champ	Description
Adresse de destination	Cliquez sur **Add (Ajouter)** pour ajouter des adresses de destination ou des groupes d'adresses (valeur par défaut : indifférent). Par défaut, la règle s'applique à **Any (Toute)** adresse IP. Faites votre sélection dans la liste déroulante ou cliquez sur **Address (Adresse)** ou sur **Address Group (Groupe d'adresses)** en bas de la liste déroulante et définissez les paramètres.
Application/Service	Sélectionnez des applications ou des services spécifiques pour la règle PBF. Pour définir de nouvelles applications, reportez-vous à la Définition des applications. Pour définir des groupes d'applications, reportez-vous à Objets > Groupes d'applications. *Il n'est pas recommandé d'utiliser les règles propres à une application avec le transfert basé sur une politique (PBF). Lorsque cela est possible, utilisez un objet de service, qui est le port de couche 4 (TCP ou UDP) utilisé par le protocole ou l'application.* Vous pouvez consulter les détails sur ces applications en passant la souris sur l'objet dans la colonne **Application**, en cliquant sur la flèche vers le bas et en sélectionnant **Value (Valeur)**. Ainsi, vous pouvez facilement accéder aux informations des applications directement depuis la politique sans passer par les onglets Objet. *Vous ne pouvez pas utiliser d'applications personnalisées, de filtres d'applications ou de groupes d'applications dans les règles PBF*

Onglet Transfert du transfert basé sur une politique

Sélectionnez l'onglet **Forwarding (Transfert)** pour définir les informations relatives aux actions et au réseau appliquées au trafic correspondant à la règle de transfert. Le trafic peut être transféré vers une adresse IP de saut suivant, un système virtuel ou être abandonné.

Champ	Description
Action (Action)	Sélectionnez l'une des options suivantes :

Champ	Description
	• **Forward (Transférer)** - Précisez l'adresse IP du saut suivant et l'interface de sortie (l'interface prise par le paquet pour accéder au saut suivant spécifié). • **Forward To VSYS (Transférer à VSYS)** - Choisissez le système virtuel vers lequel effectuer le transfert dans la liste déroulante. • **Discard (Supprimer)** : abandonne le paquet. • **No PBF (Aucun PBF)** - Pas de modification du chemin que le paquet suivra. Cette option exclut les paquets qui correspondent aux critères de la source/de la destination/de l'application/du service définis dans la règle. Les paquets correspondants utilisent la table de routage au lieu du transfert basé sur une politique ; le pare-feu utilise la table de routage pour exclure le trafic correspondant du port redirigé.  *Utilisez **Forward (Transfert)** ou **Forward to VSYS (Transfert au système virtuel)** en tant qu'action, pour que vous puissiez appliquer un profil de surveillance au trafic. (Vous ne pouvez appliquer un profil de surveillance lorsque l'action ne transfère par le trafic.) Les profils de surveillance surveillent l'adresse IP. En cas d'échec de la connectivité à l'adresse IP, les profils de surveillance précisent l'action.*
Interface de trafic sortant	Dirige le paquet vers une interface de sortie spécifique
Saut suivant	Si vous dirigez le paquet vers une interface spécifique, indiquez l'adresse IP du saut suivant du paquet de l'une des façons suivantes : • **IP Address (Adresse IP)** : Sélectionnez l'adresse IP et sélectionnez un objet d'adresse (ou créez un nouvel objet d'adresse) qui utilise une adresse IPv4 ou IPv6. • **FQDN** : Sélectionnez FQDN et sélectionnez un objet d'adresse (ou créez un nouvel objet d'adresse) qui utilise un FQDN. • **None (Aucun)** : Il n'y a pas de saut suivant ; le paquet est abandonné.
surveiller	Activez la surveillance pour vérifier la connexion à une **IP Address (Adresse IP)** cible ou à l'adresse IP de **Next Hop (Saut suivant)**. Sélectionnez **Monitor (Surveillance)** et associez un **Profile (Profil)** de surveillance (par défaut ou personnalisé, **Network [Réseau]** > **Network Profiles [Profils réseau]** > **Monitor [Surveillance]**) qui indique l'action lorsque l'adresse IP est inaccessible.  *Configurez les profils de surveillance et activez la surveillance pour que, en cas d'échec de l'interface de sortie ou de l'itinéraire, le pare-feu suit l'action du profil et minimise ou empêche l'interruption du service.*

Champ	Description
Appliquer le retour symétrique	(Obligatoire pour les environnements de routage asymétrique) Sélectionnez **Appliquer le retour symétrique**, puis saisissez une ou plusieurs adresses IP dans la Liste d'**Adresses du saut suivant**. L'activation du retour symétrique permet de s'assurer que le trafic de retour (par exemple, depuis la zone approuvée sur le réseau local vers Internet) est transféré via la même interface que celle au niveau de laquelle le trafic arrive d'Internet.
Programmer	Pour limiter les dates et les heures auxquelles la règle est en vigueur, sélectionnez un calendrier dans la liste déroulante. Pour définir de nouveaux calendriers, reportez-vous à Paramètres pour contrôler le trafic SSL déchiffré.

Onglet Cible du transfert basé sur une politique

- (Panorama uniquement) **Policies (Politiques)** > **Policy Based Forwarding (Transfert basé sur les politiques)** > **Target (Cible)**

Sélectionnez l'onglet **Target (Cible)** pour sélectionner les pare-feux gérés du groupe de périphériques auxquels appliqués la règle de politique. Vous pouvez préciser à quels pare-feux gérés appliquer en sélectionnant les pare-feux gérés ou en attribuant une étiquette. De plus, vous pouvez configurer la cible de la règle de politique à appliquer à tous les pare-feux gérés sauf ceux indiqués.

Règle NAT - Paramètres de la cible	Description
Tous (cible tous les périphériques)	Activez (cochez) pour valider la règle de politique de tous les pare-feux gérés du groupe de périphériques.
Périphériques	Sélectionnez un ou plusieurs pare-feux gérés associés au groupe de périphériques pour valider la règle de politique.
Étiquettes	**Add (Ajoutez)** une ou plusieurs étiquettes pour valider la règle de politique des pare-feux gérés dans le groupe de périphériques ayant l'étiquette indiquée.
Cibler tous les périphériques sauf ceux spécifiés	Activez (cochez) pour valider la règle de politique pour tous les pare-feux gérés associés au groupe de périphériques sauf pour le(s) périphérique(s) et étiquette(s) sélectionnés.

Politiques > Déchiffrement

Vous pouvez configurer le pare-feu de manière à déchiffrer le trafic à des fins de visibilité, de contrôle et de sécurité granulaire. Les politiques de chiffrement peuvent s'appliquer au protocole SSL (Secure Sockets Layer/couche de sockets sécurisés), notamment les protocoles encapsulés SSL tels que IMAP(S), POP3(S), SMTP(S), FTP(S) et le trafic SSH (Secure Shell). L'option SSH vous permet de déchiffrer le trafic SSH sortant et entrant pour vous assurer que des protocoles sécurisés ne sont pas utilisés pour établir un tunnel pour des applications et du contenu non autorisés.

Ajoutez une règle de politiques de déchiffrement pour définir le trafic que vous voulez déchiffrer (par exemple, vous pouvez déchiffrer le trafic en fonction de la catégorisation d'URL). Les règles des politiques de déchiffrement sont comparées au trafic dans un ordre précis, donc les règles les plus spécifiques doivent précéder les règles plus générales.

Le déchiffrement du proxy de transfert SSL nécessite la configuration d'un certificat de confiance qui est présenté à l'utilisateur si le serveur auquel il se connecte possède un certificat signé par une autorité de certification de confiance. Créez un certificat sur la page **Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)**, puis cliquez sur le nom du certificat et sélectionnez **Forward Trust Certificate (Transférer le certificat sécurisé)**.

Le pare-feu ne déchiffre par les applications qui interrompent le déchiffrement techniquement, par exemple, parce qu'elles utilisent des certificats épinglés ou l'authentification du client.

Reportez-vous à la Liste des applications exclues du déchiffrement SSL.

Les tableaux suivants décrivent les paramètres d'une politique de déchiffrement :

- Onglet Général du déchiffrement
- Onglet déchiffrement de la source
- Onglet Déchiffrement de la destination
- Onglet Service de déchiffrement / catégorie d'URL
- Onglet Options de Déchiffrement
- (Panorama uniquement) Onglet cible de déchiffrement

Vous souhaitez en savoir plus ?

Voir déchiffrement

Onglet Général du déchiffrement

Sélectionnez l'onglet **Général** pour définir un nom et une description pour la politique de déchiffrement. Vous pouvez également configurer une étiquette afin de pouvoir trier ou filtrer les politiques lorsqu'il existe un grand nombre de politiques.

Champ	Description
Name (Nom)	Donnez un nom à la règle afin de l'identifier. Le nom est sensible à la casse et peut comporter jusqu'à 63 caractères qui peuvent être

Champ	Description
	des lettres, des nombres, des espaces, des traits d’union et des traits de soulignement. Le nom doit être unique sur un pare-feu et, dans Panorama, unique au sein de son groupe de périphériques et des groupes de périphériques anciens ou descendants.
Description	Saisissez une description de la règle (1024 caractères maximum).
Étiquette	Si vous avez besoin d’étiqueter la politique, cliquez sur **Ajouter** et indiquez l’étiquette. Une étiquette de politique est un mot-clé ou une expression qui vous permet de trier ou de filtrer les politiques. Cela est utile lorsque vous avez défini de nombreuses politiques et que vous souhaitez afficher celles qui sont identifiées par un mot-clé particulier. Par exemple, vous pouvez ajouter l'étiquette Trafic entrant vers la zone DMZ à certaines politiques de sécurité, les mots Déchiffrement et Aucun déchiffrement aux politiques de déchiffrement, ou utiliser le nom d'un centre de données spécifique pour les politiques associés à cet emplacement.
Regrouper des règles par étiquette	Saisissez une étiquette selon laquelle regrouper des règles de politique similaires. L’étiquette de groupe vous permet d'afficher votre base de règles de politique en fonction de ces étiquettes. Vous pouvez regrouper les règles en fonction d’une **Tag (Étiquette)**.
Commentaire d’audit	Saisissez un commentaire pour auditer la création ou la modification d’une règle de politique. Le commentaire d’audit est sensible à la casse et peut comporter jusqu’à 256 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d’union et des traits de soulignement.
Archive des commentaires d’audit	Afficher les **Audit Comments (Commentaires d’audit)** précédents pour la règle de politique. Vous pouvez exporter l’archive des commentaires d’audit au format CSV.

Onglet déchiffrement de la source

Sélectionnez l'onglet **Source** pour définir la zone ou l'adresse source qui définit le trafic source entrant auquel la politique de déchiffrement est appliquée.

Champ	Description
Zone source	Cliquez sur **Ajouter** pour choisir des zones source (valeur par défaut : indifférent). Les zones doivent être du même type (couche 2, couche 3 ou câble virtuel). Pour définir de nouvelles zones, voir Réseau > Zones. Il est possible d'utiliser plusieurs zones pour simplifier la gestion. Par exemple, si vous possédez trois zones internes différentes (marketing,

Champ	Description
	ventes et relations publiques) qui sont toutes reliées à la zone de destination non approuvée, vous pouvez créer une règle qui couvre tous les cas possibles.
Adresse source	Cliquez sur **Add (Ajouter)** pour ajouter des adresses, des groupes d'adresses ou des régions source (valeur par défaut : indifférent). Faites votre sélection dans la liste déroulante ou cliquez sur **Adresse**, **Groupe d'adresses** ou **Régions** en bas de la liste déroulante et définissez les paramètres. Sélectionnez **inverser** pour choisir n'importe quelle adresse sauf celles configurées.
Utilisateur source	Cliquez sur **Add (Ajouter)** pour choisir les utilisateurs ou les groupes d'utilisateurs source soumis à la politique. Les types d'utilisateur source suivants sont pris en charge'A0;: • **tout** - Inclut tout trafic, quelles que soient les données utilisateur. • **pré-ouverture de session** - Inclut les utilisateurs distants connectés au réseau à l'aide de GlobalProtect mais non connectés à leur système. Lorsque l'option Pré-ouverture de session est configurée sur le portail des applications GlobalProtect, tout utilisateur non connecté à sa machine est identifié avec le nom d'utilisateur pre-logon. Vous pouvez ensuite créer des politiques pour les utilisateurs pre-logon. Bien que l'utilisateur ne soit pas directement connecté, sa machine est authentifiée sur le domaine, comme s'il était complètement connecté. • **known-user (utilisateur connu)** - Inclut tous les utilisateurs authentifiés, c'est-à-dire toute adresse IP dont les données utilisateur sont mappées. Cette option est équivalente au groupe « utilisateurs » du domaine sur un domaine. • **inconnu** - Inclut tous les utilisateurs non authentifiés, c'est-à-dire les adresses IP non mappées à un utilisateur. Par exemple, vous pouvez utiliser l'option Inconnu pour accéder à quelque chose au niveau invité, car les invités ont une adresse IP sur votre réseau, mais ne sont pas authentifiés sur le domaine et ne disposent d'aucune information de mappage nom d'utilisateur/adresse IP sur le pare-feu. • **Sélection** - Inclut les utilisateurs sélectionnés dans cette fenêtre. Par exemple, vous pouvez ajouter un utilisateur, une liste d'individus, certains groupes ou des utilisateurs manuellement.  *Si le pare-feu collecte les informations utilisateur depuis un serveur RADIUS, TACACS+ ou le serveur du fournisseur d'identité SAML et non depuis l'agent User-ID™, la liste des utilisateurs ne s'affiche pas ; vous devez saisir les informations de l'utilisateur manuellement.*

Onglet Déchiffrement de la destination

Sélectionnez l’onglet **Destination** pour définir la zone ou l’adresse de destination qui définit le trafic de destination auquel la politique sera appliquée.

Champ	Description
Zone de destination	Cliquez sur **Ajouter** pour choisir des zones de destination (valeur par défaut : indifférent). Les zones doivent être du même type (couche 2, couche 3 ou câble virtuel). Pour définir de nouvelles zones, reportez-vous à la section Réseau > Zones. Il est possible d'utiliser plusieurs zones pour simplifier la gestion. Par exemple, si vous possédez trois zones internes différentes (marketing, ventes et relations publiques) qui sont toutes reliées à la zone de destination non approuvée, vous pouvez créer une règle qui couvre tous les cas possibles.
Adresse de destination	Cliquez sur **Ajouter** pour ajouter des adresses, des groupes d'adresses ou des régions de destination (valeur par défaut : indifférent). Faites votre sélection dans la liste déroulante ou cliquez sur **Adresse**, **Groupe d'adresses** ou **Régions** en bas de la liste déroulante et définissez les paramètres. Sélectionnez **inverser** pour choisir n'importe quelle adresse sauf celles configurées.

Onglet Service de déchiffrement / catégorie d’URL

Sélectionnez l'onglet **Service/Catégorie d'URL** pour appliquer la politique de déchiffrement au trafic en fonction de numéros de ports TCP ou à n'importe quelle catégorie d'URL (ou une liste de catégories).

Champ	Description
Service	Appliquez la politique de déchiffrement au trafic en fonction de numéros de ports TCP spécifiques. Choisissez l'une des options suivantes dans la liste déroulante : • **tout** - Les applications sélectionnées sont autorisées ou non sur n'importe quel protocole ou port. • **application-défaut** - Les applications sélectionnées sont décryptées (ou non) seulement sur les ports des applications définis par défaut par Palo Alto Networks. • **Sélection** - Cliquez sur **Ajouter**. Sélectionnez un service existant ou indiquez un nouveau **Service** ou **Groupe de services**. (Ou sélectionnez Objets > Services et Objets > Groupes de services).

Champ	Description
Catégorie d'URL	Sélectionnez des catégories d'URL pour la règle de déchiffrement. • Choisissez **tout** pour appliquer la règle à toutes les sessions, quelle que soit la catégorie d'URL. • Pour indiquer une catégorie, cliquez sur **Ajouter** et sélectionnez une catégorie spécifique (y compris une catégorie personnalisée) dans la liste déroulante. Vous pouvez ajouter plusieurs catégories. Pour plus d'informations sur la définition de catégories personnalisées, reportez-vous à cette section.

Onglet Options de Déchiffrement

Sélectionnez l'onglet **Options** pour déterminer si le trafic correspondant doit être décrypté ou non. Si l'option **Déchiffrer** est définie, indiquez le type de déchiffrement. Vous pouvez également ajouter des fonctions de déchiffrement supplémentaires en configurant ou en sélectionnant un profil de déchiffrement.

Champ	Description
Action	Sélectionnez **déchiffrement** ou **aucun déchiffrement** pour le trafic.
Type	Sélectionnez le type de trafic à déchiffrer dans la liste déroulante : • **Proxy de transfert SSL** - Précise que la politique déchiffrera le trafic client destiné à un serveur externe. • **SSH Proxy (Proxy SSH)** - Précise que la politique déchiffrera le trafic SSH. Cette option vous permet de contrôler la tunnellisation SSH dans les politiques en précisant l'App-ID ssh-tunnel.

Champ	Description
	• **Inspection SSL entrante —**Spécifie que la stratégie déchiffre le trafic SSL entrant. • Certificats—Ajoutez les certificats du serveur interne auquel le trafic SSL entrant est destiné. *Après avoir renouvelé ou remplacé un certificat de serveur existant, importez le groupe de certificats en tant que fichier unique sur votre pare-feu et ajoutez-le à votre règle de stratégie de décryptage SSL Inbound Inspection. La mise à jour préalable de la règle de stratégie garantit que le déchiffrement se poursuit sans interruption lorsque vous installez éventuellement le nouveau certificat sur votre serveur Web.* Configure SSL Inbound Inspection *explique cette meilleure pratique plus en détail.* Vous pouvez également ajouter des certificats pour les domaines hébergés par votre serveur Web. Un maximum de 12 certificats est pris en charge par règle de stratégie.
Profil de décryptage	Associez un profil de déchiffrement à une règle de politique afin de bloquer et de contrôler certains aspects du trafic. Pour plus d'informations concernant la création d'un profil de déchiffrement, sélectionnez Objets > Profils de déchiffrement.
Paramètres des journaux	
Journaliser une communication SSL réussie	(En option) Crée des journaux détaillés des communication de décryptage SSL réussies. Cette option est désactivée par défaut. *Les journaux consomment de l'espace de stockage. Avant de journaliser les communications SSL réussies, assurez-vous d'avoir les ressources nécessaires pour stocker les journaux. Modifiez* ***Device (Périphérique)*** *>* ***Setup (Configuration)*** *>* ***Management (Gestion)*** *>* ***Logging and Reporting Settings (Paramètres de journalisation et de création de rapports)*** *pour vérifier l'attribution de mémoire de journaux actuelle et réattribuer de la mémoire de journaux entre les types de journaux.*
Journaliser une communication SSL avortée	Crée des journaux détaillés des communications de décryptage SSL avortées afin que vous puissiez trouver la cause des problèmes de décryptage. Cette option est activée par défaut.

Champ	Description
	*Les journaux consomment de l'espace de stockage. Pour attribuer plus (ou moins) d'espace de stockage de journaux aux journaux de décryptage, modifiez l'attribution de mémoire de journaux (**Périphérique** > **Configuration** > **Gestion** > **Journalisation et création de rapports**).*
Transfert des journaux	Indiquez la méthode et l'emplacement de transfert des journaux (de décryptage) de communication GlobalProtect SSL.

Onglet cible de déchiffrement

- (Panorama uniquement) **Politiques** > **Déchiffrement** > **cible**

Sélectionnez l'onglet **Cible** pour sélectionner les pare-feux gérés du groupe de périphériques auxquels appliqués la règle de politique. Vous pouvez préciser à quels pare-feux gérés appliquer en sélectionnant les pare-feux gérés ou en attribuant une étiquette. De plus, vous pouvez configurer la cible de la règle de politique à appliquer à tous les pare-feux gérés sauf ceux indiqués.

Règle NAT - Paramètres de la cible	Description
Tous (cible tous les périphériques)	Activez (cochez) pour valider la règle de politique de tous les pare-feux gérés du groupe de périphériques.
Périphériques	Sélectionnez un ou plusieurs pare-feux gérés associés au groupe de périphériques pour valider la règle de politique.
Étiquettes	**Add (Ajoutez)** une ou plusieurs étiquettes pour valider la règle de politique des pare-feux gérés dans le groupe de périphériques ayant l'étiquette indiquée.
Cibler tous les périphériques sauf ceux spécifiés	Activez (cochez) pour valider la règle de politique pour tous les pare-feux gérés associés au groupe de périphériques sauf pour le(s) périphérique(s) et étiquette(s) sélectionnés.

Politiques >Broker de paquets de réseau

Les règles de politique de Broker de paquets de réseau définissent le trafic à transférer vers une chaîne externe d'appareils de sécurité tierces (une chaîne de sécurité) en fonction des applications, des utilisateurs, des zones, des périphériques et des adresses IP. Le Broker de paquets de réseau peut transférer le trafic TLS déchiffré, TLS non déchiffré et non TLS vers une chaîne de sécurité. Vous attachez un profil de Broker de paquets à chaque règle de politique du Broker de paquets de réseau. La règle de politique définit le trafic à transférer vers la chaîne de sécurité et le profil définit comment transférer ce trafic, y compris les interfaces de transfert du pare-feu, la surveillance de l'intégrité, la distribution de session entre plusieurs chaînes et le choix si la chaîne est routée (couche 3) ou en Passerelle transparente (couche 1).

Les tableaux suivants décrivent les paramètres des règles de politique et les options de l'optimiseur de politique de Broker de paquets de réseau :

- Onglet Général du Broker de paquets de réseau
- Onglet Source du Broker de paquets réseau
- Onglet Destination du Broker de paquets réseau
- Onglet Application/Service/Trafic du Broker de paquets de réseau
- Onglet Sélection du chemin d’accès du Broker de paquets de réseau
- Utilisation de la règle d’optimisation de la politique du Broker de paquets de réseau

Onglet Général du Broker de paquets de réseau

Sélectionnez l'onglet **General (Général)** pour configurer un nom et une description pour la politique. Vous pouvez également configurer une étiquette afin de pouvoir trier ou filtrer les politiques lorsqu’il existe un grand nombre de politiques.

Champ	Description
Name (Nom)	Donnez un nom à la règle afin de l'identifier. Le nom est sensible à la casse et peut comporter jusqu’à 63 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d’union et des traits de soulignement. Le nom doit être unique sur un pare-feu et, dans Panorama, unique au sein de son groupe de périphériques et des groupes de périphériques anciens ou descendants.
Description	Saisissez une description de la politique (1024 caractères maximum).
Étiquette	Si vous avez besoin d’étiqueter la politique, cliquez sur **Ajouter** et indiquez l’étiquette. Une étiquette de politique est un mot-clé ou une expression qui vous permet de trier ou de filtrer les politiques. Cela est utile lorsque vous avez défini de nombreuses politiques et que vous souhaitez afficher les politiques qui sont identifiées par un mot-clé particulier. Par exemple, la balise peut indiquer l'emplacement du réseau, les chaînes de sécurité de couche 3 ou les chaînes de sécurité de couche 1.

Champ	Description
Regrouper des règles par étiquette	Saisissez une étiquette selon laquelle regrouper des règles de politique similaires. La balise de groupe vous permet d'afficher des groupes de règles de politique basées sur ces balises.
Commentaire d’audit	Saisissez un commentaire pour auditer la création ou la modification d’une règle de politique. Le commentaire d’audit est sensible à la casse et peut comporter jusqu’à 256 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d’union et des traits de soulignement.
Archive des commentaires d’audit	Afficher les **Audit Comments (Commentaires d’audit)** précédents pour la règle de politique. Vous pouvez exporter l’archive des commentaires d’audit au format CSV.

Onglet Source du Broker de paquets réseau

Sélectionnez l'onglet **Source** pour définir les zones sources, les adresses IP, les utilisateurs et les périphériques de trafic à transmettre à une chaîne de sécurité du Broker de paquets de réseau.

Champ	Description
Source Zone (Zone source)	Pour choisir des zones source (valeur par défaut : indifférent), cliquez sur **Add (Ajouter)** et faites votre sélection dans la liste déroulante. Pour définir de nouvelles zones, voir Réseau > Zones. Vous pouvez ajouter plusieurs zones pour simplifier la gestion.
Adresse source	Cliquez sur **Add (Ajouter)** des adresses, des groupes d’adresses ou des régions source (la valeur par défaut est **Any [indifférent]**). Faites votre sélection dans la liste déroulante ou sélectionnez l’objet d’**Adresse**, le **Groupe d'adresses** ou les **Régions** (en bas de la liste déroulante) pour définir les paramètres. Objects>Addresses (Objets > Adresses) et Objects>Address Groupes (Objets > Groupes d’adresses) décrivent les types d’objets d’adresses et les groupes d’adresses, respectivement, qu’une règle de politiques de sécurité prend en charge. Si vous sélectionnez l’option **Negate (Nier)**, la règle appliquera les adresses source de la zone spécifiée, à l’exception des adresses spécifiées.
Utilisateur source	Cliquez sur **Add (Ajouter)** pour choisir les utilisateurs ou les groupes d'utilisateurs source soumis à la politique. Les types d'utilisateur source suivants sont pris en charge'A0;: • **any (indifférent)** - Inclut tout trafic, quelles que soient les données utilisateur. • **pre-logon (pré-ouverture de session)** - Inclut les utilisateurs distants connectés au réseau à l’aide de GlobalProtect™ mais non connectés à leur système. Lorsque l'option Pré-ouverture de session est configurée

Champ	Description
	sur le portail des applications GlobalProtect, tout utilisateur non connecté à sa machine est identifié avec le nom d'utilisateur pre-logon. Vous pouvez ensuite créer des politiques pour les utilisateurs pre-logon. Bien que l'utilisateur ne soit pas directement connecté, sa machine est authentifiée sur le domaine, comme s'il était complètement connecté. • **known-user (utilisateur connu)** - Inclut tous les utilisateurs authentifiés, c'est-à-dire toute adresse IP dont les données utilisateur sont mappées. Cette option est équivalente au groupe « utilisateurs » du domaine sur un domaine. • **unknown (inconnu)** - Inclut tous les utilisateurs non authentifiés, c'est-à-dire les adresses IP non mappées à un utilisateur. Par exemple, vous pouvez utiliser l'option Inconnu pour accéder à quelque chose au niveau invité, car les invités ont une adresse IP sur votre réseau, mais ne sont pas authentifiés sur le domaine et ne disposent d'aucune information de mappage nom d'utilisateur/adresse IP sur le pare-feu. • **Select (Sélection)** - Inclut les utilisateurs sélectionnés dans cette fenêtre. Par exemple, vous pouvez ajouter un utilisateur, une liste d'individus, certains groupes ou des utilisateurs manuellement. *Si le pare-feu collecte les informations utilisateur depuis un serveur RADIUS, TACACS+ ou le serveur du fournisseur d'identité SAML et non depuis l'agent User-ID™, la liste des utilisateurs ne s'affiche pas ; vous devez saisir les informations de l'utilisateur manuellement.*
Périphérique source	**Ajoutez** les périphériques hôtes soumis à la politique : • **Tout** : inclut n'importe quel périphérique. • **pas de hip** – Les informations HIP ne sont pas requises. Ce paramètre permet d'accéder à des périphériques tiers qui ne peuvent pas collecter ou soumettre des informations HIP. • **sélectionner** : Inclut les périphériques sélectionnés comme déterminé par votre configuration. Par exemple, vous pouvez ajouter un périphérique sur la base d'un modèle, OS, famille d'OS ou fournisseur.

Onglet Destination du Broker de paquets réseau

Sélectionnez l'onglet **Destination** pour définir les zones de destination, les adresses IP et les périphériques de trafic à transmettre à une chaîne de sécurité du Broker de paquets de réseau.

Champ	Description
Zone de destination	Pour choisir des zones source (valeur par défaut : indifférent), cliquez sur **Add (Ajouter)** et faites votre sélection dans la liste déroulante. Pour définir de nouvelles zones, voir Réseau > Zones. Vous pouvez ajouter plusieurs zones pour simplifier la gestion.
Adresse de destination	Cliquez sur **Ajouter** des adresses, des groupes d'adresses ou des régions de destination (la valeur par défaut est **n'importe laquelle**). Faites votre sélection dans la liste déroulante ou cliquez sur l'objet d'**Adresse**, le **Groupe d'adresses** ou les **Régions** (en bas de la liste déroulante) pour définir les paramètres d'adresses. Objects>Addresses (Objets > Adresses) et Objects>Address Groupes (Objets > Groupes d'adresses) décrivent les types d'objets d'adresses et les groupes d'adresses, respectivement, qu'une règle de politiques de sécurité prend en charge. Si vous sélectionnez l'option **Negate (Nier)**, la règle appliquera les adresses de destination de la zone spécifiée, à l'exception des adresses spécifiées.
Périphérique de destination	**Add (Ajoutez)** individuellement les appareils hôtes soumis à la stratégie ou sélectionnez **Any (n'importe lequel)** pour inclure tous les appareils.

Onglet Application/Service/Trafic du Broker de paquets de réseau

Sélectionnez l'onglet **Application/Service/Traffic (Application/Service/Trafic)** pour définir le type de trafic, les applications et les services à transférer vers une chaîne de sécurité du Broker de paquets de réseau. Vous pouvez transférer n'importe quelle combinaison de trafic TLS déchiffré, TLS non déchiffré et non TLS vers une chaîne de sécurité.

Champ	Description
Type de trafic	Sélectionnez le ou les types de trafic à transférer vers la chaîne de sécurité. Vous pouvez sélectionner un, certains ou tous les types de trafic dans une seule règle : • **Forward TLS(Decrypted) Traffic (Transférer le trafic TLS (déchiffré)**: (par défaut) Transfère le trafic TLS déchiffré vers la chaîne de sécurité spécifiée par le profil du broker de paquets lié à la politique de broker de paquets. • **Forward TLS(Non-Decrypted) Traffic (Transférer le trafic TLS (non déchiffré)** : transfère le trafic TLS non déchiffré vers la chaîne de sécurité spécifiée par le profil de broker de paquets lié à la politique de broker de paquets. • **Forward Non-TLS Traffic (Transférer le trafic non-TLS)**: transfère le trafic en texte clair (non-TLS) vers la chaîne de sécurité spécifiée par le profil du broker de paquets lié à la politique de broker de paquets.

Champ	Description
Application	**Add (Ajoutez)** des applications spécifiques pour la règle de politique du broker de paquets de réseau. Si une application présente plusieurs fonctions, vous pouvez sélectionner l'application dans son ensemble ou des fonctions individuelles. Si vous sélectionnez l'application conteneur, toutes les applications fonctionnelles sont incluses et la définition de l'application est automatiquement mise à jour à mesure que les futures applications fonctionnelles sont ajoutées à l'application conteneur.
Service	Sélectionnez les services que vous souhaitez limiter à des numéros de ports TCP et/ou UDP spécifiques. Choisissez l'une des options suivantes dans la liste déroulante : • **any (n'importe laquelle)**—(Par défaut) Les applications sélectionnées sont transmises sur n'importe quel protocole ou port. • **application-default (application par défaut)**: les applications sélectionnées sont transmises uniquement si elles se trouvent sur leurs ports par défaut tels que définis par Palo Alto Networks®. (Les applications qui s'exécutent sur des ports et des protocoles non standard, si elles ne sont pas intentionnelles, peuvent être un signe de comportement et d'utilisation indésirables des applications, et si elles sont intentionnelles, peuvent être un signe de comportement malveillant. Toutefois, les applications personnalisées internes peuvent utiliser des ports non standard et nécessiter des exceptions.) • **Select (Sélectionnez)** - **Add (Ajoutez)** un service existant ou choisissez **Service** ou **Service Group (Groupe de services)** pour définir une nouvelle entrée. (Ou sélectionnez Objets > Services et Objets > Groupes de services).

Onglet Sélection du chemin d'accès du Broker de paquets de réseau

Sélectionnez **Path Selection Tab (onglet sélection du chemin d'accès)** pour choisir le profil du Broker de paquets à appliquer au trafic défini par la politique du Broker de paquets. La politique définit le trafic à transférer vers une chaîne de sécurité et le profil définit comment transférer le trafic (quelles interfaces de transfert de pare-feu utiliser, si la chaîne de sécurité est une chaîne de couche 3 routée ou une chaîne de couche 1 de pont transparent, méthodes de surveillance de l'intégrité, etc.).

Utilisez la liste déroulante pour sélectionner un profil précédemment configuré ou pour créer un nouveau profil de Broker de paquets pour la règle de politique.

Utilisation de la règle d'optimisation de la politique du Broker de paquets de réseau

Pour les règles de politique du Broker de paquets de réseau, l'optimisateur de politique affiche les statistiques de **Rule Usage (Utilisation des règles)** que vous pouvez utiliser pour déterminer si une politique est en cours d'utilisation. Vous pouvez afficher l'utilisation des règles sur différentes périodes

et rechercher pourquoi une règle n’a pas été utilisée comme prévu et supprimer les règles inutilisées ou obsolètes.

Champ	Description
Délai	La durée (nombre de jours) pendant laquelle les données sont affichées.
Usage	• **Any n’importe laquelle)** de toutes les règles de politique du Broker de paquets de réseau sur le pare-feu dans le **Timeframe (délai indiqué)**, quel que soit le trafic qui a correspondu aux règles (règles utilisées) ou non (règles non utilisées). • Règles **Unused (non utilisées)** auxquelles le trafic n’a pas correspondu dans le **Timeframe (délai)** indiqué. • Règles **Used (utilisées)** auxquelles le trafic a correspondu dans le **Timeframe (délai)** indiqué.
Exclure la réinitialisation des règles au cours des «n» derniers jours	Omet d’afficher les règles pour lesquelles vous **Reset Rule Hit Counter (Réinitialiser le Compteur d’accès de la règle)** pendant le nombre de jours indiqué (de 1 à 5 000 jours). Par exemple, cela vous permet d’examiner des règles plus anciennes qui n’ont pas correspondu au trafic pendant un **Timeframe (délai)** tout en excluant les règles plus récentes qui n’ont peut-être pas eu le temps de correspondre au trafic.
Nom	Nom de la règle de politique du Broker de paquets de réseau.
Broker de paquets	• **Profile (Profil)**: nom du profil du Broker de paquets associé à la règle de stratégie. • **Traffic Type (Type de trafic)** : type ou types de trafic que la règle contrôle (un ou plusieurs trafics TLS déchiffrés, TLS non déchiffrés et non TLS).
Rule Usage (Utilisation d'une règle)	• **Hit Count (Nombre de correspondances)** : Le nombre de fois où le trafic a correspondu à la règle. • **Last Hit (Dernière correspondance)** : La dernière correspondance du trafic à la règle. • **First Hit (Première correspondance)** : La première correspondance du trafic à la règle. • **Reset Date (Date de réinitialisation)** : La dernière date à laquelle le compteur de correspondance de la règle a été réinitialisé.
Modifié	La date et l'heure de modification de la règle.
Créé	La date et l'heure de création de la règle.

Politiques > Inspection des tunnels

Vous pouvez configurer le pare-feu pour inspecter le contenu du trafic des protocoles de tunnel de texte en clair suivants :

- encapsulation générique de routage (GRE) ;
- protocole de tunnellisation du service général de radiocommunication par paquets (GPRS Tunneling Protocol) pour les données utilisateur (GTP-U) ; pris en charge uniquement par les pare-feu qui prennent en charge GTP.
- trafic IPSec non chiffré (Algorithme de chiffrement NULL pour IPSec et mode de transport IPSec AH) ;
- Réseau local (LAN) virtuel extensible (VXLAN)

Vous pouvez utiliser l'inspection du contenu du tunnel pour appliquer les règles de sécurité, la Protection DoS et les politiques de trafic QoS dans ces types de tunnels et sur le trafic imbriqué dans un autre tunnel de texte en clair (par exemple, IPSec chiffré Null à l'intérieur d'un tunnel GRE).

Créez une politique d'Inspection de tunnel qui, lorsqu'elle correspond à un paquet entrant, détermine les protocoles de tunnel dans le paquet que le pare-feu inspectera et spécifie les conditions dans lesquelles le pare-feu supprime ou continue à traiter le paquet. Vous pouvez consulter les journaux d'inspection de tunnel et l'activité du tunnel dans l'ACC pour vérifier que le trafic par tunnel est conforme aux politiques de sécurité et d'utilisation de votre entreprise.

Le pare-feu supporte l'inspection du contenu du tunnel sur les interfaces et les sous-interfaces Ethernet, les interfaces AE, les interfaces VLAN et les tunnels VPN et LSVPN. La fonctionnalité est prise en charge dans les interfaces de niveau 3, de niveau 2, le câble virtuel et les déploiements Tap. L'inspection du contenu du tunnel fonctionne sur les passerelles partagées et sur les communications de système vers système virtuel.

Que voulez-vous savoir ?	Reportez-vous à la section :
Quels sont les champs disponibles pour créer une politique d'Inspection des tunnels ?	Blocs de construction dans une politique d'inspection des tunnels
Comment puis-je consulter les journaux d'inspection du tunnel ?	Types de journaux et Niveaux de gravité
Vous souhaitez en savoir plus ?	Inspection du contenu du tunnel

Blocs de construction dans une politique d'inspection des tunnels

Sélectionnez **Politiques** > **Inspection des tunnels** pour ajouter une règle de politique d'inspection des tunnels. Vous pouvez utiliser le pare-feu pour inspecter le contenu des protocoles de tunnel de texte en clair (GRE, GTP-U, protocole IPSec non chiffrés et VXLAN) et utiliser l'inspection du contenu du tunnel pour appliquer les politiques de sécurité, de Protection DoS et de trafic QoS sur le trafic de ces types de tunnels. Tous les modèles de pare-feu prennent en charge l'inspection du contenu du tunnel des tunnels GRE et IPSec non chiffrés, mais seuls les pare-feu qui prennent en charge GTP prennent en charge

l’inspection du contenu des tunnels GTP-U. Le tableau suivant décrit les champs que vous configurez pour une politique d’Inspection des tunnels.

Blocs de construction dans une politique d’inspection des tunnels	Configuré dans	Description
Nom	**Général**	Saisissez un nom pour la politique d’Inspection des tunnels, commençant par un caractère alphanumérique et pouvant contenir des zéros ou d’autres caractères alphanumériques, des traits de soulignement, des traits d’union, des points et des espaces.
Description		(Facultatif) Saisissez une description de la politique d’inspection des Tunnels.
Étiquettes		(Facultatif) Saisissez un ou plusieurs tags pour la journalisation et la génération de rapports qui identifient les paquets soumis à la politique d’Inspection des tunnels.
Regrouper des règles par étiquette		Saisissez une étiquette selon laquelle regrouper des règles de politique similaires. L’étiquette de groupe vous permet d'afficher votre base de règles de politique en fonction de ces étiquettes. Vous pouvez regrouper les règles en fonction d’une **Tag (Étiquette)**.
Commentaire d’audit		Saisissez un commentaire pour auditer la création ou la modification d’une règle de politique. Le commentaire d’audit est sensible à la casse et peut comporter jusqu’à 256 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d’union et des traits de soulignement.
Archive des commentaires d’audit		Afficher les **Audit Comments (Commentaires d’audit)** précédents pour la règle de politique. Vous pouvez exporter l’archive des commentaires d’audit au format CSV.
Zone source	**Source**	Veuillez **Ajouter** une ou plusieurs zones sources de paquets auxquelles s’applique la politique d’Inspection des tunnels (la valeur par défaut est **Any (Indifférent)**).
Adresse source		(Facultatif) Veuillez **Ajouter** les adresses sources IPv4 ou IPv6, les groupes d’adresses ou les objets d’adresse de la Région géographique des paquets auxquels

Blocs de construction dans une politique d'inspection des tunnels	Configuré dans	Description
		s'applique la politique d'Inspection des tunnels (la valeur par défaut est **toute**).
Utilisateur source		(Facultatif) Veuillez **Ajouter** les utilisateurs sources de paquets auxquels s'applique la politique d'Inspection des tunnels (la valeur par défaut est **toute**).
Inverser		(Facultatif) Sélectionnez **Inverser** pour choisir n'importe quelle adresse sauf celles étant spécifiées.
Zone de destination	**Destination**	Veuillez **Ajouter** une ou plusieurs zones de destination de paquets auxquelles s'applique la politique d'Inspection des tunnels (la valeur par défaut est **tout**).
Adresse de destination		(Facultatif) Veuillez **Ajouter** les adresses de destination IPv4 ou IPv6, les groupes d'adresses ou les objets d'adresse de la Région géographique des paquets auxquels s'applique la politique d'Inspection des tunnels (la valeur par défaut est **tout**).
Inverser		(Facultatif) Sélectionnez **Inverser** pour choisir n'importe quelle adresse sauf celles étant spécifiées.
Protocole de tunnel	**Inspection**	Veuillez **Add (Ajouter)** un ou plusieurs **Protocols (Protocoles)** de tunnels que vous souhaitez que le pare-feu inspecte : • **GRE** – Le pare-feu inspecte les paquets qui utilisent l'Encapsulation générique de routage dans le tunnel. • **GTP-U** – Le pare-feu inspecte les paquets qui utilisent le protocole de tunnellisation (service général de radiocommunication par paquets ; GPRS) dans le tunnel. • **IPSec non chiffré)** – Le pare-feu inspecte les paquets qui utilisent le protocole IPSec non chiffré (IPSec non chiffré ou mode de transport AH IPSec) dans le tunnel. • **VXLAN** – Le pare-feu inspecte la charge utile VXLAN pour déceler le contenu encapsulé ou les applications du tunnel. Pour supprimer un protocole de votre liste, sélectionnez-le et cliquez sur **Supprimer** pour le supprimer.

Blocs de construction dans une politique d'inspection des tunnels	Configuré dans	Description
Niveaux maximums d'inspection des tunnels	**Inspection** > **Options d'inspection**	Précisez si le pare-feu inspectera **Un niveau** (par défaut) ou **Deux niveaux (Un tunnel dans un tunnel)** d'encapsulation. Pour VXLAN, sélectionnez **Un niveau**, car l'inspection ne se produit que sur la couche externe.
Abandonner le paquet en cas de dépassement du niveau maximum d'inspection des tunnels		(Facultatif) Abandonnez les paquets qui contiennent plus de niveaux d'encapsulation que ceux indiqués pour les Niveaux maximums d'inspection des tunnels.
Abandonner le paquet en cas d'échec de la vérification stricte de l'en-tête pour le protocole de tunnel		(Facultatif) Abandonnez les paquets qui contiennent un protocole de tunnel qui utilise un en-tête qui n'est pas conforme au document RFC pour ce protocole. Les en-têtes non conformes indiquent des paquets suspects. Cette option permet au pare-feu de vérifier les en-têtes par rapport au document RFC 2890. *N'activez pas cette option si votre pare-feu met GRE en tunnel avec un périphérique qui met en œuvre une version de GRE plus ancienne que le document RFC 2890.*
Abandonner le paquet en cas de protocole inconnu dans le tunnel		(Facultatif) Abandonnez les paquets contenant un protocole dans le tunnel que le pare-feu ne parvient pas à identifier.
Retourner le tunnel VXLAN analysé vers la source		(Facultatif) Activez cette option pour retourner le trafic au point de terminaison du tunnel VXLAN(VTEP) d'origine. Par exemple, utilisez cette option pour retourner le paquet encapsulé au VTEP source. Pris en charge uniquement sur la couche 3, la sous-interface de couche 3, l'interface agrégée de couche 3 et VLAN.
Activer les options de sécurité	**Inspection** > **Options de sécurité**	(Facultatif) Veuillez **Activer les options de sécurité** pour affecter des zones de sécurité pour un traitement du contenu du tunnel par chaque politique de Sécurité. Le contenu source interne appartient à la **Tunnel Source Zone (Zone source du tunnel)** que vous indiquez et le contenu de destination interne appartient à la **Tunnel**

Blocs de construction dans une politique d’inspection des tunnels	Configuré dans	Description
		Destination Zone (Zone de destination du tunnel) que vous indiquez. Si vous n’effectuez pas l’action consistant à **Activer les options de sécurité**, le contenu source interne appartient par défaut à la même zone que la source extérieure du tunnel et le contenu de destination interne appartient à la même zone que la destination extérieure du tunnel. Par conséquent, tant le contenu source interne que le contenu de destination interne sont soumis aux mêmes politiques de Sécurité qui s’appliquent aux zones source et de destination du tunnel extérieur.
Zone source du tunnel		Si vous **Activer les options de sécurité**, sélectionnez une zone du tunnel que vous avez créée, et le contenu interne utilisera cette zone source pour l'application de la politique. Autrement, le contenu source interne appartient par défaut à la même zone que la source extérieure du tunnel et les politiques de la zone de la source extérieure du tunnel s’appliquent également à la zone de contenu source interne.
Zone de destination du tunnel		Si vous **Activer les options de sécurité**, sélectionnez une zone du tunnel que vous avez créée, et le contenu interne utilisera cette zone de destination pour l'application de la politique. Autrement, le contenu de destination interne appartient par défaut à la même zone que la destination extérieure du tunnel et les politiques de la zone de la destination extérieure du tunnel s’appliquent également à la zone de contenu de destination interne.
Nom de la surveillance	**Inspection** > **Options de surveillance**	(Facultatif) Saisissez un nom de surveillance pour regrouper le trafic similaire afin de surveiller le trafic dans les journaux et les rapports.
Balise de surveillance (numéro)		(Facultatif) Saisissez un numéro de balise de surveillance qui peut regrouper le trafic similaire pour la journalisation et la génération de rapports (plage de 1 à 16, 777, 215). Le numéro de l’étiquette est défini de manière globale.

Blocs de construction dans une politique d’inspection des tunnels	Configuré dans	Description
		Ce champ ne s'applique pas au protocole VXLAN. Les journaux VXLAN utilisent automatiquement l’Identificateur réseau VXLAN (VNI) dans l’en-tête VXLAN.
Se connecter au début de la session		(Facultatif) Sélectionnez cette option pour générer un journal au début de la session de tunnel de texte en clair qui correspond à la politique d’inspection des tunnels. Ce paramètre remplace le paramètre Se connecter au début de la session qui figure dans la règle de Politique de Sécurité qui s’applique à la session. Les journaux de tunnel sont stockés séparément des journaux de trafic. Les informations de la session de tunnel extérieur (GRE, protocole IPSec non chiffré ou GTP-U) sont stockées dans les journaux de tunnel et les flux de trafic intérieur, dans les journaux de trafic. Cette séparation permet de facilement faire état de l'activité du tunnel (par opposition à l'activité du contenu interne) avec l’ACC et ses fonctions de production de rapports. *Pour ce qui est des journaux de tunnel, il est recommandé de Journaliser au début de la session et de Journaliser en fin de la session, puisque, aux fins de la journalisation, les tunnels peuvent avoir une très longue durée de vie. Par exemple, les tunnels GRE peuvent être créés lors du démarrage du routeur pour prendre fin uniquement au redémarrage du routeur. Si vous ne sélectionnez pas Journaliser au début de la session, vous ne verrez jamais qu’il y a un tunnel GRE actif dans l’ACC.*
Se connecter en fin de session		(Facultatif) Sélectionnez cette option pour générer un journal en fin de session de tunnel de texte en clair qui correspond à la politique d’inspection des tunnels. Ce paramètre remplace le paramètre Journaliser en fin de session qui figure dans la règle de Politique de Sécurité qui s’applique à la session.

Blocs de construction dans une politique d’inspection des tunnels	Configuré dans	Description
Transfert des journaux		(Facultatif) Sélectionnez un profil de Transfert des journaux dans la liste déroulante pour préciser l’endroit où transférer les journaux d'inspection des tunnels. (Ce paramètre est distinct du paramètre de Transfert des journaux d’une règle de politique de Sécurité, qui s’applique aux journaux de trafic.)
Nom	**ID du tunnel** Par défaut, si vous ne configurez **pas** d’ID VXLAN, tout le trafic est inspecté. Si vous configurez un ID VXLAN, vous pouvez l’utiliser comme critère de correspondance pour restreindre l’inspection du trafic à des VNI précis.	(Facultatif) Un nom commence par un caractère alphanumérique et pouvant contenir des zéros ou d’autres caractères alphanumériques, des traits de soulignement, des traits d’union, des points et des espaces. Le **Nom** décrit les VNI que vous regroupez. Le nom sert d’élément pratique, mais ne sert pas de facteur dans la journalisation, la surveillance ou l’établissement de rapports.
ID VXLAN (VNI)		(Facultatif) Saisissez un seul VNI, une liste de VNI séparés par des virgules, une plage d’un maximum de 16 millions de VNI (un tiret faisant office de séparateur), ou une combinaison de ces éléments. Par exemple : 1-54,1024,1677011-1677038,94 Le nombre maximal d’ID VXLAN par stratégie est de 4 096. Pour préserver la mémoire de configuration, utilisez les plages lorsque possible.
Tous (cible tous les périphériques) Panorama uniquement	**Cible**	Activez (cochez) pour valider la règle de politique de tous les pare-feux gérés du groupe de périphériques.
Périphériques Panorama uniquement		Sélectionnez un ou plusieurs pare-feux gérés associés au groupe de périphériques pour valider la règle de politique.
Étiquettes Panorama uniquement		**Add (Ajoutez)** une ou plusieurs étiquettes pour valider la règle de politique des pare-feux gérés dans le groupe de périphériques ayant l’étiquette indiquée.

Blocs de construction dans une politique d’inspection des tunnels	Configuré dans	Description
Cibler tous les périphériques sauf ceux spécifiés Panorama uniquement		Cochez pour valider la règle de politique pour tous les pare-feux gérés associés au groupe de périphériques sauf pour le(s) périphérique(s) et étiquette(s) sélectionnés.

Politiques > Contrôle prioritaire sur l'application

Pour modifier la manière dont le pare-feu classe le trafic réseau par application, vous pouvez définir des politiques de contrôle prioritaire sur l’application. Par exemple, si vous voulez contrôler l'une de vos applications personnalisées, une politique de contrôle prioritaire sur l'application peut être utilisée pour identifier le trafic pour cette application en fonction de la zone, de l'adresse source et de destination, du port et du protocole. Si certaines de vos applications réseau sont classées comme « inconnues », vous pouvez créer de nouvelles définitions d'application qui leur correspondent (reportez-vous à la section Définition des applications).

Si possible, évitez d’utiliser des politiques de contrôle prioritaire sur l’application, car elles empêchent le pare-feu d’utiliser App-ID pour identifier les applications et d'effectuer l'inspection de couche 7 pour y déceler des menaces. Pour soutenir les applications propriétaires internes, il est préférable de créer des applications personnalisées *qui incluent la signature d’application pour que le pare-feu effectue l’inspection de couche 7 et analyse le trafic d'applications pour y déceler des menaces. Si une application commerciale ne dispose pas d’un App-ID,* soumettez une demande de nouvel App-ID. *Si la définition d’une application publique (ports ou signature par défaut) change et que le pare-feu n’identifie plus correctement l’application, créez un billet d’assistance pour que Palo Alto Networks puisse mettre à jour la définition. Entre-temps, créez une application personnalisée pour que le pare-feu continue d’effectuer l'inspection de la couche 7 du trafic.*

Comme les politiques de sécurité, les politiques de contrôle prioritaire sur l'application peuvent avoir une portée générale ou spécifique, selon les besoins. Les règles des politiques sont comparées au trafic dans un ordre précis, donc les règles les plus spécifiques doivent précéder les règles plus générales.

Étant donné que le moteur App-ID de PAN-OS classe le trafic en identifiant le contenu spécifique aux applications dans le trafic réseau, les définitions d’application personnalisées ne peuvent se contenter d’utiliser un numéro de port comme identifiant. Elles doivent également inclure le trafic (restreint par zone source, adresse IP source, zone de destination et adresse IP de destination).

Pour créer une application personnalisée avec contrôle prioritaire sur l'application'A0;:

- Créer une application personnalisée (voir Définition des applications). Il n'est pas nécessaire de définir des signatures pour l'application si celle-ci est utilisée uniquement dans des règles de contrôle prioritaire sur l'application.
- Définissez une politique de contrôle prioritaire sur l'application qui précise quand l'application personnalisée doit être invoquée. En général, une politique inclut l'adresse IP du serveur exécutant l'application personnalisée et un ensemble limité d'adresses IP source ou une zone source.

Les tableaux suivants vous permettent de configurer une règle de contrôle prioritaire sur l'application.

- Onglet Général d’outre-passement sur l’application
- Onglet Source outre-passement d’une l’application
- Onglet outrepasser Destination sur l’application
- Onglet Application/ Protocole d’outrepasser l’application
- (Panorama uniquement) Onglet cible Outrepasser l’application

Vous souhaitez en savoir plus ?

Voir Utilisation des objets application dans une politique.

Onglet Général d’outre-passement sur l’application

Sélectionnez l'onglet **Général** pour définir un nom et une description pour la politique d’outre-passement sur l'application. Une étiquette peut également être configurée et vous permettre de trier ou de filtrer les politiques lorsqu'il en existe un grand nombre.

Champ	Description
Name (Nom)	Donnez un nom à la règle afin de l'identifier. Le nom est sensible à la casse et peut comporter jusqu’à 63 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d’union et des traits de soulignement. Le nom doit être unique sur un pare-feu et, dans Panorama, unique au sein de son groupe de périphériques et des groupes de périphériques anciens ou descendants.
Description	Saisissez une description de la règle (1024 caractères maximum).
Étiquette	Si vous avez besoin d’étiqueter la politique, cliquez sur **Ajouter** et indiquez l’étiquette. Une étiquette de politique est un mot-clé ou une expression qui vous permet de trier ou de filtrer les politiques. Cela est utile lorsque vous avez défini de nombreuses politiques et que vous souhaitez afficher celles qui sont identifiées par un mot-clé particulier. Par exemple, vous pouvez ajouter l'étiquette Trafic entrant vers la zone DMZ à certaines politiques de sécurité, les mots Déchiffrement et Aucun déchiffrement aux politiques de déchiffrement, ou utiliser le nom d'un centre de données spécifique pour les politiques associés à cet emplacement.
Regrouper des règles par étiquette	Saisissez une étiquette selon laquelle regrouper des règles de politique similaires. L’étiquette de groupe vous permet d'afficher votre base de règles de politique en fonction de ces étiquettes. Vous pouvez choisir de regrouper les règles en fonction d’une **Tag (Étiquette)**.
Commentaire d’audit	Saisissez un commentaire pour auditer la création ou la modification d’une règle de politique. Le commentaire d’audit est sensible aux majuscules et minuscules et peut comporter jusqu’à 256 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d’union et des traits de soulignement.
Archive des commentaires d’audit	Afficher les **Audit Comments (Commentaires d’audit)** précédents pour la règle de politique. L’archive des commentaires d'audit peut être exportée au format CSV.

Onglet Source outre-passement d’une l’application

Sélectionnez l'onglet **Source** pour définir la zone ou l'adresse source qui définit le trafic source entrant auquel la politique d’outre-passement sur l'application est appliquée.

Champ	Description
Zone source	Il faut **Ajouter** des zones source (la valeur par défaut est **n’importe laquelle**). Les zones doivent être du même type (couche 2, couche 3 ou câble virtuel). Pour définir de nouvelles zones, reportez-vous à la section Réseau > Zones. Il est possible d'utiliser plusieurs zones pour simplifier la gestion. Par exemple, si vous possédez trois zones internes différentes (marketing, ventes et relations publiques) qui sont toutes reliées à la zone de destination non approuvée, vous pouvez créer une règle qui couvre tous les cas possibles.
Adresse source	Cliquez sur **Ajouter** des adresses, des groupes d’adresses ou des régions source (la valeur par défaut est **indifférent**). Faites votre sélection dans la liste déroulante ou cliquez sur **Adresse**, **Groupe d'adresses** ou **Régions** en bas de la liste déroulante et définissez les paramètres. Sélectionnez **inverser** pour choisir n'importe quelle adresse sauf celles configurées.

Onglet outrepasser Destination sur l’application

Sélectionnez l’onglet **Destination** pour définir la zone ou l’adresse de destination qui définit le trafic de destination auquel la politique sera appliquée.

Champ	Description
Zone de destination	Cliquez sur **Ajouter** pour choisir des zones de destination (valeur par défaut : indifférent). Les zones doivent être du même type (couche 2, couche 3 ou câble virtuel). Pour définir de nouvelles zones, reportez-vous à la section Réseau > Zones. Il est possible d'utiliser plusieurs zones pour simplifier la gestion. Par exemple, si vous possédez trois zones internes différentes (marketing, ventes et relations publiques) qui sont toutes reliées à la zone de destination non approuvée, vous pouvez créer une règle qui couvre tous les cas possibles.
Adresse de destination	Cliquez sur **Ajouter** pour ajouter des adresses, des groupes d'adresses ou des régions de destination (valeur par défaut : indifférent). Faites votre sélection dans la liste déroulante ou

Champ	Description
	cliquez sur **Adresse**, **Groupe d'adresses** ou **Régions** en bas de la liste déroulante et définissez les paramètres. Sélectionnez **inverser** pour choisir n'importe quelle adresse sauf celles configurées.

Onglet Application/ Protocole d’outrepasser l’application

Sélectionnez l'onglet **Protocole/Application** pour définir le protocole (TCP ou UDP), le port et l'application qui précisent les attributs de l'application correspondants à la politique.

Champ	Description
Protocole	Sélectionnez le protocole (**TCP** ou **UDP**) pour lequel autoriser le contrôle prioritaire sur l’application.
Port	Saisissez le numéro de port (de 0 à 65535) ou la plage de numéros de ports (port1-port2) pour les adresses de destination définies. Utilisez des virgules pour séparer les ports ou les plages.
Application	Sélectionnez l'application contrôle prioritaire pour les flux de trafic qui remplissent les critères de la règle. Lors du contrôle prioritaire d'une application personnalisée, aucune inspection des menaces n'est effectuée, sauf si l’outre-passement porte sur une application prédéfinie qui prend en charge l'inspection des menaces. Pour définir de nouvelles applications, reportez-vous à la section Objets > Applications.

Onglet cible Outrepasser l’application

- (Panorama uniquement) **Policies (Politiques)** > **outrepasser l'application** > **Cible**

Sélectionnez l’onglet **Cible** pour sélectionner les pare-feux gérés du groupe de périphériques auxquels appliqués la règle de politique. Vous pouvez préciser à quels pare-feux gérés appliquer en sélectionnant les pare-feux gérés ou en attribuant une étiquette. De plus, vous pouvez configurer la cible de la règle de politique à appliquer à tous les pare-feux gérés sauf ceux indiqués.

Règle NAT - Paramètres de la cible	Description
Tous (cible tous les périphériques)	Activez (cochez) pour valider la règle de politique de tous les pare-feux gérés du groupe de périphériques.

Règle NAT - Paramètres de la cible	Description
Périphériques	Sélectionnez un ou plusieurs pare-feux gérés associés au groupe de périphériques pour valider la règle de politique.
Étiquettes	**Add (Ajoutez)** une ou plusieurs étiquettes pour valider la règle de politique des pare-feux gérés dans le groupe de périphériques ayant l'étiquette indiquée.
Cibler tous les périphériques sauf ceux spécifiés	Activez (cochez) pour valider la règle de politique pour tous les pare-feux gérés associés au groupe de périphériques sauf pour le(s) périphérique(s) et étiquette(s) sélectionnés.

Politiques > Authentification

Votre politique d'Authentification vous permet d'authentifier les utilisateurs finaux avant qu'ils puissent accéder aux ressources du réseau.

Que voulez-vous savoir ?	Reportez-vous à la section :
Quels sont les champs disponibles pour créer une règle d'Authentification ?	Blocs de construction d'une règle de politique d'authentification
Comment puis-je utiliser l'interface Web pour gérer les politiques d'Authentification ?	Créer et gérer la politique d'authentification Pour Panorama, reportez-vous à Déplacer ou cloner une règle de stratégie
Vous souhaitez en savoir plus ?	Politique d'authentification

Blocs de construction d'une règle de politique d'authentification

Chaque fois qu'un utilisateur demande une ressource (par exemple lorsqu'il se rend sur une page Web), le pare-feu évalue la politique d'Authentification. En fonction de la règle de la politique de correspondance, le pare-feu invite alors l'utilisateur à répondre à une ou plusieurs demandes provenant de divers facteurs (types), comme la connexion et le mot de passe, la voix, le SMS, la fonction push ou l'authentification du mot de passe à usage unique (OTP). Une fois que l'utilisateur répond à tous les facteurs, le pare-feu évalue la politique de Sécurité (voir Politiques > Sécurité) pour déterminer s'il faut autoriser l'accès à la ressource.

Le pare-feu n'invite pas les utilisateurs à s'authentifier s'ils ont accès à des ressources non basées sur le Web (comme une imprimante) par le biais d'une passerelle GlobalProtect™, c'est-à-dire en mode interne ou en mode tunnel. Au lieu de cela, les utilisateurs voient des messages indiquant l'échec de connexion. Pour s'assurer que les utilisateurs peuvent accéder à ces ressources, configurez un portail d'authentification et formez les utilisateurs à le consulter lorsqu'ils remarquent des échecs de connexion. Consultez votre service informatique pour configurer un portail d'authentification.

La table suivante décrit chaque bloc de construction ou composant d'une règle de politique d'Authentification. Avant d'Ajouter une règle, exécutez les tâches préalables décrites dans Créer et gérer la politique d'authentification.

Blocs de construction dans une règle d'authentificatio	Configuré dans	Description
Numéro de règle	N/A	Chaque règle est automatiquement numérotée et son ordre change à mesure que les règles sont déplacées. Lorsque vous filtrez des règles pour qu'elles correspondent à des filtres spécifiques, la page des **Politiques** > **Authentification** répertorie chaque règle avec son numéro dans le contexte de l'ensemble des règles de la base de règles et sa position dans l'ordre d'évaluation. Pour plus d'information, reportez-vous à la section séquence de règles et son ordre d'évaluation
Nom	**Général**	Donnez un nom à la règle afin de l'identifier. Le nom est sensible à la casse et peut comporter jusqu'à 63 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement. Le nom doit être unique sur un pare-feu et, dans Panorama, unique au sein de son groupe de périphériques et des groupes de périphériques anciens ou descendants.
Description		Saisissez une description de la règle (1024 caractères maximum).
Étiquette		Sélectionnez une étiquette pour trier et filtrer les règles (voir Objets > Étiquettes).
Regrouper des règles par étiquette		Saisissez une étiquette selon laquelle regrouper des règles de politique similaires. L'étiquette de groupe vous permet d'afficher votre base de règles de politique en fonction de ces étiquettes. Vous pouvez regrouper les règles en fonction d'une **Tag (Étiquette)**.
Commentaire d'audit		Saisissez un commentaire pour auditer la création ou la modification d'une règle de politique. Le commentaire d'audit est sensible à la casse et peut comporter jusqu'à 256 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement.
Archive des commentaires d'audit		Afficher les **Audit Comments (Commentaires d'audit)** précédents pour la règle de politique. Vous pouvez exporter l'archive des commentaires d'audit au format CSV.

Blocs de construction dans une règle d'authentificatio	Configuré dans	Description
Zone source	**Source**	Veuillez **Ajouter** des zones pour appliquer la règle uniquement au trafic provenant des interfaces dans les zones que vous indiquez (la valeur par défaut est **toute**). Pour définir de nouvelles zones, voir Réseau > Zones.
Adresse source		Veuillez **Ajouter** les adresses ou les groupes d'adresses pour appliquer la règle uniquement au trafic provenant des sources que vous indiquez (la valeur par défaut est **toute**). Sélectionnez **inverse** pour choisir n'importe quelle adresse sauf celles qui sont sélectionnées. Pour définir de nouvelles adresses ou de nouveaux groupes d'adresses, voir Objets > Adresses et Objets > Groupes d'adresses.
Utilisateur source	**Utilisateur**	Sélectionnez les utilisateurs sources ou les groupes d'utilisateurs auxquels s'applique la règle : • **tout** – Inclut tout trafic, quel que soit l'utilisateur source. • **préouverture de session** – Inclut les utilisateurs distants qui ne sont pas connectés à leurs systèmes client, mais dont les systèmes client se connectent au réseau par le biais de la fonctionnalité de préouverture de session GlobalProtect • **utilisateur connu** – Inclut tous les utilisateurs pour lesquels le pare-feu possède déjà des mappages adresse IP / nom d'utilisateur avant que la règle évoque l'authentification. • **inconnu** – Inclut tous les utilisateurs pour lesquels le pare-feu ne dispose pas de mappages adresse IP / nom d'utilisateur. Une fois que la règle évoque l'authentification, le pare-feu crée des mappages d'utilisateurs pour les utilisateurs inconnus en fonction des noms d'utilisateur qu'ils ont saisis. • **Sélectionner** – Inclut uniquement les utilisateurs et les groupes d'utilisateurs que vous avez décidé d'**Ajouter** à la liste Utilisateur source.

Blocs de construction dans une règle d'authentificatio	Configuré dans	Description
		Si le pare-feu collecte les informations utilisateur depuis un serveur RADIUS, TACACS+ ou le serveur du fournisseur d'identité SAML et non depuis l'agent User-ID™, la liste des utilisateurs ne s'affiche pas ; vous devez saisir les informations de l'utilisateur manuellement.
Profil HIP source		**Ajouter** des profils HIP (profils d'informations sur l'hôte) vous permet de collecter des informations sur l'état de sécurité de vos hôtes, à savoir s'ils ont installé les derniers correctifs de sécurité et les dernières définitions antivirus. Pour plus d'informations et pour définir de nouveaux profils HIP, voir Objets > GlobalProtect > Profils HIP.
Zone de destination	**Destination**	Veuillez **Ajouter** des zones pour appliquer la règle uniquement au trafic à destination des interfaces dans les zones que vous indiquez (la valeur par défaut est **toute**). Pour définir de nouvelles zones, voir Réseau > Zones.
Adresse de destination		Veuillez **Ajouter** les adresses ou les groupes d'adresses pour appliquer la règle uniquement aux destinations que vous indiquez (la valeur par défaut est **toute**). Sélectionnez **inverse** pour choisir n'importe quelle adresse sauf celles qui sont sélectionnées. Pour définir de nouvelles adresses ou de nouveaux groupes d'adresses, voir Objets > Adresses et Objets > Groupes d'adresses.
Service	**Catégorie de service/ URL**	Choisissez une option parmi les options suivantes pour appliquer la règle uniquement aux services sur les numéros de ports TCP et UDP spécifiques : • **Tout** – Indique les services sur n'importe quel port utilisant n'importe quel protocole. • **par défaut** – Indique les services uniquement sur les ports par défaut définis par Palo Alto Networks. • **Sélectionner** – Vous permet d'**Ajouter** des services ou des groupes de services. Pour créer de nouveaux

Blocs de construction dans une règle d'authentificatio	Configuré dans	Description
		services et de nouveaux groupes de services, voir Objets > Services et Objets > Groupes de services. *La sélection par défaut est **service-http**. Lorsque vous utilisez la politique d'authentification pour le portail d'authentification, activez également **service-https** pour veiller à ce que le pare-feu découvre le mappage utilisateur/adresse ip pour tout le trafic Web.*
Catégorie d'URL		Sélectionnez les catégories d'URL auxquelles la règle s'applique : • Sélectionnez **tout** pour indiquer tout le trafic indépendamment de la catégorie d'URL. • Vous devez **Ajouter** des catégories. Pour définir des catégories personnalisées, voir Objets > Objets personnalisés > Catégorie d'URL.
Application de l'authentification	**Actions**	Sélectionnez l'objet d'application de l'authentification (Objets > Authentification) qui indique la méthode (comme le portail d'authentification ou le défi de navigation) et le profil d'authentification que le pare-feu utilise pour authentifier les utilisateurs. Le profil d'authentification définit si les utilisateurs répondent à une seul demande d'authentification ou à une authentification multifacteur (voir Périphérique > Profil d'authentification). Vous pouvez sélectionner un objet d'application d'authentification prédéfini ou personnalisé. *Si vous devez exclure des hôtes ou des serveurs d'une politique de portail d'authentification, ajoutez-les à un profil d'authentification qui spécifie **aucun portail captif** en tant que **Application de l'authentification**. Cependant, les politiques du portail d'authentification aident le pare-feu à découvrir le mappage utilisateur/adresse IP. On devrait les utiliser lorsque possible.*

Blocs de construction dans une règle d’authentificatio	Configuré dans	Description
délai d'expiration		Pour réduire la fréquence des demandes d’authentification qui interrompent le flux de travail de l’utilisateur, vous pouvez indiquer l’intervalle en minutes (60 étant la valeur par défaut) auquel le pare-feu invite l’utilisateur à s’authentifier une seule fois pour un accès répété aux ressources. Si l’objet de l’**Application de l’authentification** indique l’authentification multi-facteur, l’utilisateur doit s’authentifier une fois pour chaque facteur. Le pare-feu enregistre un horodatage et republie une demande uniquement lorsque le délai d’expiration d’un facteur expire. La Redistribution des horodatages vers d’autres pare-feu vous permet d’appliquer le délai d’expiration même si le pare-feu qui autorise initialement l’accès à un utilisateur n’est pas le même pare-feu qui contrôle ultérieurement l’accès pour cet utilisateur.

Blocs de construction dans une règle d'authentificatio	Configuré dans	Description
		*Le **Délai d'expiration** est un compromis entre une sécurité plus stricte (période plus courte entre les invites d'authentification) et l'expérience utilisateur (période plus longue entre les invites d'authentification). Une authentification plus fréquente est souvent le choix le plus indiqué pour accéder aux systèmes critiques et aux zones sensibles, comme un centre de données. Une authentification moins fréquente est souvent indiquée au périmètre du réseau de même que pour les entreprises pour lesquelles l'expérience utilisateur est clé.* *Définissez la valeur des ressources du périmètre sur 480 minutes (8 heures) et définissez une valeur plus faible, comme 60 minutes, pour les ressources du centre de données et les systèmes critiques pour renforcer la sécurité. Surveillez et ajustez les valeurs, au besoin.*
Délais d'authentification des journaux		Sélectionnez cette option (désactivée par défaut) si vous souhaitez que le pare-feu génère des journaux d'Authentification chaque fois que le **Délai d'expiration** associé à un facteur d'authentification expire. L'activation de cette option fournit plus de données pour résoudre les problèmes d'accès. En conjonction avec les objets de corrélation, vous pouvez également utiliser les journaux d'Authentification pour identifier l'activité suspecte sur votre réseau (comme les attaques par force brute). *L'activation de cette option augmente le trafic de journaux.*
Transfert des journaux		Sélectionnez un profil de Transfert des journaux si vous souhaitez que le pare-feu transfère des journaux d'Authentification à Panorama ou à des services

Blocs de construction dans une règle d'authentificatio	Configuré dans	Description
		externes comme un serveur Syslog (voir Objets > Transfert de journaux).
Tous (cible tous les périphériques) Panorama uniquement	**Cible**	Activez (cochez) pour valider la règle de politique de tous les pare-feux gérés du groupe de périphériques.
Périphériques Panorama uniquement		Sélectionnez un ou plusieurs pare-feux gérés associés au groupe de périphériques pour valider la règle de politique.
Étiquettes Panorama uniquement		**Add (Ajoutez)** une ou plusieurs étiquettes pour valider la règle de politique des pare-feux gérés dans le groupe de périphériques ayant l'étiquette indiquée.
Cibler tous les périphériques sauf ceux spécifiés Panorama uniquement		Cochez pour valider la règle de politique pour tous les pare-feux gérés associés au groupe de périphériques sauf pour le(s) périphérique(s) et étiquette(s) sélectionnés.

Créer et gérer la politique d'authentification

Sélectionnez la page **Politiques** > **Authentification** pour créer et gérer les règles de la politique d'Authentification :

Tâche	Description
Ajouter	Effectuez les tâches préalables suivantes avant de créer les règles de la politique d'Authentification : ❑ Configurez les paramètres du Portail d'authentification User-ID™ (voir Périphérique > Identification de l'utilisateur > Paramètres du d'authentification). Le pare-feu utilise le Portail d'authentification pour afficher le premier facteur d'authentification requis par la règle d'Authentification. Le Portail d'authentification permet également au pare-feu d'enregistrer l'horodatage associé aux délais d'expiration d'authentification et de mettre à jour les mappages d'utilisateurs.

Tâche	Description
	❑ Configurez un profil de serveur qui précise la manière dont le pare-feu peut accéder au service qui authentifiera les utilisateurs (se reporter à la section Périphérique > Profils de serveur). ❑ Affectez le profil de serveur à un profil d'authentification qui indique les paramètres d'authentification (voir Périphérique > Profil d'authentification). ❑ Affectez le profil d'authentification à un objet d'application d'authentification qui indique le mode d'authentification (voir Objets > Authentification). Pour créer une règle, effectuez l'une des étapes suivantes, puis renseignez les champs décrits dans Blocs de construction d'une règle de politique d'authentification : • Cliquez sur **Ajouter**. • Sélectionnez une règle sur laquelle baser la nouvelle règle et cliquez sur **Cloner la règle**. Le pare-feu insère la règle copiée, appelée <rulename># sous la règle sélectionnée, où « # » représente le premier nombre entier disponible qui caractérise le nom de la règle et génère un nouvel UUID pour la règle clonée. Pour plus d'informations, reportez-vous à la section Déplacement ou clonage d'une règle de politique.
Modifier	Pour modifier une règle, cliquez sur la règle Nom et modifiez les champs décrits dans Blocs de construction d'une règle de politique d'authentification. *Si le pare-feu a reçu la règle de Panorama, la règle est en lecture seule ; vous ne pouvez l'éditer que sur Panorama.*
Se déplacer	Lors de la correspondance du trafic, le pare-feu évalue les règles de haut en bas dans l'ordre dans lequel la page **Politiques** > **Authentification** les répertorie. Pour modifier l'ordre d'évaluation, sélectionnez une règle et cliquez sur **Déplacer en haut**, **Déplacer en bas**, **Déplacer vers le haut** ou **Déplacer vers le bas**. Pour plus d'informations, reportez-vous à la section Déplacement ou clonage d'une règle de politique.
Supprimer	Pour supprimer une règle existante, vous devez la sélectionner et l'**Effacer**.
Activer/ désactiver	Pour désactiver une règle, vous devez la sélectionner et la **Désactiver**. Pour réactiver une règle désactivée, vous devez la sélectionner et l'**Activer**.
Surligner les règles inutilisées	Pour identifier les règles qui n'ont pas correspondu au trafic depuis le dernier redémarrage du pare-feu, sélectionnez **Surligner les règles inutilisées**. Vous pourrez ensuite décider de désactiver ou de supprimer les règles inutilisées. La page met en évidence les règles inutilisées sur un arrière-plan jaune pointillé.
Prévisualiser les règles (Panorama uniquement)	Cliquez sur l'option **Prévisualiser les règles** pour afficher une liste des règles avant de les appliquer sur les pare-feu gérés. Dans chaque base de règles, la page délimite visuellement la hiérarchie des règles pour chaque groupe de périphériques (et pare-feu géré) pour faciliter la numérisation de nombreuses règles.

Politiques > Protection DoS

Une politique de Protection DoS vous permet de protéger les ressources critiques individuelles contre les attaques DoS en spécifiant s'il faut refuser ou autoriser les paquets qui correspondent à une interface, une zone, une adresse ou un utilisateur source et/ou une interface, une zone ou un utilisateur de destination.

Vous pouvez également choisir l'action de Protection et spécifier un profil DoS où vous définissez les seuils (sessions ou paquets par seconde) qui déclenchent une alarme, activent une mesure de protection et indiquent le taux maximum au-dessus duquel toutes les nouvelles connexions sont abandonnées. Ainsi, vous pouvez contrôler le nombre de sessions entre des interfaces, des zones, des adresses et des pays en vous basant sur des sessions ou des adresses IP source et/ou de destination agrégées. Par exemple, vous pouvez contrôler le trafic depuis et vers certaines adresses ou groupes d'adresses, de certains utilisateurs et pour certains services.

Le pare-feu applique les règles de la politique de Protection DoS avant les règles de politique de Sécurité afin de s'assurer que le pare-feu utilise ses ressources de la manière la plus efficace. Si une règle de politique de Protection DoS refuse un paquet, ce paquet n'atteint jamais de règle de politique de Sécurité.

Les tableaux suivants décrivent les paramètres des politiques de Protection DoS :

- Onglet Général de protection DoS ;
- Onglet Source de protection DoS
- Onglet Destination de protection DoS
- Onglet Option / Protection de protection DoS.
- (Panorama uniquement) Onglet cible de protection DoS

Vous souhaitez en savoir plus ?

Voir Profils de protection DoS et Objets > Profils de sécurité > Protection DoS.

Onglet Général de protection DoS ;

- **Politiques** > **Protection DoS** > **Général**

Sélectionnez l'onglet **Général** pour configurer un nom et une description pour la politique de Protection DoS. Vous pouvez également configurer une étiquette afin de pouvoir trier ou filtrer les politiques lorsqu'il en existe un grand nombre.

Champ	Description
Name (Nom)	Saisissez un nom pour identifier la règle de politique de Protection DoS. Le nom est sensible à la casse et peut comporter jusqu'à 63 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement. Le nom doit être unique sur un pare-feu et, dans Panorama, unique au sein de son groupe de périphériques et des groupes de périphériques anciens ou descendants.
Description	Saisissez une description de la règle (1024 caractères maximum).
Étiquettes	Si vous avez voulez étiqueter la politique, cliquez sur **Ajouter** et indiquer l'étiquette.

Champ	Description
	Une étiquette de politique est un mot-clé ou une expression qui vous permet de trier ou de filtrer les politiques. Une étiquette est utile lorsque vous avez défini de nombreuses politiques et que vous souhaitez afficher celles qui sont identifiées par un mot-clé particulier. Par exemple, il se peut que vous souhaitiez ajouter une étiquette Trafic entrant vers la zone DMZ à certaines politiques de sécurité, ajouter une étiquette avec les mots Déchiffrement ou Aucun déchiffrement aux politiques de déchiffrement ou utiliser le nom d'un centre de données spécifique pour les politiques associées à cet emplacement.
Regrouper des règles par étiquette	Saisissez une étiquette selon laquelle regrouper des règles de politique similaires. L'étiquette de groupe vous permet d'afficher votre base de règles de politique en fonction de ces étiquettes. Vous pouvez regrouper les règles en fonction d'une **Tag (Étiquette)**.
Commentaire d'audit	Saisissez un commentaire pour auditer la création ou la modification d'une règle de politique. Le commentaire d'audit est sensible à la casse et peut comporter jusqu'à 256 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement.
Archive des commentaires d'audit	Afficher les **Audit Comments (Commentaires d'audit)** précédents pour la règle de politique. Vous pouvez exporter l'archive des commentaires d'audit au format CSV.

Onglet Source de protection DoS ;

Sélectionnez l'onglet **Source** pour définir l'interface ou les interfaces source ou la/les zone(s) source, et éventuellement l'adresse ou les adresses source et le/les utilisateurs source qui définissent le trafic entrant auquel s'applique la règle de la politique DoS.

Champ	Description
Type	Sélectionnez le type de source à laquelle s'applique la règle de politique de Protection DoS : • **Interface** – Appliquez la règle au trafic en provenance de l'interface spécifiée ou du groupe d'interfaces spécifié. • **Zone** – Applique la règle au trafic provenant de n'importe quelle interface dans une zone spécifiée. Cliquez sur **Ajouter** pour sélectionner plusieurs interfaces ou zones.
Source Address (Adresse source)	Sélectionnez **Tout** ou **Ajouter** et spécifiez une ou plusieurs adresses sources auxquelles s'applique la règle de politique de Protection DoS. (Facultatif) Sélectionnez **Refuser** pour spécifier que la règle s'applique à toutes les adresses, à l'exception de celles qui sont spécifiées.

Champ	Description
Source User (Utilisateur source)	Spécifiez un ou plusieurs utilisateurs source auxquels s'applique la règle de la politique de Protection DoS : • **Tout** – Inclut les paquets sans tenir compte de l'utilisateur source. • **Pré-ouverture de session** – Inclut les paquets provenant des utilisateurs distants connectés au réseau à l'aide de GlobalProtect, mais qui ne sont pas connectés à leur système. Lorsque l'option **pre-logon (pré-ouverture de session)** est configurée sur le Portail des applications GlobalProtect, tout utilisateur actuellement non connecté à sa machine est identifié avec la pré-ouverture de session avec le nom d'utilisateur. Vous pouvez ensuite créer des politiques pour les utilisateurs en pré-ouverture de session. Bien que l'utilisateur ne soit pas directement connecté, sa machine est authentifiée sur le domaine, comme s'il était complètement connecté. • **Utilisateur connu** – Inclut tous les utilisateurs authentifiés, c'est-à-dire toute adresse IP dont les données utilisateur sont mappées. Cette option est équivalente au groupe « utilisateurs » du domaine sur un domaine. • **unknown (inconnu)** - Inclut tous les utilisateurs non authentifiés, c'est-à-dire les adresses IP non mappées à un utilisateur. Par exemple, vous pouvez utiliser l'option **Inconnu** pour accéder à quelque chose au niveau invité, car les invités ont une adresse IP sur votre réseau, mais ne sont pas authentifiés sur le domaine et ne disposent d'aucune information de mappage nom d'utilisateur/adresse IP sur le pare-feu. • **Sélectionner** – Inclut les utilisateurs spécifiés dans cette fenêtre. Par exemple, vous pouvez sélectionner un utilisateur, une liste d'individus, certains groupes ou des utilisateurs manuellement. *Si le pare-feu collecte les informations utilisateur depuis un serveur RADIUS, TACACS+ ou le serveur du fournisseur d'identité SAML et non depuis l'agent User-ID™, la liste des utilisateurs ne s'affiche pas ; vous devez saisir les informations de l'utilisateur manuellement.*

Onglet Destination de protection DoS ;

Sélectionnez l'onglet **Destination** pour définir la zone ou l'interface et l'adresse de destination qui définissent le trafic de destination auquel la politique s'applique.

Champ	Description
Type	Sélectionnez le type de destination auquel s'applique la règle de politique de protection DoS : • **Interface** – Appliquez la règle aux paquets destinés à l'interface spécifiée ou au groupe d'interfaces spécifié. Cliquez sur **Ajouter** et sélectionnez une ou plusieurs interfaces.

Champ	Description
	• **Zone** – Appliquez la règle aux paquets destinés à n'importe quelle interface de la zone spécifiée. Cliquez sur **Ajouter** et sélectionnez une ou plusieurs zones.
Adresse de destination	Sélectionnez **Tout** ou **Ajouter** et spécifiez une ou plusieurs adresses de destination auxquelles s'applique la règle de politique de Protection DoS. (Facultatif) Sélectionnez **Refuser** pour spécifier que la règle s'applique à toutes les adresses, à l'exception de celles qui sont spécifiées.

Onglet Option / Protection de protection DoS.

Sélectionnez l'onglet **Option/Protection (Option/protection)** pour configurer des options pour la règle de politique de Protection DoS, notamment le type de service auquel la règle s'applique, l'action à effectuer par rapport aux paquets qui correspondent à la règle et le déclenchement ou non du transfert des journaux pour le trafic correspondant. Vous pouvez définir un calendrier afin d'indiquer quand la règle est active.

Vous pouvez également sélectionner un Profil de protection DoS agrégé et/ou un Profil de protection DoS classé qui déterminent les taux de seuils qui, lorsqu'ils sont dépassés, incitent le pare-feu à prendre des mesures de protection, comme déclencher une alarme, activer une action telle que Random Early Drop, et supprimer les paquets qui dépassent le taux de seuil maximal.

Champ	Description
Service (Service)	Cliquez sur **Ajouter** et sélectionnez un ou plusieurs services auxquels s'applique la politique de Protection DoS. La valeur par défaut est **Tout** service. Par exemple, si la politique DoS protège les serveurs Web, spécifiez HTTP, HTTPS et les autres ports de service appropriés pour les applications Web.  *Pour les serveurs critiques, créez des règles de protection DoS distinctes pour protéger les ports de service non utilisés afin d'empêcher les attaques ciblées.*
Action (Action)	Sélectionnez l'action que le pare-feu effectue sur les paquets qui correspondent à la règle de la politique de Protection DoS : • **Refuser** – Désélectionnez tous les paquets qui correspondent à la règle. • **Autoriser** – Autorisez tous les paquets qui correspondent à la règle. • **Protect (Protéger)** – Appliquez les protections précisées dans le profil de protection DoS aux paquets qui correspondre à la règle. Les paquets qui correspondent à la règle sont comptabilisés en fonction des taux de seuil dans le profil de Protection DoS qui, à son tour, déclenche une alarme, active une autre action et déclenche des suppressions de paquets lorsque le taux maximal est dépassé.

Champ	Description
	*L'application de la protection DoS vise à vous protéger des attaques DoS. Vous devriez donc normalement utiliser l'option **Protect (Protéger)**. **Deny (Refuser)** abandonne le trafic légitime et le trafic DoS et **Allow (Autoriser)** n'arrête pas les attaques DoS. Utilisez **Deny (Refuser)** et **Allow (Autoriser)** uniquement pour faire des exceptions au sein d'un groupe. Par exemple, vous pouvez refuser le trafic provenant de la plupart des groupes, mais autoriser un sous-réseau de ce trafic, ou autoriser le trafic provenant de la plupart des groupes, mais refuser un sous-réseau de ce trafic.*
Programmer	Spécifiez le calendrier durant lequel la règle de la politique de protection DoS est en vigueur. Le paramètre par défaut **Aucun** indique l'absence de calendrier ; la politique est toujours en vigueur. Autrement, sélectionnez un calendrier ou créez un nouveau calendrier pour contrôler le moment où la règle de la politique de Protection DoS est en vigueur. Saisissez un **Nom** pour identifier le calendrier. Sélectionnez **Partagé** pour partager ce calendrier avec chaque système virtuel d'un pare-feu à plusieurs systèmes virtuels. Sélectionnez une **Récurrence** parmi **Quotidien**, **Hebdomadaire**, ou **Non récurrent**. Ajoutez une **Heure de début** et une **Heure de fin** dans heures:minutes, en fonction d'une horloge de 24 heures.
Transfert des journaux	Si vous souhaitez déclencher le transfert des entrées du journal des menaces pour le trafic correspondant vers un service externe, comme un serveur Syslog ou Panorama, sélectionnez un profil de Transfert des journaux ou cliquez sur **Profil** pour en créer un nouveau. *Le pare-feu journalise et transfère uniquement le trafic qui correspond à une action de la règle.* *Pour faciliter la gestion, transférez les journaux DoS séparément des autres journaux des menaces. Transmettez-les tous deux directement aux* administrateurs par e-mail et à serveur de journaux.
Agréger	Les profils de protection DoS agrégés définissent les seuils qui s'appliquent au groupe combiné de périphériques précisés dans la règle de protection DoS pour protéger ces groupes de serveur. Par exemple, si vous définissez un seuil de taux d'alarme de 10 000 CPS, cela signifie que lorsque le nouveau CPS total de l'ensemble du groupe dépasse 10 000 CPS, le pare-feu déclenche un message d'alarme. Sélectionne un profil de protection DoS agrégé qui spécifie les taux de seuil auxquels les connexions entrantes par seconde déclenchent une alarme, activent une action et dépassent un taux maximal. Toutes les connexions entrantes (agrégé) sont prises en compte dans les seuils spécifiés dans un profil de protection DoS agrégé. Le paramètre de profil agrégé **Aucun** signifie qu'il n'y a pas de paramètres de seuil en place pour le trafic agrégé. Voir Objets > Profils de sécurité > Protection DoS.

Champ	Description
Classés	Les profils de protection DoS classés définissent les seuils qui s'appliquent à chaque périphérique individuel précisé dans la règle de protection DoS pour protéger des serveurs critiques individuel ou de petits groupes de serveurs critiques. Par exemple, si vous définissez un seuil de taux d'alarme de 10 000 CPS, cela signifie que lorsque le nouveau CPS total d'un serveur individuel précisé dans la règle dépasse 10 000 CPS, le pare-feu déclenche un message d'alarme. Sélectionnez cette option et indiquez les éléments suivants : • **Profil** – Sélectionnez un profil de protection DoS classé pour appliquer cette règle. • **Adresse** – Choisissez si les connexions entrantes sont prises en compte pour les seuils du profil si elles correspondent **uniquement à l'IP source**, **uniquement à l'IP de destination**, ou **à la fois à l'IP source et à l'IP de destination**. *Le pare-feu consomme plus de ressources pour suivre le compteur **src-dest-ip-both (à la fois à l'IP source et à l'IP de destination)** que pour suivre uniquement les compteurs d'adresses IP source ou d'adresses IP de destination.* Si vous spécifiez un profil de Protection DoS classé, seules les connexions entrantes qui correspondent à une adresse IP source, une adresse IP de destination ou une paire d'adresses IP source et de destination sont prises en compte dans les seuils spécifiés dans le profil. Par exemple, vous pouvez indiquer un profil de Protection DoS classé avec un **Taux max.** de 100 cps et indiquer un paramètre **Adresse** dans la règle à définir sur **adresse IP source uniquement**. Vous obtenez alors une limite de 100 connexions par seconde cette adresse IP source en particulier. *N'utilisez pas **source-ip-only (ip source uniquement)** ou **src-dest-ip-both (à la fois à l'IP source et à l'IP de destination)** pour les zones Internet, car le pare-feu ne peut pas stocker des compteur pour toutes les adresses IP Internet possibles. Utilisez **destination-ip-only (ip de destination uniquement)** dans les zones du périmètre.* *Utilisez **destination-ip-only (ip de destination uniquement)** pour protéger les périphériques critiques individuels.* *Utilisez **source-ip-only (ip source uniquement)** et le seuil d'**Alarm (alarme)** pour surveiller les hôtes suspects dans des zones qui ne sont pas connectées à l'Internet.* Voir Objets > Profils de sécurité > Protection DoS.

Onglet cible de protection DoS

- (Panorama uniquement) **Policies (Politiques)** > **DoS Protection (Protection DoS)** > **Target (cible)**

Sélectionnez l’onglet **Target (Cible)** pour sélectionner les pare-feux gérés du groupe de périphériques auxquels appliqués la règle de politique. Vous pouvez préciser à quels pare-feux gérés appliquer en sélectionnant les pare-feux gérés ou en attribuant une étiquette. De plus, vous pouvez configurer la cible de la règle de politique à appliquer à tous les pare-feux gérés sauf ceux indiqués.

Règle NAT - Paramètres de la cible	Description
Tous (cible tous les périphériques)	Activez (cochez) pour valider la règle de politique de tous les pare-feux gérés du groupe de périphériques.
Périphériques	Sélectionnez un ou plusieurs pare-feux gérés associés au groupe de périphériques pour valider la règle de politique.
Étiquettes	**Add (Ajoutez)** une ou plusieurs étiquettes pour valider la règle de politique des pare-feux gérés dans le groupe de périphériques ayant l’étiquette indiquée.
Cibler tous les périphériques sauf ceux spécifiés	Activez (cochez) pour valider la règle de politique pour tous les pare-feux gérés associés au groupe de périphériques sauf pour le(s) périphérique(s) et étiquette(s) sélectionnés.

Politiques > SD-WAN

Ajoutez une politique SD-WAN pour configurer les paramètres de gestion du chemin d'accès du lien sur la base de chaque application, ou pour un groupe d'applications qui passent par le même lien sur la base des mesures de santé en termes de gigue, latence et perte de paquets que vous configurez. Lorsque certains chemins d'accès entre la source et la destination pour des applications critiques subissent une dégradation, la règle de politique SD-WAN sélectionne un nouveau chemin d'accès optimal afin de garantir que les applications sensibles et critiques se comportent conformément au profil de qualité du chemin d'accès qui leur est attribué dans la règle de politique SD-WAN.

- Onglet Général SD-WAN
- Onglet Source SD-WAN
- Onglet Destination SD-WAN
- Onglet Application/Service SD-WAN
- Onglet Sélection du chemin d'accès SD-WAN
- (Panorama uniquement) Onglet Cible SD-WAN

Onglet Général SD-WAN

- **Politiques** > **SD-WAN** > **Général**

Sélectionnez l'onglet **General (Général)** pour définir un nom et une description pour la politique SD-WAN. Une étiquette peut également être configurée et vous permettre de trier ou de filtrer les politiques lorsqu'il en existe un grand nombre.

Champ	Description
Name (Nom)	Donnez un nom à la règle afin de l'identifier. Le nom est sensible à la casse et peut comporter jusqu'à 63 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement. Le nom doit être unique sur un pare-feu et, dans Panorama, unique au sein de son groupe de périphériques et des groupes de périphériques anciens ou descendants.
Description	Saisissez une description de la règle (1 024 caractères maximum).
Étiquette	Si vous avez besoin d'étiqueter la politique, cliquez sur **Ajouter** et indiquez l'étiquette. Une étiquette de politique est un mot-clé ou une expression qui vous permet de trier ou de filtrer les politiques. Cela est utile lorsque vous avez défini de nombreuses politiques et que vous souhaitez afficher celles qui sont identifiées par un mot-clé particulier. Par exemple, il se peut que vous souhaitiez ajouter des étiquettes uniques à certaines politiques SD-WAN pour identifier leurs hubs ou branches spécifiques auxquelles les règles s'appliquent.

Champ	Description
Regrouper des règles par étiquette	Saisissez une étiquette selon laquelle regrouper des règles de politique similaires. L'étiquette de groupe vous permet d'afficher votre base de règles de politique en fonction de ces étiquettes. Vous pouvez choisir de regrouper les règles en fonction d'une **Tag (Étiquette)**.
Commentaire d'audit	Saisissez un commentaire pour auditer la création ou la modification d'une règle de politique. Le commentaire d'audit est sensible à la casse et peut comporter jusqu'à 256 caractères qui peuvent être des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement.
Archive des commentaires d'audit	Afficher les **Audit Comments (Commentaires d'audit)** précédents pour la règle de politique. L'archive des commentaires d'audit peut être exportée au format CSV.

Onglet Source SD-WAN

- **Politiques** > **SD-WAN** > **Source**

Sélectionnez l'onglet **Source** pour définir les zones sources, les adresses sources et les utilisateurs sources qui définissent les paquets entrants auxquels la politique SD-WAN s'applique.

Champ	Description
Source Zone (Zone source)	Pour spécifier une zone source, sélectionnez **Add (Ajouter)** et sélectionnez une ou plusieurs zones, ou sélectionnez **Any (N'importe quelle)** zone. Spécifier plusieurs zones peut simplifier la gestion. Par exemple, si vous avez trois branches dans différentes zones et vous voulez que les critères de correspondance ainsi que la sélection du chemin d'accès soient les mêmes pour les trois branches, vous pouvez créer une règle SD-WAN et spécifier les trois zones sources pour couvrir les trois branches. *Seules les zones de type Couche 3 sont prises en charge par les règles de politique SD-WAN.*
Source Address (Adresse source)	Pour spécifier des adresses sources, **Add (Ajoutez)** des adresses sources ou des listes dynamiques externes (EDL), sélectionnez dans le menu déroulant ou sélectionnez **Address (adresse)** et créez un nouvel objet adresse. Vous pouvez également sélectionner **Any (n'importe quelle)** adresse source (par défaut).
Source User (Utilisateur source)	Pour spécifier certains utilisateurs, sélectionnez **Add (ajouter)** (le type indique ensuite **select [sélectionner]**) et saisissez un utilisateur, une liste d'utilisateurs ou des groupes d'utilisateurs. Vous pouvez également sélectionner un type d'utilisateur :

Champ	Description
	• **any (indifférent)** - (par défaut) Inclut tout utilisateur, quelles que soient les données utilisateur. • **pre-logon (pré-ouverture de session)** - Inclut les utilisateurs distants connectés au réseau à l'aide de GlobalProtect™ mais non connectés à leur système. Lorsque l'option Pré-ouverture de session est configurée sur le portail des applications GlobalProtect, tout utilisateur non connecté à sa machine est identifié avec le nom d'utilisateur pre-logon. Vous pouvez ensuite créer des politiques pour les utilisateurs pre-logon. Bien que l'utilisateur ne soit pas directement connecté, sa machine est authentifiée sur le domaine, comme s'il était complètement connecté. • **Utilisateur connu** – Inclut tous les utilisateurs authentifiés, c'est-à-dire toute adresse IP dont les données utilisateur sont mappées. Cette option est équivalente au groupe « utilisateurs » du domaine sur un domaine. • **unknown (inconnu)** - Inclut tous les utilisateurs non authentifiés, c'est-à-dire les adresses IP non mappées à un utilisateur. Par exemple, vous pouvez sélectionner l'option **unknown (inconnu)** pour accéder à quelque chose au niveau invité, car les invités ont une adresse IP sur votre réseau, mais ne sont pas authentifiés sur le domaine et ne disposent d'aucune information de mappage utilisateur/adresse IP sur le pare-feu. *Si le pare-feu collecte les informations utilisateur depuis un serveur RADIUS, TACACS+ ou le serveur du fournisseur d'identité SAML et non depuis l'agent User-ID™, la liste des utilisateurs ne s'affiche pas ; vous devez saisir les informations de l'utilisateur manuellement.*

Onglet Destination SD-WAN

- **Politiques** > **SD-WAN** > **Destination**

Sélectionnez l'onglet **Destination** pour définir la ou les zones de destination ou la ou les adresses de destination qui définissent le trafic auquel la règle de politique SD-WAN s'applique.

Champ	Description
Destination Zone (Zone de destination)	**Add (Ajoutez)** des zones de destination (la valeur par défaut est any [n'importe laquelle]). Les zones doivent être de Couche 3. Pour définir de nouvelles zones, voir Réseau > Zones. Ajoutez plusieurs zones pour simplifier la gestion. Par exemple, si vous possédez trois zones internes différentes (marketing, ventes et relations publiques) qui sont toutes reliées à la zone de destination non approuvée, vous pouvez créer une règle qui couvre tous les cas possibles.

Champ	Description
Adresse de destination	**Add (Ajoutez)** des adresses, des groupes d'adresses, des listes dynamiques externes (EDL) ou des régions de destination (valeur par défaut : **any [indifférent]**). Faites votre sélection dans la liste déroulante ou cliquez sur **Address (Adresse)** ou sur **Address Group (Groupe d'adresses)** en bas de la liste déroulante et définissez les paramètres. Sélectionnez **Negate (Ignorer)** pour choisir n'importe quelle adresse sauf celles configurées.

Onglet Application/Service SD-WAN

- **Politiques** > **SD-WAN** > **Application/Service**

Sélectionnez l’onglet **Application/Service** pour indiquer les services ou les applications auxquels la règle de politique SD-WAN s’applique et indiquer les profils (profils de qualité du chemin d’accès, qualité SaaS et correction des erreurs) qui s’appliquent aux applications ou services.

Champ	Description
Path Quality Profile (Profil de qualité du chemin d’accès)	Sélectionnez un profil de qualité du chemin d’accès qui détermine le pourcentage maximum de gigue, de latence et de perte de paquets que vous voulez appliquer aux applications et aux services spécifiés. Si un profil de qualité du chemin d’accès n’a pas encore été créé, vous pouvez créer un **New SD-WAN Path Quality (Nouveau profil de qualité du chemin d’accès SD-WAN**.
Profil de qualité SaaS	Sélectionnez un profil de qualité SaaS pour indiquer les seuils de qualité du chemin d’accès en termes de latence, gigue et perte de paquets pour un pare-feu de plate-forme ou branche qui a un lien d’Accès direct à Internet (DIA) vers une application Logiciel en tant que service (SaaS). Si un profil de qualité Saas n’a pas encore été créé, vous pouvez créer un **New SaaS Quality Profile (nouveau profil de qualité SaaS)**. Par défaut **None (disabled) (Aucun - désactivé)**.
Profil de correction des erreurs	Sélectionnez un **Error Correction Profile (Profil de correction des erreurs)** ou créez un nouveau Error Correction Profile (Profil de correction des erreurs), qui précise les paramètres de contrôle de transfert de correction des erreurs (FEC) ou de duplication de chemin d’accès pour les applications or services précisés dans la règle. Ce profil peut être utilisé par le pare-feu de la plate-forme ou de la branche. Par défaut **None (disabled) (Aucun - désactivé)**.
Applications	**Add (Ajoutez)** des applications spécifiques pour la règle de politique SD-WAN ou sélectionnez **Any (toutes)**. Si une application présente plusieurs fonctions, sélectionnez l'application dans son ensemble ou des fonctions individuelles. Si vous sélectionnez l'application dans

Champ	Description
	son ensemble, toutes les fonctions seront incluses et la définition de l'application sera automatiquement mise à jour lors de l'ajout de fonctions supplémentaires. Si vous utilisez des groupes d'applications, des filtres ou des conteneurs dans la règle de politique SD-WAN, consultez les détails en passant la souris sur l'objet dans la colonne Application, en ouvrant la liste déroulante et en sélectionnant **Valeur (Value)**. Ainsi, vous pourrez accéder aux membres des applications directement depuis la politique, sans passer par l'onglet **Object (Objet)**.  *Ajoutez uniquement les services critiques à l'entreprise qui sont affectés par la latence, la gigue et la perte de paquets. Évitez d'ajouter des catégories ou des sous-catégories d'applications, car celles-ci sont trop générales et ne permettent par le contrôle par application.*
Service	**Ajoutez des** services spécifiques pour la règle de stratégie SD-WAN et sélectionnez les ports sur lesquels les paquets de ces services sont autorisés ou refusés : • **any : les**services sélectionnés sont autorisés ou refusés sur n'importe quel protocole ou port. • **application-default**: les services sélectionnés sont autorisés ou refusés uniquement sur leurs ports par défaut **définis par Palo Alto Networks®**. Cette option est recommandée pour les stratégies qui spécifient l'action **d'autorisation** car elle empêche les services de s'exécuter sur des ports et des protocoles inhabituels qui, s'ils ne sont pas intentionnels, peuvent être un signe de comportement et d'utilisation indésirables du service.  *Lorsque vous utilisez cette option, seul le port par défaut correspond à la stratégie SD-WAN et l'action est appliquée. D'autres services qui ne se trouvent pas sur le port par défaut peuvent être autorisés en fonction de la règle de stratégie de sécurité, mais ne correspondent pas à la stratégie SD-WAN et aucune action de règle de stratégie SD-WAN n'est entreprise.*

Champ	Description
	*Pour la plupart des services, utilisez **la valeur par défaut** de l'application pour empêcher le service d'utiliser des ports non standard ou de présenter d'autres comportements d'évitement. Si le port par défaut du service change, le pare-feu met automatiquement à jour la règle en utilisant le bon port par défaut. Pour les services qui utilisent des ports non standard, comme les services personnalisés internes, modifiez le service ou créez une règle qui spécifie les ports non standard et appliquez la règle uniquement au trafic qui exige le service.* • **Select (Sélectionnez)** - **Add (Ajoutez)** un service existant ou choisissez **Service** ou **Service Group (Groupe de services)** pour définir une nouvelle entrée. (Ou sélectionnez Objets > Services et Objets > Groupes de services).

Onglet Sélection du chemin d'accès SD-WAN

- **Politiques** > **SD-WAN** > **Sélection du chemin**

Sélectionnez l'onglet **Path selection (sélection du chemin d'accès)** pour définir des chemins d'accès pour le trafic des applications ou des services afin de basculer si la qualité du chemin d'accès principal dépasse les seuils de qualité du chemin d'accès configuré dans le Profil de qualité de chemin d'accès.

Champ	Description
Profil de distribution du trafic	Dans la liste déroulante, sélectionnez un profil de distribution du trafic afin de déterminer comment le pare-feu sélectionne un autre chemin d'accès pour le trafic des applications ou des services lorsque les mesures d'état d'un des chemins d'accès privilégiés dépassent le seuil configuré dans le profil de qualité du chemin d'accès dans la règle.

Onglet Cible SD-WAN

- **Politiques** > **SD-WAN** > **Cible**

Sélectionnez l'onglet **Target (Cible)** pour sélectionner les périphériques gérés qui appliqueront la règle de politique SD-WAN. Cet onglet est pris en charge uniquement sur le serveur de gestion Panorama.

Champ	Description
Tous (cible tous les périphériques)	Activez (cochez) pour appliquer la règle de politique SD-WAN à tous les périphériques du serveur de gestion Panorama.

Champ	Description
Périphériques	Sélectionnez un ou plusieurs périphériques auxquels appliquer la règle de politique SD-WAN. Vous pouvez filtrer les périphériques sur la base de l'état du périphérique, la plate-forme, le groupe de périphériques, les modèles, les étiquettes ou le statut HA.
Étiquettes	Spécifiez l'étiquette pour la politique. Une étiquette de politique est un mot-clé ou une expression qui vous permet de trier ou de filtrer les politiques. Cela est utile lorsque vous avez défini de nombreuses politiques et que vous souhaitez afficher celles qui sont identifiées par un mot-clé particulier. Par exemple, vous pouvez ajouter des étiquettes à certaines règles avec des mots spécifiques, tels que Déchiffrement et Aucun déchiffrement, ou utiliser le nom d'un centre de données spécifique pour les politiques associées à cet emplacement. Vous pouvez également ajouter des étiquettes aux règles par défaut.
Cibler tous les périphériques sauf ceux spécifiés	Activez (cochez) pour cibler et appliquer la règle de politique à tous les périphériques, sauf les **Devices (Périphériques)** et les **Tags (Étiquettes)** sélectionnés.

Objets

Les objets sont les éléments qui vous permettent de construire, de programmer et de chercher des règles de politique, et les profils de sécurité fournissent une protection contre les menaces dans les règles de sécurité.

Cette section décrit la configuration des profils de sécurité et des objets que vous pouvez utiliser avec les politiques :

- Déplacement, clonage, remplacement ou rétablissement des objets
- Objets > Adresses
- Objets > Groupes d'adresses
- Objets > Régions
- Objets > Applications
- Objets > Groupe d'applications
- Objets > Filtres d'applications
- Objets > Services
- Objets > Groupes de services
- Objets > Étiquettes
- Objets > Périphériques
- Objets > GlobalProtect > Objets HIP
- Objets > GlobalProtect > Profils HIP
- Objets > Listes dynamiques externes
- Objets > Objets personnalisés
- Objets > Profils de sécurité
- Objets > Profils de sécurité > Protection du réseau mobile
- Objets > Profils de sécurité > Protection SCTP
- Objets > Groupes de profils de sécurité
- Objets > Transfert des journaux
- Objets > Authentification
- Objets > Profils de déchiffrement
- Objets > Gestion des liens SD-WAN
- Objets > Calendriers

Déplacement, clonage ou rétablissement des objets ou application d’un contrôle prioritaire sur ceux-ci

Consultez les rubriques suivantes pour connaître les options qui s'offrent à vous pour modifier les objets existants :

- Déplacement ou clonage d’un objet
- Contrôle prioritaire et rétablissement d’un objet

Déplacement ou clonage d’un objet

Lorsque vous déplacez ou clonez des objets, vous pouvez définir une **Destination** (un système virtuel sur un pare-feu ou un groupe de périphériques sur Panorama™) pour laquelle vous disposez d’autorisations d’accès, y compris l’emplacement partagé.

Pour déplacer un objet, sélectionnez-le dans l'onglet **Objects (Objets)**, cliquez sur **Move (Déplacer)**, sélectionnez **Move to other vsys (Déplacer vers d'autres vsys)** (pare-feu uniquement) ou **Move to other device group (Déplacer vers un autre groupe de périphériques)** (Panorama uniquement), remplissez les champs du tableau suivant, puis cliquez sur **OK**.

Pour cloner un objet, sélectionnez-le dans l'onglet **Objects (Objets)**, cliquez sur **Clone (Cloner)**, remplissez les champs du tableau suivant, puis cliquez sur **OK**.

Paramètres de déplacement/ clonage	Description
Objets sélectionnés	Affiche le nom et l'emplacement actuel (système virtuel ou groupe de périphériques) des politiques ou objets que vous avez sélectionnés pour l'opération.
Destination	Sélectionnez le nouvel emplacement de la politique ou de l'objet : un système virtuel, un groupe de périphériques ou un emplacement partagé. La valeur par défaut est le **Virtual System (Système virtuel)** ou le **Device Group (Groupe de périphériques)** que vous avez sélectionné dans l'onglet **Policies (Politiques)** ou **Objects (Objets)**.
Erreur sortante dès la première erreur détectée lors de la validation	Sélectionnez cette option (sélectionnée par défaut) pour que le pare-feu ou Panorama affiche la première erreur trouvée et arrête de rechercher d'autres erreurs. Par exemple, une erreur se produit si la **Destination** ne contient aucun objet référencé dans la règle de la politique que vous déplacez. Si vous désélectionnez cette option, le pare-feu ou Panorama trouvera toutes les erreurs avant de les afficher.

Contrôle prioritaire et rétablissement d’un objet

Dans Panorama, vous pouvez imbriquer des groupes de périphériques dans une arborescence pouvant contenir jusqu’à quatre niveaux. Au niveau inférieur, un groupe de périphériques peut avoir des groupes

de périphériques parents, grands-parents et arrière-grands-parents à des niveaux supérieurs successifs (collectivement appelés *anciens*) dont le groupe de périphériques de niveau inférieur hérite des politiques et objets. Au niveau supérieur, un groupe de périphériques peut avoir des groupes de périphériques enfants, petits-enfants et arrière-petits-enfants — collectivement appelés *descendants*. Vous pouvez appliquer un contrôle prioritaire sur un objet dans un descendant afin que ses valeurs soient différentes de celles d'un ancien Cette capacité de contrôle prioritaire est activée par défaut. Toutefois, vous ne pouvez pas appliquer un contrôle prioritaire sur des objets partagés ou par défaut (préconfigurés). L'interface Web affiche l'icône pour indiquer qu'un objet a hérité des valeurs et affiche l'icône pour indiquer qu'un objet hérité contient des valeurs qui ont été forcées.

- **Appliquer un contrôle prioritaire sur un objet** - Cliquez sur l'onglet **Objects (Objets)**, sélectionnez le descendant **Device Group (Groupe de périphériques)** qui contiendra la version forcée, sélectionnez l'objet, cliquez sur **Override (Contrôle prioritaire)** et modifiez les paramètres. Vous ne pouvez pas appliquer un contrôle prioritaire sur les paramètres **Name (Nom)** ou **Shared (Partagé)**.
- **Rétablir les valeurs héritées d'un objet dont les valeurs ont été forcées** - Cliquez sur l'onglet **Objects (Objets)**, sélectionnez le **Device Group (Groupe de périphériques)** contenant la version forcée, sélectionnez l'objet, cliquez sur **Revert (Rétablir)**, puis sur **Yes (Oui)** pour confirmer l'opération.
- **Désactiver le contrôle prioritaire des valeurs d'un objet** - Cliquez sur l'onglet **Objects (Objets)**, sélectionnez le **Device Group (Groupe de périphériques)** dans lequel se trouve l'objet, cliquez sur le nom de l'objet pour le modifier, sélectionnez l'option **Disable override (Désactiver le contrôle prioritaire)** et cliquez sur **OK**. Les contrôles prioritaires pour cet objet sont alors désactivés dans tous les groupes de périphériques qui héritent de l'objet du **Groupe de périphériques** sélectionné.
- **Rétablir les valeurs héritées de l'emplacement partagé ou des groupes de périphériques anciens des objets dont les valeurs ont eu un contrôle prioritaire dans Panorama** - Sélectionnez **Panorama** > **Setup (Configuration)** > **Management (Gestion)**, modifiez les paramètres de Panorama, sélectionnez **Ancestor Objects Take Precedence (Les objets anciens sont prioritaires)** et cliquez sur **OK**. Vous devez ensuite les valider dans Panorama et dans les groupes de périphériques contenant des valeurs de contrôle prioritaire pour transmettre les valeurs héritées.

Objets > Adresses

Un objet d'adresse peut inclure une adresse IPv4 ou une adresse IPv6 (une adresse IP unique, une plage d'adresses ou un sous-réseau), un FQDN ou une adresse générique (une adresse IPv4 suivie d'une barre oblique et d'un masque générique). Un objet d'adresse vous permet de réutiliser cette même adresse ou ce même groupe d'adresses comme adresse source ou de destination dans les règles de politique, les filtres et les autres fonctions du pare-feu sans ajouter chaque adresse manuellement pour chaque instance. Vous créez un objet d'adresses à l'aide de l'interface Web ou de la CLI. Par ailleurs, les modifications doivent faire l'objet d'une opération de validation pour que l'objet soit intégré à la configuration.

Vous devez d'abord **Add (Ajouter)** un nouvel objet d'adresse, puis préciser les valeurs suivantes :

Paramètres de l'objet de l'adresse	Description
Name (Nom)	Saisissez un nom (maximum de 63 caractères) qui décrit les adresses que vous intégrerez à cet objet. Ce nom apparaît dans la liste d'adresses lors de la définition des règles de politique de sécurité. Le nom est sensible à la casse, doit être unique et peut inclure uniquement des lettres, chiffres, espaces, traits d'union et traits de soulignement.
Partagé	Sélectionnez cette option si vous souhaitez partager cet objet d'adresse avec : • **Tous les systèmes virtuels (vsys) sur un pare-feu comportant plusieurs vsys** - Si vous ne sélectionnez pas cette option, l'objet d'adresse est disponible uniquement pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • **Every device group on Panorama (Tous les groupes de périphériques sur Panorama)** - Si vous ne sélectionnez pas cette option, l'objet d'adresse sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de cet objet d'adresse dans les groupes de périphériques qui héritent de cet objet. Cette sélection est désactivée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l'objet.
Description	Saisissez une description de l'objet (1 023 caractères maximum).
Type	Spécifiez le type d'objet d'adresses et l'entrée : • **IP Netmask (Masque réseau IP)** - Saisissez l'adresse'A0;IPv4 ou IPv6 ou la plage d'adresses'A0;IP selon la notation suivante : *adresse_ip/masque* or *adresse_IP* où le masque correspond au nombre de valeurs binaires les plus significatives utilisées pour la portion

Paramètres de l’objet de l’adresse	Description
	réseau de l’adresse. Idéalement, pour les adresses IPv6, vous indiquez uniquement la partie réseau et non la partie hôte. Par exemple : • **192.168.80.150/32** : indique une adresse. • **192.168.80.0/24** : indique toutes les adresses comprises entre 192.168.80.0 et 192.168.80.255 • **2001:db8:32** • **2001:db8:123:1::/64** • **IP Range (Plage d’adresses IP)** - Saisissez une plage d’adresses en utilisant le format suivant : *ip_address*-*ip_address* où les deux extrémités de la plage sont des adresses IPv4 ou des adresses IPv6. Par exemple : 2001:db8:123:1::1-2001:db8:123:1::22 • **Masque générique IP** saisissez une adresse IP générique au format d’une adresse IPv4 suivie d’une barre oblique et d’un masque (qui doivent commencer par zéro) ; par exemple, 10.182.1.1/0.127.248.0. Dans le masque générique, un zéro (0) indique que le bit faisant l’objet de la comparaison doit correspondre au bit qui est indiqué dans l'adresse IP qui est couverte par le 0. Dans le masque générique, un bit de un (1) est un bit générique, ce qui indique que le bit faisant l’objet de la comparaison doit correspondre au bit qui est indiqué dans l'adresse IP qui est couverte par le 1. Convertissez l'adresse IP et le masque générique en binaire. Pour illustrer la correspondance : sur l’extrait binaire 0011, un masque générique de 1010 donne quatre correspondances (0001, 0011, 1001 et 1011). *Vous pouvez utiliser un objet d’adresse de type IP Wildcard Mask uniquement dans une règle de stratégie de sécurité.* • **FQDN** : saisissez le nom de domaine. Le FQDN est résolu au moment de la validation. Le FQDN est ultérieurement actualisé selon la TTL du FQDN, si la TTL est supérieure ou égale à la Minimum FQDN Refresh Time (Fréquence d'actualisation minimale du FQDN) ; autrement, le FQDN est actualisé selon la Fréquence d’actualisation minimale du FQDN. Le FQDN est résolu par le serveur DNS du système ou un objet proxy DNS, si un proxy est configuré.
Résoudre	Après avoir sélectionné le type d’adresse et saisi une adresse IP ou un FQDN, cliquez sur **Resolve (Résoudre)** pour voir les FQDN ou les adresses IP associés, respectivement (selon la configuration DNS du pare-feu ou de Panorama). Vous pouvez faire passer un objet d’adresse d’un FQDN à un masque réseau IP et vice-versa. Pour passer d’un FQDN à un Masque réseau IP, cliquez sur **Resolve (Résoudre)** pour voir les adresses IP auxquelles le FQDN est résolu, sélectionnez en une, puis cliquez sur **Use this**

Paramètres de l’objet de l’adresse	Description
	address (Utiliser cette adresse). Le Type d’objet d'adresse est modifié de manière dynamique en un Masque réseau IP et l’adresse IP que vous avez sélectionnée apparaît dans le champ texte. De même, pour que l’objet d’adresse passe d’un Masque réseau IP à un FQDN, cliquez sur **Resolve (Résoudre)** pour voir le nom DNS auquel le Masque réseau est résolu, puis sélectionnez le FQDN et cliquez sur **Use this FQDN (Utiliser ce FQDN)**. Le Type passe à FQDN et le FQDN apparaît dans le champ texte.
Étiquettes	Sélectionnez ou saisissez les étiquettes que vous souhaitez appliquer à cet objet d'adresse. Vous pouvez définir une étiquette ici ou utiliser l'onglet Objets > Étiquettes pour créer de nouvelles étiquettes.

Objets > Groupes d'adresses

Pour simplifier la création des politiques de sécurité, les adresses qui requièrent les mêmes paramètres de sécurité peuvent être combinées en groupes d’adresses. Un groupe d'adresses peut être statique ou dynamique.

- Groupes d’adresses dynamiques : un groupe d'adresses dynamique charge ses membres de manière dynamique à l'aide de recherches d'étiquettes et de filtres par étiquette. Les groupes d'adresses dynamiques sont très utiles si vous disposez d'une infrastructure virtuelle étendue, dans laquelle les changements d'emplacement des machines virtuelles et d'adresse'A0;IP sont fréquents. Par exemple, vous avez une configuration de basculement sophistiquée ou configurez fréquemment de nouvelles machines virtuelles et souhaitez appliquer la politique au trafic depuis ou vers la nouvelle machine, sans modifier la configuration/les règles sur le pare-feu.

  Pour utiliser un groupe d’adresses dynamique dans une politique, vous devez effectuer les tâches suivantes :

  - Définissez un groupe d'adresses dynamique et faites-y référence dans une règle de politique.
  - Informez le pare-feu des adresses'A0;IP et des étiquettes correspondantes, de manière à ce que les membres du groupe d'adresses dynamique puissent être formés. Pour ce faire, vous pouvez utiliser des scripts externes qui appellent l’API XML sur le pare-feu ou, si vous disposez d’un environnement VMware, vous pouvez sélectionner **Device (Périphérique)** > **VM Information Sources (Sources d’informations de machine virtuelle)** pour configurer les paramètres du pare-feu.

  les groupes d'adresses dynamiques peuvent également inclure des objets d'adresse définis de manière statique. Si vous créez un objet d'adresse et que vous appliquez les mêmes étiquettes que vous avez affectées à un groupe d'adresses dynamiques, ce dernier inclura tous les objets statiques et dynamiques correspondant aux étiquettes. Vous pouvez ainsi utiliser les étiquettes pour rassembler les objets statiques et dynamiques dans le même groupe d'adresses.
- Groupes d’adresses statiques : Un groupe d'adresses statiques peut inclure des objets d'adresse statiques, des groupes d'adresses dynamiques ou être une combinaison d'objets d'adresses statiques et de groupes d'adresses dynamiques.

  Pour créer un groupe d'adresses, cliquez sur **Add (Ajouter)** et renseignez les champs suivants :

Paramètres du groupe d’adresses	Description
Name (Nom)	Saisissez un nom qui décrit le groupe d'adresses (**63** caractères maximum). Ce nom apparaît dans la liste d'adresses lors de la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement.
Partagé	Sélectionnez cette option si vous souhaitez que le groupe d'adresses soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le groupe d'adresses sera uniquement

Paramètres du groupe d’adresses	Description
	disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le groupe d'adresses sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce groupe d’adresses dans les groupes de périphériques qui héritent de l’objet. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l’objet.
Description	Saisissez une description de l'objet (1023 caractères maximum).
Type	Sélectionnez **Static (Statique)** ou **Dynamic (Dynamique)**. Pour créer un groupe d'adresses dynamique, utilisez les critères de correspondance pour rassembler les membres à inclure dans le groupe. Définissez les critères **Match (Correspondance)** à l'aide des opérateurs **AND (ET)** et **OR (OU)**. La négation n’est pas prise en charge. *pour afficher la liste des attributs des critères de correspondance, vous devez avoir configuré le pare-feu pour accéder et récupérer les attributs de la source/ l'hôte. Chaque machine virtuelle sur la(les) source(s) d’informations configurée(s) est enregistrée auprès du pare-feu ; le pare-feu peut sonder la machine pour récupérer les changements d’adresse IP ou de configuration, sans qu’aucune modification ne soit effectuée sur le pare-feu.* Pour un groupe d'adresses statiques, cliquez sur **Add (Ajouter)** et sélectionnez une ou plusieurs **Addresses (Adresses)**. Cliquez sur **Add (Ajouter)** pour ajouter un objet ou un groupe d'adresses au groupe d'adresses. Ce groupe peut contenir des objets d'adresse, ainsi que des groupes d'adresses statiques et dynamiques.
Étiquettes	Sélectionnez ou saisissez les étiquettes que vous souhaitez appliquer à ce groupe d'adresses. Pour plus d’informations sur les étiquettes, voir Objets > Étiquettes.
Nombre de membres et adresses	Après avoir ajouté un groupe d’adresses, la colonne Nombre de membres sur la page **Objects (Objets)** > **Address Groups (Groupes d’adresses)** indique si les objets du groupe sont renseignés dynamiquement ou statiquement.

Paramètres du groupe d’adresses	Description
	• Pour un groupe d’adresses statiques, vous pouvez afficher le nombre de membres dans le groupe d’adresses. • Pour un groupe d’adresses utilisant des étiquettes pour remplir dynamiquement les membres ou ayant des membres statiques et dynamiques, cliquez sur le lien **More... (Plus...)** dans la colonne Adresse pour afficher les membres. Vous pouvez maintenant visualiser les adresses IP qui sont enregistrées dans le groupe d’adresses. • Le type indique si l’adresse IP est un objet d’adresse statique ou si elle est enregistrée dynamiquement et affiche l’adresse IP. • L’action vous permet d’**Annuler l’enregistrement des étiquettes** à partir d’une adresse IP. Cliquez sur le lien pour **Ajouter** la source d’enregistrement et spécifier les étiquettes dont il faut annuler l’enregistrement.

Objets > Régions

Le pare-feu prend en charge la création de règles de politique qui s’appliquent à des pays spécifiques ou à d’autres régions. L'option région est disponible lors de la définition de la source et de la destination des politiques de sécurité, des politiques de déchiffrement et des politiques DoS. Vous pouvez faire votre choix parmi une liste standard de pays ou utiliser les paramètres régionaux décrits dans cette section pour définir des régions personnalisées à inclure sous forme d'options dans les règles des politiques de sécurité.

Les tableaux suivants décrivent les paramètres régionaux :

Paramètres régionaux	Description
Région	Sélectionnez un nom dans le menu déroulant qui décrit la région. Ce nom apparaît dans la liste d'adresses lors de la définition de politiques de sécurité.
Emplacement géographique	Pour indiquer la latitude et la longitude, sélectionnez cette option et renseignez les valeurs (format xxx.xxxxxx). Ces informations sont utilisées dans les cartes du trafic et des menaces pour définir la portée d'application. Voir Surveillance > Journaux.
Adresses	Renseignez une adresse'A0;IP, une plage d'adresses'A0;IP ou un sous-réseau pour identifier la région, en respectant les formats suivants : x.x.x.x x.x.x.x-a.a.a.a x.x.x.x/n

Objets > Groupes d’utilisateurs dynamiques

Pour créer un groupe d’utilisateurs dynamiques, sélectionnez **Objects (Objets)** > **Dynamic User Groups (Groupes d’utilisateurs dynamiques)**, **Add (Ajoutez)** un nouveau groupe d’utilisateurs dynamiques et configurez les paramètres suivants :

Paramètres de groupe d’utilisateurs dynamiques	Description
Name (Nom)	Saisissez un **Name (Nom)** qui décrit le groupe d'utilisateurs dynamiques (63 caractères maximum). Ce nom apparaît dans la liste d’utilisateurs sources lors de la définition des règles de politique de sécurité. Le nom doit être unique et utiliser uniquement des caractères alphanumériques, des espaces, des traits d'union et des traits de soulignement.
Description	Saisissez une **Description** de l'objet (1 023 caractères maximum).
Partagé (Panorama uniquement)	Sélectionnez cette option si vous voulez que les critères de correspondance du groupe d’utilisateurs dynamiques soient disponibles pour tous les groupes de périphériques sur Panorama. *Panorama ne partage pas l’information des membres du groupe avec les groupes de périphériques.* Si vous désélectionnez cette option, les critères de correspondance du groupe d’utilisateurs dynamiques seront uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le remplacement (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce groupe d’utilisateurs dynamiques dans les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l’objet.
Correspondance	**Add Match Criteria (Ajoutez des critères de correspondance)** pour définir les membres dans le groupe d’utilisateurs dynamiques en utilisant les opérateurs **AND (ET)** ou **OR (OU)** pour inclure plusieurs étiquettes. La négation n'est pas prise en charge. *Lorsque vous **Add Match Criteria (Ajoutez des critères de correspondance)**, uniquement les étiquettes existantes s’afficheront. Vous pouvez sélectionner une étiquette existante ou créer de nouvelles étiquettes.*

Paramètres de groupe d’utilisateurs dynamiques	Description
Étiquettes	(Optional [Facultatif]) Sélectionnez ou saisissez les étiquettes d’objet statique que vous voulez appliquer sur l’objet de groupe d’utilisateurs dynamiques. Ceci permet d’étiqueter l’objet de groupe d’utilisateurs dynamiques lui-même et non les membres du groupe. Les étiquettes que vous sélectionnez vous permettent de group related items (regrouper des éléments associés) et ne sont pas reliées aux critères de correspondance. Pour plus d’informations sur les étiquettes, voir Objets > Étiquettes.

Après avoir ajouté un groupe d’utilisateurs dynamiques, vous pouvez afficher les informations suivantes pour le groupe :

Colonne des groupes d’utilisateurs dynamiques	Description
Location (Emplacement) (Panorama uniquement)	Identifie si les critères de correspondance du groupe d’utilisateurs dynamiques sont disponibles pour tous les groupes d’appareils sur Panorama (**Shared [Partagé]**) ou seulement pour le groupe d’appareils sélectionné.
Users (Utilisateurs)	Sélectionnez **more (plus)** pour voir la liste des utilisateurs dans le groupe d’utilisateurs dynamiques. • Pour ajouter des étiquettes aux utilisateurs pour leur intégration dans le groupe, **Register Users (Enregistrez les utilisateurs)**, puis sélectionnez **Registration Source (Source d’enregistrement)** et les **Tags (Étiquettes)** que vous voulez appliquez à l’utilisateur. Lorsque les étiquettes d’un utilisateur correspondent aux critères de correspondance d’un groupe, le pare-feu ajoute l’utilisateur au groupe d’utilisateurs dynamiques. • (Optional [Facultatif]) Spécifiez un **Timeout (Délai d'expiration)** en minutes (par défaut : 0 ; plage comprise entre 0 et 43 200) pour supprimer les utilisateurs d’un groupe quand le délai spécifié expire. • (Optional [Facultatif]) **Add (Ajoutez)** des **Users (Utilisateurs)** au groupe ou **Delete (Supprimez)** des utilisateurs du groupe. • Pour supprimer des étiquettes des utilisateurs et les empêcher de devenir des membres d’un groupe, sélectionnez les utilisateurs et cliquez sur **Unregister Users (Annuler l’enregistrement des utilisateurs)**, puis sélectionnez **Registration Source (Source d’enregistrement)** et **Tags (Étiquettes)**.

Colonne des groupes d’utilisateurs dynamiques	Description
	• Lorsque vous avez terminer de vérifier ou de modifier la liste des utilisateurs du groupes d’utilisateurs dynamiques, cliquez sur **Close (Fermer)**.

Objets > Applications

Les rubriques suivantes décrivent la page **Applications**.

Que voulez-vous faire ?	Reportez-vous à la section
Comprendre les paramètres et les attributs de l'application affichés sur la page Applications.	Présentation des applications Actions prises en charge sur les applications
Ajouter une nouvelle application ou modifier une application existante.	Définition des applications

Présentation des applications

La page Applications dresse la liste des divers attributs de chaque définition d'application, tels que le risque relatif pour la sécurité que présente l'application (de 1 à 5). Le risque est évalué sur des critères tels que la capacité de l'application à partager des fichiers, le fait qu'elle soit sujette à une utilisation frauduleuse ou tente de contourner les pare-feu. Plus la valeur est élevée, plus le risque est important.

La partie supérieure de la page affiche une liste des attributs que vous pouvez utiliser pour filtrer la liste, comme illustré ci-dessous. Le nombre à gauche de chaque entrée représente le nombre total d'applications dotées de cet attribut.

Toutes les semaines, le contenu affiche de nouveaux décodeurs et contextes pour lesquels vous pouvez développer des signatures.

Le tableau suivant décrit les détails de l'application (les applications personnalisées et les applications de Palo Alto® Networks peuvent afficher certains ou tous ces champs).

Détails de l'application	Description
Nom	Nom de l'application.
Description	Description de l'application (255 caractères maximum).
Informations complémentaires	Liens vers des sources en ligne (Wikipédia, Google et Yahoo!) qui présentent des informations supplémentaires sur l'application.

Détails de l’application	Description
Ports standard	Ports que l'application utilise pour communiquer avec le réseau.
Dépend de	Liste d'autres applications qui sont nécessaires pour que cette application fonctionne. Lors de la création d'une règle de politique pour autoriser l'application sélectionnée, vous devez aussi vérifier que vous autorisez toutes les autres applications dont l'application dépend.
Utilise implicitement	Les autres applications dont dépend l’application sélectionnée, mais que vous n’avez pas besoin d’ajouter à vos règles de politique de Sécurité pour autoriser l’application sélectionnée, car ces applications sont implicitement prises en charge.
Précédemment identifié en tant que	Pour les nouveaux App-ID™ ou les App-ID ayant été modifiés, cet élément indique que l’application a été précédemment identifiée en tant que. Il vous permet d'évaluer si une politique doit être modifiée en fonction des modifications apportées à l'application. Si un App-ID est désactivé, les sessions associées à cette application vont correspondre à la politique de l'application précédemment identifiée. De même, les App-ID désactivés vont apparaître dans les journaux tels qu'ils étaient précédemment identifiés dans l'application.
Refuser l'action	Les App-ID sont développés avec une action de refus par défaut qui dicte la manière dont le pare-feu répond lorsque l'application est incluse dans une règle de politique de sécurité avec une action de refus. L'action de refus par défaut peut indiquer un blocage silencieux ou une réinitialisation TCP. Vous pouvez appliquer un contrôle prioritaire sur cette action par défaut dans la politique de Sécurité.
Caractéristiques	
Évasif	Utilise un port ou un protocole dans un but autre que celui visé initialement et dans l'espoir qu'il traverse un pare-feu.
Bande passante excessive	Utilise de manière régulière 1 Mbit/s minimum dans des conditions normales d'utilisation.
Sujet à une utilisation frauduleuse	Généralement utilisé à des fins malveillantes ou peut être facilement configuré afin d'exposer d'autres utilisateurs en plus de celui visé.
SaaS	Sur le pare-feu, le SaaS (Software as a Service/logiciel à la demande) se caractérise comme service sur lequel le fournisseur de services de l'application détient et gère le logiciel et l'infrastructure mais sur lequel vous gardez un contrôle intégral sur les données, y compris les personnes pouvant créer, accéder, partager et transférer ces données. N'oubliez pas que dans le contexte de caractérisation d'une application, les applications SaaS sont différentes des services Web.

Détails de l’application	Description
	Les services Web sont des applications hébergées dont l'utilisateur n'est pas propriétaire des données (par exemple, Pandora) ou dont le service consiste principalement à partager des données fournies par de nombreux abonnés à des fins sociales (par exemple : LinkedIn, Twitter ou Facebook).
Peut transférer des fichiers	Est en mesure de transférer un fichier entre deux systèmes d'un réseau.
Véhicule d'autres applications	Est en mesure de transporter d'autres applications sur son protocole.
Utilisé par un logiciel malveillant	Un programme malveillant est connu pour utiliser l'application à des fins de propagation, d'attaque ou de vol de données ou est intégré à un programme malveillant.
Contient des vulnérabilités connues	Comporte des vulnérabilités rendues publiques.
Répandue	Concerne plus de 1000000 d'utilisateurs.
Poursuivre l’analyse d’autres applications	Indique au pare-feu de continuer à essayer de faire correspondre d'autres signatures d'applications. Si cette option n'est pas sélectionnée, le pare-feu arrêtera de rechercher des correspondances pour l'application dès la première mise en correspondance de la signature.
Caractéristiques SaaS	
Violations des données	Applications qui pourraient avoir divulgué des informations sécurisées à une source non fiables au cours des trois dernières années.
Conditions d'utilisation insuffisantes	Applications offrant de piètres modalités de service qui pourraient compromettre les données de l’entreprise.
Absence de certification	Applications dont la conformité aux programmes ou aux certifications du section, comme SOC1, SOC2, SSAE16, PCI, HIPAA, FINRAA ou FEDRAMP est insuffisante.
Faible viabilité financière	Applications qui pourraient cesser leurs activités au cours des 18 à 24 prochains mois.
Aucune restriction IP	Applications sans restrictions IP pour l’accès utilisateur.
par application	
Catégorie	La catégorie de l'application sera l'une des suivantes :

Détails de l’application	Description
	• systèmes professionnels • collaboration • Internet grand public • multimédia • Mise en réseau • inconnue
Sous-catégorie	Sous-catégorie dans laquelle l'application est classée. Différentes catégories contiennent différentes sous-catégories qui lui sont associées. Par exemple, les sous-catégories de la catégorie Collaboration contiennent E-mail, Partage de fichiers, Messagerie instantanée, Conférence par Internet, Entreprise sociale, Réseau social, Vidéo VoIP et Annonce Web. Alors que les sous-catégories de la catégorie Systèmes professionnels contiennent Service d'autorisation, Base de données, CRM ERP, Activité générale, Gestion, Programmes de bureaux, Mise à jour logicielle et Sauvegarde de la mémoire.
Technologie	La technologie de l'application sera l'une des suivantes : • client/serveur : Une application qui utilise un modèle client/serveur dans lequel un ou plusieurs clients communiquent avec un serveur du réseau. • protocole réseau : Une application qui est généralement utilisée pour la communication entre systèmes et qui simplifie le fonctionnement du réseau. Ceci inclut la plupart des protocoles IP. • poste à poste : Une application qui communique directement avec d'autres clients pour transférer des informations, plutôt que de recourir à un serveur central, afin de simplifier la communication. • basé sur navigateur : Une application dont le fonctionnement dépend d'un navigateur Web.
Risque	Risque affecté à l'application. Pour personnaliser ce paramètre, cliquez sur le lien **Personnaliser**, saisissez une valeur (entre 1 et 5) et cliquez sur **OK**.
Étiquettes	Étiquettes attribuées à une application. **Modifier les étiquettes** pour ajouter ou supprimer les étiquettes attribuées à une application.
Options	
Délai d'expiration de la session	Délai, en secondes, au bout duquel la session de l'application expire en cas d'inactivité (plage allant de 1 à 604 800 secondes). Ce délai

Détails de l’application	Description
	d'expiration concerne les protocoles autres que TCP ou UDP. Pour ces derniers, reportez-vous aux lignes suivantes dans ce tableau. Pour personnaliser ce paramètre, cliquez sur le lien **Personnaliser**, saisissez une valeur et cliquez sur **OK**.
Délai d'attente TCP (secondes)	Délai d'expiration, en secondes, requis pour mettre fin au débit d'une application TCP (plage allant de 1 à 604 800 secondes). Pour personnaliser ce paramètre, cliquez sur le lien **Personnaliser**, saisissez une valeur et cliquez sur **OK**. Une valeur de 0 indique que le minuteur de session général sera utilisé, à savoir 3 600 secondes pour TCP.
Délai d'attente UDP (secondes)	Délai d'expiration, en secondes, requis pour mettre fin au débit d'une application UDP (plage allant de 1 à 604 800 secondes). Pour personnaliser ce paramètre, cliquez sur le lien **Personnaliser**, saisissez une valeur et cliquez sur **OK**.
Délai d'attente des sessions TCP à moitié fermées (en secondes)	Durée maximale, en secondes, pendant laquelle une session reste dans la table des sessions, entre la réception du premier paquet FIN et celle du second paquet FIN ou RST. Si le délai expire, la session sera fermée (plage allant de 1 à 604 800 secondes). Par défaut : si ce délai n'est pas configuré au niveau de l'application, le paramètre global est utilisé. Si cette valeur est configurée au niveau de l'application, elle appliquera un contrôle prioritaire sur le paramètre **Délai d'attente des sessions TCP à moitié fermées** Réglage.
Délai d'attente des sessions TCP (en secondes)	Durée maximale, en secondes, pendant laquelle une session reste dans la table des sessions, après la réception du second paquet FIN ou RST. Si le délai expire, la session sera fermée (plage allant de 1 à 600 secondes). Par défaut : si ce délai n'est pas configuré au niveau de l'application, le paramètre global est utilisé. Si cette valeur est configurée au niveau de l'application, elle appliquera un contrôle prioritaire sur le paramètre **Délai d'attente des sessions TCP** Réglage.
compatible App-ID	Indique si l'App-ID est activé ou désactivé. Si un App-ID est désactivé, le trafic de cette application sera traité comme l'App-ID **Précédemment identifié en tant que** dans la politique de sécurité et dans les journaux. Pour les applications ajoutées après la version 490 du contenu, vous pouvez les désactiver pendant que vous passez en revue l'impact de la politique de la nouvelle application. Après avoir passé en revue la politique, vous pouvez **activer** l'App-ID.

Détails de l’application	Description
	Vous pouvez également **désactiver** une application que vous avez précédemment activée. Sur un pare-feu en mode multi-vsys, vous pouvez désactiver les App-ID séparément dans chaque système virtuel.

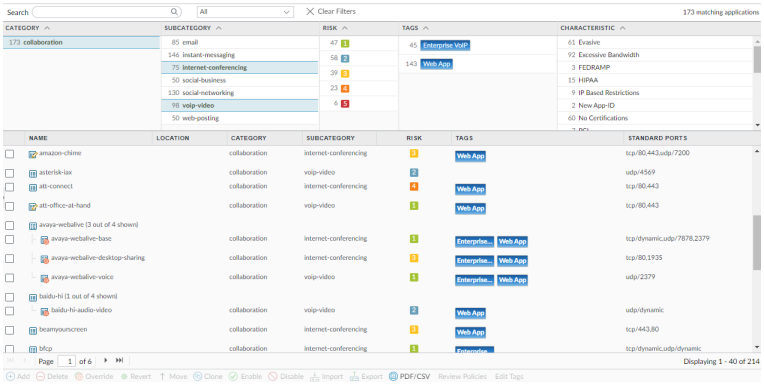
Lorsque le pare-feu n'est pas capable d'identifier une application à l'aide de l'App-ID, le trafic sera classé comme inconnu (« unknown ») : « unknown-tcp » ou « unknown-udp ». Ce comportement s'applique à toutes les applications inconnues, à l'exception de celles qui émule complètement le protocole HTTP. Pour en savoir plus, reportez-vous à la section Surveillance > Botnet.

Vous pouvez créer de nouvelles définitions pour les applications inconnues, puis définir des politiques de sécurité correspondantes. En outre, les applications qui nécessitent les mêmes paramètres de sécurité peuvent être combinées en groupe d'applications pour simplifier la création des politiques de sécurité.

Actions prises en charge sur les applications

Sur cette page, vous pouvez effectuer les actions suivantes :

Actions prises en charge pour les applications	Description
Filtrer par application	• Pour rechercher une application spécifique, saisissez le nom ou la description de l’application dans le champ **Rechercher** et appuyez sur **Entrée**. La liste déroulante vous permet de rechercher et de filtrer une application donnée ou d’afficher **Toutes** les applications, les **applications personnalisées**, les **applications désactivées** ou les **applications étiquetées**. L’application apparaît dans la liste et les colonnes de filtrage sont mises à jour pour afficher des statistiques relatives aux applications qui correspondent à la recherche. La recherche fonctionne avec des chaînes partielles. Lorsque vous définissez des politiques de sécurité, vous pouvez rédiger des règles qui s’appliquent à toutes les applications correspondant à un filtre sauvegardé. Ces règles sont mises à jour de manière dynamique lorsqu’une nouvelle application est ajoutée par le biais d’une mise à jour du contenu qui correspond au filtre. • Pour filtrer par attributs de l’application affichés sur la page, cliquez sur un élément qui servira de base pour le filtrage. Par exemple, pour limiter la liste à la catégorie Collaboration, cliquez

Actions prises en charge pour les applications	Description
	sur **Collaboration**pour que la liste n'affiche que les applications correspondantes.  • Pour filtrer la liste en fonction d'autres colonnes, sélectionnez une entrée dans ces colonnes. Le filtrage est appliqué selon un ordre précis : Les filtres Catégorie sont appliqués en premier, suivis des filtres Sous-catégorie, puis des filtres Technologie et, enfin, des filtres Caractéristiques. Par exemple, si vous appliquez les filtres Catégorie, Sous-catégorie et Risque, la colonne Technologie sera automatiquement limitée aux technologies correspondant aux catégories et sous-catégories sélectionnées, même si un filtre Technologie n'est pas explicitement appliqué. Lorsque vous appliquez un filtre, la liste des applications sera automatiquement mise à jour. Pour créer un nouveau filtre d'application, voir Objets > Filtres d'application.
Ajouter une nouvelle application.	Pour ajouter une nouvelle application, reportez-vous à la section Définition des applications.
Afficher ou personnaliser les détails de l'application.	Cliquez sur le lien du nom de l'application pour afficher la description de l'application, y compris le port standard et les caractéristiques de l'application ainsi que le risque. Pour plus d'informations sur les paramètres de l'application, consultez la section Définition des applications. Si l'icône située à gauche du nom de l'application comporte un crayon jaune (), l'application est une application personnalisée.
Désactiver une application	Vous pouvez **Désactiver** une application (ou plusieurs applications) de sorte que la signature de l'application ne corresponde pas au trafic. Les règles de sécurité définies pour bloquer, autoriser ou mettre en œuvre une application correspondante ne sont pas appliquées au trafic de l'application si celle-ci est désactivée. Vous pouvez choisir de désactiver une application incluse avec une nouvelle version du contenu car la

Actions prises en charge pour les applications	Description
	mise en œuvre de la politique dans l'application risque de changer lorsque celle-ci est uniquement identifiée. Par exemple, le pare-feu autorise une application identifiée en tant que trafic de type navigation Web avant l'installation d'une nouvelle version du contenu ; après avoir installé la mise à jour du contenu, l'application uniquement identifiée ne correspondra plus à la règle de Sécurité autorisant le trafic de type navigation Web. Dans ce cas, vous pouvez choisir de désactiver l'application afin que le trafic correspondant à la signature de l'application continue d'être classé en tant que trafic de type navigation Web et soit autorisé.
Activer une application	Vous pouvez sélectionner une application désactivée et l'**Activer** de sorte que le pare-feu puisse gérer l'application conformément à vos politiques de sécurités configurées.
Importer une application	Pour importer une application, cliquez sur **Importer**. Accédez au fichier et sélectionnez le système virtuel cible dans la liste déroulante **Destination**.
Exporter une application	Pour exporter une application, sélectionnez cette option correspondant à l'application et cliquez sur **Exporter**. Suivez les instructions pour sauvegarder le fichier.
Exporter un tableau de configuration des applications.	Exportez les informations sur les applications au format **PDF/CSV**. Seules les colonnes qui sont visibles dans l'interface Web sont exportées. Consultez la section Exportation des données du tableau de configuration.
Évaluer l'impact des politiques après l'installation d'une nouvelle version du contenu	Il est nécessaire de **Réviser les politiques** pour évaluer la mise en œuvre basée sur les politiques pour les applications avant et après l'installation d'une version du contenu. La boîte de dialogue Évaluer les politiques permet d'évaluer l'impact d'une politique sur les nouvelles applications incluses dans une version téléchargée du contenu. Cette boîte de dialogue vous permet d'ajouter ou de supprimer une application en attente (une application téléchargée avec une version du contenu, mais qui n'est pas installée sur le pare-feu) dans ou depuis une règle de politique de Sécurité existante. Les modifications apportées aux politiques d'applications en attente ne seront effectives qu'après avoir installé la version du contenu correspondant. Vous pouvez également accéder à la boîte de dialogues Réviser les politiques lors du téléchargement et de l'installation de versions de contenu sur la page **Périphérique** > **Mises à jour dynamiques**.
Étiqueter une application	Une étiquette prédéfinie nommée **approuvée** est disponible pour que vous étiquetiez des applications SaaS. Bien qu'une application SaaS soit identifiée en tant que **Saas=oui** dans caractéristiques de l'application,

Actions prises en charge pour les applications	Description
	vous pouvez utiliser l'étiquette approuvée pour n'importe quelle application. *Étiquetez l'application en tant que **approuvée** pour permettre de distinguer le trafic des applications SaaS approuvées du trafic des applications SaaS non approuvées, par exemple, lorsque vous examinez le rapport d'utilisation d'application SaaS ou lorsque vous évaluez les applications sur votre réseau.* Sélectionnez une application, cliquez sur **Modifier les étiquettes** et à partir de la liste déroulante, sélectionnez l'étiquette **approuvée** prédéfinie pour identifier toute application que vous souhaitez explicitement autoriser sur votre réseau. Lorsque vous générez le rapport d'utilisation de l'application SaaS (voir Surveillances > Rapports au format PDF > Utilisation de l'application SaaS), vous pouvez comparer les statistiques sur l'application que vous avez approuvée par rapport aux applications SaaS non approuvées qui sont utilisées sur votre réseau. Lorsque vous étiquetez une application comme étant approuvée, les restrictions suivantes s'appliquent : • L'étiquette Approuvée ne peut être appliquée à un groupe d'applications. • L'étiquette Approuvée ne peut être appliquée au niveau **Partagé** ; vous ne pouvez étiqueter une application que par groupe de périphériques ou par système virtuel. • L'étiquette Approuvée ne peut être utilisée pour étiqueter des applications comprises dans une application incorporante, comme facebook-mail, qui fait partie de l'application incorporante Facebook. Vous pouvez également **Supprimer l'étiquette** ou **Appliquer un remplacement sur l'étiquette**. L'option remplacement n'est offerte que sur un pare-feu qui a hérité de paramètres d'un groupe de périphériques qui ont été transmis par Panorama.

Définition des applications

Sélectionnez **Objets** > **Applications** pour **Ajouter** une nouvelle application personnalisée à évaluer par le pare-feu lors de l'exécution de politiques.

Paramètres de la nouvelle application	Description
Onglet Configuration	

Paramètres de la nouvelle application	Description
Nom	Saisissez le nom de l’application (31 caractères maximum). Ce nom apparaît dans la liste d'applications lors de la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. N'utilisez que des lettres, des chiffres, des espaces, des points, des tirets et des caractères de soulignement. Le caractère final doit être une lettre.
Partagé	Sélectionnez cette option si vous souhaitez que l'application soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, l'application sera uniquement disponible pour le **Système virtuel** sélectionné dans l'onglet **Objets**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, l'application sera uniquement disponible pour le **Groupe de périphériques** sélectionné dans l'onglet **Objets**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de cet objet applicatif pour les groupes de périphériques qui héritent de l’objet. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l’objet.
Description	Saisissez une description de l'application à titre de référence générale (255 caractères maximum).
Catégorie	Sélectionnez la catégorie de l'application, par exemple **courrier électronique** ou **base de données**. La catégorie est utilisée pour générer le diagramme du Top 10 des catégories d’applications et à des fins de filtrage (reportez-vous à la section ACC).
Sous-catégorie	Sélectionnez la sous-catégorie de l'application, par exemple **courrier électronique** ou **base de données**. La sous-catégorie est utilisée pour générer le diagramme du Top 10 des catégories d’applications et à des fins de filtrage (reportez-vous à la section ACC).
technologies	Sélectionnez la technologie de l'application. Par défaut, la colonne Technologie n’est pas affichée. **Afficher la colonne Technologie** pour sélectionner les technologies à ajouter à votre filtre d’application.
App parent	Désignez une application parent pour cette application. Ce paramètre s'applique lorsqu'une session correspond à la fois à l'application parent et à l'application personnalisée'A0;; toutefois, l'application personnalisée est reportée car elle est plus spécifique.
Risque	Sélectionnez le niveau de risque associé à cette application (1 = le plus faible, 5 = le plus élevé).

Paramètres de la nouvelle application	Description
Caractéristiques	Sélectionnez les caractéristiques de l'application qui peuvent présenter un risque pour cette dernière. Pour obtenir une description de chaque caractéristique, reportez-vous à la section Caractéristiques.
Onglet Avancé	
Port	Si l'application utilise le protocole TCP et/ou UDP, sélectionnez **Port** et saisissez une ou plusieurs combinaisons de protocole et de numéro de port (une entrée par ligne). Le format courant est : *<protocol>/<port>* où le *<port>* est un numéro de port unique, ou **dynamique** en cas d'attribution de port dynamique. Exemples : TCP/dynamic ou UDP/32. Ce paramètre est appliqué lors de l'utilisation de la valeur **app-défaut** dans la colonne Service d'une règle de sécurité.
Protocole IP	Pour indiquer un protocole IP autre que TCP ou UDP, sélectionnez **IP Protocol (Protocole IP)** et saisissez le numéro de protocole (de 1 à 255).
Type ICMP	Pour spécifier un type Internet Control Message Protocol version 4 (ICMP), sélectionnez **ICMP Type (Type ICMP)** et saisissez le numéro de type (plage 0-255).
Type ICMP6	Pour spécifier un type ICMPv6 (Internet Control Message Protocol/ protocole de message de contrôle Internet version 6), sélectionnez **ICMP6 Type (Type ICMP6)** et saisissez le numéro de type (plage 0-255).
None	Pour spécifier des signatures indépendantes de tout protocole, sélectionnez **Aucun**.
délai d'expiration	Saisissez le nombre de secondes avant l'arrêt d'un flux d'application inactif (intervalle compris entre 0 et 604 800 secondes). La valeur 0 indique que le délai avant expiration par défaut de l'application est utilisé. Cette valeur est utilisée pour les protocoles autres que TCP et UDP dans tous les cas et pour les délais d'attente TCP et UDP lorsque ces derniers ne sont pas définis.
Délai d'attente TCP	Saisissez le nombre de secondes avant l'arrêt d'un flux d'application TCP inactif (intervalle compris entre 0 et 604 800 secondes). La valeur 0 indique que le délai avant expiration par défaut de l'application est utilisé.

Paramètres de la nouvelle application	Description
Délai d'attente UDP	Saisissez le nombre de secondes avant l'arrêt d'un flux d'application UDP inactif (intervalle compris entre 0 et 604 800 secondes). La valeur 0 indique que le délai avant expiration par défaut de l'application est utilisé.
Délai d'attente des sessions TCP à moitié fermées	Saisissez la durée maximale pendant laquelle une session reste dans la table des sessions, entre la réception du premier FIN et celle du second FIN ou RST. Si le délai expire, la session est fermée. Par défaut : Si ce délai n'est pas configuré au niveau de l'application, le paramètre global est utilisé (intervalle compris entre 1 et 604 800 secondes). Si cette valeur est configurée au niveau de l'application, elle appliquera un contrôle prioritaire sur le paramètre global Délai d'attente des sessions TCP à moitié fermées.
Délai d'attente des sessions TCP en état time_wait	Saisissez la durée maximale pendant laquelle une session reste dans la table des sessions, après la réception du second FIN ou RST. Si le délai expire, la session est fermée. Par défaut : Si ce délai n'est pas configuré au niveau de l'application, le paramètre global est utilisé (intervalle compris entre 1 et 600 secondes). Si cette valeur est configurée au niveau de l'application, elle appliquera un contrôle prioritaire sur le paramètre global Délai d'attente des sessions TCP en état time_wait.
Analyse en cours	Sélectionnez les types d'analyse que vous voulez autoriser, en fonction des profils de sécurité (types de fichier, modèles de données et virus).
Onglet Signatures	
Signatures	Cliquez sur **Ajouter** pour ajouter une nouvelle signature, et renseignez les informations suivantes : • **Nom de la signature** - Saisissez un nom permettant d'identifier la signature. • **Commentaire** - Saisissez une description (facultatif). • **Correspondance de l'état ordonné** - Indiquez si l'ordre dans lequel les conditions de la signature sont définies a son importance. • **capacité** - Indiquez s'il faut appliquer cette signature à la **Transaction** en cours seulement pendant toute la **Session** utilisateur. Précisez les conditions qui identifient la signature. Ces conditions servent à générer la signature que le pare-feu utilise pour faire correspondre les modèles de l'application et contrôler le trafic :

Paramètres de la nouvelle application	Description
	• Pour ajouter une condition, sélectionnez **Ajouter une condition AND** ou **Ajouter une condition OR**. Pour ajouter une condition au sein d'un groupe, sélectionnez-le puis cliquez sur **Ajouter une condition**. • Sélectionnez un **Opérateur** dans la liste déroulante. Les options sont les suivantes : **Correspondance des modèles**, **Supérieur à**, **Inférieur à** et **Egal à**, et précisez les options suivantes : (Pour la correspondance des modèles uniquement) • **Contexte** - Choisissez parmi les contextes disponibles. Ces contextes sont mis à jour à l'aide des mises à jour de contenu dynamiques. • **Modèle** - Indiquez une expression régulière pour préciser des valeurs de chaîne uniques qui s'appliquent à l'application personnalisée.  *Exécutez une capture de paquets pour identifier le contexte. Reportez-vous à la section* Syntaxe des règles des modèles *pour connaître les règles concernant les expressions régulières.* (Pour les options Supérieur à, Inférieur à) • **Contexte** - Choisissez parmi les contextes disponibles. Ces contextes sont mis à jour à l'aide des mises à jour de contenu dynamiques. • **Valeur** - Précisez une valeur pour la mise en correspondance (intervalle compris entre 0 et 4 294 967 295). • **Qualificatif et Valeur** - (Facultatif) Ajoutez des paires qualificatif/valeur. (Pour l'option Égal à uniquement) • **Contexte** – Sélectionnez parmi les requêtes inconnues et les réponses pour le protocole TCP ou UDP (par exemple, unknown-

Paramètres de la nouvelle application	Description
	req-tcp) ou parmi les autres contextes disponibles via les mises à jour du contenu dynamiques (par exemple, dnp3-req-func-code). Pour les requêtes inconnues et les réponses pour le protocole TCP ou UDP, précisez : • **Position** - Faites votre choix parmi les quatre premiers ou les quatre seconds octets de la charge utile. • **Mask (Masque)** - Renseignez une valeur hexadécimale 4 octets, par exemple 0xffffff00. • **Valeur** - Renseignez une valeur hexadécimale 4 octets, par exemple 0xaabbccdd. Pour tous les autres contextes, précisez une **Valeur** qui est pertinente à l'application. Pour déplacer une condition au sein d'un groupe, sélectionnez la condition et cliquez sur la flèche **Déplacer en haut** ou **Déplacer en bas**. Pour déplacer un groupe, sélectionnez-le et cliquez sur la flèche **Déplacer en haut** ou **Déplacer en bas**. Vous ne pouvez pas déplacer les conditions d'un groupe vers un autre.

Il n'est pas nécessaire de définir des signatures pour l'application si celle-ci est utilisée uniquement dans des règles de contrôle prioritaire sur l'application.

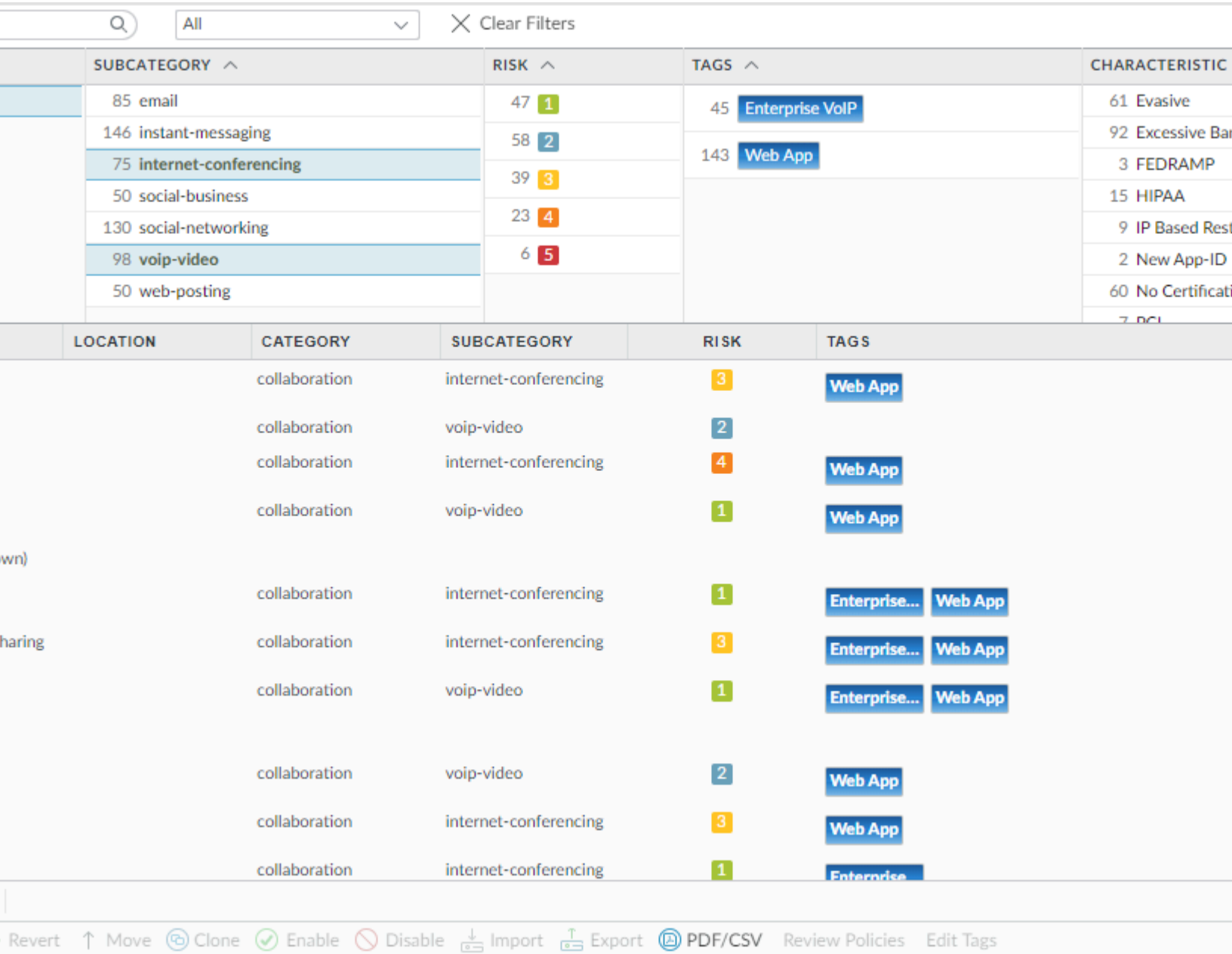
Objets > Groupes d'applications

Pour simplifier la création de politiques de sécurité, les applications qui requièrent les mêmes paramètres de sécurité peuvent être combinées en créant un groupe d’applications. (Pour définir une nouvelle application, reportez-vous à la section Définition des applications.)

Paramètres du nouveau groupe d’applications	Description
Name (Nom)	Saisissez un nom qui décrit le groupe d'applications (31 caractères maximum). Ce nom apparaît dans la liste d'applications lors de la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement.
Partagé	Sélectionnez cette option si vous souhaitez que le groupe d'applications soit disponible pour : Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le groupe d'applications sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le groupe d'applications sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de cet objet de groupe d’applications dans les groupes de périphériques qui héritent de l’objet. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l’objet.
Applications	Cliquez sur **Add (Ajouter)** et sélectionnez des applications, des filtres d'applications et/ou d'autres groupes d'applications à inclure dans ce groupe.

Objets > Filtres d'applications

Les filtres d’application permettent de simplifier les recherches répétées. Pour définir un filtre d’application, vous devez **Ajouter** et saisir un nom pour votre nouveau filtre. Dans la partie supérieure de la fenêtre, cliquez sur un élément qui servira de base pour le filtrage. Par exemple, pour limiter la liste à la catégorie Collaboration, cliquez sur **collaboration**.



Pour filtrer la liste en fonction d'autres colonnes, sélectionnez une entrée dans ces colonnes. Le filtrage est successif : d'abord par catégorie, suivi du filtrage par sous-catégorie, par technologie, par risque, par étiquette et enfin par caractéristique.

Lorsque vous sélectionnez les filtres, la liste des applications qui s’affichent sur la page est automatiquement mise à jour.

Objets > Services

Lorsque vous définissez des politiques de Sécurité pour des applications spécifiques, vous pouvez sélectionner un ou plusieurs services pour limiter les numéros de ports que les applications peuvent utiliser. Le service par défaut est **indifférent**, ce qui autorise tous les ports TCP et UDP. Les services HTTP et HTTPS sont prédéfinis, mais vous pouvez ajouter des définitions supplémentaires. Les services qui sont souvent affectés ensemble peuvent être combinés en groupe de services pour simplifier la création de politiques de sécurité (reportez-vous à la section Objects > Service Groups (Objets > Groupes de services)).

Par ailleurs, vous pouvez utiliser ces objets de services pour définir des délai d'expiration de session selon le service, ce qui veut dire que vous pouvez appliquer différents délai d'expiration à différents groupes d'utilisateurs, et ce, même lorsque ces groupes utilisent le même service TCP ou UDP ou, si vous passez d'une politique de Sécurité basée sur les ports avec applications personnalisées à une politique de Sécurité basée sur les applications, vous pouvez facilement conserver vos délai d'expiration d'applications personnalisés.

Le tableau suivant décrit les paramètres des services'A0;:

Paramètres des services	Description
Name (Nom)	Saisissez un nom pour le service (**63** caractères maximum). Ce nom apparaît dans la liste de services lors de la définition de politiques de Sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Description	Saisissez une description du service (1023 caractères maximum).
Partagé	Sélectionnez cette option si vous souhaitez que l'objet de service soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, l'objet de service sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, l'objet de service sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de cet objet de service dans les groupes de périphériques qui héritent de l'objet. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l'objet.
Protocole	Sélectionnez le protocole utilisé par le service (**TCP** ou **UDP**).

Paramètres des services	Description
Port de destination	Saisissez le numéro de port de destination (de 0 à 65535) ou la plage de numéros de ports (port1-port2) utilisé(e) par le service. Utilisez des virgules pour séparer les ports ou les plages. Le port de destination doit être renseigné.
Port source	Saisissez le numéro de port source (de 0 à 65535) ou la plage de numéros de ports (port1-port2) utilisé(e) par le service. Utilisez des virgules pour séparer les ports ou les plages. Le port source est facultatif.
Délai d'expiration de la session	Définissez le délai d'expiration de la session pour le service : • **Inherit from application (Hériter de l'application)** (par défaut) : aucun délai d'expiration basé sur le service n'est appliqué ; c'est le délai d'expiration des applications qui est appliqué. • **Override (Exercer un contrôle prioritaire)** : définissez un délai d'expiration de la session personnalisé pour le service. Continuez à renseigner les champs Délai d'expiration TCP, Délai d'attente des sessions TCP à moitié fermées et Délai d'attente TCP.
Les paramètres suivants ne s'affichent que si vous choisissez de remplacer les délais d'expiration des applications et de créer des délais d'expiration de session personnalisés pour un service :	
Délai d'attente TCP	Définissez la durée maximale, en secondes, pendant laquelle une session TCP peut demeurer ouverte après le début de la transmission des données. Lorsque ce délai expire, la session est fermée. La plage est comprise entre 1 et 604 800. La valeur par défaut est de 3 600 secondes.
Délai d'attente des sessions TCP à moitié fermées	Définissez la durée maximale, en secondes, pendant laquelle une session demeure ouverte lorsqu'un seul côté de la connexion a tenté de mettre fin à la connexion. Ce paramètre s'applique à : • La période de temps après que le pare-feu a reçu le premier paquet FIN (ce qui indique qu'un côté de la connexion tente de mettre fin à la session), mais avant qu'il ne reçoive le second paquet FIN (ce qui indique que l'autre côté de la connexion met fin à la session) • La période de temps avant la réception d'un paquet RST (ce qui indique une tentative de rétablir la connexion). Si le délai expire, la session est fermée. La plage est comprise entre 1 et 604 800. La valeur par défaut est de 120 secondes.
Délai d'attente TCP	Définissez la durée maximale, en secondes, pendant laquelle une session demeure ouverte après la réception du second paquet FIN requis pour

Paramètres des services	Description
	mettre fin à la session ou après réception d’un paquet RST visant à rétablir une connexion. Lorsque le délai expire, la session est fermée. La plage est comprise entre 1 et 600. La valeur par défaut est de 15 secondes.

Objets > Groupes de services

Pour simplifier la création de politiques de sécurité, vous pouvez combiner les services qui disposent des mêmes paramètres de sécurité en groupes de services. Pour définir de nouveaux services, reportez-vous à la section Objets > Services.

Le tableau suivant décrit les paramètres des groupes de services'A0;:

Paramètres des groupes de services	Description
Name (Nom)	Saisissez un nom pour le groupe de services (**63** caractères maximum). Ce nom apparaît dans la liste de services lors de la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Partagé	Sélectionnez cette option si vous souhaitez que le groupe de services soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le groupe de services sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le groupe de services sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de cet objet de groupe de service dans les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l'objet.
Service (Service)	Cliquez sur **Add (Ajouter)** pour ajouter des services au groupe. Faites votre sélection dans la liste déroulante ou cliquez sur **Service** en bas de la liste déroulante et renseignez les paramètres. Reportez-vous à la section Objets > Services pour obtenir une description des paramètres.

Objets > Étiquettes

Les étiquettes vous permettent de regrouper des objets à l'aide de mots-clés ou d'expressions. Vous pouvez appliquer des étiquettes à des objets d'adresse, à des groupes d'adresses (statiques et dynamiques), à des applications, à des zones, à des services, à des groupes de services et à des règles de politique. Vous pouvez aussi utiliser un profil d'interface SD-WAN pour appliquer une étiquette de liens à une interface Ethernet. Vous pouvez utiliser des étiquettes pour trier ou filtrer des objets, mais aussi pour distinguer visuellement des objets selon leurs couleurs. Lorsque vous appliquez une couleur à une étiquette, l'onglet **Policy (Politique)** affiche l'objet avec sa couleur d'arrière-plan.

Vous devez créer une étiquette avant de pouvoir regrouper des règles à l'aide de cette étiquette. Après avoir affecté des règles regroupées par étiquette, **View Rulebase as Groups (Afficher la base de règles en tant que groupes)** pour afficher une représentation visuelle de votre base de règles de politique selon les étiquettes affectées. Lorsque vous affichez votre base de règles en tant que groupes, l'ordre de la politique et la priorité sont maintenus. Dans cette vue, sélectionnez l'étiquette de groupe pour afficher toutes les règles groupées en fonction de cette étiquette.

Une étiquette prédéfinie nommée **Sanctioned (Sanctionné)** est disponible pour les applications d'étiquetage (**Objects (Objets)** > **Applications**). Ces étiquettes sont requises pour suivre avec précision (Surveillance > Rapports PDF> Utilisation de l'application SaaS).

Que voulez-vous savoir ?	Reportez-vous à la section :
Comment créer des étiquettes ?	Création d'étiquettes
Comment puis-je afficher la base de règles en tant que groupes ?	Afficher la base de règles en tant que groupes
Rechercher des règles contenant des étiquettes. Regrouper des règles en utilisant des étiquettes. Afficher les étiquettes d'une politique. Appliquer les étiquettes à la politique.	Gestion des étiquettes
Vous souhaitez en savoir plus ?	• Utilisation d'étiquettes pour regrouper et distinguer visuellement les objets • SD-WAN Link Tag (Étiquette de liens SD-WAN)

Création d'étiquettes

- **Objets** > **Étiquettes**

Sélectionnez **Étiquettes** pour créer une étiquette, affecter une couleur ou supprimer, renommer et cloner des étiquettes. Chaque objet peut comporter jusqu'à 64 étiquettes ; lorsqu'un objet dispose de plusieurs étiquettes, il affiche la couleur de la première étiquette appliquée.

Sur le pare-feu, l'onglet **Étiquettes** affiche les étiquettes que vous avez définies localement sur le pare-feu ou transférées depuis Panorama vers le pare-feu. Sur Panorama, l'onglet **Étiquettes** affiche les étiquettes que vous définissez sur Panorama. Cet onglet n'affiche pas les étiquettes qui sont dynamiquement récupérées des sources d'informations VM définies sur le pare-feu pour former des groupes d'adresses dynamiques et n'affiche pas les étiquettes qui sont définies à l'aide de l'API XML ou REST.

Lorsque vous créez une nouvelle étiquette, elle est automatiquement créée dans le système virtuel ou dans le groupe de périphériques actuellement sélectionné sur le pare-feu ou sur Panorama.

Paramètres des étiquettes	Description
Nom	Saisissez un nom de tag unique (127 caractères maximum). Ce nom n'est pas sensible à la casse.
Partagé	Sélectionnez cette option si vous souhaitez que l'étiquette soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, l'étiquette est uniquement disponible pour le **Système virtuel** sélectionné dans l'onglet **Objets**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez (décochez) cette option, l'étiquette sera uniquement disponible pour le **Groupe de périphériques** sélectionné dans l'onglet **Objets**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de cette étiquette dans les groupes de périphériques qui héritent de l'étiquette. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l'étiquette.
Couleur	Sélectionnez une couleur de la palette de couleurs dans la liste déroulante (la valeur par défaut est Aucune).
Commentaires	Ajoutez une étiquette ou une description pour décrire l'utilisation à laquelle l'étiquette est destinée.

- Ajouter une étiquette : **Ajoutez** une étiquette, puis remplissez les champs suivants :

  Vous pouvez également créer une nouvelle étiquette lors de la création ou de la modification d'une politique dans l'onglet **Politiques**. L'étiquette est automatiquement créée dans le groupe de périphériques ou dans le système virtuel actuellement sélectionné.
- Modifier une étiquette : Cliquez sur une étiquette pour modifier ou renommer une étiquette ou pour les affecter une couleur.
- Supprimer une étiquette : Cliquez sur **Supprimer**, puis sélectionnez l'étiquette. Vous ne pouvez pas supprimer d'étiquette prédéfinie.

- Déplacer ou cloner une étiquette : Les options permettant de déplacer ou de cloner une étiquette vous permettent de copier une étiquette ou da le déplacer vers un autre Groupe de périphériques ou vers un autre Système virtuel sur les pare-feu pouvant comporter plusieurs systèmes virtuels.

  Déplacez ou clonez et sélectionnez l'étiquette. Sélectionnez l'emplacement de **Destination** (Groupe de périphériques ou Système virtuel). Désélectionnez (clear) l'option **Erreur sortante dès la première erreur détectée lors de la validation** pour que le processus de validation identifie toutes les erreurs de l'objet avant de les afficher. Cette option est activée par défaut, et le processus de validation s'arrête dès la détection de la première erreur et affiche uniquement l'erreur.
- Appliquer un contrôle prioritaire ou Rétablir un étiquette (Panorama uniquement) : L'option **écraser** est disponible uniquement si vous n'aviez pas sélectionné l'option **Désactiver écraser** lors de la création de l'étiquette. L'option **écraser** vous permet d'appliquer un contrôle prioritaire sur la couleur assignée à l'étiquette qui a été héritée d'un groupe de périphériques partagés ou ancêtres. Le champ **Emplacement** correspond au groupe de périphériques actuel. Vous pouvez également **Désactiver écraser** pour empêcher les tentatives ultérieures d'exercer un contrôle prioritaire.

  Annulez les modifications pour annuler les récentes modifications apportées à une étiquette. Lors du rétablissement d'une étiquette, le champ **Remplacement** affiche le groupe de périphériques ou le système virtuel ayant transmis l'étiquette.

Afficher la base de règles en tant que groupes

- **Politiques** > **<Rulebase Type>**

Sélectionnez **View Rulebase as Groups (Afficher la base de règles en tant que groupes)** pour afficher la base de règles de la politique au moyen de l'étiquette de groupe. Lorsque vous affichez votre base de règles en tant que groupes, l'ordre de la politique et la priorité sont maintenus. Dans cette vue, sélectionnez l'étiquette de groupe pour afficher toutes les règles groupées en fonction de cette étiquette.

Lorsque vous affichez votre base de règle en tant que groupes, cliquez sur **Group (Groupe)** pour déplacer, modifier, supprimer ou cloner toutes les règles dans le groupe d'étiquettes sélectionné. Le tableau suivant décrit les options de gestion des règles qui sont disponibles lorsque vous affichez votre base de règle en tant que groupes.

Option	Description
Déplacer les règles du groupe vers une autre base de règles ou un autre groupe de périphériques	Déplace toutes les règles de politique du groupe d'étiquettes sélectionné vers une autre base de règles ou groupe de périphériques.
Modifier le groupe de toutes les règles	Déplace toutes les règles du groupe d'étiquettes sélectionné vers un autre groupe d'étiquettes.
Déplacer toutes les règles du groupe	Déplace toutes les règles du groupe d'étiquettes sélectionné au sein de la base de règles.
Supprimer toutes les règles du groupe	Supprimer toutes les règles du groupe d'étiquettes sélectionné.

Option	Description
Dupliquer toutes les règles du groupe	Dupliquer toutes les règles du groupe d’étiquettes sélectionné.

Déplacer les règles du groupe vers une autre base de règles ou un autre groupe de périphériques

Si vous devez réorganiser votre base de règles, sélectionnez le groupe d’étiquettes qui contient les règles que vous souhaitez déplacer et **Move Rules in Group to Different Rulesbase or Device Group (Déplacez les règles du groupe vers une autre base de règles ou un autre groupe de périphériques)** pour les réaffecter à une autre base de règles ou à un autre groupe de périphériques (plutôt que de déplacer chaque règle individuellement). Le groupe de périphériques doit déjà exister (vous ne pouvez le créer lors du processus) avant de déplacer les règles d’un groupe d’étiquettes vers un autre groupe de périphériques. De plus, vous pouvez déplacer les règles d’un groupe d’étiquettes vers une autre base de règles faisant partie du même groupe de périphériques.

Pour déplacer les règles vers une autre base de règles ou vers un autre groupe de périphériques, saisissez les informations suivantes :

Champ	Description
Destination	Le groupe de périphériques cible pour le déplacement des règles de politique.
(Panorama uniquement) Type de destination	Sélectionnez si vous souhaitez modifier les règles vers la **Pre-Rulebase (Base de règles avant)** ou vers la **Post-Rulebase (Base de règles après)** du groupe de périphériques de destination.
Ordre des règles	Sélectionnez l’endroit de la base de règles où modifier les règles. Vous avez le choix entre les actions suivantes : • **Move Top (Déplacer vers le haut)** : déplacez les règles clonées au haut de la base de règles du groupe de périphériques de destination. • **Move Bottom (Déplacer vers le bas)** : déplacez les règles à la fin de la base de règles du groupe de périphériques de destination. • **Before Rule (Avant la règle)** : déplacez les règles avant la règle sélectionnée de la base de règles du groupe de périphériques de destination. • **After Rule (Après la règle)** : déplacez les règles après la règle sélectionnée de la base de règles du groupe de périphériques de destination.
Erreur sortante dès la première erreur détectée lors de la validation	Cochez la case pour déterminer comment les erreurs décelées au cours de la validation s’affichent. Si elle est cochée, chaque erreur s'affiche individuellement. Si elle est décochée, les erreurs sont groupées et s’affichent en tant qu’une seule erreur.

Champ	Description
	Les erreurs détectées au cours de la validation entraînent l'échec du déplacement. Aucune règle n'est ainsi déplacée dans le groupe de périphériques de destination.

Modifier le groupe de toutes les règles

Plutôt que de modifier chaque règle, **Modifiez le groupe de toutes les règles** pour déplacer un ensemble complet de règles de politique d'un groupe d'étiquettes à un autre groupe d'étiquettes existant. L'ordre des règles au sein du groupe d'étiquettes est maintenu lorsque celles-ci sont déplacées vers le nouveau groupe d'étiquettes. Vous avez toutefois le choix de placer les nouvelles règles devant les règles du groupe d'étiquettes de destination, ou après.

Pour déplacer les règles vers un autre groupe d'étiquettes, précisez le groupe d'étiquettes de destination et l'endroit où placer les règles déplacées.

Champ	Description
Sélectionner un groupe pour son ordre d'apparition	Sélectionnez le groupe d'étiquettes de destination.
Déplacer vers le haut	**Déplacer vers le haut** insère les règles au haut du groupe d'étiquettes de destination.
Déplacer vers le bas	**Déplacer vers le bas** insère les règles au bas du groupe d'étiquettes de destination.

Déplacer toutes les règles du groupe

Plutôt que de réorganiser chaque règle individuellement, **Move All Rules in Group (Déplacer toutes les règles du groupe)** pour déplacer toutes les règles dans le groupe d'étiquettes sélectionné vers le haut ou le bas de la hiérarchie de la règle. L'ordre des règles déplacées au sein du groupe d'étiquettes est maintenu lorsque vous déplacez le groupe d'étiquettes. Vous avez toutefois le choix de placer les règles devant les règles du groupe d'étiquettes de destination, ou après.

Pour déplacer les règles, précisez le groupe d'étiquettes de destination et l'endroit où placer les règles déplacées.

Champ	Description
Sélectionner un groupe pour son ordre d'apparition	Sélectionnez le groupe d'étiquettes de destination.
Déplacer vers le haut	**Move Top (Déplacer vers le haut)** insère les règles avant le groupe d'étiquettes de destination.

Champ	Description
Déplacer vers le bas	**Move botton (Déplacer vers le bas)** insère les règles après le groupe d'étiquettes de destination.

Supprimer toutes les règles du groupe

Pour simplifier la gestion des règles, vous pouvez **Supprimer toutes les règles du groupe** afin de réduire vos risques de sécurité et de maintenir la base de règles de politique organisée en supprimant les règles non voulues ou non utilisées qui sont associées à un groupe d'étiquettes sélectionné.

Dupliquer toutes les règles du groupe

Plutôt que de recréer manuellement des règles de politique existantes dans un groupe d'étiquettes, **Dupliquez toutes les règles du groupe** pour rapidement reproduire les règles du groupe d'étiquettes sélectionné du groupe de périphériques et de la base de règles de votre choix. Le groupe de périphériques doit déjà exister (vous ne pouvez le créer lors du processus) avant de dupliquer les règles d'un groupe d'étiquettes vers un autre groupe de périphériques. De plus, vous pouvez dupliquer les règles d'un groupe d'étiquettes vers une autre base de règles faisant partie du même groupe de périphériques.

Le nom de la règle est ajouté aux règles dupliquées, selon le format suivant : `<Rule Name>-1`. Si une règle dupliquée se trouve au même emplacement que la première règle et que le nom ne change pas, le nom est alors joint. Par exemple, `<Rule Name>-2`, `<Rule Name>-3`, et ainsi de suite.

Pour dupliquer des règles, configurez les champs suivants.

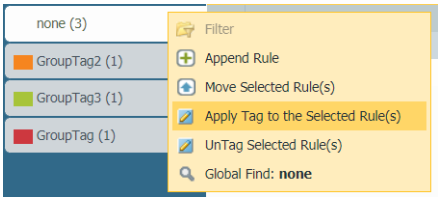
Champ	Description
Destination	Le groupe de périphériques cible des règles de politique dupliquées.
(Panorama uniquement) Type de destination	Sélectionnez si vous souhaitez dupliquer les règles vers la **Base de règles en amont** ou vers la **Base de règles en avale** du groupe de périphériques de destination.
Ordre des règles	Sélectionnez l'endroit de la base de règles où dupliquer les règles. Vous avez le choix entre les actions suivantes: • **Déplacer vers le haut** : insérez les règles dupliquées au haut de la base de règles du groupe de périphériques de destination. • **Déplacer vers le bas** : insérez les règles dupliquées au bas de la base de règles du groupe de périphériques de destination. • **Avant la règle** : insérez les règles dupliquées avant la règle sélectionnée de la base de règles du groupe de périphériques de destination. • **Après la règle** : insérez les règles dupliquées après la règle sélectionnée de la base de règles du groupe de périphériques de destination.

Champ	Description
Erreur sortante dès la première erreur détectée lors de la validation	Sélectionnez cette option pour déterminer comment les erreurs décelées au cours de la validation s'affichent. Si elle est activée, chaque erreur s'affiche individuellement. Si elle est désactivée (décochée), les erreurs sont groupées et s'affichent en tant qu'une seule erreur. Les erreurs détectées au cours de la validation entraînent l'échec du clonage. Aucune règle n'est ainsi dupliquée dans le groupe de périphériques de destination.

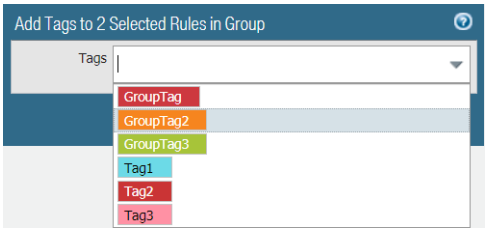
Gestion des étiquettes

Le tableau suivant répertorie les actions que vous pouvez effectuer lorsque vous regroupez des règles par étiquettes de groupes.

- Attribuer une étiquette à une règle.
  1. Sélectionnez **View Rules as Groups (Afficher les règles en tant que groupes)**.
  2. Sélectionnez une ou plusieurs règles dans le volet de droite.
  3. Dans le menu déroulant dans étiquettes de groupes, **Apply Tag to the Selected Rules (Appliquez les étiquettes aux groupes sélectionnés)**.

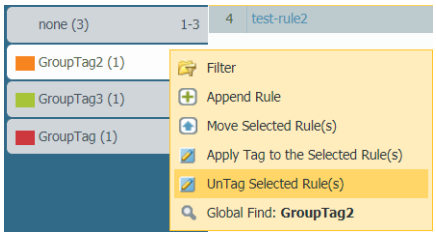


  4. Ajoutez des étiquettes aux règles sélectionnées.

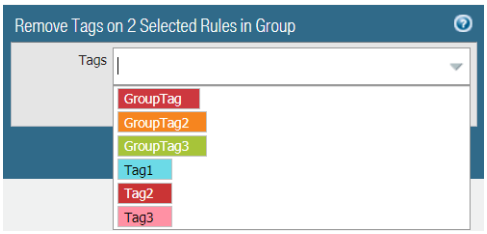


- Affichez les règles affectées à un groupe d'étiquettes.
  1. Sélectionnez **View Rulebase as Groups (Afficher la base de règles en tant que groupes)** pour afficher les étiquettes de groupes auxquelles vos règles sont affectées.
  2. Le volet de droite se met à jour et affiche les étiquettes de groupe contenant n'importe lesquelles des étiquettes sélectionnées.
  3. Sélectionnez l'étiquette de groupes pour afficher les règles associées à ce groupe. Les règles qui ne sont pas affectées à une étiquette de groupes sont répertoriées dans le groupe **none (aucune)**.

- Annuler l'attribution d'une étiquette à une règle.
  1. Sélectionnez **View Rulebase as Groups (Afficher la base de règles en tant que groupes)** pour afficher les étiquettes de groupes auxquelles vos règles sont affectées.
  2. Sélectionnez une ou plusieurs règles dans le volet de droite.
  3. Dans le menu déroulant dans étiquettes de groupes, **Apply Tag to the Selected Rules (Appliquez les étiquettes aux groupes sélectionnés)**.

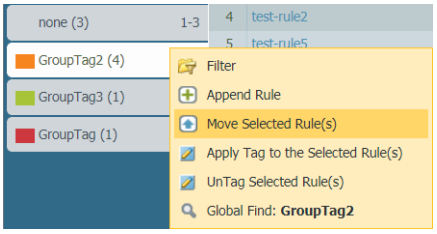


  4. Supprimez les étiquettes des règles sélectionnées. De plus, vous pouvez **Delete All (supprimer toutes)** les étiquettes affectées à la règle.



- Réorganiser une règle en utilisant des étiquettes.

  Lorsque vous **View Rulebase as Groups (Affichez la base de règles en tant que groupes)**, sélectionnez une ou plusieurs règles d'une étiquette de groupes, glissez la souris sur le numéro de la règle et sélectionnez **Move Selected Rule(s) (Déplacer la règle sélectionnée(s) dans la liste)** dans le menu déroulant. Ne sélectionnez aucune règle si vous souhaitez déplacer toutes les règles dans l'étiquette de groupe sélectionnée.



  Sélectionnez une étiquette de groupe dans la liste déroulante de la fenêtre Déplacer une règle et indiquez si vous voulez **Move Before (Avancer)** ou **Move After (Reculer)** l'étiquette sélectionnée dans la liste déroulante.

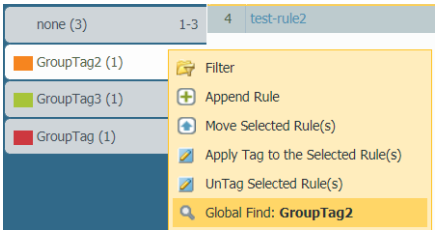
- Ajouter une nouvelle règle qui s'applique aux étiquettes sélectionnées.

  Lorsque vous **View Rulebase as Groups (Affichez la base de règles en tant que groupes)**, glissez la souris sur l'étiquette de groupe et sélectionnez l'option **Append Rule (Ajouter la règle)** dans le menu déroulant.

  La nouvelle règle est ajoutée à la fin de la liste de règles affectées à l'étiquette de groupe.

- Rechercher une étiquette de groupe.

  Lorsque vous **View Rulebase as Groups (Affichez la base de règles en tant que groupes)**, glissez la souris sur l'étiquette de groupe et sélectionnez l'option **Global Find (Recherche générale)** dans le menu déroulant.



- Exporter le tableau de configuration des étiquettes.

  Les rôles administrateurs peuvent exporter le tableau de configuration des objets au format **PDF/CSV** et peuvent appliquer des filtres pour personnaliser les sorties du tableau afin qu'elles n'intègrent que les colonnes dont vous avez besoin. Seules les colonnes qui sont visibles dans le dialogue d'Exportation sont exportées. Consultez la section Exportation des données du tableau de configuration.

Objets > Périphériques

Egalement connu sous le nom de Dictionnaire des périphériques, cette page contient les métadonnées des objets de périphériques. Passez en revue les informations des objets de périphériques existants ou ajoutez de nouveaux objets de périphériques. L'utilisation d'objets de périphériques comme critères de correspondance dans une politique de sécurité vous permet de créer une politique basés sur un périphérique selon laquelle le pare-feu met à jour de façon dynamique et applique la politique de sécurité aux nouveaux périphériques existants. Palo Alto Networks met à jour le dictionnaire des périphériques via des mises à jour dynamiques, que vous pouvez afficher dans **Le** > **contenu Device Dynamic Updates** > **Device-ID.**

Bouton/Champs	Description
Name (Nom)	Le nom de l'objet de périphérique
Emplacement	L'emplacement du groupe de périphériques pour l'objet de périphérique.
Catégorie	La catégorie de l'objet de périphérique (par exemple, `Video Audio Conference (conférence audio et vidéo)`).
Profil	Le profil de périphérique pour l'objet de périphérique.
Modèle	Le modèle de l'objet de périphérique
OS Version (Version de système d'exploitation)	La version de l'OS (Système d'exploitation) de l'objet du périphérique.
Famille de système d'exploitation	La famille de l'OS (Système d'exploitation) de l'objet du périphérique.
Constructeur	Le fournisseur de l'objet de périphérique.
Ajouter	Cliquez sur **Add (Ajouter)** pour ajouter un nouvel objet de périphérique. Saisissez un **Name (Nom)** et saisissez éventuellement une **Description**. Sélectionnez des métadonnées supplémentaires pour le périphérique comme **Category (Catégorie)**, **OS (Système d'exploitation)**, et **Model (Modèle)**. Vous pouvez aussi **Browse (Naviguez)** dans la liste des périphériques pour sélectionner le périphérique que vous voulez ajouter. Cliquez sur **OK** pour confirmer vos modifications.
Supprimer	Sélectionnez un objet de périphérique dont vous n'avez plus besoin et **Delete (Supprimez)** celui-ci.
Se déplacer	Sélectionnez l'objet de périphérique que vous voulez déplacer puis **Move (déplacez)** celui-ci.

Bouton/Champs	Description
Cloner	Sélectionnez l’objet de périphérique sur lequel baser le nouveau profil de périphérique et **Clone (clonez)** celui-ci.
PDF/CSV	Exportez la liste des périphérique au format **PDF/CSV**. Vous pouvez appliquer des filtres pour créer des résultats plus spécifiques en fonction de vos besoins. Seules les colonnes qui sont visibles dans l’interface Web seront exportées. Reportez-vous à la section Exportation du tableau de configuration.

Objets > Listes dynamiques externes

Une external dynamic list (liste dynamique externe)est un objet d'adresse basé sur une liste importée d'adresses IP, URL, noms de domaine, Identités d'équipement mobile internationales(IMEIs), ou identités d'abonné mobile internationales (IMSIs) que vous pouvez utiliser dans des règles de politique pour bloquer ou autoriser le trafic. Cette liste doit être un fichier texte enregistré sur un serveur Web accessible par le pare-feu. Par défaut, le pare-feu utilise l'interface de gestion (MGT) pour récupérer cette liste.

Avec une licence de prévention des menaces active, Palo Alto Networks fournit plusieurs listes d'adresses IP dynamiques intégrées que vous pouvez utiliser pour bloquer des hôtes malveillants. Nous mettons à jour les listes quotidiennement en fonction de nos plus récentes recherches sur les menaces.

Vous pouvez utiliser une liste d'adresses IP comme objet d'adresse dans la source et la destination de vos règles de politique. Vous pouvez utiliser une liste des URL dans un profil de URL Filtering (Objects > Security Profiles > URL Filtering (Objets > Profils de sécurité > URL Filtering)) ou comme critère de correspondance dans les règles de politique de sécurité. Vous pouvez également utiliser une liste des domaines Objects > Security Profiles > Anti-Spyware Profile (Objets > Profils de sécurité > Profil antispyware) en tant que piège pour les noms de domaines spécifiés.

Sur chaque modèle de pare-feu, vous pouvez utiliser jusqu'à 30 listes dynamiques externes avec des sources uniques à travers toutes les règles des politiques de Sécurité. Le nombre maximal d'entrées que le pare-feu prend en charge pour chaque type de liste varie en fonction du modèle de pare-feu (reportez-vous aux différentes limites de pare-feu pour chaque type de liste dynamique externe). Les entrées de la liste sont comptabilisées dans la limite maximale uniquement si la liste dynamique externe est utilisée dans une règle de politique. Si vous dépassez le nombre maximal d'entrées qui sont prises en charge sur un modèle, le pare-feu génère un journal système et ignore toutes les entrées qui dépassent cette limite. Pour vérifier le nombre d'adresses IP, de domaines, d'URL, d'identifiants IMEI et IMSI actuellement utilisés dans la politique et le nombre total pris en charge sur le pare-feu, cliquez sur le pare-feu et sélectionnez **List Capacities (Capacités de la liste)** (pare-feu uniquement).

Les listes dynamiques externes s'affichent dans l'ordre dans lequel elles sont évaluées, de haut en bas. Pour réorganiser les listes, utilisez les contrôles directionnels en bas de la page. Vous pouvez déplacer les listes dynamiques externes avec les entrées les plus importantes vers le haut pour vous assurer qu'elles sont validées avant d'atteindre les limites de capacité.

*Vous ne pouvez pas modifier l'ordre de vos listes dynamiques externes lorsque l'option **Grouper par type** est activée.*

Pour récupérer la dernière version d'une liste dynamique externe à partir du serveur qui l'héberge, sélectionnez la liste dynamique externe et cliquez sur **Import Now (Importer maintenant)**.

Vous ne pouvez pas supprimer, cloner ou modifier les paramètres des flux d'adresses IP malveillantes de Palo Alto Networks.

Add (Ajoutez) une nouvelle liste dynamique externe et configurez les paramètres décrits dans le tableau ci-dessous.

Paramètres de la liste dynamique externe	Description
Name (Nom)	Saisissez un nom pour identifier la liste dynamique externe (32 caractères maximum). Ce nom identifie la liste pour l'application de la règle de politique.
Partagé (Systèmes virtuels multiples (multi-vsys) et Panorama uniquement)	Activez cette option si vous souhaitez que la liste dynamique externe soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez (décochez) cette option, la liste dynamique externe est uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez (décochez) cette option, la liste dynamique externe est uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Activez cette option pour empêcher les administrateurs de remplacer les paramètres de cette liste dynamique externe dans les groupes de périphériques qui héritent de l'objet. Cette option est désactivée (décochée) par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l'objet.
Vérifier l'URL source (pare-feu uniquement)	**Test Source URL (Testez l'URL source)** pour vérifier que le pare-feu peut se connecter au serveur qui héberge la liste dynamique externe. *Ce test ne vérifie pas si le serveur est authentifié avec succès.*
Onglet Créer liste	
Type	Faites votre sélection à partir des types de listes dynamiques externes suivants :

Paramètres de la liste dynamique externe	Description

Vous ne pouvez mélanger les adresses IP, les URL et les noms de domaine dans une seule liste. Chaque liste doit comprendre des entrées d'un seul type.	• **Predefined IP List (Liste d'IP prédéfinies)** : Utilisez une liste que Palo Alto Networks identifie comme des adresses IP blindées, adresses IP malveillantes connues ou adresses IP à risque élevé en tant que source d'entrées de la liste (nécessite une licence active de Prévention des menaces).
	• **Predefined URL List (Liste d'URL prédéfinies)**: Utilisez une liste de domaines que Palo Alto Networks identifie comme étant fiable pour exclure ces domaines de la police d'authentification.
	• **IP List (Liste d'IP)** (par défaut) : chaque liste peut inclure des adresses IPv4 or IPv6, fourchettes d'adresses et réseaux secondaires. La liste doit contenir une seule adresse IP, une seule plage ou un seul sous-réseau par ligne. Par exemple :
	`192.168.80.150/32 2001:db8:123:1::1 ou 2001:db8:123:1::/64 192.168.80.0/24 2001:db8:123:1::1 - 2001:db8:123:1::22 Dans l'exemple ci-dessus`
	la première ligne indique toutes les adresses de 192.168.80.0 à 192.168.80.255. Un sous-réseau ou une plage d'adresses IP comme 92.168.20.0/24 ou 192.168.20.40 – 192.168.20.50, sont comptabilisés comme une entrée d'adresse IP et pas comme plusieurs adresses IP.
	• **Domain List (Liste des domaines)** - Chaque liste ne peut contenir qu'une seule entrée de nom de domaine par ligne. Par exemple :
	`www.p301srv03.paloalonetworks.com ftp.example.co.uk test.domain.net`
	Pour la liste des domaines inclus dans la liste dynamique externe, le pare-feu crée un ensemble de signatures personnalisées du type de logiciel espion de gravité moyenne afin que vous puissiez utiliser l'action sinkhole pour une liste personnalisée de domaines.

Paramètres de la liste dynamique externe	Description
	• **URL List (Liste des URL)** - Chaque liste ne peut posséder qu'une seule entrée d'URL par ligne. Par exemple : `financialtimes.co.in www.wallaby.au/joey www.exyang.com/auto-tutorials/How-to-enter-Data-for-Success.aspx *.example.com/*` L'action par défaut pour chaque liste d'URL est **Autoriser**. Pour modifier l'action par défaut, voir Objets > Profils de sécurité > URL Filtering. Reportez-vous aux instructions de mise en forme de la liste dynamique externehttps://docs.paloaltonetworks.com/pan-os/11-0/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/formatting-guidelines-for-an-external-dynamic-listlors de la création d'une entrée IP, d'un domaine ou d'une liste d'URL.
Type (suite)	• **Subscriber Identity List (Liste d'identité des abonnés)** : chaque liste contient des ID d'abonnés du réseau 3G, 4G, ou 5G. Dans le champ source, saisissez une URL pour que le pare-feu accède à la liste. • **Equipment Identity List (Liste d'identité des équipements)** : chaque liste contient des ID des équipements du réseau 3G, 4G, ou 5G. Dans le champ source, saisissez une URL pour que le pare-feu accède à la liste. *Déterminez quel modèle de pare-feu acheter sur la base du nombre total d'identifiants de réseau 3G, 4G et 5G que votre liste dynamique externe et vos entrées statiques devront supporter.*
Description	Saisissez une description de la liste dynamique externe (255 caractères maximum).
Source	• Si la liste dynamique externe est une liste des adresses IP prédéfinies, sélectionnez **Palo Alto Networks - Bulletproof IP adresses (adresses IP blindées)**, **Palo Alto Networks - High risk IP addresses (Adresse IP à haut risque)** ou **Palo Alto Networks - Known malicious IP addresses (Adresses IP malveillantes connues)** en tant que source de la liste. • Si la liste dynamique externe est une liste d'URL prédéfinies, le paramètre par défaut est **panw-auth-portal-exclude-list**. • Si la liste dynamique externe est une liste d'IP, une liste de domaines ou une liste d'URL, saisissez un chemin d'URL HTTP or HTTPS URL qui contient le fichier texte (par exemple, **`http://192.0.2.20/myfile.txt`**).

Paramètres de la liste dynamique externe	Description
	• Si la liste dynamique externe est une liste de domaines, vous pouvez **Automatically expand to include subdomains (développer automatiquement pour inclure des sous-domaines)**. Cette option permet au logiciel PAN-OS® d'évaluer tous les composants de niveau inférieur des noms de domaines indiqués dans le fichier de liste dynamique externe. Cette option est désactivée par défaut. • Si la liste dynamique externe est une liste d'identités d'abonnés ou une liste d'identités d'équipements, saisissez un chemin URL qui contient la liste. *Si votre Liste dynamique externe contient des sous-domaines, ces entrées étendues sont incluses dans le calcul de la capacité du modèle de votre appareil. Pour définir manuellement des sous-domaines, vous pouvez désactiver cette fonctionnalité. Toutefois, si vous désactivez cette fonctionnalité, les sous-domaines ne seront pas évalués par des règles de stratégie, sauf si vous les définissez explicitement dans la liste.*
Profil de certificat (liste IP, liste de domaines ou liste d'URL uniquement)	Si la liste dynamique externe comporte une URL d'accès HTTPS, sélectionnez un profil de certificat existant (pare-feu et Panorama) ou créez un nouveau **Profil de certificat** (pare-feu uniquement) pour authentifier le serveur Web qui héberge la liste. Pour plus d'informations sur la configuration d'un profil de certificat, voir Périphérique > Gestion des certificats > Profil du certificat. Par défaut : **Aucun (Désactiver le profil de certificat)** *Pour maximiser le nombre de listes dynamiques externes que vous pouvez utiliser pour appliquer la stratégie, utilisez le même profil de certificat pour authentifier les listes dynamiques externes à partir de la même URL source. Ces listes ne comptent que comme une seule liste dynamique externe. Autrement, les listes dynamiques externes provenant de la même URL source qui utilisent différents profils de certificats sont comptabilisées comme des listes dynamiques externes uniques.*
Authentification du client	Activez cette option (désactivée par défaut) pour ajouter un nom d'utilisateur et un mot de passe que pare-feu utilisera pour accéder à une source de listes dynamiques externes nécessitant une authentification HTTP basique. Ce paramètre n'est disponible que lorsque la liste dynamique externe possède une URL HTTPS.

Paramètres de la liste dynamique externe	Description
	• **Nom d'utilisateur** – Saisissez un nom d'utilisateur valide pour accéder à la liste. • **Mot de passe / Confirmer le mot de passe** - Saisissez, puis confirmez le mot de passe du nom d'utilisateur.
Rechercher des mises à jour	Spécifiez la fréquence à laquelle le pare-feu récupère la liste du serveur Web. Vous pouvez définir l'intervalle **sur Toutes les cinq minutes** (par défaut), **Toutes les heures**, **Tous les jours**, **Toutes**, les semaines ou **Tous les mois**. L'intervalle est fonction de la dernière validation. Par exemple, si vous sélectionnez l'intervalle de cinq minutes, une validation se produit en 5 minutes si la dernière validation remonte à une heure. La validation met à jour toutes les règles de stratégie qui font référence à la liste. *Vous n'avez pas à indiquer une fréquence pour une liste prédéfinie d'adresses IP parce que le pare-feu reçoit dynamiquement des mises à jour de contenu avec une licence active de prévention des menaces.*
Onglet des entrées et des exceptions de la liste	
Entrées de la liste	Affiche les entrées dans la liste dynamique externe. • **Add an entry as a list exception (Ajouter une entrée en tant qu'exception de liste)** – Sélectionnez jusqu'à 100 entrées et cliquez sur **Submit (Envoyer)** (→). • **View an AutoFocus threat intelligence summary for an item (Affichez un récapitulatif des renseignements sur les menaces AutoFocus pour un objet)** – Passez sur une entrée et cliquez sur **Autofocus** dans le menu déroulant. Vous devez avoir une licence AutoFocus™ et activer les renseignements de menaces AutoFocus pour afficher un récapitulatif des objets (sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** et modifiez les paramètres **AutoFocus**). • **Check if an IP address, domain, or URL is in the external dynamic list (Vérifiez si une adresse IP, un domaine ou une URL se trouve dans la liste dynamique externe)**– Saisissez une valeur dans le champ de filtrage et cliquez sur **Apply Filter (Appliquer le filtre)** (→). **Désactivez Filtre** (**[X]**) pour revenir à la liste complète.
Exceptions manuelles	Affiche les exceptions de la liste dynamique externe.

Paramètres de la liste dynamique externe	Description
	• **Edit an exception (Modifier une exception)** – Sélectionnez une exception et faites vos modifications. • **Manually enter an exception (Saisir manuellement une exception)** – **Add (Ajoutez)** une nouvelle exception manuellement. • **Remove an exception from the Manual Exceptions list (Supprimer une exception de la liste des Exceptions manuelles)** – Sélectionnez une exception et cliquez sur **Delete (Effacer)**. • **Check if an IP address, domain, or URL is in the Manual Exceptions list (Vérifiez si une adresse IP, un domaine ou une URL se trouve dans la liste des Exceptions manuelles)** – Saisissez une valeur dans le champ de filtrage et cliquez sur **Apply Filter (Appliquer le filtre)** (→). **Désactivez Filtre** (**[X]**) pour revenir à la liste complète. Si vous avez des entrées en double dans la liste Exceptions manuelles, vous ne pouvez pas enregistrer vos modifications dans la liste dynamique externe.

Objets > Objets personnalisés

Créez des modèles de données, des signatures contre les logiciels malveillants ou contre les vulnérabilités ainsi que des catégories d'URL personnalisées à utiliser avec les politiques :

- Objets > Objets personnalisés > Modèles de données
- Objets > Objets personnalisés > Logiciels espions / vulnérabilité
- Objets > Objets personnalisés > Catégories d'URL

Objets > Objets personnalisés > Modèles de données

Les rubriques suivantes décrivent les modèles de données.

Que voulez-vous faire ?	Reportez-vous à la section :
Créer un modèle de données.	Paramètres des modèles de données
En savoir plus sur la syntaxe des expressions régulières pour les modèles de données et voir quelques exemples.	Syntaxe pour les modèles de données d’expression régulière Exemples de modèles de données d’expression régulière

Paramètres des modèles de données

Sélectionnez **Objets** > **Objets personnalisés** > **Modèles de données** pour définir les catégories d’informations sensibles que vous souhaitez filtrer. Pour plus d’informations sur la définition des profils de filtrage de données, sélectionnez Objets > Profils de sécurité> Filtrage des données.

Vous pouvez créer trois types de modèles de données pour le pare-feu. Vous pourrez utiliser ces modèles lors de la recherche d’informations sensibles :

- **Prédéfini** – Utilise les modèles de données prédéfinis pour analyser les fichiers de la sécurité sociale et les numéros des cartes de crédit.
- **Expression régulière** – Crée des modèles de données personnalisés en utilisant des expressions régulières.
- **Propriétés du fichier** – Analyse les fichiers pour les propriétés et les valeurs de fichiers spécifiques.

Paramètres des modèles de données	Description
Nom	Saisissez le nom du modèle de données (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement.
Description	Saisissez une description du modèle de données (255 caractères maximum).

Paramètres des modèles de données	Description
Partagé	Sélectionnez cette option si vous souhaitez que le modèle de données soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le modèle de données sera uniquement disponible pour le **Système virtuel** sélectionné dans l'onglet **Objets**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le modèle de données sera uniquement disponible pour le **Groupe de périphériques** sélectionné dans l'onglet **Objets**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres du modèle de données de l'objet pour les groupes de périphériques qui héritent de l'objet. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l'objet.
Type de modèle	Sélectionnez le type de modèle de données que vous voulez créer : • Modèle prédéfini • Expression régulière • Propriétés du fichier
Modèle prédéfini	Palo Alto Networks fournit des modèles de données prédéfinis pour analyser certains types de renseignements dans les fichiers comme, par exemple, les numéros de carte de crédit ou les numéros de sécurité sociale. Pour configurer le filtrage des données en fonction d'un modèle prédéfini, cliquez sur **Ajouter** un motif et sélectionnez ce qui suit : • **Nom** – Sélectionnez le modèle prédéfini qui sera utilisé pour filtrer les données sensibles. Lorsque vous choisissez un modèle prédéfini, le champ **Description** se remplit automatiquement. • Sélectionnez le **Type de fichier** dans lequel vous souhaitez détecter le modèle prédéfini.
Expression régulière	Cliquez sur **Ajouter** un modèle de données personnalisé. Donnez au modèle un **Nom** descriptif, configurez le **Type de fichier** que vous souhaitez analyser pour le motif de données et saisissez l'expression régulière qui définit le **Modèle de données**. Pour les détails et les exemples de syntaxe des modèles d'informations d'expression régulière, veuillez vous référer aux sections suivantes : • Syntaxe pour les modèles de données d'expression régulière • Exemples de modèles de données d'expression régulière
Propriétés du fichier	Créez un modèle de données pour analyser les propriétés du fichier et les valeurs associées. Par exemple, cliquez sur **Ajouter** un modèle de

Paramètres des modèles de données	Description
	données pour filtrer les documents Microsoft Word et les fichiers PDF lorsque le titre du document comprend les mots « sensible », « interne » ou « confidentiel ». • Donnez un **Nom** descriptif au modèle de données. • Sélectionnez le **Type de fichier** que vous souhaitez analyser. • Sélectionnez la **Propriété de fichier** que vous souhaitez analyser pour une valeur spécifique. • Saisissez la **Valeur de propriété** que vous souhaitez analyser.

Syntaxe pour les modèles de données d’expression régulière

Les besoins en modèle général et en syntaxe pour créer des modèles de données dépendent du moteur de correspondance de modèle que vous activez : classique ou amélioré (par défaut).

Besoins en modèle	Classique	Amélioré
Longueur du modèle	Nécessite 7 caractères alphabétiques, qui ne peuvent pas inclure un point (`.`), un astérisque (*), un signe plus (+), ni une fourchette (`[a-z]`).	Nécessite deux caractères alphabétiques
Non sensible à la casse	Nécessite que vous définissiez des modèles pour toutes les chaînes possibles pour qu’elles correspondent à toutes les variations d’un terme. Exemple : Pour correspondre à des documents désignés comme étant confidentiels, vous devrez créer un modèle pour « confidentiel », « Confidentiel » et « CONFIDENTIEL ».	Permet d’utiliser l’option **`i`** dans un sous-modèle. Exemple : **`((?i)\bconfidentiel\b)`** correspond à `Confidentiel`

La syntaxe des expressions régulières dans PAN-OS® est similaire à celle des moteurs traditionnels, mais chaque modèle est unique. Les tableaux Classic Syntax (syntaxe classique) et Enhanced Syntax (Syntaxe améliorée) décrivent la syntaxe compatible avec les moteurs de correspondance de modèle PAN-OS.

Classic Syntax (Syntaxe classique)

Syntaxe du modèle	Description
.	Renvoie n'importe quel caractère unique.

Syntaxe du modèle	Description
?	Renvoie le caractère ou l'expression qui précède 0 ou une fois. Vous devez inclure l'expression générale entre parenthèses. Exemple : **(abc)?**
*	Renvoie le caractère ou l'expression qui précède 0 ou plusieurs fois. Vous devez inclure l'expression générale entre parenthèses. Exemple : **(abc)***
+	Renvoie le caractère ou l'expression régulière qui précède une ou plusieurs fois. Vous devez inclure l'expression générale entre parenthèses. Exemple : **(abc)+**
|	Spécifie un « OU » un autre. *Vous devez inclure les sous-chaînes alternatives entre parenthèses.* Exemple : **((bif)|(scr)|(exe))** renvoie `bif`, `scr` ou `exe`.
-	Spécifie une plage. Exemple : **[c-z]** renvoie tout caractère entre `c` et `z` inclus.
[ ]	Renvoie n'importe quel caractère spécifié. Exemple : **[abz]** renvoie n'importe lequel des caractères `a`, `b` ou `z`.
^	Renvoie n'importe quel caractère à l'exception des caractères spécifiés. Exemple : **[^abz]** renvoie n'importe lequel des caractères sauf ceux indiqués : `a`, `b` ou `z`.
{ }	Renvoie une chaîne qui contient un minimum et un maximum. Exemple : **{10-20}** renvoie n'importe quelle chaîne comprise entre 10 et 20 octets inclus. Vous devez spécifier ceci directement devant une chaîne fixe et vous ne pouvez utiliser qu'un trait d'union (**-**).
\	Effectue une correspondance littérale sur n'importe quel caractère. Vous devez faire précéder le caractère spécifié d'une barre oblique inversée (\).
&amp	La perluète (&) est un caractère spécial, donc si vous recherchez & dans une chaîne, vous devez utiliser **&amp**».

Enhanced Syntax (Syntaxe améliorée)

Le moteur de correspondance de modèle amélioré est compatible avec la Classic Syntax (syntaxe classique) et la syntaxe suivante :

Syntaxe du modèle	Description
Shorthand character classes (catégories de caractères abrégés) Symboles qui remplacent un caractère d'un type spécifique, comme un chiffre ou un espace. Vous pouvez invalider n'importe laquelle de ces catégories de caractères abrégés en utilisant des caractères en majuscule.	
\s	Correspond à n'importe quel espace. Exemple : **`\s`** correspond à un espace, un tabulation, un saut de ligne ou un saut de page.
\d	Correspond à un caractère qui est un chiffre [0-9]. Exemple : **`\d`** correspond à`0`.
\w	Correspond à un caractère ASCII [A-Za-z0-9_]. Exemple : **`\w\w\w`** correspond à`PAN`.
\v	Correspond à un caractère d'espacement vertical qui comprend tous les caractères de saut de ligne unicode. Exemple : **`\v`** correspond à un caractère d'espacement vertical.
\h	Correspond à un espace horizontal qui comprend la tabulation et tous les caractères unicode de « séparateur par un espace ». Exemple : **`\h`** correspond à un caractère d'espacement horizontal.
Bounded repeat quantifiers (quantificateurs de répétition limités) Précisez combien de fois il faut répéter l'élément précédent.	
{n}	Correspond exactement à un nombre (*n*) de fois. Exemple : **`a{2}`** correspond à `aa`.
{n,m}	**`{n,m}`** correspond à de *n* à *m* fois. Exemple : **`a{2,4}`** correspond à `aa`, `aaa`, et `aaaa`
{n, }	**`{n,}`** correspond à au moins *n* fois.

Syntaxe du modèle	Description
	Exemple : **a{2,}** correspond à aaaaa dans aaaaab.
Anchor characters (caractères d'ancrage) Précise où correspondre à une expression.	
^	Correspond au début d'une chaîne. Correspond aussi après chaque saut de ligne lorsque le mode multi-ligne (**m**) est activé. Exemple : Etant donné la chaîne abc, **^a** correspond à a, mais **^b**ne correspond à rien car b n'apparait pas en début de chaîne.
$	Correspond à la fin d'une chaîne ou avant le caractère d'une nouvelle ligne à la fin d'une chaîne. Correspond aussi avant chaque saut de ligne lorsque le mode multi-ligne (**m**) est activé. Exemple : Etant donné la chaîne abc, **c$** correspond à c, mais **a$**ne correspond à rien car a n'apparait pas en fin de chaîne.
\A	Correspond au début d'une chaîne. Ne correspond pas après des sauts de ligne, même lorsque le mode multi-ligne (**m**) est activé.
\Z	Correspond à la fin d'une chaîne et avant le dernier saut de ligne. Ne correspond pas après les autres sauts de ligne, même lorsque le mode multi-ligne (**m**) est activé.
\z	Correspond à la fin absolue d'une chaîne. Ne correspond pas avant des sauts de ligne.
Option modifiers (Modificateurs d'option) Modifier le comportement d'un sous-modèle. Entrez **(?** <option>) pour activer ou **(?-** <option>) pour désactiver.	
i	Active la non-sensibilité à la casse Exemple : **((?i)\bconfidentiel\b)** correspond à Confidentiel.
m	Fait que **^** et **$** correspondent au début et à la fin des lignes.

Syntaxe du modèle	Description
s	Fait que `.` corresponde à n’importe quoi, y compris des caractères de saut de ligne.
x	Ignore les espaces entre des occurrences d’expressions régulières.

Exemples de modèles de données d’expression régulière

Voici des exemples de modèles personnalisés valides:

- .*((Confidentiel)|(CONFIDENTIEL))
  - Recherche le mot « Confidentiel » ou « CONFIDENTIEL » partout
  - « .* » indique que la recherche porte sur n'importe quelle partie de la chaîne
  - Selon que votre décodeur est sensible à la casse ou pas, le terme « confidentiel » (en minuscules) risque de ne pas faire partie des correspondances.
- .*((Exclusif &amp Confidentiel)|(Exclusif et Confidentiel))
  - Recherche « Exclusif & Confidentiel » ou « Exclusif et Confidentiel »
  - Plus précis que « Confidentiel »
- .*(Communiqué de presse).*((Ebauche)|(EBAUCHE)|(ébauche))
  - Recherche « Communiqué de presse », suivi par diverses formes du mot « ébauche », ce qui peut indiquer que le communiqué de presse n'est pas prêt à être divulgué
- .*(Trinidad)
  - Recherche un nom de code de projet, par exemple « Trinidad »

Objets > Objets personnalisés > Logiciels espions / vulnérabilité

Le pare-feu prend en charge la création de signatures personnalisées contre les logiciels espions et les vulnérabilités grâce à son moteur de détection des menaces. Vous pouvez rédiger des modèles d'expressions régulières personnalisés pour identifier les communications 'AB; phone home 'BB; des logiciels espions ou les exploitations de vulnérabilités. Les modèles obtenus peuvent être utilisés dans n'importe quel profil personnalisé de protection contre les vulnérabilités. Le pare-feu recherche les modèles personnalisés dans le trafic réseau et prend l'action définie pour lutter contre l'exploitation de la vulnérabilité détectée.

Toutes les semaines, le contenu affiche de nouveaux décodeurs et contextes pour lesquels vous pouvez développer des signatures.

En option, vous pouvez inclure un attribut de temps dans la définition des signatures personnalisées, en précisant un seuil par intervalle pour le déclenchement des actions possibles en réponse à une attaque. L'action n'est prise qu'une fois le seuil atteint.

La page **Custom Spyware Signature (Signatures personnalisées contre les logiciels espions)** permet de définir des signatures pour les profils de protection contre les logiciels espions. La page **Custom Vulnerability Signature (Signatures personnalisées contre les vulnérabilités)** permet de définir des signatures pour les profils de protection contre les vulnérabilités.

Paramètres de signature contre les vulnérabilités et les logiciels espions personnalisés	Description
Onglet Configuration	
ID de menace	Saisissez un identifiant numérique pour la configuration (l'intervalle des signatures contre les logiciels espions est compris entre 15 000 et 18 000 et entre 6 900 001 et 7 000 000 ; l'intervalle des signatures contre les vulnérabilités est compris entre 41 000 et 45 000 et entre 6 800 001 et 6 900 000).
Name (Nom)	Indiquez le nom de la menace.
Partagé	Sélectionnez cette option si vous souhaitez que la signature personnalisée soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, la signature personnalisée sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, la signature personnalisée sera uniquement disponible pour

Paramètres de signature contre les vulnérabilités et les logiciels espions personnalisés	Description
	le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de cette signature dans les groupes de périphériques qui héritent de la signature. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de la signature.
Commentaire	Saisissez un commentaire (facultatif).
Sévérité	Affectez un niveau qui indique la gravité de la menace.
Action par défaut	Affectez l'action par défaut à prendre si les conditions de la menace sont réunies. Pour une liste d'actions, reportez-vous à la section Actions dans des profils de sécurité.
Direction	Indiquez si la menace est évaluée depuis le client vers le serveur, depuis le serveur vers le client ou les deux.
Système affecté	Indiquez si la menace implique le client, le serveur ou les deux. S'applique aux signatures contre les vulnérabilités, mais non aux signatures contre les logiciels espions.
CVE	Indiquez l'identifiant CVE à titre de référence externe pour une analyse plus approfondie.
Constructeur	Indiquez l'identifiant du constructeur à titre de référence externe pour une analyse plus approfondie.
Bugtraq	Indiquez le bugtraq (similaire à l'identifiant CVE) à titre de référence externe pour une analyse plus approfondie.
Référence	Ajoutez tout lien qui permet une analyse plus approfondie. Ces informations s'affichent lorsqu'un utilisateur clique sur la menace depuis l'ACC, les journaux ou le profil de protection contre les vulnérabilités.
Onglet Signatures	
Signature standard	Sélectionnez **Standard**, puis **Ajoutez** une nouvelle signature. Renseignez les informations suivantes'A0;: • **Standard** - Saisissez un nom permettant d'identifier la signature. • **Comment (Commentaire)** - Saisissez une description (facultatif).

Paramètres de signature contre les vulnérabilités et les logiciels espions personnalisés	Description
	• **Ordered Condition Match (Correspondance de l'état ordonné)** - Indiquez si l'ordre dans lequel les conditions de la signature sont définies a son importance. • **Scope (Portée)** - Indiquez s'il faut appliquer cette signature à la transaction en cours seulement pendant toute la session utilisateur. Ajoutez une condition en cliquant sur **Add Or Condition (Ajouter une condition OU)** ou **Add And Condition (Ajouter une condition ET)**. Pour ajouter une condition au sein d'un groupe, sélectionnez-le puis cliquez sur **Add Condition (Ajouter une condition)**. Ajoutez une condition à une signature afin que celle-ci soit générée pour le trafic lorsque les paramètres que vous avez définis pour la condition sont vrais. Sélectionnez un **Operator (Opérateur)** dans la liste déroulante. L'opérateur définit le type de condition qui doit être vrai pour que la signature personnalisée corresponde au trafic. Faites votre sélection parmi les opérateurs **Less Than (Inférieur à)**, **Equal To (Égal à)**, **Greater Than (Supérieur à)** ou **Pattern Match (Correspondance des modèles)**. • Si vous avez choisi un opérateur **Pattern Match (Correspondance des modèles)**, alors les éléments suivants devront être vrais pour que la signature corresponde au trafic : • **Context (Contexte)** - Choisissez parmi les contextes disponibles. • **Pattern (Modèle)** - Précisez une expression régulière. Reportez-vous à la section Syntaxe des règles des modèles pour connaître les règles concernant les expressions régulières. • **Qualifier and Value (Qualificatif et Valeur)** - Ajoutez des paires qualificatif/valeur (facultatif). • **Negate (Ignorer)** - Sélectionnez l'option **Negate (Ignorer)** pour que la signature personnalisée corresponde au trafic uniquement lorsque la condition Correspondance des modèles définie n'est pas vraie. Ceci permet de vous assurer que la signature personnalisée ne se déclenche pas sous certaines conditions. *Une signature personnalisée ne peut pas uniquement être créée avec les conditions Ignorer ; au moins une condition positive doit être incluse pour qu'une condition Ignorer puisse être définie. De même, si l'étendue de la signature est définie sur Session, une condition Ignorer ne peut pas être configurée comme dernière condition pour pouvoir correspondre au trafic.* Vous pouvez définir des exceptions pour les signatures personnalisées contre les logiciels malveillants ou contre les

Paramètres de signature contre les vulnérabilités et les logiciels espions personnalisés	Description
	vulnérabilités en utilisant la nouvelle option permettant d'ignorer la génération de signatures lorsque le trafic correspond à une signature et l'exception à la signature. Cette option permet d'autoriser un trafic donné dans votre réseau qui, autrement, serait classé en tant qu'exploitation de vulnérabilité ou de logiciel malveillant. Dans ce cas, la signature est générée pour le trafic correspondant au modèle, le trafic correspondant au modèle mais aussi à l'exception du modèle qui est exclu de la génération de signature et de toute action de la politique associée (comme une interdiction ou un abandon). Par exemple, vous pouvez choisir de générer une signature pour des URL redirigées. Cependant, vous pouvez désormais créer une exception dans laquelle aucune signature ne sera générée pour les URL redirigeant vers un domaine de confiance.
	• Si vous avez choisi un opérateur **Equal To (Égal à)**, **Less Than (Inférieur à)** ou **Greater Than (Supérieur à)**, alors les éléments suivants devront être vrais pour que la signature corresponde au trafic : • **Context (Contexte)** - Faites votre choix parmi les requêtes inconnues et les réponses pour le protocole TCP ou UDP. • **Position** - Faites votre choix parmi les quatre premiers ou les quatre seconds octets de la charge utile. • **Mask (Masque)** - Renseignez une valeur hexadécimale 4 octets, par exemple 0xffffff00. • **Value (Valeur)** - Renseignez une valeur hexadécimale 4 octets, par exemple 0xaabbccdd.
Association de signatures	Sélectionnez **Combination (Association)** et indiquez les informations suivantes : Sélectionnez l'option **Combination Signatures (Association de signatures)** pour indiquer les conditions de définition des signatures : • Ajoutez une condition en cliquant sur **Add AND Condition (Ajouter une condition AND)** ou **Add OR Condition (Ajouter une condition OR)**. Pour ajouter une condition au sein d'un groupe, sélectionnez-le puis cliquez sur **Add Condition (Ajouter une condition)**. • Pour déplacer une condition au sein d'un groupe, sélectionnez la condition et cliquez sur **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)**. Pour déplacer un groupe, sélectionnez-le et cliquez sur la flèche **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)**. Vous ne pouvez pas déplacer les conditions d'un groupe vers un autre.

Paramètres de signature contre les vulnérabilités et les logiciels espions personnalisés	Description
	Sélectionnez l'option **Time Attribute (Attribut temporel)** pour indiquer les informations suivantes : • **Number of Hits (Nombre d'accès)** - Spécifiez le seuil de déclenchement d'une action basée sur une politique sous la forme d'un nombre d'accès (1-1000) dans un certain nombre de secondes (1-3600). • **Aggregation Criteria (Critères d'agrégation)** - Précisez si les accès sont comptabilisés par adresse IP source, adresse IP de destination, ou une combinaison des deux. • Pour déplacer une condition au sein d'un groupe, sélectionnez la condition et cliquez sur **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)**. Pour déplacer un groupe, sélectionnez-le et cliquez sur la flèche **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)**. Vous ne pouvez pas déplacer les conditions d'un groupe vers un autre.

Objets > Objets personnalisés > Catégories d'URL

Utilisez la page Catégorie d'URL personnalisée pour créer votre liste d'URL personnalisée et utilisez-la dans un profil de filtrage des URL ou en tant que critères de correspondance dans les règles de la politique. Dans une catégorie d'URL personnalisée, vous pouvez ajouter des entrées d'URL individuellement ou vous pouvez importer un fichier texte qui contient une liste d'URL.

Les URL ajoutées aux catégories personnalisées sont sensibles à la casse.

Le tableau suivant décrit les paramètres des URL personnalisées.

Paramètres de la catégorie d'URL personnalisée	Description
Name (Nom)	Saisissez un nom pour identifier la catégorie d'URL personnalisée (31 caractères maximum). Ce nom apparaît dans la liste de catégories pour la définition de politiques de filtrage des URL ainsi que dans les critères de correspondance des catégories d'URL définies dans les règles de la politique. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Description	Saisissez une description de la catégorie d'URL (255 caractères maximum).
Type	Sélectionnez le type de catégorie : • **Category Match (Correspondance à la catégorie)** - Sélectionnez **Category match (Correspondance à la catégorie)** afin de définir une nouvelle catégorie personnalisée contenant les URL correspondants à toutes les catégories de URL spécifiées (un URL doit correspondre à toutes les catégories dans la liste). Spécifiez de 2 à 4 catégories. • **URL List (Liste des URL)** - Sélectionnez **URL List (Liste de URLS)** pour ajouter ou importer une liste de URL dans la catégorie. Ce type de catégorie contient aussi des URL ajoutés avant PAN-OS 9.0.
Partagé	Sélectionnez cette option si vous souhaitez que la catégorie d'URL soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez (décochez) cette option, la catégorie d'URL est uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez (décochez) cette option, la catégorie d'URL

Paramètres de la catégorie d'URL personnalisée	Description
	est uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de cet objet des URL personnalisées dans les groupes de périphériques qui héritent de l'objet. Cette sélection est décochée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l'objet.
Sites	Gérez les sites pour la catégorie des URL personnalisées (chaque URL ajouté ou importé est limité à 255 caractères). • **Add (Ajoutez)** : **Add (Ajoutez)** des URL, mais une seule par ligne. Chaque URL peut être au format « www.example.com » ou peut inclure des caractères génériques, comme « *.example.com ». Pour obtenir plus d'informations sur les formats pris en charge, consultez la liste d'interdictions à la section Objets > Profils de sécurité > URL Filtering. • **Import (Importer)** : **Import (Importez)** et accédez au fichier texte qui contient la liste des URL. Ne saisissez qu'un seul URL par ligne. Chaque URL peut être au format « www.example.com » ou peut inclure des caractères génériques, comme « *.example.com ». Pour obtenir plus d'informations sur les formats pris en charge, consultez la liste d'interdictions à la section Objets > Profils de sécurité > URL Filtering. • **Export (Exporter)** : **Export (Exportez)** les entrées d'URL personnalisées comprises dans la liste (exportées sous forme de fichier texte). • **Delete (Supprimer) - Delete (Supprimez)** une entrée pour supprimer l'URL de la liste. *Pour supprimer une catégorie personnalisée que vous avez utilisée dans un profil de URL Filtering, vous devez définir l'action sur Aucun avant de pouvoir procéder. Consultez les actions de la Catégorie dans la section* Objets > Profils de sécurité > URL Filtering.

Objets > Profils de sécurité

Les profils de sécurité fournissent une protection contre les menaces dans les politiques de sécurité. Chaque règle de politique de sécurité peut inclure un ou plusieurs profils de sécurité. Les types de profil disponibles sont les suivants :

- Profils antivirus visant à assurer une protection contre les vers, les virus et les chevaux de Troie, mais aussi à bloquer les téléchargements de logiciels espions. Reportez-vous à la section Objets > Profils de sécurité > Antivirus.
- Profils Antispyware visant à bloquer les tentatives de communications phone-home ou de signalement sur les serveurs (C2) de commande et de contrôle externes par les logiciels espions sur les hôtes compromis. Reportez-vous à la section Objets > Profils de sécurité > Profil antispyware.
- Profils de protection contre les vulnérabilités visant à bloquer les tentatives d'exploitation des failles du système ou d'accès non autorisé aux systèmes. Reportez-vous à la section Objets > Profils de sécurité > Protection contre les vulnérabilités.
- Profils de filtrage des URL visant à limiter l'accès des utilisateurs à des sites Web et/ou des catégories de sites Web spécifiques, tels que les sites commerciaux ou de jeux d'argent. Reportez-vous à la section Objets > Profils de sécurité > Filtrage des URL.
- Profils de blocage des fichiers visant à bloquer les types de fichiers sélectionnés et dans le sens spécifié du flux de la session (entrant et/ou sortant). Reportez-vous à la section Objets > Profils de sécurité > Blocage des fichiers.
- Profils d'analyse WildFire™ visant à indiquer le fichier à analyser localement sur l'équipement WildFire ou dans le Cloud WildFire. Reportez-vous à la section Objets > Profils de sécurité > Analyse WildFire.
- Profils de filtrage des données visant à empêcher les informations sensibles, telles que les numéros de carte de crédit ou de sécurité sociale, de quitter un réseau protégé. Reportez-vous à la section Objets > Profils de sécurité > Filtrage des données.
- Les profils de protection DoS sont utilisés avec les règles de politique de protection DoS pour protéger le pare-feu contre les attaques à volume élevé à l'encontre d'une session et de plusieurs sessions. Voir Objets > Profils de sécurité > Protection DoS.
- Les profils de Mobile Network Protection (protection de réseau mobile) permettent au pare-feu d'inspecter, de valider et de filtrer le trafic GTP.

Outre les profils individuels, vous pouvez combiner des profils qui sont souvent appliqués ensemble et ainsi créer des groupes de profils de sécurité (**Objects (Objets)** > **Security Profile Groups (Groupes de profils de sécurité)**).

Actions dans des profils de sécurité

Une action indique la manière dont le pare-feu répond à une menace. Chaque signature de menace ou de virus définie par Palo Alto Networks contient une action par défaut, généralement définie sur **Alerter,** qui vous indique d'utiliser l'option que vous avec activée pour les notifications ou sur **Réinitialiser les deux**, qui réinitialise les deux côtés de la connexion. Cependant, vous pouvez définir ou appliquer un contrôle prioritaire sur l'action sur le pare-feu. Les actions suivantes peuvent être appliquées lors de la définition de profils Antivirus, de profils Antispyware, de profils de Protection contre les vulnérabilités, d'objets Logiciels espions personnalisés, d'objets Vulnérabilité personnalisés ou de Protection DoS.

Action	Description	Profil antivirus	Profil antispyware	Profil de protection contre les vulnérabilit	Objet personnalisé - Logiciels espions et Vulnérabilit	profil de protection du dos
Par défaut	L'action par défaut définie en interne est appliquée pour chaque signature de menace. Pour les profils antivirus, l'action par défaut est appliquée pour la signature de virus.	✓	✓	✓	—	Abandon anticipé aléatoire
autoriser	Autorise le trafic de l'application. *L'action **Autoriser** ne génère pas de journaux associés aux signatures ou aux profils.*	✓	✓	✓	✓	—
alerter	Génère une alerte pour chaque flux de trafic de l'application. L'alerte est sauvegardée dans le journal des menaces.	✓	✓	✓	✓	✓ Génère une alerte lorsque le volume d'attaque (cps) atteint le Seuil d'alarme défini dans le profil.

Action	Description	Profil antivirus	Profil antispyware	Profil de protection contre les vulnérabilit	Objet personnalisé - Logiciels espions et Vulnérabilit	profil de protection du dos
Blocage	Bloque le trafic de l'application.	✓	✓	✓	✓	—
Réinitialiser le client	Pour le protocole TCP, la connexion côté client est réinitialisée. Pour le protocole UDP, la connexion est bloquée.	✓	✓	✓	✓	—
Réinitialiser le serveur	Pour le protocole TCP, la connexion côté serveur est réinitialisée. Pour le protocole UDP, la connexion est bloquée.	✓	✓	✓	✓	—
Réinitialiser les deux	Pour le protocole TCP, la connexion est réinitialisée sur le client et le serveur. Pour le protocole UDP, la connexion est bloquée.	✓	✓	✓	✓	—
Bloquer IP	Bloque le trafic d'une source ou d'une paire source-destination ; configurable pendant une durée déterminée.	—	✓	✓	✓	✓
Entonnoir	Cette action dirige les requêtes DNS provenant de domaines malveillants vers une adresse IP entonnoir. Cette action est disponible pour les	—	—	—	—	—

Action	Description	Profil antivirus	Profil antispyware	Profil de protection contre les vulnérabilit	Objet personnalisé - Logiciels espions et Vulnérabilit	profil de protection du dos
	signatures DNS Palo Alto Networks et pour les domaines personnalisés inclus dans Objets > Listes dynamiques externes.					
Blocage aléatoire anticipé	Amène le pare-feu à supprimer les paquets de manière aléatoire lorsque les connexions par seconde atteignent le seuil de Taux d'activation dans un profil de Protection DoS appliqué à une règle de Protection DoS.	—	—	—	—	✓
cookies SYN ;	Amène le pare-feu à générer des cookies SYN pour authentifier un SYN envoyé par un client lorsque les connexions par seconde atteignent le seuil du Taux d'activation dans un profil de Protection DoS appliqué à une règle de Protection DoS.	—	—	—	—	✓

Vous ne pouvez pas supprimer un profil utilisé dans une règle de politique ; vous devez d'abord supprimer le profil de la règle de politique.

Objets > Profils de sécurité > Antivirus

La page **Antivirus Profiles (Profils antivirus)** vous permet de configurer pour le pare-feu des options d'analyse antivirus du trafic défini. Définissez les applications qui doivent être analysées et l'action à effectuer lorsqu'un virus est détecté. Le profil par défaut inspecte l'ensemble des décodeurs de protocole répertoriés à la recherche de virus, génère des alertes pour les protocoles Simple Mail Transport Protocol (SMTP), Internet Message Access Protocol (IMAP) et Post Office Protocol Version 3 (POP3) et prend l'action par défaut pour d'autres applications (alerte ou refus), en fonction du type de virus détecté. Le profil est ensuite associé à une règle de politique de sécurité pour déterminer le trafic traversant certaines zones à inspecter.

Il est possible d'utiliser des profils personnalisés pour limiter les inspections antivirus sur le trafic entre des zones de sécurité de confiance ou au contraire les renforcer sur le trafic provenant de zones non sécurisées comme Internet, ainsi que sur le trafic vers des destinations hautement sensibles comme des batteries de serveurs.

Pour ajouter un nouveau profil antivirus, sélectionnez l’option Ajouter et saisissez les paramètres suivants :

Champ	Description
Name (Nom)	Saisissez un nom pour le profil (31 caractères maximum). Ce nom apparaît dans la liste de profils antivirus pour la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. N'utilisez que des lettres, des chiffres, des espaces, des tirets, des points et des caractères de soulignement.
Description	Saisissez une description du profil (255 caractères maximum).
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que le profil soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce profil antivirus dans les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres de tous les groupes de périphériques qui héritent du profil.
Action Tab (onglet action) Précisez l'action à effectuer pour les différents types de trafic, tels que FTP et HTTP.	

Champ	Description
Activez la capture de paquets	Sélectionnez cette option pour capturer des paquets identifiés.
Décodeurs et actions	Pour chaque type de trafic que vous voulez inspecter, choisissez une action dans la liste déroulante. Vous pouvez définir différentes actions pour les signatures standard d'antivirus (colonne **Signature Action (Action de signature)**), pour les signatures générées par le système WildFire (**WildFire Signature Action (Action de signature WildFire)**) et pour les menaces malveillantes détectées en temps réel par les modèles WildFire Inline ML (colonne **WildFire Inline ML Action (Action WildFire Inline ML)**). Il se peut que certains environnements exigent une durée d'exposition plus longue pour les signatures antivirus'A0;; par conséquent, cette option vous permet de définir des actions pour les deux types de signature antivirus fournis par Palo Alto Networks. Par exemple, les signatures antivirus standard passent par une période d'exposition plus longue avant d'être publiées (24'A0;heures), tandis que les signatures WildFire peuvent être générées et publiées dans les 15'A0;minutes suivant la détection d'une menace. Vous pouvez alors choisir l'action Alerte au lieu de Bloquer en cas de signature'A0;WildFire. *Pour accroître la sécurité, clonez le profil antivirus par défaut et définissez l'action et l'action WildFire de tous les décodeurs sur **reset-both (réinitialiser les deux)** et associez le profil à toutes les règles de politiques de sécurité qui autorisent le trafic.*
Exceptions d'applications et actions	Le tableau **Applications Exception (Exceptions d'applications)** vous permet de définir les applications à ne pas inspecter. Par exemple, pour bloquer l'ensemble du trafic HTTP excepté pour une application spécifique, vous pouvez définir un profil antivirus pour lequel l'application est une exception. L'action **Block (Bloquer)** est utilisée pour le décodeur HTTP, et l'action **Allow (Autoriser)** pour faire de l'application une exception. Pour chaque exception d'application, sélectionnez l'action à prendre lorsqu'une menace est détectée. Pour une liste d'actions, reportez-vous à la section Actions dans des profils de sécurité. Pour trouver une application, commencez à saisir le nom de l'application dans la zone de saisie. Une liste d'applications correspondantes s'affiche pour vous permettre de faire votre choix. *Si vous croyez qu'une application légitime est mal identifiée comme portant un virus (faux positif), ouvrez un dossier d'assistance auprès du TAC, pour que Palo Alto Networks puisse analyser et résoudre le virus incorrectement identifié. Une fois le problème réglé, supprimez l'exception du profil.*

Champ	Description
Signature Exceptions Tab (Onglet des exceptions de signature) Utilisez l'onglet **Signature Exceptions (Exceptions de signature)** pour définir une liste de menaces que le profil antivirus ignorera. *Créez une exception uniquement si vous êtes certain qu'un virus identifié n'est pas une menace (faux positif). Si vous croyez avoir découvert un faux positif, ouvrez un dossier d'assistance auprès du TAC, pour que Palo Alto Networks puisse analyser et résoudre la signature de virus incorrectement identifiée. Une fois le problème réglé, supprimez immédiatement l'exception du profil.*	
ID de menace	Pour ajouter des menaces précises que vous souhaitez ignorer, saisissez un ID de menace à la fois et cliquez sur **Add (Ajouter)**. Les ID de menace figurent dans le journal des menaces. Voir Surveillance > Journaux.
WildFire Inline ML Tab (Onglet WildFire Inline ML) Utilisez l'onglet **WildFire Inline ML** pour activer et configurer l'analyse WildFire en temps réel pour les fichiers qui utilisent un modèle d'apprentissage machine basé sur le pare-feu. *Palo Alto Networks conseille de transférer des échantillons au cloud WildFire lorsque WildFire inline ML est activé. Cela permet aux échantillons qui déclenchent un faux positif d'être automatiquement corrigés lors d'une analyse secondaire. De plus, il fournit des données d'amélioration des modèles ML pour les mises à jour à venir.*	
Modèles disponibles	Pour chaque **Model (modèle)** Inline ML disponible, vous pouvez sélectionner un des paramètres suivants : • **enable (activer) (hériter des actions par protocole)** : le trafic est inspecté en fonction de vos sélections dans la colonne **Action WildFire Inline ML** dans la section décodeurs de l'onglet **Action**. • **alert-only (override more strict actions to alert) (alrte uniquement - remplace les actions d'alerte plus strictes)** : le trafic est inspecté en fonction de vos sélections dans la colonne **Action WildFire Inline ML** dans la section décodeurs de l'onglet **Action**. Toute action d'un niveau de gravité supérieur à l'alerte (supprimer, réinitialiser le client, réinitialiser le serveur, réinitialiser les deux) sera remplacée par une alerte permettant au trafic de passer tout en générant et en sauvegardant une alerte dans les journaux des menaces. • **disable (désactiver) (pour tous les protocoles)** : Le trafic est autorisé à passer sans aucune action de politique.
Exceptions de fichier	Le tableau **File Exceptions (Exceptions de fichier)** vos permet de définir les fichiers spécifiques que vous ne voulez pas analyser, comme les faux positifs.

Champ	Description
	Pour créer une nouvelle entrée d’exception de fichier, **Add (Ajoutez)** une nouvelle entrée et indiquez le hachage partiel, le nom du fichier et la description du fichier que vous souhaitez exclure de l’application. Pour trouver une exception de fichier existante, commencez par saisir la valeur de hachage partielle, le nom du fichier ou la description dans l’encadré de texte. Une liste des exceptions de fichier correspondant à un de ces valeurs est affichée.  *Vous pouvez trouver des hachages partiels dans les journaux des menaces (**Monitor > Logs > Threat (Surveiller > Journaux > Menace)**).*

Objets > Profils de sécurité > Profil antispyware

Vous pouvez joindre un profil antispyware à une règle de politique de sécurité pour détecter des connexions initiées par des logiciels espions et divers types de logiciels malveillants de commande et de contrôle (C2) installés sur les systèmes de votre réseau. Vous pouvez choisir l'un des deux profils antispyware prédéfinis à associer à une règle de politique de sécurité. Chaque profil présente un ensemble de règles prédéfinies (avec des signatures de menaces) classées en fonction de la gravité de la menace ; chaque signature de menace contient une action par *défaut* définie par Palo Alto Networks.

- Par défaut : le profil par défaut utilise l'action par défaut pour chaque signature, comme indiqué par le package de contenu Palo Alto Networks, lors de la création d'une signature.
- Strict : le profil strict applique un contrôle prioritaire sur l'action définie dans le fichier de signature, dans le cas de menaces présentant un niveau de gravité critique, élevé et moyen, par une action **reset-both (réinitialiser les deux)**. L'action par défaut est exécutée dans le cas de menaces présentant un niveau de gravité moyen et informatif.
- Vous pouvez également créer des profils personnalisés. Par exemple, vous pouvez diminuer la rigueur de l'inspection antispyware pour le trafic entre des zones de sécurité de confiance et maximiser l'inspection du trafic reçu d'Internet ou du trafic envoyé à des actifs protégés, tels que les fermes de serveurs.

Les tableaux suivants décrivent les paramètres des profils antispyware :

Paramètres des profils antispyware	Description
Name (Nom)	Saisissez un nom pour le profil (31 caractères maximum). Ce nom apparaît dans la liste de profils antispyware lors de la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. N'utilisez que des lettres, des chiffres, des espaces, des tirets, des points et des caractères de soulignement.
Description	Saisissez une description du profil (255 caractères maximum).
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que le profil soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce profil antispyware dans les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie

Paramètres des profils antispyware	Description
	que les administrateurs peuvent remplacer les paramètres de tous les groupes de périphériques qui héritent du profil.
Signature Policies Tab (onglet politiques de signature) Les règles antispyware vous permettent de définir une action et un niveau de gravité personnalisés à l'égard des menaces, un nom de menace contenant le texte que vous saisissez et/ou une catégorie de menace, comme les logiciels publicitaires. Cliquez pour **Ajouter** une nouvelle règle, ou vous pouvez sélectionner une règle existante et sélectionnez **Rechercher des signatures correspondantes** pour filtrer les signatures de menaces en fonction de cette règle.	
Nom de la règle	Indiquez le nom de la règle.
Nom de la menace	Saisissez **any (indifférent)** pour que toutes les signatures soient vérifiées, ou saisissez du texte pour vérifier les signatures dont le nom contient le texte saisi.
Catégorie	Choisissez une catégorie ou choisissez **any (n'importe laquelle)** pour faire correspondre toutes les catégories.
Action (Action)	Sélectionnez une action pour chaque menace. Pour une liste d'actions, reportez-vous à la section Actions dans des profils de sécurité. L'action **Default (Par défaut)** est basée sur l'action prédéfinie incluse dans chaque signature fournie par Palo Alto Networks. Pour afficher l'action par défaut correspondant à une signature, sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Anti-Spyware** et cliquez sur **Add (Ajouter)** ou sélectionnez un profil existant. Cliquez sur l'onglet **Exceptions** puis sur **Show all signatures (Montrer toutes les signatures)** pour voir une liste de toutes les signatures et l'**Action** associée. *Pour accroître la sécurité, utilisez les paramètres d'action du profil **strict** prédéfini.*
Capture de paquets	Sélectionnez cette option pour capturer des paquets identifiés. Sélectionnez **single-packet (un seul paquet)** pour capturer un seul paquet lorsqu'une menace est détectée, ou **extended-capture (capture étendue)** pour capturer de 1 à 50 paquets (la valeur par défaut est de 5 paquets). La capture étendue détaille le contexte de la menace, lors de l'analyse des journaux des menaces. Pour visualiser la capture de paquets, sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menace)**, puis recherchez l'entrée du journal qui vous intéresse et cliquez sur la flèche vers le bas de couleur verte dans la seconde colonne. Pour définir le nombre de paquets à capturer, sélectionnez **Device (Périphérique)** >

Paramètres des profils antispyware	Description
	Setup (Configuration) > **Content-ID**, puis modifiez les paramètres Content-ID™. Si l’action d’une menace donnée est autorisé, le pare-feu ne déclenche pas de journal des menaces et ne capture pas de paquets. Si l’action est une alerte, vous pouvez régler la capture de paquets sur un seul paquet ou capture étendue. Toutes les actions de blocage (abandon, blocage et redémarrage) capturent un seul paquet. Le package de contenu sur le périphérique détermine l’action par défaut.  *Activez la capture étendue pour les événements présentant un niveau de gravité critique, élevé et moyen. Utilisez la valeur de capture étendue par défaut de 5 paquets, qui procure suffisamment d’informations pour analyser la menace dans la plupart des cas. (Un trafic de capture de paquets trop important peut entraîner l’abandon des capture de paquets.) N'activez pas la capture étendue pour les événements informatifs et présentant un niveau de gravité faible, car elle n’est pas très utile comparativement à la capture d’informations sur les événements présentant une gravité plus élevée et crée un volume relativement élevé de trafic de faible valeur.*
Sévérité	Choisissez un niveau de gravité (**critical (critique)**, **high (élevé)**, **medium (moyen)**, **low (faible)** ou **informational (informations)**).
Signature Exceptions Tab (Onglet des exceptions de signature) Cet onglet vous permet de modifier l’action d’une signature spécifique. Par exemple, vous pouvez générer des alertes pour un ensemble spécifique de signatures et bloquer tous les paquets correspondant à toutes les autres signatures. Les exceptions de menaces sont généralement configurées lorsque des faux positifs se produisent. Pour faciliter la gestion des exceptions de menaces, vous pouvez les ajouter directement depuis la liste **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menaces)**. Vérifiez que vous disposez des dernières mises à jour afin d’être protégé contre de nouvelles menaces. Vérifiez également que vous disposez des nouvelles signatures contre tout faux positif.	
Exceptions	Sélectionnez **Enable (Activer)** pour chaque menace à laquelle vous voulez affecter une action, ou sélectionnez **All (Tout)** pour répondre à toutes les menaces répertoriées. La liste dépend de l'hôte, de la catégorie et du niveau de gravité sélectionnés. Si la liste est vide, il n'existe aucune menace pour les sélections en cours. Utilisez les exemptions d’adresses IP pour ajouter des filtres d’adresse IP à une exception de menace. Si des adresses IP sont ajoutées à une exception de menace, l’action d’exception pour cette signature ne l’emporte sur l’action de la règle que si la signature est déclenchée par une session dont l’adresse IP source ou de destination correspond à une adresse IP de l’exception. Vous pouvez ajouter jusqu'à 100 adresses IP par signature.

Paramètres des profils antispyware	Description
	Avec cette option, vous n'avez pas besoin de créer une nouvelle règle de politique et un nouveau profil de vulnérabilité pour créer une exception pour une adresse IP spécifique. *Créez une exception uniquement si vous êtes certain qu'un signature identifiée en tant que spyware n'est pas une menace (faux positif). Si vous croyez avoir découvert un faux positif, ouvrez un dossier d'assistance auprès du TAC, pour que Palo Alto Networks puisse analyser et résoudre la signature incorrectement identifiée. Une fois le problème réglé, supprimez l'exception du profil.*

DNS Policies Tab (Onglet politiques DNS)

Le paramètre **DNS Policies (Politiques DNS)** offre un moyen supplémentaire d'identifier les hôtes infectés sur un réseau. Ces signatures détectent les requêtes DNS de noms d'hôte associés à des menaces basées sur DNS.

Vous pouvez configurer des sources de signature DNS spécifiques avec des actions de politique, un niveau de gravité de journal et une capture de paquet séparés. Les hôtes qui lancent des requêtes DNS associées à des sites malveillants figureront dans le rapport du Botnet. De plus, vous pouvez spécifier les adresses IP entonnoirs dans les **DNS Sinkhole Settings (Paramètres de mise en entonnoir DNS)** si vous mettez en entonnoir des requêtes DNS malveillantes.

Signature DNS source	Cette option vous permet de sélectionner les listes auxquelles vous voulez affecter une action lorsqu'une requête DNS survient. Il existe deux options de politique de signature DNS source par défaut : • **Palo Alto Networks Content (contenu Palo Alto Networks)** : une liste de signatures téléchargeable locale qui est mise à jour par les mises à jour de contenu dynamiques. • **Sécurité DNS de Palo Alto Networks** : un service de sécurité DNS basé sur le nuage qui effectue l'analyse proactive des données DNS et qui fournit un accès en temps réel à la base de données complète des signatures DNS de Palo Alto Networks. *Le service exige l'achat et l'activation de la licence de sécurité DNS en plus de la licence de prévention des menaces.* • **External Dynamic Lists (Listes dynamiques externes)** : les listes EDL fonctionnant comme une liste de domaines peuvent être utilisées pour appliquer une action spécifique pour une sélection de domaines,

Paramètres des profils antispyware	Description
	par exemple, en tant que liste d'alerte. Par défaut, les actions de politique pour les listes de domaines sont configurées sur Autoriser. *Une liste d'autorisation EDL n'a pas la priorité sur l'action de politique de domaine spécifiée sous Sécurité DNS. Par conséquent, lorsqu'il existe une correspondance de domaine avec une entrée dans l'EDL et une catégorie de domaine de sécurité DNS, l'action spécifiée sous Sécurité DNS est toujours appliquée, même lorsque l'EDL est explicitement configuré avec une action d'autorisation. Si vous souhaitez ajouter des exceptions de domaine DNS, configurez un EDL avec une action d'alerte ou ajoutez-les à la **DNS Domain/ FQDN Allow List (liste d'autorisation de domaine DNS/FQDN)** située dans l'onglet **DNS Exceptions (Exceptions DNS)**.* Par défaut, les signatures DNS de contenu Palo Alto Networks accessibles localement sont mises en entonnoir, tandis que la sécurité DNS basée sur le cloud est définie sur autoriser. Si vous souhaitez activer la mise en entonnoir à l'aide de la sécurité DNS, vous devez configurer l'action des requêtes DNS pour la mise en entonnoir. L'adresse par défaut utilisée pour la mise en entonnoir appartient à Palo Alto Networks (sinkhole.paloaltonetworks.com). Cette adresse n'est pas statique et ne peut être modifiée par l'intermédiaire d'une mise à jour de contenu sur le pare-feu ou Panorama. **Add (Ajoutez)** une nouvelle liste dynamique externe correspondant au type de domaine que vous avez créé. Pour créer une nouvelle liste, voir Objets > Listes dynamiques externes.
Gravité des journaux	Vous permet de préciser le niveau de gravité des journaux enregistré lorsque que pare-feu détecte un domaine correspondant à une signature DNS.
Action de politique	Choisissez une action à prendre lorsque des requêtes DNS correspondant à des sites malveillants connus sont envoyées. Les options sont les suivantes : **alert (alerte)**, **allow (autoriser)**, **block (bloquer)** ou **sinkhole (mise en entonnoir)**. La **sinkhole (mise en entonnoir)** est l'action par défaut pour les signatures DNS de Palo Alto Networks. L'action DNS Sinkhole (piège DNS) permet aux administrateurs d'identifier les hôtes infectés sur le réseau à l'aide du trafic DNS, même lorsque le pare-feu est au nord d'un serveur DNS local (le pare-feu ne peut pas voir l'auteur de la requête DNS). Lorsqu'une licence de prévention des menaces est installée et qu'un profil antispyware est activé dans un profil de sécurité, une signature DNS se déclenche en cas de requête DNS dirigée vers des domaines malveillants. Dans un déploiement type où le pare-

Paramètres des profils antispyware	Description
	feu est au nord du serveur DNS local, le journal des menaces identifie le résolveur DNS local comme la source du trafic plutôt que l'hôte réellement infecté. La mise en entonnoir des requêtes DNS malveillantes résout ce problème de visibilité en falsifiant des réponses aux requêtes dirigées vers des domaines malveillants, de manière à ce que les clients tentant de se connecter à ces domaines (pour la commande et le contrôle, par exemple) se connectent plutôt à une adresse IP définie par l'administrateur. Les hôtes infectés peuvent ensuite être facilement identifiés dans les journaux du trafic, car tout hôte tentant de se connecter à l'adresse IP entonnoir est probablement infecté par des logiciels malveillants. *Activez la mise en entonnoir DNS lorsque le pare-feu ne peut pas voir l'auteur de la requête DNS (normalement lorsque le pare-feu est au nord d'un serveur DNS local) afin de pouvoir identifier les hôtes infectés. Si vous ne pouvez mettre le trafic en entonnoir, bloquez-le.*
Capture de paquets	Sélectionnez cette option pour une source donnée pour capturer des paquets identifiés. *Activez la capture de paquets sur le trafic mis en entonnoir afin de pouvoir l'analyser et d'obtenir des renseignements sur l'hôte infecté.*
Paramètres de la mise en entonnoir DNS	Après que l'action Entonnoir est définie pour une source de signature DNS, précisez l'adresse IPv4 ou IPv6 qui sera utilisée pour la mise en entonnoir. Par défaut, l'adresse IP entonnoir est définie sur un serveur de Palo Alto Networks. Vous pouvez ensuite utiliser les journaux du trafic ou concevoir un rapport personnalisé qui filtre l'adresse IP entonnoir afin d'identifier les clients infectés. Voici la séquence d'événements qui se produit lorsqu'une requête DNS est mise en entonnoir : Un logiciel malveillant se trouvant sur un ordinateur client infecté envoie une requête'A0;DNS pour résoudre un hôte malveillant sur Internet. La requête DNS du client est envoyée à un serveur DS interne, qui interroge ensuite un serveur DNS public de l'autre côté du pare-feu. La requête DNS correspond à une entrée DNS dans la base de données de signatures DNS précisée ; ainsi l'action Entonnoir sera effectuée dans le cas de cette requête. Le client infecté tente ensuite de démarrer une session avec l'hôte, mais utilise l'adresse IP falsifiée à la place. L'adresse IP falsifiée est l'adresse définie dans l'onglet Signatures DNS des profils antispyware, lorsque l'action Entonnoir est sélectionnée.

Paramètres des profils antispyware	Description
	L’administrateur est alerté lors de la présence d’une requête DNS malveillante dans le journal des menaces. Il peut alors rechercher l’adresse IP entonnoir dans les journaux du trafic et facilement localiser l’adresse IP du client qui tente de démarrer une session avec l’adresse IP entonnoir.
Bloquer les types d’enregistrements DNS	Sélectionnez le(s) type(s) d’enregistrement de ressource DNS utilisé(s) par les requêtes DNS chiffrées que vous souhaitez bloquer. Cela empêche le client de chiffrer le client hello pendant le processus de résolution DNS, bloquant ainsi l’échange de toute information de clé. Les options incluent **SVCB** (type 64), **HTTPS** (type 65) et **ANY** (type 255). *Pour maintenir un fonctionnement optimal des services de sécurité du pare-feu, Palo Alto Networks recommande de bloquer tous les types d’enregistrements prenant en charge ECH.*

DNS Exceptions Tab (Onglet exceptions DNS)

Les exceptions de signature DNS vous permettent d’exclure des ID de menace spécifiques de l’application de politique ainsi que de préciser des listes d’autorisation de domaine/FQDN pour les sources de domaine approuvées.

Pour ajouter des menaces spécifiques que vous souhaitez exclure de la politique, sélectionnez ou cherchez un **Threat ID (ID de menace)**, puis cliquez sur **Enable (Activer)**. Chaque entrée fournit l’**ID de menace**, le **Name (Nom)** et le **FQDN** de l’objet.

Pour **Add (Ajouter)** une liste d’autorisation de domaine ou FQDN, indiquez l’emplacement de la liste d’autorisation ainsi qu’une description appropriée.

Analyse cloud Inline

Inline Cloud Analysis vous permet d'activer et de configurer les paramètres d'analyse en temps réel des menaces C2 avancées par moteur de détection.

Enable cloud inline analysis (Activer l'analyse inline dans le cloud) : permet une analyse en temps réel des menaces C2 avancées sur tous les moteurs d'analyse en ligne disponibles dans le cloud.

Moteurs d’analyse disponibles	Pour chaque moteur d'analyse disponible représentant une catégorie de menace, vous pouvez sélectionner l'une des actions suivantes que vous souhaitez que le pare-feu applique lorsqu'une menace correspondante est détectée : • **Allow (Autoriser)** : Le site Web est autorisé et aucune entrée de journal n'est créée. • **Alerte (Alerter)** : Le site Web est autorisé et une entrée de journal est créée dans le journal de URL Filtering.

Paramètres des profils antispyware	Description
	• **Drop**: abandonne le trafic. Aucune action réinitialisation n'est envoyée à l'hôte/application. • **Reset Client (Réinitialiser le client)** : la connexion côté client est réinitialisée. • **Reset Server (Réinitialiser le serveur)** : la connexion côté serveur est réinitialisée. • **Réinitialiser les deux**: la connexion est réinitialisée sur le client et le serveur. *L'action par défaut pour tous les moteurs d'analyse est l'alerte.*
Exclure de l’analyse du cloud en ligne	Vous permet de sélectionner une liste d'exceptions d'URL ou d'adresses IP qui contourne les moteurs d'analyse de cloud en ligne. Les exceptions peuvent être spécifiées à l'aide d'URL et/ou d'adresses IP. Les exceptions d'URL incluent une EDL (liste dynamique externe) ou une catégorie d'URL personnalisée, tandis que les exceptions d'adresse IP incluent une EDL ou un objet Adresse. Cliquez sur **Add (Ajouter)** pour afficher et sélectionner les options disponibles. Vous pouvez sélectionner les types de liste suivants : • **URL EDL**— Listes dynamiques externes contenant une série d'URL ou une catégorie d'URL personnalisée. • **Adresse IP**— Listes d'adresses IP définies dans une liste dynamique externe ou dans un objet Adresse. *Ne créez des exceptions d'adresse IP et d'URL que lorsque les menaces identifiées ne présentent pas de danger, comme dans le cas d'un faux positif.*

Objets > Profils de sécurité > Protection contre les vulnérabilités

Une règle de politique de sécurité peut inclure la définition d’un profil de protection contre les vulnérabilités qui détermine le niveau de protection en fonction d’un dépassement de capacité de la mémoire tampon, de l’exécution non autorisée de code et d’autres tentatives d’exploitation des vulnérabilités du système. Il existe deux profils prédéfinis disponibles pour la fonction Protection contre les vulnérabilités'A0;:

- Le profil **default (par défaut)** applique l'action par défaut à l'ensemble des vulnérabilités du client et du serveur dont le niveau de gravité est critique, élevé et moyen. Il ne détecte pas les événements de protection contre les vulnérabilités dont le niveau de gravité est faible et informations. Le package de contenu Palo Alto Networks sur le périphérique détermine l’action par défaut.
- Le profil **strict** applique la réponse de blocage à l'ensemble des événements de protection contre les logiciels espions du client et du serveur dont le niveau de gravité est critique, élevé et moyen. Par ailleurs, il utilise l'action par défaut pour les événements de protection contre les vulnérabilités dont le niveau de gravité est faible et informations.

Il est possible d'utiliser des profils personnalisés pour limiter les inspections de vulnérabilité sur le trafic entre des zones de sécurité de confiance ou au contraire renforcer la protection sur le trafic provenant de zones non sécurisées comme Internet, ainsi que sur le trafic vers des destinations hautement sensibles comme des batteries de serveurs. Pour appliquer des profils de protection contre les vulnérabilités à des politiques de sécurité, reportez-vous à la section Politiques > Sécurité.

Appliquez un profil de protection contre les vulnérabilités à chaque règle de politique de sécurité qui autorise le trafic en vue d'assurer la protection contre le dépassement de capacité de la mémoire tampon, l'exécution non autorisée de code et d'autres tentatives d'exploitation des vulnérabilités côté client et côté serveur.

Les paramètres Règles définissent des ensembles de signatures à activer, ainsi que des actions à prendre lorsqu'une signature est déclenchée.

Le paramètre Exceptions vous permet de modifier la réponse à une signature spécifique. Par exemple, vous pouvez bloquer tous les paquets qui correspondent à une signature à l'exception de celui sélectionné, ce qui génère une alerte. L'onglet **Exception** offre des fonctions de filtrage.

La page **Vulnerability Protection (Protection contre les vulnérabilités)** présente un ensemble de colonnes par défaut. D'autres colonnes d'informations sont disponibles depuis le sélecteur de colonnes. Cliquez sur la flèche à droite de l'en-tête d'une colonne et faites votre sélection dans le sous-menu Colonnes.

Les tableaux suivants décrivent les paramètres des profils de protection contre les vulnérabilités :

Paramètres des profils de protection contre les vulnérabilités	Description
Name (Nom)	Saisissez un nom pour le profil (31 caractères maximum). Ce nom apparaît dans la liste de profils de protection contre les vulnérabilités pour la

Paramètres des profils de protection contre les vulnérabilités	Description
	définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. N'utilisez que des lettres, des chiffres, des espaces, des tirets, des points et des caractères de soulignement.
Description	Saisissez une description du profil (255 caractères maximum).
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que le profil soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce profil de Protection contre la vulnérabilité dans les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres de tous les groupes de périphériques qui héritent du profil.
Onglet Règles	
Nom de la règle	Indiquez un nom permettant d'identifier la règle.
Nom de la menace	Indiquez une chaîne textuelle à vérifier. Le pare-feu applique un ensemble de signatures à la règle en recherchant cette chaîne textuelle dans les noms des signatures.
CVE	Indiquez quelles sont les failles et vulnérabilités communes (CVE) si vous voulez limiter les signatures à celles qui correspondent également aux CVE définies. Chaque CVE se présente sous le format CVE-aaaa-xxxx, où aaaa correspond à l'année et xxxx est son identifiant unique. Vous pouvez effectuer une recherche de chaîne dans ce champ. Par exemple, pour trouver les vulnérabilités correspondant à l'année 2011, saisissez « 2011 ».
Type d'hôte	Précisez s'il faut limiter les signatures pour la règle à celles qui se trouvent du côté du client, à celles qui se trouvent du côté du serveur ou aux deux (**any (indifférent)**).
Sévérité	Sélectionnez le niveau de gravité à vérifier (**informational (informations)**, **low (faible)**, **medium (moyen)**, **high (élevé)** ou **critical (critique)**) si

Paramètres des profils de protection contre les vulnérabilités	Description
	vous voulez limiter les signatures à celles qui correspondent également au niveau de gravité spécifié.
Action (Action)	Sélectionnez l'action à appliquer lors du déclenchement d'une règle. Pour une liste d'actions, reportez-vous à la section Actions dans des profils de sécurité. L'action **Default (Par défaut)** est basée sur l'action prédéfinie incluse dans chaque signature fournie par Palo Alto Networks. Pour afficher l'action par défaut correspondant à une signature, sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Vulnerability Protection (Protection contre les vulnérabilités)** et cliquez sur **Add (Ajouter)** ou sélectionnez un profil existant. Cliquez sur l'onglet **Exceptions** puis sur **Show all signatures (Montrer toutes les signatures)** pour voir une liste de toutes les signatures et l'**Action** associée. *Pour renforcer la sécurité, définissez l'action des événements du client et du serveur dont le niveau de gravité est critique, élevé et moyen sur **reset-both (réinitialiser les deux événements)** et utilisez l'action par défaut pour les événements informatifs et présentant un niveau de gravité faible.*
Capture de paquets	Sélectionnez cette option pour capturer des paquets identifiés. Sélectionnez **single-packet (un seul paquet)** pour capturer un seul paquet lorsqu'une menace est détectée, ou **extended-capture (capture étendue)** pour capturer de 1 à 50 paquets (la valeur par défaut est de 5 paquets). La capture étendue détaille le contexte de la menace, lors de l'analyse des journaux des menaces. Pour visualiser la capture de paquets, sélectionnez **Monitor (Surveillance)** > **Logs (Journaux)** > **Threat (Menaces)**, puis recherchez l'entrée du journal qui vous intéresse et cliquez sur la flèche vers le bas de couleur verte dans la seconde colonne. Pour définir le nombre de paquets à capturer, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Content-ID** puis modifiez les paramètres Content-ID. Si l'action d'une menace donnée est autorisé, le pare-feu ne déclenche pas de journal des menaces et ne capture pas de paquets. Si l'action est une alerte, vous pouvez régler la capture de paquets sur un seul paquet ou capture étendue. Toutes les actions de blocage (abandon, blocage et redémarrage) capturent un seul paquet. Le package de contenu sur le périphérique détermine l'action par défaut.

Paramètres des profils de protection contre les vulnérabilités	Description
	Activez la capture étendue pour les événements présentant un niveau de gravité critique, élevé et moyen et la capture d'un seul paquet pour les événements présentant un niveau de gravité faible. Utilisez la valeur de capture étendue par défaut de 5 paquets, qui procure suffisamment d'informations pour analyser la menace dans la plupart des cas. (Un trafic de capture de paquets trop important peut entraîner l'abandon des capture de paquets.) N'activez pas la capture des paquets pour les événements informatifs, car elle n'est pas très utile comparativement à la capture d'informations sur les événements présentant une gravité plus élevée et crée un volume relativement élevé de trafic de faible valeur. *Appliquez la capture des paquets étendue en utilisant la même logique que vous utilisez pour décider du trafic à journaliser ; prenez des captures étendues du trafic que vous journalisez, y compris le trafic que vous bloquez.*
Onglet Exceptions	
Activer	Sélectionnez **Enable (Activer)** pour chaque menace à laquelle vous voulez affecter une action, ou sélectionnez **All (Tout)** pour répondre à toutes les menaces répertoriées. La liste dépend de l'hôte, de la catégorie et du niveau de gravité sélectionnés. Si la liste est vide, il n'existe aucune menace pour les sélections en cours.
ID	
ID constructeur	Indiquez des ID constructeur si vous voulez limiter les signatures à celles correspondant également aux ID constructeur définis. Par exemple, les ID constructeur correspondant à Microsoft se présentent sous la forme MSaa-xxx, où aa correspond à l'année au format deux chiffres et xxx est son identifiant unique. Pour trouver le constructeur Microsoft pour l'année 2009, saisissez « MS09 » dans le champ de recherche.

Paramètres des profils de protection contre les vulnérabilités	Description
Nom de la menace	*Créez une exception uniquement si vous êtes certain qu'une menace identifiée n'est pas une menace (faux positif). Si vous croyez avoir découvert un faux positif, ouvrez un dossier d'assistance auprès du TAC, pour que Palo Alto Networks puisse enquêter sur la menace incorrectement identifiée. Une fois le problème réglé, supprimez immédiatement l'exception du profil.* La base de données des signatures contre les vulnérabilités contient des signatures qui indiquent une attaque par force brute ; par exemple, l'ID de menace 40001 est déclenché par une attaque FTP par force brute. Les signatures de force brute sont déclenchées lorsqu'un événement survient au-delà d'un seuil temporel donné. Les seuils sont préconfigurés pour les signatures de force brute et peuvent être modifiés en cliquant sur modifier () à côté du nom de la menace sous l'onglet **Vulnerability (Vulnérabilité)** (avec sélection de l'option **Custom (Personnaliser)**). Vous pouvez définir le nombre d'accès par unité de temps et si le seuil s'applique à la source, la destination ou les deux. Des seuils peuvent être appliqués à une adresse IP source, une adresse IP de destination ou à une combinaison d'adresses IP source et de destination. l'action par défaut est indiquée entre parenthèses.
Exceptions d'adresse IP	Cliquez sur la colonne **IP Address Exemptions (Exemptions d'adresses IP)** pour **Add (ajouter)** des filtres d'adresse IP à une exception de menace. Lorsque vous ajoutez une adresse IP à une exception de menace, l'action d'exception pour cette signature ne l'emportera sur l'action de la règle que si la signature est déclenchée par une session dont l'adresse IP source ou de destination correspond à une adresse IP de l'exception. Vous pouvez ajouter jusqu'à 100 adresses IP par signature. Vous devez entrer une adresse IP unicast (c'est-à-dire une adresse sans masque de réseau), telle que 10.1.7.8 ou 2001:db8:123:1::1. En ajoutant des exemptions d'adresses IP, vous n'avez pas besoin de créer une nouvelle règle de politique et un nouveau profil de vulnérabilité pour créer une exception pour une adresse IP spécifique.
règle	
CVE	La colonne **CVE** affiche les identifiants correspondant aux failles et vulnérabilités communes (CVE). Ces identifiants uniques concernent les vulnérabilités de sécurité informatique courantes.
Hôte	

Paramètres des profils de protection contre les vulnérabilités	Description
Catégorie	Sélectionnez une catégorie de vulnérabilité si vous voulez limiter les signatures à celles correspondant à cette catégorie.
Sévérité	
Action (Action)	Choisissez une action dans la liste déroulante ou dans le menu **Action** en haut de la liste pour appliquer la même action à l'ensemble des menaces.
Capture de paquets	Sélectionnez **Packet Capture (Capture de paquets)** pour capturer des paquets identifiés.
Afficher toutes les signatures	Activez **Show all signatures (Afficher toutes les signatures)** pour obtenir la liste de toutes les signatures. Si **Show all signatures (Afficher toutes les signatures)**, est désactivé, seules les signatures qui sont des exceptions sont affichées.

Analyse cloud Inline

Inline Cloud Analysis (analyse en ligne dans le Cloud) vous permet d'activer et de configurer les paramètres d'analyse en temps réel des vulnérabilités d'injection de commandes et d'injection SQL par moteur de détection.

Activer l'analyse en ligne dans le cloud : active les moteurs de détection de deep learning en ligne utilisés pour détecter les vulnérabilités d'injection de commandes et d'injection SQL sur tous les moteurs d'analysecloud en ligne disponibles.

Moteurs d'analyse disponibles	Pour chaque moteur d'analyse disponible représentant une catégorie de menace, vous pouvez sélectionner l'une des actions suivantes que vous souhaitez que le pare-feu applique lorsqu'une vulnérabilité correspondante est détectée : • **Allow (Autoriser)** : La demande est autorisée et aucune entrée de journal n'est créée. • **Alerte**: la demande est autorisée et une entrée de journal des menaces est générée. • **Reset Client (Réinitialiser le client)** : la connexion côté client est réinitialisée. • **Reset Server (Réinitialiser le serveur)** : la connexion côté serveur est réinitialisée. • **Réinitialiser les deux**: la connexion est réinitialisée sur le client et le serveur. *L'action par défaut pour tous les moteurs d'analyse est l'alerte.*

Paramètres des profils de protection contre les vulnérabilités	Description
Exclure de l’analyse du cloud en ligne	Vous permet de sélectionner une liste d'exceptions d'URL ou d'adresses IP qui contourne les moteurs d'analyse de cloud en ligne. Les exceptions peuvent être spécifiées à l'aide d'URL et/ou d'adresses IP. Les exceptions d'URL incluent une EDL (liste dynamique externe) ou une catégorie d'URL personnalisée, tandis que les exceptions d'adresse IP incluent une EDL ou un objet Adresse. Cliquez sur **Add (Ajouter)** pour afficher et sélectionner les options disponibles. Vous pouvez sélectionner les types de liste suivants : • **URL EDL**— Listes dynamiques externes contenant une série d'URL ou une catégorie d'URL personnalisée. • **Adresse IP**— Listes d'adresses IP définies dans une liste dynamique externe ou dans un objet Adresse.  *Ne créez des exceptions d'adresse IP et d'URL que lorsque les menaces identifiées ne présentent pas de danger, comme dans le cas d'un faux positif.*

Objets > Profils de sécurité > URL Filtering

Vous pouvez utiliser les profils de URL filtering (URL Filtering) pour non seulement contrôler l'accès au contenu Web, mais également pour contrôler l’interaction des utilisateurs avec le contenu Web.

Que voulez-vous faire ?	Reportez-vous à la section :
Contrôler l’accès aux sites Web en fonction de la catégorie URL.	Catégories de filtrage des URL
Détectez les envois d’informations d’identification d’entreprise, puis décidez les catégories d’URL auxquelles les utilisateurs peuvent soumettre des informations d’identification.	Détection des informations d'identification de l'utilisateur Catégories de URL Filtering
Bloquez les résultats de la recherche si l’utilisateur final n’utilise pas les paramètres de recherche sécurisée les plus stricts dans la recherche.	Paramètres de filtrage des URL
Activer la journalisation des en-têtes HTTP.	Paramètres de filtrage des URL
Contrôler l'accès aux sites Web au moyen d’en-têtes HTTP personnalisés.	Insertion de l'en-tête HTTP
Activez la catégorisation en ligne dans le cloud et locale pour analyser les pages Web en temps réel à la recherche de contenu malveillant.	Catégorisation en ligne
Vous souhaitez en savoir plus ?	• En savoir plus sur la configuration du URL Filtering. • Utilisez les catégories d’URL pour prevent credential phishing (empêcher l’hameçonnage des informations d’identification). • Pour créer des catégories d’URL personnalisées, voir Objets > Objets personnalisés > Catégorie d’URL. • Pour importer une liste d’URL que vous souhaitez appliquer, sélectionnez Objets > Listes dynamiques externes.

Paramètres généraux du filtrage des URL

Le tableau suivant décrit les paramètres généraux de filtrage des URL.

Paramètres généraux	Description
Name (Nom)	Saisissez un nom pour le profil (31 caractères maximum). Ce nom apparaît dans la liste de profils de filtrage des URL pour la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Description	Saisissez une description du profil (255 caractères maximum).
Partagé	Sélectionnez cette option si vous souhaitez que le profil soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce profil de filtrage des URL dans les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres de tous les groupes de périphériques qui héritent du profil.

Catégories de URL Filtering

Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **URL Filtering (URL Filtering)** > **Categories (Catégories)** pour contrôler l'accès aux sites Web en fonction des catégories d'URL.

Paramètres de catégories	Description
Catégorie	Affiche les catégories d'URL et les listes pour lesquelles vous pouvez définir l'accès Web et la politique d'utilisation. Par défaut, les autorisations **Site Access (Accès au site)** et **User Credential Submission (Envoi des informations d'identification de l'utilisateur)** pour toutes les catégories sont définies sur **Allow (Autoriser)**. Les catégories d'URL et les listes sont groupées dans trois menus déroulants : • **Custom URL Categories (Catégories d'URL personnalisées)** : Sélectionnez Objets > Objets personnalisés > Catégories d'URL pour définir une catégorie d'URL personnalisée. Vous pouvez fonder les

Paramètres de catégories	Description
	catégories d'URL personnalisées sur une liste d'URL ou sur plusieurs catégories prédéfinies. • **External Dynamic URL Lists (Listes d'URL dynamiques externes)** : Sélectionnez Objets > Listes dynamiques externes pour permettre au pare-feu d'importer une liste d'URL d'un serveur Web. • **Pre-defined Categories (Catégories prédéfinies)** : Dresse la liste de toutes les catégories d'URL définies par PAN-DB, l'URL Palo Alto Networks et la base de données IP du cloud. ***Block (Bloquez)*** *toutes les catégories d'URL dangereuses qui sont connues pour vous protéger contre l'infiltration d'exploitations, le téléchargement de fichiers malveillants, les activités de commande et de contrôle et l'exfiltration de données :* ***command-and-control (commande et contrôle)***, ***copyright-infringement (violation des droits d'auteur)***, ***dynamic-dns (DNS dynamique)***, ***extremism (extrémisme)***, ***malware (logiciel malveillant)***, ***phishing (hameçonnage)***, ***proxy-avoidance-and-anonymizers (évitement de proxy et anonymiseurs)***, ***unknown (inconnu)***, ***newly-registered-domain (domaine nouvellement enregistré)***, ***grayware (logiciel indésirable)*** *et* ***parked (parqué)***. *Pour introduire graduellement une politique d'interdiction, définissez les catégories sur Continuer et créez une page de réponse personnalisée pour informer vos utilisateurs de vos politiques d'utilisation et les prévenir qu'ils consultent un site qui pourrait présenter une menace. À l'issue d'une période de temps appropriée, passez à une politique qui bloque ces sites éventuellement malveillants.*
Accès au site	Pour chaque catégorie d'URL, sélectionnez la mesure à prendre si un utilisateur tente d'accéder à une URL de cette catégorie : • **alert (alerte)** - Autorise l'accès au site Web, mais ajoute une alerte dans le journal des URL chaque fois qu'un utilisateur accède à cette URL. *Définissez la valeur d'****alert (alerte)*** *en tant qu'action pour les catégories de trafic que vous ne bloquez pas. Ainsi, il journalise les tentatives d'accès et procure un aperçu du trafic.*

Paramètres de catégories	Description
	• **allow (autoriser)** - Autorise l'accès au site Web. *Comme l'option **allow (autoriser)** ne journalise pas le trafic non bloqué, définissez **alert (alerter)** en tant qu'action pour les catégories de trafic que vous ne bloquez pas si vous voulez journaliser les tentatives d'accès et obtenir un aperçu du trafic.* • **block (bloquer)** - Interdit l'accès au site Web. Si l'Accès au site à une catégorie d'URL est défini sur bloqué, les autorisations d'Envoi des informations d'identification de l'utilisateur sont également automatiquement définies sur bloquer. • **Continue (continuer)** : affiche aux utilisateurs une page d'avertissement pour les décourager d'accéder au site Web. L'utilisateur doit alors **Continue (continuer)** vers le site Web s'il décide d'ignorer l'avertissement. *Les pages continue (avertissement) ne s'affichent pas correctement sur les machines client configurées pour utiliser un serveur proxy.* • **override (remplacer)** : affiche une page de réponse qui invite l'utilisateur à saisir un mot de passe valide afin d'accéder au site. Configurez les paramètres de Contrôle prioritaire sur l'URL par l'administrateur (**Device (Périphérique)** > **Setup (Configuration)** > **Content ID (ID de contenu)**) pour gérer le mot de passe et les autres paramètres de contrôle prioritaire. (Reportez-vous également au tableau Paramètres de gestion dans Périphérique > Configuration > Content-ID). *Les pages Override (Contrôle prioritaire) ne s'affichent pas correctement sur les machines client configurées pour utiliser un serveur proxy.* • **none (aucun)** (catégorie d'URL personnalisée uniquement) – Si vous avez créé des catégories d'URL personnalisées, définissez l'action sur **none (aucun)** pour autoriser le pare-feu à hériter de la catégorie de filtrage des URL que lui a assignée votre fournisseur de base de données d'URL. La définition de l'action sur **none (aucune)** vous donne la souplesse d'ignorer des catégories personnalisées dans votre profil de filtrage des URL tout en vous permettant d'utiliser la catégorie d'URL personnalisée en tant que critère de correspondance dans les règles de politique (sécurité, déchiffrement et de QoS) afin d'effectuer des exceptions ou d'affecter diverses actions. Pour supprimer une catégorie d'URL personnalisée, vous devez définir l'action sur **none (aucune)** dans tous les profils où la catégorie personnalisée est utilisée. Pour plus

Paramètres de catégories	Description
	d'informations sur les catégories d'URL personnalisées, voir Objets > Objets personnalisés > Catégorie d'URL.
Envoi des informations d'identification de l'utilisateur	Pour chaque catégorie d'URL, sélectionnez les **User Credential Submissions (Envois des informations d'identification de l'utilisateur)** pour autoriser les utilisateurs à saisir des informations d'identification d'entreprise valides sur une URL de cette catégorie ou le leur interdire. Avant de pouvoir contrôler les envois des informations d'identification de l'utilisateur en fonction de la catégorie d'URL, vous devez activer la détection d'envoi d'informations d'identification (sélectionnez l'onglet **Détection des informations d'identification de l'utilisateur**). Les catégories d'URL avec **Site Access (Accès au site)** défini sur bloquer sont automatiquement configurées pour bloquer les envois d'informations d'identification de l'utilisateur. • **alert (alerter)** – Autorise les utilisateurs à saisir des informations d'identification sur le site Web, mais génère un journal de Filtrage des URL chaque fois qu'un utilisateur saisit des informations d'identification sur les sites de cette catégorie. • **allow (autoriser)** (par défaut) – Autorise les utilisateurs à saisir des informations d'identification sur le site Web. • **block (bloquer)** - Empêche les utilisateurs de saisir des informations d'identification sur le site Web. Une page de réponse anti-hameçonnage par défaut bloque les envois d'informations d'identification de l'utilisateur. • **continue (continuer)** – Affiche une page de réponse aux utilisateurs qui les invite à sélectionner Continuer pour saisir des informations d'identification sur le site. Par défaut, une page de poursuite anti-hameçonnage s'affiche pour avertir les utilisateurs lorsqu'ils tentent de saisir des informations d'identification sur des sites pour lesquels la saisie d'informations d'identification n'est pas recommandée. Vous pouvez choisir de créer une page de réponse personnalisée pour avertir les utilisateurs contre les tentatives d'hameçonnage ou pour leur apprendre à ne pas réutiliser des informations d'identification d'entreprise valides sur d'autres sites Web.
Vérifier la catégorie d'URL	Cliquez pour accéder à la base de données PAN-DB URL Filtering où vous pouvez saisir une URL ou une adresse IP pour afficher les informations de catégorisation.
Filtrage dynamique des URL (activé par défaut) (Configurable pour BrightCloud uniquement)	Sélectionnez cette option pour activer la recherche sur le Cloud afin de catégoriser l'URL. Cette option est appelée si la base de données locale ne parvient pas à catégoriser l'URL. Si l'URL n'est pas résolue au bout de 5 secondes, la réponse qui s'affiche est `Not résolu URL`.

Paramètres de catégories	Description
	Pour PAN-DB, cette option est activée par défaut et n'est pas configurable.

Paramètres de URL Filtering

Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **URL Filtering (URL Filtering)** > **URL Filtering Settings (Paramètres de URL Filtering)** pour appliquer des paramètres de recherche sécurisés et pour activer la journalisation des en-têtes HTTP.

Paramètres de filtrage des URL	Descriptions
Consigner la page de conteneur uniquement Par défaut : Activé	Sélectionnez cette option pour ne consigner que les URL qui correspondent au type de contenu défini. Le pare-feu ne journalise pas les liens Web liés aux journaux au cours de la session, comme les liens de publicités et de contenu, qui réduit la journalisation et la charge mémoire tout en journalisant les URL pertinents. *Si vous utilisez des proxys qui masquent l'adresse IP initiale de la source, activez l'option **X-Forwarded-For** de la journalisation de l'en-tête HTTP pour préserver l'adresse IP initiale de l'utilisateur qui initie la requête de la page Web.*
Activer la mise en œuvre de la recherche sécurisée Par défaut : Désactivé Une licence de filtrage des URL n'est pas requise pour utiliser cette fonctionnalité.	Sélectionnez cette option pour mettre en œuvre le filtrage strict de la recherche sécurisée. De nombreux moteurs de recherche incluent un paramètre de recherche sécurisée qui filtre les images et vidéos réservées aux adultes dans le trafic renvoyé d'une recherche. Lorsque vous sélectionnez le paramètre pour Activer la mise en œuvre de la recherche sécurisée, le pare-feu bloque les résultats de la recherche si l'utilisateur final n'utilise pas les paramètres de recherche sécurisée les plus stricts dans sa recherche. Le pare-feu peut appliquer la recherche sécurisée pour les moteurs de recherche suivants : Google, Yahoo, Bing, Yandex et YouTube. Il s'agit d'un paramètre visant à fournir le meilleur résultat possible et les moteurs de recherche ne garantissent nullement que son fonctionnement soit compatible avec tous les sites Web. Pour utiliser la mise en œuvre de la recherche sécurisée, vous devez activer ce paramètre, puis associer le profil de filtrage des URL à une règle de politique de Sécurité. Le pare-feu bloquera alors tout trafic renvoyé d'une recherche correspondant qui n'utilise pas les paramètres de recherche sécurisée les plus stricts.

Paramètres de filtrage des URL	Descriptions
	Si vous effectuez une recherche sur Yahoo Japan (yahoo.co.jp) alors que vous êtes connecté à votre compte Yahoo, l'option de verrouillage du paramètre de recherche doit également être activée. *Pour empêcher les utilisateurs de contourner cette fonction en utilisant d'autres moteurs de recherche, configurez le profil de filtrage des URL pour bloquer la catégorie Moteurs de recherche et autoriser l'accès à Google, Bing, Yahoo, Yandex et YouTube.*
Journalisation de l'en-tête HTTP	L'activation de la journalisation de l'en-tête HTTP fournit une visibilité des attributs inclus dans la demande HTTP envoyée à un serveur. Lorsque cette option est activée, une ou plusieurs des paires attributs/valeurs suivantes sont enregistrées dans le journal de filtrage des URL : • User-Agent : le navigateur Web utilisé par l'utilisateur pour accéder à l'URL. Ces informations sont incluses dans la demande HTTP envoyée au serveur. Par exemple, la valeur User-Agent dans le journal peut être Internet Explorer ou Firefox. Celle-ci peut contenir 1024 caractères maximum. • Referer : l'URL de la page Web associée qui relie l'utilisateur à une autre page Web ; il s'agit de la source qui a redirigé (référé) l'utilisateur vers (à) la page Web demandée. La valeur référente peut contenir 256 caractères maximum. • X-Forwarded-For : champ d'en-tête qui conserve l'adresse IP de l'utilisateur ayant demandé la page Web. Elle vous permet d'identifier l'adresse IP de l'utilisateur, ce qui est particulièrement utile si vous disposez d'un serveur proxy sur votre réseau ou que vous avez mis en œuvre la traduction NAT source, qui masque l'adresse IP de l'utilisateur de telle manière que toutes les demandes semblent provenir de l'adresse IP du serveur proxy ou d'une adresse IP commune. La valeur X-Forwarded-For peut contenir 128 caractères maximum.

Détection des informations d'identification de l'utilisateur

Sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **URL Filtering (URL Filtering)** > **User Credential Detection(Détection des informations d'identification de l'utilisateur)** pour que le pare-feu détecte les situations où les utilisateurs soumettent leurs informations d’identification d’entreprise.

Configurez la détection des informations d'identification de l'utilisateur pour que les utilisateurs puissent transmettre leurs informations d'identification uniquement aux sites qui correspondent à des catégories d'URL spécifiées, ce qui permet de réduire la surface d'attaque en empêchant la soumission d'informations d'identification à des sites appartenant à des catégories non approuvées. Si vous bloquez toutes les catégories d'URL dans un profil de filtrage des URL pour la soumission des informations d'identification, vous n'avez pas à vérifier les informations d'identification.

Le pare-feu utilise une des trois méthodes pour détecter les informations d'identification valides saisies sur ces pages Web. Chaque méthode nécessite l'utilisation de User-ID™ qui permet au pare-feu de comparer les envois de nom d'utilisateur et de mot de passe aux pages Web et des informations d'identification d'entreprise valides. Sélectionnez une de ces méthodes pour ensuite continuer à prevent credential phishing (Empêcher l'hameçonnage des informations d'identification) en fonction de la catégorie d'URL.

Vous devez configurer le pare-feu pour decrypt (déchiffrer) le trafic que vous voulez surveiller pour les informations d'identification des utilisateurs.

Paramètres de Détection des informations d'identification de l'utilisateur	Description
Utilisateur IP	Cette méthode de détection des informations d'identification vérifie les envois de noms d'utilisateur valides. Vous pouvez utiliser cette méthode pour détecter les envois d'informations d'identification incluant un nom d'utilisateur d'entreprise valide (quel que soit le mot de passe qui l'accompagne). Le pare-feu détermine une correspondance de nom d'utilisateur en vérifiant que le nom d'utilisateur correspond à l'utilisateur connecté à l'adresse IP source de la session. Pour utiliser cette méthode, le pare-feu fait correspondre le nom d'utilisateur saisi à la table de mappage adresse IP / nom d'utilisateur. Pour utiliser cette méthode, vous pouvez utiliser n'importe laquelle des méthodes de mappage d'utilisateur décrites dans Mappage d'adresses IP à des utilisateurs.
mappage de groupe	Le pare-feu détermine si le nom d'utilisateur qu'un utilisateur saisit sur un site restreint correspond à un nom d'utilisateur d'entreprise valide. Pour ce faire, le pare-feu fait correspondre le nom d'utilisateur saisi à la liste des noms d'utilisateur dans sa table de mappage utilisateur / groupe pour détecter quand les utilisateurs saisissent un nom d'utilisateur sur un site d'une catégorie restreinte. Cette méthode ne vérifie que les envois de noms d'utilisateur d'entreprise en fonction de l'appartenance à un groupe LDAP, ce qui simplifie la configuration, mais l'expose davantage aux faux positifs. Vous devez activer le mappage de groupe pour utiliser cette méthode.

Paramètres de Détection des informations d'identification de l'utilisateur	Description
Informations d'identification du domaine	Cette méthode de détection des informations d'identification permet au pare-feu de vérifier un nom d'utilisateur d'entreprise valide et le mot de passe y étant associé. Le pare-feu détermine si le nom d'utilisateur et le mot de passe saisis par un utilisateur correspondent au nom d'utilisateur d'entreprise et au mot de passe de ce même utilisateur. Pour ce faire, le pare-feu doit être capable de faire correspondre les envois d'informations d'identification à des noms d'utilisateur et des mots de passe d'entreprise valides et vérifier que le nom d'utilisateur saisi correspond à l'adresse IP de l'utilisateur connecté. Ce mode est pris en charge uniquement avec l'agent User-ID basé sur Windows et exige que l'agent User-ID soit installé sur un contrôleur de domaine en lecture seule (RODC) et équipé de l'Extension service d'informations d'identification User-ID. Pour utiliser cette méthode, vous devez également activer l'option permettant à User-ID de map IP addresses to users (effectuer le Mappage d'adresses IP vers des utilisateurs) en utilisant l'une des méthodes de mappage d'utilisateur prises en charge, y compris la Politique d'authentification, Authentication Portal et GlobalProtect™. Reportez-vous à la section Empêcher le hameçonnage des informations d'identification pour plus d'informations sur chacune des méthodes que le pare-feu peut utiliser pour vérifier les envois d'informations d'identification d'entreprise valides et sur les étapes permettant d'activer la prévention contre l'hameçonnage.
Gravité des journaux détectée par un nom d'utilisateur valide	Définissez la gravité pour les journaux qui indiquent que le pare-feu a détecté une saisie de nom d'utilisateur valide sur un site Web. Cette gravité des journaux est associée à des événements où un nom d'utilisateur valide est saisi sur des sites Web avec des autorisations d'envoi des informations d'identification pour alerter, bloquer ou continuer. Les journaux qui enregistrent quand un utilisateur saisit un nom d'utilisateur valide sur un site Web pour lequel les envois d'informations d'identification sont autorisés ont une gravité de niveau information. Sélectionnez **Catégories** pour vérifier ou ajuster les catégories d'URL auxquelles les envois d'informations d'identification sont autorisés et bloqués. *Définissez la gravité des journaux sur moyenne ou plus.*

Insertion de l'en-tête HTTP

Pour activer la gestion de l’accès aux applications Web par le pare-feu en insérant des en-têtes HTTP et leurs valeurs dans des requêtes HTTP, sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **URL Filtering (Filtrage des URL)** > **HTTP Header Insertion (Insertion de l'en-tête HTTP)**.

Le pare-feu prend en charge l’insertion d’en-têtes pour le trafic HTTP/1.x uniquement ; le pare-feu ne prend pas en charge l’insertion d’en-têtes pour trafic HTTP/2.

Vous pouvez créer des entrées d’insertion en fonction d’un type d’insertion d’en-tête HTTP prédéfini ou vous pouvez créer votre propre type personnalisé. L’insertion d’en-têtes s’effectue généralement pour les en-têtes HTTP personnalisés, mais vous pouvez également insérer des en-têtes HTTP standard.

L’insertion d’un en-tête se produit lorsque :

1. Une requête HTTP correspond à une règle de politique de sécurité qui possède une ou plusieurs entrées d’insertion d'un en-tête HTTP configurées.
2. Un domaine spécifié correspond à un domaine qui se trouve dans l’en-tête Hôte HTTP.
3. L’action est tout sauf `block (bloquer)`.

Le pare-feu peut procéder à l’insertion de l'en-tête HTTP seulement pour les méthodes GET, POST, PUT et HEAD.

Si vous activez l’insertion de l'en-tête HTTP et que l’en-tête identifié est absent d’une requête, le pare-feu insère l’en-tête. Si l’en-tête identifié existe déjà dans la requête, le pare-feu remplace alors les valeurs de l’en-tête par celles que vous avez indiquées.

Add (Ajoutez) une entrée d’insertion ou sélectionnez une entrée d’insertion existante pour la modifier. Au besoin, vous pouvez également sélectionner une entrée d’insertion et la **Delete (Supprimer)**.

L’action de la liste d'interdictions prise par défaut à l’égard d’une nouvelle entrée d’insertion d'en-tête HTTP est `block (bloquer)`. Si vous souhaitez qu’une action différente soit prise, allez à Catégories de URL Filtering *et sélectionnez l’action appropriée. Vous pouvez également ajouter l’entrée d’insertion à un profil pour lequel l'action souhaitée est configurée.*

Paramètres d’insertion de l'en-tête HTTP	Description
Name (Nom)	Le **Name (Nom)** de cette entrée d’insertion de l'en-tête HTTP.
Type	Le **Type** d’entrée que vous voulez créer. Les entrées peuvent être prédéfinies ou personnalisées. Le pare-feu utilise les mises à jour du contenu pour remplir et maintenir les entrées prédéfinies. Pour inclure le nom d'utilisateur dans l’en-tête HTTP, sélectionnez **Dynamic Fields (Champs dynamiques)**.

Paramètres d’insertion de l'en-tête HTTP	Description
Domaines	L’insertion d’un en-tête se produit lorsqu’un domaine de cette liste correspond à l’en-tête Hôte de la requête HTTP. Si vous créez une entrée prédéfinie, la liste des domaines est prédéfinie dans une mise à jour de contenu. Cette façon de faire suffit pour la plupart des cas pratiques, mais vous pouvez ajouter ou supprimer des domaines, au besoin. Pour créer une entrée personnalisée, **Add (Ajouter)** au moins un domaine à la liste. Chaque nom de domaine peut comporter un maximum de 256 caractères et vous pouvez identifier un maximum de 50 domaines pour chaque entrée. Vous pouvez utiliser un astérisque (*) comme caractère générique pour trouver une correspondance avec toute requête de domaine spécifié (par exemple, *.etrade.com).
En-tête	Lorsque vous créez une entrée prédéfinie, la liste des en-têtes est renseignée dans le cadre d’une mise à jour de contenu. Cette façon de faire suffit pour la plupart des cas pratiques, mais vous pouvez ajouter ou supprimer des en-têtes, au besoin. Lorsque vous créez une entrée personnalisée, ajoutez un ou plusieurs en-têtes (maximum de cinq) à cette liste. Les noms des en-têtes peuvent comporter un maximum de 100 caractères, mais ne peuvent inclure d’espace. Pour inclure le nom d'utilisateur dans l’en-tête HTTP, sélectionnez **X-Authenticated-User** puis sélectionnez la **Value (Valeur)**, ou **Add (Ajoutez)** un nouvel en-tête.
Valeur	Configurez la **Value (Valeur)** en utilisant un maximum de 16K caractères. La valeur d’en-tête varie selon l’information que vous désirez inclure dans l’en-tête HTTP pour les domaines spécifiés. Par exemple, manage user access to SaaS applications (gérez l’accès des utilisateurs aux applications SaaS) en sélectionnant des predefined types (types prédéfinis) ou en utilisant des custom entries (saisies personnalisées). Pour inclure le nom d'utilisateur dans l’en-tête HTTP, sélectionnez le domaine et le format du nom d'utilisateur que le périphérique de sécurité nécessite : • **`($domain)\($user)`** • **`WinNT://($domain)/($user)`** Vous pouvez également saisir un format personnalisé en utilisant les jetons dynamiques **`($user)`** et **`($domain)`** (par exemple, **`($user)@($domain)`**).

Paramètres d'insertion de l'en-tête HTTP	Description
	Le pare-feu remplit les jetons dynamiques de l'utilisateur et du domaine en utilisant le nom d'utilisateur principal dans le profil de mappage de groupe. *Utilisez chaque jeton dynamique* ***($user)*** *et* ***($domain)*** *une seule fois par valeur.*
Journaux	Sélectionnez **Log (Journal)** pour activer la journalisation de cette entrée d'insertion d'en-tête.

Catégorisation en ligne

Sélectionnez **Objets** > **Profils** > **de sécurité Filtrage d'URL** > **Catégorisation Inline** pour activer et configurer l'analyse de page Web en temps réel.

Champ	Description
Utilisez l'onglet **Catégorisation Inline** pour activer l'analyse des pages Web en temps réel et gérer les exceptions d'URL.	
L'analyse d'URL en temps réel est disponible localement en tant que mécanisme de détection basé sur un pare-feu et dans le cloud dans le cadre du service de filtrage d'URL avancé. • **Activer la catégorisation locale inline** : permet une analyse en temps réel du trafic URL à l'aide de modèles d'apprentissage automatique basés sur un pare-feu, afin de détecter et d'empêcher les variantes de phishing malveillantes et les exploits JavaScript d'entrer dans votre réseau. • **Activer la catégorisation Inline** dans le cloud : permet l'analyse en temps réel des URL en transférant le contenu suspect des pages Web vers le cloud pour une analyse supplémentaire, à l'aide de détecteurs basés sur l'apprentissage automatique qui complètent les moteurs d'analyse utilisés par le ML en ligne local.	
Exceptions	Vous pouvez définir des **exceptions** d'URL pour des sites Web spécifiques que vous ne souhaitez pas analyser à l'aide de la catégorisation en ligne. Pour ajouter des exceptions d'URL, vous devez d'abord définir une EDL (external dynamic list) ou une catégorie d'URL personnalisée. Cliquez sur **Add (Ajouter)** pour afficher et sélectionner les options disponibles.

Objets > Profils de sécurité > Blocage des fichiers

Vous pouvez joindre un profil de blocage des fichiers à une règle de politique de sécurité (Politiques > Sécurité) pour empêcher les utilisateurs de charger ou de télécharger des types de fichiers donnés ou de générer une alerte lorsqu'un utilisateur tente de charger ou de télécharger des types de fichiers donnés.

*Pour accroître la sécurité, appliquez le profil **strict** prédéfini. Si vous devez prendre en charge des applications critiques qui utilisent un type de fichier que le profil **strict** bloque, clonez le profil **strict** et n'apportez que les exceptions de type de fichier dont vous avez besoin. Appliquez le profil cloné à une règle de politique de sécurité qui restreint l'exception uniquement aux sources, aux destinations et aux utilisateurs qui doivent utiliser le type de fichier. Vous pouvez également utiliser la **Direction** pour restreindre l'exception au chargement ou au téléchargement.*

*Si vous ne bloquez pas l'ensemble des fichiers PE Windows, envoyez tous les fichiers inconnus à WildFire pour qu'ils soient analysés. Pour les comptes d'utilisateur, définissez l'action sur **continue (continuer)** pour empêcher les téléchargements drive-by dans le cadre desquels des sites Web, des courriels ou des fenêtres contextuelles malveillants amènent les utilisateurs à télécharger des fichiers malveillants par inadvertance. Informez les utilisateurs qu'une invite à continuer le transfert d'un fichier qui a été lancé à leur insu pourrait indiquer qu'ils sont en train d'effectuer un téléchargement malveillant.*

Les tableaux suivants décrivent les paramètres des profils de blocage des fichiers.

Paramètres des profils de blocage des fichiers	Description
Name (Nom)	Saisissez un nom pour le profil (31 caractères maximum). Ce nom apparaît dans la liste de profils de blocage des fichiers pour la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Description	Saisissez une description du profil (255 caractères maximum).
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que le profil soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.

Paramètres des profils de blocage des fichiers	Description
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce profil de blocage des fichiers dans les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres de tous les groupes de périphériques qui héritent du profil.
Règles	Définissez une ou plusieurs règles pour préciser l'action à prendre (le cas échéant) pour les types de fichier sélectionnés. Pour ajouter une règle, renseignez les informations suivantes et cliquez sur **Add (Ajouter)** : • **Name (Nom)** - Saisissez un nom pour la règle (31 caractères maximum). • **Applications** - Sélectionnez les applications auxquelles la règle s'applique ou sélectionnez **any (indifférent)**. • **File Types (Types de fichier)** - Cliquez dans le champ Types de fichier, puis cliquez sur **Add (Ajouter)** pour afficher une liste des types de fichier pris en charge. Cliquez sur un type de fichier pour l'ajouter au profil ; continuez à ajouter d'autres types de fichier, au besoin. Si vous sélectionnez **any (indifférent)**, l'action définie est prise à l'égard de tous les types de fichier pris en charge. • **Direction** - Sélectionnez la direction du transfert de fichiers (**Upload (Charger)**, **Download (Télécharger)** ou **Both (Les deux)**). • **Action** - Sélectionnez l'action à prendre lorsque les types de fichier sélectionnés sont détectés : • **alert (alerte)** - Une entrée est ajoutée dans le journal des menaces. • **continue (continuer)** - Un message indique à l'utilisateur qu'un téléchargement a été demandé et exige sa confirmation. L'objectif est de prévenir l'utilisateur d'un possible téléchargement effectué à son insu (téléchargement 'AB; drive-by 'BB;) et de lui donner l'opportunité de poursuivre ou d'arrêter le téléchargement. Lorsque vous créez un profil de blocage des fichiers à l'aide de l'action **continue (continuer)**, vous pouvez uniquement choisir l'application **web-browsing (navigation-web)**. Si vous choisissez une autre application, le trafic correspondant à la règle de politique de sécurité ne traverse pas le pare-feu car aucune page vous invitant à continuer ne s’affiche. • **block (bloquer)** - Le fichier est bloqué.

Objets > Profils de sécurité > Analyse WildFire

Utilisez un profil d'analyse WildFire pour indiquer le fichier WildFire à analyser localement sur l'équipement WildFire ou dans le Cloud WildFire. Vous pouvez indiquer le trafic à transférer vers le Cloud public ou privé en fonction du type de fichier, de l'application ou du sens de transmission du fichier (chargement ou téléchargement). Après avoir créé un profil d'analyse WildFire, l'ajout de ce profil à une politique (**Policies (Politiques)** > **Security (Sécurité)**) vous permettra d'appliquer les paramètres du profil à n'importe quel trafic correspondant à cette politique (par exemple, une catégorie d'URL définie dans la politique).

Utilisez le profil par défaut prédéfini pour transférer tous les fichiers inconnus à WildFire à des fins d'analyse. De plus, définissez les mises à jour de contenu des appareils WildFire pour qu'elles soient téléchargées et installées toutes les minutes. Vous disposerez ainsi du soutien le plus récent.

Paramètres du profil d'analyse WildFire	
Name (Nom)	Donnez un nom descriptif au profil d'analyse WildFire (31 caractères maximum). Ce nom apparaîtra dans la liste des profils d'analyse WildFire disponibles au moment de la définition d'une règle de politique de sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Description	Décrivez éventuellement les règles du profil ou l'utilisation prévue du profil (255 caractères maximum).
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que le profil soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce profil de Protection contre la vulnérabilité dans les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres de tous les groupes de périphériques qui héritent du profil.
Règles	Définissez une ou plusieurs règles pour indiquer le trafic à transférer vers le Cloud public WildFire ou vers l'équipement WildFire (Cloud privé) pour analyse.

Paramètres du profil d’analyse WildFire	
	• Donnez un **Name (Nom)** descriptif aux règles que vous ajoutez au profil (31 caractères maximum). • Ajoutez une **Application** afin que le trafic de l'application corresponde à la règle et qu'il soit transféré vers la destination d'analyse définie. • Sélectionnez un **File Type (Type de fichier)** à analyser dans la destination d'analyse définie de la règle.  *Un cloud privé Wildfire (hébergé par un appareil WildFire) ne prend pas en charge l’analyse des fichiers APK, Mac OS X, d’archivage ou linux.* • Appliquez la règle au trafic en fonction du **Direction (Sens)** du transfert. Vous pouvez appliquer la règle pour charger du trafic et/ou télécharger du trafic. • Sélectionnez la destination du trafic à transférer pour **Analyse** :  *Par mesure de précaution, lorsqu'un cloud hybride est déployé, les fichiers qui correspondent aux règles établies pour le cloud privé ainsi qu'à celles établies pour le cloud public sont transférés uniquement vers le cloud privé.* • Sélectionnez Cloud public afin que l'ensemble du trafic correspondant à la règle soit transféré vers le Cloud public WildFire pour analyse. • Sélectionnez Cloud privé afin que l'ensemble du trafic correspondant à la règle soit transféré vers l'équipement WildFire pour analyse.

Objets > Profils de sécurité > Filtrage des données

Le filtrage de données permet au pare-feu de détecter des informations sensibles, telles que les numéros de carte de crédit ou de sécurité sociale ou les documents internes de l'entreprise, et d'empêcher ces données de quitter un réseau sécurisé. Avant d'activer le filtrage des données, sélectionnez Objets > Objets personnalisés > Modèles de données pour définir le type de données que vous souhaitez filtrer (comme les numéros de sécurité sociale ou les titres des documents contenant le mot « confidentiel »). Vous pouvez ajouter plusieurs objets de modèle de données à un seul profil de filtrage des données et, lorsqu'il est joint à une règle de politique de sécurité, le pare-feu analyse le trafic autorisé pour chaque motif de données et bloque le trafic correspondant en fonction des paramètres du profil de filtrage de données.

Paramètres des profils de filtrage des données	Description
Name (Nom)	Saisissez un nom pour le profil (31 caractères maximum). Ce nom apparaît dans la liste de profils de transfert des journaux pour la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Description	Saisissez une description du profil (255 caractères maximum).
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que le profil soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce profil de filtrage des données dans les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres de tous les groupes de périphériques qui héritent du profil.
Capture de données	Sélectionnez cette option pour collecter automatiquement les données bloquées par le filtre. *Indiquez un mot de passe pour l'option Gérer la protection des données à la page Paramètres pour afficher vos données capturées. Reportez-vous à la section* Périphérique > Configuration > Gestion.

Paramètres des profils de filtrage des données	Description
Modèle de données	Ajoutez un modèle de données existant qui sera utilisé pour filtrer ou sélectionnez **Nouveau** pour configurer un nouvel objet de modèle de données (Objets > Objets personnalisés > Modèles de données).
Applications	Désignez les applications à inclure dans la règle de filtrage'A0;: • Choisissez **any (indifférent)** pour appliquer le filtre à toutes les applications répertoriées. Cette sélection ne bloque pas toutes les applications possibles, mais seulement celles qui sont répertoriées. • Cliquez sur **Add (Ajouter)** pour désigner des applications individuelles.
Types de fichier	Indiquez les types de fichier à inclure dans la règle de filtrage : • Choisissez **any (indifférent)** pour appliquer le filtre à tous les types de fichier répertoriés. Cette sélection ne bloque pas tous les types de fichier possibles mais seulement ceux qui sont répertoriés. • Cliquez sur **Add (Ajouter)** pour désigner des types de fichier individuels.
Direction	Précisez si le filtre doit être appliqué dans la direction du chargement, du téléchargement ou dans les deux directions.
Seuil d'alerte	Précisez combien de fois le modèle de données doit être détecté dans un fichier pour déclencher une alerte.
Seuil de blocage	Bloquez les fichiers qui contiennent de nombreux exemples du modèle de données.
Gravité des journaux	Définissez la gravité du journal enregistrée pour les événements qui correspondent à cette règle de profil du filtrage des données.

Objets > Profils de sécurité > Protection DoS

Les profils de protection DoS permettent le ciblage de haute précision et l'amélioration des profils de protection de zone. Un profil de protection DoS indique les taux de seuil auxquels les nouvelles connexions par seconde (cps) déclenchent une alarme et une mesure (indiquée dans la politique de protection DoS). Le profil de protection DoS indique également le taux maximal de connexions par seconde et la durée pendant laquelle une adresse IP bloquée reste sur la liste des adresses IP bloquées. Vous spécifiez un profil de protection DoS dans une règle de politique de protection DoS, dans laquelle vous spécifiez les critères selon lesquels les paquets correspondent à la règle, et la règle de politique détermine les périphériques auxquels le profil s'applique.

Créez les profils et politiques de protection DoS visant à protéger les périphériques individuels critiques ou les petits groupes de périphériques, particulièrement les périphériques Internet, comme les serveurs Web et les serveurs de bases de données.

Vous pouvez configurer des profils de protection DoS agrégés et classés. Vous pouvez appliquer un profil agrégé, un profil classé ou un profil de chaque type à une règle de politique de protection DoS. Si vous appliquez les deux types de profil à une règle, le pare-feu applique d'abord le profil agrégé, puis applique le profil classé, au besoin.

- Dans un profil de protection DoS classé, **Classified (Classé)** est sélectionné en tant que **Type**. Lorsque vous appliquez un profil de protection DoS classé à une règle de protection DoS dont l'action est définie sur **Protect (Protéger)**, le pare-feu compte les connexions vers les seuils cps du profil si le paquet répond au type d'adresse spécifié : source-ip-only, destination-ip-only ou src-dest-ip-both.
- L'option **Aggregate (Agrégé)** d'un profil de protection DoS est sélectionnée en tant que **Type**. Lorsque vous appliquez un profil de protection DoS agrégé à une règle de protection DoS dont l'action est définie sur **Protect (Protéger)**, le pare-feu compte toutes les connexions (le nombre combiné de connexions pour le groupe de périphériques spécifiés dans la règle) qui répondent aux critères de la règle vers les seuils CPS du profil.

Pour appliquer un profil de protection DoS à une politique de protection DoS, voir Politiques > Protection DoS.

Si vous disposez d'un environnement de systèmes virtuels multiples (multi-vsys) et que vous avez configuré les paramètres suivants :

- *les zones externes pour permettre la communication entre les systèmes virtuels et*
- *les passerelles partagées pour permettre aux systèmes virtuels de partager une interface commune et une adresse IP unique pour les communications externes, alors*

Les mécanismes de protection DoS et de zone suivants sont désactivés dans la zone externe :

- *Cookies SYN*
- *Fragmentation IP*
- *ICMPv6*

Pour activer la fragmentation IP et la protection ICMPv6, vous devez créer un profil de protection de zone distinct pour la passerelle partagée.

Pour protéger la passerelle partagée contre la saturation SYN, vous pouvez appliquer un profil de protection contre la saturation SYN avec l'abandon anticipé aléatoire ou les cookies SYN. Sur une zone externe, seul Abandon anticipé aléatoire est disponible pour la protection contre la saturation SYN.

Paramètres d'un profil de protection DoS	
Name (Nom)	Saisissez un nom pour le profil (31 caractères maximum). Ce nom apparaît dans la liste de profils de transfert des journaux pour la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Description	Saisissez une description du profil (255 caractères maximum).
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que le profil soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.

Paramètres d’un profil de protection DoS	
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce profil de protection DoS dans les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres de tous les groupes de périphériques qui héritent du profil.
Type	Sélectionnez l’un des types de profil suivants : • **Aggregate (Agrégé)** - Appliquez les seuils DoS configurés dans le profil à l’ensemble des connexions qui correspondent aux critères de la règle à laquelle ce profil est appliqué. Par exemple, une règle agrégée disposant d’un **Alarm Rate (taux d’alarme)** de saturation SYN de 10 000 CPS compte les connexions combinées de tous les périphériques correspondant à la règle DoS. Lorsque le CPS du groupe est supérieur à 10 000 CPS, l'alarme est alors déclenchée, peu importe la répartition des CPS parmi les périphériques. • **Classified (Classé)** - Appliquez les seuils DoS configurés dans le profil à chaque connexion individuelle qui correspond aux critères de classification (adresse IP source, adresse IP de destination ou paire d’adresses IP source et de destination). Par exemple, une règle classée comportant un **Alarm Rate (Taux d’alarme)** de saturation SYN de 10 000 CPS permet un maximum de 10 000 CPS par périphérique et déclenche une alarme lorsqu’un périphérique individuel spécifié dans la règle DoS dépasse 10 000 CPS.
Onglet Protection contre la saturation	
Onglet Saturation SYN Onglet Saturation UDP Onglet Saturation ICMP Onglet Saturation ICMPv6 Onglet Saturation Autre IP	Sélectionnez cette option pour activer le type de protection contre la saturation indiqué sur l’onglet et précisez les paramètres suivants : • **Action** – (**Saturation SYN** uniquement) Action que le pare-feu effectue si l’action de la politique de protection DoS est **Protégée** et si les CPS atteignent le **Activate Rate (Taux d’activation)**. Choisissez l’une des options suivantes : • **Abandon anticipé aléatoire** – Abandonne des paquets de façon aléatoire lorsque les connexions par seconde atteignent le seuil du **Taux d’activation**.

Paramètres d’un profil de protection DoS	
	• **Cookies SYN** - Utilisation de cookies SYN pour indiquer qu’il n’est pas nécessaire d’abandonner des connexions face à une attaque par saturation SYN. *Commencez par les cookies SYN, qui traitent le trafic légitime équitablement, mais consomment plus de ressources du pare-feu. Surveillez le processus et l’utilisation de la mémoire, et si les cookies SYN consomment un trop grand nombre de ressources, passez à RED. Utilisez toujours RED si vous ne disposez pas d’un périphérique de prévention DDoS dédié devant le réseau (Internet) pour vous protéger d’attaques DoS de grand volume.* • **Alarm Rate (Taux d’alarme)** - Indiquez le taux de seuil (cps) pour générer une alarme DoS (plage de 0 à 2 000 000 cps ; valeur par défaut de 10 000 cps). Pour les profils classés, la meilleure pratique consiste à fixer le seuil de 15 à 20 % au-dessus du taux de CPS moyen du périphérique afin de composer avec les fluctuations normales et à ajuster le seuil si vous recevez un trop grand nombre d’alarmes. Pour les profils agrégés, la meilleure pratique consiste à fixer le seuil de 15 à 20 % au-dessus du taux de CPS moyen. Surveillez et ajustez les seuils selon vos besoins. • **Taux d’activation** - Indiquez le taux de seuil (cps) auquel une réponse DoS est activée. La réponse DoS est configurée dans le champ **Action** du profil de protection DoS (abandon anticipé aléatoire ou cookies SYN). La plage du **Taux d’activation** est comprise entre 0 et 2 000 000 cps. La valeur par défaut est 10 000 cps. Si le profil **Action** est défini sur **Abandon anticipé aléatoire** (RED), lorsque les connexions entrantes par seconde atteignent le seuil du **Taux d’activation**, RED se produit. Si le taux de cps augmente, le taux RED augmente en fonction d’un algorithme. Le pare-feu continue avec RED jusqu’à ce que le taux de cps atteigne le seuil du **Max Rate (Taux max)**. Les profils classés appliquent des limites CPS exactes à des périphériques individuels et vous fondez ces limites sur la capacité des périphériques protégés. Ainsi, vous n’avez donc pas à limiter le CPS graduellement et vous pouvez définir le **Activate Rate (Taux d'activation)** au même seuil que le **Max Rate (Taux max.)**. Définissez le **Activate Rate (Taux d'activation)** sur une valeur plus faible que celle du **Max Rate (Taux max.)** uniquement si vous souhaitez commencer à abandonner le trafic en direction d’un serveur individuel avant qu’il n’atteigne le **Max Rate (Taux max.)**. Pour les profils agrégés, fixez le seuil juste au-dessus du taux de CPS du groupe. Surveillez et ajustez les seuils selon vos besoins.

Paramètres d’un profil de protection DoS	
	• **Taux max.** - Indiquez le taux de seuil des connexions entrantes par seconde autorisées par le pare-feu. Lorsque le seuil du **Taux max** est atteint, le pare-feu abandonne l’ensemble des nouvelles connexions (la plage est comprise entre 2 et 2 000 000 cps ; la valeur par défaut est 40 000 cps). Pour les profils classés, fondez le **Max Rate (Taux max)** sur la capacité des périphériques que vous protégez afin d’éviter leur saturation. Pour les profils agrégés, fixez le **Max Rate (Taux max.)** sur une valeur allant de 80 à 90 % de la capacité du groupe. Surveillez et ajustez les seuils selon vos besoins. • **Durée du blocage** – Indiquez la durée (secondes) pendant laquelle l’adresse IP offensante reste sur la liste des adresses IP bloquées et pendant laquelle les connexions avec l’adresse IP sont bloquées. Le pare-feu ne compte pas les paquets qui arrivent pendant la durée du blocage à l’égard des seuils du Taux d’alarme, du Taux d’activation ou du Taux max (la plage est comprise entre 1 et 21 600 secondes ; la valeur par défaut est 300 secondes).
Onglet Protection des ressources	
Sessions	Sélectionnez cette option pour activer la protection des ressources.
Nombre maximum de sessions simultanées	Indiquez le nombre maximum de sessions simultanées. • Pour le type de profil **agrégé**, cette limite s’applique à l’ensemble du trafic correspondant à la règle de protection DoS à laquelle le profil de protection DoS est appliqué. • Pour le type de profil **classé**, cette limite s’applique au trafic classé (IP source, IP de destination ou les deux) correspondant à la règle de protection DoS à laquelle le profil de protection DoS est appliqué.

Objets > Profils de sécurité > Protection du réseau mobile

Le profil de Protection de réseau mobile permet au pare-feu d'inspecter GTP et HTTP/2 dans le trafic 5G Service Based Architecture (SBA). Pour afficher ce profil, vous devez activer la sécurité GTP dans Périphérique > Configuration > Gestion.

Utilisez les options de ce profil pour activer l'inspection d'état de GTP 5G HTTP/2, GTP v1-C, GTP v2-C et GTP-U, pour activer la validation du protocole pour GTPv1-C, GTPv2-C et GTP-U, pour activer l'inspection du contenu de GTP-U pour analyser les données utilisateur dans les tunnels GTP-U. Il vous permet aussi de filtrer les sessions GTP sur la base de l'APN, du préfix IMSI/IMSI, et du RAT et d'éviter l'usurpation de l'adresse IP de l'utilisateur final.

Paramètres d'un profil d'inspection GTP	
Inspection GTP	
GTP-C	• Sélectionnez **Inspection d'état** pour permettre au pare-feu d'inspecter **GTPv1-C**, **GTPv2-C** ou les deux. Lorsque vous activez l'inspection d'état, le pare-feu utilise l'adresse IP source, le port source, l'adresse IP de destination, le port de destination, le protocole et les identifiants du point d'extrémité du tunnel (TEID) pour assurer le suivi d'une session GTP. Il vérifie et valide également l'ordre des différents types de messages GTP qui sont utilisés pour établir un tunnel GTP. Le TEID identifie de manière unique les points d'extrémité du tunnel GSN. Les tunnels pour une liaison montante et une liaison descendante sont séparés et utilisent un TEID différent. • Sélectionnez l'**Action Blocage** ou **Alerte** prise par le pare-feu pour répondre à une absence de vérification de la validité. L'action d'alerte permet le trafic, mais génère un journal tandis que l'action de blocage rejette le trafic et génère un journal. • Indiquez les contrôles de validité que le pare-feu doit effectuer sur un en-tête GTP et sur les éléments d'informations (IE) d'une charge utile. Le pare-feu utilise l'action de blocage ou d'alerte que vous sélectionnez ci-dessous pour gérer l'erreur. Vous pouvez configurer le pare-feu pour valider : • **IE réservé**— Vérifie les messages GTPv1-C ou GTPv2-C qui utilisent des valeurs IE réservées. • **Order IE (Éléments d'informations de commande)** (GTPv1-C only (GTPV1-C uniquement)) – Vérifie que l'ordre des IE dans les messages GTPv1-C est exact. • **Longueur des éléments d'informations** – Vérifie les messages GTPv1-C ou GTPv2-C ayant une longueur d'IE invalide. • **Champ réservé dans l'en-tête** – Vérifie les paquets mal formés qui utilisent des valeurs invalides ou des valeurs réservées dans un en-tête.

Paramètres d’un profil d’inspection GTP	
	• **Type de message non pris en charge** – Vérifie les types de messages inconnus ou incorrects.
GTP-U	L’activation de l’inspection par état pour GTPv1-C et/ou GTPv2-C active automatiquement l’inspection par état GTP-U. Vous pouvez spécifier les contrôles de validité suivants pour les charges utiles GTP-U. • **Éléments d’informations réservés** – Vérifie les messages GTP-U qui utilisent des valeurs d’IE réservés. • **Éléments d’informations hors ligne** – Vérifie que l’ordre des IE dans les messages GTP-U est correct. • **Longueur des éléments d’informations** – Vérifie les messages ayant une longueur d’IE incorrecte. • **Drapeau supplémentaire dans l’en-tête** – Vérifie les paquets mal formés qui utilisent des valeurs invalides ou des valeurs réservées dans un en-tête. • **Type de message non pris en charge** – Vérifie les types de messages inconnus ou incorrects. De plus, vous pouvez également configurer une action d’autorisation, de blocage ou d’alerte pour : • **Usurpation de l’adresse IP de l’utilisateur final** – Configurez le pare-feu pour bloquer ou émettre une alerte lorsque l’adresse IP source dans un paquet GTP-U de l’équipement utilisateur de l’abonné n’est pas identique à l’adresse IP dans le message GTP-C correspondant échangé pendant la configuration du tunnel. *Si vous activez l'inspection avec état PFCP, cette option n'est pas disponible.* • **GTP dans GTP –** Vous pouvez configurer le pare-feu pour bloquer ou émettre une alerte lorsqu’il détecte un message GTP dans GTP. Lors de la détection, le pare-feu génère un journal GTP avec un niveau de gravité critique. • **Log at GTP-U session start (Journal au début de la session GTP-U)**— Enregistrez l'adresse IP associée et l'ID de point de terminaison du tunnel dans les journaux GTP au début d'une session GTP-U. • **Log at GTP-U session end (Journal à la fin de la session GTP-U)**— Enregistrez l'adresse IP associée et l'ID de point de terminaison du tunnel dans les journaux GTP à la fin d'une session GTP-U. • Pour la 4G et la 3G, activez **GTP-U Content Inspection (Inspection du contenu GTP-U)** pour inspecter et appliquer la politique à la charge utile des données utilisateur dans un paquet GTP-U. L’inspection du contenu GTP-U vous permet de mettre en corrélation les informations

Paramètres d’un profil d’inspection GTP	
	IMSI et les informations IMEI issues des messages GTP-C avec le trafic IP encapsulé dans les paquets GTP-U.
5G-C	Pour la 5G, activez **5G-HTTP2** afin de permettre l’inspection des paquets de contrôle 5G HTTP/2 qui peuvent contenir les ID de l’abonné, les ID de l’équipement et des informations de tranche de réseau. Cela vous permet de corréler l’ID de l’abonné (IMSI), l’ID de l’équipement (IMEI) et les information de l’ID de la tranche de réseau héritées des messages HTTP/2 avec le trafic IP encapsulé dans les paquets GTP-U. L’activation de **5G-HTTP2** désactive GTP-C pour le profil.
PFCP	Pour Packet Forwarding Control Protocol (PFCP), activez **Stateful Inspection (inspection de l’état)** pour inspecter le trafic PFCP. Lorsque vous activez l'inspection avec état pour le trafic PFCP, le pare-feu inspecte le trafic entre le MEC et le site distant ou central pour aider à prévenir les attaques telles que le déni de service (DOS) ou l'usurpation d'identité. *Si vous activez cette option, les actions pour l'usurpation d'adresse IP de l'utilisateur final GTP-U ne sont pas disponibles.* Vous pouvez spécifier les contrôles d'état suivants : • **Check Association Messages (Vérifier les messages d'association)** : vérifie les messages d'association PFCP qui sont en panne ou qui ont été rejetés. • **Check Session Messages (Vérifier les messages de session)** : vérifie les messages de session PFCP qui ne sont pas en ordre ou qui ont été rejetés. • **Check Sequence Number (Vérifier le numéro de séquence** : confirme que le numéro de séquence dans le PFCP correspond au numéro de séquence dans le message de demande PFCP. Vous pouvez ensuite spécifier l'**Action** (**Allow (Autoriser)**, **Alert (Alerter)** ou **Block (Bloquer)**) que le pare-feu doit exécuter lorsque la vérification échoue. Vous pouvez également choisir si vous souhaitez que le pare-feu crée un journal au début ou à la fin des associations ou sessions PFCP.
Corrélation	
Corrélation UEIP	Permet la corrélation entre l'identifiant de l'abonné et l'identifiant de l'équipement avec le trafic IP de l'équipement utilisateur (UE) pour l'inspection du contenu GTP-U.

Paramètres d’un profil d’inspection GTP	
Mode	• **Loose (libre)**— (Par défaut) Lorsque le pare-feu détecte le trafic interne GTP-U, il interroge l'adresse source ou de destination pour trouver les informations IMEI ou IMSI corrélées. S'il n'y a aucun résultat, le pare-feu transfère le trafic. • **Strict**— Supprime le trafic si la requête GTP-U ne renvoie aucun résultat.
Source	Sélectionnez la source que vous souhaitez utiliser pour corréler les informations.  *Pour les déploiements utilisant CUPS, sélectionnez PFCP.*
Se connecter au démarrage de l'UEIP	Consigner les événements de corrélation UEIP lorsque le pare-feu alloue une adresse IP à l'UE.
Se connecter à la fin de l'UEIP	Consigner les événements de corrélation UEIP lorsque le pare-feu libère l'adresse IP allouée.
Options de filtrage	
Filtrage RAT	Toutes les technologies d’accès radioélectrique (RAT) sont autorisées par défaut. Les messages GTP-C de demande de création de PDF et de demande de création de sessions sont filtrés ou autorisés en fonction du filtre RAT. Vous pouvez indiquer s’il faut autoriser, bloquer ou alerter les RAT suivantes que l’équipement utilisateur utilise pour accéder au réseau mobile principal : • **UTRAN** • **GERAN** • **RÉSEAU LOCAL SANS FIL** • **GAN** • **Évolution HSPA** • **EUTRAN** • **Virtuel** • **EUTRAN-NB-IoT** • **LTE-M** • **NR** Les RAT sont disponibles lorsque vous activez **5G-HTTP2**: • **RÉSEAU LOCAL SANS FIL** • **EUTRAN**

Paramètres d’un profil d’inspection GTP	
	• **Virtuel** • **NR**
Filtrage IMSI	L’IMSI (International Mobile Subscriber Identity) est une identification unique associée à un abonné aux réseaux GSM, UMTS et LTE qui est approvisionné par la carte du module d’identification de l’abonné (SIM). Une IMSI est généralement présentée comme un nombre de 15 chiffres (8 octets), mais elle peut être plus courte. L’IMSI se compose de trois parties : • Code mobile de pays (MCC) composé de trois chiffres. Le MCC identifie uniquement le pays de domicile de l’abonné mobile. • Code de réseau mobile (MNC) composé de deux ou trois chiffres ; 2 chiffres standard européens ou 3 chiffres standard nord-américains. Le MNC identifie le PLMN domestique de l’abonné mobile. • Numéro d’identification de l’abonné mobile (MSIN) identifiant l’abonné mobile dans un PLMN. Le **IMSI Prefix (Préfixe IMSI)** combine le MCC et le MNC et vous permet d’**allow (autoriser)**, de **block (bloquer)** ou d’**alert (émettre une alerte)** concernant le trafic GTP d’un PLMN spécifique. Par défaut, tous les IMSI sont autorisés. Vous pouvez saisir manuellement ou importer un fichier CSV avec un IMSI ou des préfixes IMSI dans le pare-feu. L’IMSI peut comprendre des caractères génériques, par exemple, 310* ou 240011*. Le pare-feu prend en charge, au maximum, 5 000 IMSI ou préfixes IMSI.
Filtrage APN	Le point d’accès du réseau (APN) est le point de référence entre le GGSN et le PGW dont un équipement utilisateur a besoin pour se connecter à Internet. En 5G, un format de Nom de réseau de données (DNN) est l’APN. L’APN se compose d’un ou deux identifiants : • L’identificateur réseau APN qui définit le réseau externe auquel le GGSN/PGW est connecté et éventuellement un service requis par la station mobile. Cette partie de l’APN est obligatoire. • L’identificateur de l’opérateur APN qui définit dans quelle ossature PLMN GPRS/EPS est situé le GGSN/PGW. Cette partie de l’APN est facultative. Tous les APN sont autorisés par défaut. Le filtre APN vous permet d’autoriser, de bloquer ou d’émettre une alerte sur le trafic GTP en fonction de la valeur APN. Les messages GTP-C de demande de création de PDF et de demande de création de sessions sont filtrés ou autorisés en fonction des règles définies pour le filtre APN. Vous pouvez ajouter manuellement ou importer une liste de filtres APN dans le pare-feu. La valeur pour l’APN doit inclure l’ID du réseau ou le

Paramètres d’un profil d’inspection GTP	
	nom de domaine du réseau (par exemple, exemple.com) et, le cas échéant, l’ID de l’opérateur. Pour le filtrage APN, le caractère générique * vous permet de chercher tous les APN. Une combinaison de * et d’autres caractères n’est pas prise en charge pour les caractères génériques. Par exemple, « internet.mnc* » est traité comme un APN ordinaire et ne filtrera pas toutes les entrées qui commencent par internet.mnc. Le pare-feu prend en charge, au maximum, 1 000 filtres APN.
Limite de tunnels GTP	
Nombre max. de tunnels simultanés autorisés par destination	Vous permet de limiter le nombre maximal de tunnels GTP-U à une adresse IP de destination, par exemple pour le GGSN (plage de 0 à 100 000 000 tunnels)
Alerte lorsque le nombre max. de tunnels simultanés par destination est atteint	Spécifiez le seuil auquel le pare-feu déclenche une alerte lorsque le nombre de tunnels GTP-U maximum à destination a été établi. Un message de journal GTP de gravité critique est généré lorsque la limite configurée pour le tunnel est atteinte.
Fréquence de journalisation	Le nombre d’événements comptés par le pare-feu avant que ce dernier génère un journal lorsque les limites configurées pour le tunnel GTP sont dépassées. Ce paramètre vous permet de réduire le volume aux messages enregistrés (plage de 0 à 100 000 000 ; la valeur par défaut est de 100).
Protection contre la surfacturation	Sélectionnez le système virtuel qui sert de pare-feu Gi/SGi sur votre pare-feu. Le pare-feu Gi/SGi inspecte le trafic IP de l’abonné mobile qui parcourt l’interface Gi/SGi depuis le PGW/GGSN vers le PDN externe (réseau de données par paquets), comme Internet, et sécurise l’accès à Internet pour les abonnés mobiles. La surfacturation peut survenir lorsqu’un GGSN attribue une adresse IP précédemment utilisée depuis le pool d’adresses IP de l’utilisateur final à un abonné mobile. Lorsqu’un serveur malveillant sur Internet continue à envoyer des paquets à cette adresse IP, car il n’a pas fermé la session initiée pour l’abonné précédent et que la session est encore ouverte sur le pare-feu Gi. Pour interdire la livraison des données, chaque fois qu’un tunnel GTP est supprimé (détecté par le message de suppression du PDP ou le message de suppression de la session) ou expiré, le pare-feu activé pour la protection contre la surfacturation informe le pare-feu Gi/SGi qu’il doit supprimer toutes les sessions qui appartiennent à l’abonné de la table de session. La sécurité GTP et le pare-feu SGi/Gi doivent être configurés sur le même pare-feu physique, mais ils peuvent être dans des systèmes virtuels différents. Afin de supprimer des sessions en fonction des événements GTP-C, le pare-feu doit disposer de toutes les informations de session pertinentes, ce qui n’est possible que lorsque vous gérez le trafic à

Paramètres d’un profil d’inspection GTP	
	partir des interfaces SGi, S11 ou S5 pour GTPv2 et les interfaces Gi et Gn pour GTPv1 dans le réseau mobile principal.

Autres paramètres des journaux

Par défaut, le pare-feu ne consigne pas les messages GTP ou PFCP autorisés. Vous pouvez activer de manière sélective la journalisation des messages GTP et PFCP autorisés lorsque cela est nécessaire à des fins de dépannage puisque cela générera un important volume de journaux. En plus des messages des journaux autorisés, cet onglet vous permet également d’activer de manière sélective l’enregistrement des informations de localisation des utilisateurs.

Messages GTPv1-C autorisés	Cet onglet vous permet d’activer de manière sélective la journalisation des messages GTPv1-C autorisés, si vous avez activé l’inspection d’état pour GTPv1?C. Ces messages génèrent des journaux pour vous aider à résoudre les problèmes au besoin. Par défaut, le pare-feu ne consigne pas les messages autorisés. Les options de journalisation pour les messages GTPv1-C autorisés sont les suivantes : • **Tunnel Management (Gestion du tunnel)** – Ces messages GTPv1-C sont utilisés pour gérer les tunnels GTP-U qui acheminent des paquets IP encapsulés et des messages de signalisation entre une paire donnée de nœuds de réseau tels que SGSN et GGSN. Il comprend des messages, tels que Créer une demande contextuelle PDP, Créer une réponse contextuelle PDP, Mettre à jour la demande contextuelle PDP, Mettre à jour la réponse contextuelle PDP, Supprimer la demande contextuelle PDP, Supprimer la réponse contextuelle PDP. • **Path Management (Gestion des chemins)** – Ces messages GTPv1-C sont généralement envoyés par le GSN ou le Contrôleur de réseau radio (RNC) à un autre GSN ou RNC pour savoir si la paire est active. Il comporte des messages tels que Demande et Réponse d’écho. • **Others (Autres)** – Ces messages incluent la gestion des emplacements, la gestion de la mobilité, la gestion des informations RAN et les messages du service de diffusion / multidiffusion de multimédia (MBMS).
Emplacement de l'utilisateur du journal	Vous permet d’inclure les informations de localisation de l’utilisateur, comme le code de zone et l’ID de cellule, dans les journaux GTP.
Capture de paquets	Vous permet de capturer des événements GTP.
Messages GTPv2-C autorisés	Cet onglet vous permet d’activer de manière sélective la journalisation des messages GTPv2-C autorisés, si vous avez activé l’inspection d’état pour GTPv2-C. Ces messages génèrent des journaux pour vous aider à résoudre les problèmes au besoin. Par défaut, le pare-feu ne consigne pas les messages autorisés. Les options de journalisation pour les messages GTPv2-C autorisés sont les suivantes :

Paramètres d’un profil d’inspection GTP	
	• **Tunnel Management (Gestion du tunnel)** – Ces messages GTPv2-C sont utilisés pour gérer les tunnels GTP-U qui acheminent des paquets IP encapsulés et des messages de signalisation entre une paire donnée de nœuds de réseau tels que SGW et PGW. Il comprend les types de messages suivants : Créer une demande de session, Créer une réponse de session, Créer une demande de porteur, Créer une réponse de porteur, Modifier la demande de porteur, Modifier la réponse du porteur, Supprimer une demande de session et Supprimer la réponse de session. • **Path Management (Gestion des chemins)** – Ces messages GTPv2-C sont généralement envoyés par un nœud de réseau comme SGW ou PGW à un autre PGW ou SGW pour savoir si l’homologue est actif. Il comporte des messages tels que Demande et Réponse d’écho. • **Others (Autres)** – Ces messages incluent les messages de gestion de la mobilité et les messages liés à l’accès non-3GPP.
Messages GTP-U autorisés	Cet onglet vous permet d’activer de manière sélective la journalisation des messages GTP-U autorisés, si vous avez activé l’inspection d’état pour GTPv2-C ou GTPv1-C. Ces messages génèrent des journaux pour vous aider à résoudre les problèmes au besoin. Les options de journalisation pour les messages GTP-U autorisés sont les suivantes : • **Tunnel Management (Gestion du tunnel)** – Il s’agit de messages de signalisation GTP-U tels que l’Indication d’erreur. • **Path Management (Gestion des chemins)** – Ces messages GTP-U sont envoyés par un nœud de réseau (tel que eNodeB) à un autre nœud de réseau (comme SGW) pour voir si la paire est active. Il comporte des messages tels que Demande / Réponse d’écho. • **G-PDU** – Le G-PDU (GTP-U PDU) est utilisé pour transférer des paquets de données utilisateur au sein des nœuds de réseau dans le réseau de base mobile ; il se compose d’un en-tête GTP et d’un T-PDU.
Paquets G-PDU consignés par nouveau tunnel GTP-U	Activez cette option pour vérifier que le pare-feu inspecte les PDU GTP-U. Le pare-feu génère un journal pour le nombre spécifié de paquets G-PDU dans chaque nouveau tunnel GTP-U (plage de 1 à 10 ; la valeur pare-feu est de 1).
Messages 5G-C autorisés	Sélectionnez **N11** pour activer de façon sélective la journalisation des messages N11 autorisés. Les messages N11 vous aident lors du dépannage et vous offrent une meilleure visibilité sur les messages HTTP/2 échangés sur une interface N11 pour différentes procédures. Ce champ n’est disponible que si vous avez activé **5G-HTTP2** dans l’onglet **5G-C** dans le profil de Protection de réseau mobile.

Paramètres d’un profil d’inspection GTP	
Messages PFCP autorisés	Vous permet d’activer de manière sélective la journalisation des messages PFCP autorisés, si vous avez activé l’inspection d’état pour PFCP. Ces messages génèrent des journaux pour vous aider à résoudre les problèmes au besoin. Les options de journalisation pour les messages PFCP autorisés sont les suivantes : • **Session Establishment (Établissement de session)** : ces messages PFCP configurent la session, y compris l'établissement du tunnel GTP-U. • **Session Modification (Modification de session)** : ces messages PFCP sont envoyés si l'ID de session ou l'ID PDR change (par exemple, suite au passage d'un réseau 4G à un réseau 5G. Il comprend des messages tels que la demande de modification de session PFCP et la réponse de modification de session PFCP. • **Session Deletion (Suppression de session)** : ces messages PFCP mettent fin à la session PFCP, y compris la libération des ressources associées.

Objets > Profils de sécurité > Protection SCTP

Créez un profil de protection Stream Control Transmission Protocol (protocole de transmission de contrôle de flux ; SCTP) pour préciser comment le pare-feu doit valider et filtrer les blocs SCTP. Vous devez d'abord activer la Sécurité SCTP (**Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **General Settings (Paramètres généraux)**) pour voir ce type de profil sous Security Profiles (Profils de sécurité). Vous pouvez également restreindre le nombre d'adresses IP par point de terminaison SCTP dans un environnement à connexions multiples et vous pouvez préciser les situations dans lesquelles le pare-feu journalise les événements SCTP. Après avoir créé un profil de protection SCTP, vous devez appliquer le profil à une règle de politique de Sécurité d'une zone.

Les modèles de pare-feu qui prennent en charge la sécurité SCTP disposent d'un profil de protection SCTP prédéfini (*default-ss7*) que vous pouvez utiliser tel quel ou que vous pouvez cloner pour vous servir de base pour la création d'un nouveau profil de protection SCTP. Sélectionnez **Object (Objets)** > **Security Profiles (Profils de sécurité)** > **SCTP Protection (Protection SCTP)**, puis sélectionnez **default-ss7** pour voir les Codes d'opération qui déclenchent une alerte pour ce profil prédéfini.

Paramètres des profils de protection SCTP	
Name (Nom)	Donnez un nom au profil de protection SCTP.
Description	Saisissez une description pour le profil de protection SCTP.
Inspection SCTP	
Bloc inconnu	Sélectionnez l'action que prend le pare-feu lorsqu'il reçoit un paquet SCTP avec un bloc inconnu (le bloc n'est pas défini dans RFC3758, dans RFC4820, dans RFC4895, RFC4960, dans RFC5061 ni dans RFC 6525) : • **allow (autoriser)** (par défaut) : autorise le paquet à passer sans modification. • **alert (alerter)** : autorise le paquet à passer sans modification et génère un journal SCTP (vous devez allouer un espace au stockage de ces journaux ; consultez l'onglet Stockage des journaux sous les paramètres de journalisation et de génération de rapports : Périphérique > Configuration > Gestion). • **block (bloquer)** : invalide le bloc avant de faire passer le paquet et génère un journal SCTP.
Indicateurs de blocs	Sélectionnez l'action que prend le pare-feu lorsqu'il reçoit un paquet SCTP avec un indicateur de blocs qui ne correspond pas à RFC4960 : • **allow (autoriser)** (par défaut) : autorise le paquet à passer sans modification. • **alert (alerter)** : autorise le paquet à passer sans modification et génère un journal SCTP (vous devez allouer un espace au stockage de ces journaux ; consultez l'onglet Stockage des

Paramètres des profils de protection SCTP	
	journaux sous les paramètres de journalisation et de génération de rapports : Périphérique > Configuration > Gestion). • **block (bloquer)** : abandonne le paquet et génère un journal SCTP.
Longueur non valide	Sélectionnez l'action que prend le pare-feu lorsqu'il reçoit un bloc SCTP avec une longueur non valide : • **allow (autoriser)** (par défaut) : autorise le paquet ou le bloc à passer sans modification. • **block (bloquer)** : abandonne le paquet et génère un journal SCTP (vous devez allouer un espace au stockage de ces journaux ; consultez l'onglet Stockage des journaux.
Limite d'adresses IP pour le multi-hébergement	Saisissez le nombre maximal d'adresses IP que vous pouvez configurer pour un point de terminaison SCTP avant que le pare-feu ne génère un message d'alerte (plage est comprise entre 1 et 8 ; par défaut 4). Le multi-hébergement SCTP est la capacité d'un point de terminaison à prendre en charge plus d'une adresse IP pour une association avec un homologue. En cas d'échec d'un chemin vers un point de terminaison, SCTP sélectionne l'une des autres adresses IP de destination fournies pour cette association.
Paramètres des journaux	Sélectionnez n'importe quelle combinaison de paramètres pour générer les journaux SCTP, soit selon les blocs autorisés, le début et la fin d'une association et les événements d'échec d'un état : • **Journaliser au début de la session** • **Journaliser en fin de session** • **Journaliser les blocs d'initialisation d'association autorisés** • **Journaliser les blocs de pulsation autorisés** • **Journaliser les blocs de fin d'association autorisés** • **Journaliser tous les blocs de contrôle** • **Journaliser les événements d'échec d'un état** Pour que le pare-feu stocke les journaux SCTP, vous devez allouer de l'espace au stockage des journaux SCTP (reportez-vous à l'onglet Stockage des journaux sous les paramètres de journalisation et de génération de rapports : Périphérique > Configuration > Gestion).
Options de filtrage	
Filtrage SCTP	
Nom	Saisissez un nom à donner au filtre SCTP.

Paramètres des profils de protection SCTP	
PPID	Précisez un PPID pour le filtre SCTP : • **any (indifférent)** : amène le pare-feu à prendre l'Action que vous avez définie pour tous les blocs de données SCTP qui contiennent un PPID. • **3GPP PUA** • **3GPP RNA** • **LCS-AP** • **M2PA** • **M2UA** • **M3UA** • **NBAP** • **RUA** • **S1AP** • **SBc-AP** • **SUA** • **X2AP** • Entrez une valeur PPID valide (une valeur qui ne se trouve pas dans la liste déroulante). Par exemple, la valeur PPID de H.323 est 13. Chaque filtre SCTP ne peut définir qu'un seul PPID. Vous pouvez toutefois définir plusieurs filtres SCTP pour un profil de Protection SCTP.
Action (Action)	Définissez l'action que le pare-feu doit prendre à l'égard des blocs de données qui contiennent le PPID indiqué : • **allow (autoriser)** (par défaut) : autorise le bloc à passer sans modification. • **alert (alerter)** : autorise le bloc à passer sans modification et génère un journal SCTP (vous devez allouer un espace au stockage de ces journaux ; consultez l'onglet Stockage des journaux sous les paramètres de journalisation et de génération de rapports : Périphérique > Configuration > Gestion). • **block (bloquer)** : abandonne le bloc avant de laisser passer le paquet et génère un journal SCTP (vous devez allouer un espace au stockage de ces journaux ; consultez l'onglet Stockage des journaux sous les paramètres de journalisation et de génération de rapports : Périphérique > Configuration > Gestion).

Les paquets SCTP sont mis en correspondance avec les filtres de la liste, de haut en bas. Si vous créez plus d'un filtre SCTP pour un profil, l'ordre dans lequel les filtres SCTP apparaissent importe.

Paramètres des profils de protection SCTP	
Sélectionner un filtre, puis **Move Up (Déplacez vers le haut)** ou **Move Down (Déplacez vers le bas)** pour modifier sa priorité relative au sein de la liste de Filtrage SCTP.	
Filtrage Diameter	
Nom	Saisissez un nom à donner au filtre Diameter.
Action (Action)	Définissez l'action que prend le pare-feu à l'égard des blocs Diameter qui contiennent les ID d'application Diameter, les codes de commande et les AVP définis. Si les blocs faisant l'objet d'une inspection comprennent l'ID d'application Diameter défini *et* n'importe lequel des Codes de commande Diameter définis *et* n'importe laquelle des AVP Diameter définies, alors : • **allow (autoriser)** (par défaut) : autorise le bloc à passer sans modification. • **alert (alerter)** : autorise le bloc à passer sans modification et génère un journal SCTP (vous devez allouer un espace au stockage de ces journaux ; consultez l'onglet Stockage des journaux sous les paramètres de journalisation et de génération de rapports : Périphérique > Configuration > Gestion). • **block (bloquer)** : abandonne le bloc avant de laisser passer le paquet et génère un journal SCTP (vous devez allouer un espace au stockage de ces journaux ; consultez l'onglet Stockage des journaux sous les paramètres de journalisation et de génération de rapports : Périphérique > Configuration > Gestion).
ID d'application Diameter	Définissez l'ID d'application Diameter d'un bloc à l'égard duquel le pare-feu prend l'action définie. • **Indifférent** • **3GPP-Rx** • **3GPP-S6a/S6d** • **3GPP-S6c** • **3GPP-S9** • **3GPP-S13/S13** • **3GPP-Sh** • **Diameter Base Accounting** • **Diameter Common Messages** • **Diameter Credit Control** Vous pouvez également entrer une valeur numérique pour un ID d'application Diameter (la plage est comprise entre 0 et 4 294 967 295). Un filtre Diameter ne peut posséder qu'un seul ID d'application.

Paramètres des profils de protection SCTP	
Code de commande Diameter	Définissez les Codes de commande Diameter d'un bloc à l'égard duquel le pare-feu prend l'action définie. Sélectionnez **any (indifférent)**, sélectionnez un Code de commande Diameter dans la liste déroulante et saisissez une valeur donnée (la plage est comprise entre 0 et 16 777 215). La liste déroulante n'inclut que les codes de commande qui s'appliquent à l'ID d'application Diameter sélectionné. Vous pouvez ajouter plusieurs Codes de commande Diameter dans un filtre Diameter.
AVP Diameter	Définissez la Attribute-Value Pair (paire attribut-valeur ; AVP) Diameter d'un bloc à l'égard duquel le pare-feu prend l'action définie. Saisissez un ou plusieurs codes ou valeurs AVP (la plage est comprise entre 1 et 16 777 215).
Si vous créez plus d'un filtre Diameter pour un profil, l'ordre dans lequel les filtres Diameter apparaissent importe. Sélectionner un filtre, puis **Move Up (Déplacez vers le haut)** ou **Move Down (Déplacez vers le bas)** pour régler sa priorité relative au sein de la liste de Filtrage Diameter.	
Filtrage SS7	
Nom	Saisissez un nom à donner au filtre SS7.
Action (Action)	Définissez l'action que le pare-feu doit prendre à l'égard des blocs SS7 qui contiennent les éléments de filtrage SS7 définis. Si le bloc faisant l'objet de l'inspection contient le SSN du demandeur du sous-système de commande de connexions sémaphores *et* n'importe laquelle des valeurs Global Title (appellation globale ; GT) du demandeur du sous-système de commande de connexions sémaphores définies *et* n'importe lequel des Codes d'opération définis, alors : • **allow (autoriser)** (par défaut) : autorise le bloc à passer sans modification. • **alert (alerter)** : autorise le bloc à passer sans modification et génère un journal SCTP (vous devez allouer un espace au stockage de ces journaux ; consultez l'onglet Stockage des journaux sous les paramètres de journalisation et de génération de rapports : Périphérique > Configuration > Gestion). • **block (bloquer)** : abandonne le bloc avant de laisser passer le paquet et génère un journal SCTP (vous devez allouer un espace au stockage de ces journaux ; consultez l'onglet Stockage des journaux sous les paramètres de journalisation et de génération de rapports : Périphérique > Configuration > Gestion).
SSN du demandeur du sous-système de commande de connexions sémaphores	Définissez le SSN du demandeur du sous-système de commande de connexions sémaphores d'application pour un bloc à l'égard duquel le pare-feu prend l'action définie. Sélectionnez **any-**

Paramètres des profils de protection SCTP	
	map (indifférent-mappage) ou **Add (Ajoutez)** un des SSN de demandeur du sous-système de commande de connexions sémaphores à partir de la liste déroulante : • **HLR(MAP)** • **VLR(MAP)** • **MSC(MAP)** • **EIR(MAP)** • **GMLC(MAP)** • **gsmSCF(MAP)** • **SIWF(MAP)** • **SGSN(MAP)** • **GGSN(MAP)** • **CSS(MAP)** • **CAP** • **INAP** • **Gestion SCCP** Un filtre SS7 ne peut posséder qu'un seul SSN du demandeur du sous-système de commande de connexions sémaphores.
GT du demandeur du sous-système de commande de connexions sémaphores	Définissez la valeur GT du demandeur du sous-système de commande de connexions sémaphores d'application pour un bloc à l'égard duquel le pare-feu prend l'action définie. Sélectionnez **Any (Indifférent)** ou **Add (Ajoutez)** une valeur numérique comportant jusqu'à 15 chiffres. Vous pouvez également saisir un groupe de valeurs GT du demandeur du sous-système de commande de connexions sémaphores à l'aide d'un préfixe. Par exemple : 876534*. Vous pouvez ajouter plusieurs valeurs GT du demandeur du sous-système de commande de connexions sémaphores dans un filtre SS7. Pour le SSN du demandeur du sous-système de commande de connexions sémaphores : **INAP** et **SCCP Management (Gestion SCCP)**, cette option est désactivée.
Code d'opération	Définissez le code d'opération d'un bloc à l'égard duquel le pare-feu prend l'action définie. Pour les SSN de demandeur du sous-système de commande de connexions sémaphores suivants, sélectionnez **any (indifférent)** ou un code d'opération dans la liste déroulante, ou saisissez une valeur précise (plage comprise entre 1 et 255) : • **HLR(MAP)** • **VLR(MAP)**

Paramètres des profils de protection SCTP	
	• **MSC(MAP)** • **EIR(MAP)** • **GMLC(MAP)** • **gsmSCF(MAP)** • **SIWF(MAP)** • **SGSN(MAP)** • **GGSN(MAP)** • **CSS(MAP)** Pour le SSN du demandeur du sous-système de commande de connexions sémaphores : **CAP**, saisissez une valeur (plage comprise entre 1 et 255). Pour le SSN du demandeur du sous-système de commande de connexions sémaphores : **INAP** et **SCCP Management (Gestion SCCP)**, cette option est désactivée. Vous pouvez ajouter plusieurs Codes d’opération dans un filtre SS7.
Si vous créez plus d’un filtre SS7 pour un profil, l’ordre dans lequel les filtres SS7 apparaissent importe. Sélectionner un filtre, puis **Move Up (Déplacez vers le haut)** ou **Move Down (Déplacez vers le bas)** pour régler sa priorité relative au sein de la liste de Filtrage SS7.	

Objets > Groupes de profils de sécurité

Le pare-feu prend en charge la création de groupes de profils de sécurité, ce qui permet de définir des ensembles de profils de sécurité pouvant être traités en tant qu'unités, puis ajoutés aux politiques de sécurité. Par exemple, vous pouvez créer un groupe de profils de sécurité « *menaces* » qui inclut des profils antivirus, antispyware et de protection contre les vulnérabilités, puis créer une politique de sécurité comprenant ce profil « menaces ».

Les profils antivirus, antispyware, de protection contre les vulnérabilités, de filtrage des URL et de blocage des fichiers qui sont souvent appliqués ensemble peuvent être combinés en groupes de profils pour simplifier la création de politiques de sécurité.

Pour définir un nouveau profil de sécurité, sélectionnez **Objects (Objets)** > **Security Profiles (Profils de sécurité)**.

Le tableau suivant décrit les paramètres des profils de sécurité :

Paramètres des groupes de profils de sécurité	Description
Name (Nom)	Saisissez un nom pour le groupe de profils (31 caractères maximum). Ce nom apparaît dans la liste de profils lors de la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que le groupe de profils soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le groupe de profils sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le groupe de profils sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de cet objet de Groupes de profils de sécurité dans les groupes de périphériques qui héritent de l'objet. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l'objet.
Profils	Sélectionnez un profil antivirus, antispyware, de protection contre les vulnérabilités, de filtrage des URL et/ou de blocage des fichiers à inclure dans ce groupe. Les profils de filtrage des données peuvent également figurer dans les groupes de profils de sécurité. Reportez-vous à la section Objets > Profils de sécurité > Filtrage des données.

Objets > Transfert des journaux

Par défaut, les journaux générés par le pare-feu demeurent uniquement dans leur stockage local. Toutefois, vous pouvez utiliser Panorama™, le Service de journalisation ou des services externes (tel qu'un serveur Syslog) pour surveiller centralement les informations du journal en définissant un profil de Transfert des journaux et en l'affectant aux règles de politique de sécurité, d'authentification, de protection DoS et d'inspection des tunnels. Les profils de transfert de journaux définissent les destinations de transfert pour les Types de journaux suivants : Authentification, Filtrage des données, GTP, SCTP, Menaces, Trafic, Tunnel, Filtrage des URL et envois WildFire®.

Vous devriez transférer les journaux à Panorama ou au stockage externe pour diverses raisons, y compris la conformité, la redondance, l'exécution d'analyses, la surveillance centralisée et l'examen des comportements des menaces et des tendances à long terme. De plus, le pare-feu dispose d'une capacité de stockage des journaux limitée et supprime les plus vieux journaux au fur et à mesure que l'espace est plein. Veillez donc à transférer les journaux des menaces et les journaux WildFire.

Pour transférer d'autres types de journaux, voir Périphérique > Paramètres des journaux.

Pour activer le transfert à WildFire® des journaux ou des fichiers sur un pare-feu PA-7000 Series, vous devez d'abord configurer une Interface de carte de journal sur le pare-feu PA-7000 Series. Dès que vous configurez cette interface, le pare-feu utilise automatiquement ce port. Aucune configuration spéciale n'est requise. Vous n'avez qu'à configurer un port de données sur l'une des Network Processing Cards (cartes de traitement réseau ; NPC) du pare-feu de la série PA-7000 comme interface de type carte de journal et à vous assurer que le réseau que vous utilisez communique avec vos serveurs de journaux. Pour le transfert WildFire, le réseau doit communiquer correctement avec le cloud ou l'équipement WildFire (ou les deux).

Le tableau suivant décrit les paramètres du profil de transfert des journaux :

Paramètres des profils de transfert des journaux	Description
Name (Nom)	Saisissez un nom (jusqu'à 64 caractères) pour identifier le profil. Ce nom apparaît dans la liste de profils de transfert des journaux pour la définition de règles de politiques de sécurité. Le nom est sensible à la casse, doit être unique et peut inclure uniquement des lettres, chiffres, espaces, traits d'union et traits de soulignement.
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que le profil soit disponible pour : • **Tous les systèmes virtuels (vsys) sur un pare-feu comportant plusieurs vsys** - Si vous désactivez (décochez) cette option, le profil est disponible uniquement dans le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**.

Paramètres des profils de transfert des journaux	Description
	• **Tous les groupes de périphériques sur Panorama** - Si vous désactivez (décochez) cette option, le profil est disponible uniquement dans le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Permettez la journalisation améliorée des applications à Cortex Data Lake (y compris les journaux de trafic et les journaux URL) (Panorama uniquement)	Les journaux améliorés des applications pour les services de cloud Palo Alto Networks sont disponibles avec un abonnement à Cortex Data Lake. La journalisation améliorée des applications permet au pare-feu de collecter les données spécialement conçues pour accroître la visibilité des activités réseau pour les applications exécutant dans l'environnement des Services de cloud Palo Alto Networks.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce profil de transfert de journaux dans les groupes de périphériques qui héritent du profil. Cette sélection est désactivée (décochée) par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres de tous les groupes de périphériques qui héritent du profil.
Description	Saisissez une description pour expliquer le but de ce profil de transfert des journaux.
Liste de correspondance (non étiquetée)	Il vous faut **Ajouter** un ou plusieurs profils de liste de correspondance (jusqu'à 64) qui spécifient les destinations de transfert, les filtres de journal avec attributs pour contrôler quels journaux sont transférés par le pare-feu, et les mesures à prendre pour les journaux (tel que l'étiquetage automatique). Complétez les deux champs suivants (Nom et Description) pour chaque profil de liste de correspondance.
Nom (profil de liste de correspondance)	Saisissez un nom (jusqu'à 31 caractères) pour identifier le profil de la liste de correspondance.
Description (profil de liste de correspondance)	Saisissez une description (jusqu'à 1 023 caractères) pour expliquer le but de ce profil de liste de correspondance.
Type de journal	Sélectionnez le type de journal auquel profil de liste de correspondance s'applique : authentification (**auth**), **data (données)**, **gtp**, **sctp**, **threat (menaces)**, **traffic (trafic)**, **tunnel**, **URL** ou **WildFire**.
Filtre	Par défaut, le pare-feu transfère **Tous les journaux** des **Types de journaux** sélectionnés. Pour transférer un sous-ensemble des journaux, sélectionnez un filtre existant dans le menu déroulant ou sélectionnez **Générateur de filtre** pour ajouter un nouveau filtre. Pour chaque requête dans un nouveau filtre, il vous faut renseigner les champs suivants et **Add (Ajouter)** la requête :

Paramètres des profils de transfert des journaux	Description
	• **Connector (Connecteur)** – Sélectionnez le connecteur logique (et/ou) pour la requête. Sélectionnez **Negate (Ignorer)** si vous ne voulez pas appliquer le connecteur logique. Par exemple, pour éviter de transférer les journaux à partir d'une zone non approuvée, sélectionnez **Negate (Ignorer)**, sélectionnez **Zone** en tant qu'attribut, sélectionnez **equal (égal)** en tant qu'Opérateur et saisissez le nom de la Zone non approuvée dans la colonne Valeur. • **Attribute (Attribut)** – Sélectionnez un attribut de journal. Les attributs disponibles dépendent du **Type de journal**. • **Operator (Opérateur)** - Sélectionnez des critères pour déterminer si un attribut s'applique (comme =). Les critères disponibles dépendent du **Type de journal**. • **Value (Valeur)** : indiquez la valeur de l'attribut à faire correspondre. Pour display or export (afficher ou exporter) les journaux que le filtre met en correspondance, sélectionnez l'option **View Filtered Logs (Afficher les journaux filtrés)**, qui fournit les mêmes options que les pages de l'onglet **Monitoring (Surveillance)** (comme **Monitoring (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)**).
Panorama Panorama/Service de journalisation (Panorama uniquement)	Sélectionnez **Panorama** si vous souhaitez transmettre des journaux aux collecteurs de journaux, au serveur de gestion Panorama ou au Service de journalisation. Si vous activez cette option, vous devez configurer le transfert des journaux vers Panorama. Pour utiliser le Service de journalisation, vous devez également **Enable (Activer)** le Service de journalisation sous Périphérique > Configuration > Gestion.
SNMP	Cliquez pour **Ajouter** un ou plusieurs profils de serveur pour transférer des journaux en tant que pièges SNMP (voir Périphérique > Profils de serveur > Piège SNMP).
Messagerie	Cliquez pour **Ajouter** un ou plusieurs profils de serveur de messagerie pour transférer des journaux en tant que notifications par e-mail (voir Périphérique > Profils de serveur > E-mail).
Syslog	Cliquez pour **Ajouter** un ou plusieurs profils de serveur Syslog pour transférer des journaux en tant que messages Syslog (voir Périphérique > Profils de serveur > Syslog).
HTTP	Cliquez pour **Ajouter** un ou plusieurs profils de serveur HTTP pour transférer des journaux en tant que requêtes HTTP (voir Périphérique > Profils de serveur > HTTP).

Paramètres des profils de transfert des journaux	Description
Actions intégrées	Vous pouvez sélectionner deux types d'actions intégrées lorsqu vous **Add (Ajouter)** une action à faire : l'Étiquetage et l'Intégration. • **Étiquetage** : Ajoutez ou supprimez automatiquement une étiquette à l'adresse IP source ou de destination dans une entrée de journal et enregistrez l'adresse IP et le mappage des étiquettes pour l'agent User-ID sur le pare-feu ou Panorama ou pour un agent User-ID distant afin que vous puissiez répondre à un événement et que vous puissiez appliquer dynamiquement la politique de sécurité. La possibilité d'étiqueter une adresse IP et d'appliquer dynamiquement une politique à l'aide de groupes d'adresses dynamiques vous offre une meilleure visibilité, un meilleur contexte et un meilleur contrôle pour appliquer de manière cohérente la politique de sécurité indépendamment de l'endroit où l'adresse IP se déplace sur votre réseau. Configurez les paramètres suivants: • Cliquez pour **Ajouter** une action et saisissez un nom pour la décrire. • Sélectionnez l'adresse IP cible que vous souhaitez étiqueter – **Adresse source** ou **Adresse de destination**. Vous pouvez prendre une mesure pour tous les types de journaux qui incluent une adresse IP source ou de destination dans l'entrée de journal. Vous pouvez uniquement étiqueter l'adresse IP source, dans les journaux de corrélation et les journaux de correspondance HIP. Vous ne pouvez pas configurer une action pour les journaux système et les journaux de configuration, car le type de journal ne comporte pas une adresse IP dans l'entrée de journal. • Sélectionnez l'action – **Add Tag (Ajouter une étiquette)** ou **Remove Tag (Supprimer une étiquette)**. • Choisissez si vous souhaitez enregistrer l'adresse IP et étiqueter le mappage sur l'agent **Local User-ID (User-ID local)** sur ce pare-feu ou Panorama, ou sur un agent **Remote User-ID (User-ID à distance)**. • Pour enregistrer l'adresse IP et étiqueter le mappage sur un agent **User-ID à distance**, sélectionnez le profil de serveur HTTP (Périphérique > Profils de serveur > HTTP) qui permettra le transfert. • Configurez le **Timeout (Délai)**, en minutes, de l'indicateur d'adresse IP à définir, la période de temps pendant laquelle le mappage adresse IP/étiquette est maintenu. Si vous définissez le délai sur 0, le mappage de l'indicateur d'adresse IP n'expire jamais (la plage est définie entre 0 et 43 200 [30 jours] ; la valeur par défaut est 0). *Vous pouvez uniquement configurer un délai avec l'action **Add Tag (Ajouter une étiquette)**.*

Paramètres des profils de transfert des journaux	Description
	• Saisissez ou sélectionnez les **Tags (Étiquettes)** que vous souhaitez appliquer ou supprimer de la source cible ou de l'adresse IP de destination. • **Intégration** : disponible uniquement pour les pare-feu VM-Series dans Azure. Cette option vous permet de transférer les journaux sélectionnés au Centre de sécurité Azure via l'action **Azure-Security-Center-Integration (Intégration au Centre de sécurité Azure)**. Pour ajouter un périphérique à la liste de quarantaine sur la base du filtre du profil de transfert des journaux, sélectionnez **Quarantine (Quarantaine)**.

Objets > Authentification

Un objet d'application d'authentification indique la méthode et le service à utiliser pour les utilisateurs finaux s'authentifiant qui accèdent à vos ressources réseau. Vous affectez l'objet aux règles de la politique d'Authentification qui appellent la méthode d'authentification et le service lorsque le trafic correspond à une règle (voir Policies > Authentication (Politiques > Authentification).

Le pare-feu possède les objets d'application d'authentification prédéfinis suivants (en lecture seule) :

- **Défi de navigation par défaut** - Le pare-feu obtient de façon transparente les informations d'identification d'authentification de l'utilisateur. Si vous sélectionnez cette action, vous devez activer l'ouverture de session unique (SSO) Kerberos ou l'authentification NTLM (NT LAN Manager) lors de la configure Authentication Portal (Configuration du portail d'authentification). En cas d'échec de l'authentification SSO Kerberos, le pare-feu revient à l'authentification NTLM. Si vous n'avez pas configuré NTLM, ou si l'authentification NTLM échoue, le pare-feu revient à la méthode d'authentification spécifiée dans l'objet **formulaire Web par défaut** prédéfini.
- **default-web-form (Formulaire Web par défaut)** – Pour authentifier les utilisateurs, le pare-feu utilise le profil de certificat ou le profil d'authentification que vous avez spécifié lors de la configuring Authentication Portal (configuration du portail d'authentification). Si vous avez indiqué un profil d'authentification, le pare-feu ignore tous les paramètres Kerberos SSO du profil et présente une page du Portail d'Authentification pour que l'utilisateur saisisse ses informations d'authentification.
- **Aucun portail captif par défaut** – Le pare-feu évalue la politique de Sécurité sans authentifier les utilisateurs.

Avant de créer un objet d'application d'authentification personnalisé :

- Configurez un profil de serveur qui spécifie la façon de se connecter au service d'authentification (reportez-vous à la section Device > Server Profiles (Périphérique > Profils de serveur)).
- Affectez le profil de serveur à un profil d'authentification qui indique les paramètres d'authentification comme les paramètres d'ouverture de session Kerberos unique (voir Device > Authentication Profile (Périphérique > Profil d'authentification)).

Pour créer un objet d'application d'authentification personnalisé, cliquez sur **Ajouter** et remplissez les champs suivants :

Paramètres de l'application d'authentification	Description
Name (Nom)	Saisissez un nom descriptif (jusqu'à 31 caractères) pour vous aider à identifier l'objet lors de la définition des règles d'Authentification. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que l'objet soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous décochez cette sélection, l'objet sera disponible uniquement sur le **Système virtuel** sélectionné dans l'onglet **Objets**.

Paramètres de l’application d’authentification	Description
	• Chaque groupe de périphériques sur Panorama. Si vous décochez cette sélection, l’objet sera disponible uniquement sur le **Groupe de périphériques** sélectionné dans l’onglet **Objets**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de cet objet d’application d’authentification dans les groupes de périphériques qui héritent de l’objet. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de l’objet.
Méthode d’authentification	Sélectionnez une méthode : • **Défi de navigation** - Le pare-feu obtient de façon transparente les informations d’identification d’authentification de l’utilisateur. Si vous sélectionnez cette action, le **Authentication Profile (Profil d'authentification)** que vous sélectionnez doit avoir Kerberos SSO activé. • **Web-form (Formulaire Web)** – Pour authentifier les utilisateurs, le pare-feu utilise le profil de certificat que vous avez indiqué lors de la configuring Authentication Portal (configuration du portail d’authentification) ou le **Authentication Profile (Profil d’authentification)** que vous sélectionnez dans l’objet d’application d’authentification. Si vous sélectionnez un **Authentication Profile (Profil d’authentification)**, le pare-feu ignore tous les paramètres Kerberos SSO du profil et présente une page du Portail captif pour que l’utilisateur saisisse ses informations d’authentification. • **Aucun portail captif** – Le pare-feu évalue la politique de Sécurité sans authentifier les utilisateurs.
Profil d'authentification	Sélectionnez le profil d’authentification qui indique le service à utiliser pour valider l’identité des utilisateurs.
Message	Saisissez les instructions qui indiquent aux utilisateurs comment répondre à la première demande d’authentification qu’ils voient lorsque leur trafic déclenche la règle d’Authentification. Le message s’affiche dans la**Authentication Portal Comfort Page (Page confort du portail d’authentification)**. Si vous ne saisissez pas de message, la page **Captive Portal Comfort Page (Page Confort du portail captif**par défaut s’affiche (voir Device > Response Pages (Périphérique > Pages de réponse)).

Paramètres de l’application d’authentification	Description
	*Le pare-feu affiche la **Authentication Portal Comfort Page (Page Confort du portail d’authentification)** uniquement pour la première demande d’authentification (facteur) que vous définissez dans l’onglet **Authentication (Authentification)** du **Authentication Profile (Profil d’authentification)** (voir Device > Authentication Profile (Périphérique > Profil d'authentification)). Pour les demandes d’authentification multi-facteur (MFA) que vous définissez dans l’onglet **Factors (Facteurs)** du profil, le pare-feu affiche la **MFA Login Page (Page de connexion MFA)**.*

Objets > Profils de déchiffrement

Les profils de déchiffrement vous permettent de bloquer et de contrôler des aspects précis du trafic SSL et SSH devant être déchiffré ainsi que du trafic que vous avez explicitement exclu du déchiffrement. Après avoir créé un profil de déchiffrement, vous pourrez ensuite l'ajouter à une politique de déchiffrement ; tout trafic correspondant à cette politique de déchiffrement est mis en œuvre selon les paramètres du profil.

Un profil de déchiffrement par défaut est configuré sur le pare-feu et est automatiquement inclus dans les nouvelles politiques de déchiffrement (vous ne pouvez pas modifier le profil de déchiffrement par défaut). Cliquez sur **Add (Ajouter)** pour créer un nouveau profil de déchiffrement ou sélectionnez un profil existant et cliquez sur **Clone (Cloner)** pour le cloner ou le modifier.

Que voulez-vous faire ?	Reportez-vous à la section :
Ajouter un nouveau profil de déchiffrement. Activer la mise en miroir des ports pour le trafic déchiffré.	Paramètres généraux des profils de déchiffrement
Bloquer et contrôler le trafic SSL déchiffré.	Paramètres de contrôle du trafic SSL décrypté
Bloquer et contrôler le trafic que vous avez exclu du déchiffrement (par exemple, le trafic classé comme services relatifs à la santé, au domaine médical et à la finance).	Paramètres de contrôle du trafic non déchiffré
Bloquer et contrôler le trafic SSH déchiffré.	Paramètres de contrôle du trafic SSH déchiffré

Paramètres généraux des profils de déchiffrement

Le tableau suivant décrit les paramètres généraux des profils de déchiffrement.

Profil de déchiffrement – Paramètres généraux	Description
Name (Nom)	Saisissez un nom pour le profil (**31** caractères maximum). Ce nom apparaît dans la liste des profils de déchiffrement lors de la définition des politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement.

Profil de déchiffrement – Paramètres généraux	Description
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que le profil soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le profil sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de ce profil de Décryptage pour les groupes de périphériques qui héritent du profil. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres de tous les groupes de périphériques qui héritent du profil.
Interface de mise en miroir du déchiffrement (Prise en charge sur tous les modèles, sauf le pare-feu VM-Series sur AWS, sur Azure, sur Édition NSX, sur Citrix SDX.)	Sélectionnez une **Interface** à utiliser pour la Mise en miroir du port de déchiffrement. *Avant d'activer la mise en miroir du port de déchiffrement, vous devez obtenir une licence Mise en miroir du port de déchiffrement, l'installer et redémarrer le pare-feu.*
Transmis uniquement (Prise en charge sur tous les modèles, sauf le pare-feu VM-Series sur AWS, sur Azure, sur Édition NSX, sur Citrix SDX.)	Sélectionnez **Transmis uniquement** pour mettre en miroir le trafic décrypté uniquement après la mise en œuvre de la politique de sécurité. Avec cette option, seul le trafic qui est transféré vers le pare-feu est mis en miroir. Cette option est utile si vous transférez le trafic décrypté vers d'autres périphériques de détection des menaces, tels qu'un périphérique DLP (prévention des fuites de données) ou un autre système de prévention des intrusions (IPS). Si vous désélectionnez cette option (paramètre par défaut), le pare-feu mettra en miroir tout le trafic décrypté sur l'interface avant de rechercher des politiques de sécurité, ce qui vous permettra de rejouer les événements et d'analyser le trafic qui génère une menace ou déclenche une action d'abandon.

Paramètres de contrôle du trafic SSL déchiffré

Le tableau suivant décrit les paramètres que vous pouvez utiliser pour contrôler le trafic que le pare-feu a déchiffré à l'aide du déchiffrement du proxy de transfert ou de l'inspection entrante (y compris l'onglet des Paramètres de protocole SSL). Vous pouvez utiliser ces paramètres pour limiter ou bloquer des sessions

TLS basées sur des critères, notamment l'état du certificat du serveur externe, l'utilisation de suites de chiffrement ou de versions de protocoles non prises en charge ou la disponibilité de ressources système pour traiter le déchiffrement.

Paramètres de l’onglet Déchiffrement SSL	Description
ONGLET PROXY DE TRANSFERT SSL Sélectionnez des options pour limiter ou bloquer le trafic TLS déchiffré à l'aide du proxy de transfert.	
Validation des certificats du serveur – Sélectionnez des options pour contrôler les certificats du serveur dans le trafic déchiffré.	
Bloquer les sessions avec un certificat expiré	Mettez fin à la connexion TLS si le certificat du serveur a expiré. Cela empêche les utilisateurs d'accepter des certificats expirés et de poursuivre une session TLS.  *Bloquez les sessions avec des certificats expirés pour empêcher l’accès aux sites éventuellement non sécuritaires.*
Bloquer les sessions avec des émetteurs non approuvés	Mettez fin à la session TLS si l'émetteur des certificats du serveur n'est pas approuvé.  *Bloquez les sessions avec des émetteurs non approuvés, car un émetteur non approuvé peut indiquer la présence d’une attaque par hôte interposé, d’une attaque par rejeu ou d’un autre type d’attaque.*
Bloquer les sessions dont l'état du certificat est inconnu	Mettez fin à la session TLS si un serveur renvoie l'état « inconnu » pour la révocation d'un certificat. L'état de révocation du certificat indique si la confiance d'un certificat a été révoquée ou pas.  *Pour disposer de la sécurité la plus stricte, bloquez les sessions dont l’état du certificat est inconnu. Cependant, comme l’état des certificats peut être inconnu pour une diversité de raisons, la sécurité pourrait être trop stricte. Si le blocage de l’état des certificats inconnu affecte des sites que vous devez utiliser à des fins commerciales, ne bloquez pas les sessions dont l'état du certificat est inconnu.*
Bloquer les sessions dont le délai d'attente de vérification de l'état du certificat a expiré	Mettez fin à la session TLS si l'état du certificat ne peut pas être récupéré lors du délai pendant lequel le pare-feu est configuré pour arrêter d'attendre la réponse d'un service de rapport sur l'état du certificat. Vous pouvez configurer la valeur de **Certificate Status Timeout (Délai d’expiration du statut du certificat)** lors de la création ou de la modification d’un profil de certificat (**Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificate Profile (Profil de certificat)**).

Paramètres de l’onglet Déchiffrement SSL	Description
	Le blocage des sessions lors de la temporisation de la vérification de l’état est un compromis entre une sécurité plus stricte et une meilleure expérience utilisateur. Si les serveurs de révocation du certificat répondent lentement, le blocage lors de l'expiration du délai peut bloquer des sites qui disposent de certificats valides. Vous pouvez augmenter la valeur de délai d'attente de la vérification de la révocation du certificat et du protocole OCSP si vous vous préoccupez des certificats valides arrivant à expiration.
Limiter les extensions de certificat	Limite les extensions de certificat utilisées pour le certificat du serveur dynamique à l'utilisation de la clé et à l'utilisation améliorée de la clé. *Restreignez les extensions de certificat si votre déploiement exige aucune autre extension de certificat.*
Ajouter la valeur CN du certificat à l’extension SAN	Permettez au pare-feu d'ajouter une extension Subject Alternative Name (autre nom de l'objet ; SAN) au certificat d’emprunt d’identité qu’il présente au client dans le cadre du déchiffrement de proxy de transfert. Lorsqu’un certificat de serveur contient uniquement un nom commun (CN), le pare-feu ajoute une extension SAN au certificat d’emprunt d’identité basé sur le certificat de serveur CN. Cette option est utile dans les cas où les navigateurs exigent des certificats de serveur pour utiliser un SAN et ne prennent plus en charge la correspondance de certificats basée sur des CDN ; il garantit que les utilisateurs finaux peuvent continuer à accéder aux ressources Web demandées et que le pare-feu peut continuer à déchiffrer les sessions même si un certificat de serveur ne contient qu’un CN. *Ajoutez la valeur CN du certificat à l’extension SAN pour garantir l’accès aux ressources Web demandées.*
Vérifications des modes non pris en charge – Sélectionnez des options pour contrôler les applications TLS non prises en charge.	
Bloquer les sessions avec une version non prise en charge	Mettez fin à la session si PAN-OS ne prend pas en charge le message « client hello ». PAN-OS est compatible avec SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, et TLSv1.3.

Paramètres de l’onglet Déchiffrement SSL	Description
	*Bloquez toujours les sessions avec une version non prise en charge pour empêcher l’accès à des sites disposant de protocoles faibles. À l’onglet **SSL Protocol Settings (Paramètres du protocole SSL)**, définissez la version du protocole minimale sur TLSv1.2 pour bloquer les sites ayant des versions de protocole faibles. Si un site auquel vous devez accéder à des fins professionnelles utilise un protocole plus fiable, créez un profil de déchiffrement distinct qui autorise le protocole plus faible et précisez-le dans une règle de politique de déchiffrement qui s’applique uniquement aux sites pour lesquels vous autorisez le protocole le plus faible.*
Bloquer les sessions avec des suites de cryptage non prises en charge	Mettez fin à la session si la suite de chiffrement définie dans la négociation TLS n'est pas prise en charge par PAN-OS. *Bloquez les sessions qui utilisent des suites de chiffrement que vous ne prenez pas en charge. Vous configurez les suites de chiffrement (algorithmes de chiffrement) à autoriser à l’onglet **SSL Protocol Settings (Paramètres du protocole SSL)**. N'autorisez pas les utilisateurs à se connecter à des sites ayant des suites de chiffrement faibles.*
Bloquer les sessions avec authentification du client	Mettez fin aux sessions avec authentification du client pour le trafic du proxy de transfert. *Bloquez les sessions avec authentification du client sauf si une application importante l'exige. Dans ce cas, vous devriez créer un profil de déchiffrement distinct et l’appliquer uniquement au trafic qui exige l’authentification du client.*
Vérification des échecs – Sélectionnez la mesure à prendre si les ressources du système ne sont pas disponibles pour traiter le décryptage.	
Bloquer les sessions si les ressources ne sont pas disponibles	Mettez fin aux sessions si les ressources du système ne sont pas disponibles pour traiter le déchiffrement. La décision de bloquer les sessions lorsque les ressources ne sont pas disponibles est un compromis entre une sécurité plus stricte et une meilleure expérience utilisateur. Si vous ne bloquez pas les sessions lorsque les ressources ne sont pas disponibles, le pare-feu n’arrivera pas à déchiffrer le trafic que vous souhaitez déchiffrer lorsque les ressources sont touchées. Cependant, le fait de bloquer des sessions lorsque les ressources ne sont pas disponibles peut influer sur l’expérience utilisateur, car les

Paramètres de l’onglet Déchiffrement SSL	Description
	sites qui sont normalement disponibles peuvent devenir temporairement indisponibles.
Bloquer les sessions si HSM n'est pas disponible	Mettez fin aux sessions si aucun module de sécurité matériel n'est disponible pour signer les certificats. La décision de bloquer les sessions si le HSM n'est pas disponible dépend de vos règles de conformité sur la provenance de vos clés privés et de votre manière de gérer le trafic chiffré si le HSM n'est pas disponible.
Bloquer le déclassement en l’absence de ressources	Trine la session si les ressources du système ne sont pas disponibles pour traiter la communication TLSv1.3 (au lieu de déclasser en TLSv1.2). La décision de bloquer les sessions lorsque les ressources ne sont pas disponibles est un compromis entre une sécurité plus stricte et une meilleure expérience utilisateur. Si vous bloquez le déclassement de la communication vers TLSv1.2 lorsque les ressources TLSv1.3 ne sont pas disponibles, le pare-feu annule la session. Si vous ne bloquez pas le déclassement de la communication, alors si les ressources ne sont pas disponibles pour la communication TLSv1.3, le pare-feu déclasse vers TLSv1.2.
Extension client	
Enlever l’ALPN	Le pare-feu traite et inspecte le trafic HTTP/2 par défaut. Cependant, vous pouvez désactiver l’inspection HTTP/2 en indiquant que le pare-feu doit **Strip ALPN (Enlever l’ALPN)**. Lorsque cette option est sélectionnée, le pare-feu supprime la valeur contenue dans l’extension TLS Application-Layer Protocol Negotiation (ALPN)). Comme ALPN est utilisé pour sécuriser les connexions HTTP/2 connections, lors qu’aucune valeur n’est indiquée pour cet extension TLS, le pare-feu déclasse le trafic HTTP/2 en HTTP/1.1 ou le classe en tant que trafic TCP inconnu.

pour les modes et les défaillances non pris en charge, les informations de session sont mises en cache pendant 12 heures, par conséquent, les sessions à venir entre les mêmes paires d'hôtes et de serveurs ne sont pas déchiffrées. Activez plutôt les options pour bloquer ces sessions.

ONGLET INSPECTION SSL ENTRANTE

Sélectionnez les options pour limiter ou bloquer le trafic déchiffré à l'aide de l’inspection entrante.

Vérifications des modes non pris en charge – Sélectionnez ces options pour contrôler des sessions si des modes non pris en charge sont détectés dans le trafic TLS.

Paramètres de l’onglet Déchiffrement SSL	Description
Bloquer les sessions avec une version non prise en charge	Mettez fin à la session si PAN-OS ne prend pas en charge le message « client hello ». PAN-OS est compatible avec SSLv3, TLSv1.0, TLSv1.1, TLSv1.2, et TLSv1.3. *Bloquez toujours les sessions avec une version non prise en charge pour empêcher l’accès à des sites disposant de protocoles faibles. À l’onglet **SSL Protocol Settings (Paramètres du protocole SSL)**, définissez la version du protocole minimale sur TLSv1.2 pour bloquer les sites ayant des versions de protocole faibles. Si un site auquel vous devez accéder à des fins professionnelles utilise un protocole plus fiable, créez un profil de déchiffrement distinct qui autorise le protocole plus faible et précisez-le dans une règle de politique de déchiffrement qui s’applique uniquement aux sites pour lesquels vous autorisez le protocole le plus faible.*
Bloquer les sessions avec des suites de cryptage non prises en charge	Mettez fin à la session si la suite de chiffrement utilisée n'est pas prise en charge par PAN-OS. *Bloquez les sessions qui utilisent des suites de chiffrement que vous ne prenez pas en charge. Vous configurez les suites de chiffrement (algorithmes de chiffrement) à autoriser à l’onglet **SSL Protocol Settings (Paramètres du protocole SSL)**. N'autorisez pas les utilisateurs à se connecter à des sites ayant des suites de chiffrement faibles.*
Vérification des échecs – Sélectionnez la mesure à prendre si les ressources du système ne sont pas disponibles.	
Bloquer les sessions si les ressources ne sont pas disponibles	Mettez fin aux sessions si les ressources du système ne sont pas disponibles pour traiter le déchiffrement. La décision de bloquer les sessions lorsque les ressources ne sont pas disponibles est un compromis entre une sécurité plus stricte et une meilleure expérience utilisateur. Si vous ne bloquez pas les sessions lorsque les ressources ne sont pas disponibles, le pare-feu n’arrivera pas à déchiffrer le trafic que vous souhaitez déchiffrer lorsque les ressources sont touchées. Cependant, le fait de bloquer des sessions lorsque les ressources ne sont pas disponibles peut influer sur l’expérience utilisateur, car les sites qui sont normalement disponibles peuvent devenir temporairement indisponibles.
Bloquer les sessions si HSM n'est pas disponible	Mettez fin aux sessions si aucun module de sécurité matériel n'est disponible pour déchiffrer la clé de session.

Paramètres de l’onglet Déchiffrement SSL	Description
	La décision de bloquer les sessions si le HSM n'est pas disponible dépend de vos règles de conformité sur la provenance de vos clés privés et de votre manière de gérer le trafic chiffré si le HSM n'est pas disponible.
Bloquer le déclassement en l’absence de ressources	Trine la session si les ressources du système ne sont pas disponibles pour traiter la communication TLSv1.3 (au lieu de déclasser en TLSv1.2). La décision de bloquer les sessions lorsque les ressources ne sont pas disponibles est un compromis entre une sécurité plus stricte et une meilleure expérience utilisateur. Si vous bloquez le déclassement de la communication vers TLSv1.2 lorsque les ressources TLSv1.3 ne sont pas disponibles, le pare-feu annule la session. Si vous ne bloquez pas le déclassement de la communication, alors si les ressources ne sont pas disponibles pour la communication TLSv1.3, le pare-feu déclasse vers TLSv1.2.
ONGLET DES PARAMÈTRES DU PROTOCOLE SSL Sélectionnez les paramètres suivants pour mettre en œuvre les versions de protocole et les suites de déchiffrement du trafic de la session TLS.	
Versions du protocole	Imposez l'utilisation des versions minimales et maximales du protocole pour la session TLS.
Version min	Définissez la version minimale du protocole qui peut être utilisée pour établir la connexion TLS. *Définissez la version minimale sur TLSv1.2 afin de fournir la sécurité la plus forte. Passez en revue les sites qui ne prennent pas en charge TLSv1.2 pour voir s’ils ont un véritable objectif commercial. Pour les sites auxquels vous devez accéder qui ne prennent pas en charge TLSv1.2, créez un profil de déchiffrement distinct qui spécifie la version la plus forte du protocole qu’ils prennent en charge et appliquez-le à une règle de politique de déchiffrement qui restreint l’utilisation de la version faible uniquement aux sites nécessaires, provenant uniquement des sources nécessaires (zones, adresses, utilisateurs).*
Version max	Définissez la version maximale du protocole qui peut être utilisée pour établir la connexion TLS. Vous pouvez choisir l'option Max où aucune version maximale n'est spécifiée ; dans ce cas, les versions du protocole qui sont équivalentes ou ultérieures à la version minimale sélectionnée sont prises en charge.

Paramètres de l'onglet Déchiffrement SSL	Description
	*Définissez la version maximale sur **Max**, pour que, lorsque les protocoles s'améliorent, le pare-feu les prend automatiquement en charge.* *Cependant, si votre Politique de décryptage est compatible avec des applications mobiles, dont beaucoup utilisent des certificats intégrés, réglez la **Max Version (Version max.)** sur **TLSv1.2**. Parce que TLSv1.3 crypte les informations du certificat qu n'étaient pas cryptées dans les versions TLS antérieures, le pare-feu ne peut pas ajouter automatiquement des exclusions de décryptage sur la base des informations du certificat, ce qui affecte certaines applications mobiles. Par conséquent, si vous activez TLSv1.3, le pare-feu peut annuler certains trafics d'application mobile sauf si vous créez une Politique de non déchiffrement pour ce trafic. Si vous connaissez les applications mobiles que vous utilisez pour votre entreprise, envisagez de créer une politique et un profil de déchiffrement séparés pour ces applications afin de pouvoir activer TLSv1.3 pour le reste du trafic.*
Algorithmes d'échange de clés	Imposez l'utilisation des algorithmes d'échange de clés sélectionnés pour la session TLS. Les trois algorithmes (**RSA**, **DHE** et **ECDHE**) sont activés par défaut. Le **DHE** (Diffie-Hellman) et le **ECDHE** (Diffie-Hellman basé sur les courbes elliptiques) activent le Perfect Forward Secrecy (PFS) pour le déchiffrement du proxy de transfert ou de l'inspection sortante.
Algorithmes de chiffrement	Imposez l'utilisation des algorithmes de chiffrement sélectionnés pour la session TLS. *Ne prenez pas en charge les algorithmes de chiffrement **3DES** ou **RC4**. (Le pare-feu bloque automatiquement ces deux algorithmes lorsque vous utilisez TLSv1.2 ou une version supérieure comme version de protocole minimale.) Si vous devez faire une exception et que vous devez prendre en charge une version de protocole plus faible, décochez **3DES** et **RC4** dans le profil de déchiffrement. S'il y a des sites auxquels vous devez accéder à des fins professionnelles qui utilisent les algorithmes de chiffrement **3DES** ou **RC4**, créez un profil de déchiffrement distinct et appliquez-le à une règle de politique de déchiffrement qui s'applique uniquement à ces sites.*

Paramètres de l'onglet Déchiffrement SSL	Description
Algorithmes d'authentification	Imposez l'utilisation des algorithmes d'authentification sélectionnés pour la session TLS. *Bloquez l'ancien algorithme MD5 plus faible (bloqué par défaut). Si aucun site nécessaire n'utilise l'authentification SHA1, bloquez SHA1. S'il y a des sites auxquels vous devez accéder à des fins professionnelles qui utilisent SHA1, créez un profil de déchiffrement distinct et appliquez-le à une règle de politique de déchiffrement qui s'applique uniquement à ces sites.*

Paramètres de contrôle du trafic non déchiffré

Vous pouvez utiliser l'onglet **No Decryption (Aucun déchiffrement)** pour que les paramètres bloquent le trafic correspondant à une politique de déchiffrement configurée avec l'action **No Decrypt (Pas de déchiffrement)** (**Policies (Politiques)** > **Decryption (Déchiffrement)** > **Action**). Ces options permettent de contrôler les certificats des serveurs de la session, bien que le pare-feu ne déchiffre et n'inspecte pas le trafic de la session.

Paramètres de l'onglet Aucun déchiffrement	Description
Bloquer les sessions avec un certificat expiré	Mettez fin à la connexion SSL si le certificat du serveur a expiré. Cela empêche les utilisateurs d'accepter des certificats expirés et de poursuivre une session SSL. *Bloquez les sessions avec des certificats expirés pour empêcher l'accès aux sites éventuellement non sécuritaires.*
Bloquer les sessions avec des émetteurs non approuvés	Mettez fin à la session SSL si l'émetteur des certificats du serveur n'est pas approuvé. *Bloquez les sessions avec des émetteurs non approuvés, car un émetteur non approuvé peut indiquer la présence d'une attaque par hôte interposé, d'une attaque par rejeu ou d'un autre type d'attaque.*

Paramètres de contrôle du trafic SSH déchiffré

Le tableau suivant décrit les paramètres que vous pouvez utiliser pour contrôler le trafic SSH déchiffré entrant et sortant. Ces paramètres vous permettent de limiter ou de bloquer le trafic SSH tunnellisé en fonction de critères, notamment l'utilisation d'algorithmes non pris en charge, la détection d'erreurs SSH ou la disponibilité des ressources pour traiter le déchiffrement du proxy SSH.

Paramètres de l’onglet Proxy SSH	Description
Vérifications des modes non pris en charge – Utilisez ces options pour contrôler des sessions si des modes non pris en charge sont détectés dans le trafic SSH. La version SSH prise en charge est SSH version 2.	
Bloquer les sessions avec une version non prise en charge	Mettez fin aux sessions si le message « client hello » n'est pas pris en charge par PAN-OS. *Bloquez toujours les sessions avec une version non prise en charge pour empêcher l’accès à des sites disposant de protocoles faibles. À l’onglet **SSL Protocol Settings (Paramètres du protocole SSL)**, définissez la version du protocole minimale sur TLSv1.2 pour bloquer les sites ayant des versions de protocole faibles. Si un site auquel vous devez accéder à des fins professionnelles utilise un protocole plus fiable, créez un profil de déchiffrement distinct qui autorise le protocole plus faible et précisez-le dans une règle de politique de déchiffrement qui s’applique uniquement aux sites pour lesquels vous autorisez le protocole le plus faible.*
Bloquer les sessions avec des algorithmes non pris en charge	Mettez fin aux sessions si l'algorithme défini par le client ou le serveur n'est pas pris en charge par PAN-OS. *Bloquez toujours les sessions avec des algorithmes non pris en charge pour empêcher l’accès à des sites disposant des algorithmes faibles.*
Vérification des échecs – Sélectionnez les actions à prendre si des erreurs SSH surviennent et si les ressources du système ne sont pas disponibles.	
Bloquer les sessions avec des erreurs SSH	Mettez fin aux sessions si des erreurs SSH surviennent.
Bloquer les sessions si les ressources ne sont pas disponibles	Mettez fin aux sessions si les ressources du système ne sont pas disponibles pour traiter le déchiffrement. La décision de bloquer les sessions lorsque les ressources ne sont pas disponibles est un compromis entre une sécurité plus stricte et une meilleure expérience utilisateur. Si vous ne bloquez pas les sessions lorsque les ressources ne sont pas disponibles, le pare-feu n’arrivera pas à déchiffrer le trafic que vous souhaitez déchiffrer lorsque les ressources sont touchées. Cependant, le fait de bloquer des sessions lorsque les ressources ne sont pas disponibles peut influer sur l’expérience utilisateur, car les sites qui sont normalement disponibles peuvent devenir temporairement indisponibles.

Objets > Profil de broker de paquets

Le profil du Broker de paquet définit la manière dont le pare-feu transfère le trafic vers une chaîne de sécurité, qui est un ensemble de dispositifs de sécurité tierces en ligne qui fournit une inspection et une application de sécurité supplémentaires. Le profil définit les interfaces de pare-feu utilisées pour se connecter à la chaîne de sécurité, le type de chaîne de sécurité (pont transparent de couche 3 ou de couche 1), les premier et dernier dispositifs d'une chaîne de sécurité de couche 3, la répartition de session (équilibrage de charge) entre plusieurs chaînes de couche 3, ainsi que la surveillance de l'état et les actions à entreprendre en cas de défaillance de chemin ou de latence HTTP. Vous attachez un profil de Broker de paquets à une règle de politique du Broker de paquets. La règle de politique définit le trafic à transférer vers la chaîne de sécurité et le profil définit comment transférer ce trafic.

Avant de pouvoir configurer un profil de Broker de paquets, vous devez dédier au moins deux interfaces de couche 3 sur le pare-feu pour transférer le trafic vers la chaîne de sécurité.

1. Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet**.
2. Sélectionnez une interface à utiliser pour le transfert du Broker de paquets.
3. Définissez **Interface Type (Type d'interface)** sur **Layer 3 (Couche 3)**.
4. Sélectionnez **Avancées** > **autres informations**.
5. Sélectionnez **Network Packet Broker (Broker de paquets de réseau)** pour activer l'interface.
6. Répétez ces étapes avec une autre interface Ethernet. Si vous souhaitez plusieurs connexions dédiées (par exemple, pour vous connecter à plusieurs chaînes de sécurité), configurez une paire d'interfaces Ethernet pour chaque connexion dédiée.

Paramètres du profil Broker de paquets	Description
Name (Nom)	Donnez un nom descriptif au profil.
Description	Vous pouvez décrire les paramètres ou l'objectif du profil en option.
Onglet Général	
Type de chaîne de sécurité	Sélectionnez le type de chaîne de sécurité à laquelle le pare-feu transfère le trafic déchiffré : • **Routed (Layer 3) (Acheminé (de couche 3)** : Les périphériques de ce type de chaîne de sécurité utilisent des interfaces de couche 3 pour se connecter au réseau de la chaîne de sécurité. Chaque interface doit avoir une adresse IP et un masque de sous-réseau attribués. Les périphériques d'une chaîne de sécurité sont configurés avec des itinéraires statiques ou le routage dynamique pour acheminer le trafic entrant et sortant au prochain périphérique de la chaîne de sécurité et le retourner au pare-feu. • **Transparent Bridge (Pont transparent)** : Dans un réseau de chaîne de sécurité en passerelle transparente, tous les périphériques de la chaîne de sécurité sont configurés avec deux interfaces connectées au réseau

Paramètres du profil Broker de paquets	Description
	de la chaîne de sécurité. Les interfaces de passerelle transparente n'ont pas d'adresses IP, de masques de sous-réseau, de passerelles par défaut ou de tables de routage locales. Les dispositifs de chaîne de sécurité reçoivent le trafic sur une interface, analysent le trafic et appliquent la sécurité, puis le trafic s'éloigne de l'autre interface vers le périphérique de chaîne de sécurité suivant.
Activer IPv6	(Mode Passerelle transparente uniquement) Activez le transfert de trafic IPv6.
Sens du flux	Indiquez si le trafic entre dans la chaîne de sécurité à partir d'une interface de pare-feu et quitte la sécurité vers l'autre interface de pare-feu, ou si le trafic peut entrer et sortir de la chaîne de sécurité à partir des deux interfaces de pare-feu. • **Unidirectional (Unidirectionnel)**: le pare-feu transfère tout le trafic vers la chaîne de sécurité via **Interface #1** et reçoit le trafic de la chaîne de sécurité sur **Interface #2**. *Les deux interfaces doivent être dans la même zone.* • **Bidirectional (Bidirectionnel)** : le pare-feu transfère le trafic client-serveur à la chaîne de sécurité via **Interface #1** et reçoit le trafic de la chaîne de sécurité sur **Interface #2** . Le pare-feu transfère le trafic de serveur à client vers la chaîne de sécurité via **Interface #2** et reçoit le trafic de la chaîne de sécurité sur **Interface #1**. Le sens d'écoulement que vous sélectionnez dépend du type d'appareils dans la chaîne de sécurité. Par exemple, si une chaîne de sécurité se compose de périphériques sans état qui peuvent examiner les deux côtés d'une session, vous choisiriez le flux unidirectionnel.
Interface 1	Interfaces du Broker de paquets de réseau que le pare-feu utilise pour transférer le trafic vers une chaîne de sécurité et le recevoir. Vous devez configurer chaque interface en tant qu'interface du Broker de paquets de réseau, comme décrit au début de cette rubrique d'aide.
Interface 2	

Onglet Chaînes de sécurité

Configurez une ou plusieurs chaînes de sécurité de couche 3 (pour l'équilibrage de charge ou la redondance) sur une paire d'interfaces de pare-feu du Broker de paquets de réseau. Pour le type de chaîne de sécurité **Routed (Layer 3) (Routée (couche 3))**, vous devez configurer au moins une chaîne de sécurité pour spécifier où transférer le trafic. Pour plusieurs chaînes de sécurité, aswitch ou un autre périphérique doit gérer le routage entre le pare-feu et les chaînes.

Paramètres du profil Broker de paquets	Description
Les options de cet onglet ne sont disponibles que pour les chaînes de sécurité de couche 3 (routées).	
Activer	Activez la chaîne de sécurité.
Name (Nom)	Donnez un nom descriptif à la chaîne de sécurité.
Premier périphérique Dernier périphérique	Sélectionnez l'adresse IPv4 du premier périphérique et du dernier périphérique de la chaîne de sécurité ou définissez un nouvel Objet d'adresse pour facilement faire référence au périphérique.
Méthode de Distribution de Sessions	Lors du transfert à plusieurs chaînes de sécurité **Routed (Layer 3) (routées (couche 3)**, choisissez la méthode que le pare-feu utilisera pour distribuer les sessions déchiffrées parmi les chaînes de sécurité : • **IP Modulo (Modulo IP)** : le pare-feu attribue les sessions selon le hachage module des adresses IP source et de destination. • **IP Hash (Hachage IP)** : le pare-feu attribue les sessions selon le hachage IP des adresses IP source et de destination et des numéros de port. • **Round Robin (Permutation circulaire)** : le pare-feu alloue les sessions également entre les chaînes de sécurité. • **Lowest Latency (Plus faible latence)** : le pare-feu alloue un plus grand nombre de sessions à la chaîne de sécurité ayant la plus faible latence. Pour que cette méthode fonctionne comme prévu, vous devez également activer la Surveillance de la latence et la Surveillance HTTP dans **Health Monitor (Contrôle de fonctionnement)**).
Onglet Contrôle de fonctionnement	
Sur échec du contrôle de fonctionnement	Lorsque vous activez les vérifications de**Path Monitoring ((surveillance des chemins d'accès)**, **HTTP Monitoring (surveillance HTTP)**, ou **HTTP Monitoring Latency (Latence de surveillance HTTP)**, vous décidez également de ce qui se passe en cas de défaillance d'une chaîne (ou de toutes les chaînes s'il existe plusieurs chaînes). S'il existe plusieurs chaînes et qu'une ou plusieurs chaînes échouent à une vérification de l'état mais qu'au moins une chaîne est toujours saine, le pare-feu distribue le trafic aux chaînes restantes en fonction de la **Session Distribution Method (méthode de distribution de session)**. Si toutes les chaînes associées à une paire d'interfaces du Broker de paquets de réseau de pare-feu, vous pouvez : • **Bypass Security Chain (Contourner la chaîne de sécurité)** : le pare-feu transfère le trafic vers sa destination plutôt que vers la ou les chaînes défaillantes. Le pare-feu applique toujours des profils de sécurité et des protections configurés au trafic.

Paramètres du profil Broker de paquets	Description
	• **Block Session (Bloquer la session)** : le pare-feu bloque la session.
Condition d'échec du contrôle de fonctionnement	Si vous configurez plusieurs vérifications de l'état (vous pouvez configurer les trois vérifications de l'état d'une chaîne), configurez la façon dont le pare-feu définit une défaillance : • **OR Condition (Condition OU)** :si une vérification de l'état sélectionnée échoue, l'action **On Health Check Failure (Échec de la vérification de fonctionnement)** se produit. • **AND Condition (Condition ET)** : si toutes les vérifications d'intégrité sélectionnées échouent, l'action **On Health Check Failure (Échec de la vérification de fonctionnement)** se produit.
Surveillance des chemins Surveillance de la latence Surveillance HTTP	Activez le chemin d'accès, la latence HTTP ou la surveillance HTTP, ou une combinaison des trois vérifications de l'état pour identifier quand les chaînes de sécurité rencontrent une défaillance et configurez les mesures qui déterminent quand une défaillance s'est produite : • **Path Monitoring (Surveillance des chemins d'accès)**: vérifie la connectivité de l'appareil ; définissez le nombre de pings, l'intervalle de ping en secondes et le temps de maintien de la récupération en secondes. • **HTTP Monitoring (Surveillance HTTP)** : Vérifie la disponibilité et le temps de réponse des périphériques ; définissez le nombre HTTP et l'intervalle HTTP en secondes. • **HTTP Monitoring Latency (Latence de surveillance HTTP)** : vérifie la vitesse et l'efficacité du traitement des périphériques ; définissez la latence maximale en millisecondes, la durée de latence en secondes et la latence du journal qui dépasse la durée. Lorsque vous sélectionnez **HTTP Monitoring Latency (Latence de surveillance HTTP)**, **HTTP Monitoring (Surveillance HTTP)** est automatiquement sélectionnée. Les deux doivent être sélectionnés pour activer la surveillance de la latence.

Objets > Gestion des liens SD-WAN

Créez des profils à appliquer à des ensembles d'applications et services indiqués dans les règles de politique SD-WAN. Chaque type de profil contrôle différents aspects de la gestion de liens SD-WAN.

- Objects > SD-WAN Link Management > Path Quality Profile (Objets > Gestion des liens SD-WAN > Profil de qualité des chemins d'accès)
- Objects > SD-WAN Link Management > SaaS Quality Profile (Objets > Gestion des liens SD-WAN > Profil de qualité SaaS)
- Objets > Gestion des liens SD-WAN > Profil de distribution du trafic
- Objets > Gestion des liens SD-WAN > Profil de correction des erreurs

Objects > SD-WAN Link Management > Path Quality Profile (Objets > Gestion des liens SD-WAN > Profil de qualité des chemins d'accès)

SD-WAN vous permet de créer un profil de qualité de chemin d'accès pour chaque ensemble d'applications, les filtres d'applications, les groupes d'applications, les services, les objets de services et les objets de groupes de services qui ont des besoins de qualité de réseau uniques et de référencer le profil dans une règle de politique SD-WAN. Dans le profil, vous définissez le seuil maximum de trois paramètres : la latence, la gigue et la perte de paquets. Lorsqu'un lien SD-WAN dépasse un de ces seuils, le pare-feu sélectionne un meilleur chemin d'accès pour les paquets qui correspond à la règle SD-WAN où vous appliquez ce profil.

Un réglage de sensibilité pour chaque paramètre de qualité du chemin vous permet d'indiquer au pare-feu quel paramètre est plus important (préféré) pour la ou les applications auxquelles le profil s'applique. Le pare-feu accorde plus d'importance à un paramètre avec un réglage élevé plutôt qu'un paramètre avec un réglage moyen ou bas. Par exemple, certaines applications sont plus sensibles à la perte de paquets qu'à la gigue ou la latence, donc vous pouvez régler la sensibilité à la perte de paquets à « élevée » et le pare-feu examinera la perte de paquets en premier.

Si vous laissez les réglages de sensibilité de la latence, de la gigue et de la perte de paquets reste sur paramètre par défaut (moyen) ou si vous réglez les trois paramètres au même niveau de sensibilité, l'ordre de préférence du profil est comme suit : la perte de paquets, la latence et la gigue.

Par défaut, le pare-feu mesure la latence et la gigue toutes les 200 ms et fait une moyenne des trois dernières mesures pour évaluer la qualité du chemin sur une fenêtre glissante. Vous pouvez modifier ce comportement en sélectionnant une surveillance des chemins agressive ou souple lorsque vous configurez un profil d'interface SD-WAN.

	Réglages du profil de qualité du chemin d'accès
Name (Nom)	Saisissez un nom pour le profil de qualité du chemin d'accès à l'aide d'un maximum de 32 caractères alphanumériques, underscore, trait d'union, espace et point.
Partagé (Panorama uniquement)	Sélectionnez pour que le profil Qualité des chemins soit disponible pour tous les groupes de périphériques sur Panorama et sur chaque système

	Réglages du profil de qualité du chemin d’accès
	virtuel sur une plate-forme ou une branche multi-vsys sur laquelle vous appliquez la configuration.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez pour empêcher les administrateurs de remplacer les paramètres de ce profil de Qualité des chemins pour les groupes de périphériques qui héritent du profil. (Désactiver le contrôle prioritaire est indisponible si Partagé est sélectionné.)
Latence (ms)	**Threshold (Seuil)** - Saisissez le nombre de millisecondes autorisées pour qu’un paquet quitte le pare-feu, arrive à l’extrémité opposée du tunnel SD-WAN et qu'un paquet de réponse soit renvoyé au pare-feu avant que le seuil ne soit dépassé (la plage est comprise entre 10 et 2 000 ; par défaut : 100).
	Sensitivity (Sensibilité) - Sélectionnez **high (élevée)**, **medium (moyenne)** ou**low (faible)** (la valeur par défaut est **medium (moyenne)**.
Gigue (ms)	Threshold (seuil) : Saisissez le nombre de millisecondes (la fourchette va de 10 à 2 000 ; par défaut on a 100).
	Sensitivity (Sensibilité) - Sélectionnez **high (élevée)**, **medium (moyenne)** ou**low (faible)** (la valeur par défaut est **medium (moyenne)**.
Perte de paquets (%)	**Threshold (Seuil)** - Saisissez le pourcentage de perte de paquets sur le lien avant que le seuil ne soit dépassé (la plage est comprise entre 1 et 100 ; par défaut : 1).
	Sensitivity (Sensibilité) : le réglage de sensibilité pour la perte de paquets n’a aucun effet et vous pouvez garder le réglage par défaut (**medium (moyenne)**).

Objects > SD-WAN Link Management > SaaS Quality Profile (Objets > Gestion des liens SD-WAN > Profil de qualité SaaS)

SD-WAN vous permet de créer un profile de qualité Logiciel en tant que service (SaaS) pour mesurer la santé du chemin d’accès entre votre pare-feu de plate-forme ou branche et des applications SaaS du côté du serveur afin de surveiller avec précision la fiabilité de l’autoriser SaaS et de basculer les chemins d’accès si la qualité de santé des chemins d’accès se dégrade. Cela permet au pare-feu de déterminer avec précision quand basculer vers un lien d’Accès Internet Direct (DIA) différent.

Le profil de qualité SaaS vous permet d’indiquer l’application SaaS à surveiller en utilisant un algorithme d’apprentissage adaptatif qui surveille l’activité de l’application ou en indiquant l’application SaaS qui utilise l’adresse IP, le FQDN ou l’URL de l’application.

	Réglages du profil de qualité SaaS
Name (Nom)	Saisissez un nom pour le profil de qualité du chemin d'accès à l'aide de caractères alphanumériques, underscore, trait d'union, espace et point.
Partagé (Panorama uniquement)	Cochez (activez) pour que le profil de qualité SaaS soit partagé entre tous les groupes de périphériques.
Désactiver le contrôle prioritaire (Panorama uniquement)	Cochez (activez) pour désactiver la capacité à prendre le contrôle prioritaire des paramètres du profil de qualité SaaS en local sur le pare-feu géré.
Mode de surveillance SaaS	
Adaptatif	L'activité de la session de l'application SaaS est surveillée lors de l'envoi et de la réception de l'activité et le statut de la santé du chemin d'accès est dérivé automatiquement sans autres vérifications de la santé sur l'interface SD-WAN. Cette option est sélectionnée par défaut.
Adresse IP statique	**IP Address/Object (Adresse IP/objet)** : précise l'application SaaS à surveiller en utilisant l'adresse IP de l'application. • **Adresse IP** – L'adresse IP de l'application SaaS. • **Probe Interval (Sec) (Intervalle de sondage en sec)** : Indique, en secondes, l'intervalle pendant lequel le pare-feu sonde la santé de la qualité du chemin d'accès entre le pare-feu et l'application SaaS. La valeur par défaut est 3 secondes. Jusqu'à 4 adresses IP statiques sont prises en charge.
	FQDN : précise l'application Saas à surveiller en utilisant le Fully Qualified Domain Name (FQDN) de l'application. • **FQDN** : le FQDN de l'application SaaS. Vous devez configurer un address object (objet de l'adresse) du FQDN pour indiquer un FQDN. Le FQDN de l'application SaaS doit pouvoir être résolu afin de surveiller correctement l'application SaaS. • **Probe Interval (sec) (Intervalle de sondage en sec)** : Indique, en secondes, l'intervalle pendant lequel le pare-feu sonde la santé de la qualité du chemin d'accès entre le pare-feu de branche et l'application SaaS. La valeur par défaut est 3 secondes.
HTTP/HTTPS	Indiquez l'application SaaS à surveiller en utilisant l'URL HTTP ou HTTPS. • **Monitored URL (URL surveillée)** : l'URL HTTP ou HTTPS de l'application SaaS. • **Probe Interval (sec) (Intervalle de sondage en sec)** : Indique, en secondes, l'intervalle pendant lequel le pare-feu sonde la santé de la

	Réglages du profil de qualité SaaS
	qualité du chemin d'accès entre le pare-feu et l'application SaaS. La valeur par défaut est 3 secondes.

Objets > Gestion des liens SD-WAN > Profil de distribution du trafic

Pour ce profil de distribution du trafic, sélectionnez la méthode utilisée par le pare-feu pour distribuer les sessions et basculer vers un meilleur chemin lorsque la qualité du chemin se détériore. Ajoutez les étiquettes de liens que le pare-feu doit considérer lorsqu'il détermine le lien par lequel il transfère le trafic SD-WAN. Vous appliquez un profil de distribution du trafic à chaque règle de politique SD-WAN que vous créez.

	Profil de distribution du trafic
Name (Nom)	Saisissez un nom pour le profil de distribution du trafic en utilisant un maximum de 31 caractères composée de caractères alphanumériques, trait d'union, d'espace, trait de soulignement et point.
Partagé	Sélectionnez Partagé uniquement si vous souhaitez utiliser ce profil de Distribution du trafic pour tous les Groupes de périphériques (hubs et branches).
Best Available Path (Meilleur chemin disponible)	Si le coût n'est pas un facteur déterminant et les applications peuvent utiliser n'importe quel chemin d'accès sur la branche sélectionnez le Meilleur chemin disponible. Le pare-feu distribue le trafic et bascule sur un des liens appartenant aux Etiquettes de liens dans la liste basée sur les mesures de la qualité d'un chemin d'accès pour ainsi fournir la meilleure expérience de l'application aux utilisateurs.
Priorité descendante	Si vous avez des liens onéreux ou à faible capacité et vous souhaitez qu'ils soient utilisés uniquement en dernier ressort ou comme un lien de secours, utilisez la méthode de Priorité descendante et placez les étiquettes qui comprennent ces liens en dernier dans la liste des étiquettes de liens dans ce profil. Le pare-feu utilise la première étiquette de lien de la liste afin de déterminer les liens sur lesquels charger le trafic de la session et ceux sur lesquels basculer. Si aucun des liens de la première Etiquette de liens n'est qualifié, le pare-feu sélectionne un lien dans la deuxième Etiquette de liens dans la liste. Si aucun des liens de la deuxième étiquette de liens n'est validé, la procédure continue aussi longtemps que nécessaire jusqu'à ce que le pare-feu trouve un lien validé dans la dernière étiquette de liens. Si tous les liens associés sont surchargés et qu'aucun lien ne respecte les seuils de qualité, le pare-feu utilise la méthode du Meilleur chemin disponible pour sélectionner un lien vers lequel transférer le trafic. Si la gigue, la latence ou la perte de paquets de l'application dépasse son seuil configuré, le pare-feu commence en haut de la liste de priorité descendante des Etiquettes de liens pour trouver un lien sur lequel basculer.

	Profil de distribution du trafic
Distribution pondérée de sessions	Sélectionnez la méthode Distribution de session pondérée si vous souhaitez charger le trafic (qui correspond à la règle) manuellement vers votre ISP et vos liens WAN et que vous n'avez pas besoin de basculer lors de conditions de dégradation Vous indiquez manuellement la charge du lien lorsque vous appliquez un pourcentage statique de nouvelles sessions que les interfaces regroupées avec une seule étiquette obtiendront. Vous pouvez sélectionner cette méthode pour les applications qui ne sont pas sensibles à la latence et qui ont besoin d'une grande capacité de bande passante du lien, comme des sauvegardes importantes de branche et des transferts de gros fichiers. Souvenez-vous que si le lien subit une panne, le pare-feu ne transmet pas le trafic correspondant vers un lien différent.
Étiquettes de liens	Ajoutez les Étiquettes de liens que vous voulez que le pare-feu considère lors du processus de sélection du lien que vous avez choisi pour ce profil. L'ordre des étiquettes est importante si vous choisissez la méthode Priorité descendante ; vous pouvez cliquer sur Monter ou Descendre pour changer l'ordre des étiquettes.
Poids	Si vous choisissez la méthode de distribution pondérée de sessions, saisissez un pourcentage pour chaque Etiquette de liens que vous ajoutez. La somme des valeurs en pourcentage doit être égale à 100 %.

Objets > Gestion des liens SD-WAN > Profil de correction des erreurs

Si votre trafic SD-WAN inclut une application qui est sensible à la perte de paquets ou à la corruption, comme de l'audio, VoIP ou vidéo-conférence, vous pouvez appliquer soit la Forward Error Correction (FEC) ou la duplication de paquets en tant que moyen de correction de l'erreur. Avec FEC, le pare-feu récepteur (décodeur) peut récupérer des paquets perdus ou corrompus en utilisant des bits de parité que l'encodeur intègre dans un flux d'application. La duplication de paquet est une autre méthode de correction d'erreur dans laquelle une session d'application est dupliquée depuis un tunnel vers un second tunnel. Les deux méthodes nécessitent une bande passante supplémentaire et des ressources CPU ; par conséquent, appliquez la méthode FEC ou de duplication de paquet uniquement aux applications qui peuvent tirer parti de ces méthodes. Pour utiliser une de ces méthodes, créez un Profil de correction des erreurs et référencez-le dans une règle de politique SD-WAN pour des applications spécifiques.

(Vous devez aussi indiquer quelles interfaces sont disponibles pour la sélection par le pare-feu pour la correction des erreurs en indiquant dans un SD-WAN Interface Profile (profil d'interface SD-WAN) que les interfaces ont **Eligible for Error Correction Profile interface selection (éligibles à la sélection du profil de correction des erreurs)**.)

	Paramètres du profil de correction des erreurs
Name (Nom)	Ajoutez un nom descriptif du Profil de correction des erreurs en utilisant un maximum de 31 caractères alphanumériques.
Partagé	Sélectionnez pour que le Profil de correction des erreurs soit disponible pour tous les groupes de périphériques sur Panorama et sur chaque

	Paramètres du profil de correction des erreurs
	système virtuel sur une plate-forme ou une branche multi-vsys sur laquelle vous appliquez la configuration.
Désactiver le contrôle prioritaire	Sélectionnez pour empêcher les administrateurs de remplacer les paramètres de ce profil de correction des erreurs pour les groupes de périphériques qui héritent du profil. (**Disable override (Désactiver le contrôle prioritaire)** est indisponible si **Shared (Partagé)** est sélectionné.)
Seuil d'activation (% de perte de paquet)	Lorsque la perte de paquet dépasse ce pourcentage, la méthode FEC ou de duplication de paquet est activée pour les applications configurés dans la règle de politique SD-WAN où le Profil de correction des erreurs s'applique. La plage est comprise entre 1 et 99 ; la valeur par défaut est 2.
Transfert de correction des erreurs / Duplication de paquet	Sélectionnez s'il faut utiliser le transfert de correction des erreurs (FEC) ou la duplication de paquet. La duplication de paquet nécessite encore plus de ressources que la méthode FEC.
Ration de correction de la perte de paquet	(Transfert de correction des erreurs uniquement o) Ration de bits de parité par rapport aux paquets de données. Plus le ratio de bits de parité par rapport aux paquets de données que l'encodeur envoie au décodeur est élevé, plus la probabilité que le décodeur puisse réparer la perte de paquet est élevée. Cependant, un ratio plus élevé nécessite plus de redondance et par conséquent plus de ressources en bande passante, ce qui est un compromis permettant la correction des erreurs. Sélectionnez un des ratios prédéfinis : • **10 % (20:2)** (par défaut) • **20 % (20:4)** • **30 % (20:6)** • **40 % (20:8)** • **50 % (20:10)** Le ratio de parité s'applique à l'encodage du trafic sortant du pare-feu. Par exemple, si le ratio de parité de la plate-forme est de 50 % et que le ratio de parité de la branche est de 20 %, la plate-forme recevra un ratio de 20 % et la branche recevra un ration de 50 %.
Durée de récupération (en ms)	Nombre maximum de millisecondes que le pare-feu récepteur (décodeur) peut passer pour effectuer la récupération de paquets de données perdus en utilisant les paquets de parité qu'il a reçus ; plage de 1 à 5 000 ; valeur par défaut de 1 000. Le pare-feu envoie immédiatement les paquets de données qu'il reçoit vers la destination. Au cours de la durée de récupération pour un bloc de données, le pare-feu procède à une récupération de paquets pour tous

	Paramètres du profil de correction des erreurs
	les paquets de données perdus. Lorsque la durée de récupération expire, les bits de parité associés pour ce bloc sont éliminés. L’encodeur envoie la valeur de Durée de récupération au décodeur ; le paramètre de Durée de récupération sur le décodeur n’a aucun impact.

Objets > Calendriers

Par défaut, les règles des politiques de sécurité sont en vigueur en tout temps (toutes les dates et heures). Pour limiter l'application d'une règle de politique de sécurité à des horaires spécifiques, vous pouvez définir des calendriers puis les appliquer aux politiques concernées. Pour chaque calendrier, vous pouvez définir une date et une plage horaire fixes ou récurrentes. Pour appliquer des calendriers à des politiques de sécurité, reportez-vous à la section Politiques > Sécurité.

Lorsqu'une règle de politique de sécurité est invoquée par un calendrier défini, seules les nouvelles sessions sont affectées par la règle de politique de sécurité appliquée. Les sessions existantes ne sont pas affectées par la politique planifiée.

Paramètres des calendriers	Description
Name (Nom)	Saisissez un nom pour le calendrier (31 caractères maximum). Ce nom apparaît dans la liste de calendriers lors de la définition de politiques de sécurité. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Partagé (Panorama uniquement)	Sélectionnez cette option si vous souhaitez que le calendrier soit disponible pour : • Chaque système virtuel (vsys) sur un pare-feu en mode multi-vsys. Si vous désélectionnez cette option, le calendrier sera uniquement disponible pour le **Virtual System (Système virtuel)** sélectionné dans l'onglet **Objects (Objets)**. • Chaque groupe de périphériques sur Panorama. Si vous désélectionnez cette option, le calendrier sera uniquement disponible pour le **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Sélectionnez cette option pour empêcher les administrateurs de remplacer les paramètres de cette planification dans les groupes de périphériques qui héritent de la planification. Cette sélection est effacée par défaut, ce qui signifie que les administrateurs peuvent remplacer les paramètres pour tout groupe de périphériques qui hérite de la planification.
Récurrence	Sélectionnez le type de calendrier (**Quotidien**, **Hebdomadaire** ou **Non récurrent**).
Quotidien	Cliquez sur **Ajouter** et renseignez une **Heure de début** et une **Heure de fin** au format 24 heures (HH:MM).
Hebdomadaire	Cliquez sur **Ajouter**, sélectionnez un **Jour de la semaine**, et précisez une **Heure de début** et une **Heure de fin** au format 24 heures (HH:MM).

Paramètres des calendriers	Description
Non récurrent	Cliquez sur **Ajouter** et indiquez une **Date de début**, une **Heure de début**, une **Date de fin** et une **Heure de fin**.

Réseau

Les rubriques suivantes décrivent les paramètres réseau du pare-feu.

- Réseau > Interfaces
- Réseau > Zones
- Réseau > VLAN
- Réseau > Câbles virtuels
- Réseau > Routeurs virtuels
- Réseau > Routage > Routeurs logiques
- Réseau > Tunnels'A0;IPSec
- Réseau > Tunnels GRE
- Réseau > DHCP
- Réseau > Proxy DNS
- Réseau > Proxy
- Réseau > QoS
- Réseau > LLDP
- Réseau > Profils réseau

Vous souhaitez en savoir plus ?

Le PAN-OS Networking Administrator’s Guide (Guide de l'administrateur réseau PAN-OS) fournit des informations sur vos interfaces réseau, la prise en charge de plusieurs routeurs virtuels, les routes statiques, les protocoles de routage dynamique et d'autres fonctionnalités majeures qui prennent en charge la mise en réseau sur le pare-feu.

Réseau > Interfaces

Les interfaces de pare-feu (ports) permettent à un pare-feu de se connecter à d'autres périphériques réseau, ainsi qu'à d'autres interfaces du pare-feu. Les rubriques suivantes expliquent les types d'interfaces et comment les configurer :

Que voulez-vous faire ?	Reportez-vous à la section
Quelles sont les interfaces de pare-feu ?	Présentation des interfaces de pare-feu
Je ne connais pas les interfaces de pare-feu ; quels sont les composants d'une interface de pare-feu ?	Composants communs des interfaces de pare-feu Composants communs des interfaces de pare-feu PA-7000 Series
Je connais déjà les interfaces de pare-feu ; comment puis-je trouver des informations sur la configuration d'un type d'interface spécifique ?	**Interfaces physiques (Ethernet)** Interface Tap Interface HA Interface du câble virtuel Sous-interface de câble virtuel Interface de niveau 2 de la série PA-7000 Sous-interface de niveau 2 de la série PA-7000 Interface de niveau 3 de la série PA-7000 Interface de niveau 3 Sous-interface de couche 3 Interface de la carte de journal Sous-interface de la carte de journal Interface miroir de décryptage Groupe d’interfaces Ethernet agrégées (AE) Interfaces Ethernet agrégées (AE) **Interfaces logiques** Réseau > Interfaces > VLAN Réseau > Interfaces > En boucle Réseau > Interfaces > De tunnel Réseau > Interfaces > SD-WAN Réseau > Interfaces > PoE

Que voulez-vous faire ?	Reportez-vous à la section
Vous souhaitez en savoir plus ?	Mise en réseau

Présentation des interfaces de pare-feu

Les configurations d'interface des ports de données du pare-feu permettent au trafic d'entrer et de sortir du pare-feu. Un pare-feu Palo Alto Networks® peut fonctionner simultanément dans plusieurs déploiements, car vous pouvez configurer les interfacespour prendre en charge différents déploiements. Par exemple, vous pouvez configurer les interfaces Ethernet d'un pare-feu pour le câble virtuel, le niveau 2, le niveau 3 et le mode Tap. Les interfaces prises en charge par le pare-feu sont les suivantes :

- **Interfaces physiques** – Le pare-feu prend en charge deux types de supports (cuivre et fibre optique) qui peuvent envoyer et recevoir du trafic à différents taux de transmission. Vous pouvez configurer des interfaces Ethernet selon les types suivants : Tap, HA (haute disponibilité, carte de journal (interface et sous-interface), miroir de déchiffrement, câble virtuel (interface et sous-interface), couche 2 (interface et sous-interface), couche 3 (interface et sous-interface) et Ethernet agrégée. Les types d'interfaces disponibles et les taux de transmission varient selon le modèle matériel.
- **Interfaces logiques** - Ce sont notamment les interfaces de réseau local virtuel (VLAN), les interfaces en boucle, les interfaces de tunnel et les interface SD-WAN. Vous devez configurer l'interface physique avant de définir une interface VLAN, une interface SD-WAN ou une interface de tunnel.

Composants communs des interfaces de pare-feu

Sélectionnez **Réseau** > **Interfaces** pour afficher et configurer les composants qui sont communs à la plupart des types d'interfaces.

Pour obtenir la description des composants uniques ou différents lors de la configuration d'interfaces sur un pare-feu de la série PA-7000 ou lors de l'utilisation de Panorama™ pour configurer des interfaces sur un pare-feu, reportez-vous à la section Composants communs des interfaces de pare-feu PA-7000 Series.

Étapes de Configuration de l'interface de pare-feu	Description
Interface (nom de l'interface)	Le nom de l'interface est prédéfini et vous ne pouvez pas le modifier. Vous pouvez toutefois ajouter un suffixe numérique aux sous-interfaces, interfaces agrégées, interfaces VLAN, interfaces en boucle, interfaces de tunnel et interfaces SD-WAN.
Type d'interface	Pour les interfaces Ethernet (**Réseau** > **Interfaces** > **Ethernet**), vous pouvez sélectionner le type d'interface : • **Tap** • **HA**

Étapes de Configuration de l’interface de pare-feu	Description
	• **Decrypt Mirror (Miroir de déchiffrement)** (Pris en charge sur tous les pare-feu, à l’exception des pare-feu pare-feu VM-Series Édition NSX, Citrix SDX, AWS et Azure.) • **Virtual Wire** • **Couche 2** • **Couche 3** • **Carte de journal** (pare-feu de la série PA-7000 uniquement) ; • **Ethernet agrégé**
Profil de gestion	Sélectionnez un **Profil de gestion** (**Réseau** > **Interfaces** > **<if-config** > **Avancé** > **Autres informations**) qui définit les protocoles (par exemple, SSH, Telnet et HTTP) à utiliser pour gérer le pare-feu dans cette interface.
état des liaisons	Pour les interfaces Ethernet, l'état des liaisons indique si l'interface est actuellement accessible et peut recevoir du trafic sur le réseau : • **Vert** - configurée et active • **Rouge** - Configurée, mais inactive ou désactivée • **Gris** - non configurée Pointez l'état des liaisons pour afficher une infobulle qui indique les paramètres duplex et de vitesse de liaison de l'interface.
Adresse IP	(Facultatif) Configurez l'adresse IPv4 ou IPv6 de l'interface Ethernet, VLAN ou de tunnel. Pour une adresse IPv4, vous pouvez également sélectionner le mode d'adressage (**Type**) de l'interface : **Statique**, **client DHCP** ou **PPPoE**.
routeur virtuel - VR	Affectez un routeur virtuel à l’interface ou cliquez sur **Routeur virtuel** pour en définir un nouveau (voir Réseau > Routeurs virtuels). Sélectionnez **Aucun** pour supprimer l'affectation de routeur virtuel de l'interface.
Étiquette (sous-interface uniquement)	Saisissez l'étiquette VLAN (1-4 094) de la sous-interface.
Réseau local virtuel	Vous devez sélectionner **Réseau** > **Interfaces** > **VLAN**, puis modifier un **VLAN** existant ou **Ajouter** un nouveau (reportez-vous à la section Réseau > VLANs). Sélectionnez **Aucun** pour supprimer l'affectation de VLAN de l'interface. Pour activer le basculement entre les interfaces de couche 2 ou pour activer le routage via une interface VLAN, vous devez configurer un objet VLAN.
système virtuel - vsys	Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système virtuel (vsys) pour

Étapes de Configuration de l’interface de pare-feu	Description
	l'interface ou cliquez sur le lien **Virtual System (Système virtuel)** pour en définir un nouveau.
Zone de sécurité	Sélectionnez une **Zone de sécurité** (**Network** > **Interfaces** > **<if config** > **Configuration**)pour l'interface ou sélectionnez **Zone** pour en définir une nouvelle. Sélectionnez **Aucune** pour supprimer l'affectation de zone de l'interface.
Caractéristiques	Pour les interfaces Ethernet, cette colonne indique si les fonctions suivantes sont activées :  Client DHCP  Proxy DNS  Passerelle GlobalProtect™ activée  LACP (protocole d'agrégation de liaisons)  LLDP (protocole de découverte de couche liaison)  Surveillance NDP  Profil NetFlow  Profil de qualité de service (QoS)  SD-WAN
Commentaire	Une description de la fonction de l'interface.

Composants communs des interfaces de pare-feu PA-7000 Series

Le tableau suivant décrit les composants de la page **Réseau** > **Interfaces** > **Ethernet** qui sont uniques ou différents lors de la configuration d’interfaces sur un pare-feu de la série PA-7000 ou lors de l’utilisation de Panorama pour configurer des interfaces sur n’importe quel pare-feu. Cliquez sur **Ajouter une**

interface pour créer une nouvelle interface ou sélectionnez une interface existante (Ethernet1/1, par exemple) pour la modifier.

Sur les pare-feu de la série PA-7000, vous devez configurer une Interface de la carte des journaux *sur un seul port de données.*

Étapes de Configuration de l'interface de pare-feu de la série PA-7000	Description
Logement	Sélectionnez le numéro de logement (1-12) de l'interface. Seuls les pare-feu PA-7000 Series disposent de plusieurs logements. Si vous utilisez Panorama pour configurer une interface pour n'importe quel autre modèle de pare-feu, sélectionnez le **Logement 1**.
nom de l'interface	Choisissez le nom d'une interface associée au **logement** sélectionné.

Interface Tap

- Réseau > Interfaces > Ethernet

Vous pouvez utiliser une interface Tap pour surveiller le trafic sur un port.

Pour configurer une interface Tap, cliquez sur le nom d'une interface (Ethernet1/1, par exemple) non configurée et indiquez les informations suivantes :

Paramètres d'une interface Tap	Configuré dans	Description
Nom de l'interface	**Interface Ethernet**	Le nom de l'interface est prédéfini et vous ne pouvez pas le modifier.
Commentaire		Saisissez une description de l'interface (facultatif).
Type d'interface		Sélectionnez **Tap**.
profil NetFlow ;		Si vous souhaitez exporter le trafic IP unidirectionnel traversant une interface d'entrée vers un serveur NetFlow, sélectionnez le profil de serveur ou cliquez sur **Netflow Profile (Profil NetFlow)** pour en définir un nouveau (reportez-vous à la section Périphérique > Profils de serveur > NetFlow). Sélectionnez **None (Aucun)** pour supprimer l'affectation de serveur NetFlow de l'interface.
Système virtuel	**Interface Ethernet** > **Configuration**	Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système

Paramètres d'une interface Tap	Configuré dans	Description
		virtuel pour l'interface ou cliquez sur **Virtual System (Système virtuel)** pour en définir un nouveau.
Zone de sécurité		Sélectionnez une zone de sécurité pour l'interface ou cliquez sur **Zone** pour en définir une nouvelle. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de l'interface.
Vitesse de liaison	**Interface Ethernet** > **Avancé** > **Paramètres de lien**	Sélectionnez la vitesse de l'interface en Mbits/s ou sélectionnez **auto** pour que le pare-feu détermine automatiquement la vitesse.
Mode duplex de la liaison		Indiquez si le mode de transmission de l'interface est en duplex intégral (**full (intégral)**), semi-duplex (**half (semi)**) ou automatiquement négocié (**auto**).
état des liaisons		Indiquez si l'état de l'interface est activé (**up (actif)**), désactivé **down (inactif)**) ou automatiquement déterminé (**auto**).
Alimentation Rsvd PoE	**Interface Ethernet** > **Avancé** > **Paramètres PoE** (Supported firewalls only (Pare-feu pris en charge uniquement))	Sélectionnez la quantité de puissance allouée en Watts si PoE est activé.
PoE activé		Sélectionnez pour activer PoE sur cette interface.

Interface HD

- Réseau > Interfaces > Ethernet

Chaque interface haute disponibilité (HA) a une fonction spécifique : une interface sert à synchroniser la configuration et les pulsations, et l'autre sert à synchroniser l'état. Si la HA active/active est activée, le pare-feu peut utiliser une interface HA tierce pour transférer les paquets.

Certains pare-feu Palo Alto Networks contiennent des ports physiques dédiés à l'utilisation dans des déploiements HA (l'un pour la liaison de contrôle et l'autre pour la liaison de données). Pour les pare-feu n'incluant pas de ports dédiés, vous devez définir des ports de données qui vont être utilisés pour la HA. Pour plus d'informations sur HA, reportez-vous à « Périphérique > Systèmes virtuels ».

Pour configurer une interface HA, cliquez sur le nom d'une interface (Ethernet1/1, par exemple) non configurée et indiquez les informations suivantes :

Paramètres d'une interface HA	Configuré dans	Description
Nom de l'interface	**Interface Ethernet**	Le nom de l'interface est prédéfini et vous ne pouvez pas le modifier.
Commentaire		Saisissez une description de l'interface (facultatif).
Type d'interface		Sélectionnez **HA**.
Vitesse de liaison	**Interface Ethernet** > **Avancé** > **Paramètres du lien**	Sélectionnez la vitesse de l'interface en Mbits/s ou sélectionnez **auto** pour que le pare-feu détermine automatiquement la vitesse.
Mode duplex de la liaison		Indiquez si le mode de transmission de l'interface est en duplex intégral (**full (intégral)**), semi-duplex (**half (semi)**) ou automatiquement négocié (**auto**).
état des liaisons		Indiquez si l'état de l'interface est activé (**up (actif)**), désactivé **down (inactif)**) ou automatiquement déterminé (**auto**).
PoE Rsvd Pwr	**Interface Ethernet** > **Avancé** > **Paramètres PoE** (Supported firewalls only (Pare-feu pris en charge uniquement))	Sélectionnez la quantité de puissance allouée en Watts si PoE est activé.
PoE activé		Sélectionnez pour activer PoE sur cette interface.

Interface du câble virtuel

- Réseau > Interfaces > Ethernet

Un câble virtuel relie logiquement deux interfaces Ethernet, ce qui permet d'autoriser la circulation de l'ensemble du trafic entre les interfaces ou uniquement le trafic doté des étiquettes VLAN sélectionnées (aucun autre service de basculement ou de routage n'est disponible). Vous pouvez créer des sous-interfaces de câble virtuel pour classer le trafic en fonction d'une adresse IP, d'une plage d'adresses IP ou d'un sous-réseau. Un câble virtuel n'exige aucune modification des périphériques réseau adjacents. Un câble virtuel peut relier deux interfaces Ethernet de matériel analogue (deux interfaces en cuivre ou deux interfaces en fibre optique), ou relier une interface en cuivre à une interface en fibre optique.

Pour établir un câble virtuel, vous devez décider quelles sont les deux interfaces à relier(**Network (Réseau)** > **Interfaces** > **Ethernet**) et configurer leurs paramètres comme le décrit la table suivante.

Si vous utilisez une interface existante pour le câble virtuel, retirez d'abord l'interface de n'importe quelle zone de sécurité associée.

Paramètre d'une Interface de câble virtuel	Configuré dans	Description
Nom de l'interface	**Interface Ethernet**	Le nom de l'interface est prédéfini et vous ne pouvez pas le modifier.
Commentaire		Saisissez une description de l'interface (facultatif).
Type d'interface		Sélectionnez **Virtual Wire (Câble virtuel)**.
Virtual Wire	**Interface Ethernet** > **Configuration**	Sélectionnez un câble virtuel ou cliquez sur **Virtual Wire (Câble virtuel)** pour en définir un nouveau (Réseau > Câbles virtuels). Sélectionnez **None (Aucun)** pour supprimer l'affectation de câble virtuel de l'interface.
Virtual System (système virtuel - vsys)		Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système virtuel pour l'interface ou cliquez sur **Virtual System (Système virtuel)** pour en définir un nouveau.
Zone de sécurité		Sélectionnez une zone de sécurité pour l'interface ou cliquez sur **Zone** pour en définir une nouvelle. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de l'interface.
Vitesse de liaison	**Interface Ethernet** > **Avancé** > **Paramètres de lien**	Sélectionnez la vitesse de l'interface en Mbits/s ou sélectionnez **auto** pour que le pare-feu détermine automatiquement la vitesse.
Mode duplex de la liaison		Indiquez si le mode de transmission de l'interface est en duplex intégral (**full (intégral)**), semi-duplex (**half (semi)**) ou automatiquement négocié (**auto**). Les deux interfaces du câble virtuel doivent avoir le même mode de transmission.
état des liaisons		Indiquez si l'état de l'interface est activé (**up (actif)**), désactivé **down (inactif)**) ou automatiquement déterminé (**auto**).
PoE Rsvd Pwr	**Interface Ethernet** > **Avancé** > **Paramètres PoE** (Supported firewalls only (Pare-feu pris	Sélectionnez la quantité de puissance allouée en Watts si PoE est activé.
PoE activé		Sélectionnez pour activer PoE sur cette interface.

Paramètre d'une Interface de câble virtuel	Configuré dans	Description
	en charge uniquement))	
Activer LLDP	**Interface Ethernet** > **Avancé** > **LLDP**	Sélectionnez cette option pour activer LLDP (Link Layer Discovery Protocol/protocole de découverte de couche liaison) sur l'interface. LLDP fonctionne sur la couche de liaison pour détecter les périphériques voisins et leurs fonctionnalités.
Profil		Si LLDP est activé, sélectionnez un profil LLDP à affecter à l'interface ou cliquez sur **LLDP Profile (Profil LLDP)** pour créer un nouveau profil (reportez-vous à la section Réseau > Profils réseau > Profil LLDP). Sélectionnez **None (Aucun)** pour configurer le pare-feu de sorte qu'il utilise les paramètres généraux par défaut.
Activation à l'état HA passif		Si LLDP est activé, sélectionnez pour configurer un pare-feu HA passif pour qu'il pré-négocie LLDP avec son homologue avant que le pare-feu devienne actif. Si LLDP n'est pas activé, sélectionnez pour configurer un pare-feu HA passif pour qu'il ne fasse que passer les paquets LLDP à travers du pare-feu.

Sous-interface de câble virtuel

- Réseau > Interfaces > Ethernet

Les sous-interfaces de câble virtuel vous permettent de séparer le trafic par étiquette VLAN ou une combinaison d'étiquette VLAN et de classificateur d'adresses IP, d'affecter le trafic étiqueté à une zone et à un système virtuel différents, puis d'appliquer les politiques de sécurité relatives au trafic correspondant aux critères définis.

Pour ajouter un Interface du câble virtuel, sélectionnez la ligne pour cette interface, cliquez sur **Add Subinterface (Ajouter une sous-interface)** et spécifiez les informations suivantes.

Paramètres d'une sous-interface de câble virtuel	Description
Nom de l'interface	**Interface Name (Nom de l'interface)** en lecture seule affiche le nom de l'interface de câble virtuel sélectionnée. Dans le champ adjacent, saisissez un suffixe numérique (1-9 999) pour identifier la sous-interface.
Commentaire	Saisissez une description de la sous-interface (facultatif).

Paramètres d’une sous-interface de câble virtuel	Description
Étiquette	Saisissez le l’étiquette) VLAN (0-4 094) de la sous-interface.
profil NetFlow ;	Si vous souhaitez exporter le trafic IP unidirectionnel traversant une sous-interface d'entrée vers un serveur NetFlow, sélectionnez le profil de serveur ou cliquez sur **Netflow Profile (Profil NetFlow)** pour en définir un nouveau (reportez-vous à la section Périphérique > Profils de serveur > NetFlow). SélectionnezNone (Aucun) pour supprimer l'affectation de serveur NetFlow de la sous-interface.
Classificateur IP	Cliquez sur **Add (Ajouter)** et saisissez une adresse IP, une plage d'adresses IP ou un sous-réseau pour classer le trafic sur cette sous-interface de câble virtuel.
Virtual Wire	Sélectionnez un câble virtuel ou cliquez sur **Virtual Wire (Câble virtuel)** pour en définir un nouveau (reportez-vous à la section Réseau > Câbles virtuels). Sélectionnez **None (Aucun)** pour supprimer l'affectation de câble virtuel de la sous-interface.
Virtual System (système virtuel - vsys)	Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système virtuel pour la sous-interface ou cliquez sur **Virtual System (Système virtuel)** pour en définir un nouveau.
Zone de sécurité	Sélectionnez une zone de sécurité pour la sous-interface ou cliquez sur **Zone** pour en définir une nouvelle. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de la sous-interface.

Interface de niveau 2 de la série PA-7000

- Réseau > Interfaces > Ethernet

Sélectionnez **Network (Réseau)** > **Interfaces** > **Ethernet** pour configurer une interface de couche 2. Cliquez sur le nom d'une interface (Ethernet1/1, par exemple) non configurée et indiquez les informations suivantes.

Paramètres d’une interface de niveau 2	Configuré dans	Description
Nom de l'interface	**Interface Ethernet**	Le nom de l'interface est prédéfini et vous ne pouvez pas le modifier.
Commentaire		Saisissez une description de l'interface (facultatif).

Paramètres d’une interface de niveau 2	Configuré dans	Description
Type d'interface		Sélectionnez **Layer2 (IPv6)**.
profil NetFlow ;		Si vous voulez exporter le trafic IP unidirectionnel traversant une interface d’entrée vers un serveur NetFlow, sélectionnez le profil de serveur ou cliquez sur **Netflow Profile (Profil Netflow)** pour définir un nouveau profil (Voir Périphérique > Profils de serveur > NetFlow). Sélectionnez **None (Aucun)** pour supprimer l'affectation de serveur NetFlow de l'interface.
Réseau local virtuel	**Interface Ethernet** > **Configuration**	Pour activer le basculement entre des interfaces de niveau 2 ou pour activer le routage via une interface VLAN, sélectionnez un VLAN existant ou cliquez sur **VLAN** pour définir un nouveau VLAN (reportez-vous à la section Réseau > VLAN). Sélectionnez **None (Aucun)** pour supprimer l'affectation de VLAN de l'interface.
Virtual System (système virtuel - vsys)		Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système virtuel pour l'interface ou cliquez sur **Virtual System (Système virtuel)** pour en définir un nouveau.
Zone de sécurité		Sélectionnez une **Security Zone (Zone de sécurité)** pour l'interface ou cliquez sur **Zone** pour en définir une nouvelle. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de l'interface.
Vitesse de liaison	**Interface Ethernet** > **Avancé**	Sélectionnez la vitesse de l'interface en Mbits/s ou sélectionnez **auto** pour que le pare-feu détermine automatiquement la vitesse.
Mode duplex de la liaison		Indiquez si le mode de transmission de l'interface est en duplex intégral (**full (intégral)**), semi-duplex (**half (semi)**) ou automatiquement négocié (**auto**).
état des liaisons		Indiquez si l'état de l'interface est activé (**up (actif)**), désactivé **down (inactif)**) ou automatiquement déterminé (**auto**).
Activer LLDP	**Interface Ethernet** > **Avancé** > **LLDP**	Sélectionnez cette option pour activer LLDP (Link Layer Discovery Protocol/protocole de découverte de couche liaison) sur l'interface. LLDP fonctionne sur la couche de liaison pour détecter les périphériques voisins et leurs fonctionnalités.
LLDP Profile (profil LLDP)		Si LLDP est activé, sélectionnez un profil LLDP à affecter à l’interface ou cliquez sur **LLDP Profile (Profil LLDP)** pour créer un nouveau profil (reportez-vous à la section Réseau > Profils réseau > Profil LLDP). Sélectionnez **None (Aucun)** pour

Paramètres d’une interface de niveau 2	Configuré dans	Description
		configurer le pare-feu de sorte qu'il utilise les paramètres généraux par défaut.
Activation à l'état HA passif		Si LLDP est activé, sélectionnez cette option pour permettre à un pare-feu HA passif de pré-négocier LLDP avec son homologue avant que le pare-feu ne devienne actif.

Sous-interface de niveau 2 de la série PA-7000

- Réseau > Interfaces > Ethernet

Pour chaque port Ethernet configuré en tant qu'interface physique de couche 2, vous pouvez définir une interface de couche 2 logique supplémentaire (sous-interface) pour chaque étiquette VLAN assignée au trafic reçu par le port. Pour activer le basculement entre les sous-interfaces de couche 2, assignez-leur le même objet VLAN.

Pour configurer une Interface de niveau 2 de la série PA-7000, sélectionnez la ligne de cette interface physique, puis cliquez sur **Ajouter une sous-interface** et indiquez les informations suivantes.

Paramètres d’une sous-interface de couche 2	Description
Nom de l'interface	Le Nom de l'interface en lecture seule affiche le nom de l'interface physique sélectionnée. Dans le champ adjacent, saisissez un suffixe numérique (1-9 999) pour identifier la sous-interface.
Commentaire	Saisissez une description de la sous-interface (facultatif).
Étiquette	Saisissez l'étiquette VLAN (1-4 094) de la sous-interface.
profil NetFlow ;	Si vous souhaitez exporter le trafic IP unidirectionnel traversant une sous-interface d’entrée vers un serveur NetFlow, sélectionnez le profil de serveur ou cliquez sur **Profil NetFlow** pour définir un nouveau profil (voir Périphérique > Profils de serveur > NetFlow). Sélectionnez **None (Aucun)** pour supprimer l'affectation de serveur NetFlow de la sous-interface.
Réseau local virtuel	Pour activer le basculement entre des interfaces de niveau 2 ou pour activer le routage via une interface VLAN, sélectionnez un VLAN ou cliquez sur **VLAN** pour définir un nouveau VLAN (reportez-vous à la section Réseau > VLAN). Sélectionnez **None (Aucun)** pour supprimer l'affectation de VLAN de la sous-interface.

Paramètres d’une sous-interface de couche 2	Description
Virtual System (système virtuel - vsys)	Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système virtuel pour la sous-interface ou cliquez sur **Virtual System (Système virtuel)** pour en définir un nouveau.
Zone de sécurité	Sélectionnez une zone de sécurité pour la sous-interface ou cliquez sur **Zone** pour en définir une nouvelle. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de la sous-interface.

Interface de niveau 3 de la série PA-7000

- Réseau > Interfaces > Ethernet

Pour configurer une interface de niveau 3, sélectionnez une interface (Ethernet1/1, par exemple) et indiquez les informations suivantes.

Paramètres d’une interface de couche 3	Configuré dans	Description
Nom de l'interface	**Interface Ethernet**	Le nom de l'interface est prédéfini et vous ne pouvez pas le modifier.
Commentaire		Saisissez une description de l'interface (facultatif).
Type d'interface		Sélectionnez **Layer3 (Couche 3)**.
profil NetFlow ;		Si vous voulez exporter le trafic IP unidirectionnel traversant une interface d’entrée vers un serveur NetFlow, sélectionnez le profil de serveur ou cliquez sur **Netflow Profile (Profil Netflow)** pour définir un nouveau profil (Voir Périphérique > Profils de serveur > NetFlow). Sélectionnez **None (Aucun)** pour supprimer l'affectation de serveur NetFlow de l'interface.
routeur virtuel - VR	**Interface Ethernet** > **Configuration**	Sélectionnez un routeur virtuel ou cliquez sur **Virtual Router (Routeur virtuel)** pour en définir un nouveau (reportez-vous à la section Réseau > Routeurs virtuels). Sélectionnez **None (Aucun)** pour supprimer l'affectation de routeur virtuel de l'interface.
Virtual System (système virtuel - vsys)		Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système

Paramètres d'une interface de couche 3	Configuré dans	Description
		virtuel (vsys) pour l'interface ou cliquez sur le lien **Virtual System (Système virtuel)** pour en définir un nouveau.
Zone de sécurité		Sélectionnez une zone de sécurité pour l'interface ou cliquez sur **Zone** pour en définir une nouvelle. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de l'interface.
Activer SD-WAN	**Interface Ethernet** > **IPv4**	Sélectionnez **Enable SD-WAN (Activer SD-WAN)** pour activer la fonctionnalité SD-WAN de l'interface Ethernet.
Type		Sélectionnez la méthode d'affectation d'un type d'adresse IPv4 à l'interface : • **Static (Statique)** - Vous devez indiquer manuellement l'adresse IP. • **PPPoE** - Le pare-feu utilisera l'interface pour le protocole PPPoE (Point-to-Point Protocol over Ethernet/protocole point à point sur Ethernet). • **DHCP Client (Client DHCP)** - Permet à l'interface d'agir en tant que client DHCP (Dynamic Host Configuration Protocol/protocole d'attribution dynamique des adresses) et de recevoir une adresse IP assignée de façon dynamique. *Les pare-feu en mode haute disponibilité (HA) active/active ne prennent pas en charge PPPoE ni le client DHCP.* Les options affichées dans l'onglet varient selon le choix de la méthode de sélection d'adresse IP.
Type d'adresse IPv4 = **Static (Statique)**		
Adresse IP	**Interface Ethernet** > **IPv4**	Cliquez sur **Add (Ajouter)**, puis suivez l'une des étapes ci-dessous pour indiquer l'adresse IP statique et le masque réseau de l'interface. • Saisissez l'entrée en notation CIDR (Classing Inter-Domain Routing, routage inter-domaine sans classes) : *adresse_ip/masque* (par exemple, 192.168.2.0/24). • Sélectionnez un objet d'adresse existant de type **IP netmask (Masque réseau IP)**. • Cliquez sur **Address (Adresse)** pour créer un objet d'adresse de type **netmask (Masque réseau IP)**.

Paramètres d'une interface de couche 3	Configuré dans	Description
		Vous pouvez saisir plusieurs adresses IP pour l'interface. La base d'informations de transfert (FIB) utilisée par votre pare-feu détermine le nombre maximum d'adresses IP. Pour supprimer une adresse IP, sélectionnez-la et cliquez sur **Delete (Supprimer)**.
Type d'adresse IPV4 = **PPPoE**		
Activer	**Interface Ethernet** > **IPv4** > **PPPoE** > **Général**	Sélectionnez cette option pour activer l'interface de la terminaison PPPoE.
Username (Nom d'utilisateur)		Saisissez le nom d'utilisateur pour la connexion de point à point.
Mot de passe/ Confirmer le mot de passe		Saisissez, puis confirmez le mot de passe du nom d'utilisateur.
Afficher les informations d'exécution du client PPPoE		(Facultatif) Une fenêtre de dialogue s'ouvre pour afficher les paramètres que le pare-feu a négociés avec le fournisseur de services Internet pour établir une connexion. Les informations affichées dépendent du fournisseur de services Internet.
Authentification	**Interface Ethernet** > **IPv4** > **PPPoE** > **Avancé**	Sélectionnez le protocole d'authentification des communications PPPoE : **CHAP** (Challenge-Handshake Authentication Protocol/protocole d'authentification par défi-réponse), **PAP** (Password Authentication Protocol/ protocole d'authentification de mot de passe) ou la valeur **Auto (Automatique)** par défaut (le pare-feu détermine le protocole). Sélectionnez **None (Aucun)** pour supprimer l'affectation de protocole de l'interface.
Adresse statique		Suivez l'une des étapes ci-dessous pour indiquer l'adresse IP assignée par le fournisseur de services Internet (aucune valeur par défaut) : • Saisissez l'entrée en notation CIDR (Classing Inter-Domain Routing, routage inter-domaine sans classes) : *adresse_ip/masque* (par exemple, 192.168.2.0/24). • Sélectionnez un objet d'adresse existant de type **IP netmask (Masque réseau IP)**. • Cliquez sur **Address (Adresse)** pour créer un objet d'adresse de type **netmask (Masque réseau IP)**.

Paramètres d'une interface de couche 3	Configuré dans	Description
		• Sélectionnez **None (Aucune)** pour supprimer l'affectation d'adresse de l'interface.
Créer automatiquement un itinéraire par défaut en direction de l'homologue		Sélectionnez cette option pour créer automatiquement un itinéraire par défaut pointant vers l'homologue PPPoE lorsqu'il est connecté.
Mesure d'itinéraire par défaut		(Facultatif) Pour l'itinéraire entre le pare-feu et le fournisseur de services Internet, saisissez une mesure d'itinéraire (un niveau de priorité) à associer à l'itinéraire par défaut et à utiliser pour la sélection du chemin (intervalle compris entre 1 et 65 535). Plus la valeur numérique est grande, plus le niveau de priorité est élevé.
Accéder au concentrateur		(Facultatif) Saisissez le nom du concentrateur d'accès se trouvant à l'extrémité du fournisseur de services Internet auquel le pare-feu se connecte (aucune valeur par défaut).
Service (Service)		(Facultatif) Saisissez la chaîne de service (aucune valeur par défaut).
Passif		Sélectionnez cette option pour utiliser le mode passif. En mode passif, un point d'extrémité PPPoE attend que le concentrateur d'accès envoie la première trame.
Type d'adresse IPv4 = **DHCP**		
Activer	**Interface Ethernet** > **IPv4**	Sélectionnez pour activer le client DHCP sur l'interface.
Créer automatiquement un itinéraire par défaut en direction de la passerelle par défaut fournie par le serveur		Sélectionnez pour créer automatiquement un itinéraire par défaut pointant vers la passerelle par défaut fournie par le serveur DHCP.
Envoyer le nom d'hôte		Choisissez si le pare-feu (en tant que client DHCP) doit envoyer le nom d'hôte de l'interface (option 12) au serveur DHCP. Si vous envoyez un nom d'hôte le nom d'hôte du pare-feu est alors le choix indiqué dans le champ Nom d'hôte par défaut. Vous pouvez envoyer ce nom ou saisir un nom d'hôte personnalisé (64 caractères maximum, y compris des lettres majuscules ou

Paramètres d'une interface de couche 3	Configuré dans	Description
		minuscules, des chiffres, des points, des tirets et des traits de soulignement).
Mesure d'itinéraire par défaut		Pour l'itinéraire entre le pare-feu et le fournisseur de serveur DHCP, vous pouvez saisir une mesure d'itinéraire (un niveau de priorité) à associer à l'itinéraire par défaut et à utiliser pour la sélection du chemin (intervalle compris entre 1 et 65 535, aucune valeur par défaut). Plus la valeur numérique est grande, plus le niveau de priorité est élevé.
Afficher les informations d'exécution du client DHCP		Sélectionnez pour afficher tous les paramètres reçus par le serveur DHCP, y compris le statut du bail DHCP, l'attribution de l'adresse IP dynamique, le masque de sous-réseau, la passerelle, les paramètres du serveur (DNS, NTP, domaine, WINS, NIS, POP3 et SMTP).
Activer IPv6 sur l'interface	**Interface Ethernet** > **IPv6**	Sélectionnez pour activer l'adressage IPv6 sur cette interface.
ID de l'interface		Saisissez l'identifiant unique étendu sur 64'A0;bits (EUI-64) au format hexadécimal (par exemple, 00:26:08:FF:FE:DE:4E:29). Si ce champ n'est pas renseigné, le pare-feu utilise l'identifiant unique étendu sur 64'A0;bits (EUI-64) généré à partir de l'adresse MAC de l'interface physique. Si vous activez l'option **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** lors de l'ajout d'une adresse, le pare-feu utilise l'ID de l'interface comme partie hôte de l'adresse.
Adresse		Cliquez sur **Add (Ajouter)** et configurez les paramètres suivants pour chaque adresse IPv6 : • **Address (Adresse)** - Saisissez une adresse IPv6 et une longueur de préfixe (par exemple, 2001:400:f00::1/64). Vous pouvez également sélectionner un objet d'adresse IPv6 existant ou cliquer sur **Address (Adresse)** pour en créer un nouveau. • **Enable address on interface (Activer l'adresse sur l'interface)** - Sélectionnez cette option pour activer l'adresse IPv6 sur l'interface. • **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** - Sélectionnez cette option pour utiliser l'**ID de l'interface** comme partie hôte de l'adresse IPv6. • **Anycast** - Sélectionnez cette option pour inclure le routage via le nœud le plus proche.

Paramètres d’une interface de couche 3	Configuré dans	Description
		• **Send Router Advertisement (Envoyer la publication de routeur)** - Sélectionnez pour activer la publication de routeur (RA) pour cette adresse IP. (Vous devez également activer l'option globale **Enable Router Advertisement (Activer la publication de routeur** sur l'interface.) Pour plus d’informations sur la RA, reportez-vous à la section Activation de la publication de routeur. Les champs restants s'appliquent uniquement si vous activez la RA. • **Valid Lifetime (Durée de vie valide)** - La durée, en secondes, pendant laquelle le pare-feu considère l’adresse comme valide. La durée de vie valide doit être supérieure ou égale à **Preferred Lifetime (durée de vie préférée)** (valeur par défaut de 2 592 000). • **Preferred Lifetime (Durée de vie préférée)** - La durée, en secondes, pendant laquelle l’adresse valide est préférée, ce qui signifie que le pare-feu peut l’utiliser pour envoyer et recevoir du trafic. Lorsque la durée de vie préférée expire, le pare-feu ne peut plus utiliser l’adresse pour établir de nouvelles connexions, mais toute connexion existante reste valide jusqu’à ce que **Valid Lifetime (Durée de vie valide** expire (valeur par défaut de 604 800). • **On-link (Sur la liaison)** - Sélectionnez si les systèmes qui disposent d’adresses dans le préfixe sont accessibles sans routeur. • **Autonomous (Autonome)** - Sélectionnez cette option si les systèmes peuvent créer une adresse IP de façon indépendante en combinant le préfixe publié et l’ID d’une interface.
Activer la détection des doublons d'adresses	**Interface Ethernet** > **IPv6** > **Résolution d’adresses**	Sélectionnez pour activer la Détection des doublons d’adresses (DAD) puis configurez les autres champs de cette section.
Tentatives DAD		Indiquez le nombre de tentatives DAD dans l'intervalle de sollicitation de voisins (**NS Interval (intervalle NS)**) avant que la tentative d'identification n'échoue (intervalle compris entre 1 et 10 ; valeur par défaut : 1).

Paramètres d’une interface de couche 3	Configuré dans	Description
Durée d'accessibilité		Indiquez la durée (en secondes) pendant laquelle un voisin reste accessible après une requête et une réponse réussies (plage de 10 à 36 000 ; valeur par défaut de 30).
Intervalle NS (neighbor solicitation interval/intervalle de sollicitation de voisins)		Indiquez le nombre de secondes pour des tentatives DAD avant qu'un échec ne soit signalé (intervalle compris entre 1 et 10 ; valeur par défaut : 1).
Activer la surveillance NDP		Sélectionnez pour activer la surveillance du Protocole de découverte des voisins (NDP). Une fois activé, vous pouvez sélectionner Surveillance NDP ( dans la colonne Fonctions) et visualiser des informations sur un voisin que le pare-feu a découvert, comme l’adresse IPv6, l’adresse MAC correspondante et l’ID utilisateur (selon le cas).
Activer la publication des routeurs	**Interface Ethernet** > **IPv6** > **Publicité de routeur**	Pour réaliser une SLAAC (stateless address auto-configuration / auto-configuration d’adresse sans état) sur les interfaces IPv6, sélectionnez cette option et renseignez les autres champs de cette section. Les clients DNS IPv6 qui reçoivent les messages de publication de routeur utilisent ces informations. La RA permet au pare-feu d'agir en tant que passerelle par défaut pour les hôtes IPv6 qui ne sont pas configurés de façon statique et de fournir à l'hôte un préfixe IPv6 qui lui permet de configurer une adresse. Vous pouvez utiliser un serveur DHCPv6 distinct conjointement avec cette fonctionnalité pour fournir un DNS et d'autres paramètres aux clients. Il s’agit d’un paramètre global de l’interface. Si vous souhaitez définir des options de publication de routeur pour les adresses IP individuelles, cliquez sur **Add (Ajouter)** dans la table d’adresses IP et configurez l’adresse. Si vous définissez des options de publication de routeur pour une adresse IP, vous devez sélectionner l'option **Enable Router Advertisement (Activer la publication de routeur)** sur l'interface.
Intervalle min. (s)		Indiquez l’intervalle minimum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 3 et 1 350 ; valeur par défaut : 200). Le pare-feu envoie les publications de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales configurées.

Paramètres d’une interface de couche 3	Configuré dans	Description
Intervalle max. (s)		Indiquez l’intervalle maximum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 4 et 1 800 ; valeur par défaut : 600). Le pare-feu envoie les publications de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales configurées.
Limite de saut		Indiquez la limite de saut à appliquer aux clients pour les paquets sortants (intervalle compris entre 1 et 255 ; valeur par défaut : 64). Saisissez 0 pour indiquer l’absence de limite de saut.
MTU de liaison		Indiquez l'unité de transmission maximale (MTU) de liaison à appliquer aux clients. Sélectionnez **unspecified (non spécifiée)** pour indiquer l'absence de MTU de liaison (intervalle compris entre 1 280 et 9 192 ; valeur par défaut : non spécifiée).
Durée d'accessibilité (ms)		Indiquez la durée d'accessibilité (en millisecondes) que le client va utiliser pour supposer l'accessibilité d'un voisin après avoir reçu un message de confirmation d'accessibilité. Sélectionnez **unspecified (non spécifiée)** pour indiquer l'absence de valeur pour la durée d'accessibilité (intervalle compris entre 0 et 3 600 000 ; valeur par défaut : non spécifiée).
Durée de retransmission (ms)		Indiquez le minuteur de retransmission qui détermine la durée d'attente du client (en millisecondes) avant la retransmission des messages de sollicitation de voisins. Sélectionnez **unspecified (non spécifiée)** pour indiquer l'absence de valeur pour la durée de retransmission (intervalle compris entre 0 et 4 294 967 295 ; valeur par défaut : non spécifiée).
Durée de vie du routeur (s)		Indiquez la durée pendant laquelle le client utilise le pare-feu comme passerelle par défaut (plage comprise entre 0 et 9 000 ; valeur par défaut : 1 800). Une valeur de 0 indique que le pare-feu n'est pas la passerelle par défaut. Lorsque la durée de vie expire, le client supprime l'entrée du pare-feu de sa liste de routeurs par défaut et utilise un autre routeur comme passerelle par défaut.
Préférence de routeur		Si le segment de réseau dispose de plusieurs routeurs IPv6, le client utilise ce champ pour sélectionner un routeur préféré. Indiquez si le routeur de pare-feu publié a une priorité **High (Élevée)**, **Medium (Moyenne)** (par défaut) ou **Low (Faible)** par rapport aux autres routeurs se trouvant sur le segment.

Paramètres d'une interface de couche 3	Configuré dans	Description
Configuration gérée		Sélectionnez cette option pour indiquer au client que les adresses sont disponibles via DHCPv6.
Vérification de cohérence	**Interface Ethernet** > **IPv6** > **Envoyer la publication des routeurs**	Sélectionnez si vous souhaitez que le pare-feu vérifie que les RA reçues des autres routeurs publient des informations cohérentes sur la liaison. Le pare-feu consigne toutes les incohérences dans un journal système de type **Ipv6nd**.
Autre configuration		Sélectionnez pour indiquer au client que d'autres informations d'adresse (par exemple, des paramètres associés au DNS) sont disponibles via DHCPv6.
Inclure les informations DNS dans la publication de routeur	**Interface Ethernet** > **IPv6** > **Prise en charge DNS**	Sélectionnez pour permettre au pare-feu d'envoyer des informations DNS dans les messages de publication de routeur (RA) NDP à partir de cette interface Ethernet IPv6. Les autres champs de Prise en charge DNS de ce tableau ne sont visibles qu'après sélection de cette option.
Serveur		Il est possible d'**Ajouter** une ou plusieurs adresses de serveur DNS (RDNS) récursives pour que le pare-feu envoie des publications de routeur NDP à partir de cette interface Ethernet IPv6. Les serveurs RDNS envoient une série de requêtes de recherches DNS aux serveurs DNS racines et aux serveurs DNS fiables pour finalement fournir une adresse IP au client DNS. Vous pouvez configurer un maximum de huit serveurs RDNS que le pare-feu envoie, dans l'ordre indiqué de haut en bas, dans une publication de routeur NDP au destinataire, qui utilise ensuite ces adresses dans le même ordre. Vous devez sélectionner un serveur et **Déplacer en haut** ou **Déplacer en bas** pour modifier l'ordre des serveurs ou **Supprimer** un serveur de la liste lorsque vous n'en avez plus besoin.
Durée de vie		Saisissez le nombre maximum de secondes après que le client DNS IPv6 a reçu la publication du routeur avant que le client puisse utiliser les serveurs RDNS afin de résoudre les noms de domaine (la plage est la valeur d'Intervalle max. (sec) jusqu'à deux fois l'intervalle maximal, la valeur par défaut est de 1 200).
Suffixe		Il vous faut **Ajouter** et configurer un ou plusieurs noms de domaine (suffixes) pour la liste de recherche DNS (DNSSL). 255 octets maximum. Une liste de recherche DNS est une liste de suffixes de domaine qu'un routeur de client DNS ajoute (un à la fois) à un nom

Paramètres d'une interface de couche 3	Configuré dans	Description
		de domaine non qualifié avant d'entrer le nom dans une requête DNS, en utilisant un nom de domaine complet dans la requête DNS. Par exemple, si un client DNS essaie de soumettre une requête DNS pour « qualité » sans suffixe, le routeur ajoute une période et le premier suffixe DNS du DNS cherche ce nom dans la liste puis transmet la requête DNS. Si le premier suffixe DNS sur la liste est « company.com », la requête DNS qui résulte du routeur est « quality.company.com » pour le FQDN. Si la requête DNS échoue, le routeur ajoute le deuxième suffixe DNS de la liste au nom non qualifié et transmet une nouvelle requête DNS. Le routeur essaie les suffixes DNS jusqu'à ce qu'une recherche DNS soit réussie (ignore les suffixes restants) ou jusqu'à ce que le routeur ait essayé tous les suffixes de la liste. Configurez le pare-feu avec les suffixes que vous souhaitez fournir au routeur du client DNS dans une option Découverte de voisins DNSSL ; le client DNS recevant l'option DNSSL utilise les suffixes pour ses requêtes DNS non qualifiées. Vous pouvez configurer un maximum de huit noms de domaine (suffixes) pour une liste de recherche DNS que le pare-feu envoie (dans l'ordre, de haut en bas) dans une publication de routeur NDP au destinataire, qui utilise ces adresses dans le même ordre. Sélectionnez un suffixe et utilisez les options **Déplacer vers le haut** ou **Déplacer vers le bas** pour modifier l'ordre ou **Supprimer** un suffixe lorsque vous n'en avez plus besoin.
Durée de vie		Saisissez le nombre maximal de secondes après que le client DNS IPv6 reçoit la publication du routeur lui indiquant qu'il peut utiliser un nom de domaine (suffixe) sur la Liste de recherche DNS (la plage est comprise entre la valeur de l'Intervalle max. [sec] et deux fois l'intervalle maximal ; la valeur par défaut est 1 200).
État d'une interface SD-WAN	**Interface Ethernet** > **SD-WAN**	Si vous avez sélectionné **Enable SD-WAN (Activer SD-WAN)** dans l'onglet **IPv4**, le pare-feu indique `l'état de l'interface SD-WAN. Activé`. Si vous n'avez pas sélectionné **Enable SD-WAN (Activer SD-WAN)**, il indique `Disabled (Désactivé)`.
Profil d'interface SD-WAN		Sélectionnez un profil d'interface SD-WAN existant pour l'appliquer à cette interface Ethernet ou ajoutez un nouveau profil d'interface SD-WAN.

Paramètres d'une interface de couche 3	Configuré dans	Description
		*Vous devez **Enable SD-WAN (Activer SD-WAN)** pour l'interface avant que vous ne puissiez appliquer un profil d'interface SD-WAN.*
NAT en amont		Si votre plate-forme ou branche SD-WAN se trouve derrière un périphérique qui effectue un NAT, **Enable (Activez)** le NAT en amont pour cette plate-forme ou cette branche.
Type d'adresse IP NAT		Sélectionnez le type d'attribution d'adresse IP et indiquez l'adresse IP ou FQDN de l'interface publique sur ce périphérique effectuant le NAT ou indiquez que le DDNS dérive l'adresse. Ainsi, Auto VPN peut utiliser l'adresse comme terminal du tunnel de la plate-forme ou de la branche. • **Static IP (IP statique)** : Sélectionnez le **Type** qui sera **IP Address (Adresse IP)** ou **FQDN** et saisissez l'adresse IPv4 ou FQDN. • **DDNS** : le DNS dynamique (DDNS) dérive l'adresse IP du périphérique NAT en amont.
Vitesse de liaison	**Interface Ethernet** > **Avancé**	Sélectionnez la vitesse de l'interface en Mbits/s (**10**, **100** ou **1 000**) ou sélectionnez **Auto**.
Mode duplex de la liaison		Indiquez si le mode de transmission de l'interface est en duplex intégral (**full (intégral)**), semi-duplex (**half (semi)**) ou automatiquement négocié (**auto**).
état des liaisons		Indiquez si l'état de l'interface est activé (**up (actif)**), désactivé **down (inactif)**) ou automatiquement déterminé (**auto**).
Profil de gestion	**Interface Ethernet** > **Avancé** > **Autres infos**	Sélectionnez un profil qui définit les protocoles (par exemple, SSH, Telnet et HTTP) à utiliser pour gérer le pare-feu dans cette interface. Sélectionnez **None (Aucune)** pour supprimer l'affectation de profil de l'interface.
MTU		Saisissez l'unité de transmission maximale (MTU) en octets par paquet envoyé sur cette interface (intervalle compris entre 576 et 9 192 ; valeur par défaut : 1 500). Si les machines situées de chaque côté du pare-feu effectuent une détection du chemin MTU (PMTUD) et que l'interface reçoit un paquet dépassant la valeur MTU, le pare-feu renvoie à la source un message de *fragmentation ICMP obligatoire* indiquant que le paquet est trop volumineux.

Paramètres d’une interface de couche 3	Configuré dans	Description
Ajuster TCP MSS		Sélectionnez pour ajuster la taille de segment maximale (MSS) afin de tolérer les octets de tous les en-têtes qui respectent la taille en octets de la MTU de l’interface. La taille en octets de la MTU moins la taille d'ajustement de la MSS équivaut à la taille en octets de la MSS, laquelle varie selon le protocole IP : • **IPv4 MSS Adjustment Size (Taille d'ajustement MSS IPv4)** - intervalle compris entre 40 et 300 ; valeur par défaut : 40. • **IPv6 MSS Adjustment Size (Taille d'ajustement MSS IPv4)** - intervalle compris entre 60 et 300 ; valeur par défaut : 60. Servez-vous de ces paramètres pour faire face aux situations où un **tunnel** réseau nécessite une plus petite MSS. Si un paquet a plus d'octets que la MSS sans faire l'objet d'une fragmentation, ce paramètre permet son ajustement. L'encapsulation rallonge les en-têtes. Il peut donc s'avérer utile de configurer la taille d'ajustement MSS de façon à autoriser les octets d'éléments tels que des en-têtes MPLS ou le trafic par tunnel ayant une étiquette VLAN.
Sous-interface non étiquetée		Indique que toutes les sous-interfaces appartenant à cette interface de couche 3 ne sont pas étiquetées. PAN-OS® sélectionne une sous-interface non étiquetée comme interface d’entrée en fonction de la destination du paquet. Si la destination est l'adresse IP d'une sous-interface non étiquetée, il effectue un mappage vers la sous-interface. Cela signifie aussi que l'adresse source des paquets allant dans la direction inverse doit être traduite en adresse IP de la sous-interface non étiquetée. Une conséquence indirecte de ce mécanisme de classification est que tous les paquets multicast et de diffusion sont assignés à l'interface de base et non à l'une des sous-interfaces. Comme OSPF (Open Shortest Path First/premier chemin ouvert le plus court) utilise le multicast, le pare-feu ne le prend pas en charge sur les sous-interfaces non étiquetées.
Adresse IP Adresse MAC	**Interface Ethernet** > **Avancé** > **Entrées ARP**	Pour ajouter une ou plusieurs entrées ARP (Address Resolution Protocol / protocole de résolution d’adresse) statiques, cliquez sur **Add (Ajouter)**, puis saisissez une adresse IP et son adresse matérielle associée (MAC). Pour supprimer une entrée, sélectionnez-la et cliquez sur **Delete (Supprimer)**. Les entrées ARP statiques minimisent le traitement ARP et protègent des attaques par hôte interposé pour les adresses définies.

Paramètres d’une interface de couche 3	Configuré dans	Description
Adresse IPv6 Adresse MAC	**Interface Ethernet** > **Avancé** > **Entrées ND**	Afin de fournir des informations de voisinage pour NDP (Neighbor Discovery Protocol / protocole de découverte des voisins) cliquez sur **Add (Ajouter)** et saisissez l’adresse IP et l’adresse MAC du voisin.
Activer le proxy NDP	**Interface Ethernet** > **Avancé** > **Proxy NDP**	Sélectionnez cette option pour activer le proxy NDP (Neighbor Discovery Protocol / protocole de découverte des voisins) sur l’interface. Le pare-feu répondra aux paquets ND demandant des adresses MAC pour les adresses IPv6 de cette liste. Dans la réponse ND, le pare-feu envoie sa propre adresse MAC pour l'interface pour indiquer qu'il agira en tant que proxy en répondant aux paquets destinés à ces adresses. Il est recommandé de sélectionner l'option **Enable NDP Proxy (Activer le proxy NDP)** si vous utilisez NPTv6 (Network Prefix Translation/traduction de préfixe réseau IPv6). Si l'option **Enable NDP Proxy (Activer le proxy NDP)** est sélectionnée, vous pouvez filtrer de nombreuses entrées d'adresse en saisissant une chaîne de recherche et en cliquant sur Appliquer le filtre (→).
Adresse		Cliquez sur **Add (Ajouter)** pour saisir une ou plusieurs adresses IPv6, plages d'adresses IP, sous-réseaux IPv6 ou objets d'adresse pour lesquels le pare-feu agira comme proxy NDP. Idéalement, l'une de ces adresses est identique à celle de la traduction source dans NPTv6. L'ordre des adresses n'a pas d'importance. Si l'adresse est un sous-réseau, le pare-feu enverra une réponse ND pour toutes les adresses du sous-réseau. Par conséquent, il est recommandé d'ajouter également les voisins IPv6 du pare-feu et de sélectionner **Negate (Ignorer)** pour que le pare-feu ne réponde pas à ces adresses IP.
Inverser		Sélectionnez **Negate (Ignorer)** en regard d'une adresse afin d'empêcher le proxy NDP pour cette adresse. Vous pouvez ignorer un sous-ensemble de la plage d'adresses IP ou du sous-réseau IP spécifié.
Activer LLDP	**Interface Ethernet** > **Avancé** > **LLDP**	Sélectionnez cette option pour activer LLDP (Link Layer Discovery Protocol/protocole de découverte de couche liaison) sur l'interface. LLDP fonctionne sur la couche de liaison pour détecter les périphériques voisins et leurs fonctionnalités.

Paramètres d'une interface de couche 3	Configuré dans	Description
LLDP Profile (profil LLDP)		Si LLDP est activé, sélectionnez un profil LLDP à affecter à l'interface ou cliquez sur **LLDP Profile (Profil LLDP)** pour créer un nouveau profil (reportez-vous à la section Réseau > Profils réseau > Profil LLDP). Sélectionnez **None (Aucun)** pour configurer le pare-feu de sorte qu'il utilise les paramètres généraux par défaut.
Activation à l'état HA passif		Si LLDP est activé, sélectionnez cette option pour permettre au pare-feu défini comme pare-feu HA passif de pré-négocier LLDP avec son homologue avant que le pare-feu devienne actif.
Paramètres	**Interface Ethernet** > **Avancé** > **DDNS**	Sélectionnez **Settings (Paramètres)** pour que les champs DDNS puissent être configurés.
Activer		Activer DDNS sur l'interface Vous devez d'abord activer DDNS pour le configurer. (Si vous n'avez pas terminé de configurer DDNS, vous pouvez enregistrer la configuration sans l'activer, ce qui vous évitera de perdre la configuration partielle.)
Intervalle de mise à jour (jours)		Saisissez l'intervalle (en jours) entre les mises à jour que le pare-feu envoie au serveur DDNS pour mettre à jour les adresses IP associées aux FQDN (la plage est comprise entre 1 et 30 ; la valeur par défaut est 1). *Le pare-feu met également à jour DDNS à la réception d'une nouvelle adresse IP pour l'interface du serveur DHCP.*
Profil du certificat		Créez un profil de certificat pour vérifier le service DDNS. Le service DDNS présente au pare-feu un certificat signé par l'autorité de certification (CA).
Nom d'hôte		Saisissez un nom d'hôte pour l'interface, qui est inscrit auprès du serveur DDNS (par exemple, hôte123.domaine123.com ou hôte123). Le pare-feu ne valide pas le nom d'hôte, sauf pour confirmer que la syntaxe utilise les caractères valides autorisés par DNS pour un nom de domaine.
Constructeur		Sélectionnez le fournisseur DDNS (et la version) qui fournit un service DDNS à cette interface : • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1**

Paramètres d’une interface de couche 3	Configuré dans	Description
		• **FreeDNS Afraid.org v1** • **No-IP v1** • **Palo Alto Networks DDNS**—Vous devez l’utiliser pour les interfaces SD-WAN AE et les sous-interfaces SD-WAN de couche 3. *Si vous sélectionnez une version antérieure d’un service DDNS qui, selon le pare-feu, sera supprimée avant une date donnée, passez à la nouvelle version.* Les champs **Name (Nom)** et **Value (Valeur)** qui suivant le nom du fournisseur sont propres au fournisseur. Les champs en lecture seule vous avisent des paramètres que le pare-feu utilise pour se connecter au service DDNS. Configurez les autres champs, comme un mot de passe que le service DDNS vous fournit et le délai que le pare-feu utilise s’il ne reçoit pas de réponse du service DDNS.
Onglet IPv4 - IP		Ajoutez les adresses IPv4 configurées sur l’interface et sélectionnez-les. Toutes les adresses IP sélectionnées sont inscrites auprès du fournisseur DDNS.
Onglet IPv6 - IPv6		Ajoutez les adresses IPv6 configurées sur l’interface et sélectionnez-les. Toutes les adresses IP sélectionnées sont inscrites auprès du fournisseur DDNS.
Show Runtime Info		Affiche l’inscription DDNS : fournisseur DDNS, FQDN résolu et les adresses IP mappées avec un astérisque (*) indiquant l'adresse IP principale. Chaque fournisseur DDNS possède ses propres codes de retour pour indiquer l’état de la mise à jour du nom d’hôte et une date de retour à des fins de résolution de problèmes.

Interface de niveau 3

- Réseau > Interfaces > Ethernet

Configurez une interface Ethernet de couche 3 à laquelle vous pouvez acheminer le trafic.

Paramètres d’une interface de couche 3	Configuré dans	Description
Nom de l'interface	**Interface de couche 3**	Le champ **Interface Name (Nom de l'interface)** en lecture seule affiche le nom de l'interface physique sélectionnée.
Commentaire		Saisissez une description conviviale de l’interface.
Type d'interface		Sélectionnez **Layer3 (Couche 3)**.
Profil NetFlow		Si vous voulez exporter le trafic IP unidirectionnel traversant une interface d’entrée vers un serveur NetFlow, sélectionnez le profil Netflow ou sélectionnez **Netflow Profile (Profil Netflow)** pour créer un nouveau profil (Voir Périphérique > Profils de serveur > NetFlow). Sélectionnez **None (Aucun)** pour supprimer l'affectation de serveur NetFlow de l'interface.
routeur virtuel - VR	**Interface de couche 3** > **Configuration**	Affectez un routeur virtuel à l’interface ou cliquez sur **Virtual Router (Routeur virtuel)** pour en définir un nouveau (voir Réseau > Routeurs virtuels). Sélectionnez **None (Aucun)** pour supprimer l'affectation de routeur virtuel de l'interface.
Routeur logique		Attribuez un routeur logique à l'interface ou cliquez sur **Logical Router (Routeur logique)** pour en définir un nouveau (voir Network > Routing > Logical Routers (Réseau > Routage > Routeurs logiques)). Sélectionnez **None (Aucun)** pour supprimer l'affectation de routeur virtuel de l'interface.
Système virtuel		Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système virtuel (vsys) pour l'interface ou sélectionnez **Virtual System (Système virtuel)** pour en définir un nouveau.
Zone de sécurité		Sélectionnez une zone de sécurité pour l'interface ou sélectionnez **Zone** pour en définir une nouvelle. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de l'interface.
Activer SD-WAN	**Interface de couche 3** > **IPv4**	Sélectionnez **Enable SD-WAN (Activer SD-WAN)** pour activer la fonctionnalité SD-WAN de l’interface Ethernet.
Activer Bonjour Reflector		(séries PA-220, PA-800 et PA-3200 uniquement) Lorsque vous activez cette option, le pare-feu transfère les alertes et les requêtes multicast Bonjour reçues et transférées à cette interface aux autres interfaces et sous-interfaces L3 et AE lorsque vous activez cette option. Cela aide à garantir l’accès utilisateur et la découverte du périphérique sur les environnements de réseau qui utilisent la segmentation pour acheminer le trafic pour des besoins de sécurité

Paramètres d’une interface de couche 3	Configuré dans	Description
		ou administratifs. Vous pouvez activer cette option jusqu’à 16 interfaces.
Adresse IP	**Interface de couche 3** > **IPv4, Type = Statique**	**Add (Ajoutez)** et suivez l’une des étapes ci-dessous pour indiquer une adresse IP statique et un masque réseau de l’interface ou de l’interface AE. • Saisissez l’entrée en notation CIDR (Classing Inter-Domain Routing, routage inter domaine sans classes) : *adresse_ip/masque* (par exemple, 192.168.2.0/24). • Sélectionnez un objet d'adresse existant de type **IP netmask (Masque réseau IP)**. • Créez un objet d’**Address (Adresse)** de type **IP netmask (Masque réseau IP)**. Vous pouvez saisir plusieurs adresses IP pour l'interface. La base d'informations de transfert (FIB) utilisée par votre système détermine le nombre maximum d'adresses IP. Il est possible de **Supprimer** une adresse IP lorsque vous n’en avez plus besoin.
Passerelle SD-WAN		Si vous avez sélectionné la fonction **Enable SD-WAN (Activer SD-WAN)**, saisissez l’adresse IPv4 de la passerelle SD-WAN.
Activer	**Interface de couche 3** > **IPv4** > **Général, type = PPPoE**	Sélectionnez **Enable (Activer)** pour activer l’interface pour la terminaison PPPoE (Point-to-Point Protocol over Ethernet/ protocole point à point sur Ethernet). L'interface en tant que point de terminaison Point-to-Point Protocol over Ethernet (protocole point-à-point sur Ethernet ; PPPoE) prend en charge la connectivité dans un environnement Digital Subscriber Line (ligne d'accès numérique ; DSL) où se trouve un modem DSL, mais aucun autre périphérique PPPoE pour terminer la connexion.
Username (Nom d’utilisateur)		Saisissez le nom d'utilisateur fourni par votre ISP pour la connexion de point à point.
Mot de passe et confirmation de mot de passe		Saisissez le mot de passe et confirmez le mot de passe.
Afficher les informations		électionnez pour afficher les informations de l’interface PPPoE.

Paramètres d’une interface de couche 3	Configuré dans	Description
d'exécution du client PPPoE		
Authentification	**Interface de couche 3** > **IPv4** > **Avancé, Type = PPPoE**	Sélectionnez la méthode d'authentification : • **None (Aucune)** : (par défaut) Il n’y a aucune authentification pour l’interface PPPoE. • **CHAP** - Le pare-feu utilise le Challenge Handshake Authentication Protocol (protocole d’authentification de négociation par défi, CHAP) - RFC-1994 - sur l’interface PPPoE. • **PAP** - Le pare-feu utilise le Password Authentication Protocol (protocole d’authentification par mot de passe, PAP) sur l’interface PPPoE. Le PAP est moins sécuritaire que le CHAP ; le PAP envoie les noms d’utilisateur et les mots de passe en texte brut. • **auto** - Le pare-feu négocie la méthode d’authentification (CHAP ou PAP) avec le serveur PPPoE.
Adresse statique		Requête du serveur PPPoE d’une adresse IPv4 souhaitée. Le serveur PPPoE peut attribuer cette adresse ou une autre adresse.
Créer automatiquement un itinéraire par défaut en direction de l’homologue		Sélectionnez cette option pour créer automatiquement un itinéraire par défaut pointant vers la passerelle par défaut fournie par le serveur PPPoE.
Mesure d'itinéraire par défaut		Saisissez la mesure d’itinéraire par défaut (niveau de priorité) pour la connexion PPPoE (par défaut : 10). Plus la valeur de l'itinéraire est faible, plus sa priorité de sélection est élevée. Par exemple, un itinéraire avec une valeur de mesure de 10 est utilisé avant un itinéraire avec une valeur de mesure de 100.
Accéder au concentrateur		Si votre ISP vous a fourni le nom d’un concentrateur d’accès, saisissez-le. Le pare-feu se connectera à ce concentrateur d’accès du côté de l’IPS. Ceci est une valeur de chaîne de 0 à 255 caractères.
Service (Service)		Le pare-feu (client PPPoE) peut fournir la demande de service désirée au serveur PPPoE. Ceci est une valeur de chaîne de 0 à 255 caractères.

Paramètres d’une interface de couche 3	Configuré dans	Description
Passif		Le pare-feu (client PPPoE) attend que le serveur PPPoE initie la connexion. Si l’option n’est pas activée, le pare-feu initie la connexion.
Activer	**Interface de couche 3** > **IPv4, Type = Client DHCP**	Permet à l'interface d'agir en tant que client DHCP (Dynamic Host Configuration Protocol/protocole d'attribution dynamique des adresses) et de recevoir une adresse IP assignée de façon dynamique. *Les pare-feu en mode haute disponibilité (HD) active/active ne prennent pas en charge le client DHCP.*
Créer automatiquement un itinéraire par défaut en direction de la passerelle par défaut fournie par le serveur		Sélectionnez cette option pour que le pare-feu de crée un itinéraire statique vers une passerelle par défaut. La passerelle par défaut est utile lorsque les clients tentent d'accéder à de nombreuses destinations qui n'ont pas besoin de conserver des itinéraires dans une table de routage sur le pare-feu.
Envoyer le nom d'hôte		Sélectionnez cette option pour affecter un nom d'hôte à l’interface du client DHCP et envoyer ce nom d'hôte (option 12) à un serveur DHCP. qui peut enregistrer le nom d'hôte auprès du serveur DNS. Le serveur DNS peut ensuite gérer automatiquement les résolutions de nom d’hôte/adresse IP dynamique. Les hôtes externes peuvent identifier l’interface par son nom d’hôte. La valeur par défaut indique `system-hostname (nom de l’hôte système)`, qui correspond au nom d’hôte du pare-feu que vous avez configuré sous **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **General Settings (Paramètres généraux)**. Vous pouvez également saisir un nom d’hôte pour l’interface, d’un maximum de 64 caractères, y compris des lettres majuscules et minuscules, des chiffres, des points, des tirets et des traits de soulignement.
Mesure d'itinéraire par défaut	**Interface de couche 3** > **IPv4, Type = Client DHCP**	Saisissez une mesure d'itinéraire par défaut (niveau de priorité) pour l'itinéraire entre le pare-feu et le serveur DHCP (plage comprise entre 1 et 65 535 ; aucune valeur de mesure par défaut). Plus la valeur de l'itinéraire est faible, plus sa priorité de sélection est élevée. Par exemple, un itinéraire avec une valeur de mesure de 10 est utilisé avant un itinéraire avec une valeur de mesure de 100.

Paramètres d’une interface de couche 3	Configuré dans	Description
Afficher les informations d'exécution du client DHCP		Sélectionnez cette option pour afficher tous les paramètres que le client a reçus de son serveur DHCP, y compris le statut du bail DHCP, l’attribution de l’adresse IP dynamique, le masque de sous-réseau, la passerelle et les paramètres du serveur (DNS, NTP, domaine, WINS, NIS, POP3 et SMTP).
Activer IPv6 sur l'interface	**Interface de couche 3** > **IPv6**	Sélectionnez pour activer l’adressage IPv6 sur l’interface.
ID de l'interface		Saisissez l'identifiant unique étendu sur 64 bits (**EUI-64**) au format hexadécimal (par exemple, 00:26:08:FF:FE:DE:4E:29). Si ce champ n'est pas renseigné, le pare-feu utilise l'identifiant unique étendu sur 64'A0;bits (EUI-64) généré à partir de l'adresse MAC de l'interface physique. Si vous activez l'option **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** lors de l'ajout d'une adresse, le pare-feu utilise l'ID de l'interface comme partie hôte de l'adresse.
Adresse	**Interface de couche 3** > **IPv6** > **Attribution d'adresse, type = statique**	Ajoutez une adresse IPv6 et une longueur de préfixe (par exemple, 2001:400:f00::1/64). Vous pouvez également sélectionner un objet d'adresse IPv6 existant ou en créer un nouveau.
Activer l’adresse sur l’interface		Sélectionnez pour activer l’adresse IPv6 sur l’interface.
Utiliser l’ID de l’interface comme partie hôte.		Sélectionnez cette option pour utiliser l’**ID de l’interface** comme partie hôte de l’adresse IPv6.
Anycast		Sélectionnez cette option pour inclure le routage via le nœud le plus proche.
Envoyer la publication des routeurs	**Interface de couche 3** > **IPv6** > **Attribution d'adresse, type = statique**	Sélectionnez cette option pour activer la publication de routeur (RA) pour cette adresse IP. (Vous devez également activer l'option globale **Enable Router Advertisement (Activer la publication de routeur** sur l'interface.) Pour plus d’informations sur la RA, reportez-vous à la section Activer la publication de routeur dans ce tableau. Les champs suivants s’appliquent uniquement si vous activez la publication du routeur : • **Valid Lifetime (Durée de vie valide)** - La durée, en secondes, pendant laquelle le pare-feu considère l’adresse comme valide. La durée de vie valide doit être supérieure ou égale à **Preferred**

Paramètres d’une interface de couche 3	Configuré dans	Description
		Lifetime (durée de vie préférée). La valeur par défaut est de 2 592 000. • **Preferred Lifetime (Durée de vie préférée)** - La durée, en secondes, pendant laquelle l’adresse valide est préférée, ce qui signifie que le pare-feu peut l’utiliser pour envoyer et recevoir du trafic. Lorsque la durée de vie préférée expire, le pare-feu ne peut plus utiliser l'adresse pour établir de nouvelles connexions, mais toute connexion existante reste valide jusqu'à ce que la **Valid Lifetime (Durée de vie valide)** expire. La valeur par défaut est de 604 800. • **On-link (Sur la liaison)** - Sélectionnez si les systèmes qui disposent d’adresses dans le préfixe sont accessibles sans routeur. • **Autonomous (Autonome)** - Sélectionnez cette option si les systèmes peuvent créer une adresse IP de façon indépendante en combinant le préfixe publié et l’ID d’une interface.
Accepter l'itinéraire annoncé par le routeur	**Interface de couche 3** > **IPv6** > **Attribution d'adresse, Type = Client DHCPv6**	Sélectionnez cette option pour autoriser le client DHCPv6 à accepter le RA du serveur DHCPv6.
Mesure d'itinéraire par défaut		Saisissez une métrique de route par défaut pour la route entre l'interface et le FAI ; la plage est de 1 à 65 535 ; la valeur par défaut est 10.
Préférence		Sélectionnez la préférence de l'interface client DHCPv6 (**low (faible)**, **medium (moyen)**ou **high (élevé)**) de sorte que, dans le cas où vous avez deux interfaces (chacune étant connectée à un FAI différent pour la redondance), vous puissiez attribuer à l'un des FAI une préférence plus élevée que la l'interface avec l'autre FAI. Le FAI connecté à l'interface préférée sera le FAI qui fournit le préfixe délégué à envoyer à une interface faisant face à l'hôte. Si les interfaces ont la même préférence, les deux FAI fournissent un préfixe délégué et l'hôte décide quel préfixe utiliser.
Activer l'adresse IPv6	**Interface de couche 3** > **IPv6** > **Attribution d'adresse, Type = Client DHCPv6**	Activez l'adresse IPv6 reçue pour ce client DHCPv6.
Adresse non temporaire		Demandez une adresse non temporaire que le pare-feu doit attribuer à cette interface client DHCPv6 qui fait face au routeur délégant et au FAI. (Ce type d'adresse a une durée de vie plus longue qu'une adresse temporaire).

Paramètres d’une interface de couche 3	Configuré dans	Description
	> **Options DHCPv6**	*Que vous demandiez une adresse non temporaire ou une adresse temporaire pour l'interface dépend de votre discrétion et de la capacité du serveur DHCPv6; certains serveurs ne peuvent fournir qu'une adresse temporaire. La meilleure pratique consiste à sélectionner à la fois Adresse non temporaire et Adresse temporaire, auquel cas le pare-feu préférera l'Adresse non temporaire.*
Adresse temporaire		Demandez une adresse temporaire que le pare-feu doit attribuer à cette interface client DHCPv6 qui fait face au routeur délégant et au FAI. Sélectionnez Adresse temporaire pour un niveau de sécurité supérieur, car l'adresse est destinée à être utilisée pendant une courte période.
Validation rapide		Sélectionnez cette option pour utiliser le processus DHCP des messages Solliciter et Répondre, plutôt que le processus des messages Solliciter, Annoncer, Demander et Répondre.
Activer la délégation de préfixe	**Interface de couche 3** > **IPv6** > **Attribution d'adresse, Type = Client DHCPv6** > **Délégation de préfixe**	Activez la délégation de préfixe pour permettre au pare-feu de prendre en charge la fonctionnalité de délégation de préfixe. Cela signifie que l'interface accepte un préfixe du serveur DHCPv6 en amont et place le préfixe dans le pool de préfixes que vous sélectionnez, à partir duquel le pare-feu délègue un préfixe à un hôte via RA. La possibilité d'activer ou de désactiver la délégation de préfixe pour une interface permet au pare-feu de prendre en charge plusieurs FAI (un FAI par interface). L'activation de la délégation de préfixe sur cette interface contrôle quel FAI fournit le préfixe.
Conseil sur la longueur du préfixe DHCP		Sélectionnez pour permettre au pare-feu d'envoyer une longueur de préfixe DHCPv6 préférée au serveur DHCPv6.
Longueur du préfixe DHCP (bits)		Entrez la longueur de préfixe DHCPv6 préférée dans la plage de 48 à 64 bits, qui est envoyée comme indice au serveur DHCPv6. Le serveur DHCPv6 a le pouvoir discrétionnaire d'envoyer la longueur de préfixe qu'il choisit.

Paramètres d’une interface de couche 3	Configuré dans	Description
		Demander une longueur de préfixe de 48, par exemple, laisse 16 bits restants pour les sous-réseaux (64-48), ce qui indique que vous avez besoin de nombreuses subdivisions de ce préfixe pour déléguer. D'autre part, demander une longueur de préfixe de 63 laisse 1 bit pour ne déléguer que deux sous-réseaux. Sur les 128 bits, il reste encore 64 bits pour l'adresse de l'hôte. L'interface peut recevoir un préfixe /48, mais déléguer un préfixe /64, par exemple, ce qui signifie que le pare-feu subdivise le préfixe qu'il délègue.
Nom du pool de préfixes		Saisissez un nom pour le pool de préfixes dans lequel le pare-feu stocke le préfixe reçu. Le nom doit être unique et contenir un maximum de 63 caractères alphanumériques, traits d'union, points et traits de soulignement. *Utilisez un nom de pool de préfixes qui reflète le FAI pour une reconnaissance facile.*
Nom	**Interface de couche 3 > IPv6 > Attribution d'adresse, type = hérité**	**Add (Ajoutez)** un pool en saisissant un nom de pool. Le nom peut comporter au maximum 63 caractères alphanumériques, traits d'union, points et traits de soulignement.
Type d'adresse		Sélectionnez parmi les choix suivants : • **GUA from pool (AUG du pool)**— Adresse Unidiffusion globale (AUG) provenant du pool de préfixes choisi. • **ULA**—Unique Local Address est une adresse privée dans la plage d'adresses fc00::/7 pour la connectivité au sein d'un réseau privé. Sélectionnez ULA s'il n'y a pas de serveur DHCPv6.
Activer sur l'interface		Activez l’adresse IPv6 sur l’interface.
Pool de préfixes		Sélectionnez le pool de préfixes à partir duquel obtenir le GUA.
Assignment Type (Type d'affectation)	**Interface de couche 3 > IPv6 > Attribution d'adresse, type = hérité**	Sélectionnez le type de devoir : • **Dynamic (Dynamique)** — Le client DHCPv6 est responsable du choix d'un identifiant pour configurer l'interface héritée. • **Dynamic with Identifier (Dynamique avec identifiant)**— Vous êtes responsable du choix d'un identifiant dans la plage de

Paramètres d’une interface de couche 3	Configuré dans	Description
		0 à 4 000 et de la gestion d'un identifiant unique sur les clients DHCPv6.
Envoyer la publication des routeurs		Sélectionnez pour envoyer des annonces de routeur (AR) de l'interface aux hôtes LAN.
On-Link		Sélectionnez si les systèmes qui disposent d’adresses dans le préfixe sont accessibles sans routeur.
Autonome		Sélectionnez cette option si les systèmes peuvent créer une adresse IP de façon indépendante en combinant le préfixe publié et l’ID d’une interface.
Activer la fonction Duplicate Address Detection (détection des doublons d'adresses ; DAD).	**Interface de couche 3** > **IPv6** > **Résolution d’adresses**	Sélectionnez pour activer la Détection des doublons d’adresses (DAD) puis configurez les autres champs de cette section.
Tentatives DAD		Indiquez le nombre de tentatives DAD dans l'intervalle de sollicitation de voisins (**NS Interval (intervalle NS)**) avant que la tentative d'identification n'échoue (intervalle compris entre 1 et 10 ; valeur par défaut : 1).
Durée d'accessibilité (s)		Indiquez la durée (en secondes) pendant laquelle un voisin reste accessible après une requête et une réponse réussies (plage de 1 à 36 000 ; valeur par défaut de 30).
Intervalle (s)		Indiquez le nombre de secondes pour des tentatives DAD avant qu'un échec ne soit signalé (intervalle compris entre 1 et 3,600 ; valeur par défaut : 1).
Activer la surveillance NDP		Sélectionnez pour activer la surveillance du Protocole de découverte des voisins (NDP). Lorsque cette option est activée, vous pouvez sélectionner NDP ( dans la colonne Caractéristiques) pour visualiser des informations sur un voisin détecté par le pare-feu, comme l’adresse IPv6, l’adresse MAC correspondante et l’User-ID (dans le meilleur des cas).

Paramètres d’une interface de couche 3	Configuré dans	Description
Activer la publication des routeurs	**Interface de couche 3 > IPv6 > Annonce de routeur, Type = Statique ou Type = Hérité**	Pour assurer la Découverte des voisins sur les interfaces IPv6, sélectionnez et configurez les autres champs de cette section. Les clients DNS IPv6 qui reçoivent les messages de publication de routeur utilisent ces informations. La RA permet au pare-feu d'agir en tant que passerelle par défaut pour les hôtes IPv6 qui ne sont pas configurés de façon statique et de fournir à l'hôte un préfixe IPv6 qui lui permet de configurer une adresse. Vous pouvez utiliser un serveur DHCPv6 distinct conjointement avec cette fonctionnalité pour fournir un DNS et d'autres paramètres aux clients. Il s’agit d’un paramètre global de l’interface. Si vous souhaitez définir des options de publication de routeur (RA) pour les adresses IP individuelles, il vous faut **Add (Ajouter)** et configurer une adresse IPv6 dans la table d’adresses IP. Si vous définissez des options de publication de routeur pour une adresse IPv6, vous devez **Enable Router Advertisement (Activer la publication de routeur)** sur l’interface.
Intervalle min. (s)		Indiquez l’intervalle minimum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 3 et 1 350 ; valeur par défaut : 200). Le pare-feu envoie les publications de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales que vous configurez.
Intervalle max. (s)		Indiquez l’intervalle maximum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 4 et 1 800 ; valeur par défaut : 600). Le pare-feu envoie les publications de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales que vous configurez.
Limite de saut		Indiquez la limite de saut à appliquer aux clients pour les paquets sortants (intervalle compris entre 1 et 255 ; valeur par défaut : 64) ou indiquez **unspecified (non spécifié)**, ce qui correspond à la valeur par défaut du système.
MTU de liaison	**Interface de couche 3 > IPv6 > Annonce de routeur, Type = Statique ou Type = Hérité**	Indiquez l’unité de transmission maximale (MTU) de liaison à appliquer aux clients (la plage est comprise entre 1 280 et 1 500) ou indiquez **unspecified (non spécifié)**, ce qui correspond à la valeur par défaut du système.
Durée d'accessibilité (ms)		Indiquez la durée d'accessibilité (en millisecondes) que le client va utiliser pour supposer l'accessibilité d'un voisin après avoir reçu un message de confirmation d'accessibilité (la plage est comprise

Paramètres d’une interface de couche 3	Configuré dans	Description
		entre 0 et 3 600 000), ou indiquez **unspecified (non spécifié)**, ce qui correspond à la valeur par défaut du système.
Durée de retransmission (ms)		Indiquez le minuteur de retransmission, qui détermine la durée d'attente du client (en millisecondes) avant la retransmission des messages de sollicitation de voisins. (la plage est comprise entre 0 et 4 294 967 295) ou indiquez **unspecified (non spécifié)**, ce qui correspond à la valeur par défaut du système.
Durée de vie du routeur (s)		Indiquez la durée, en secondes, pendant laquelle le client utilise le pare-feu comme passerelle par défaut (plage comprise entre 0 et 9 000 ; valeur par défaut : 1 800). Une valeur de 0 indique que le pare-feu n'est pas la passerelle par défaut. Lorsque la durée de vie expire, le client supprime l'entrée du pare-feu de sa liste de routeurs par défaut et utilise un autre routeur comme passerelle par défaut.
Préférence de routeur		Si le segment de réseau dispose de plusieurs routeurs IPv6, le client utilise ce champ pour sélectionner un routeur préféré. Indiquez si le routeur de pare-feu publié a une priorité **High (Élevée)**, **Medium (Moyenne)** (par défaut) ou **Low (Faible)** par rapport aux autres routeurs se trouvant sur le segment.
Configuration gérée	**Interface de couche 3** > **IPv6** > **Annonce de routeur, Type = Statique ou Type = Hérité**	Sélectionnez cette option pour indiquer au client que les adresses sont disponibles via DHCPv6.
Autre configuration		Sélectionnez pour indiquer au client que d’autres informations d’adresse (par exemple, des paramètres associés au DNS) sont disponibles via DHCPv6.
Vérification de cohérence		Sélectionnez si vous souhaitez que le pare-feu vérifie que les RA reçues des autres routeurs publient des informations cohérentes sur la liaison. Le pare-feu consigne toutes les incohérences dans un journal système de type **Ipv6nd**.
Inclure les informations DNS dans la publication de routeur	**Interface de couche 3** > **IPv6** > **Prise en charge DNS, Type = Statique**	DNS Support Tab (Onglet Prise en charge DNS) est disponible si vous sélectionnez l’option **Enable Router Advertisement (Activer la publication du routeur)** dans l’onglet Publication du routeur. Sélectionnez le pare-feu pour transmettre des informations DNS vers les publications du routeur NDP à partir de cette interface Ethernet IPv6. Les autres champs de Prise en charge DNS (serveur, durée de vie, suffixe et durée de vie) ne sont visibles qu’après sélection de cette option.

Paramètres d'une interface de couche 3	Configuré dans	Description
Serveur		Il est possible d'**Ajouter** une ou plusieurs adresses de serveur DNS (RDNS) récursives pour que le pare-feu envoie des publications de routeur NDP à partir de cette interface Ethernet IPv6. Les serveurs RDNS envoient une série de demandes de recherche DNS aux serveurs DNS racine et aux serveurs DNS autoritaires pour finalement fournir une adresse IP au client DNS. Vous pouvez configurer un maximum de huit Serveurs RDNS que le pare-feu envoie (dans l'ordre indiqué, de haut en bas) dans une publication de routeur NDP au destinataire, qui les utilise ensuite dans le même ordre. Vous devez sélectionner un serveur et **Déplacer en haut** ou **Déplacer en bas** pour modifier l'ordre des serveurs ou **Supprimer** un serveur de la liste lorsque vous n'en avez plus besoin.
Durée de vie		Saisissez le nombre maximum de secondes après que le client DNS IPv6 a reçu la publication du routeur avant que le client puisse utiliser un serveur RDNS afin de résoudre les noms de domaine (la plage est comprise entre la valeur de **Max Interval (sec) [Intervalle maximal (s)]** et deux fois **Max Interval (sec) [Intervalle maximal (s)]** ; la valeur par défaut est 1 200).
Liste de recherche de domaine	**Interface de couche 3** > **IPv6** > **Prise en charge DNS, Type = Statique** **Interface de couche 3** > **IPv6** > **Prise en charge DNS**	Il vous faut **ajouter** un ou plusieurs noms de domaine (suffixes) pour la liste de recherche DNS (DNSSL). 255 octets maximum. Une liste de recherche DNS est une liste de suffixes de domaine qu'un routeur de client DNS ajoute (un à la fois) à un nom de domaine non qualifié avant d'entrer le nom dans une requête DNS, en utilisant un nom de domaine complet dans la requête. Par exemple, si un client DNS essaie de soumettre une requête DNS pour le nom « qualité » sans suffixe, le routeur ajoute un point et le premier suffixe DNS de la liste de recherche DNS au nom et transmet la requête DNS. Si le premier suffixe DNS sur la liste est « company.com », la requête qui résulte du routeur est « quality.company.com » pour le nom de domaine complet. Si la requête DNS échoue, le routeur ajoute le deuxième suffixe DNS de la liste au nom non qualifié et transmet une nouvelle requête DNS. Le routeur utilise les suffixes DNS jusqu'à ce qu'une recherche DNS soit fructueuse (il ignore les suffixes restants) ou jusqu'à ce que le routeur ait essayé tous les suffixes de la liste. Configurez le pare-feu avec les suffixes que vous souhaitez fournir au routeur du client DNS dans une option Découverte de voisins DNSSL ; le client DNS recevant l'option DNSSL utilise les suffixes pour ses requêtes DNS non qualifiées.

Paramètres d’une interface de couche 3	Configuré dans	Description
		Vous pouvez configurer un maximum de huit noms de domaine (suffixes) pour une liste de recherche DNS que le pare-feu envoie (dans l’ordre, de haut en bas) dans une publication de routeur NDP au destinataire, qui les utilise dans le même ordre. Sélectionnez un suffixe et utilisez les options **Déplacer vers le haut** ou **Déplacer vers le bas** pour modifier l’ordre ou **Supprimer** un suffixe lorsque vous n’en avez plus besoin.
Durée de vie		Saisissez le nombre maximal de secondes après que le client DNS IPv6 reçoit la publication du routeur lui indiquant qu’il peut utiliser un nom de domaine (suffixe) sur la liste de recherche DNS (la plage est comprise entre la valeur de **Max Interval (sec) [Intervalle maximal (s)]** et deux fois **Max Interval (sec) [Intervalle maximal (s)]** ; la valeur par défaut est 1 200).
Serveur de noms récursif DNS	**Interface de couche 3** > **IPv6** > **Prise en charge DNS, type = client DHCPv6 ou hérité**	Activez et sélectionnez : • **DHCPv6**—Pour que le serveur DHCPv6 envoie les informations DNS Recursive Name Server. • **Manual (Manuel)** — Pour configurer manuellement le serveur de noms DNS Recursive. Si vous choisissez **Manual (Manuel)**, **Add (ajoutez)** l'adresse IPv6 d'un **Server (serveur)** DNS récursif (RDNS) (par exemple, 2001:4860:4860:0:0:8888) pour que le pare-feu envoie des annonces de routeur NDP à partir de cette interface VLAN IPv6. Les serveurs RDNS envoient une série de requêtes de recherches DNS aux serveurs DNS racines et aux serveurs DNS fiables pour finalement fournir une adresse IP au client DNS. Vous pouvez configurer un maximum de huit serveurs RDNS que le pare-feu envoie (dans l’ordre indiqué, de haut en bas) dans une publication de routeur NDP au destinataire, qui les utilise ensuite dans le même ordre. Vous devez sélectionner un serveur et **Déplacer en haut** ou **Déplacer en bas** pour modifier l’ordre des serveurs ou **Supprimer** un serveur de la liste lorsque vous n’en avez plus besoin. Indiquez la **Lifetime (Durée de vie)** en secondes. Il s'agit de la durée de temps maximale pendant laquelle le client peut utiliser le serveur RDNS donné pour résoudre des noms de domaine. La plage est comprise entre 4 et 3,600 ; la valeur par défaut est 1,200.
Liste de recherche de domaine	**Interface de couche 3** > **IPv6** > **Prise en charge DNS,**	Enable and select (Activez et sélectionnez) : • **DHCPv6**— Pour que le serveur DHCPv6 envoie les informations de la liste de recherche de domaine.

Paramètres d’une interface de couche 3	Configuré dans	Description
	type = client DHCPv6 ou hérité	• **Manual (manuel)**— Pour configurer manuellement la liste de recherche de domaine. Si vous choisissez **Manual (manuel)**, **Add (Ajoutez)** et configurez un ou plusieurs Noms de **Domain(domaine)** (suffixes) pour la liste de recherche DNS (DNSSL). La longueur maximale du suffixe est de 255 octets. Une liste de recherche DNS est une liste de suffixes de domaine qu’un routeur de client DNS ajoute (un à la fois) à un nom de domaine non qualifié avant d’entrer le nom dans une requête DNS, en utilisant un nom de domaine complet dans la requête DNS. Par exemple, si un client DNS essaie de soumettre une requête DNS pour le nom « qualité » sans suffixe, le routeur ajoute un point et le premier suffixe DNS de la liste de recherche DNS au nom et transmet ensuite la requête DNS. Si le premier suffixe DNS de la liste est « company.com », la requête DNS résultante du routeur concerne le nom de domaine complet « quality.companyFully Qualified Domain Name (nom de domaine complet - FQDN).com ». Si la requête DNS échoue, le routeur ajoute le deuxième suffixe DNS de la liste au nom non qualifié et transmet une nouvelle requête DNS. Le routeur essaie les suffixes DNS jusqu'à ce qu'une recherche DNS réussisse (ignore les suffixes restants) ou jusqu'à ce que le routeur ait essayé tous les suffixes de la liste. Configurez le pare-feu avec les suffixes que vous souhaitez fournir au routeur client DNS dans une option DNSSL de découverte de voisin ; le client DNS recevant l'option DNSSL utilise les suffixes dans ses requêtes DNS non qualifiées. Entrez une **durée de vie** en secondes, qui est la durée maximale pendant laquelle le client peut utiliser la liste de recherche de domaine spécifique. La plage est comprise entre 4 et 3,600 ; la valeur par défaut est 1,200. Vous pouvez configurer un maximum de huit noms de domaine (suffixes) pour une liste de recherche DNS que le pare-feu envoie (dans l’ordre, de haut en bas) dans une publication de routeur NDP au destinataire, qui utilise ces adresses dans le même ordre. Sélectionnez un suffixe et utilisez les options **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)** pour modifier l’ordre des suffixes ou **Delete (Supprimer)** un suffixe de la liste lorsque vous n’en avez plus besoin.

Paramètres d'une interface de couche 3	Configuré dans	Description
État d'une interface SD-WAN	**Interface de couche 3** > **SD-WAN**	Si vous avez sélectionné **Enable SD-WAN (Activer SD-WAN)** dans l'onglet **IPv4**, le pare-feu indique `l'état de l'interface SD-WAN. Activé`. Si vous n'avez pas sélectionné **Enable SD-WAN (Activer SD-WAN)**, il indique `Disabled (Désactivé)`.
Profil d'interface SD-WAN		Sélectionnez un profil d'interface SD-WAN existant pour l'appliquer à cette interface Ethernet ou ajoutez un nouveau profil d'interface SD-WAN. *Vous devez **Enable SD-WAN (Activer SD-WAN)** pour l'interface avant que vous ne puissiez appliquer un profil d'interface SD-WAN.*
NAT en amont		Si votre plate-forme ou branche SD-WAN se trouve derrière un périphérique qui effectue un NAT, **Enable (Activez)** le NAT en amont pour cette plate-forme ou cette branche.
Type d'adresse IP NAT		Sélectionnez le type d'attribution d'adresse IP et indiquez l'adresse IP ou FQDN de l'interface publique sur ce périphérique effectuant le NAT ou indiquez que le DDNS dérive l'adresse. Ainsi, Auto VPN peut utiliser l'adresse comme terminal du tunnel de la plate-forme ou de la branche. • **Static IP (IP statique)** : Sélectionnez le **Type** qui sera **IP Address (Adresse IP)** ou **FQDN** et saisissez l'adresse IPv4 ou FQDN. • **DDNS** : le DNS dynamique (DDNS) dérive l'adresse IP du périphérique NAT en amont.
Vitesse de liaison	**Interface Ethernet** > **Avancé** > **Paramètres de lien**	Sélectionnez la vitesse de l'interface en Mbits/s ou sélectionnez **auto** pour que le pare-feu détermine automatiquement la vitesse.
Mode duplex de la liaison		Indiquez si le mode de transmission de l'interface est en duplex intégral (**full (intégral)**), semi-duplex (**half (semi)**) ou automatiquement négocié (**auto**).
état des liaisons		Indiquez si l'état de l'interface est activé (**up (actif)**), désactivé **down (inactif)**) ou automatiquement déterminé (**auto**).
PoE Rsvd Pwr	**Interface Ethernet** > **Avancé** >	Sélectionnez la quantité de puissance allouée en Watts si PoE est activé.
PoE activé		Sélectionnez pour activer PoE sur cette interface.

Paramètres d’une interface de couche 3	Configuré dans	Description
	Paramètres PoE (Supported firewalls only (Pare-feu pris en charge uniquement))	
Profil de gestion	**Interface de couche 3** > **Avancé** > **Autres infos**	Sélectionnez un profil de gestion qui définit les protocoles (par exemple, SSH, Telnet et HTTP) à utiliser pour gérer le pare-feu dans cette interface. Sélectionnez **None (Aucune)** pour supprimer l'affectation de profil de l'interface.
MTU		Saisissez l’unité de transmission maximale (MTU) en octets par paquet envoyé sur cette interface (plage de 576 à 9 192 ; par défaut 1 500). Si les machines situées de chaque côté du pare-feu effectuent une détection du chemin MTU (PMTUD) et que l'interface reçoit un paquet dépassant la valeur MTU, le pare-feu renvoie à la source un message de *fragmentation ICMP obligatoire* indiquant que le paquet est trop volumineux.
Ajuster TCP MSS		Sélectionnez pour ajuster la taille de segment maximale (MSS) afin de tolérer les octets de tous les en-têtes qui respectent la taille en octets de la MTU de l’interface. La taille en octets de la MTU moins la taille d'ajustement de la MSS équivaut à la taille en octets de la MSS, laquelle varie selon le protocole IP : • **IPv4 MSS Adjustment Size (Taille d'ajustement MSS IPv4)** - intervalle compris entre 40 et 300 ; valeur par défaut : 40. • **IPv6 MSS Adjustment Size (Taille d'ajustement MSS IPv4)** - intervalle compris entre 60 et 300 ; valeur par défaut : 60. Servez-vous de ces paramètres pour faire face aux situations où un **tunnel** réseau nécessite une plus petite MSS. Si un paquet a plus d'octets que la MSS sans faire l'objet d'une fragmentation, ce paramètre permet son ajustement. L'encapsulation rallonge les en-têtes. Il peut donc s'avérer utile de configurer la taille d'ajustement MSS de façon à autoriser les octets d'éléments tels que des en-têtes MPLS ou le trafic par tunnel ayant une étiquette VLAN.
Sous-interface non étiquetée		Sélectionnez cette option si les sous-interfaces correspondantes à cette interface ne sont pas étiquetées.

Paramètres d’une interface de couche 3	Configuré dans	Description
Adresse IP Adresse MAC	**Interface de couche 3** > **Avancé** > **Entrées ARP**	Pour ajouter une ou plusieurs entrées ARP (Address Resolution Protocol/protocole de résolution d’adresse) statiques, **Add (Ajoutez)** une adresse IP et son adresse matérielle associée (Media Access Control/commande d’accès au support ou MAC). Pour supprimer une entrée, sélectionnez-la et cliquez sur **Delete (Supprimer)**. Les entrées ARP statiques réduisent le traitement ARP.
Adresse IPv6 Adresse MAC	**Interface de couche 3** > **Avancé** > **Entrées ND**	Afin de fournir des informations de voisinage pour NDP (Neighbor Discovery Protocol/protocole de découverte des voisins), **Add (Ajoutez)** l'adresse IPv6 et l'adresse MAC du voisin.
Activer le proxy NDP	**Interface de couche 3** > **Avancé** > **Proxy NDP**	Activez le proxy NDP (Neighbor Discovery Protocol / protocole de découverte des voisins) sur l’interface. Le pare-feu répondra aux paquets ND demandant des adresses MAC pour les adresses IPv6 de cette liste. Dans la réponse ND, le pare-feu envoie sa propre adresse MAC pour l'interface de manière à recevoir les paquets destinés aux adresses de la liste. Il est recommandé d'activer le proxy NDP si vous utilisez NPTv6 (Network Prefix Translation IPv6). Si l'option **Enable NDP Proxy (Activer le proxy NDP)** est sélectionnée, vous pouvez filtrer de nombreuses entrées **Address (Adresse)** en saisissant un filtre et en cliquant sur Appliquer le filtre (la flèche grise).
Adresse		Vous devez **Add (Ajouter)** une ou plusieurs adresses IPv6, plages d’adresses IP, sous-réseaux IPv6 ou objets d’adresse pour lesquels le pare-feu agira comme proxy NDP. Idéalement, l'une de ces adresses est identique à celle de la traduction source dans NPTv6. L'ordre des adresses n'a pas d'importance. Si l'adresse est un sous-réseau, le pare-feu enverra une réponse ND pour toutes les adresses du sous-réseau. Par conséquent, il est recommandé d'ajouter également les voisins IPv6 du pare-feu et de cliquer sur **Negate (Ignorer)** pour que le pare-feu ne réponde pas à ces adresses IP.
Inverser		Sélectionnez **Negate (Ignorer)** une adresse afin d’empêcher le proxy NDP d’opérer sur cette adresse. Vous pouvez ignorer un sous-ensemble de la plage d'adresses IP ou du sous-réseau IP spécifié.
Activer LLDP	**Interface de couche 3** >	Sélectionnez cette option pour activer LLDP (Link Layer Discovery Protocol/protocole de découverte de couche liaison) sur

Paramètres d'une interface de couche 3	Configuré dans	Description
	Avancé > **LLDP**	l'interface. LLDP fonctionne sur la couche de liaison pour détecter les périphériques avoisinants et leurs fonctionnalités en envoyant des unités de données LLDP aux périphériques avoisinants et en recevant des unités de données LLDP de ceux-ci.
LLDP Profile (profil LLDP)		Sélectionnez un profil LLDP ou créez un nouveau LLDP Profile (profil LLDP). Le profil vous permet de configurer le mode LLDP, d'activer les notifications SNMP et Syslog, ainsi que de configurer les éléments TLV (Type-Longueur-Valeur) que vous souhaitez transmettre aux homologues LLDP.
Paramètres	**Interface de couche 3** > **Avancé** > **DDNS**	Sélectionnez **Settings (Paramètres)** pour que les champs DDNS puissent être configurés.
Activer		Activer DDNS sur l'interface Vous devez d'abord activer DDNS pour le configurer. (Si vous n'avez pas terminé de configurer DDNS, vous pouvez enregistrer la configuration sans l'activer, ce qui vous évitera de perdre la configuration partielle.)
Intervalle de mise à jour (jours)		Saisissez l'intervalle (en jours) entre les mises à jour que le pare-feu envoie au serveur DDNS pour mettre à jour les adresses IP associées aux FQDN (la plage est comprise entre 1 et 30 ; la valeur par défaut est 1). *Le pare-feu met également à jour DDNS à la réception d'une nouvelle adresse IP pour l'interface du serveur DHCP.*
Profil du certificat		Créez un profil de certificat pour vérifier le service DDNS. Le service DDNS présente au pare-feu un certificat signé par l'autorité de certification (CA).
Nom d'hôte		Saisissez un nom d'hôte pour l'interface, qui est inscrit auprès du serveur DDNS (par exemple, hôte123.domaine123.com ou hôte123). Le pare-feu ne valide pas le nom d'hôte, sauf pour confirmer que la syntaxe utilise les caractères valides autorisés par DNS pour un nom de domaine.
Constructeur	**Interface de couche 3** > **Avancé** > **DDNS**	Sélectionnez le fournisseur DDNS (et la version) qui fournit un service DDNS à cette interface : • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1**

Paramètres d’une interface de couche 3	Configuré dans	Description
		• **Free DNS Afraid.org v1** • **No-IP v1** • **Palo Alto Networks DDNS** (s'applique au SD-WAN Full Mesh avec DDNS, aux sous-interfaces SD-WAN AE et aux sous-interfaces SD-WAN Couche 3) *Si vous sélectionnez une version antérieure d’un service DDNS qui, selon le pare-feu, sera supprimée avant une date donnée, passez à la nouvelle version.* Les champs **Name (Nom)** et **Value (Valeur)** qui suivant le nom du fournisseur sont propres au fournisseur. Les champs en lecture seule vous avisent des paramètres que le pare-feu utilise pour se connecter au service DDNS. Configurez les autres champs, comme un mot de passe que le service DDNS vous fournit et le délai que le pare-feu utilise s’il ne reçoit pas de réponse du service DDNS.
Onglet IPv4		Ajoutez les adresses IPv4 configurées sur l’interface, puis sélectionnez-les. Vous pouvez sélectionner le nombre d’adresses IPv4 que le fournisseur DDNS permet. Toutes les adresses IP sélectionnées sont inscrites auprès du fournisseur DDNS.
Onglet IPv6		Ajoutez les adresses IPv6 configurées sur l’interface, puis sélectionnez-les. Vous pouvez sélectionner le nombre d’adresses IPv6 que le fournisseur DDNS permet. Toutes les adresses IP sélectionnées sont inscrites auprès du fournisseur DDNS.
Show Runtime Info		Affiche l’inscription DDNS : fournisseur DDNS, FQDN résolu et les adresses IP mappées avec un astérisque (*) indiquant l'adresse IP principale. Chaque fournisseur DDNS possède ses propres codes de retour pour indiquer l’état de la mise à jour du nom d’hôte et une date de retour à des fins de résolution de problèmes.

Sous-interface de couche 3

- Réseau > Interfaces > Ethernet

Vous pouvez définir des interfaces logiques de couche 3 (sous-interfaces) supplémentaires pour chaque port Ethernet configuré comme interface physique de couche 3. Vous pouvez créer une sous-interface de couche 3 pour un client PPPoE pour VLAN IEEE 802.1Q lorsque votre FAI utilise une balise VLAN 802.1Q sur une sous-interface PPPoE.

Vous pouvez également configurer des sous-interfaces de couche 3 pour une interface SD-WAN AE. Créez un groupe d'interfaces SD WAN AE, sélectionnez le groupe et **Add Subinterface (ajoutez une sous-interface)**, puis spécifiez les informations suivantes.

Pour configurer une Interface de niveau 3 de la série PA-7000, sélectionnez une interface physique, puis cliquez sur **Add Subinterface (Ajouter une sous-interface)** et indiquez les informations suivantes.

Paramètres d'une sous-interface de niveau 3	Configuré dans	Description
Nom de l'interface	**Sous-interface de couche 3**	Le champ **Interface Name (Nom de l'interface)** en lecture seule affiche le nom de l'interface physique sélectionnée. Dans le champ adjacent, saisissez un suffixe numérique (1 à 9 999) pour identifier la sous-interface.
Commentaire		Saisissez une description de la sous-interface (facultatif).
Étiquette		Saisissez l'étiquette VLAN (1 à 4 094) de la sous-interface. Pour faciliter l'utilisation, utilisez le même numéro que le suffixe numérique pour le nom de l'interface.
profil NetFlow ;		Si vous souhaitez exporter le trafic IP unidirectionnel traversant une sous-interface d'entrée vers un serveur NetFlow, sélectionnez le profil de serveur ou cliquez sur **Profil NetFlow** pour définir un nouveau profil (voir Périphérique > Profils de serveur > NetFlow). Sélectionnez **None (Aucun)** pour supprimer l'affectation de serveur NetFlow de la sous-interface.
routeur virtuel - VR	**Sous-interface de couche 3** > **Configuration**	Affectez un routeur virtuel à l'interface ou cliquez sur **Virtual Router (Routeur virtuel)** pour en définir un nouveau (voir Réseau > Routeurs virtuels). Sélectionnez **None (Aucun)** pour supprimer l'affectation de routeur virtuel de l'interface.
Virtual System (système virtuel - vsys)		Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système virtuel pour la sous-interface ou cliquez sur **Virtual System (Système virtuel)** pour en définir un nouveau.
Zone de sécurité		Sélectionnez une zone de sécurité pour la sous-interface ou cliquez sur **Zone** pour en définir une nouvelle. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de la sous-interface.
Activer SD-WAN	**Sous-interface de couche 3** > **IPv4**	Sélectionnez cette option pour activer SD-WAN sur la sous-interface de couche 3 pour une interface de couche 3 ou un groupe d'interfaces SD-WAN AE.

Paramètres d’une sous-interface de niveau 3	Configuré dans	Description
Activer Bonjour Reflector		(séries PA-220, PA-800 et PA-3200 uniquement) Lorsque vous activez cette option, le pare-feu transfère les alertes et les requêtes multicast Bonjour reçues et transférées à cette interface aux autres interfaces et sous-interfaces L3 et AE lorsque vous activez cette option. Cela aide à garantir l’accès utilisateur et la découverte du périphérique sur les environnements de réseau qui utilisent la segmentation pour acheminer le trafic pour des besoins de sécurité ou administratifs. Vous pouvez activer cette option sur un maximum de 16 interfaces.
Type		Sélectionnez la méthode d'attribution d'une adresse IPv4 à la sous-interface : • **Static (Statique)** : vous devez **Add (ajouter)** manuellement l'adresse **IP** et le masque de sous-réseau et saisir la **Next Hop Gateway (passerelle du tronçon suivant)**. • **PPPoE** — Permet à la sous-interface d’agir comme un client PPPoE (Point-to-Point Protocol over Ethernet) et de recevoir son adresse IPv4 du FAI, ainsi que d’autres informations, telles que l’adresse IP du serveur, les informations DNS et le MTU. • **DHCP Client (Client DHCP)** - Permet à la sous-interface d'agir en tant que client DHCP (Dynamic Host Configuration Protocol) et de recevoir une adresse IP assignée de façon dynamique. *Les pare-feu en mode haute disponibilité (HD) active/active ne prennent pas en charge le client DHCP.* Les options affichées dans l'onglet varient selon le choix de la méthode de sélection d'adresse IP.
Adresse IP	**Sous-interface de couche 3** > **IPv4, Type = Statique**	Cliquez sur **Add (Ajouter)** et suivez l’une des étapes ci-dessous pour indiquer une adresse IP statique et un masque réseau de l’interface. • Saisissez l’entrée en notation CIDR (Classing Inter-Domain Routing, routage inter-domaine sans classes) : *adresse_ip/masque* (par exemple, 192.168.2.0/24). • Sélectionnez un objet d'adresse existant de type **IP netmask (Masque réseau IP)**. • Créez un objet d’**Address (Adresse)** de type **IP netmask (Masque réseau IP)**.

Paramètres d’une sous-interface de niveau 3	Configuré dans	Description
		Vous pouvez saisir plusieurs adresses IP pour l'interface. La base d'informations de transfert (FIB) utilisée par votre système détermine le nombre maximum d'adresses IP. Il est possible de **Supprimer** une adresse IP lorsque vous n’en avez plus besoin.
Activer	**Sous-interface de couche 3 > IPv4, Type = PPPoE > Général**	Activez la sous-interface PPPoE.
Nom d’utilisateur	**Sous-interface de couche 3 > IPv4, Type = PPPoE > Général**	Entrez le nom d'utilisateur correspondant au type d'authentification que vous allez sélectionner.
Mot de passe	**Sous-interface de couche 3 > IPv4, Type = PPPoE > Général**	Entrez le mot de passe correspondant au type d'authentification que vous sélectionnerez, puis **Confirm Password (Confirmez le mot de passe)**.
Authentification	**Sous-interface de couche 3 > IPv4, Type = PPPoE > Avancé**	Sélectionnez le type d'authentification pour la sous-interface PPPoE: • **None (Aucune)** (par défaut) Si None est sélectionné, le pare-feu utilise l'authentification **auto (automatique)**. • **CHAP** : le pare-feu utilise le protocole CHAP (Challenge Handshake Authentication Protocol). • **PAP** : le pare-feu utilise le protocole PAP(Password Authentication Protocol). Le PAP envoie les noms d’utilisateur et les mots de passe en texte brut et est moins sécuritaire que le CHAP. • **auto** - Le pare-feu négocie la méthode d’authentification (CHAP ou PAP) avec le serveur PPPoE.
Adresse statique	**Sous-interface de couche 3 > IPv4, Type = PPPoE > Avancé**	Spécifiez une adresse statique pour demander que le serveur PPPoE attribue cette adresse IPv4 à la sous-interface. (Le serveur PPPoE peut attribuer l’adresse demandée ou une adresse différente à sa discrétion.) Valeur par défaut : **Aucune**.

Paramètres d’une sous-interface de niveau 3	Configuré dans	Description
Créer automatiquement un itinéraire par défaut en direction de l’homologue	**Sous-interface de couche 3** > **IPv4, Type = PPPoE** > **Avancé**	Crée un itinéraire par défaut qui pointe vers la passerelle par défaut que le serveur PPPoE fournit.
Mesure d'itinéraire par défaut	**Sous-interface de couche 3** > **IPv4, Type = PPPoE** > **Avancé**	Entrez la métrique d’itinéraire par défaut (niveau de priorité) de la connexion PPPoE; la plage est de 1 à 65 535; la valeur par défaut est 10. Plus la valeur de l'itinéraire est faible, plus sa priorité de sélection est élevée. Par exemple, un itinéraire avec une valeur de mesure de 10 est utilisé avant un itinéraire avec une valeur de mesure de 100.
Accéder au concentrateur	**Sous-interface de couche 3** > **IPv4, Type = PPPoE** > **Avancé**	Entrez le nom du concentrateur d'accès que votre FAI a fourni, le cas échéant (valeur de chaîne de 0 à 255 caractères). Le pare-feu se connectera à ce concentrateur d’accès du côté de l’IPS.
Service	**Sous-interface de couche 3** > **IPv4, Type = PPPoE** > **Avancé**	Entrez le Service fourni par votre FAI, le cas échéant (valeur de chaîne de 0 à 255 caractères).
Passif	**Sous-interface de couche 3** > **IPv4, Type = PPPoE** > **Avancé**	Si vous souhaitez que le client PPPoE (pare-feu) attende que le serveur PPPoE initie une connexion, sélectionnez Passif. Si l’option Passif n’est pas sélectionnée, le pare-feu est autorisé à établir une connexion.
Activer	**Sous-interface de couche 3** > **IPv4, type = DHCP**	Sélectionnez pour activer le client DHCP sur l’interface.
Créer automatiquement un itinéraire par défaut en direction de la passerelle par défaut fournie par le serveur		Sélectionnez pour créer automatiquement un itinéraire par défaut pointant vers la passerelle par défaut fournie par le serveur DHCP.
Envoyer le nom d'hôte		Choisissez si le pare-feu (en tant que client DHCP) doit envoyer le nom d’hôte de l’interface (option 12) au serveur DHCP. Si vous envoyez un nom d'hôte, par défaut, le nom d’hôte du pare-feu est alors le choix indiqué dans le

Paramètres d’une sous-interface de niveau 3	Configuré dans	Description
		champ Nom d'hôte par défaut. Vous pouvez envoyer ce nom ou saisir un nom d’hôte personnalisé (64 caractères maximum, y compris des lettres majuscules ou minuscules, des chiffres, des points, des tirets et des traits de soulignement).
Mesure d'itinéraire par défaut		(Facultatif) Pour l'itinéraire entre le pare-feu et le fournisseur de serveur DHCP, vous pouvez saisir une mesure d'itinéraire (un niveau de priorité) à associer à l'itinéraire par défaut et à utiliser pour la sélection du chemin (intervalle compris entre 1 et 65 535 ; il n'y a aucune valeur par défaut). Plus la valeur numérique est grande, plus le niveau de priorité est élevé.
Afficher les informations d'exécution du client DHCP		Sélectionnez **Show DHCP Client Runtime Info (Afficher les informations d'exécution du client DHCP)** pour afficher tous les paramètres reçus par le serveur DHCP, y compris le statut du bail DHCP, l'attribution de l'adresse IP dynamique, le masque de sous-réseau, la passerelle, les paramètres du serveur (DNS, NTP, domaine, WINS, NIS, POP3 et SMTP).
Activer IPv6 sur l'interface	**Sous-interface de couche 3** > **IPv6**	Sélectionnez pour activer l’adressage IPv6 sur cette interface.
ID de l'interface		Saisissez l'identifiant unique étendu sur 64'A0;bits (EUI-64) au format hexadécimal (par exemple, 00:26:08:FF:FE:DE:4E:29). Si ce champ n'est pas renseigné, le pare-feu utilise l'identifiant unique étendu sur 64'A0;bits (EUI-64) généré à partir de l'adresse MAC de l'interface physique. Si vous activez l'option **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** lors de l'ajout d'une adresse, le pare-feu utilise l'ID de l'interface comme partie hôte de l'adresse.
Type		Sélectionnez le type d'adresse IPv6: **Static (Statique)**, **DHCPv6 Client (client DHCPv6)** ou **Inherited (hérité)**.
Adresse	**Sous-interface de couche 3** > **IPv6** > **Attribution d'adresse, type = statique**	**Add (Ajoutez)** une adresse IPv6 et une longueur de préfixe (par exemple, 2001:400:f00::1/64). Vous pouvez également sélectionner un objet d'adresse IPv6 ou créer un nouvel objet d'adresse.
Activer l’adresse sur l’interface		Sélectionnez pour activer l’adresse IPv6 sur l’interface.
Utiliser l’ID de l’interface comme partie hôte.		Sélectionnez cette option pour utiliser l’**ID de l’interface** comme partie hôte de l’adresse IPv6.

Paramètres d’une sous-interface de niveau 3	Configuré dans	Description
Anycast		Sélectionnez cette option pour inclure le routage via le nœud le plus proche.
Envoyer la publication des routeurs	**Sous-interface de couche 3** > **IPv6** > **Attribution d'adresse, type = statique**	Sélectionnez cette option pour activer la publication de routeur (RA) pour cette adresse IP. (Vous devez également **Enable Router Advertisement (activer les annonces du router)** sur l’interface. Pour plus d’informations sur la RA, reportez-vous à la section Activer la publication de routeur dans ce tableau. Les champs restants s'appliquent si vous **Send Router Advertisement (envoyez une annonce de router)**. • **Valid Lifetime (Durée de vie valide) (sec)** - La durée, en secondes, pendant laquelle le pare-feu considère l’adresse comme valide. La durée de vie valide doit être supérieure ou égale à **Preferred Lifetime (durée de vie préférée)**. La valeur par défaut est 2 592 000. • **Preferred Lifetime (Durée de vie préférée) (sec)** - La durée, en secondes, pendant laquelle l’adresse valide est préférée, ce qui signifie que le pare-feu peut l’utiliser pour envoyer et recevoir du trafic. Lorsque la durée de vie préférée expire, le pare-feu ne peut plus utiliser l'adresse pour établir de nouvelles connexions, mais toute connexion existante reste valide jusqu'à ce que la **Valid Lifetime (Durée de vie valide)** expire. Par défaut, 604,800. • **On-link (Sur la liaison)** - Sélectionnez si les systèmes qui disposent d’adresses dans le préfixe sont accessibles sans routeur. • **Autonomous (Autonome)** - Sélectionnez cette option si les systèmes peuvent créer une adresse IP de façon indépendante en combinant le préfixe publié et l’ID d’une interface.
Accepter l'itinéraire annoncé par le routeur	**Sous-interface de couche 3** > **IPv6** > **Attribution d'adresse, Type = Client DHCPv6**	Sélectionnez cette option pour autoriser le client DHCPv6 à accepter le RA du serveur DHCPv6.
Mesure d'itinéraire par défaut		Saisissez une métrique de route par défaut pour la route entre l'interface et le FAI ; la plage est de 1 à 65 535 ; la valeur par défaut est 10.
Préférence		Sélectionnez la préférence de l'interface client DHCPv6 (**low (faible)**, **medium (moyen)**ou **high (élevé)**) de sorte que, dans le cas où vous avez deux interfaces (chacune étant connectée à un FAI différent pour la redondance), vous puissiez attribuer à

Paramètres d'une sous-interface de niveau 3	Configuré dans	Description
		l'un des FAI une préférence plus élevée que la l'interface avec l'autre FAI. Le FAI connecté à l'interface préférée sera le FAI qui fournit le préfixe délégué à envoyer à une interface faisant face à l'hôte. Si les interfaces ont la même préférence, les deux FAI fournissent un préfixe délégué et l'hôte décide quel préfixe utiliser.
Activer l'adresse IPv6	**Sous-interface de couche 3** > **IPv6** > **Attribution d'adresse, Type = Client DHCPv6** > **Options DHCPv6**	Activez l'adresse IPv6 reçue pour ce client DHCPv6.
Adresse non temporaire		Demandez une adresse non temporaire que le pare-feu doit attribuer à cette interface client DHCPv6 qui fait face au routeur délégant et au FAI. Une adresse non temporaire a une durée de vie plus longue qu'une adresse temporaire. Une adresse non temporaire peut être renouvelée. *Que vous demandiez une adresse non temporaire ou une adresse temporaire pour l'interface dépend de votre discrétion et de la capacité du serveur DHCPv6; certains serveurs ne peuvent fournir qu'une adresse temporaire. La meilleure pratique consiste à sélectionner à la fois Adresse non temporaire et Adresse temporaire, auquel cas le pare-feu préférera l'Adresse non temporaire.*
Adresse temporaire		Demandez une adresse temporaire que le pare-feu doit attribuer à cette interface client DHCPv6 qui fait face au routeur délégant et au FAI. Sélectionnez Adresse temporaire pour un niveau de sécurité supérieur, car l'adresse est destinée à être utilisée pendant une courte période. Une adresse temporaire peut être renouvelée ou non.
Validation rapide		Sélectionnez cette option pour utiliser le processus DHCP des messages Solliciter et Répondre, plutôt que le processus des messages Solliciter, Annoncer, Demander et Répondre.
Activer la délégation de préfixe	**Sous-interface de couche 3** > **IPv6** > **Attribution d'adresse, Type = Client DHCPv6** >	Activez la délégation de préfixe pour permettre au pare-feu de prendre en charge la fonctionnalité de délégation de préfixe. Cela signifie que l'interface accepte un préfixe du serveur DHCPv6 en amont et place le préfixe dans le pool de préfixes que vous sélectionnez, à partir duquel le pare-feu délègue un préfixe à un hôte via RA. La possibilité d'activer ou de désactiver la délégation de préfixe pour une interface permet au pare-feu de prendre en charge plusieurs FAI (un FAI par

Paramètres d’une sous-interface de niveau 3	Configuré dans	Description
	Délégation de préfixe	interface). L'activation de la délégation de préfixe sur cette interface contrôle quel FAI fournit le préfixe.
Conseil sur la longueur du préfixe DHCP		Sélectionnez pour permettre au pare-feu d'envoyer une longueur de préfixe DHCPv6 préférée au serveur DHCPv6.
Longueur du préfixe DHCP (bits)		Entrez la longueur de préfixe DHCPv6 préférée dans la plage de 48 à 64 bits, qui est envoyée comme indice au serveur DHCPv6. *Demander une longueur de préfixe de 48, par exemple, laisse 16 bits restants pour les sous-réseaux (64-48), ce qui indique que vous avez besoin de nombreuses subdivisions de ce préfixe pour déléguer. D'autre part, demander une longueur de préfixe de 63 laisse 1 bit pour ne déléguer que deux sous-réseaux. Sur les 128 bits, il reste encore 64 bits pour l'adresse de l'hôte.*
Préfixe Nom du pool		Saisissez un nom pour le pool de préfixes dans lequel le pare-feu stocke le préfixe reçu. Le nom doit être unique et contenir un maximum de 63 caractères alphanumériques, traits d'union, points et traits de soulignement. *Utilisez un nom de pool de préfixes qui reflète le FAI pour une reconnaissance facile.*
Nom	**Sous-interface de couche 3 > IPv6 > Attribution d'adresse, type = hérité**	**Add (Ajoutez)** un pool en saisissant un nom de pool. Le nom peut comporter au maximum 63 caractères alphanumériques, traits d'union, points et traits de soulignement.
Type d'adresse		Sélectionnez parmi les choix suivants : • **GUA from pool (AUG du pool)**— Adresse Unidiffusion globale (AUG) provenant du pool de préfixes choisi. • **ULA**—Unique Local Address est une adresse privée dans la plage d'adresses fc00::/7 pour la connectivité au sein d'un réseau privé. Sélectionnez ULA s'il n'y a pas de serveur DHCPv6.
Activer sur l'interface		Activez l’adresse IPv6 sur l’interface.

Paramètres d’une sous-interface de niveau 3	Configuré dans	Description
Pool de préfixes		Sélectionnez le pool de préfixes à partir duquel obtenir le GUA.
Assignment Type (Type d'affectation)	**Sous-interface de couche 3** > **IPv6** > **Attribution d'adresse, type = hérité**	Sélectionnez le type de devoir : • **Dynamic (Dynamique)** — Le client DHCPv6 est responsable du choix d'un identifiant pour configurer l'interface héritée. • **Dynamic with Identifier (Dynamique avec identifiant)**— Vous êtes responsable du choix d'un identifiant dans la plage de 0 à 4 000 et de la gestion d'un identifiant unique sur les clients DHCPv6.
Envoyer la publication des routeurs		Sélectionnez pour envoyer des annonces de routeur (AR) de l'interface aux hôtes LAN.
On-Link		Sélectionnez si les systèmes qui disposent d’adresses dans le préfixe sont accessibles sans routeur.
Autonome		Sélectionnez cette option si les systèmes peuvent créer une adresse IP de façon indépendante en combinant le préfixe publié et l’ID d’une interface.
Activer la détection des doublons d'adresses	**Sous-interface de couche 3** > **IPv6** > **Résolution d’adresses**	Sélectionnez pour activer la Détection des doublons d’adresses (DAD) puis configurez les autres champs de cette section.
Tentatives DAD		Indiquez le nombre de tentatives DAD dans l'intervalle de sollicitation de voisins (**NS Interval (intervalle NS)**) avant que la tentative d'identification n'échoue (intervalle compris entre 1 et 10 ; valeur par défaut : 1).
Durée d'accessibilité (s)		Spécifiez la durée, en secondes, que le client utilisera pour supposer qu'un voisin est joignable après avoir reçu un message de confirmation d'accessibilité (la plage est de 10 à 36 000; la valeur par défaut est de 30).
Intervalle (s)		Spécifiez l'intervalle de sollicitation des voisins (NS), qui est le nombre de secondes pour les tentatives de DAD avant que l'échec ne soit indiqué (la plage est de 1 à 3 600; par défaut est 1).

Paramètres d’une sous-interface de niveau 3	Configuré dans	Description
Activer la surveillance NDP		Sélectionnez pour activer la surveillance du Protocole de découverte des voisins (NDP). Lorsque cela est activé, vous pouvez sélectionner NDP ( dans la colonne Caractéristiques) pour visualiser des informations sur un voisin détecté par le pare-feu, comme l’adresse IPv6, l’adresse MAC correspondante et l’User-ID (dans le meilleur des cas).
Activer la publication des routeurs	**Sous-interface de couche 3** > **IPv6** > **Annonce de routeur, Type = Statique ou Type = Hérité**	Pour assurer la Découverte des voisins sur les interfaces IPv6, sélectionnez et configurez les autres champs de cette section. Les clients DNS IPv6 qui reçoivent les messages de publication de routeur utilisent ces informations. La RA permet au pare-feu d'agir en tant que passerelle par défaut pour les hôtes IPv6 qui ne sont pas configurés de façon statique et de fournir à l'hôte un préfixe IPv6 qui lui permet de configurer une adresse. Vous pouvez utiliser un serveur DHCPv6 distinct conjointement avec cette fonctionnalité pour fournir un DNS et d'autres paramètres aux clients. Il s’agit d’un paramètre global de l’interface. Si vous souhaitez définir des options de publication de routeur (RA) pour les adresses IP individuelles, il vous faut **Ajouter** et configurer une Adresse dans la table d’adresses IP. Si vous définissez des options de publication de routeur pour une adresse IP, vous devez **nable Router Advertisement (Activer la publication de routeur)** sur l’interface.
Intervalle min. (s)		Indiquez l’intervalle minimum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 3 et 1 350 ; valeur par défaut : 200). Le pare-feu envoie les publications de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales configurées.
Intervalle max. (s)		Indiquez l’intervalle maximum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 4 et 1 800 ; valeur par défaut : 600). Le pare-feu envoie les publications de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales configurées.
Limite de saut		Indiquez la limite de saut à appliquer aux clients pour les paquets sortants (intervalle compris entre 1 et 255 ; valeur par défaut : 64). Saisissez 0 pour indiquer l’absence de limite de saut.

Paramètres d'une sous-interface de niveau 3	Configuré dans	Description
MTU de liaison		Indiquez l'unité de transmission maximale (MTU) de liaison à appliquer aux clients. Sélectionnez **unspecified (non spécifiée)** pour indiquer l'absence de MTU de liaison (intervalle compris entre 1 280 et 9 192 ; valeur par défaut : non spécifiée).
Durée d'accessibilité (ms)		Indiquez la durée d'accessibilité (en millisecondes) que le client va utiliser pour supposer l'accessibilité d'un voisin après avoir reçu un message de confirmation d'accessibilité. Sélectionnez **unspecified (non spécifiée)** pour indiquer l'absence de valeur pour la durée d'accessibilité (intervalle compris entre 0 et 3 600 000 ; valeur par défaut : non spécifiée).
Durée de retransmission (ms)		Indiquez le minuteur de retransmission qui détermine la durée d'attente du client (en millisecondes) avant la retransmission des messages de sollicitation de voisins. Sélectionnez **unspecified (non spécifiée)** pour indiquer l'absence de valeur pour la durée de retransmission (intervalle compris entre 0 et 4 294 967 295 ; valeur par défaut : non spécifiée).
Durée de vie du routeur (s)		Indiquez la durée, en secondes, pendant laquelle le client utilise le pare-feu comme passerelle par défaut (plage comprise entre 0 et 9 000 ; valeur par défaut : 1 800). Une valeur de 0 indique que le pare-feu n'est pas la passerelle par défaut. Lorsque la durée de vie expire, le client supprime l'entrée du pare-feu de sa liste de routeurs par défaut et utilise un autre routeur comme passerelle par défaut.
Préférence de routeur		Si le segment de réseau dispose de plusieurs routeurs IPv6, le client utilise ce champ pour sélectionner un routeur préféré. Indiquez si le routeur de pare-feu publié a une priorité **High (Élevée)**, **Medium (Moyenne)** (par défaut) ou **Low (Faible)** par rapport aux autres routeurs se trouvant sur le segment.
Configuration gérée		Sélectionnez cette option pour indiquer au client que les adresses sont disponibles via DHCPv6.
Autre configuration		Sélectionnez pour indiquer au client que d'autres informations d'adresse (par exemple, des paramètres associés au DNS) sont disponibles via DHCPv6.
Préférence de routeur	**Sous-interface de couche 3** > **IPv6** > **Annonce de routeur, Type**	Définissez la préférence du routeur au cas où il y aurait deux interfaces ou plus sur des routeurs différents envoyant des RA à un hôte. **Élevé**, **Moyen** ou **Bas** est la priorité que l'AR

Paramètres d’une sous-interface de niveau 3	Configuré dans	Description
	= Statique ou Type = Hérité	annonce indiquant la priorité relative et l'hôte utilise le préfixe du routeur à priorité plus élevée.
Configuration gérée		Sélectionnez cette option pour indiquer au client que les adresses sont disponibles via DHCPv6.
Autre configuration		Sélectionnez cette option pour indiquer au client que d’autres informations d’adresse (comme les paramètres associés au DNS) sont disponibles via DHCPv6.
Vérification de cohérence		Sélectionnez si vous souhaitez que le pare-feu vérifie que les RA reçues des autres routeurs publient des informations cohérentes sur la liaison. Le pare-feu consigne toutes les incohérences dans un journal système de type **Ipv6nd**.
Inclure les informations DNS dans la publication de routeur	**Sous-interface de couche 3** > **IPv6** > **Prise en charge DNS, Type = Statique**	Sélectionnez le pare-feu pour transmettre des informations DNS vers les publications du routeur NDP à partir de cette sous-interface Ethernet IPv6. Les autres champs de Prise en charge DNS de ce tableau ne sont visibles qu’après sélection de cette option.
Serveur		Il est possible d’**Ajouter** une ou plusieurs adresses de serveur DNS (RDNS) récursives pour que le pare-feu envoie des publications de routeur NDP à partir de cette interface Ethernet IPv6. Les serveurs RDNS envoient une série de demandes de recherche DNS aux serveurs DNS racine et aux serveurs DNS autoritaires pour finalement fournir une adresse IP au client DNS. Vous pouvez configurer un maximum de huit Serveurs RDNS que le pare-feu envoie (dans l’ordre de haut en bas) dans une publication de routeur NDP au destinataire, qui les utilise ensuite dans le même ordre. Vous devez sélectionner un serveur et **Déplacer en haut** ou **Déplacer en bas** pour modifier l’ordre des serveurs ou **Supprimer** un serveur de la liste lorsque vous n’en avez plus besoin.
Durée de vie		Saisissez le nombre maximum de secondes après que le client DNS IPv6 a reçu la publication du routeur avant que le client puisse utiliser un serveur RDNS afin de résoudre les noms de domaine (la plage est la valeur d’Intervalle max. (sec) jusqu’à deux fois l’intervalle maximal, la valeur par défaut est de 1 200).

Paramètres d’une sous-interface de niveau 3	Configuré dans	Description
Liste de recherche de domaine	**Sous-interface de couche 3** > **IPv6** > **Prise en charge DNS, Type = Statique**	Il vous faut **ajouter** un ou plusieurs noms de domaine (suffixes) pour la liste de recherche DNS (DNSSL). 255 octets maximum. Une liste de recherche DNS est une liste de suffixes de domaine qu’un routeur de client DNS ajoute (un à la fois) à un nom de domaine non qualifié avant d’entrer le nom dans une requête DNS, en utilisant un nom de domaine complet dans la requête. Par exemple, si un client DNS essaie de soumettre une requête DNS pour le nom « qualité » sans suffixe, le routeur ajoute un point et le premier suffixe DNS de la liste de recherche DNS au nom et transmet la requête DNS. Si le premier suffixe DNS sur la liste est « company.com », la requête qui résulte du routeur est « quality.company.com » pour le nom de domaine complet. Si la requête DNS échoue, le routeur ajoute le deuxième suffixe DNS de la liste au nom non qualifié et transmet une nouvelle requête DNS. Le routeur utilise les suffixes DNS jusqu’à ce qu’une recherche DNS soit fructueuse (il ignore les suffixes restants) ou jusqu’à ce que le routeur ait essayé tous les suffixes de la liste. Configurez le pare-feu avec les suffixes que vous souhaitez fournir au routeur du client DNS dans une option Découverte de voisins DNSSL ; le client DNS recevant l’option DNSSL utilise les suffixes pour ses requêtes DNS non qualifiées. Vous pouvez configurer un maximum de huit noms de domaine (suffixes) pour une liste de recherche DNS que le pare-feu envoie (dans l’ordre, de haut en bas) dans une publication de routeur NDP au destinataire, qui les utilise dans le même ordre. Sélectionnez un suffixe et utilisez les options **Déplacer vers le haut** ou **Déplacer vers le bas** pour modifier l’ordre ou **Supprimer** un suffixe lorsque vous n’en avez plus besoin.
Durée de vie		Saisissez le nombre maximum de secondes qui s’est écoulé après réception de la publication du routeur par le client DNS IPv6. Celle-ci stipule qu’il est possible d’utiliser un nom de domaine (suffixe) sur la liste de recherche DNS (l’intervalle est la valeur de l’Intervalle max. [s] jusqu’à deux fois l'intervalle maximal ; la valeur par défaut est 1 200).
Serveur de noms récursif DNS	**Sous-interface de couche 3** > **IPv6** > **Prise en**	Activez et sélectionnez : • **DHCPv6**—Pour que le serveur DHCPv6 envoie les informations DNS Recursive Name Server.

Paramètres d’une sous-interface de niveau 3	Configuré dans	Description
	charge DNS, type = client DHCPv6 ou hérité	• **Manual (Manuel)** — Pour configurer manuellement le serveur de noms DNS Recursive. Si vous choisissez **Manuel**, **ajoutez** l'adresse IPv6 d'un **serveur** DNS récursif (RDNS) pour que le pare-feu envoie des publicités de routeurs NDP à partir de cette interface VLAN IPv6. Les serveurs RDNS envoient une série de requêtes de recherches DNS aux serveurs DNS racines et aux serveurs DNS fiables pour finalement fournir une adresse IP au client DNS. Vous pouvez configurer un maximum de huit serveurs RDNS que le pare-feu envoie (dans l’ordre indiqué, de haut en bas) dans une publication de routeur NDP au destinataire, qui les utilise ensuite dans le même ordre. Vous devez sélectionner un serveur et **Move up (Déplacer en haut)** ou **Move down (Déplacer en bas)** pour modifier l’ordre des serveurs ou **Delete (Supprimer)** un serveur de la liste lorsque vous n’en avez plus besoin. Indiquez la **Lifetime (Durée de vie)** en secondes. Il s'agit de la durée de temps maximale pendant laquelle le client peut utiliser le serveur RDNS donné pour résoudre des noms de domaine. La plage est comprise entre 4 et 3,600 ; la valeur par défaut est 1,200.
Liste de recherche de domaine	**Sous-interface de couche 3 > IPv6 > Prise en charge DNS, type = client DHCPv6 ou hérité**	Enable and select (Activez et sélectionnez) : • **DHCPv6**— Pour que le serveur DHCPv6 envoie les informations de la liste de recherche de domaine. • **Manual (manuel)**— Pour configurer manuellement la liste de recherche de domaine. Si vous choisissez **Manual (manuel)**, **Add (Ajoutez)** et configurez un ou plusieurs Noms de **Domain(domaine)** (suffixes) pour la liste de recherche DNS (DNSSL). La longueur maximale du suffixe est de 255 octets. Une liste de recherche DNS est une liste de suffixes de domaine qu’un routeur de client DNS ajoute (un à la fois) à un nom de domaine non qualifié avant d’entrer le nom dans une requête DNS, en utilisant un nom de domaine complet dans la requête DNS. Par exemple, si un client DNS essaie de soumettre une requête DNS pour le nom « qualité » sans suffixe, le routeur ajoute un point et le premier suffixe DNS de la liste de recherche DNS au nom et transmet ensuite la requête DNS. Si le premier suffixe DNS de la liste est « company.com », la requête DNS résultante du routeur concerne le nom de domaine complet « quality.companyFully Qualified Domain Name (nom de domaine complet - FQDN).com ».

Paramètres d’une sous-interface de niveau 3	Configuré dans	Description
		Si la requête DNS échoue, le routeur ajoute le deuxième suffixe DNS de la liste au nom non qualifié et transmet une nouvelle requête DNS. Le routeur essaie les suffixes DNS jusqu'à ce qu'une recherche DNS réussisse (ignore les suffixes restants) ou jusqu'à ce que le routeur ait essayé tous les suffixes de la liste. Configurez le pare-feu avec les suffixes que vous souhaitez fournir au routeur client DNS dans une option DNSSL de découverte de voisin ; le client DNS recevant l'option DNSSL utilise les suffixes dans ses requêtes DNS non qualifiées. Entrez une **durée de vie** en secondes, qui est la durée maximale pendant laquelle le client peut utiliser la liste de recherche de domaine spécifique. La plage est comprise entre 4 et 3,600 ; la valeur par défaut est 1,200. Vous pouvez configurer un maximum de huit noms de domaine (suffixes) pour une liste de recherche DNS que le pare-feu envoie (dans l’ordre, de haut en bas) dans une publication de routeur NDP au destinataire, qui utilise ces adresses dans le même ordre. Sélectionnez un suffixe et utilisez les options **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)** pour modifier l’ordre des suffixes ou **Delete (Supprimer)** un suffixe de la liste lorsque vous n’en avez plus besoin.
Profil d’interface SD-WAN	**Sous-interface de couche 3** > **SD-WAN**	Sélectionnez un profil d'interface SD-WAN à attribuer à cette sous-interface ou créez un nouveau profil.
Profil de gestion	**Sous-interface de couche 3** > **Avancé** > **Autre info**	**Management Profile (Profil de gestion)** - Sélectionnez un profil qui définit les protocoles (par exemple, SSH, Telnet et HTTP) à utiliser pour gérer le pare-feu dans cette interface. Sélectionnez **None (Aucune)** pour supprimer l'affectation de profil de l'interface.
MTU		Saisissez l’unité de transmission maximale (MTU) en octets par paquet envoyé sur cette interface (plage de 576 à 9 192 ; par défaut 1 500). Si les machines situées de chaque côté du pare-feu effectuent une détection du chemin MTU (PMTUD) et que l'interface reçoit un paquet dépassant la valeur MTU, le pare-feu renvoie à la source un message de *fragmentation ICMP obligatoire* indiquant que le paquet est trop volumineux.
Ajuster TCP MSS	**Sous-interface de couche 3**	Sélectionnez pour ajuster la taille de segment maximale (MSS) afin de tolérer les octets de tous les en-têtes qui respectent la taille en octets de la MTU de l’interface. La taille en octets de

Paramètres d’une sous-interface de niveau 3	Configuré dans	Description
	> **Avancé** > **Autre info**	la MTU moins la taille d'ajustement de la MSS équivaut à la taille en octets de la MSS, laquelle varie selon le protocole IP : • **IPv4 MSS Adjustment Size (Taille d'ajustement MSS IPv4)** - intervalle compris entre 40 et 300 ; valeur par défaut : 40. • **IPv6 MSS Adjustment Size (Taille d'ajustement MSS IPv4)** - intervalle compris entre 60 et 300 ; valeur par défaut : 60. Servez-vous de ces paramètres pour faire face aux situations où un **tunnel** réseau nécessite une plus petite MSS. Si un paquet a plus d'octets que la MSS sans faire l'objet d'une fragmentation, ce paramètre permet son ajustement. L'encapsulation rallonge les en-têtes. Il peut donc s'avérer utile de configurer la taille d'ajustement MSS de façon à autoriser les octets d'éléments tels que des en-têtes MPLS ou le trafic par tunnel ayant une étiquette VLAN.
Adresse IP Adresse MAC	**Sous-interface de couche 3** > **Avancé** > **Entrées ARP**	Pour ajouter une ou plusieurs entrées ARP (Address Resolution Protocol/protocole de résolution d’adresse) statiques, **Add (Ajoutez)** une adresse IP et son adresse matérielle associée (Media Access Control/commande d’accès au support ou MAC). Pour supprimer une entrée, sélectionnez-la et cliquez sur **Delete (Supprimer)**. Les entrées ARP statiques réduisent le traitement ARP.
Adresse IPv6 Adresse MAC	**Sous-interface de couche 3** > **Avancé** > **Entrées ND**	Afin de fournir des informations de voisinage pour NDP (Neighbor Discovery Protocol/protocole de découverte des voisins), **Add (Ajoutez)** l'adresse IP et l'adresse MAC du voisin.
Activer le proxy NDP	**Sous-interface de couche 3** > **Avancé** > **Proxy NDP**	Activez le proxy NDP (Neighbor Discovery Protocol / protocole de découverte des voisins) sur l’interface. Le pare-feu répondra aux paquets ND demandant des adresses MAC pour les adresses IPv6 de cette liste. Dans la réponse ND, le pare-feu envoie sa propre adresse MAC pour l'interface de manière à recevoir les paquets destinés aux adresses de la liste. Il est recommandé d'activer le proxy NDP si vous utilisez NPTv6 (Network Prefix Translation IPv6). Si l'option **Enable NDP Proxy (Activer le proxy NDP)** est sélectionnée, vous pouvez filtrer de nombreuses entrées **Address (Adresse)** en saisissant un filtre et en cliquant sur Appliquer le filtre (la flèche grise).

Paramètres d’une sous-interface de niveau 3	Configuré dans	Description
Adresse		Vous devez **Add (Ajouter)** une ou plusieurs adresses IPv6, plages d’adresses IP, sous-réseaux IPv6 ou objets d’adresse pour lesquels le pare-feu agira comme proxy NDP. Idéalement, l'une de ces adresses est identique à celle de la traduction source dans NPTv6. L'ordre des adresses n'a pas d'importance. Si l'adresse est un sous-réseau, le pare-feu enverra une réponse ND pour toutes les adresses du sous-réseau. Par conséquent, il est recommandé d'ajouter également les voisins IPv6 du pare-feu et de cliquer sur **Negate (Ignorer)** pour que le pare-feu ne réponde pas à ces adresses IP.
Inverser		Sélectionnez **Negate (Ignorer)** une adresse afin d’empêcher le proxy NDP d’opérer sur cette adresse. Vous pouvez ignorer un sous-ensemble de la plage d'adresses IP ou du sous-réseau IP spécifié.
Paramètres	**Sous-interface de couche 3** > **Avancé** > **DDNS**	Sélectionnez **Settings (Paramètres)** pour que les champs DDNS puissent être configurés.
Activer		Activer DDNS sur l'interface Vous devez d’abord activer DDNS pour le configurer. (Si vous n’avez pas terminé de configurer DDNS, vous pouvez enregistrer la configuration sans l'activer, ce qui vous évitera de perdre la configuration partielle.)
Intervalle de mise à jour (jours)	**Sous-interface de couche 3** > **Avancé** > **DDNS**	Saisissez l’intervalle (en jours) entre les mises à jour que le pare-feu envoie au serveur DDNS pour mettre à jour les adresses IP associées aux FQDN (la plage est comprise entre 1 et 30 ; la valeur par défaut est 1). *Le pare-feu met également à jour DDNS à la réception d’une nouvelle adresse IP pour l’interface du serveur DHCP.*
Profil du certificat		Créez un profil de certificat pour vérifier le service DDNS. Le service DDNS présente au pare-feu un certificat signé par l’autorité de certification (CA).
Nom d'hôte		Saisissez un nom d’hôte pour l’interface, qui est inscrit auprès du serveur DDNS (par exemple, hôte123.domaine123.com ou hôte123). Le pare-feu ne valide pas le nom d’hôte, sauf pour confirmer que la syntaxe utilise les caractères valides autorisés par DNS pour un nom de domaine.

Paramètres d’une sous-interface de niveau 3	Configuré dans	Description
Constructeur	**Sous-interface de couche 3** > **Avancé** > **DDNS**	Sélectionnez le fournisseur DDNS (et la version) qui fournit un service DDNS à cette interface : • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1** • **No-IP v1** • **Palo Alto Networks DDNS** : vous devez choisir ce fournisseur pour les sous-interfaces SD-WAN AE ou les sous-interfaces SD-WAN de couche 3.  *Si vous sélectionnez une version antérieure d’un service DDNS qui, selon le pare-feu, sera supprimée avant une date donnée, passez à la nouvelle version.* Les champs **Name (Nom)** et **Value (Valeur)** qui suivant le nom du fournisseur sont propres au fournisseur. Les champs en lecture seule vous avisent des paramètres que le pare-feu utilise pour se connecter au service DDNS. Configurez les autres champs, comme un mot de passe que le service DDNS vous fournit et le délai que le pare-feu utilise s’il ne reçoit pas de réponse du service DDNS.
Onglet IPv4 - IP		Ajoutez les adresses IPv4 configurées sur l’interface, puis sélectionnez-les. Vous pouvez sélectionner le nombre d’adresses IPv4 que le fournisseur DDNS permet. Toutes les adresses IP sélectionnées sont inscrites auprès du fournisseur DDNS.
Onglet IPv6 - IPv6		Ajoutez les adresses IPv6 configurées sur l’interface, puis sélectionnez-les. Vous pouvez sélectionner le nombre d’adresses IPv6 que le fournisseur DDNS permet. Toutes les adresses IP sélectionnées sont inscrites auprès du fournisseur DDNS.
Show Runtime Info	**Sous-interface de couche 3** > **Avancé** > **DDNS**	Affiche l’inscription DDNS : fournisseur DDNS, FQDN résolu et les adresses IP mappées avec un astérisque (*) indiquant l'adresse IP principale. Chaque fournisseur DDNS possède ses propres codes de retour pour indiquer l’état de la mise à jour du nom d’hôte et une date de retour à des fins de résolution de problèmes.

Interface de la carte des journaux

- Réseau > Interfaces > Ethernet

Si vous configurez le transfert des journaux sur un pare-feu de la série PA-7000 doté d'une carte de traitement des journaux (LPC), vous devez configurer un port de données comme type **Log Card (Carte des journaux)**. Vous devez effectuer cette action car les fonctions de trafic et de journalisation de ce modèle de pare-feu dépassent les fonctions de l'interface de gestion (MGT). Un port de données de carte de journal effectue le transfert des journaux pour Syslog, la messagerie, SNMP (Simple Network Management Protocol), le transfert des journaux Panorama et le transfert de fichiers WildFire™.

*Vous ne pouvez configurer qu'un seul port sur le pare-feu comme type **Log Card (Carte des journaux)**. Si vous activez le transfert des journaux mais ne configurez aucune interface avec le type de **Log Card (Carte des journaux)**, une erreur de validation se produit.*

Ces informations concernent la configuration d'une carte de traitement de journal (LPC). Pour savoir comment configurer une Carte de transfert des journaux (LFC), voir Périphérique > Carte de transfert des journaux

Pour configurer une interface de carte de journal, sélectionnez une interface non configurée (Ethernet1/16, par exemple) et configurez les paramètres décrits dans le tableau suivant.

Paramètres d'une interface de carte des journaux	Configuré dans	Description
Logement	**Interface Ethernet**	Sélectionnez le numéro de logement (1-12) de l'interface.
Nom de l'interface		Le nom de l'interface est prédéfini et vous ne pouvez pas le modifier.
Commentaire		Saisissez une description de l'interface (facultatif).
Type d'interface		Sélectionnez **Log Card (Carte des journaux)**.
IPv4	**Interface Ethernet** > **Transfert de carte de journal**	Si votre réseau utilise IPv4, définissez les options suivantes : • **IP address (Adresse IP)** - Adresse IPv4 du port. • **Netmask (Masque réseau)** - Masque réseau de l'adresse IPv4 du port. • **Default Gateway (Passerelle par défaut)** - Adresse IPv4 de la passerelle par défaut du port.
IPv6		Si votre réseau utilise IPv6, définissez les options suivantes : • **IP address (Adresse IP)** - Adresse IPv6 du port. • **Default Gateway (Passerelle par défaut)** - Adresse IPv6 de la passerelle par défaut du port.

Paramètres d'une interface de carte des journaux	Configuré dans	Description
Vitesse de liaison	**Interface Ethernet** > **Avancé**	Sélectionnez la vitesse de l'interface en Mbits/s (**10**, **100** ou **1000**) ou sélectionnez **Auto** (par défaut) pour que le pare-feu détermine automatiquement la vitesse en fonction de la connexion. **Auto** est la seule option possible pour les interfaces dont la vitesse ne peut être configurée. *La vitesse minimale recommandée pour la connexion est **1 000** (Mbits/s).*
Mode duplex de la liaison		Indiquez si le mode de transmission de l'interface est en duplex intégral (**full (intégral)**), semi-duplex (**half (semi)**) ou automatiquement négocié en fonction de la connexion (**auto**). La valeur par défaut est **auto**.
état des liaisons		Indiquez si l'état de l'interface est activé (**up (actif)**), désactivé **down (inactif)**) ou automatiquement déterminé en fonction de la connexion (**auto**). La valeur par défaut est **auto**.

Sous-interface de la carte des journaux

- Réseau > Interfaces > Ethernet

Pour ajouter Interface de la carte des journaux, sélectionnez la ligne pour cette interface, cliquez sur **Add Subinterface (Ajouter une sous-interface)** et spécifiez les informations suivantes.

Paramètres d'une sous-interface de carte des journaux	Configuré dans	Description
Nom de l'interface	**Sous-interface LPC**	**Nom de l'interface** (en lecture seule) affiche le nom de l'interface de carte de journal sélectionnée. Dans le champ adjacent, saisissez un suffixe numérique (1-9 999) pour identifier la sous-interface.
Commentaire		Saisissez une description de l'interface (facultatif).
Étiquette		Saisissez le **Tag (Étiquette)** VLAN (0-4 094) de la sous-interface. *Donnez à l'étiquette le même numéro que la sous-interface pour simplifier son utilisation.*

Paramètres d'une sous-interface de carte des journaux	Configuré dans	Description
Système virtuel	**Sous-interface LPC** > **Configuration**	Sélectionnez le système virtuel auquel la sous-interface LPC (Log Processing Card/carte de traitement des journaux) est affectée. Sinon, vous pouvez cliquer sur **Virtual Systems (Systèmes virtuels)** pour ajouter un nouveau système virtuel. Une fois qu'une sous-interface LPC est affectée à un système virtuel, cette interface est utilisée comme interface source pour tous les services qui transfèrent les journaux (Syslog, messagerie, SNMP) depuis la carte des journaux.
IPv4	**Interface Ethernet** > **Transfert de carte de journal**	Si votre réseau utilise IPv4, définissez les options suivantes : • **IP address (Adresse IP)** - Adresse IPv4 du port. • **Netmask (Masque réseau)** - Masque réseau de l'adresse IPv4 du port. • **Default Gateway (Passerelle par défaut)** - Adresse IPv4 de la passerelle par défaut du port.
IPv6		Si votre réseau utilise IPv6, définissez les options suivantes : • **IP address (Adresse IP)** - Adresse IPv6 du port. • **Default Gateway (Passerelle par défaut)** - Adresse IPv6 de la passerelle par défaut du port.

Interface miroir de déchiffrement

- Réseau > Interfaces > Ethernet

Pour pouvoir utiliser la fonction Mise en miroir du port de déchiffrement, vous devez sélectionner le type d'interface **Miroir de déchiffrement**. Cette fonction permet de créer une copie du trafic décrypté provenant d'un pare-feu et de l'envoyer à un outil de collecte du trafic, tel que NetWitness ou Solera, capable de recevoir des captures de paquets bruts, en vue de leur archivage et de leur analyse. Cette fonction est nécessaire pour les entreprises qui ont besoin de captures de données complètes à des fins médico-légales ou historiques, ou de la fonctionnalité de prévention des fuites de données (DLP). Pour activer cette fonction, vous devez acquérir et installer la licence gratuite.

La Mise en miroir du port de déchiffrement n'est pas offerte sur les pare-feu VM-Series pour plateformes de cloud public (AWS, Azure, Google Cloud Platform), VMware NSX et Citrix SDX.

Pour configurer une interface miroir de déchiffrement, cliquez sur le nom d'une interface (Ethernet1/1, par exemple) non configurée et indiquez les informations suivantes :

Paramètres d’une interface miroir de déchiffrement	Description
Nom de l'interface	Le nom de l'interface est prédéfini et vous ne pouvez pas le modifier.
Commentaire	Saisissez une description de l'interface (facultatif).
Type d'interface	Sélectionnez **Miroir de déchiffrement**.
Vitesse de liaison	Sélectionnez la vitesse de l'interface en Mbits/s (**10**, **100** ou **1000**) ou sélectionnez **auto** pour que le pare-feu détermine automatiquement la vitesse.
Mode duplex de la liaison	Indiquez si le mode de transmission de l'interface est en duplex intégral (**full (intégral)**), semi-duplex (**half (semi)**) ou automatiquement négocié (**auto**).
état des liaisons	Indiquez si l'état de l'interface est activé (**up (actif)**), désactivé **down (inactif)**) ou automatiquement déterminé (**auto**).

Groupe d’interfaces Ethernet agrégées (AE)

- Réseau > Interfaces > Ethernet > Ajouter un groupe agrégé

Un groupe d'interfaces Ethernet agrégé (AE) se base sur la norme IEEE 802.1AX d'agrégation de liens pour combiner de multiples interfaces Ethernet en une seule interface virtuelle qui connecte un pare-feu à un autre périphérique ou à un autre pare-feu. Un groupe d'interfaces Ethernet agrégées augmente la bande passante qui existe entre des homologues en équilibrant la charge du trafic qui passe par les interfaces combinées. Ce dernier assure également la redondance ; en cas de défaillance d'une interface, les autres interfaces continuent de prendre en charge le trafic. Le SD-WAN prend en charge les groupes d’interfaces AE de couche 3.

Avant de configurer un groupe d'interfaces Ethernet agrégées, vous devez d'abord configurer les interfaces qui le composent. Parmi les interfaces affectées à un groupe agrégé donné, le matériel peut différer (par exemple, vous pourriez allier la fibre optique et le cuivre), mais la bande passante (10 Gbit/s, 10 Gbit/s, 40 Gbit/s ou 100 Gbit/s) et le type d'interface (HA3, câble virtuel, couche 2 ou couche 3) doivent être identiques.

Le nombre de groupes d’interfaces AE que vous pouvez ajouter dépend du modèle de pare-feu. Le outil de sélection du produit indiquez le `Maximum d’interface agrégées` que chaque modèle de pare-feu peut supporter. Chaque groupe d'interfaces AE peut avoir jusqu'à huit interfaces.

Sur les pare-feux des séries PA-3200 et PA-5200 et ceux de la série PA-7000, QoS est compatible uniquement que les huit premiers groupes d’interfaces AE.

Tous les pare-feu Palo Alto Networks, à l'exception des modèles VM-Series, prennent en charge les groupes d'interfaces Ethernet agrégées.

Vous pouvez agréger les interfaces HA3 (transfert de paquets) dans une configuration haute disponibilité (HD) active / active, mais uniquement sur les modèles de pare-feu suivants :

- *PA-220*
- *Série PA-800*
- *PA-3200 Series*
- *Série PA-5200*

Pour configurer un groupe d'interfaces AE, vous devez **Ajouter un groupe agrégé**, configurer les paramètres décrits dans le tableau suivant, puis affecter les interfaces au groupe (reportez-vous à la section Interface Ethernet agrégée [AE]).

Paramètres d'un groupe d'interfaces agrégées	Configuré dans	Description
Nom de l'interface	**Agréger via l'interface Ethernet**	**Interface Name (Nom de l'interface)** en lecture seule est défini sur **ae**. Dans le champ adjacent, saisissez un suffixe numérique pour identifier le groupe d'interfaces Ethernet agrégées. La fourchette de suffixe numérique dépend du nombre de groupes AE que le modèle de pare-feu supporte. Consultez `Maximum d'interface agrégées` que chaque modèle de pare-feu peut supporter dans le outil de sélection du produit.
Commentaire		(Facultatif) Saisissez une description de l'interface.
Type d'interface		Sélectionnez le type d'interface, qui contrôle les exigences et les options de configuration restantes : • **HA** – Sélectionnez uniquement si l'interface est une liaison HA3 entre deux pare-feu et un déploiement actif/actif. Sélectionnez facultativement un **Profil Netflow** et configurez les paramètres dans onglet **LACP** (reportez-vous à la section Activation de LACP). • **Câble virtuel**—(en option) Sélectionnez un **Profil Netflow** et configurez les paramètres dans les onglets**Config** et **Avancé** tel que cela est décrit dans Paramètres de câble virtuel. • **Couche 2**—(en option) Sélectionnez un **profil Netflow**; configurez les paramètres dans l'onglet **Config** et l'onglet **avancés** tel que cela est décrit dans Paramètres de l'interface de

Paramètres d’un groupe d’interfaces agrégées	Configuré dans	Description
		Couche 2; et, en option, configurez l’onglet **LACP** (voir Activer LACP). • **Niveau 3** – Sélectionnez facultativement un Profil Netflow, configurez les onglets **Configuration, IPv4, IPv6** et **Avancé** comme décrit dans les **Paramètres d’une interface de niveau 3**. Configurez facultativement l’onglet LACP (reportez-vous à la section **Activation de LACP**). Le SD-WAN prend en charge les groupes d’interfaces AE des interfaces et sous-interfaces de couche 3.
profil NetFlow ;		Si vous voulez exporter le trafic IP unidirectionnel traversant une interface d’entrée vers un serveur NetFlow, sélectionnez le profil de serveur ou **Profil Netflow** pour définir un nouveau profil (Voir Périphérique > Profils de serveur > NetFlow). Sélectionnez **Aucun** pour supprimer l'affectation de serveur NetFlow du groupe d'interfaces Ethernet agrégées.
Activer LACP	**Agréger via l'interface Ethernet** > **LACP**	Sélectionnez si vous souhaitez activer LACP (protocole d’agrégation de liens) pour le groupe d’interfaces Ethernet agrégées. LACP est désactivé par défaut. Si vous activez LACP, la détection des échecs de l'interface se fait automatiquement aux niveaux de la liaison de données et physique, peu importe si le pare-feu et son homologue LACP sont connectés directement. (Sans LACP, la détection des échecs de l'interface est automatique uniquement au niveau physique entre des homologues connectés directement.) LACP assure également un basculement automatique aux interfaces qui sont en veille si vous configurez des disques de secours (reportez-vous à la section Nombre maximum de ports).
Mode		Sélectionnez le mode LACP du pare-feu. Entre deux homologues LACP, nous conseillons de configurer un comme actif et l’autre comme passif. LACP ne peut pas fonctionner si les deux homologues sont passifs. • **Passif** par défaut) - Le pare-feu répond de façon passive aux requêtes d'état LACP des périphériques homologues. • **Actif** - Le pare-feu interroge de façon active l'état LACP (disponible ou non réactif) des périphériques homologues.
Taux de transmission		Sélectionnez le taux auquel le pare-feu échange des requêtes et des réponses avec les périphériques homologues'A0;: • **Élevé** - Toutes les secondes.

Paramètres d’un groupe d’interfaces agrégées	Configuré dans	Description
		• **Faible** (par défaut) - toutes les 30 secondes
Basculement rapide		Sélectionnez cette option si, en cas de défaillance d’une interface, vous souhaitez que le pare-feu bascule vers une interface opérationnelle en une seconde. Sinon, le basculement se produit à la vitesse définie par la norme'A0;IEEE'A0;802.1AX (au moins trois secondes).
Priorité du système	**Agréger via l'interface Ethernet** > **LACP (suite)**	Ce nombre détermine si le pare-feu ou son homologue a un remplacement sur l'autre en ce qui concerne les priorités de port (reportez-vous à **Max Ports (Nombre maximum de ports)** ci-dessous). *Veuillez noter que plus le nombre est petit, plus la priorité est grande (plage comprise entre 1 et 65 535 ; valeur par défaut : 32 768).*
Nombre maximal d’interfaces		Le nombre d'interfaces (1 à 8) qui peuvent être actives à un moment donné dans un groupe LACP agrégé. Cette valeur ne peut pas dépasser le nombre d'interfaces affectées au groupe. Si le nombre d'interfaces affectées dépasse le nombre d'interfaces actives, le pare-feu utilise les priorités de port LACP des interfaces pour déterminer celles qui sont en mode veille. Vous définissez les priorités de port LACP lors de la configuration de chaque interface du groupe (reportez-vous à la section Interface Ethernet agrégée [EA]).
Activation à l'état HA passif		Si les pare-feu sont déployés dans une configuration active/passive (HA), sélectionnez pour permettre au pare-feu passif de prénégocier LACP avec son homologue actif avant qu’un basculement ait lieu. Cette négociation préalable accélère le basculement, puisque le pare-feu actif n'a plus à négocier LACP avant de devenir actif.
Même adresse MAC système pour la haute disponibilité active/passive	**Agréger via l'interface Ethernet** > **LACP (suite)**	Ceci ne s’applique qu’aux pare-feu déployés dans une HA actif/passif configuration ; les pare-feu qui sont déployés dans une actif/passif configuration nécessitent des adresses MAC uniques. Les pare-feu homologues HA ont la même valeur de priorité système. Cependant, dans un déploiement HA actif/passif, l'ID système de chacun peut être identique ou différent, selon que vous affectiez la même adresse MAC ou non.

Paramètres d’un groupe d’interfaces agrégées	Configuré dans	Description
		Lorsque les homologues LACP (également en mode HA) sont virtualisés (apparaissent sur le réseau comme périphérique unique), l'utilisation de la même adresse MAC système pour les pare-feu réduit la latence lors du basculement. Lorsque les homologues LACP ne sont pas virtualisés, l'utilisation de l'adresse MAC unique de chaque pare-feu réduit la latence lors du basculement. LACP utilise l'adresse MAC afin de dériver un ID système pour chaque homologue LACP. Si la paire de pare-feu et la paire d'homologues ont les mêmes valeurs de priorité système, LACP utilise les valeurs d'ID système afin de déterminer celle qui a un contrôle prioritaire sur l'autre en ce qui concerne les priorités de port. Si les deux pare-feu ont la même adresse MAC, ils ont également le même ID système, qui est supérieur ou inférieur à l'ID système des homologues LACP. Si les pare-feu HA ont chacun une adresse MAC unique, l'un peut avoir un ID système supérieur à celui des homologues LACP, tandis que l'autre a un ID système inférieur. Dans le dernier cas, lorsqu'un basculement se produit sur les pare-feu, les priorités de port basculent entre les homologues LACP et le pare-feu qui devient actif.
Adresse MAC	**Agréger via l'interface Ethernet** > **LACP (suite)**	Si vous **Utilisez la même adresse MAC système**, sélectionnez une adresse MAC générée par le système, ou saisissez votre propre adresse MAC, pour les deux pare-feu de la paire (HA) actif/passif. Vous devez vérifier que l'adresse globale est unique.
Profil d’interface SD-WAN	**Agréger via l'interface Ethernet** > **SD-WAN**	Sélectionnez un profil d’interface SD-WAN à appliquer au groupe d’interfaces AE ou créez un nouveau profil.
Profil de gestion	**Agréger via l'interface Ethernet** > **Avancé** > **Autres infos**	Sélectionnez un profil de gestion qui définit les protocoles (par exemple, SSH, Telnet et HTTP) à utiliser pour gérer le pare-feu dans cette interface. Sélectionnez **None (Aucune)** pour supprimer l'affectation de profil de l'interface.
MTU		Saisissez l’unité de transmission maximale (MTU) en octets par paquet envoyé sur cette interface (plage de 576 à 9 192 ; par défaut 1 500). Si les machines situées de chaque côté du pare-feu effectuent une détection du chemin MTU (PMTUD) et que l'interface reçoit un paquet dépassant la valeur MTU, le pare-feu

Paramètres d’un groupe d’interfaces agrégées	Configuré dans	Description
		renvoie à la source un message de *fragmentation ICMP obligatoire* indiquant que le paquet est trop volumineux.
Ajuster TCP MSS		Sélectionnez pour ajuster la taille de segment maximale (MSS) afin de tolérer les octets de tous les en-têtes qui respectent la taille en octets de la MTU de l’interface. La taille en octets de la MTU moins la taille d'ajustement de la MSS équivaut à la taille en octets de la MSS, laquelle varie selon le protocole IP : • **IPv4 MSS Adjustment Size (Taille d'ajustement MSS IPv4)** - intervalle compris entre 40 et 300 ; valeur par défaut : 40. • **IPv6 MSS Adjustment Size (Taille d'ajustement MSS IPv4)** - intervalle compris entre 60 et 300 ; valeur par défaut : 60. Servez-vous de ces paramètres pour faire face aux situations où un **tunnel** réseau nécessite une plus petite MSS. Si un paquet a plus d'octets que la MSS sans faire l'objet d'une fragmentation, ce paramètre permet son ajustement. L'encapsulation rallonge les en-têtes. Il peut donc s'avérer utile de configurer la taille d'ajustement MSS de façon à autoriser les octets d'éléments tels que des en-têtes MPLS ou le trafic par tunnel ayant une étiquette VLAN.
Sous-interface non étiquetée		Sélectionnez cette option si les sous-interfaces correspondantes à cette interface ne sont pas étiquetées.
Adresse IP Adresse MAC	**Agréger via l'interface Ethernet** > **Avancé** > **Entrées ARP**	Pour ajouter une ou plusieurs entrées ARP (Address Resolution Protocol/protocole de résolution d’adresse) statiques, **Add (Ajoutez)** une adresse IP et son adresse matérielle associée (Media Access Control/commande d’accès au support ou MAC). Pour supprimer une entrée, sélectionnez-la et cliquez sur **Delete (Supprimer)**. Les entrées ARP statiques réduisent le traitement ARP.
Adresse IPv6 Adresse MAC	**Agréger via l'interface Ethernet** > **Avancé** > **Entrées ND**	Afin de fournir des informations de voisinage pour NDP (Neighbor Discovery Protocol/protocole de découverte des voisins), **Add (Ajoutez)** l'adresse IPv6 et l'adresse MAC du voisin.
Activer le proxy NDP	**Agréger via l'interface Ethernet** >	Activez le proxy NDP (Neighbor Discovery Protocol / protocole de découverte des voisins) sur l’interface. Le pare-feu répondra aux paquets ND demandant des adresses MAC pour les adresses IPv6 de cette liste. Dans la réponse ND, le pare-feu envoie sa propre

Paramètres d’un groupe d’interfaces agrégées	Configuré dans	Description
	Avancé > **Proxy NDP**	adresse MAC pour l'interface de manière à recevoir les paquets destinés aux adresses de la liste. Il est recommandé d'activer le proxy NDP si vous utilisez NPTv6 (Network Prefix Translation IPv6). Si l'option **Enable NDP Proxy (Activer le proxy NDP)** est sélectionnée, vous pouvez filtrer de nombreuses entrées **Address (Adresse)** en saisissant un filtre et en cliquant sur Appliquer le filtre (la flèche grise).
Adresse		Vous devez **Add (Ajouter)** une ou plusieurs adresses IPv6, plages d’adresses IP, sous-réseaux IPv6 ou objets d’adresse pour lesquels le pare-feu agira comme proxy NDP. Idéalement, l'une de ces adresses est identique à celle de la traduction source dans NPTv6. L'ordre des adresses n'a pas d'importance. Si l'adresse est un sous-réseau, le pare-feu enverra une réponse ND pour toutes les adresses du sous-réseau. Par conséquent, il est recommandé d'ajouter également les voisins IPv6 du pare-feu et de cliquer sur **Negate (Ignorer)** pour que le pare-feu ne réponde pas à ces adresses IP.
Inverser		Sélectionnez **Negate (Ignorer)** une adresse afin d’empêcher le proxy NDP d’opérer sur cette adresse. Vous pouvez ignorer un sous-ensemble de la plage d'adresses IP ou du sous-réseau IP spécifié.
Activer LLDP	**Agréger via l'interface Ethernet** > **Avancé** > **LLDP**	Sélectionnez cette option pour activer LLDP (Link Layer Discovery Protocol/protocole de découverte de couche liaison) sur l'interface. LLDP fonctionne sur la couche de liaison pour détecter les périphériques avoisinants et leurs fonctionnalités en envoyant des unités de données LLDP aux périphériques avoisinants et en recevant des unités de données LLDP de ceux-ci.
LLDP Profile (profil LLDP)		Sélectionnez un profil LLDP ou créez un nouveau LLDP Profile (profil LLDP). Le profil vous permet de configurer le mode LLDP, d'activer les notifications SNMP et Syslog, ainsi que de configurer les éléments TLV (Type-Longueur-Valeur) que vous souhaitez transmettre aux homologues LLDP.
Paramètres	**Agréger via l'interface Ethernet** > **Avancé** > **DDNS**	Sélectionnez **Settings (Paramètres)** pour que les champs DDNS puissent être configurés.
Activer		Activer DDNS sur l'interface Vous devez d’abord activer DDNS pour le configurer. (Si vous n’avez pas terminé de configurer

Paramètres d'un groupe d'interfaces agrégées	Configuré dans	Description
		DDNS, vous pouvez enregistrer la configuration sans l'activer, ce qui vous évitera de perdre la configuration partielle.)
Intervalle de mise à jour (jours)		Saisissez l'intervalle (en jours) entre les mises à jour que le pare-feu envoie au serveur DDNS pour mettre à jour les adresses IP associées aux FQDN (la plage est comprise entre 1 et 30 ; la valeur par défaut est 1). *Le pare-feu met également à jour DDNS à la réception d'une nouvelle adresse IP pour l'interface du serveur DHCP.*
Profil du certificat		Créez un profil de certificat pour vérifier le service DDNS. Le service DDNS présente au pare-feu un certificat signé par l'autorité de certification (CA).
Nom d'hôte		Saisissez un nom d'hôte pour l'interface, qui est inscrit auprès du serveur DDNS (par exemple, hôte123.domaine123.com ou hôte123). Le pare-feu ne valide pas le nom d'hôte, sauf pour confirmer que la syntaxe utilise les caractères valides autorisés par DNS pour un nom de domaine.
Constructeur	**Agréger via l'interface Ethernet** > **Avancé** > **DDNS**	Sélectionnez le fournisseur DDNS (et la version) qui fournit un service DDNS à cette interface : • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **Free DNS Afraid.org v1** • **No-IP v1** • **Palo Alto Networks DDNS** (s'applique au SD-WAN Full Mesh avec DDNS, aux sous-interfaces SD-WAN AE et aux sous-interfaces SD-WAN Couche 3) *Si vous sélectionnez une version antérieure d'un service DDNS qui, selon le pare-feu, sera supprimée avant une date donnée, passez à la nouvelle version.* Les champs **Name (Nom)** et **Value (Valeur)** qui suivant le nom du fournisseur sont propres au fournisseur. Les champs en lecture seule vous avisent des paramètres que le pare-feu utilise pour se connecter au service DDNS. Configurez les autres champs, comme

Paramètres d’un groupe d’interfaces agrégées	Configuré dans	Description
		un mot de passe que le service DDNS vous fournit et le délai que le pare-feu utilise s’il ne reçoit pas de réponse du service DDNS.
Onglet IPv4		Ajoutez les adresses IPv4 configurées sur l’interface, puis sélectionnez-les. Vous pouvez sélectionner le nombre d’adresses IPv4 que le fournisseur DDNS permet. Toutes les adresses IP sélectionnées sont inscrites auprès du fournisseur DDNS.
Onglet IPv6		Ajoutez les adresses IPv6 configurées sur l’interface, puis sélectionnez-les. Vous pouvez sélectionner le nombre d’adresses IPv6 que le fournisseur DDNS permet. Toutes les adresses IP sélectionnées sont inscrites auprès du fournisseur DDNS.
Show Runtime Info		Affiche l’inscription DDNS : fournisseur DDNS, FQDN résolu et les adresses IP mappées avec un astérisque (*) indiquant l'adresse IP principale. Chaque fournisseur DDNS possède ses propres codes de retour pour indiquer l’état de la mise à jour du nom d’hôte et une date de retour à des fins de résolution de problèmes.

Interfaces Ethernet agrégées (AE)

- Réseau > Interfaces > Ethernet

Pour configurer une Aggregate Ethernet (AE) Interface (interface Ethernet agrégée (AE)), ajoutez d'abord un Aggregate Ethernet (AE) Interface Group (groupe d'interfaces Ethernet agrégé (AE)). Cliquez ensuite sur le nom de l'interface que vous attribuerez à ce groupe. Parmi les interfaces que vous affectez à un groupe donné, le matériel peut différer (par exemple, vous pourriez allier la fibre optique et le cuivre), mais la bande passante et le type d'interface (comme Couche 3) doivent être identiques. De plus, l’interface doit être du même type que celle définie pour le groupe d’interfaces Ethernet agrégées ; vous modifierez toutefois le type en **Ethernet agrégée** lorsque vous configurerez chaque interface. Précisez les informations suivantes pour chaque interface que vous affectez au groupe.

*Si vous avez activé LACP (Link Aggregation Control Protocol) pour le groupe d’interfaces AE, sélectionnez la même **Vitesse de liaison** et le même **Modèle duplex de la liaison** pour chaque interface de ce groupe. Lorsque les valeurs ne correspondent pas, l’opération de validation affiche un avertissement et PAN-OS utilise la vitesse la plus élevée et le duplex intégral.*

Paramètres d’une interface agrégée	Configuré dans	Description
Nom de l'interface	**Agréger via l'interface Ethernet**	Le nom de l'interface est prédéfini et vous ne pouvez pas le modifier. Entrez un nombre après ae dans le nom de l'interface.
Commentaire		(Facultatif) Saisissez une description de l’interface.
Type d'interface		Sélectionnez **Ethernet agrégée**.
Groupe agrégé		Affectez l’interface à un groupe agrégé.
Vitesse de liaison	**Agréger via l'interface Ethernet** > **Avancé** > **Paramètres de lien**	Sélectionnez la vitesse de l'interface en Mbits/s ou sélectionnez **auto** pour que le pare-feu détermine automatiquement la vitesse.
Mode duplex de la liaison		Indiquez si le mode de transmission de l'interface est en duplex intégral (**full (intégral)**), semi-duplex (**half (semi)**) ou automatiquement négocié (**auto**).
état des liaisons		Indiquez si l'état de l'interface est activé (**up (actif)**), désactivé **down (inactif)**) ou automatiquement déterminé (**auto**).
Alimentation Rsvd PoE	**Agréger via l'interface Ethernet** > **Avancé** > **Paramètres PoE** (Supported firewalls only (Pare-feu pris en charge uniquement))	Sélectionnez la quantité de puissance allouée en Watts si PoE est activé.
PoE activé		Sélectionnez pour activer PoE sur cette interface.
Priorité du port LACP		Le pare-feu utilise ce champ uniquement si vous avez activé LACP (Link Aggregation Control Protocol/protocole d’agrégation de liens) pour le groupe agrégé. Si le nombre d’interfaces que vous affectez au groupe dépasse le nombre d’interfaces actives Nombre maximum de ports), le pare-feu utilise les priorités de port LACP des interfaces pour déterminer celles qui sont en mode veille. Plus le nombre est petit, plus la priorité est grande (intervalle compris entre 1 et 65 535 ; valeur par défaut : 32 768).
routeur virtuel - VR	**Agréger via l'interface**	Sélectionnez le routeur virtuel auquel vous affectez l’interface Ethernet agrégée.

Paramètres d’une interface agrégée	Configuré dans	Description
Zone de sécurité	**Ethernet** > **Configuration**	Sélectionnez la zone de sécurité à laquelle vous affectez l’interface Ethernet agrégée.
Activer SD-WAN	**Agréger via l'interface Ethernet** > **IPv4**	Sélectionnez pour activer la fonctionnalité SD-WAN pour l'interface.
Activer Bonjour Reflector	**Agréger via l'interface Ethernet** > **IPv4**	(séries PA-220, PA-800 et PA-3200 uniquement) Lorsque vous activez cette option, le pare-feu transfère les alertes et les requêtes multicast Bonjour reçues et transférées à cette interface aux autres interfaces et sous-interfaces L3 et AE lorsque vous activez cette option. Cela aide à garantir l’accès utilisateur et la découverte du périphérique sur les environnements de réseau qui utilisent la segmentation pour acheminer le trafic pour des besoins de sécurité ou administratifs. Vous pouvez activer cette option jusqu’à 16 interfaces.
Activer IPv6 sur l'interface	**Agréger via l'interface Ethernet** > **IPv6**	Sélectionnez pour activer IPv6 sur cette interface.
ID de l'interface		Saisissez l'identifiant unique étendu sur 64'A0;bits (EUI-64) au format hexadécimal (par exemple, 00:26:08:FF:FE:DE:4E:29). Si ce champ n'est pas renseigné, le pare-feu utilise l'identifiant unique étendu sur 64'A0;bits (EUI-64) généré à partir de l'adresse MAC de l'interface physique. Si vous utilisez l’option **Utiliser l’ID de l’interface comme partie hôte** lors de l’ajout d’une adresse, le pare-feu utilise l’ID de l’interface comme partie hôte de cette adresse.
Adresse	**Agréger via l'interface Ethernet** > **IPv6** > **Attribution d'adresse, type = statique**	Ajoutez une adresse IPv6 et une longueur de préfixe (par exemple, 2001:400:f00::1/64). Vous pouvez également sélectionner un objet d'adresse IPv6 existant ou en créer un nouveau.
Activer l’adresse sur l’interface		Sélectionnez pour activer l’adresse IPv6 sur l’interface.
Utiliser l’ID de l’interface comme partie hôte.		Sélectionnez cette option pour utiliser l’**ID de l’interface** comme partie hôte de l’adresse IPv6.

Paramètres d’une interface agrégée	Configuré dans	Description
Anycast		Sélectionnez cette option pour inclure le routage via le nœud le plus proche.
Envoyer la publication des routeurs	**Agréger via l'interface Ethernet** > **IPv6** > **Attribution d'adresse, type = statique**	Sélectionnez cette option pour activer la publication de routeur (RA) pour cette adresse IP. (Vous devez également activer l'option globale **Enable Router Advertisement (Activer la publication de routeur** sur l'interface.) Pour plus d’informations sur la RA, reportez-vous à la section Activer la publication de routeur dans ce tableau. Les champs suivants s’appliquent uniquement si vous activez la publication du routeur : • **Valid Lifetime (Durée de vie valide)** - La durée, en secondes, pendant laquelle le pare-feu considère l’adresse comme valide. La durée de vie valide doit être supérieure ou égale à **Preferred Lifetime (durée de vie préférée)**. La valeur par défaut est de 2 592 000. • **Preferred Lifetime (Durée de vie préférée)** - La durée, en secondes, pendant laquelle l’adresse valide est préférée, ce qui signifie que le pare-feu peut l’utiliser pour envoyer et recevoir du trafic. Lorsque la durée de vie préférée expire, le pare-feu ne peut plus utiliser l'adresse pour établir de nouvelles connexions, mais toute connexion existante reste valide jusqu'à ce que la **Valid Lifetime (Durée de vie valide)** expire. La valeur par défaut est de 604 800. • **On-link (Sur la liaison)** - Sélectionnez si les systèmes qui disposent d’adresses dans le préfixe sont accessibles sans routeur. • **Autonomous (Autonome)** - Sélectionnez cette option si les systèmes peuvent créer une adresse IP de façon indépendante en combinant le préfixe publié et l’ID d’une interface.
Accepter l'itinéraire annoncé par le routeur	**Agréger via l'interface Ethernet** > **IPv6** > **Attribution d'adresse, Type = Client DHCPv6**	Sélectionnez cette option pour autoriser le client DHCPv6 à accepter le RA du serveur DHCP.
Mesure d'itinéraire par défaut		Saisissez une métrique de route par défaut pour la route entre l'interface et le FAI ; la plage est de 1 à 65 535 ; la valeur par défaut est 10.
Préférence		Sélectionnez la préférence de l'interface client DHCPv6 (**low (faible)**, **medium (moyen)**ou **high (élevé)**) de sorte que, dans le cas où vous avez deux interfaces (chacune étant connectée à un FAI différent pour la redondance), vous puissiez attribuer à l'un

Paramètres d’une interface agrégée	Configuré dans	Description
		des FAI une préférence plus élevée que la l'interface avec l'autre FAI. Le FAI connecté à l'interface préférée sera le FAI qui fournit le préfixe délégué à envoyer à une interface faisant face à l'hôte. Si les interfaces ont la même préférence, les deux FAI fournissent un préfixe délégué et l'hôte décide quel préfixe utiliser.
Activer l'adresse IPv6	**Agréger via l'interface Ethernet > IPv6 > Attribution d'adresse, Type = Client DHCPv6 > Options DHCPv6**	Activez l'adresse IPv6 reçue pour ce client DHCPv6.
Adresse non temporaire		Demandez une adresse non temporaire que le pare-feu doit attribuer à cette interface client DHCPv6 qui fait face au routeur délégant et au FAI. Sélectionnez pour une durée de vie plus longue qu'une adresse temporaire. *Que vous demandiez une adresse non temporaire ou une adresse temporaire pour l'interface dépend de votre discrétion et de la capacité du serveur DHCPv6; certains serveurs ne peuvent fournir qu'une adresse temporaire. La meilleure pratique consiste à sélectionner à la fois Adresse non temporaire et Adresse temporaire, auquel cas le pare-feu préférera l'Adresse non temporaire.*
Adresse temporaire		Demandez une adresse temporaire que le pare-feu doit attribuer à cette interface client DHCPv6 qui fait face au routeur délégant et au FAI. Sélectionnez Adresse temporaire pour un niveau de sécurité supérieur, car l'adresse est destinée à être utilisée pendant une courte période.
Validation rapide		Sélectionnez cette option pour utiliser le processus DHCP des messages Solliciter et Répondre, plutôt que le processus des messages Solliciter, Annoncer, Demander et Répondre.
Activer la délégation de préfixe	**Agréger via l'interface Ethernet > IPv6 > Attribution d'adresse, Type = Client DHCPv6 > Délégation de préfixe**	Activez la délégation de préfixe pour permettre au pare-feu de prendre en charge la fonctionnalité de délégation de préfixe. Cela signifie que l'interface accepte un préfixe du serveur DHCPv6 en amont et place le préfixe dans le pool de préfixes que vous sélectionnez, à partir duquel le pare-feu délègue un préfixe à un hôte via SLAAC. La possibilité d'activer ou de désactiver la délégation de préfixe pour une interface permet au pare-feu de prendre en charge plusieurs FAI (un FAI par interface). L'activation de la délégation de préfixe sur cette interface contrôle quel FAI fournit le préfixe. Le préfixe délégué reçu du serveur DHCP ne peut pas être utilisé sur l'interface qui l'a demandé.

Paramètres d’une interface agrégée	Configuré dans	Description
Conseil sur la longueur du préfixe DHCP		Sélectionnez pour permettre au pare-feu d'envoyer une longueur de préfixe DHCPv6 préférée au serveur DHCPv6.
Longueur du préfixe DHCP (bits)		Entrez la longueur de préfixe DHCPv6 préférée dans la plage de 48 à 64 bits, qui est envoyée comme indice au serveur DHCPv6. *Demander une longueur de préfixe de 48, par exemple, laisse 16 bits restants pour les sous-réseaux (64-48), ce qui indique que vous avez besoin de nombreuses subdivisions de ce préfixe pour déléguer. D'autre part, demander une longueur de préfixe de 63 laisse 1 bit pour ne déléguer que deux sous-réseaux. Sur les 128 bits, il reste encore 64 bits pour l'adresse de l'hôte.*
Nom du pool de préfixes		Saisissez un nom pour le pool de préfixes dans lequel le pare-feu stocke le préfixe reçu. Le nom doit être unique et contenir au maximum 63 caractères alphanumériques, traits d'union, points et soulignements. *Utilisez un nom de pool de préfixes qui reflète le FAI pour faciliter la reconnaissance.*
Nom	**Agréger via l'interface Ethernet > IPv6 > Attribution d'adresse, type = hérité**	**Add (Ajoutez)** un pool en saisissant un nom de pool. Le nom peut comporter au maximum 63 caractères alphanumériques, traits d'union, points et traits de soulignement.
Type d'adresse		Sélectionnez parmi les choix suivants : • **GUA from pool (AUG du pool)**— Adresse Unidiffusion globale (AUG) provenant du pool de préfixes choisi. • **ULA**—Unique Local Address est une adresse privée dans la plage d'adresses fc00::/7 pour la connectivité au sein d'un réseau privé. Sélectionnez ULA s'il n'y a pas de serveur DHCP. Le serveur DHCPv6 a le pouvoir discrétionnaire d'envoyer la longueur de préfixe qu'il choisit.
Activer sur l'interface		Activez l’adresse IPv6 sur l’interface.
Pool de préfixes		(GUA (AUG)) Sélectionnez le pool de préfixes à partir duquel obtenir l’AUG.

Paramètres d’une interface agrégée	Configuré dans	Description
Assignment Type (Type d'affectation)	**Agréger via l'interface Ethernet > IPv6 > Attribution d'adresse, type = hérité**	(GUA (AUG)) Sélectionnez le type d'affectation : • **Dynamic (Dynamique)** — Le client DHCPv6 est responsable du choix d'un identifiant pour configurer l'interface héritée. • **Dynamic with Identifier (Dynamique avec identifiant)**— Vous êtes responsable du choix d'un identifiant dans la plage de 0 à 4 000 et de la gestion d'un identifiant unique sur les clients DHCPv6.
Activer l’adresse sur l’interface		(ULA)Activez l’adresse IPv6 sur l’interface.
Adresse		(ULA) Entrez une adresse.
Utiliser l’ID de l’interface comme partie hôte.		(ULA) Sélectionnez cette option pour utiliser l’ID de l’interface comme partie hôte de l’adresse IPv6.
Anycast		(ULA) Sélectionnez pour faire de l'adresse IPv6 (itinéraire) une adresse Anycast (itinéraire), ce qui veut dire que plusieurs emplacements peuvent publier le même préfixe et que l'adresse IPv6 envoie le trafic anycast au nœud qu'il considère le plus près selon les coûts associés au protocole de routage et d'autres facteurs.
Envoyer la publication des routeurs		Sélectionnez pour envoyer des annonces de routeur (AR) de l'interface aux hôtes LAN.
On-Link		Sélectionnez si les systèmes qui disposent d’adresses dans le préfixe sont accessibles sans routeur.
Autonome		Sélectionnez cette option si les systèmes peuvent créer une adresse IP de façon indépendante en combinant le préfixe publié et l’ID d’une interface.
Activer la détection des doublons d'adresses	**Agréger via l'interface Ethernet > IPv6 > Résolution d’adresses**	Sélectionnez cette option pour activer la détection des doublons d’adresses (DAD), ce qui vous permet ensuite d’indiquer le nombre de **Tentatives DAD**.
Tentatives DAD		Indiquez le nombre de tentatives DAD dans l'intervalle de sollicitation de voisins (**NS Interval (intervalle NS)**) avant que la

Paramètres d’une interface agrégée	Configuré dans	Description
		tentative d'identification n'échoue (intervalle compris entre 1 et 10 ; valeur par défaut : 1).
Durée d'accessibilité		Indiquez la durée (en secondes) pendant laquelle un voisin reste accessible après une requête et une réponse réussies (plage de 1 à 36 000 ; valeur par défaut de 30).
Intervalle (s)		Indiquez la durée, en secondes, avant indication d’un échec d’une tentative DAD (plage de 3,600 à 1 ; par défaut 1).
Activer la surveillance NDP		Sélectionnez cette option pour activer la surveillance du Protocole de découverte des voisins. Lorsqu’il est activé, vous pouvez sélectionner le NDP ( dans la colonne Fonctions) et afficher des informations telles que l’adresse IPv6 d’un voisin découverte par le pare-feu, l’adresse MAC et User-ID correspondants (selon la situation la plus favorable).
Activer la publication des routeurs	**Interface Ethernet agrégée > IPv6 > Publicité de routeur**	Sélectionnez cette option pour assurer la Découverte de voisins sur les interfaces IPv6 et configurer les autres champs de cette section. Les clients DNS IPv6 qui reçoivent les messages de publication de routeur utilisent ces informations. La RA permet au pare-feu d'agir en tant que passerelle par défaut pour les hôtes IPv6 qui ne sont pas configurés de façon statique et de fournir à l'hôte un préfixe IPv6 qui lui permet de configurer une adresse. Vous pouvez utiliser un serveur DHCPv6 distinct conjointement avec cette fonctionnalité pour fournir un DNS et d'autres paramètres aux clients. Il s’agit d’un paramètre global de l’interface. Si vous souhaitez définir des options de publication de routeur (RA) pour les adresses IP individuelles, il vous faut **Add (Ajouter)** et configurer une adresse IPv6 dans la table d’adresses IP. Si vous définissez des options de publication de routeur pour une adresse IP, vous devez **nable Router Advertisement (Activer la publication de routeur)** sur l’interface.
Intervalle min. (s)		Indiquez l’intervalle minimum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 3 et 1 350 ; valeur par défaut : 200). Le pare-feu envoie les publications de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales configurées.

Paramètres d’une interface agrégée	Configuré dans	Description
Intervalle max. (s)		Indiquez l’intervalle maximum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 4 et 1 800 ; valeur par défaut : 600). Le pare-feu envoie les publications de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales configurées.
Limite de saut		Indiquez la limite de saut à appliquer aux clients pour les paquets sortants (intervalle compris entre 1 et 255 ; valeur par défaut : 64). Saisissez **0** pour indiquer l’absence de limite de saut.
MTU de liaison		Indiquez l'unité de transmission maximale (MTU) de liaison à appliquer aux clients. Sélectionnez **unspecified (non spécifiée)** pour indiquer l'absence de MTU de liaison (intervalle compris entre 1 280 et 9 192 ; valeur par défaut : non spécifiée).
Durée d'accessibilité (ms)		Indiquez la durée d’accessibilité, en millisecondes, que le client va utiliser pour supposer l’accessibilité d’un voisin après avoir reçu un message de confirmation d’accessibilité. Sélectionnez **unspecified (non spécifiée)** pour indiquer l'absence de valeur pour la durée d'accessibilité (intervalle compris entre 0 et 3 600 000 ; valeur par défaut : non spécifiée).
Durée de retransmission (ms)		Indiquez le minuteur de retransmission qui détermine la durée d’attente du client, en millisecondes, avant la retransmission des messages de sollicitation de voisins. Sélectionnez **unspecified (non spécifiée)** pour indiquer l'absence de valeur pour la durée de retransmission (intervalle compris entre 0 et 4 294 967 295 ; valeur par défaut : non spécifiée).
Durée de vie du routeur (s)		Indiquez la durée, en secondes, pendant laquelle le client utilise le pare-feu comme passerelle par défaut (plage comprise entre 0 et 9 000 ; valeur par défaut : 1 800). Une valeur de 0 indique que le pare-feu n'est pas la passerelle par défaut. Lorsque la durée de vie expire, le client supprime l'entrée du pare-feu de sa liste de routeurs par défaut et utilise un autre routeur comme passerelle par défaut.
Préférence de routeur		Si le segment de réseau dispose de plusieurs routeurs IPv6, le client utilise ce champ pour sélectionner un routeur préféré. Indiquez si le routeur de pare-feu publié a une priorité **High (Élevée)**, **Medium (Moyenne)** (par défaut) ou **Low (Faible)** par rapport aux autres routeurs se trouvant sur le segment.
Configuration gérée		Sélectionnez cette option pour indiquer au client que les adresses sont disponibles via DHCPv6.

Paramètres d'une interface agrégée	Configuré dans	Description
Autre configuration		Sélectionnez cette option pour indiquer au client que d'autres informations d'adresse (comme les paramètres associés au DNS) sont disponibles via DHCPv6.
Vérification de cohérence	**Interface Ethernet agrégée > IPv6 > Envoyer la publication des routeurs**	Sélectionnez si vous souhaitez que le pare-feu vérifie que les RA reçues des autres routeurs publient des informations cohérentes sur la liaison. Le pare-feu consigne toutes les incohérences dans un journal système de type **Ipv6nd**.
Inclure les informations DNS dans la publication de routeur	**Agréger via l'interface Ethernet > IPv6 > Prise en charge DNS, Type = Statique**	Sélectionnez cette option pour que le pare-feu envoie des informations DNS dans les messages de publication de routeur (RA) NDP à partir de cette interface Ethernet agrégée IPv6. Les autres champs de Prise en charge DNS de ce tableau ne sont visibles qu'après sélection de cette option. (L'onglet **DNS Support (Prise en charge DNS)** est disponible si vous sélectionnez l'option **Enable Router Advertisement (Activer la publication du routeur)** dans l'onglet Router Advertisement (Annonce du routeur).
Serveur		Il faut **Ajouter** une ou plusieurs adresses de serveur DNS (RDNS) récursives pour que le pare-feu envoie des publications de routeur NDP à partir de cette interface Ethernet agrégée IPv6. Les serveurs RDNS envoient une série de requêtes de recherches DNS aux serveurs DNS racines et aux serveurs DNS fiables pour finalement fournir une adresse IP au client DNS. Vous pouvez configurer un maximum de huit serveurs RDNS que le pare-feu envoie, dans l'ordre indiqué de haut en bas, dans une publication de routeur NDP au destinataire, qui utilise ensuite ces adresses dans le même ordre. Sélectionnez un serveur et utilisez les options **Déplacer en haut** ou **Déplacer en bas** pour modifier l'ordre des serveurs ou **Supprimer** un serveur lorsque vous n'en avez plus besoin.
Durée de vie		Saisissez le nombre maximum de secondes qui s'est écoulé après réception de la publication du routeur par le client DNS IPv6. Celle-ci stipule qu'il est possible d'utiliser les Serveurs RDNS pour résoudre les noms de domaine (l'intervalle est la valeur de l'Intervalle max. [s] jusqu'à deux fois l'Intervalle maximal ; la valeur par défaut est 1 200).

Paramètres d'une interface agrégée	Configuré dans	Description
Liste de recherche de domaine		Il vous faut **Ajouter** et configurer un ou plusieurs noms de domaine (suffixes) pour la liste de recherche DNS (DNSSL). La longueur de suffixe maximale est de 255 octets. Une liste de recherche DNS est une liste de suffixes de domaine qu'un routeur de client DNS ajoute (un à la fois) à un nom de domaine non qualifié avant d'entrer le nom dans une requête DNS, en utilisant un nom de domaine complet dans la requête DNS. Par exemple, si un client DNS essaie de soumettre une requête DNS pour le nom « qualité » sans suffixe, le routeur ajoute un point et le premier suffixe DNS de la liste de recherche DNS au nom et transmet la requête DNS. Si le premier suffixe DNS sur la liste est « company.com », la requête DNS qui résulte du routeur est « quality.company.com » pour le nom de domaine complet. Si la requête DNS échoue, le routeur ajoute le deuxième suffixe DNS de la liste au nom non qualifié et transmet une nouvelle requête DNS. Le routeur essaie les suffixes DNS jusqu'à ce qu'une recherche DNS soit fructueuse (il ignore les suffixes restants) ou jusqu'à ce que le routeur ait essayé tous les suffixes de la liste. Configurez le pare-feu avec les suffixes que vous souhaitez fournir au routeur du client DNS dans une option Découverte de voisins DNSSL ; le client DNS recevant l'option DNSSL utilise les suffixes pour ses requêtes DNS non qualifiées. Vous pouvez configurer un maximum de huit noms de domaine (suffixes) pour une liste de recherche DNS que le pare-feu envoie (dans l'ordre, de haut en bas) dans une publication de routeur NDP au destinataire, qui les utilise dans le même ordre. Sélectionnez un suffixe et utilisez les options **Déplacer en haut** ou **Déplacer en bas** pour modifier l'ordre des suffixes ou **Supprimer** un suffixe lorsque vous n'en avez plus besoin.
Durée de vie	**Agréger via l'interface Ethernet** > **IPv6** > **Prise en charge DNS, Type = Statique**	Saisissez le nombre maximum de secondes qui s'est écoulé après réception de la publication du routeur par le client DNS IPv6. Celle-ci stipule qu'il est possible d'utiliser un nom de domaine (suffixe) sur la liste de recherche DNS (l'intervalle est la valeur de l'Intervalle max. [s] jusqu'à deux fois l'intervalle maximal ; la valeur par défaut est 1 200).
Serveur de noms récursif DNS	**Agréger via l'interface Ethernet** > **IPv6** > **Prise**	Activez et sélectionnez : • **DHCPv6**—Pour que le serveur DHCPv6 envoie les informations DNS Recursive Name Server.

Paramètres d’une interface agrégée	Configuré dans	Description
	en charge DNS, type = client DHCPv6 ou hérité	• **Manual (Manuel)** — Pour configurer manuellement le serveur de noms DNS Recursive. Si vous choisissez **Manual (Manuel)**, **Add (Ajouter)** une adresse de **Server (serveur)** DNS (RDNS) récursive pour que le pare-feu envoie des annonce de routeur NDP à partir de cette interface VLAN IPv6. Les serveurs RDNS envoient une série de requêtes de recherches DNS aux serveurs DNS racines et aux serveurs DNS fiables pour finalement fournir une adresse IP au client DNS. Vous pouvez configurer un maximum de huit serveurs RDNS que le pare-feu envoie (dans l’ordre indiqué, de haut en bas) dans une publication de routeur NDP au destinataire, qui les utilise ensuite dans le même ordre. Vous devez sélectionner un serveur et **Déplacer en haut** ou **Déplacer en bas** pour modifier l’ordre des serveurs ou **Supprimer** un serveur de la liste lorsque vous n’en avez plus besoin. Saisissez la **Lifetime (Durée de vie)** en secondes. Il s'agit de la durée de temps maximale pendant laquelle le client peut utiliser le serveur RDNS donné pour résoudre des noms de domaine. La plage est comprise entre 4 et 3,600 ; la valeur par défaut est 1,200.
Liste de recherche de domaine	**Agréger via l'interface Ethernet** > **IPv6** > **Prise en charge DNS, type = client DHCPv6 ou hérité**	Activez et sélectionnez : • **DHCPv6**— Pour que le serveur DHCPv6 envoie les informations de la liste de recherche de domaine. • **Manuak (Manuel)** — Pour configurer manuellement la liste de recherche de domaine. Si vous choisissez **Manual (manuel)**, **Add (ajoutez)** et configurez un ou plusieurs noms de **Domain (domaine)** (suffixes) pour la liste de recherche DNS (DNSSL). La longueur de suffixe maximale est de 255 octets. Une liste de recherche DNS est une liste de suffixes de domaine qu’un routeur de client DNS ajoute (un à la fois) à un nom de domaine non qualifié avant d’entrer le nom dans une requête DNS, en utilisant un nom de domaine complet dans la requête DNS. Par exemple, si un client DNS essaie de soumettre une requête DNS pour le nom « qualité » sans suffixe, le routeur ajoute un point et le premier suffixe DNS de la liste de recherche DNS au nom et transmet ensuite la requête DNS. Si le premier suffixe DNS sur la liste est « company.com », la requête DNS qui résulte du routeur est « quality.company.com » pour le nom de domaine complet. Si la requête DNS échoue, le routeur ajoute le deuxième suffixe DNS de la liste au nom non qualifié et transmet une nouvelle requête DNS. Le routeur essaie les suffixes DNS jusqu’à

Paramètres d’une interface agrégée	Configuré dans	Description
		ce qu’une recherche DNS soit fructueuse (il ignore les suffixes restants) ou jusqu’à ce que le routeur ait essayé tous les suffixes de la liste. Configurez le pare-feu avec les suffixes que vous souhaitez fournir au routeur du client DNS dans une option Découverte de voisins DNSSL ; le client DNS recevant l’option DNSSL utilise les suffixes pour ses requêtes DNS non qualifiées. Vous pouvez configurer un maximum de huit noms de domaine (suffixes) pour une liste de recherche DNS que le pare-feu envoie (dans l’ordre, de haut en bas) dans une publication de routeur NDP au destinataire, qui utilise ces adresses dans le même ordre. Sélectionnez un suffixe et utilisez les options **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)** pour modifier l’ordre des suffixes ou **Delete (Supprimer)** un suffixe lorsque vous n’en avez plus besoin. Entrez une **Lifetime (durée de vie)** en secondes, qui est la durée maximale pendant laquelle le client peut utiliser la liste de recherche de domaine spécifique. La plage est comprise entre 4 et 3,600 ; la valeur par défaut est 1,200.

Réseau > Interfaces > VLAN

Une interface VLAN peut fournir un routage dans un réseau de couche 3 (IPv4 ou IPv6). Vous pouvez ajouter un ou plusieurs ports Ethernet de niveau 2 (reportez-vous à la section Interface de niveau 2 de la série PA-7000) à une interface VLAN.

Paramètres d'une interface VLAN	Configuré dans	Description
Nom de l'interface	**Interface VLAN**	**Interface Name (Nom de l'interface)** en lecture seule est défini sur **vlan**. Dans le champ adjacent, saisissez un suffixe numérique (1 à 9 999) pour identifier l'interface.
Commentaire		Saisissez une description de l'interface (facultatif).
profil NetFlow ;		Si vous voulez exporter le trafic IP unidirectionnel traversant une interface d'entrée vers un serveur NetFlow, sélectionnez le profil de serveur ou cliquez sur **Netflow Profile (Profil Netflow)** pour définir un nouveau profil (Voir Périphérique > Profils de serveur > NetFlow). Sélectionnez **None (Aucun)** pour supprimer l'affectation de serveur NetFlow de l'interface.
Réseau local virtuel	**Interface VLAN** > **Configuration**	Sélectionnez une VLAN ou cliquez sur **VLAN** pour en définir une nouvelle (reportez-vous à la section Réseau > VLAN). Sélectionnez **None (Aucun)** pour supprimer l'affectation de VLAN de l'interface.
Virtual Router (routeur virtuel - VR)		Affectez un routeur virtuel à l'interface ou cliquez sur **Virtual Router (Routeur virtuel)** pour en définir un nouveau (voir Réseau > Routeurs virtuels). Sélectionnez **None (Aucun)** pour supprimer l'affectation de routeur virtuel de l'interface.
Virtual System (système virtuel - vsys)		Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système virtuel (vsys) pour l'interface ou cliquez sur le lien **Virtual System (Système virtuel)** pour en définir un nouveau.
Zone de sécurité		Sélectionnez une zone de sécurité pour l'interface ou cliquez sur **Zone** pour en définir une nouvelle. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de l'interface.
Adresse IPv4		
Type	**Interface VLAN** > **IPv4**	Sélectionnez la méthode d'affectation d'un type d'adresse IPv4 à l'interface : • **Static (Statique)** - Vous devez indiquer manuellement l'adresse IP.

Paramètres d’une interface VLAN	Configuré dans	Description
		• **DHCP Client (Client DHCP)** - Permet à l'interface d'agir en tant que client DHCP (Dynamic Host Configuration Protocol/ protocole d'attribution dynamique des adresses) et de recevoir une adresse IP assignée de façon dynamique. *Les pare-feu en mode haute disponibilité (HD) active/active ne prennent pas en charge le client DHCP.* Les options affichées dans l'onglet varient selon le choix de la méthode de sélection d'adresse IP.
Adresse IPv4, Type = Statique		
Adresse IP	**Interface VLAN** > **IPv4**	Cliquez sur **Add (Ajouter)**, puis suivez l'une des étapes ci-dessous pour indiquer l'adresse IP statique et le masque réseau de l'interface. • Saisissez l’entrée en notation CIDR (Classing Inter-Domain Routing, routage inter domaine sans classes) : *adresse_ip/masque* (par exemple, 192.168.2.0/24). • Sélectionnez un objet d'adresse existant de type **IP netmask (Masque réseau IP)**. • Créez un objet d’**Address (Adresse)** de type **IP netmask (Masque réseau IP)**. Vous pouvez saisir plusieurs adresses IP pour l'interface. La base d'informations de transfert (FIB) utilisée par votre système détermine le nombre maximum d'adresses IP. Il est possible de **Supprimer** une adresse IP lorsque vous n’en avez plus besoin.
Adresse IPv4, Type = Client DHCP		
Activer	**Interface VLAN** > **IPv4**	Sélectionnez pour activer le client DHCP sur l’interface.
Créer automatiquement un itinéraire par défaut en direction de la passerelle par défaut fournie par le serveur		Sélectionnez pour créer automatiquement un itinéraire par défaut pointant vers la passerelle par défaut fournie par le serveur DHCP.

Paramètres d’une interface VLAN	Configuré dans	Description
Envoyer le nom d'hôte		Sélectionnez cette option pour configurer le pare-feu (en tant que client DHCP) pour l’envoie du nom d’hôte de l’interface (option 12) au serveur DHCP. Si vous envoyez un nom d'hôte, par défaut, le nom d’hôte du pare-feu est alors le choix indiqué dans le champ Nom d'hôte. Vous pouvez envoyer ce nom ou saisir un nom d’hôte personnalisé (64 caractères maximum, y compris des lettres majuscules ou minuscules, des chiffres, des points, des tirets et des traits de soulignement).
Mesure d'itinéraire par défaut		Pour l’itinéraire entre le pare-feu et le fournisseur de serveur DHCP, vous pouvez saisir une mesure d’itinéraire (un niveau de priorité) à associer à l’itinéraire par défaut et à utiliser pour la sélection du chemin (plage de 1 à 65 535 ; il n’y a aucune valeur définie par défaut). Plus la valeur numérique est grande, plus le niveau de priorité est élevé.
Afficher les informations d'exécution du client DHCP		Sélectionnez pour afficher tous les paramètres reçus par le serveur DHCP, y compris le statut du bail DHCP, l’attribution de l’adresse IP dynamique, le masque de sous-réseau, la passerelle, les paramètres du serveur (DNS, NTP, domaine, WINS, NIS, POP3 et SMTP).
Adresse IPv6, Type = Statique		
Activer IPv6 sur l'interface	**Interface VLAN** > **IPv6**	Sélectionnez pour activer l’adressage IPv6 sur cette interface.
ID de l'interface		Saisissez l'identifiant unique étendu sur 64'A0;bits (EUI-64) au format hexadécimal (par exemple, 00:26:08:FF:FE:DE:4E:29). Si ce champ n'est pas renseigné, le pare-feu utilise l'identifiant unique étendu sur 64'A0;bits (EUI-64) généré à partir de l'adresse MAC de l'interface physique. Si vous activez l'option **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** lors de l'ajout d'une adresse, le pare-feu utilise l'ID de l'interface comme partie hôte de l'adresse.
Adresse	**Interface VLAN** > **IPv6** > **Affectation d’adresse**	Ajoutez une adresse IPv6 et une longueur de préfixe (par exemple, 2001:400:f00::1/64). Vous pouvez également sélectionner un objet d'adresse IPv6 existant ou en créer un nouveau.
Activer l’adresse sur l’interface		Activez l’adresse IPv6 sur l’interface.

Paramètres d’une interface VLAN	Configuré dans	Description
Utiliser l’ID de l’interface comme partie hôte.		Sélectionnez cette option pour utiliser l’**ID de l’interface** comme partie hôte de l’adresse IPv6.
Anycast		Sélectionnez cette option pour inclure le routage via le nœud le plus proche.
Envoyer RA	**Interface VLAN** > **IPv6** > **Affectation d’adresse**	Sélectionnez cette option pour activer la publication de routeur (RA) pour cette adresse IP. Lorsque vous sélectionnez cette option, vous devez également **Enable Router Advertisement (activer la publication du routeur)** dans l’onglet **Router Advertisement (Annonce du routeur)**. Les champs restants s'appliquent uniquement si vous activez **Send RA (envoyer RA)**. • **Valid Lifetime (Durée de vie valide)** - La durée, en secondes, pendant laquelle le pare-feu considère l’adresse comme valide. La durée de vie valide doit être supérieure ou égale à **Preferred Lifetime (durée de vie préférée)**. La valeur par défaut est 2 592 000. • **Preferred Lifetime (Durée de vie préférée)** - La durée, en secondes, pendant laquelle l’adresse valide est préférée, ce qui signifie que le pare-feu peut l’utiliser pour envoyer et recevoir du trafic. Lorsque la durée de vie préférée expire, le pare-feu ne peut plus utiliser l’adresse pour établir de nouvelles connexions, mais toute connexion existante reste valide jusqu’à ce qu’elle dépasse la **`Valid Lifetime (Durée de vie valide)`**. La valeur par défaut est 604 800. • **On-link (Sur la liaison)** – Sélectionnez cette option si les systèmes dont les adresses IP sont comprises dans le préfixe publié sont accessibles sans routeur. • **Autonomous (Autonome)** - Sélectionnez cette option si les systèmes peuvent créer une adresse IP de façon indépendante en combinant le préfixe publié et l’ID d’une interface.
Adresse IPv6, Type = Client DHCPv6		
Accepter l'itinéraire annoncé par le routeur	**Interface VLAN** > **IPv6** > **Attribution d'adresse,**	Sélectionnez cette option pour autoriser le client DHCPv6 à accepter le RA du serveur DHCP.

Paramètres d’une interface VLAN	Configuré dans	Description
Mesure d'itinéraire par défaut	**Type = Client DHCPv6**	Saisissez une métrique de route par défaut pour la route entre l'interface et le FAI ; la plage est de 1 à 65 535 ; la valeur par défaut est 10.
Préférence		Sélectionnez la préférence de l'interface client DHCPv6 (**low (faible)**, **medium (moyen)**ou **high (élevé)**) de sorte que, dans le cas où vous avez deux interfaces (chacune étant connectée à un FAI différent pour la redondance), vous puissiez attribuer à l'un des FAI une préférence plus élevée que la l'interface avec l'autre FAI. Le FAI connecté à l'interface préférée sera le FAI qui fournit le préfixe délégué à envoyer à une interface faisant face à l'hôte. Si les interfaces ont la même préférence, les deux FAI fournissent un préfixe délégué et l'hôte décide quel préfixe utiliser.
Activer l'adresse IPv6	**Interface VLAN** > **IPv6** > **Attribution d'adresse, Type = Client DHCPv6** > **Options DHCPv6**	Activez l'adresse IPv6 reçue pour ce client DHCPv6.
Adresse non temporaire		Demandez une adresse non temporaire que le pare-feu doit attribuer à cette interface client DHCPv6 qui fait face au routeur délégant et au FAI. Sélectionnez Adresse non temporaire s’il est acceptable que l’interface ait un niveau de sécurité inférieur (car l’adresse a une durée de vie plus longue). *Que vous demandiez une adresse non temporaire ou une adresse temporaire pour l'interface dépend de votre discrétion et de la capacité du serveur DHCPv6; certains serveurs ne peuvent fournir qu'une adresse temporaire. La meilleure pratique consiste à sélectionner à la fois Adresse non temporaire et Adresse temporaire, auquel cas le pare-feu préférera l'Adresse non temporaire.*
Adresse temporaire		Demandez une adresse temporaire que le pare-feu doit attribuer à cette interface client DHCPv6 qui fait face au routeur délégant et au FAI. Sélectionnez Adresse temporaire pour un niveau de sécurité supérieur, car l'adresse est destinée à être utilisée pendant une courte période.
Validation rapide		Sélectionnez cette option pour utiliser le processus DHCP des messages Solliciter et Répondre, plutôt que le processus des messages Solliciter, Annoncer, Demander et Répondre.

Paramètres d'une interface VLAN	Configuré dans	Description
Activer la délégation de préfixe	**Interface VLAN** > **IPv6** > **Attribution d'adresse, Type = Client DHCPv6** > **Délégation de préfixe**	Activez la délégation de préfixe pour permettre au pare-feu de prendre en charge la fonctionnalité de délégation de préfixe. Cela signifie que l'interface accepte un préfixe du serveur DHCPv6 en amont et place le préfixe dans le pool de préfixes que vous sélectionnez, à partir duquel le pare-feu délègue un préfixe à un hôte via SLAAC. La possibilité d'activer ou de désactiver la délégation de préfixe pour une interface permet au pare-feu de prendre en charge plusieurs FAI (un FAI par interface). L'activation de la délégation de préfixe sur cette interface contrôle quel FAI fournit le préfixe. Le préfixe délégué reçu du serveur DHCP ne peut pas être utilisé sur l'interface qui l'a demandé.
Indice de longueur du préfixe DHCP		Sélectionnez pour permettre au pare-feu d'envoyer une longueur de préfixe DHCPv6 préférée au serveur DHCPv6.
Longueur du préfixe DHCP (bits)		Entrez la longueur de préfixe DHCPv6 préférée dans la plage de 48 à 64 bits, qui est envoyée comme indice au serveur DHCPv6. *Demander une longueur de préfixe de 48, par exemple, laisse 16 bits restants pour les sous-réseaux (64-48), ce qui indique que vous avez besoin de nombreuses subdivisions de ce préfixe pour déléguer. D'autre part, demander une longueur de préfixe de 63 laisse 1 bit pour ne déléguer que deux sous-réseaux. Sur les 128 bits, il reste encore 64 bits pour l'adresse de l'hôte.*
Nom du pool de préfixe		Entrez un nom pour le pool de préfixes dans lequel le pare-feu stocke le préfixe reçu. Le nom doit être unique et contenir un maximum de 63 caractères alphanumériques, traits d'union, points et traits de soulignement. *Utilisez un nom de pool de préfixes qui reflète le FAI pour une reconnaissance facile.*
Adresse IPv6, Type = Hérité		
Nom	**Interface VLAN** > **IPv6** > **Attribution d'adresse, type = hérité**	**Add (Ajoutez)** un pool en saisissant un nom de pool. Le nom peut comporter au maximum 63 caractères alphanumériques, traits d'union, points et traits de soulignement.
Type d'adresse		Sélectionnez parmi les choix suivants :

Paramètres d’une interface VLAN	Configuré dans	Description
		• **GUA from pool (AUG du pool)**— Adresse Unidiffusion globale (AUG) provenant du pool de préfixes choisi. Obtenir ce GUA est l’objectif de l’utilisation de la délégation de préfixe. • **ULA**—Unique Local Address est une adresse privée dans la plage d'adresses fc00::/7 pour la connectivité au sein d'un réseau privé. Sélectionnez ULA s'il n'y a pas de serveur DHCP.
Activer sur l'interface		Activez l’adresse IPv6 sur l’interface.
Pool de préfixes		Sélectionnez le pool de préfixes à partir duquel obtenir le GUA.
Assignment Type (Type d'affectation)	**Interface VLAN** > **IPv6** > **Attribution d'adresse, type = hérité**	Sélectionnez le type de devoir : • **Dynamic (Dynamique)** — Le client DHCPv6 est responsable du choix d'un identifiant pour configurer l'interface héritée. • **Dynamic with Identifier (Dynamique avec identifiant)**— Vous êtes responsable du choix d'un identifiant dans la plage de 0 à 4 000 et de la gestion d'un identifiant unique sur les clients DHCPv6.
Envoyer la publication des routeurs		Sélectionnez pour envoyer des annonces de routeur (AR) de l'interface aux hôtes LAN.
On-Link		Sélectionnez si les systèmes qui disposent d’adresses dans le préfixe sont accessibles sans routeur.
Autonome		Sélectionnez cette option si les systèmes peuvent créer une adresse IP de façon indépendante en combinant le préfixe publié et l’ID d’une interface.
Activer la détection des doublons d'adresses	**Interface VLAN** > **IPv6** > **Résolution d'adresse**	Sélectionnez cette option pour activer la détection des doublons d’adresses (DAD), ce qui vous permet d’indiquer le nombre de **Attempts (Tentatives) DAD**.
Tentatives DAD		Indiquez le nombre de tentatives DAD dans l'intervalle de sollicitation de voisins (**NS Interval (intervalle NS)**) avant que la tentative d'identification n'échoue (intervalle compris entre 1 et 10 ; valeur par défaut : 1).

Paramètres d’une interface VLAN	Configuré dans	Description
Durée d'accessibilité		Indiquez la durée (en secondes) pendant laquelle un voisin reste accessible après une requête et une réponse réussies (plage de 1 à 36 000 ; valeur par défaut de 30).
Intervalle (s)		Indiquez le nombre de secondes pour des tentatives DAD avant qu'un échec ne soit signalé (intervalle compris entre 1 et 10 ; valeur par défaut : 1).
Activer la surveillance NDP		Sélectionnez cette option pour activer la surveillance du Protocole de découverte des voisins. Lorsqu’il est activé, vous pouvez sélectionner le NDP ( dans la colonne Fonctions) et afficher des informations telles que l’adresse IPv6 d’un voisin découverte par le pare-feu, l’adresse MAC et User-ID correspondants (selon la situation la plus favorable).
Adresse IPv6, Type = Statique ou Type = Hérité		
Activer la publication des routeurs	**Interface VLAN** > **IPv6** > **Annonce de routeur, Type = Statique ou Type = Hérité**	Sélectionnez cette option pour assurer la Découverte de voisins sur les interfaces IPv6 et configurer les autres champs de cette section. Les clients DNS IPv6 qui reçoivent les messages de publication de routeur utilisent ces informations. La RA permet au pare-feu d'agir en tant que passerelle par défaut pour les hôtes IPv6 qui ne sont pas configurés de façon statique et de fournir à l'hôte un préfixe IPv6 qui lui permet de configurer une adresse. Vous pouvez utiliser un serveur DHCPv6 distinct conjointement avec cette fonctionnalité pour fournir un DNS et d'autres paramètres aux clients. Il s’agit d’un paramètre global de l’interface. Si vous souhaitez définir des options de publication de routeur pour les adresses IP individuelles, vous devez **Ajouter** une Adresse dans la table d’adresses IP et la configurer. Si vous définissez des options de publication de routeur pour une adresse IP, vous devez **nable Router Advertisement (Activer la publication de routeur)** sur l’interface.
Intervalle min. (s)		Indiquez l’intervalle minimum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 3 et 1 350 ; valeur par défaut : 200). Le pare-feu envoie les publications de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales configurées.

Paramètres d’une interface VLAN	Configuré dans	Description
Intervalle max. (s)		Indiquez l’intervalle maximum, en secondes, entre les publications de routeur envoyées par le pare-feu (plage comprise entre 4 et 1 800 ; valeur par défaut : 600). Le pare-feu envoie les publications de routeur à des intervalles aléatoires compris entre les valeurs minimales et maximales configurées.
Limite de saut		Indiquez la limite de saut à appliquer aux clients pour les paquets sortants (intervalle compris entre 1 et 255 ; valeur par défaut : 64). Saisissez **0** pour indiquer l’absence de limite de saut.
MTU de liaison	**Interface VLAN** > **IPv6** > **Annonce de routeur, Type = Statique ou Type = Hérité**	Indiquez l’unité de transmission maximale (MTU) de liaison à appliquer aux clients (la plage est comprise entre 1 280 et 1 500) ou indiquez **unspecified (non spécifié)**, ce qui correspond à la valeur par défaut du système.
Durée d'accessibilité (ms)		Indiquez la durée d'accessibilité (en millisecondes) que le client va utiliser pour supposer l'accessibilité d'un voisin après avoir reçu un message de confirmation d'accessibilité (la plage est comprise entre 0 et 3 600 000), ou indiquez **unspecified (non spécifié)**, ce qui correspond à la valeur par défaut du système.
Durée de retransmission (ms)		Indiquez le minuteur de retransmission, qui détermine la durée d'attente du client (en millisecondes) avant la retransmission des messages de sollicitation de voisins. (la plage est comprise entre 0 et 4 294 967 295) ou indiquez **unspecified (non spécifié)**, ce qui correspond à la valeur par défaut du système.
Durée de vie du routeur (s)		Indiquez la durée, en secondes, pendant laquelle le client utilise le pare-feu comme passerelle par défaut (plage comprise entre 0 et 9 000 ; valeur par défaut : 1 800). Une valeur de 0 indique que le pare-feu n'est pas la passerelle par défaut. Lorsque la durée de vie expire, le client supprime l'entrée du pare-feu de sa liste de routeurs par défaut et utilise un autre routeur comme passerelle par défaut.
Préférence de routeur		Si le segment de réseau dispose de plusieurs routeurs IPv6, le client utilise ce champ pour sélectionner un routeur préféré. Indiquez si le routeur de pare-feu publié a une priorité **High (Élevée)**, **Medium (Moyenne)** (par défaut) ou **Low (Faible)** par rapport aux autres routeurs se trouvant sur le segment.
Durée d'accessibilité (ms)	**Interface VLAN** > **IPv6** > **Annonce de routeur, Type**	Indiquez la durée d'accessibilité (en millisecondes) que le client va utiliser pour supposer l'accessibilité d'un voisin après avoir reçu un message de confirmation d'accessibilité (la plage est comprise

Paramètres d'une interface VLAN	Configuré dans	Description
	= Statique ou Type = Hérité	entre 0 et 3 600 000), ou indiquez **unspecified (non spécifié)**, ce qui correspond à la valeur par défaut du système.
Durée de retransmission (ms)		Indiquez le minuteur de retransmission, qui détermine la durée d'attente du client (en millisecondes) avant la retransmission des messages de sollicitation de voisins. (la plage est comprise entre 0 et 4 294 967 295) ou indiquez **unspecified (non spécifié)**, ce qui correspond à la valeur par défaut du système.
Durée de vie du routeur (s)		Indiquez la durée, en secondes, pendant laquelle le client utilise le pare-feu comme passerelle par défaut (plage comprise entre 0 et 9 000 ; valeur par défaut : 1 800). Une valeur de 0 indique que le pare-feu n'est pas la passerelle par défaut. Lorsque la durée de vie expire, le client supprime l'entrée du pare-feu de sa liste de routeurs par défaut et utilise un autre routeur comme passerelle par défaut.
Préférence de routeur		Si le segment de réseau dispose de plusieurs routeurs IPv6, le client utilise ce champ pour sélectionner un routeur préféré. Indiquez si le routeur de pare-feu publié a une priorité **High (Élevée)**, **Medium (Moyenne)** (par défaut) ou **Low (Faible)** par rapport aux autres routeurs se trouvant sur le segment.
Configuration gérée		Sélectionnez cette option pour indiquer au client que les adresses sont disponibles via DHCPv6.
Autre configuration		Sélectionnez pour indiquer au client que d'autres informations d'adresse (par exemple, des paramètres associés au DNS) sont disponibles via DHCPv6.
Vérification de cohérence		Sélectionnez si vous souhaitez que le pare-feu vérifie que les RA reçues des autres routeurs publient des informations cohérentes sur la liaison. Le pare-feu consigne toutes les incohérences dans un journal système de type **Ipv6nd**.
Adresse IPv6, prise en charge DNS (Type = Statique)		
Inclure les informations DNS dans la publication de routeur	**Interface VLAN** > **IPv6** > **Prise en charge DNS, type = statique**	DNS Support Tab (Onglet Prise en charge DNS) est disponible si vous sélectionnez l'option **Enable Router Advertisement (Activer la publication du routeur)** dans l'onglet Publication du routeur. Sélectionnez le pare-feu pour transmettre des informations DNS vers les publications du routeur NDP à partir de cette interface Ethernet IPv6. Les autres champs de Prise en charge DNS (serveur,

Paramètres d'une interface VLAN	Configuré dans	Description
		durée de vie, suffixe et durée de vie) ne sont visibles qu'après sélection de cette option.
Serveur		Il est possible d'**Ajouter** une ou plusieurs adresses de serveur DNS (RDNS) récursives pour que le pare-feu envoie des publications de routeur NDP à partir de cette interface Ethernet IPv6. Les serveurs RDNS envoient une série de demandes de recherche DNS aux serveurs DNS racine et aux serveurs DNS autoritaires pour finalement fournir une adresse IP au client DNS. Vous pouvez configurer un maximum de huit Serveurs RDNS que le pare-feu envoie (dans l'ordre indiqué, de haut en bas) dans une publication de routeur NDP au destinataire, qui les utilise ensuite dans le même ordre. Vous devez sélectionner un serveur et **Déplacer en haut** ou **Déplacer en bas** pour modifier l'ordre des serveurs ou **Supprimer** un serveur de la liste lorsque vous n'en avez plus besoin.
Durée de vie		Saisissez le nombre maximum de secondes après que le client DNS IPv6 a reçu la publication du routeur avant que le client puisse utiliser un serveur RDNS afin de résoudre les noms de domaine (la plage est comprise entre la valeur de **Max Interval (sec) [Intervalle maximal (s)]** et deux fois **Max Interval (sec) [Intervalle maximal (s)]** ; la valeur par défaut est 1 200).
Liste de recherche de domaine		Il vous faut **ajouter** un ou plusieurs noms de domaine (suffixes) pour la liste de recherche DNS (DNSSL). 255 octets maximum. Une liste de recherche DNS est une liste de suffixes de domaine qu'un routeur de client DNS ajoute (un à la fois) à un nom de domaine non qualifié avant d'entrer le nom dans une requête DNS, en utilisant un nom de domaine complet dans la requête. Par exemple, si un client DNS essaie de soumettre une requête DNS pour le nom « qualité » sans suffixe, le routeur ajoute un point et le premier suffixe DNS de la liste de recherche DNS au nom et transmet la requête DNS. Si le premier suffixe DNS sur la liste est « company.com », la requête qui résulte du routeur est « quality.company.com » pour le nom de domaine complet. Si la requête DNS échoue, le routeur ajoute le deuxième suffixe DNS de la liste au nom non qualifié et transmet une nouvelle requête DNS. Le routeur utilise les suffixes DNS jusqu'à ce qu'une recherche DNS soit fructueuse (il ignore les suffixes restants) ou jusqu'à ce que le routeur ait essayé tous les suffixes de la liste. Configurez le pare-feu avec les suffixes que vous souhaitez fournir au routeur du client DNS dans une option Découverte de

Paramètres d'une interface VLAN	Configuré dans	Description
		voisins DNSSL ; le client DNS recevant l'option DNSSL utilise les suffixes pour ses requêtes DNS non qualifiées. Vous pouvez configurer un maximum de huit noms de domaine (suffixes) pour une liste de recherche DNS que le pare-feu envoie (dans l'ordre, de haut en bas) dans une publication de routeur NDP au destinataire, qui les utilise dans le même ordre. Sélectionnez un suffixe et utilisez les options **Déplacer vers le haut** ou **Déplacer vers le bas** pour modifier l'ordre ou **Supprimer** un suffixe lorsque vous n'en avez plus besoin.
Durée de vie		Saisissez le nombre maximal de secondes après que le client DNS IPv6 reçoit la publication du routeur lui indiquant qu'il peut utiliser un nom de domaine (suffixe) sur la liste de recherche DNS (la plage est comprise entre la valeur de **Max Interval (sec) [Intervalle maximal (s)]** et deux fois **Max Interval (sec) [Intervalle maximal (s)]** ; la valeur par défaut est 1 200).
Adresse IPv6, prise en charge DNS (Type = Client DHCPv6 ou Type = Hérité)		
Serveur de noms récursif DNS	**Interface VLAN** > **IPv6** > **Prise en charge DNS, type = client DHCPv6 ou type = hérité**	Activez et sélectionnez : • **DHCPv6**—Pour que le serveur DHCPv6 envoie les informations DNS Recursive Name Server. • **Manual (Manuel)** — Pour configurer manuellement le serveur de noms DNS Recursive. Si vous choisissez **Manual (Manuel)**, **Add (Ajouter)** une adresse de **Server (serveur)** DNS (RDNS) récursive pour que le pare-feu envoie des annonce de routeur NDP à partir de cette interface VLAN IPv6. Les serveurs RDNS envoient une série de requêtes de recherches DNS aux serveurs DNS racines et aux serveurs DNS fiables pour finalement fournir une adresse IP au client DNS. Vous pouvez configurer un maximum de huit serveurs RDNS que le pare-feu envoie (dans l'ordre indiqué, de haut en bas) dans une publication de routeur NDP au destinataire, qui les utilise ensuite dans le même ordre. Sélectionner un serveur et **Move up (Déplacer en haut)** ou **Move down (Déplacer en bas)** pour modifier l'ordre des serveurs ou **Delete (Supprimer)** un serveur de la liste lorsque vous n'en avez plus besoin.
Durée de vie		Saisissez le nombre maximum de secondes qui s'est écoulé après réception de la publication du routeur par le client DNS IPv6. Celle-ci stipule qu'il est possible d'utiliser les serveurs RDNS pour résoudre les noms de domaine (l'intervalle est la valeur de

Paramètres d'une interface VLAN	Configuré dans	Description
		l'Intervalle max. [s] jusqu'à deux fois l'Intervalle maximal ; la valeur par défaut est 1 200).
Liste de recherche de domaine	**Interface VLAN** > **IPv6** > **Prise en charge DNS, type = client DHCPv6 ou type = hérité**	Activez et sélectionnez : • **DHCPv6**: pour que le serveur DHCPv6 envoie la liste de recherche de domaine. • **Manuak (Manuel)** — Pour configurer manuellement la liste de recherche de domaine. Si vous choisissez **Manual (manuel)**, **Add (ajoutez)** et configurez un ou plusieurs noms de **Domain (domaine)** (suffixes) pour la liste de recherche DNS (DNSSL). La longueur de suffixe maximale est de 255 octets. Une liste de recherche DNS est une liste de suffixes de domaine qu'un routeur de client DNS ajoute (un à la fois) à un nom de domaine non qualifié avant d'entrer le nom dans une requête DNS, en utilisant un nom de domaine complet dans la requête DNS. Par exemple, si un client DNS essaie de soumettre une requête DNS pour le nom « qualité » sans suffixe, le routeur ajoute un point et le premier suffixe DNS de la liste de recherche DNS au nom et transmet ensuite la requête DNS. Si le premier suffixe DNS sur la liste est « company.com », la requête DNS qui résulte du routeur est « quality.company.com » pour le nom de domaine complet. Si la requête DNS échoue, le routeur ajoute le deuxième suffixe DNS de la liste au nom non qualifié et transmet une nouvelle requête DNS. Le routeur essaie les suffixes DNS jusqu'à ce qu'une recherche DNS soit fructueuse (il ignore les suffixes restants) ou jusqu'à ce que le routeur ait essayé tous les suffixes de la liste. Configurez le pare-feu avec les suffixes que vous souhaitez fournir au routeur du client DNS dans une option Découverte de voisins DNSSL ; le client DNS recevant l'option DNSSL utilise les suffixes pour ses requêtes DNS non qualifiées. Vous pouvez configurer un maximum de huit noms de domaine (suffixes) pour une liste de recherche DNS que le pare-feu envoie (dans l'ordre, de haut en bas) dans une publication de routeur NDP au destinataire, qui utilise ces adresses dans le même ordre. Sélectionnez un suffixe et utilisez les options **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)** pour modifier l'ordre des suffixes ou **Delete (Supprimer)** un suffixe lorsque vous n'en avez plus besoin.

Paramètres d’une interface VLAN	Configuré dans	Description
Durée de vie		Saisissez le nombre maximum de secondes qui s’est écoulé après réception de la publication du routeur par le client DNS IPv6. Celle-ci stipule qu’il est possible d’utiliser un nom de domaine (suffixe) sur la liste de recherche DNS (l’intervalle est la valeur de l’Intervalle max. [s] jusqu’à deux fois l'intervalle maximal ; la valeur par défaut est 1 200).
Avancé		
Profil de gestion	**Interface VLAN** > **Avancé** > **Autre info**	**Management Profile (Profil de gestion)** - Sélectionnez un profil qui définit les protocoles (par exemple, SSH, Telnet et HTTP) à utiliser pour gérer le pare-feu dans cette interface. Sélectionnez **None (Aucune)** pour supprimer l'affectation de profil de l'interface.
MTU		Saisissez l’unité de transmission maximale (MTU) en octets par paquet envoyé sur cette interface (plage de 576 à 9 192 ; par défaut 1 500). Si les machines situées de chaque côté du pare-feu effectuent une détection du chemin MTU (PMTUD) et que l'interface reçoit un paquet dépassant la valeur MTU, le pare-feu renvoie à la source un message de *fragmentation ICMP obligatoire* indiquant que le paquet est trop volumineux.
Ajuster TCP MSS		Sélectionnez pour ajuster la taille de segment maximale (MSS) afin de tolérer les octets de tous les en-têtes qui respectent la taille en octets de la MTU de l’interface. La taille en octets de la MTU moins la taille d'ajustement de la MSS équivaut à la taille en octets de la MSS, laquelle varie selon le protocole IP : • **IPv4 MSS Adjustment Size (Taille d'ajustement MSS IPv4)** - intervalle compris entre 40 et 300 ; valeur par défaut : 40. • **IPv6 MSS Adjustment Size (Taille d'ajustement MSS IPv4)** - intervalle compris entre 60 et 300 ; valeur par défaut : 60. Servez-vous de ces paramètres pour faire face aux situations où un **tunnel** réseau nécessite une plus petite MSS. Si un paquet a plus d'octets que la MSS sans faire l'objet d'une fragmentation, ce paramètre permet son ajustement. L'encapsulation rallonge les en-têtes. Il peut donc s'avérer utile de configurer la taille d'ajustement MSS de façon à autoriser les octets d'éléments tels que des en-têtes MPLS ou le trafic par tunnel ayant une étiquette VLAN.
Adresse IP Adresse MAC	**Interface VLAN** >	Pour ajouter une ou plusieurs entrées ARP (Address Resolution Protocol) statiques, cliquez sur **Add (Ajouter)**, saisissez une adresse IP et son adresse matérielle associée (MAC) et sélectionnez

Paramètres d’une interface VLAN	Configuré dans	Description
Interface	**Avancé** > **Entrées ARP**	une interface de niveau 3 pouvant accéder à l'adresse matérielle. Pour supprimer une entrée, sélectionnez-la et cliquez sur **Delete (Supprimer)**. Les entrées ARP statiques minimisent le traitement ARP et protègent des attaques par hôte interposé pour les adresses définies.
Adresse IPv6 Adresse MAC	**Interface VLAN** > **Avancé** > **Entrées ND**	Afin de fournir des informations de voisinage pour NDP (Neighbor Discovery Protocol / protocole de découverte des voisins) cliquez sur **Ajouter** et saisissez l’adresse IPv6 et l’adresse Mac du voisin.
Activer le proxy NDP	**Interface VLAN** > **Avancé** > **Proxy NDP**	Sélectionnez cette option pour activer le proxy NDP (Neighbor Discovery Protocol) sur l'interface. Le pare-feu répondra aux paquets ND demandant des adresses MAC pour les adresses IPv6 de cette liste. Dans la réponse ND, le pare-feu envoie sa propre adresse MAC pour l'interface et demande tous les paquets destinés à ces adresses. (**Recommandé**) Activez le proxy NDP si vous utilisez NPTv6 (Network Prefix Translation/traduction de préfixe réseau IPv6). Si l'option **Enable NDP Proxy (Activer le proxy NDP)** est sélectionnée, vous pouvez filtrer de nombreuses entrées **Address (Adresse)** : saisissez d'abord un filtre et appliquez-le (la flèche verte).
Adresse		**Add (Ajoutez)** une ou plusieurs adresses IPv6, plages d'adresses IP, sous-réseaux IPv6 ou objets d'adresse pour lesquels le pare-feu agira comme proxy NDP. Idéalement, l'une de ces adresses est identique à celle de la traduction source dans NPTv6. L'ordre des adresses n'a pas d'importance. Si l’adresse est un sous-réseau, le pare-feu enverra une réponse ND pour toutes les adresses du sous-réseau. Par conséquent, il est recommandé d’ajouter également les voisins IPv6 du pare-feu et de cliquer sur **Negate (Ignorer)** pour que le pare-feu ne réponde pas à ces adresses IP.
Inverser		Sélectionnez **Negate (Ignorer)** en regard d'une adresse afin d'empêcher le proxy NDP pour cette adresse. Vous pouvez ignorer un sous-ensemble de la plage d'adresses IP ou du sous-réseau IP spécifié.
Paramètres	**Interface VLAN** > **Avancé** > **DDNS**	Sélectionnez les paramètres pour que les champs DDNS puissent être configurés.

Paramètres d'une interface VLAN	Configuré dans	Description
Activer		Activer DDNS sur l'interface Vous devez d'abord activer DDNS pour le configurer. (Si vous n'avez pas terminé de configurer DDNS, vous pouvez enregistrer la configuration sans l'activer, ce qui vous évitera de perdre la configuration partielle.)
Intervalle de mise à jour (jours)		Saisissez l'intervalle (en jours) entre les mises à jour que le pare-feu envoie au serveur DDNS pour mettre à jour les adresses IP associées aux FQDN (la plage est comprise entre 1 et 30 ; la valeur par défaut est 1). *Le pare-feu met également à jour DDNS à la réception d'une nouvelle adresse IP pour l'interface du serveur DHCP.*
Profil du certificat		Sélectionnez un profil de certificat que vous avez créé (ou créez-en un nouveau) pour vérifier le service DDNS. Le service DDNS présente au pare-feu un certificat signé par l'autorité de certification (CA).
Nom d'hôte		Saisissez un nom d'hôte pour l'interface, qui est inscrit auprès du serveur DDNS (par exemple, hôte123.domaine123.com ou hôte123). Le pare-feu ne valide pas le nom d'hôte, sauf pour confirmer que la syntaxe utilise les caractères valides autorisés par DNS pour un nom de domaine.
Constructeur		Sélectionnez le fournisseur DDNS (et le numéro de version) qui fournit un service DDNS à cette interface : • **DuckDNS v1** • **DynDNS v1** • **FreeDNS Afraid.org Dynamic API v1** • **FreeDNS Afraid.org v1** • **No-IP v1** *Si vous sélectionnez une version antérieure d'un service DDNS qui, selon le pare-feu, sera supprimée avant une date donnée, passez à la nouvelle version.* Les champs **Name (Nom)** et **Value (Valeur)** qui suivant le nom du fournisseur sont propres au fournisseur. Certains champs sont en lecture seule pour vous aviser des paramètres que le pare-feu utiliser pour se connecter au service DDNS. Configurez les autres champs, comme un mot de passe que le service DDNS vous fournit

Paramètres d’une interface VLAN	Configuré dans	Description
		et le délai que le pare-feu utilise s’il ne reçoit pas de réponse du service DDNS.
Onglet IPv4 - IP		Ajoutez les adresses IPv4 configurées sur l’interface et sélectionnez-les. Toutes les adresses IP sélectionnées sont inscrites auprès du fournisseur DDNS.
Onglet IPv6 - IPv6	**VLAN Interface (Interface VLAN)** > **Advanced (Avancé)** > **DDNS**	Ajoutez les adresses IPv6 configurées sur l’interface et sélectionnez-les. Toutes les adresses IP sélectionnées sont inscrites auprès du fournisseur DDNS.
Show Runtime Info		Affiche l’inscription DDNS : fournisseur DDNS, FQDN résolu et les adresses IP mappées avec un astérisque (*) indiquant l'adresse IP principale. Chaque fournisseur DDNS possède ses propres codes de retour pour indiquer l’état de la mise à jour du nom d’hôte et une date de retour à des fins de résolution de problèmes.

Réseau > Interfaces > En boucle

Utilisez les champs suivants pour configurer une interface en boucle :

Paramètres d'une interface en boucle	Configuré dans	Description
Nom de l'interface	**Interface en boucle**	**Interface Name (Nom de l'interface)** en lecture seule est défini sur **en boucle**. Dans le champ adjacent, saisissez un suffixe numérique (1-9999) pour identifier l'interface.
Commentaire		Saisissez une description de l'interface (facultatif).
profil NetFlow ;		Si vous voulez exporter le trafic IP unidirectionnel traversant une interface d'entrée vers un serveur NetFlow, sélectionnez le profil de serveur ou cliquez sur **Netflow Profile (Profil Netflow)** pour définir un nouveau profil (Voir Périphérique > Profils de serveur > NetFlow). Sélectionnez **None (Aucun)** pour supprimer l'affectation de serveur NetFlow de l'interface.
routeur virtuel - VR	**Interface en boucle** > **Configuration**	Affectez un routeur virtuel à l'interface ou cliquez sur **Virtual Router (Routeur virtuel)** pour en définir un nouveau (voir Réseau > Routeurs virtuels). Sélectionnez **None (Aucun)** pour supprimer l'affectation de routeur virtuel de l'interface.
Virtual System (système virtuel - vsys)		Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système virtuel (vsys) pour l'interface ou cliquez sur le lien **Virtual System (Système virtuel)** pour en définir un nouveau.
Zone de sécurité		Sélectionnez une zone de sécurité pour l'interface ou cliquez sur **Zone** pour en définir une nouvelle. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de l'interface.
Profil de gestion	**en texte clair** > **Avancé** > **Autre info**	**Management Profile (Profil de gestion)** - Sélectionnez un profil qui définit les protocoles (par exemple, SSH, Telnet et HTTP) à utiliser pour gérer le pare-feu dans cette interface. Sélectionnez **None (Aucune)** pour supprimer l'affectation de profil de l'interface.
MTU		Saisissez l'unité de transmission maximale (MTU) en octets par paquet envoyé sur cette interface (intervalle compris entre 576 et 9 192, valeur par défaut : 1 500). Si les machines situées de chaque côté du pare-feu effectuent une détection du chemin MTU (PMTUD) et que l'interface reçoit un paquet dépassant la valeur MTU, le pare-feu renvoie à la source un message de *fragmentation ICMP obligatoire* indiquant que le paquet est trop volumineux.

Paramètres d’une interface en boucle	Configuré dans	Description
Ajuster TCP MSS		Sélectionnez pour ajuster la taille de segment maximale (MSS) afin de tolérer les octets de tous les en-têtes qui respectent la taille en octets de la MTU de l’interface. La taille en octets de la MTU moins la taille d'ajustement de la MSS équivaut à la taille en octets de la MSS, laquelle varie selon le protocole IP : • **IPv4 MSS Adjustment Size (Taille d'ajustement MSS IPv6)** - Intervalle compris entre 40 et 300 ; valeur par défaut : 40. • **IPv6 MSS Adjustment Size (Taille d'ajustement MSS IPv6)** - Intervalle compris entre 60 et 300 ; valeur par défaut : 60. Servez-vous de ces paramètres pour faire face aux situations où un **tunnel** réseau nécessite une plus petite MSS. Si un paquet a plus d'octets que la MSS sans faire l'objet d'une fragmentation, ce paramètre permet son ajustement. L'encapsulation rallonge les en-têtes. Il peut donc s'avérer utile de configurer la taille d'ajustement MSS de façon à autoriser les octets d'éléments tels que des en-têtes MPLS ou le trafic par tunnel ayant une étiquette VLAN.
Pour une adresse IPv4		
Adresse IP	**Interface en boucle** > **IPv4**	Cliquez sur **Add (Ajouter)**, puis suivez l'une des étapes ci-dessous pour indiquer l'adresse IP statique et le masque réseau de l'interface. • Saisissez une adresse IPv4 avec un masque de sous-réseau de /32, par exemple, 192.168.2.1/32. Seul le masque de sous-réseau /32 est pris en charge. • Sélectionnez un objet d'adresse existant de type **IP netmask (Masque réseau IP)**. • Cliquez sur **Address (Adresse)** pour créer un objet d'adresse de type **netmask (Masque réseau IP)**. Vous pouvez saisir plusieurs adresses IP pour l'interface. La base d'informations de transfert (FIB) utilisée par votre système détermine le nombre maximum d'adresses IP. Pour supprimer une adresse IP, sélectionnez-la et cliquez sur **Delete (Supprimer)**.
Pour une adresse IPv6		
Activer IPv6 sur l'interface	**Interface en boucle** > **IPv6**	Sélectionnez pour activer l’adressage IPv6 sur cette interface.

Paramètres d’une interface en boucle	Configuré dans	Description
ID de l'interface		Saisissez l'identifiant unique étendu sur 64'A0;bits (EUI-64) au format hexadécimal (par exemple, 00:26:08:FF:FE:DE:4E:29). Si ce champ n'est pas renseigné, le pare-feu utilise l'identifiant unique étendu sur 64'A0;bits (EUI-64) généré à partir de l'adresse MAC de l'interface physique. Si vous activez l'option **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** lors de l'ajout d'une adresse, le pare-feu utilise l'ID de l'interface comme partie hôte de l'adresse.
Adresse		Cliquez sur **Add (Ajouter)** et configurez les paramètres suivants pour chaque adresse IPv6 : • **Address (Adresse)** - Saisissez une adresse IPv6 et une longueur de préfixe (par exemple, 2001:400:f00::1/64). Vous pouvez également sélectionner un objet d'adresse IPv6 existant ou cliquer sur **Address (Adresse)** pour en créer un nouveau. • **Enable address on interface (Activer l’adresse sur l’interface)** - Sélectionnez cette option pour activer l’adresse IPv6 sur l’interface. • **Use interface ID as host portion (Utiliser l’ID de l’interface comme partie hôte)** - Sélectionnez cette option pour utiliser l’**ID de l’interface** comme partie hôte de l’adresse IPv6. • **Anycast** - Sélectionnez cette option pour inclure le routage via le nœud le plus proche.

Réseau > Interfaces > De tunnel

Utilisez les champs suivants pour configurer une interface de tunnel :

Paramètres d'une interface de tunnel	Configuré dans	Description
Nom de l'interface	**en texte clair**	**Interface Name (Nom de l'interface)** en lecture seule est défini sur **tunnel**. Dans le champ adjacent, saisissez un suffixe numérique (1 à 9 999) pour identifier l'interface.
Commentaire		Saisissez une description de l'interface (facultatif).
profil NetFlow ;		Si vous voulez exporter le trafic IP unidirectionnel traversant une interface d'entrée vers un serveur NetFlow, sélectionnez le profil de serveur ou cliquez sur **Netflow Profile (Profil Netflow)** pour définir un nouveau profil (Voir Périphérique > Profils de serveur > NetFlow). Sélectionnez **None (Aucun)** pour supprimer l'affectation de serveur NetFlow de l'interface.
routeur virtuel - VR	**en texte clair** > **Configuration**	Affectez un routeur virtuel à l'interface ou cliquez sur **Virtual Router (Routeur virtuel)** pour en définir un nouveau (voir Réseau > Routeurs virtuels). Sélectionnez **None (Aucun)** pour supprimer l'affectation de routeur virtuel de l'interface.
Virtual System (système virtuel - vsys)		Si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée, sélectionnez un système virtuel (vsys) pour l'interface ou cliquez sur le lien **Virtual System (Système virtuel)** pour en définir un nouveau.
Zone de sécurité		Sélectionnez une zone de sécurité pour l'interface ou cliquez sur **Zone** pour en définir une nouvelle. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de l'interface.
Profil de gestion	**en texte clair** > **Avancé** > **Autre info**	**Management Profile (Profil de gestion)** - Sélectionnez un profil qui définit les protocoles (par exemple, SSH, Telnet et HTTP) à utiliser pour gérer le pare-feu dans cette interface. Sélectionnez **None (Aucune)** pour supprimer l'affectation de profil de l'interface.
MTU		Saisissez l'unité de transmission maximale (MTU) en octets par paquet envoyé sur cette interface (plage de 576 à 9 192 ; valeur par défaut de 1 500). Si les machines situées de chaque côté du pare-feu effectuent une détection du chemin MTU (PMTUD) et que l'interface reçoit un paquet dépassant la valeur MTU, le pare-feu renvoie à la source un message de *fragmentation ICMP obligatoire* indiquant que le paquet est trop volumineux.

Paramètres d’une interface de tunnel	Configuré dans	Description
Pour une adresse IPv4		
Adresse IP	**en texte clair** > **IPv4**	Cliquez sur **Add (Ajouter)**, puis suivez l'une des étapes ci-dessous pour indiquer l'adresse IP statique et le masque réseau de l'interface. • Saisissez l’entrée en notation CIDR (Classing Inter-Domain Routing, routage inter domaine sans classes) : adresse_ip/masque (par exemple, 192.168.2.0/24). • Sélectionnez un objet d'adresse existant de type **IP netmask (Masque réseau IP)**. • Cliquez sur **Address (Adresse)** pour créer un objet d'adresse de type **netmask (Masque réseau IP)**. Vous pouvez saisir plusieurs adresses IP pour l'interface. La base d'informations de transfert (FIB) utilisée par votre système détermine le nombre maximum d'adresses IP. Pour supprimer une adresse IP, sélectionnez-la et cliquez sur **Delete (Supprimer)**.
Pour une adresse IPv6		
Activer IPv6 sur l'interface	**en texte clair** > **IPv6**	Sélectionnez pour activer l’adressage IPv6 sur cette interface.
ID de l'interface	**en texte clair** > **IPv6**	Saisissez l'identifiant unique étendu sur 64'A0;bits (EUI-64) au format hexadécimal (par exemple, 00:26:08:FF:FE:DE:4E:29). Si ce champ n'est pas renseigné, le pare-feu utilise l'identifiant unique étendu sur 64'A0;bits (EUI-64) généré à partir de l'adresse MAC de l'interface physique. Si vous activez l'option **Use interface ID as host portion (Utiliser l'ID de l'interface comme partie hôte)** lors de l'ajout d'une adresse, le pare-feu utilise l'ID de l'interface comme partie hôte de l'adresse.
Adresse		Cliquez sur **Add (Ajouter)** et configurez les paramètres suivants pour chaque adresse IPv6 : • **Address (Adresse)** - Saisissez une adresse IPv6 et une longueur de préfixe (par exemple, 2001:400:f00::1/64). Vous pouvez également sélectionner un objet d'adresse IPv6 existant ou cliquer sur **Address (Adresse)** pour en créer un nouveau. • **Enable address on interface (Activer l’adresse sur l’interface)** - Sélectionnez cette option pour activer l’adresse IPv6 sur l’interface.

Paramètres d’une interface de tunnel	Configuré dans	Description
		• **Use interface ID as host portion (Utiliser l’ID de l’interface comme partie hôte)** - Sélectionnez cette option pour utiliser l’**ID de l’interface** comme partie hôte de l’adresse IPv6. • **Anycast** - Sélectionnez cette option pour inclure le routage via le nœud le plus proche.

Réseau > Interfaces > SD-WAN

Créez une interface virtuelle SD-WAN et ajoutez des membres d’une ou plusieurs interfaces Ethernet physiques qui vont vers la même destination.

Si Panorama gère un pare-feu multi-vsys, toutes les interfaces et configurations compatibles SD-WAN doivent être configurées sur vsys1.

SD-WAN ne prend pas en charge une configuration SD-WAN sur plusieurs systèmes virtuels d'un pare-feu multi-VSYS.

Paramètres d’une interface SD-WAN	
Nom de l'interface	**Interface Name (Nom de l'interface)** en lecture seule est défini sur **sdwan**. Dans le champ adjacent, saisissez un suffixe numérique (1 à 9 999) pour identifier l'interface virtuelle SD-WAN.
Commentaire	Il est conseillé de saisir une description conviviale pour l’interface, telle que **`to internet (vers internet)`** ou **`to Western USA hub (vers un hub de l’ouest des USA)`**. Vos commentaires faciliteront l’identification des interfaces plutôt que d’essayer de décrypter des noms générés automatiquement dans les journaux et les rapports.
Étiquette de liens	Balise sur une liaison SD-WAN ; par exemple, Cheap Broadband ou Backup.
Onglet Configuration	
routeur virtuel - VR	Affectez un routeur virtuel à l’interface ou sélectionnez**Virtual Router (Routeur virtuel)** pour en définir un nouveau (voir Réseau > Routeurs virtuels). Sélectionnez **None (Aucun)** pour supprimer l'affectation de routeur virtuel de l'interface.
Système virtuel	Si le pare-feu prend en charge plusieurs systèmes virtuels et que cette fonctionnalité est activée, vous devez sélectionner **vsys1** pour l’interface.
Zone de sécurité	Sélectionnez une zone de sécurité pour l'interface ou cliquez sur **Zone** pour en définir une nouvelle. Sélectionnez **None (Aucune)** pour supprimer l'affectation de zone de l'interface. L’interface virtuelle SD-WAN et tout les membres de l’interface doivent être dans la même zone de sécurité, assurant ainsi que les mêmes règles de politique de sécurité s’appliquent à tous les chemins depuis la branche jusqu’à la même destination.
Onglet Avancé	
Interfaces	Sélectionnez les interfaces Ethernet Couche 3 (pour l’accès direct à internet [DIA]) ou les interfaces virtuelles de tunnel VPN (pour le hub) qui constituent cette interface virtuelle SD-WAN. Le routeur virtuel du pare-feu utilise cette interface virtuelle SD-WAN pour acheminer le trafic SD-WAN à un emplacement DIA ou de

Paramètres d’une interface SD-WAN	
	hub. Les interfaces peuvent avoir des étiquettes différentes. Si vous saisissez plus d’une interface, elles doivent toutes être du même type (tunnel VPN ou DIA).

Réseau > Interfaces > PoE

Vous pouvez configurer l'alimentation par Ethernet (PoE) sur les interfaces prises en charge pour transférer l'alimentation électrique du pare-feu vers un périphérique alimenté connecté (PA). Cet écran affiche un résumé de la configuration PoE sur toutes les interfaces, ainsi que le budget énergétique, l'allocation et l'utilisation définis par vos paramètres PoE.

Le tableau suivant présente chaque colonne du tableau **Interfaces PoE Details (Détails PoE des interfaces)**.

Colonne	Description
Interface	Nom de l'interface et port physique correspondant.
PoE activé	Indique **Yes (Oui)** si PoE est activé sur l'interface.
État opérationnel	Affiche l'état actuel du PoE sur l'interface. Consultez le tableau **Legend (Légende)** pour déterminer les valeurs de cette colonne.
Vérification de la connexion	Indique si une connexion est présente entre le pare-feu et un périphérique alimenté.
class	Affiche des informations de classe PoE en fonction de la sortie d'alimentation, du type d'alimentation et des normes IEEE.
Puissance allouée (W)	Quantité de puissance en watts allouée par l'interface.
Puissance utilisée (W)	Quantité de puissance en watts actuellement utilisée par l'interface.
Puissance consommée (W)	Quantité d'énergie en watts consommée par l'interface.
Rsvd Puissance / Puissance maximale (W)	Quantité de puissance réservée par l'interface sur le potentiel de puissance maximal en watts.
Fautes	Affiche des détails si la connexion PoE a rencontré une erreur sur le port donné.
Raison de la liste noire	Affiche les détails des ports qui ont été mis sur liste noire. **None (Aucun)** indique qu'un port n'est pas sur liste noire.

Certaines colonnes du tableau **Interfaces PoE Details (Détails PoE des interfaces)** ci-dessus utilisent des termes abrégés pour transmettre un état, une erreur ou d'autres circonstances. Le tableau **Legend (Légende)** ci-dessous décrit chaque terme abrégé.

Abréviation	Terme
Alloc	Alloué
Avr.	Approved (Accepté)
Configuration	Configuration
Conn-chk	Vérification de la connexion
Covc	Classe sur l’actuelle
Den	Alimentation refusée
Dis	Désactivation
Disque	Déconnecter
DS	Double signature
Ena	Activé
Flt	Faute
NOFLT	Aucune faute
Opr	Opérationnel
Pcut	Coupure de courant
Prgto	Délai d’expiration du circuit de détection de puissance suffisante
Pwr	Pouvoir
Rsvd	Réservé
Court	Court-circuit
Arrêt	Arrêter
Sig	Paire de signaux
Logiciel	Logiciels
Sp	Paire de rechange
SS	Signature unique

Abréviation	Terme
TooHigh	Capacité supérieure aux prévisions
TooLow	Résistance PD trop faible
Tstart	Courant d’afflux supérieur à max autorisé
ONU	inconnue
W	Watts

Réseau > Zones

Les rubriques suivantes décrivent les zones de sécurité réseau.

Que voulez-vous faire ?	Reportez-vous à la section :
Quel est le but d'une zone de sécurité ?	Présentation des zones de sécurité
Quels sont les champs disponibles pour configurer des zones de sécurité ?	Étapes de configuration des zones de sécurité
Vous souhaitez en savoir plus ?	Segmentation de votre réseau via les interfaces et les zones

Présentation des zones de sécurité

Les zones de Sécurité sont une façon logique de regrouper des interfaces physiques et virtuelles sur le pare-feu afin de contrôler et de journaliser le trafic qui passe par toutes des interfaces spécifiques sur votre réseau. Une interface sur le pare-feu doit être affectée à une zone de sécurité avant que l'interface puisse traiter le trafic. De multiples interfaces de même type (par exemple, tap, niveau 2, niveau 3) peuvent être affectées à une zone, mais une interface ne peut appartenir qu'à une seule zone.

Les règles des politique sur le pare-feu font appel aux zones de sécurité pour identifier l'origine du trafic et sa destination. Le trafic peut circuler librement dans une zone, mais il ne peut pas circuler entre des zones différentes jusqu'à ce que vous définissiez une règle de politique de Sécurité qui l'autorise. Pour autoriser ou refuser le trafic intrazone, les règles de politique de Sécurité doivent faire référence à une zone source et à une zone de destination (pas des interfaces) et les zones doivent être du même type ; c'est-à-dire qu'une règle de politique de Sécurité peut autoriser ou refuser le trafic d'une zone de niveau 2 uniquement vers une autre zone de niveau 2.

Étapes de configuration des zones de sécurité

Pour définir une zone de sécurité, cliquez sur **Ajouter** et renseignez les informations suivantes.

Paramètres d'une zone de sécurité	Description
Nom	Saisissez un nom pour la zone (31 caractères maximum). Ce nom apparaît dans la liste des zones lors de la définition des politiques de sécurité et de la configuration des interfaces. Celui-ci est sensible à la casse et doit être unique au sein du routeur virtuel. N'utilisez que des lettres, des chiffres, des espaces, des tirets, des points et des caractères de soulignement.

Paramètres d’une zone de sécurité	Description
Emplacement	Ce champ n'est présent que si le pare-feu prend en charge les systèmes virtuels multiples et que cette fonctionnalité est activée. Sélectionnez le système virtuel auquel la zone s'applique.
Type	Sélectionnez un type de zone (**Tap**, **Câble virtuel**, **Couche2**, **Couche3**, **Externe** ou **Tunnel**) pour afficher toutes les **Interfaces** de ce type qui n’ont pas été affectées à une zone. Les types de zones de couche 2 et de couche 3 répertorient toutes les interfaces et sous-interfaces Ethernet de ce type. **Ajoutez** les interfaces que vous souhaitez assigner à la zone. La zone externe est utilisée pour contrôler le trafic entre les systèmes virtuels multiples d'un seul pare-feu. Elle s'affiche uniquement si les pare-feu prennent en charge les systèmes virtuels multiples et uniquement si **Fonctionnalité de systèmes virtuels multiples** est activé. Pour obtenir des informations sur les zones externes, reportez-vous à la section Trafic inter-VSYS restant au sein du pare-feu. Une interface peut appartenir à une seule zone dans un système virtuel.
Interfaces	Ajoutez une ou plusieurs interfaces à cette zone.
Profils de protection de zone	Sélectionnez un profil indiquant la manière dont le pare-feu répond aux attaques provenant de cette zone. Pour créer un nouveau profil, voir Réseau > Profils réseau > Protection de zone. Il est recommandé de défendre chaque zone avec un profil de protection de zone.
Activer la protection de la mémoire tampon des paquets	Configurez la protection de la mémoire tampon des paquets (Périphérique > Configuration > Session) de manière globale et appliquez-la à chaque zone. Le pare-feu applique la protection de la mémoire tampon des paquets à la zone d'entrée uniquement. la protection de la mémoire tampon des paquets sur la base du pourcentage d’utilisation du tampon est activée par défaut. Une alternative consiste à configurer la Protection de la mémoire tampon des paquets sur la base de la latence. Il est recommandé d’activer la protection de la mémoire tampon des paquets sur chaque zone pour protéger les mémoires tampons des pare-feu.
Activer l’inspection du réseau	Facilite l’activation de L3 & L4 Header Inspection (inspection des en-têtes L3 et L4) à l’aide de règles personnalisées pour les zones de sécurité associées au profil de protection de zone. Le paramètre global pour l’inspection des en-têtes L3 et L4 doit également être activé sur le pare-feu (Device > Setup > Session (Appareil > Configuration > Session)).
Paramètre des journaux	Sélectionnez un Profil de Transfert de journal pour transférer les journaux de protection de zone vers un système externe. Si vous disposez d’un profil de Transfert des journaux nommé par défaut, ce profil est automatiquement sélectionné pour ce menu déroulant lors de la définition d’une nouvelle zone de sécurité. Vous pouvez appliquer

Paramètres d'une zone de sécurité	Description
	un contrôle prioritaire pour ce paramètre par défaut à tout moment en poursuivant la sélection d'un autre Profil de Transfert des journaux lors de la configuration d'une nouvelle zone de sécurité. Pour définir ou ajouter un nouveau profil de Transfert des journaux (et pour nommer un profil par défaut pour que ce menu déroulant soit automatiquement renseigné), cliquez sur **Nouveau** (voir Objets > Transfert des journaux). *Si vous configurez la zone dans un modèle Panorama, le menu déroulant **Paramètres des journaux** répertorie uniquement les profils de transfert des journaux partagés ; pour indiquer un profil non partagé, vous devez saisir son nom.*
Activer l'identification des utilisateurs	Si vous avez configuré User-ID™ pour effectuer un mappage nom d'utilisateur / adresse IP (détection), il est recommandé d' **activer l'identification des utilisateurs)** pour appliquer les informations de mappage au trafic de cette zone. Si vous désactivez cette option, les rapports, les politiques et les journaux du pare-feu excluront les informations de mappage utilisateur du trafic de cette zone. Par défaut, si vous sélectionnez cette option, le pare-feu applique les informations de mappage utilisateur au trafic de tous les sous-réseaux de la zone. Pour limiter les informations à des sous-réseaux spécifiques de la zone, utilisez la **Liste d'inclusion** et la **Liste d'exclusion**. *Activez User-ID uniquement sur les zones approuvées. Si vous activez User-ID et le sondage du client sur une zone externe non approuvée (comme Internet), des sondages pourraient être envoyés en dehors de votre réseau protégé, ce qui entraînerait une divulgation des informations du nom de compte du service de l'agent User-ID, du nom de domaine et du hachage du mot de passe crypté, ce qui pourrait permettre à un pirate d'obtenir un accès non autorisé aux ressources protégées.* *User-ID effectue la détection dans la zone uniquement si elle se trouve dans la plage réseau surveillée. Si la zone est à l'extérieur de la plage, le pare-feu n'applique pas les informations de mappage utilisateur au trafic de la zone, même si vous sélectionnez **Activer l'identification des utilisateurs**. Pour plus d'informations, reportez-vous à la section* Inclure ou exclure des sous-réseaux pour le mappage d'utilisateur.

Paramètres d’une zone de sécurité	Description
Liste d’inclusion de contrôle d’accès d’identification utilisateur	Par défaut, si vous ne spécifiez pas de sous-réseau dans cette liste, le pare-feu applique les informations de mappage utilisateur détectées à l'ensemble du trafic de cette zone de manière à ce qu'elles soient utilisées dans les journaux, les rapports et les politiques. Pour limiter les informations de mappage utilisateur à des sous-réseaux spécifiques de la zone, cliquez sur **Ajouter** et sélectionnez un objet d'adresse (ou de groupe d'adresses) ou saisissez la plage d'adresses IP (par exemple, 10.1.1.1/24) pour chaque sous-réseau. L'exclusion de tous les autres sous-réseaux est implicite, car la **Liste d’inclusion** est une liste d’autorisation. Vous n'avez donc pas besoin de les ajouter à la **liste d'exclusion**. Ajoutez des entrées à **liste d'exclusion** uniquement pour exclure les informations de mappage utilisateur d'un sous-ensemble des sous-réseaux de **liste d'inclusion**. Par exemple, si vous ajoutez 10.0.0.0/8 à **liste d'inclusion** et 10.2.50.0/22 à **liste d'exclusion**, le pare-feu inclut les informations de mappage utilisateur de tous les sous-réseaux de 10.0.0.0/8 de la zone, excepté 10.2.50.0/22, et exclut les informations de tous les sous-réseaux de la zone se trouvant à l'extérieur de 10.0.0.0/8. *Vous pouvez inclure uniquement des sous-réseaux qui se trouvent dans la plage réseau surveillée par User-ID. Pour plus d’informations, reportez-vous à la section* Inclure ou exclure des sous-réseaux pour le mappage d’utilisateur.
Liste d’exclusion de contrôle d’accès d’identification utilisateur	Pour exclure les informations de mappage utilisateur d’un sous-ensemble de sous-réseaux de la **Liste d’inclusion**, cliquez sur **Ajouter** un objet d’adresse (ou de groupe d’adresses) ou saisissez la plage d’adresses IP pour chaque sous-réseau à exclure. *Si vous ajoutez des entrées à **liste d'exclusion** mais pas à **liste d'inclusion**, le pare-feu exclut les informations de mappage utilisateur de tous les sous-réseaux de la zone, pas uniquement de ceux ajoutés.*

Réseau > VLAN

Le pare-feu prend en charge les VLAN qui respectent la norme IEEE 802.1Q. Chaque interface de couche 2 définie sur le pare-feu peut être associée à un VLAN. Ce même VLAN peut être assigné à plusieurs interfaces de couche 2, mais chaque interface peut appartenir à un seul VLAN.

Paramètres VLAN	Description
Name (Nom)	Saisissez un nom VLAN (31 caractères maximum). Ce nom apparaît dans la liste des VLAN lors de la configuration des interfaces. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement.
Interface VLAN	Sélectionnez un Réseau > Interfaces > VLAN pour autoriser le routage du trafic hors du VLAN.
Interfaces	Indiquez les interfaces de pare-feu du VLAN.
Configuration MAC statique	Indiquez l'interface via laquelle une adresse MAC est accessible. Un contrôle prioritaire sera appliqué sur tout mappage de l'interface vers MAC appris.

Réseau > Câbles virtuels

Sélectionnez **Network (Réseau)** > **Virtual Wires (Câbles virtuels)** pour définir des câbles virtuels après avoir défini deux interfaces de câbles virtuels sur le réseau (Réseau > Interfaces).

Paramètres d’un câble virtuel	Description
Nom du câble virtuel	Saisissez un nom pour le câble virtuel (**31** caractères maximum). Il apparaît dans la liste des câbles virtuels lors de la configuration des interfaces. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement.
Interfaces	Pour configurer un câble virtuel, sélectionnez deux interfaces Ethernet dans la liste affichée. Les interfaces sont répertoriées ici uniquement si elles disposent du type d'interface de câble virtuel et qu'elles n'ont pas été assignées à un autre câble virtuel. Pour plus d’informations sur les interfaces de câbles virtuels, consultez la section Interface du câble virtuel.
Etiquette autorisée	Saisissez un numéro d'étiquette (compris entre 0 et 4094) ou une plage de numéros d'étiquettes (étiquette1 - étiquette2) pour le trafic autorisé sur le câble virtuel. Une valeur d’étiquette de 0 indique un trafic non étiqueté (valeur par défaut). Plusieurs étiquettes ou plages doivent être séparées par des virgules. Tout trafic affichant une valeur d'étiquette exclue est supprimé. *Les valeurs d’étiquettes ne sont pas modifiées sur des paquets entrants ou sortants.* Lorsque vous utilisez des sous-interfaces de câble virtuel, la liste **Tag Allowed (Étiquettes autorisées)** va classer le trafic contenant les étiquettes répertoriées dans le câble virtuel parent. Les sous-interfaces de câble virtuel doivent utiliser des étiquettes qui n'existent pas dans la liste **Tag Allowed (Étiquettes autorisées)** du parent.
Pare-feu multicast	Sélectionnez cette option si vous voulez appliquer des règles de sécurité au trafic multicast. Si ce paramètre n'est pas appliqué, le trafic multicast est transféré dans le câble virtuel.
Transmission de l'état des liaisons	Sélectionnez cette option pour supprimer l’autre interface d’un câble virtuel en cas de détection d’un état de liaison inactif. Si vous ne sélectionnez pas cette option ou si vous la désactivez, l'état des liaisons n'est pas propagé dans le câble virtuel.

Réseau > Routeurs virtuels

Le pare-feu a besoin d'un routeur virtuel pour disposer d'itinéraires vers d'autres sous-réseaux, soit via des itinéraires statiques définis manuellement, soit via l'application de protocoles de routage de couche 3 (itinéraires dynamiques). Chaque interface de Couche 3, interface en boucle et interface VLAN définie sur le pare-feu doit être associée à un routeur virtuel. Chacune d'entre elles ne peut appartenir qu'à un seul routeur virtuel.

Pour définir un routeur virtuel, il faut des paramètres généraux et une combinaison d’itinéraires statiques ou de protocoles de routage dynamiques, selon les exigences de votre réseau. Vous pouvez également configurer d'autres fonctionnalités, comme la redistribution des itinéraires et les itinéraires ECMP.

Que voulez-vous faire ?	Reportez-vous à la section
Quels sont les éléments nécessaires d'un routeur virtuel ?	Paramètres généraux d’un routeur virtuel
Configurer :	Itinéraires statiques Redistribution de route RIP OSPF OSPFv3 BGP IP Mulitcast ECMP
Consulter les informations d’un routeur virtuel.	Statistiques d’exécution supplémentaires d’un routeur virtuel
Vous souhaitez en savoir plus ?	Mise en réseau

Paramètres généraux d’un routeur virtuel

- Réseau > Routeurs virtuels > Paramètres de routeur > Général

Tous les routeurs virtuels nécessitent l’assignation d’interfaces de couche 3 et de mesures de distance administrative, comme décrit dans le tableau suivant.

Paramètres généraux du routeur virtuel	Description
Name (Nom)	Saisissez un nom pour décrire le routeur virtuel (**31** caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Interfaces	Sélectionnez les interfaces à inclure dans le routeur virtuel. Ainsi, ils peuvent être utilisés comme interfaces sortantes dans la table de routage du routeur virtuel. Pour spécifier le type d'interface, reportez-vous à Réseau > Interfaces. lors de l'ajout d'une interface, ses itinéraires connectés sont automatiquement ajoutés.
Distances administratives	Indiquez les distances administratives suivantes'A0;: • **Static routes (Itinéraires statiques)** - Intervalle compris entre 10 et 240 ; valeur par défaut : 10). • **OSPF Int** - Intervalle compris entre 10 et 240 ; valeur par défaut : 30). • **OSPF Ext** - Intervalle compris entre 10 et 240 ; valeur par défaut : 110). • **IBGP** - Intervalle compris entre 10 et 240 ; valeur par défaut : 200). • **EBGP** - Intervalle compris entre 10 et 240 ; valeur par défaut : 20). • **RIP** - Intervalle compris entre 10 et 240 ; valeur par défaut : 120).

Itinéraires statiques

- Réseau > Routeurs virtuels > Itinéraires statiques

Vous pouvez ajouter un ou plusieurs itinéraires statiques. Cliquez sur l'onglet **IP** ou **IPv6** pour spécifier l'itinéraire utilisant une adresse IPv4 ou IPv6. Dans ce cas, vous devez généralement configure default routes (configurer des itinéraires par défaut) (0.0.0.0/0) ici. Ces derniers sont appliqués pour les destinations qui seraient alors introuvables dans la table de routage du routeur virtuel.

Paramètres d'Itinéraire statique	Description
Nom	Saisissez un nom pour identifier l'itinéraire statique (63 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Destination	Saisissez une adresse IP et un masque réseau en notation CIDR (Classless Inter-domaine Routing/routage inter-domaine sans classes) : *ip_address/masque* (par exemple, 192.168.2.0/24 pour IPv4 ou

Paramètres d’Itinéraire statique	Description
	2001:db8::/32 pour IPv6). Vous pouvez également créer un objet d'adresse de type Masque réseau IP.
Interface	Sélectionnez l'interface pour transférer des paquets vers leur destination et/ou configurer les paramètres du saut suivant.
Saut suivant	Sélectionnez l’une des options suivantes : • **IP Address** (Adresse IP) : sélectionnez pour saisir l’adresse IP du routeur du saut suivant, ou sélectionnez ou créez un objet d’adresse de type Masque réseau IP. L’objet d’adresse doit avoir un masque réseau de /32 pour IPv4 ou de /128 pour IPv6. • **Next VR (Routeur virtuel suivant)** - Sélectionnez cette option pour sélectionner un routeur virtuel dans le pare-feu en tant que saut suivant. Cela vous permet d’effectuer un routage en interne entre des routeurs virtuels dans un pare-feu unique. • **FQDN** : sélectionnez cette option pour identifier le saut suivant par FQDN. Sélectionnez ensuite un objet d’adresse de type FQDN ou créez un nouvel objet d’adresse de type FQDN. • **Discard (Supprimer)** - Indiquez si vous voulez arrêter le trafic vers cette destination. • **None (Aucun)** : sélectionnez cette option s'il n'existe aucun saut suivant pour l'itinéraire.
Distance admin	Indiquez la distance administrative de l'itinéraire statique (de 240 à 10, valeur par défaut : 10).
Mesure	Indiquez une mesure valide pour l'itinéraire statique (1 à 65535).
Table d'itinéraires	Sélectionnez la table de routage dans laquelle le pare-feu installe l’itinéraire statique : • **Unicast** – Installe l’itinéraire dans la table de routage unicast. • **Multicast** – Installe l’itinéraire dans la table de routage multicast. • **Both (Les deux)** – Installe l’itinéraire dans la table de routage unicast et multicast. • **No Install (Aucune installation)** – N’installe pas l’itinéraire dans la table de routage (RIB) ; le pare-feu conserve l’itinéraire statique pour référence ultérieure jusqu’à ce que vous supprimiez cet itinéraire.
Profil BFD	Pour activer la BFD (Bidirectional Forwarding Detection/détection de transmission bidirectionnelle) pour un itinéraire statique sur un pare-feu série PA-400, série PA-3200, série PA-3400, série PA-5200, série PA-5400, série PA-7000 ou série VM, sélectionnez l’une des options suivantes :

Paramètres d’Itinéraire statique	Description
	• **default (défaut)** (paramètres BFD par défaut) • un profil BFD que vous avez créé sur le pare-feu • **New BFD Profile (Nouveau profil BFD)** pour créer un nouveau profil BFD Sélectionnez **None (Disable BFD) (Aucun (Désactiver la BFD))** pour désactiver la BFD pour cet itinéraire statique. Pour utiliser la BFD sur un itinéraire statique : • Le pare-feu et l'homologue qui se trouvent aux extrémités de l'itinéraire statique doivent prendre en charge les sessions BFD. • Le type de **Next Hop (Saut suivant)** de l'itinéraire statique doit correspondre à l'**IP Address (Adresse IP)**, et vous devez saisir une adresse IP valide. • Le paramètre de l'**Interface** ne peut correspondre à **None (Aucun)** ; vous devez sélectionner une interface (même si vous utilisez une adresse DHCP).
Surveillance des chemins	Sélectionnez cette option pour activer la surveillance des chemins pour l’itinéraire statique.
Condition d'échec	Sélectionnez la condition selon laquelle le pare-feu considère le chemin surveillé comme inactif et considère donc l’itinéraire statique comme inactif : • **Any (N’importe laquelle)** – Si n’importe laquelle des destinations surveillées pour l’itinéraire statique n’est pas accessible par ICMP, le pare-feu supprime l’itinéraire statique de la RIB et de la FIB et ajoute l’itinéraire dynamique ou statique dont la métrique la plus faible suivante se dirige vers la même destination que la FIB. • **Tout —**Si toutes les destinations surveillées pour la route statique sont inaccessibles par ICMP, le pare-feu supprime la route statique du RIB et du FIB et ajoute la route dynamique ou statique qui a la métrique la plus basse suivante allant à la même destination au FIB. Sélectionnez **Tout** pour éviter la possibilité qu'une seule destination surveillée signale une défaillance de route statique lorsque cette destination surveillée est simplement hors ligne pour maintenance, par exemple.
Délai de maintien préemptif	Saisissez le nombre de minutes pendant lesquelles une surveillance des chemins inactifs doit conserver l’état Active (la surveillance des chemins évalue toutes les destinations surveillées de ses membres et doit rester Active avant que le pare-feu ne réinstalle l’itinéraire statique dans la RIB). Si le minuteur expire sans que la liaison devienne inactive ou instable, la liaison est jugée stable, la surveillance des chemins peut rester Active et le pare-feu peut ajouter l’itinéraire statique à la RIB.

Paramètres d’Itinéraire statique	Description
	Si la liaison devient inactive ou instable pendant le délai de maintien, la surveillance des chemins échoue et le minuteur redémarre lorsque la surveillance désactivée reprend l’état Actif. Un **Preemptive Hold Time (Délai de maintien de préemption)** de zéro permet au pare-feu de réinstaller l’itinéraire statique dans la RIB immédiatement après l’activation de la surveillance des chemins. La plage est comprise entre 0 et 1 440 ; la valeur par défaut est 2.
Name (Nom)	Saisissez un nom pour la destination surveillée (31 caractères maximum).
Activer	Sélectionnez cette option pour activer la surveillance des chemins de cette destination spécifique pour l’itinéraire statique ; le pare-feu envoie des requêtes ping ICMP à cette destination.
IP source	Sélectionnez l’adresse IP que le pare-feu utilisera en tant que source dans la requête ping ICMP vers la destination surveillée : • Si l’interface possède plusieurs adresses IP, sélectionnez-en une. • Si vous sélectionnez une interface, le pare-feu utilise la première adresse IP affectée à l’interface par défaut. • Si vous sélectionnez **DHCP (Use DHCP Client address) (DHCP (Utiliser l’adresse du client DHCP))**, le pare-feu utilise l’adresse que DHCP a affectée à l’interface. Pour consulter l’adresse DHCP, sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet** et dans la ligne de l’interface Ethernet, cliquez sur **Dynamic DHCP Client (Client DHCP dynamique)**. L’adresse IP s’affiche dans la fenêtre Statut de l’interface IP dynamique.
IP de destination	Saisissez une adresse IP fiable et stable ou un objet d’adresse pour lequel le pare-feu surveillera les chemins. La destination surveillée et la destination de l’itinéraire statique doivent utiliser la même famille d’adresses (IPv4 ou IPv6)
Intervalle des requêtes ping (sec)	Indiquez l’intervalle de la requête ping ICMP en secondes pour déterminer la fréquence à laquelle le pare-feu surveille les chemins (effectue un test ping sur la destination surveillée ; la plage est comprise entre 1 et 60 ; la valeur par défaut est 3).
Nombre de requêtes ping	Indiquez le nombre de paquets de requêtes ping ICMP consécutifs qui ne sont pas renvoyés par la destination surveillée avant que le pare-feu ne considère la liaison comme inactive. En fonction de la condition d’échec **Any (Indifférente)** ou **All (Toutes)**, si la surveillance des chemins est en état d’échec, le pare-feu supprime l’itinéraire statique de la RIB (la plage est comprise entre 3 et 10 et la valeur par défaut est 5). Par exemple, un Intervalle des requêtes ping de 3 secondes et un Nombre de requêtes ping de 5 requêtes ping manquées (le pare-feu ne reçoit pas

Paramètres d’Itinéraire statique	Description
	de requêtes ping au cours des 15 dernières secondes) signifient que la surveillance des chemins détecte un échec de la liaison. Si la surveillance des chemins est en état d’échec et que le pare-feu reçoit une requête ping après 15 secondes, la liaison est considérée comme active ; en fonction de la condition d’échec **Any (Indifférente)** ou **All (Toutes)**, la surveillance des chemins de **Any (N’importe laquelle)** ou de **All (Toutes)** les destinations surveillées peut être considérée comme activée et le Délai de maintien de préemption commence.

Redistribution d’itinéraire

- Réseau > Routeur virtuel > Profils de redistribution

Les profils de redistribution orientent le pare-feu dans le filtrage, définissent des priorités et réalisent des actions en fonction du comportement souhaité du réseau. Cette redistribution permet à des itinéraires statiques et à des itinéraires acquis par d'autres protocoles d'être publiés via des protocoles de routage définis.

Les profils de redistribution doivent être appliqués aux protocoles de routage afin d'être effectifs. En l'absence de règles de redistribution, chaque protocole s'exécute séparément et ne communique pas au-delà de son domaine. Des profils de redistribution peuvent être ajoutés ou modifiés une fois tous les protocoles de routage configurés et la topologie de réseau résultante établie.

Appliquez des profils de redistribution aux protocoles'A0;RIP et OSPF en définissant des règles d'exportation. Appliquez des profils de redistribution au protocole BGP dans l'onglet **Règles de redistribution (Redistribution Rules)**. Consultez le tableau suivant.

Paramètres de profil de redistribution	Description
Name (Nom)	Vous pouvez **Ajouter** un **Profil de redistribution** et saisir le nom du profil.
Priorité	Saisissez une priorité (comprise entre 1 et 255) pour ce profil. Les profils sont classés dans l'ordre (valeur la plus basse en premier).
Redistribuer	Indiquez si la redistribution des itinéraires doit s'effectuer en fonction des paramètres de cette fenêtre. • **Redist** - Permet de redistribuer les itinéraires candidats correspondants. Si vous sélectionnez cette option, saisissez une nouvelle valeur de mesure. Une valeur de mesure inférieure correspond à un itinéraire préféré. • **No Redist (Ne pas redist)** - Sélectionnez cette option afin de ne pas redistribuer les itinéraires candidats correspondants.

Paramètres de profil de redistribution	Description
Onglet Filtre général	
Type	Sélectionnez les types d'itinéraires de l'itinéraire candidat.
Interface	Sélectionnez des interfaces pour indiquer les interfaces de transfert d'un itinéraire candidat.
Destination	Pour indiquer la destination d'un itinéraire candidat, saisissez l'adresse IP ou le sous-réseau de destination (au format x.x.x.x ou x.x.x.x/n) et cliquez sur **Add (Ajouter)**. Pour supprimer une entrée, cliquez sur Supprimer ( ).
Saut suivant	Pour indiquer la passerelle d'un itinéraire candidat, saisissez l'adresse IP ou le sous-réseau (au format x.x.x.x ou x.x.x.x/n) qui représente le saut suivant et cliquez sur **Add (Ajouter)**. Pour supprimer une entrée, cliquez sur Supprimer ( ).
Onglet Filtre OSPF	
Type de chemin	Sélectionnez les types d'itinéraires de l'itinéraire OSPF candidat.
nominale	Indiquez l'identifiant de zone de l'itinéraire OSPF candidat. Entrez l'**OSPF area ID (ID de zone OSPF)** (au format x.x.x.x) et cliquez sur **Add (Ajouter)**. Pour supprimer une entrée, cliquez sur Supprimer ( ).
Étiquette	Indiquez des valeurs pour les étiquettes OSPF. Saisissez une valeur d'étiquette numérique (1 à 255) et cliquez sur Ajouter. Pour supprimer une entrée, cliquez sur Supprimer ( ).
Onglet Filtre BGP	
Communauté	Indiquez une communauté pour la politique de routage BGP.
Communauté étendue	Indiquez une communauté étendue pour la politique de routage BGP.

RIP

- Réseau > Routeurs virtuels > RIP

La définition d'un protocole RIP (Routing Information Protocol/protocole de routage Internet) comprend la configuration des paramètres généraux suivants :

Paramètres RIP	Description
Activer	Sélectionnez pour activer RIP.
Rejeter les itinéraires par défaut	(Recommandé) Sélectionnez si vous ne voulez pas apprendre d'itinéraires via RIP par défaut.
BFD	Pour activer la BFD (Bidirectional Forwarding Detection/détection de transmission bidirectionnelle) globalement pour RIP du routeur virtuel sur un pare-feu PA-400 Series, PA-3200 Series, PA-3400 Series ou VM-Series, sélectionnez l'une des options suivantes : • **default (défaut)** (profil ayant les paramètres BFD par défaut) • un profil BFD que vous avez créé sur le pare-feu • **New BFD Profile (Nouveau profil BFD)** pour créer un nouveau profil BFD Sélectionnez **Aucun (Désactiver BFD)** pour désactiver BFD pour toutes les interfaces RIP du routeur virtuel ; vous ne pouvez activer BFD pour une seule interface RIP.

Les paramètres RIP des onglets suivants doivent également être configurés :

- **Interfaces** : Voir Onglet Interfaces RIP.
- **Timers (Minuteurs)** : Voir Onglet Minuteurs RIP.
- **Auth Profiles (Profils d'authentification)** : Voir l'Onglet Profils d'authentification RIP.
- **Export Rules (Règles d'exportation)** : Voir l'Onglet Règles d'exportation RIP.

Onglet Interfaces RIP

- Réseau > Routeurs virtuels > RIP > Interfaces

Utilisez les champs suivants pour configurer les interfaces RIP :

RIP – Paramètres de l'interface	Description
Interface	Sélectionnez une interface exécutant le protocole RIP.
Activer	Sélectionnez cette option pour activer ces paramètres.

RIP – Paramètres de l’interface	Description
Publier	Sélectionnez cette option pour activer la publication d'un itinéraire par défaut dans les homologues RIP avec la valeur la mesure spécifiée.
Mesure	Indiquez une valeur de mesure pour la publication d'un routeur. Ce champ n'est visible que si vous activez l'option **Advertise (Publier)**.
Profil d'authentification	Sélectionnez un profil.
Mode	Sélectionnez **normal**, **passive (passif)** ou **send-only (envoyer seulement)**.
BFD	Pour activer BFD pour une interface RIP (et ainsi appliquer un contrôle prioritaire sur le paramètre BFD pour RIP, pourvu que BFD ne soit pas activé pour RIP au niveau du routeur virtuel), sélectionnez l'une des options suivantes : • **default (défaut)** (profil ayant les paramètres BFD par défaut) • un profil BFD que vous avez créé sur le pare-feu • **New BFD Profile (Nouveau profil BFD)** pour créer un nouveau profil BFD Sélectionnez **Aucun (Désactiver la BFD)** pour désactiver la BFD pour l'interface RIP.

Onglet Minuteurs RIP

- Réseau > Routeur virtuel > RIP > Minuteurs

Le tableau suivant décrit les minuteurs qui contrôlent les mises à jour et les périodes d'expiration des itinéraires RIP.

RIP – Paramètres du minuteur	Description
Timing RIP	
Intervalle en secondes (s)	Définissez la longueur de l'intervalle du minuteur en secondes. Ce délai est utilisé pour les champs restants du minuteur RIP (intervalle compris entre 1 et 60).
Intervalles de mise à jour	Saisissez le nombre d'intervalles entre les annonces de mise à jour des itinéraires (intervalle compris entre 1 et 3 600).
Intervalles d'expiration	Saisissez le nombre d'intervalles entre l'heure à laquelle l'itinéraire a été mis à jour pour la dernière fois et son expiration (intervalle compris entre 1 et 3 600).

RIP – Paramètres du minuteur	Description
Intervalles de suppression	Saisissez le nombre d'intervalles entre l'heure d'expiration de l'itinéraire et sa suppression (intervalle compris entre 1 et 3 600).

Onglet Profils d’authentification RIP

- Réseau > Routeur virtuel > RIP > Profils d'authentification

Par défaut, le pare-feu n'authentifie pas les messages RIP entre des voisins. Pour authentifier des messages RIP entre voisins, créez un profil d'authentification et appliquez-le à une interface qui exécute un protocole RIP sur un routeur virtuel. Le tableau suivant décrit les paramètres de l'onglet **Auth Profiles (Profils d'authentification)**.

RIP – Paramètres du profil d’authentification	Description
Nom du profil	Saisissez un nom pour le profil d'authentification afin d'authentifier des messages RIP.
Type de mot de passe	Sélectionnez le type de mot de passe (simple ou MD5). • Si vous sélectionnez **Simple**, saisissez le mot de passe simple et confirmez-le. • Si vous sélectionnez **MD5**, saisissez une ou plusieurs entrées de mot de passe, notamment **Key-ID (ID-Clé)** (0 à 255), **Key (Clé)** et éventuellement le statut **Preferred (Préféré)**. Cliquez sur **Add (Ajouter)** pour chaque entrée, puis cliquez sur **OK**. Pour indiquer la clé à utiliser afin d'authentifier le message sortant, sélectionnez l'option **Preferred (Préféré)**.

Onglet Règles d’exportation RIP

- Réseau > Routeur virtuel > RIP > Règles d'exportation

Les règles d'exportation RIP vous permettent de contrôler quels sont les itinéraires que le routeur virtuel distribue aux homologues.

RIP – Paramètres des règles d’exportation	Description
Autoriser la redistribution des itinéraires par défaut	Sélectionnez pour autoriser le pare-feu à redistribuer son itinéraire par défaut vers des homologues.
Profil de redistribution	Cliquez sur **Add (Ajouter)** et sélectionnez ou créez un profil de redistribution vous permettant de modifier la redistribution, les filtres,

RIP – Paramètres des règles d’exportation	Description
	la priorité et l'action d'un itinéraire en fonction du comportement réseau souhaité. Voir Redistribution de route.

OSPF

- Réseau > Routeur virtuel > OSPF

La définition du protocole OSPF (Open Shortest Path First / premier chemin ouvert le plus court) nécessite la configuration des paramètres généraux suivants (à l’exception de la BFD, qui est facultative) :

Paramètres OSPF	Description
Activer	Sélectionnez cette option pour activer le protocole OSPF.
Rejeter les itinéraires par défaut	(Recommandé) Sélectionnez cette option si vous ne voulez pas apprendre des itinéraires via OSPF par défaut.
ID de routeur	Indiquez l'ID du routeur associé à l'instance OSPF dans ce routeur virtuel. Le protocole OSPF utilise l'ID du routeur pour identifier uniquement l'instance OSPF.
BFD	Pour activer la BFD (Bidirectional Forwarding Detection/détection de transmission bidirectionnelle) globalement pour OSPF du routeur virtuel sur un pare-feu PA-400 Series, PA-3200 Series, PA-3400 Series ou VM-Series, sélectionnez l'une des options suivantes : • **default (défaut)** (paramètres BFD par défaut) • un profil BFD que vous avez créé sur le pare-feu • **New BFD Profile (Nouveau profil BFD)** pour créer un nouveau profil BFD Sélectionnez **None (Disable BFD) (Aucun (Désactiver BFD))** pour désactiver BFD pour toutes les interfaces OSPF du routeur virtuel ; vous pouvez activer BFD pour une seule interface OSPF.

De plus, vous devez configurer les paramètres OSPF dans les onglets suivants :

- **Areas (Zones)** : Voir Onglet des zones OSPF.
- **Auth Profiles (Profils d'authentification)** : Reportez-vous à la section Onglet Profils d’authentification OSPF.
- **Export Rules (Règles d'exportation)** : Reportez-vous à la section Onglet Règles d’exportation OSPF.
- **Advanced (Avancé)** : Voir Onglet avancé OSPF.

Onglet des zones OSPF

- Réseau > Routeur virtuel > OSPF > Zones

Les champs suivants décrivent les paramètres de la zone OSPF :

OSPF – Paramètres des zones	Description
Zones	
ID de zone	Configurez la zone sur laquelle les paramètres OSPF peuvent être appliqués. Saisissez un identifiant pour la zone au format x.x.x.x. Il s'agit de l'identifiant devant faire partie de la même zone et que chaque voisin doit accepter.
Type	Sélectionnez l’une des options suivantes. • **Normal (Normal)** - Aucune restriction n'est appliquée ; la zone peut accepter tout type d'itinéraire. • **Stub (Terminale)** : il n'existe aucune sortie issue de la zone. Pour atteindre une destination extérieure à la zone, vous devez passer par la bordure qui se connecte aux autres zones. Si vous choisissez cette option, sélectionnez **Accept Summary (Accepter un récapitulatif)** pour accepter ce type de publication LSA (Link State Advertisement/ annonce d'état de liaison) de la part des autres zones. Spécifiez également s’il faut inclure un LSA de routage par défaut dans les publicités vers la zone de stub avec la valeur métrique associée (plage comprise entre 1 et 255). Si l’option Accepter le **résumé** sur une interface ABR (Area Border Router) d’une zone de stub est désactivée, la zone OSPF se comportera comme une zone totalement stubby (TSA) et l’ABR ne propagera aucun LSA récapitulatif. • **NSSA** (Not-So-Stubby Area) : il est possible de quitter la zone directement, mais uniquement par des itinéraires autres que les itinéraires OSPF. Si vous choisissez cette option, sélectionnez **Accept Summary (Accepter un récapitulatif)** pour accepter ce type de publication LSA. Sélectionnez **Advertise Default Route (Publier l'itinéraire par défaut)** si vous souhaitez inclure la publication LSA d'un itinéraire par défaut dans les publications de la zone terminale ainsi que la valeur de mesure associée (1 à 255). Sélectionnez également le type d'itinéraire utilisé pour publier la LSA par défaut. Cliquez sur **Add (Ajouter)** dans la section **External Ranges (Intervalles externes)** et saisissez des intervalles pour activer ou supprimer des itinéraires externes de publication appris via la zone NSSA vers d'autres zones.

OSPF – Paramètres des zones	Description
Intervalle	Cliquez sur **Add (Ajouter)** pour agréger les adresses de destination LSA d'une zone dans des sous-réseaux. Activez ou supprimez des publications LSA correspondant au sous-réseau et cliquez sur **OK**. Répétez cette étape pour ajouter des plages supplémentaires.
Interface	Cliquez pour **Add (Ajouter)** une interface à inclure dans la zone et saisissez les informations suivantes : • **Interface** - Sélectionnez l'interface. • **Enable (Activer)** - Applique les paramètres de l'interface OSPF. • **Passive (Passif)** : sélectionnez cette option si vous ne voulez pas que l'interface OSPF envoie ou reçoive des paquets OSPF. Bien qu'aucun paquet OSPF ne soit envoyé ou reçu si vous choisissez cette option, l'interface est incluse dans la base de données LSA. • **Link type (Type de liaison)** : sélectionnez **Broadcast (Diffusion)** si vous voulez que tous les voisins accessibles via l'interface soient détectés automatiquement en multidiffusant des messages Hello OSPF, comme une interface Ethernet. Sélectionnez **p2p** (point-to-point/point à point) pour détecter automatiquement un voisin. Sélectionnez **p2mp** (point-to-multipoint/point-multipoint) lorsque les voisins doivent être définis manuellement. La définition manuelle des voisins est uniquement autorisée pour le mode p2mp. • **Metric (Mesure)** - Saisissez la mesure OSPF pour cette interface (0 à 65 535). • **Priority (Priorité)** - Saisissez la priorité OSPF pour cette interface (0 à 255). Il s'agit de la priorité d'élection d'un routeur en tant que routeur désigné (DR) ou en tant que DR de secours (BDR) conformément au protocole OSPF. Lorsque la valeur affiche 0, le routeur ne sera pas élu en tant que DR ou BDR. • **Auth Profile (Profil d'authentification)** : sélectionnez un profil d'authentification précédemment défini. • **BFD** - Pour activer BFD (Bidirectional Forwarding Detection/détection de transmission bidirectionnelle) pour une interface OSPF homologue (et ainsi appliquer un contrôle prioritaire sur le paramètre **BFD** pour OSPF, pourvu que **BFD** ne soit pas activé pour OSPF au niveau du routeur virtuel), sélectionnez l'une des options suivantes : • **default (défaut)** (paramètres BFD par défaut) • un profil BFD que vous avez créé sur le pare-feu • **New BFD Profile (Nouveau profil BFD)** pour créer un nouveau profil BFD • Sélectionnez **Aucun (Désactiver la BFD)** pour désactiver la BFD pour l'interface OSPF homologue.

OSPF – Paramètres des zones	Description
	• **Hello Interval (sec) (Intervalle Hello (s))** - Intervalle, en secondes, auquel le processus OSPF envoie des paquets Hello à ses voisins directement connectés (intervalle compris entre 0 et 3 600 ; valeur par défaut : 10). • **Dead Counts (Nombre de pertes)** - Nombre de fois que l'intervalle Hello peut se produire pour un voisin sans qu'OSPF ne reçoive un paquet Hello du voisin, avant qu'OSPF ne considère ce voisin comme inactif. L'**intervalle Hello** multiplié par le **nombre de pertes** est égal à la valeur du minuteur d'inactivité (intervalle compris entre 3 et 20 ; valeur par défaut : 4). • **Retransmit Interval (sec) (Intervalle de retransmission (s))** - Durée, en secondes, pendant laquelle OSPF attend de recevoir une publication LSA (link-state advertisement) d'un voisin avant de la retransmettre (plage de 0 à 3 600 ; valeur par défaut de 10). • **Transit Delay (sec) (Délai de transit (s))** - Durée, en secondes, pendant laquelle une publication LSA est différée avant d'être envoyée d'une interface (plage de 0 à 3 600 ; valeur par défaut de 1).
Interface (suite)	• **Graceful Restart Hello Delay (sec) (Temporisation de redémarrage en douceur Hello (s))** - S'applique à une interface OSPF lorsque la haute disponibilité active / passive est configurée. **La temporisation de redémarrage en douceur Hello** est la durée pendant laquelle le pare-feu envoie des paquets LSA à des intervalles de 1 seconde. Pendant cette période, aucun paquet Hello n'est envoyé avant le redémarrage du pare-feu. Lors du redémarrage, le minuteur d'inactivité (qui correspond à l'**Intervalle Hello** multiplié par le **Nombre de pertes**) effectue un compte à rebours. Si la valeur du minuteur d'inactivité est trop faible, l'adjacence devient inactive pendant le redémarrage en douceur en raison de la temporisation Hello. Par conséquent, il est recommandé que la valeur du minuteur d'inactivité soit au moins quatre fois celle de la **Graceful Restart Hello Delay (Temporisation de redémarrage en douceur Hello)**. Par exemple, un **Intervalle Hello** de 10 secondes et un **Nombre de pertes** de 4 sont égaux à une valeur de minuteur d'inactivité de 40 secondes. Si la **Temporisation de redémarrage en douceur Hello** est définie sur 10 secondes, la valeur du minuteur d'activité de 40 secondes est suffisante pour que l'adjacence ne devienne pas inactive (plage de 1 à 10 ; valeur par défaut de 10).
Liaison virtuelle	Configurez les paramètres de liaison virtuelle ou améliorez la connectivité de la zone du segment principal. Ces paramètres doivent être définis pour les routeurs de bordure de zone et à l'intérieur de la zone du segment principal (0.0.0.0). Cliquez sur **Add (Ajouter)**, saisissez les informations suivantes pour chaque liaison virtuelle à inclure dans la zone du segment principal et cliquez sur **OK**. • **Name (Nom)** : donnez un nom à la liaison virtuelle.

OSPF – Paramètres des zones	Description
	• **Neighbor ID (ID du voisin)** : saisissez un ID de routeur (voisin) situé de l'autre côté de la liaison virtuelle. • **Transit Area (Zone de transit)** : saisissez l'ID de la zone de transit qui contient physiquement la liaison virtuelle. • **Enable (Activer)** : sélectionnez cette option pour activer la liaison virtuelle. • **Timing (Minutage)** : il est recommandé de conserver les paramètres de minutage par défaut. • **Auth Profile (Profil d'authentification)** : sélectionnez un profil d'authentification précédemment défini.

Onglet Profils d’authentification OSPF

- Réseau > Routeur virtuel > OSPF > Profils d'authentification

Les champs suivants décrivent les paramètres des profils d’authentification OSPF :

OSPF – Paramètres des profils d’authentification	Description
Nom du profil	Donnez un nom au profil d’authentification. Pour authentifier les messages OSPF, commencez par définir les profils d’authentification, puis appliquez-les aux interfaces dans l’onglet **OSPF**.
Type de mot de passe	Sélectionnez le type de mot de passe (simple ou MD5). • Si vous sélectionnez **Simple**, saisissez le mot de passe. • Si vous sélectionnez **MD5**, saisissez une ou plusieurs entrées de mot de passe, notamment **Key-ID (ID-Clé)** (0 à 255), **Key (Clé)** et éventuellement le statut **Preferred (Préféré)**. Cliquez sur **Add (Ajouter)** pour chaque entrée, puis cliquez sur **OK**. Pour indiquer la clé à utiliser afin d'authentifier le message sortant, sélectionnez l'option **Preferred (Préféré)**.

Onglet Règles d’exportation OSPF

- Réseau > Routeur virtuel > OSPF > Règles d'exportation

Le tableau suivant décrit les champs utilisés pour exporter les itinéraires OSPF :

OSPF – Paramètres des règles d’exportation	Description
Autoriser la redistribution des itinéraires par défaut	Sélectionnez cette option pour autoriser la redistribution des itinéraires par défaut via OSPF.
Name (Nom)	Sélectionnez le nom d'un profil de redistribution. La valeur doit être un sous-réseau'A0;IP ou un nom de profil de redistribution valide.
Nouveau type de chemin	Sélectionnez le type de mesure à appliquer.
Nouvelle étiquette	Indiquez une étiquette pour l'itinéraire correspondant dont la valeur est de 32 bits.
Mesure	(Facultatif) Indiquez la mesure de l'itinéraire à associer à l'itinéraire exporté et à utiliser pour la sélection du chemin (intervalle compris entre 1 et 65 535).

Onglet Avancé OSPF

- Réseau > Routeur virtuel > OSPF > Avancé

Les champs suivants décrivent la compatibilité RFC 1583, les minuteurs OSPF et le redémarrage en douceur :

OSPF – Paramètres avancés	Description
Compatibilité avec RFC 1583	Sélectionnez pour garantir la compatibilité avec RFC 1583 (OSPF version 2).
Minuteurs	• **SPF Calculation Delay (sec) (Délai du calcul SPF (s))** - Vous permet d'ajuster le délai écoulé entre la réception de nouvelles informations sur la topologie et la réalisation d'un calcul SPF. Des valeurs inférieures permettent une reconvergence OSPF plus rapide. Les routeurs échangeant du trafic avec le pare-feu doivent être ajustés de la même manière afin d'optimiser les délais de convergence. • **LSA Interval (sec) (Intervalle LSA (s))** - Indique le délai minimum écoulé entre les transmissions de deux instances du même LSA (même routeur, même type, même ID LSA). Cela équivaut à MinLSInterval dans le document RFC 2328. Des valeurs inférieures peuvent être utilisées pour réduire les délais de reconvergence en cas de modifications de topologie.
Redémarrage sans échec	• **Enable Graceful Restart (Activer le redémarrage en douceur)** (option activée par défaut) - Un pare-feu activé pour cette fonction indique aux routeurs voisins de continuer à utiliser un itinéraire via

OSPF – Paramètres avancés	Description
	le pare-feu, lorsque qu'une transition se produit et rend le pare-feu temporairement inactif. • **Enable Helper Mode (Activer le mode Aide)** (option activée par défaut) - Un pare-feu activé pour ce mode poursuit le transfert vers un périphérique adjacent lors du redémarrage du périphérique. • **Enable Strict LSA Checking (Activer la vérification LSA stricte)** (option activée par défaut) - Cette fonction amène un pare-feu activé en mode Aide OSPF à quitter ce mode, en cas de modifications de topologie. • **Grace Period (sec) (Délai supplémentaire (s))** - Période en secondes pendant laquelle les périphériques homologues doivent poursuivre le transfert vers le pare-feu lorsque la contiguïté est rétablie ou lorsque le routeur est redémarré (plage de 5 à 1 800 ; valeur par défaut de 120). • **Max Neighbor Restart Time (Délai de redémarrage max. du voisin)** - Délai supplémentaire maximal en secondes que le pare-feu accepte en tant que routeur en mode Aide. Si les périphériques homologues offrent une période de grâce plus longue dans leur LSA de grâce, le pare-feu ne bascule pas en mode Aide (intervalle compris entre 5 et 1 800 ; valeur par défaut : 140).

OSPFv3

- Réseau > Routeur virtuel > OSPFv3

La configuration du protocole Open Shortest Path First v3 (OSPFv3) nécessite la configuration des trois premiers paramètres dans le tableau suivant (BFD est optionnel) :

Paramètres OSPFv3	Description
Activer	Sélectionnez cette option pour activer le protocole OSPF.
Rejeter les itinéraires par défaut	Sélectionnez cette option si vous ne voulez pas apprendre des itinéraires via OSPF par défaut.
ID de routeur	Indiquez l'ID du routeur associé à l'instance OSPF dans ce routeur virtuel. Le protocole OSPF utilise l'ID du routeur pour identifier uniquement l'instance OSPF.
BFD	Pour activer la BFD (Bidirectional Forwarding Detection/détection de transmission bidirectionnelle) globalement pour OSPFv3 du routeur virtuel sur un pare-feu PA-400 Series, PA-3200 Series, PA-3400 Series et VM-Series, sélectionnez l'une des options suivantes : • **default (défaut)** (paramètres BFD par défaut)

Paramètres OSPFv3	Description
	• un profil BFD que vous avez créé sur le pare-feu • **New BFD Profile (Nouveau profil BFD)** pour créer un nouveau profil BFD Sélectionnez **Aucun (Désactiver la BFD)** pour désactiver la BFD pour toutes les interfaces OSPFv3 sur le routeur virtuel. Vous ne pouvez pas activer la BFD pour une seule interface OSPFv3.

De plus, vous devez configurer les paramètres OSPFv3 dans les onglets suivants :

- **Areas (Zones)** : Voir Onglet des zones OSPFv3.
- **Auth Profiles (Profils d'authentification)** : Reportez-vous à la section Onglet Profils d’authentification OSPFv3.
- **Export Rules (Règles d'exportation)** : Reportez-vous à la section Onglet Règles d’exportation OSPFv3.
- **Advanced (Avancé)** : Voir Onglet avancé OSPFv3.

Onglet des zones OSPFv3

- Réseau > Routeur virtuel > OSPFv3 > Zones

Utilisez les champs suivants pour configurer les zones OSPFv3.

OSPv3 – Paramètres des zones	Description
Authentification	Sélectionnez le nom du profil d'authentification que vous souhaitez définir pour cette zone'A0;OSPF.
Type	Sélectionnez l'une des options suivantes : • **Normal**— Il n'y a aucune restriction ; la zone peut porter tous les types d'itinéraires. • **Stub (Terminale)** : il n'existe aucune sortie issue de la zone. Pour atteindre une destination extérieure à la zone, vous devez passer par la bordure qui se connecte aux autres zones. Si vous choisissez cette option, sélectionnez **Accept Summary (Accepter un récapitulatif)** pour accepter ce type de publication LSA (Link State Advertisement/annonce d'état de liaison) de la part des autres zones. Spécifiez également s'il faut inclure un LSA de route par défaut dans les annonces vers la zone de stub avec la valeur de métrique associée (1-255). Si l'option **Accept Summary** sur une interface Area Border Router (ABR) de zone de stub est désactivée, la zone OSPF se comportera comme une Totally Stubby Area (TSA) et l'ABR ne propagera aucun LSA de résumé.

OSPv3 – Paramètres des zones	Description
	• **NSSA** (Not-So-Stubby Area) : il est possible de quitter la zone directement, mais uniquement par des routes autres que les itinéraires OSPF. Si vous choisissez cette option, sélectionnez **Accept Summary (Accepter un récapitulatif)** pour accepter ce type de publication LSA. Indiquez si vous souhaitez inclure la publication LSA d'un itinéraire par défaut dans les publications de la zone terminale avec la valeur de mesure associée (1 à 255). Sélectionnez également le type d'itinéraire utilisé pour publier la LSA par défaut. Cliquez sur **Add (Ajouter)** dans la section **External Ranges (Intervalles externes)** et saisissez des intervalles pour activer ou supprimer des itinéraires externes de publication appris via la zone NSSA vers d'autres zones
Intervalle	Cliquez sur **Add (Ajouter)** pour agréger les adresses IPv6 de destination LSA d'une zone par sous-réseau. Activez ou supprimez des publications LSA correspondant au sous-réseau et cliquez sur **OK**. Répétez cette étape pour ajouter des plages supplémentaires.
Interface	Cliquez sur **Add (Ajouter)** et saisissez les informations suivantes pour chaque interface à inclure dans la zone et cliquez sur **OK**. • **Interface** - Sélectionnez l'interface. • **Enable (Activer)** - Applique les paramètres de l'interface OSPF. • **Instance ID (ID d'instance)** - Saisissez un numéro d'identification d'instance OSPFv3. • **Passive (Passif)** - Sélectionnez cette option si vous ne voulez pas que l'interface OSPF envoie ou reçoive des paquets OSPF. Bien qu'aucun paquet OSPF ne soit envoyé ou reçu si vous choisissez cette option, l'interface est incluse dans la base de données LSA. • **Link type (Type de liaison)** : sélectionnez **Broadcast (Diffusion)** si vous voulez que tous les voisins accessibles via l'interface soient détectés automatiquement en multidiffusant des messages Hello OSPF, comme une interface Ethernet. Sélectionnez **p2p** (point-to-point/point à point) pour détecter automatiquement un voisin. Sélectionnez **p2mp** (point-to-multipoint/point-multipoint) lorsque les voisins doivent être définis manuellement. La définition manuelle des voisins est uniquement autorisée pour le mode p2mp. • **Metric (Mesure)** - Saisissez la mesure OSPF pour cette interface (0 à 65 535). • **Priority (Priorité)** - Saisissez la priorité OSPF pour cette interface (0 à 255). Il s'agit de la priorité d'élection d'un routeur en tant que routeur désigné (DR) ou en tant que DR de secours (BDR) conformément au protocole OSPF. Lorsque la valeur affiche 0, le routeur ne sera pas élu en tant que DR ou BDR.

OSPv3 – Paramètres des zones	Description
	• **Auth Profile (Profil d'authentification)** : sélectionnez un profil d'authentification précédemment défini. • **BFD** - Pour activer BFD (Bidirectional Forwarding Detection/ détection de transmission bidirectionnelle) pour une interface OSPFv3 homologue (et ainsi appliquer un contrôle prioritaire sur le paramètre **BFD** pour OSPFv3, pourvu que **BFD** ne soit pas activé pour OSPFv3 au niveau du routeur virtuel), sélectionnez l'une des options suivantes : • **default (défaut)** (paramètres BFD par défaut) • un profil BFD que vous avez créé sur le pare-feu • **New BFD Profile (Nouveau profil BFD)** pour créer un nouveau profil BFD Sélectionnez **None (Disable BFD) (Aucun (Désactiver la BFD))** pour désactiver la BFD pour l'interface OSPFv3 homologue. • **Hello Interval (sec) (Intervalle Hello (s))** - Intervalle, en secondes, auquel le processus OSPF envoie des paquets Hello à ses voisins directement connectés (intervalle compris entre 0 et 3 600 ; valeur par défaut : 10). • **Dead Counts (Nombre de pertes)** - Nombre de fois que l'intervalle Hello peut se produire pour un voisin sans qu'OSPF ne reçoive un paquet Hello du voisin, avant qu'OSPF ne considère ce voisin comme inactif. L'**intervalle Hello** multiplié par le **nombre de pertes** est égal à la valeur du minuteur d'inactivité (intervalle compris entre 3 et 20 ; valeur par défaut : 4). • **Retransmit Interval (sec) (Intervalle de retransmission (s))** - Durée, en secondes, pendant laquelle OSPF attend de recevoir une publication LSA (link-state advertisement) d'un voisin avant de la retransmettre (plage de 0 à 3 600 ; valeur par défaut de 10). • **Transit Delay (sec) (Délai de transit (s))** - Durée, en secondes, pendant laquelle une publication LSA est différée avant d'être envoyée d'une interface par le pare-feu (plage de 0 à 3 600 ; valeur par défaut de 1).
Interface (suite)	• **Graceful Restart Hello Delay (sec) (Temporisation de redémarrage en douceur Hello (s))** - S'applique à une interface OSPF lorsque la haute disponibilité active / passive est configurée. **La temporisation de redémarrage en douceur Hello** est la durée pendant laquelle le pare-feu envoie des paquets LSA à des intervalles de 1 seconde. Pendant cette période, aucun paquet Hello n'est envoyé avant le redémarrage du pare-feu. Lors du redémarrage, le minuteur d'inactivité (qui correspond à l'**Intervalle Hello** multiplié par le **Nombre de pertes**) effectue un compte

OSPv3 – Paramètres des zones	Description
	à rebours. Si la valeur du minuteur d'inactivité est trop faible, l'adjacence devient inactive pendant le redémarrage en douceur en raison de la temporisation Hello. Par conséquent, il est recommandé que la valeur du minuteur d'inactivité soit au moins quatre fois celle de la **Graceful Restart Hello Delay (Temporisation de redémarrage en douceur Hello)**. Par exemple, un **Intervalle Hello** de 10 secondes et un **Nombre de pertes** de 4 sont égaux à une valeur de minuteur d'inactivité de 40 secondes. Si la **Temporisation de redémarrage en douceur Hello** est définie sur 10 secondes, la valeur du minuteur d'activité de 40 secondes est suffisante pour que l'adjacence ne devienne pas inactive (plage de 1 à 10 ; valeur par défaut de 10). • **Neighbors (Voisins)** - Pour les interfaces p2pmp, saisissez l'adresse IP de tous les voisins accessibles via cette interface.
Liaisons virtuelles	Configurez les paramètres de liaison virtuelle ou améliorez la connectivité de la zone du segment principal. Ces paramètres doivent être définis pour les routeurs de bordure de zone et à l'intérieur de la zone du segment principal (0.0.0.0). Cliquez sur **Add (Ajouter)**, saisissez les informations suivantes pour chaque liaison virtuelle à inclure dans la zone du segment principal et cliquez sur **OK**. • **Name (Nom)** : donnez un nom à la liaison virtuelle. • **Instance ID (ID d'instance)** - Saisissez un numéro d'identification d'instance OSPFv3. • **Neighbor ID (ID du voisin)** : saisissez un ID de routeur (voisin) situé de l'autre côté de la liaison virtuelle. • **Transit Area (Zone de transit)** : saisissez l'ID de la zone de transit qui contient physiquement la liaison virtuelle. • **Enable (Activer)** : sélectionnez cette option pour activer la liaison virtuelle. • **Timing (Minutage)** : il est recommandé de conserver les paramètres de minutage par défaut. • **Auth Profile (Profil d'authentification)** : sélectionnez un profil d'authentification précédemment défini.

Onglet Profils d'authentification OSPFv3

- Réseau > Routeur virtuel > OSPFv3 > Profils d'authentification

Utilisez les champs suivants pour configurer l'authentification pour OSPFv3.

OSPFv3 – Paramètres des profils d'authentification	Description
Nom du profil	Donnez un nom au profil d'authentification. Pour authentifier les messages OSPF, commencez par définir les profils d'authentification, puis appliquez-les aux interfaces dans l'onglet **OSPF**.
SPI	Indiquez l'index de paramètres de sécurité (SPI) pour le parcours du paquet entre le pare-feu distant et l'homologue.
Protocole	Indiquez l'un des protocoles suivants : • **ESP** - Protocole Encapsulating Security Payload/ Encapsulation sécurisée de la charge utile • **AH** - Protocole Authentication Header
Algorithme de chiffrement	Indiquez l'un des suivants : • **None (Aucun)** - Aucun algorithme de chiffrement n'est utilisé. • **SHA1** (par défaut) - Algorithme SHA 1. • **SHA256** - Algorithme Secure Hash Algorithm 2 (algorithme de hachage sécurisé 1). Un ensemble de quatre fonctions de hachage dotées d'un algorithme de 256 bits. • **SHA384** - Algorithme Secure Hash Algorithm 2 (algorithme de hachage sécurisé 1). Un ensemble de quatre fonctions de hachage dotées d'un algorithme de 384 bits. • **SHA512** - Algorithme Secure Hash Algorithm 2 (algorithme de hachage sécurisé 1). Un ensemble de quatre fonctions de hachage dotées d'un algorithme de 512 bits. • **MD5** - Algorithme Message Digest 5 (algorithme de condensé de message 5).
Clé/Confirmer la clé	Saisissez et confirmez la clé d'authentification.
Chiffrement (protocole ESP uniquement)	Indiquez l'un des suivants : • **3des** (par défaut) – applique l'algorithme de chiffrement de données triple (3DES) à l'aide de trois clés cryptographiques de 56 bits. • **aes-128-cbc** - Applique le chiffrement AES (Advanced Encryption Standard/norme de chiffrement avancé) à l'aide de clés cryptographiques de 128 bits. • **aes-192-cbc** - Applique le chiffrement AES (Advanced Encryption Standard/norme de chiffrement avancé) à l'aide de clés cryptographiques de 192 bits.

OSPFv3 – Paramètres des profils d’authentification	Description
	• **aes-256-cbc** - Applique le chiffrement AES (Advanced Encryption Standard/norme de chiffrement avancé) à l’aide de clés cryptographiques de 256 bits. • **null (aucun)** - Aucun chiffrement n’est utilisé.
Clé/Confirmer la clé	Saisissez et confirmez la clé de chiffrement.

Onglet Règles d’exportation OSPFv3

- Réseau > Routeur virtuel > OSPFv3 > Règles d’exportation

Utilisez les champs suivants pour exporter les itinéraires OSPFv3.

OSPFv3 – Paramètres des règles d’exportation	Description
Autoriser la redistribution des itinéraires par défaut	Sélectionnez cette option pour autoriser la redistribution des itinéraires par défaut via OSPF.
Name (Nom)	Sélectionnez le nom d'un profil de redistribution. La valeur doit être un sous-réseau'A0;IP ou un nom de profil de redistribution valide.
Nouveau type de chemin	Sélectionnez le type de mesure à appliquer.
Nouvelle étiquette	Indiquez une étiquette pour l'itinéraire correspondant dont la valeur est de 32 bits.
Mesure	(Facultatif) Indiquez la mesure de l'itinéraire à associer à l'itinéraire exporté et à utiliser pour la sélection du chemin (intervalle compris entre 1 et 65 535).

Onglet Avancé OSPFv3

- Réseau > Routeur virtuel > OSPFv3 > Avancé

Utilisez les champs suivants pour désactiver le routage de transit pour les calculs SPF, configurer les minuteurs OSPFv3 et configurer un redémarrage en douceur pour OSPFv3.

OSPFv3 – Paramètres avancés	Description
Désactiver le routage de l'acheminement pour le calcul SPF	Sélectionnez cette option si vous souhaitez définir le bit R dans les LSA de routeur envoyés par ce pare-feu pour indiquer que le pare-feu n’est pas actif. Lorsqu'il est dans cet état, le pare-feu prend part à OSPFv3 mais les autres routeurs n'envoient pas le trafic de l'acheminement. Dans cet état, le trafic local est transféré au pare-feu. Cela est utile lors de la maintenance sur un réseau à double interface, car le trafic peut être encore atteint lorsqu'il est réacheminé vers le pare-feu.
Minuteurs	• **SPF Calculation Delay (sec) (Délai du calcul SPF (s))** - Cette option est un temporisateur vous permettant d’ajuster le délai écoulé entre la réception de nouvelles informations sur la topologie et la réalisation d’un calcul SPF. Des valeurs inférieures permettent une reconvergence OSPF plus rapide. Les routeurs échangeant du trafic avec le pare-feu doivent être ajustés de la même manière afin d'optimiser les délais de convergence. • **LSA Interval (sec) (Intervalle LSA (s))** - Cette option indique le délai minimum écoulé entre les transmissions de deux instances du même LSA (même routeur, même type, même ID LSA). Cela équivaut à MinLSInterval dans le document RFC 2328. Des valeurs inférieures peuvent être utilisées pour réduire les délais de reconvergence en cas de modifications de topologie.
Redémarrage sans échec	• **Enable Graceful Restart (Activer le redémarrage en douceur)** (option activée par défaut) - Un pare-feu activé pour cette fonction indique aux routeurs voisins de continuer à utiliser un itinéraire via le pare-feu, lorsque qu'une transition se produit et rend le pare-feu temporairement inactif. • **Enable Helper Mode (Activer le mode Aide)** (option activée par défaut) - Un pare-feu activé pour ce mode poursuit le transfert vers un périphérique adjacent lors du redémarrage du périphérique. • **Enable Strict LSA Checking (Activer la vérification LSA stricte)** (option activée par défaut) - Cette fonction amène un pare-feu activé en mode Aide OSPF à quitter ce mode, en cas de modifications de topologie. • **Grace Period (sec) (Délai supplémentaire (s))** - Période, en secondes, pendant laquelle les périphériques homologues doivent poursuivre le transfert vers le pare-feu lorsque la contiguïté est rétablie ou lorsque le routeur est redémarré (plage de 5 à 1 800 ; valeur par défaut de 120).

OSPFv3 – Paramètres avancés	Description
	• **Max Neighbor Restart Time (Durée maximale de redémarrage des voisins)** - Période de grâce maximale en secondes que le pare-feu accepte en tant que routeur en mode Aide. Si les périphériques homologues offrent une période de grâce plus longue dans leur LSA de grâce, le pare-feu ne bascule pas en mode Aide (intervalle compris entre 5 et 800 ; valeur par défaut : 140).

BGP

- Réseau > Routeur virtuel > BGP

La configuration du Protocole de passerelle frontière (BGP) vous oblige à configurer Paramètres BGP de base pour activer BGP et configurer l'ID du routeur et le Numéro AS comme décrit dans le tableau suivant. En outre, vous devez configurer un homologue BGP dans le cadre d'un groupe d'homologues BGP.

Configurez les paramètres BGP restants dans les onglets suivants, si nécessaire pour votre réseau :

- **Général** : voir Onglet Général BGP ;
- **Avancé** : voir Onglet Avancé BGP ;
- **Groupe d'homologues** : voir Onglet Groupe d'homologues BGP.
- **Importer** : voir Onglets d'Importation et d'Exportation BGP.
- **Exporter** : voir Onglets d'Importation et d'Exportation BGP.
- **Avancé Publication conditionnelle** : voir Onglet Avancé Publication conditionnelle BGP.
- **Agréger** : voir Onglet Agrégation BGP ;
- **Règles de redistribution** : voir Onglet Règles de redistribution BGP.

Paramètres BGP de base

Pour utiliser BGP sur un routeur virtuel, vous devez activer BGP et configurer l'ID du routeur et le Numéro AS ; l'activation de BFD est facultative.

Paramètres BGP	Configuré dans	Description
Activer	**BGP**	Sélectionnez cette action pour activer BGP.
ID du routeur		Saisissez l'adresse IP à assigner à un routeur virtuel.
Numéro AS		Saisissez le numéro de l'AS auquel appartient le routeur virtuel, en fonction de l'ID du routeur (compris entre 1 et 4 294 967 295).
BFD		Pour activer la BFD (Bidirectional Forwarding Detection/détection de transmission bidirectionnelle) globalement pour BGP du routeur virtuel sur un pare-feu PA-400 Series, PA-3200 Series, PA-3400

Paramètres BGP	Configuré dans	Description
		Series, PA-5200 Series, PA-5400 Series, PA-7000 Series ou VM-Series, sélectionnez l'une des options suivantes : • **default (défaut)** (paramètres BFD par défaut) • un profil BFD existant sur le pare-feu • création d'un **nouveau profil BFD**. Sélectionnez **Aucun (Désactiver la BFD))** pour désactiver BFD pour toutes les interfaces BGP du routeur virtuel ; vous ne pouvez activer la BFD pour une seule interface BGP. *Si vous activez ou désactivez la BFD globalement, toutes les interfaces qui exécutent BGP seront désactivées et réactivées avec la fonctionnalité BFD, ce qui peut interrompre le trafic BGP. Par conséquent, activez la BFD sur les interfaces BGP lors des périodes creuses où une conversion n'influe pas sur le trafic de production.*

Onglet Général BGP

- Réseau > Routeur virtuel > BGP > Général

Utilisez les champs suivants pour configurer les paramètres généraux de BGP.

Paramètres généraux de BGP	Configuré dans	Description
Rejeter les itinéraires par défaut	**BGP** > **Général**	Sélectionnez pour ignorer les itinéraires par défaut publiés par les homologues BGP.
Installer un itinéraire		Sélectionnez pour installer des itinéraires BGP dans la table de routage générale.
Agréger MED		Sélectionnez cette option pour activer l'agrégation d'un itinéraire, même lorsque des itinéraires affichent différentes valeurs MED (Discriminateur Multi-Sortie).
Préférence locale par défaut		Indique une valeur que le pare-feu peut utiliser pour déterminer les préférences entre différents chemins.
Format AS		Sélectionnez le format 2 octets (par défaut) ou 4 octets. Ce paramètre peut être configuré à des fins d'interopérabilité.

Paramètres généraux de BGP	Configuré dans	Description
Toujours comparer MED		Activez la comparaison MED des chemins de voisins situés dans différents systèmes autonomes.
Comparaison MED déterministe		Activez la comparaison MED afin de sélectionner un itinéraire parmi ceux qui sont publiés par des homologues iBGP (homologues BGP figurant dans le même système autonome).
Profils d'authentification		Vous devez **Ajouter** un profil d'authentification et configurer les paramètres suivants : • **Nom du profil** - Saisissez un nom pour identifier le profil. • **Phrase secrète/Confirmer une phrase secrète** - Saisissez et confirmez une phrase secrète pour les communications d'homologues BGP. Supprimez () les profils vous n'en avez plus besoin.

Onglet Avancé BGP

- Réseau > Routeur virtuel > BGP > Avancé

Les paramètres avancés de BGP incluent une multitude de fonctionnalités. Vous pouvez exécuter ECMP sur plusieurs systèmes BGP autonomes. Vous pouvez exiger de la part des homologues eBGP qu'ils énumèrent leur propre AS comme premier AS dans un attribut AS_PATH (pour éviter les paquets de Mise à jour usurpés). Vous pouvez configurer le redémarrage en douceur de BGP, un moyen au moyen duquel les homologues BGP indiquent s'ils peuvent conserver l'état du transfert lors d'un redémarrage de BGP afin de minimiser les conséquences des itinéraires instables (qui montent et qui descendent). Vous pouvez configurer les réflecteurs d'itinéraires et les confédérations d'AS ; deux méthodes qui permettent d'éviter un maillage complet des appairages BGP dans un AS. Vous pouvez configurer le blocage de l'itinéraire pour éviter la convergence inutile du routeur lorsqu'un réseau BGP est instable et que les itinéraires sont instables.

Paramètres avancés BGP	Configuré dans	Description
Support de multiples AS dans ECMP	**BGP** > **Avancé**	Sélectionnez si vous activez ECMP pour un routeur virtuel et que vous souhaitez exécuter ECMP sur plusieurs systèmes BGP autonomes.
Appliquer le premier AS pour EBGP		Amène le pare-feu à supprimer un paquet de Mise à jour entrant d'un homologue eBGP qui ne répertorie pas le numéro AS de l'homologue eBGP comme premier numéro AS dans

Paramètres avancés BGP	Configuré dans	Description
		l’attribut AS_PATH. Cela empêche BGP de traiter ultérieurement un paquet de Mise à jour usurpé ou erroné qui provient d’un AS autre qu’un AS voisin. La valeur par défaut est activée.
Redémarrage sans échec		Activez l'option de redémarrage en douceur. • **Temps d’itinéraire périmé** - Indiquez la durée, en secondes, pendant laquelle un itinéraire peut rester dans l'état Obsolète (intervalle compris entre 1 et 3 600 ; valeur par défaut : 120). • **Délai de redémarrage local (s)** - Spécifiez le délai d'attente, en secondes, du pare-feu local pour redémarrer. Cette valeur est publiée chez les homologues (intervalle compris entre 1 et 3 600 ; valeur par défaut : 120). • **Durée maximale de redémarrage des homologues** - Indiquez la durée maximale, en secondes, qu'un pare-feu local accepte comme délai de redémarrage en période de grâce pour des périphériques homologues (intervalle compris entre 1 et 3 600 ; valeur par défaut : 120).
ID du groupe de réflecteurs		Indiquez un identifiant IPv4 pour représenter un groupe de réflecteurs. Un réflecteur d’itinéraire (routeur) dans une AS effectue un rôle visant à republier des itinéraires qu’il a appris à ses homologues (plutôt que d’exiger une connectivité en maillage complet et que tous les homologues s’envoient des itinéraires les uns aux autres). Le réflecteur d’itinéraire simplifie la configuration.
AS membre de la confédération		Indiquez le numéro d’identification du système autonome (AS) qui n’est visible qu’au sein de la confédération BGP (également nommé numéro de système sous-autonome). Utilisez une confédération BGP pour diviser les systèmes autonomes en systèmes sous-autonomes et réduire l’appairage de maillage complet.
Profils d'atténuation	**BGP** > **Avancé (suite)**	Le blocage de l’itinéraire est une méthode qui détermine si un itinéraire est supprimé de la publication parce qu’il est instable. Le blocage de l’itinéraire peut réduire le nombre de fois que les routeurs sont forcés à la conversion en raison de l’instabilité des itinéraires. Les paramètres sont les suivants : • **Nom du profil** - Saisissez un nom pour identifier le profil. • **Activer** - Activez le profil. • **Cutoff (Limite)** - Indiquez le seuil de retrait d'itinéraires au-delà duquel une publication d'itinéraire est supprimée (intervalle compris entre 0,0 et 1 000,0 ; valeur par défaut : 1,25).

Paramètres avancés BGP	Configuré dans	Description
		• **Réutiliser** - Indiquez le seuil de retrait d'itinéraires au-dessous duquel un itinéraire supprimé est réutilisé (intervalle compris entre 0,0 et 1 000,0 ; valeur par défaut : 5). • **Max. Durée d'attente maximale** - Indiquez la durée maximale, en secondes, au bout de laquelle un itinéraire peut être supprimé, quelle que soit son instabilité (intervalle compris entre 0 et 3 600 ; valeur par défaut : 900). • **Réduction de moitié pendant l'état accessible** – Indiquez la durée, en secondes, après laquelle la mesure de stabilité d'un itinéraire est réduite de moitié si le pare-feu est accessible (plage de 0 à 3 600 ; par défaut 300). • **Réduction de moitié pendant l'état inaccessible** – Indiquez la durée, en secondes, après laquelle la mesure de stabilité d'un itinéraire est réduite de moitié si le pare-feu est inaccessible (plage de 0 à 3 600 ; par défaut 300). Supprimez (⊖) les profils vous n'en avez plus besoin.

Onglet Groupe d'homologues BGP

- Réseau > Routeur virtuel > BGP > Groupe d'homologues

Un groupe d'homologues BGP est un ensemble d'homologues BGP qui partagent des paramètres comme le type de groupe d'homologues (EBGP, par exemple) ou le paramètre servant à supprimer des numéros AS privés de la liste AS_PATH que le routeur virtuel envoie dans les paquets de Mise à jour. Les groupes d'homologues BGP vous évitent de devoir configurer plusieurs homologues avec les mêmes paramètres. Vous devez configurer au moins un groupe d'homologues BGP afin de configurer les homologues BGP appartenant au groupe.

Paramètres du groupe d'homologues B	Configuré dans	Description
Nom	**BGP** > **Groupe d'homologues**	Saisissez un nom pour identifier le groupe d'homologues.
Activer		Sélectionnez cette option pour activer un groupe d'homologues.
Chemin AS de confédération agrégé		Sélectionnez pour inclure un chemin vers l'AS de confédération agrégé configuré.
Réinitialisation logicielle		Sélectionnez pour procéder à une réinitialisation logicielle du pare-feu après avoir mis à jour les paramètres des homologues.

Paramètres du groupe d'homologues B	Configuré dans	Description
avec les informations stockées		
Type		Indiquez le type d'homologue ou de groupe et configurez les paramètres associés (pour plus de détails sur les options **Importer le saut suivant** et **Exporter le saut suivant**, consultez le tableau ci-dessous). • **IBGP** - Spécifiez les options suivantes : • **Exporter le saut suivant** • **Conféd. EBGP** - Spécifiez les options suivantes : • **Exporter le saut suivant** • **Conféd. IBGP** - Spécifiez les options suivantes : • **Exporter le saut suivant** • **EBGP** - Indiquez les options suivantes : • **Importer le saut suivant** • **Exporter le saut suivant** • **Supprimer l'AS privé** (sélectionnez cette option si vous voulez forcer le protocole BGP à supprimer des numéros d'AS privés provenant de l'attribut AS_PATH).
Importer le saut suivant		Sélectionnez une option pour importer le saut suivant'A0;: • **Original** – Utilisez l'adresse du Saut suivant fournie dans la publication de l'itinéraire d'origine. • **Utiliser homologue** – Utilisez l'adresse IP de l'homologue en tant qu'adresse du Saut suivant.
Exporter le saut suivant		Sélectionnez une option pour exporter le saut suivant'A0;: • **Résoudre** – Résolvez l'adresse Saut suivant à l'aide de la base d'informations de transfert (FIB). • **Original** – Utilisez l'adresse du Saut suivant fournie dans la publication de l'itinéraire d'origine. • **Utiliser auto** – Remplacez l'adresse du Saut suivant par l'adresse IP du routeur virtuel afin de s'assurer qu'elle apparaîtra dans le chemin de transfert.
Supprimer l'AS privé		Sélectionnez cette option pour supprimer les systèmes autonomes privés de la liste AS_PATH.

Paramètres du groupe d'homologues B	Configuré dans	Description
Nom	**BGP** > **Groupe d'homologues** > **Homologue**	Ajouter un **Nouvel** homologue BGP et saisissez un nom pour l'identifier.
Activer		Sélectionnez cette option pour activer un homologue.
AS Homologue		Indiquez le système autonome (AS) de l'homologue.
Activer les extensions MP-BGP	**BGP** > **Groupe d'homologues** > **Homologue** > **Adressage**	Permet au pare-feu de prendre en charge l'Identifiant de la famille d'adresses de BGP multi-protocoles pour IPv4 et IPv6 et les options d'Identifiant de la famille d'adresses subséquentes conformément au protocole RFC 4760.
Type de famille d'adresses		Sélectionnez soit la famille d'adresses **IPv4** ou **IPv6** que les sessions BGP avec cet homologue prennent en charge.
Famille d'adresses subséquentes		Sélectionnez le protocole de la famille d'adresses subséquentes **Unicast** ou **Multicast** que les sessions BGP avec cet homologue transmettent.
Adresse locale – Interface		Choisissez une interface de pare-feu.
Adresse locale – IP		Choisissez une adresse IP locale.
Adresse de l'homologue — Type et adresse		Sélectionnez le type d'adresse qui identifie l'homologue : • **IP** —Sélectionnez l'adresse IP et sélectionnez un objet d'adresse qui utilise une adresse IP (ou créez un nouvel objet d'adresse qui utilise une adresse IP). • **FQDN** —Sélectionnez FQDN et sélectionnez un objet d'adresse qui utilise un FQDN (ou créez un nouvel objet d'adresse qui utilise un FQDN).
Profil d'authentification	**BGP** > **Groupe d'homologues** > **Homologue** > **Options de connexion**	Sélectionnez un profil ou sélectionnez **Nouveau profil d'authentification** dans le menu déroulant. Saisissez un **Nom** de profil et l'élément **Secret**, et **(Confirmer l'élément secret)**.
Intervalle de maintien en vie		Indiquez un intervalle après lequel les itinéraires d'un homologue sont supprimés conformément au paramètre de durée d'attente (plage comprise entre 0 et 1 200 secondes ; valeur par défaut : 30 secondes).

Paramètres du groupe d'homologues B	Configuré dans	Description
Plusieurs sauts		Définissez la valeur TTL (Time-To-Live) dans l'en-tête IP (plage comprise entre 0 et 255 ; valeur par défaut : 0). La valeur par défaut de 0 signifie 1 pour IBGP. La valeur par défaut de 0 signifie 255 pour IBGP.
Délai avant ouverture		Indiquez le délai écoulé entre l'ouverture de la connexion TCP de l'homologue et l'envoi du premier message d'ouverture BGP (plage comprise entre 0 et 240 secondes, valeur par défaut : 0 seconde).
temps d'attente		Indiquez la durée pouvant s'écouler entre des messages KEEPALIVE ou UPDATE successifs émis par un homologue avant la fermeture de la connexion d'un homologue (plage de 3 à 3 600 secondes ; par défaut 90 secondes).
Temps d'attente d'inactivité		Indiquez la durée d'attente en état inactif avant de retenter une connexion à un homologue (plage de 1 à 3 600 secondes ; par défaut 15 secondes).
Connexions entrantes – Port distant		Indiquez le numéro de port entrant et veillez à **Autoriser** le trafic vers ce port.
Connexions sortantes – Port local		Indiquez le numéro de port sortant et veillez à **Autoriser** le trafic provenant de ce port
Client réflecteur	**BGP** > **Groupe d'homologues** > **Homologue** > **Avancé**	Sélectionnez le type de client réflecteur (**Non-Client**, **Client** ou **Client avec maillage**). Les itinéraires qui sont envoyés par les clients réflecteurs sont partagés avec l'ensemble des homologues BGP internes et externes.
Type d'homologie		Indiquez un homologue Bilatéral ou laissez ce champ Non spécifié.
Nombre max. de préfixes		Spécifiez le nombre maximum de préfixes IP à importer depuis le pair (1 à 100 000 ou illimité).
Activer la détection des boucles côté expéditeur		Permet de faire en sorte que le pare-feu vérifie l'attribut AS_PATH d'un itinéraire dans sa FIB avant d'envoyer l'itinéraire dans une mise à jour afin de s'assurer que le numéro AS de l'homologue n'est pas sur la liste AS_PATH. Si c'est le cas, le pare-feu le supprime pour éviter une boucle. Généralement, le récepteur

Paramètres du groupe d'homologues B	Configuré dans	Description
		effectue la détection des boucles, mais cette fonctionnalité d'optimisation comporte la détection des boucles par l'expéditeur.
BFD		Pour activer la BFD (Bidirectional Forwarding Detection) pour un homologue BGP (et ainsi appliquer un contrôle prioritaire sur le paramètre **BFD** pour BGP, du moment que la **BFD** n'est pas désactivée pour BGP au niveau du routeur virtuel), sélectionnez le profil par défaut (paramètres BFD par défaut), un profil BFD existant, **Inherit-vr-global-setting** (pour hériter du profil BFD BGP global), ou **Nouveau profil BFD** (pour créer un nouveau profil BFD). **Désactiver la BFD** - désactive la BFD pour l'homologue BGP. *Si vous activez ou désactivez la BFG globalement, toutes les interfaces qui exécutent BGP seront désactivées et réactivées avec la fonctionnalité BFD, ce qui pourrait interrompre le trafic BGP. Lorsque vous activez la BFD sur l'interface, le pare-feu arrête la connexion BGP vers l'homologue pour programmer la BFD sur l'interface. La connexion BGP sera abandonnée sur le périphérique homologue, ce qui pourrait entraîner une reconvergence qui influera sur le trafic de production. vous devez activer la BFD sur les interfaces BGP lors des périodes creuses où une reconvergence n'influera pas sur le trafic de production.*

Onglets d'Importation et d'Exportation BGP

- Réseau > Routeur virtuel > BGP > Importation
- Réseau > Routeur virtuel > BGP > Exportation

Ajouter une nouvelle règle d'Importation ou d'Exportation pour importer ou exporter des itinéraires BGP.

Paramètres d'Importation et d'Exportation B	Configuré dans	Description
Règles	**BGP** > **Importer ou exporter** > **Général**	Indiquez un nom permettant d'identifier la règle. La règle d'importation peut comporter un maximum de 63 caractères ; La règle d'exportation peut comporter un maximum de 31 caractères. La règle doit commencer par un caractère alphanumérique et peut

Paramètres d'Importation et d'Exportation B	Configuré dans	Description
		contenir une combinaison de caractères alphanumériques, de trait de soulignement (_), de trait d'union (-), de point (.) et d'espace.
Activer		Sélectionnez pour activer la règle.
Utilisé par		Sélectionnez les groupes d'homologues qui vont utiliser cette règle.
Expression régulière du chemin AS	**BGP** > **Importer ou exporter** > **Correspondance**	Indiquez une expression régulière pour le filtrage des chemins AS.
Expression régulière de la communauté		Indiquez une expression régulière pour le filtrage des chaînes de la communauté.
Expression régulière de la communauté étendue		Indiquez une expression régulière pour le filtrage des chaînes de la communauté étendue.
Moyen		Indiquez une valeur de Discriminateur de sorties multiples pour le filtrage d'itinéraire dans la plage de 0 à 4 294 967 295.
Table d'itinéraires		Pour une **Règle d'importation**, indiquez dans quelle table de routage les itinéraires correspondants seront importés : **unicast**, **multicast** ou **les deux**. Pour une **Règle d'importation**, indiquez à partir de quelle table de routage les itinéraires correspondants seront importés : **unicast**, **multicast** ou **les deux**.
Préfixe d'adresse		Indiquez des adresses IP ou des préfixes pour le filtrage des itinéraires.
Saut suivant		Indiquez les routeurs ou les sous-réseaux du saut suivant pour le filtrage des itinéraires
De l'homologue		Indiquez les routeurs d'homologues pour le filtrage des itinéraires
Action	**BGP** > **Importer ou exporter** > **Action**	Indiquez une action (**Autoriser** ou **Refuser**) à prendre lorsque des conditions de correspondance sont respectées.

Paramètres d'Importation et d'Exportation B	Configuré dans	Description
Atténuation		Indiquez un paramètre d'atténuation, uniquement si l'action est **Autoriser**.
Préférence locale		Indiquez une mesure de préférence locale, uniquement si l'action est **Autoriser**.
Moyen		Indiquez une valeur MED, uniquement si l'action est **Allow (Autoriser)** (0 à 65 535).
Poids		Indiquez une valeur de pondération, uniquement si l'action est **Autoriser** (0 à 65 535).
Saut suivant		Indiquez un routeur de saut suivant, uniquement si l'action est **Autoriser**.
Origine		Indiquez le type de chemin de l'itinéraire d'origine : IGP, EGP ou incomplet, uniquement si l'action affiche **Autoriser**.
Limite du chemin AS		Indiquez une limite du chemin AS uniquement si l'action est **Autoriser**.
Chemin AS		Indiquez un chemin AS : **Aucun**, **Supprime)**, **Ajouter**, **Supprimer et ajouter**, uniquement si l'action affiche **Autoriser**.
Communauté		Indiquez une option de communauté : **Aucun**, **Supprimer tout**, **Supprimer Regex**, **Ajouter** ou **Écraser**, uniquement si l'action affiche **Autoriser**.
Communauté étendue		Indiquez une option de communauté : **Aucun**, **Supprimer tout**, **Supprimer Regex**, **Ajouter** ou **Écraser**, uniquement si l'action affiche **Autoriser**.
		Vous devez **Supprimer** ⊖ les règles lorsque vous n'en avez plus besoin ou **Dupliquer** une règle, le cas échéant. Vous pouvez également sélectionner des règles et **Déplacer en haut** ou **Déplacer en bas** pour modifier leur ordre.

Onglet Avancé Publication conditionnelle BGP

- Réseau > Routeur virtuel > BGP > Publication conditionnelle

Une publication conditionnelle BGP vous permet de contrôler l'itinéraire à publier au cas où un itinéraire préféré ne serait pas disponible dans la table de routage BGP local (LocRIB) et indiquerait un échec de partage de réseau ou d'accessibilité. Ceci est utile dans les cas où vous souhaitez forcer des itinéraires vers un AS en direction d'un autre. Par exemple, lorsque vous disposez de liaisons vers Internet passant par plusieurs ISP et que vous voulez que le trafic soit acheminé vers un fournisseur à la place d'un autre, sauf s'il y a une perte de connectivité avec le fournisseur préféré.

Pour la publication conditionnelle, vous configurez un filtre Inexistant qui indique les itinéraires préférés (**Préfixe d'adresse**) plus tous les autres attributs qui identifient l'itinéraire préféré (comme l'Expression régulière du chemin AS). Si n'importe quel itinéraire correspondant à un filtre Inexistant est introuvable dans la table de routage BGP local, alors ce n'est qu'à ce moment-là que le pare-feu autorisera la publication de l'itinéraire alternatif (l'itinéraire vers l'autre fournisseur non préféré) comme indiqué dans son filtre de Publication.

Pour configurer la publication conditionnelle, sélectionnez l'onglet **Publication conditionnelle**, **Ajouter** une publication conditionnelle et configurez les valeurs décrites dans le tableau suivant.

Paramètres de publication conditionnelle B	Configuré dans	Description
Politique	**BGP** > **Publication conditionnelle**	Indiquez un nom pour cette règle de politique de publication conditionnelle.
Activer		Sélectionnez cette option pour activer cette règle de politique de publication conditionnelle.
Utilisé par		Cliquez sur **Ajouter** les groupes d'homologues qui vont utiliser cette règle de politique de publication conditionnelle.
Filtre inexistant	**BGP** > **Publication conditionnelle** > **Filtres inexistants**	Cet onglet permet de définir le(s) préfixe(s) de l'itinéraire préféré. Ceci indique l'itinéraire que vous voulez publier, s'il est disponible dans la table de routage BGP local. (Si la publication d'un préfixe est prévue et qu'il correspond à un filtre Inexistant, la publication sera supprimée.) Vous devez **Ajouter** un Filtre inexistant et indiquer un nom pour identifier celui-ci.
Activer		Sélectionnez cette option pour activer le filtre Inexistant.
Expression régulière du chemin AS		Indiquez une expression régulière pour le filtrage des chemins AS.
Expression régulière de la communauté		Indiquez une expression régulière pour le filtrage des chaînes de la communauté.

Paramètres de publication conditionnelle B	Configuré dans	Description
Expression régulière de la communauté étendue		Indiquez une expression régulière pour le filtrage des chaînes de la communauté étendue.
Moyen		Indiquez une valeur MED pour le filtrage des itinéraires (la plage est de 0 à 4 294 967 295).
Table d'itinéraires		Indiquez la table de routage (**unicast**, **multicast**, ou **les deux**) que le pare-feu recherche pour voir s'il existe un itinéraire correspondant. C'est seulement si l'itinéraire correspondant n'existe pas dans cette table de routage que le pare-feu autorise la publication d'un autre itinéraire.
Préfixe d'adresse		Il vous faut **Ajouter** le préfixe (NLRI, informations d'accessibilité à la couche réseau) exact pour le ou les itinéraires préférés.
Saut suivant		Indiquez les routeurs ou les sous-réseaux du saut suivant pour filtrer l'itinéraire.
De l'homologue		Indiquez les routeurs d'homologues pour le filtrage des itinéraires.
Filtre de publication	**BGP** > **Publication conditionnelle** > **Filtres de publicité**	Utilisez cet onglet pour définir le(s) préfixe(s) de l'itinéraire dans la table de routage RIB locale à publier au cas où l'itinéraire du filtre Inexistant serait indisponible dans la table de routage local. Si la publication d'un préfixe doit être effectuée et qu'il ne correspond pas à un filtre Inexistant, la publication aura lieu. Vous devez **Ajouter** un filtre de publication et indiquer un nom pour identifier celui-ci.
Activer		Sélectionnez pour activer le filtre.
Expression régulière du chemin AS		Indiquez une expression régulière pour le filtrage des chemins AS.
Expression régulière de la communauté		Indiquez une expression régulière pour le filtrage des chaînes de la communauté.
Expression régulière de la		Indiquez une expression régulière pour le filtrage des chaînes de la communauté étendue.

Paramètres de publication conditionnelle B	Configuré dans	Description
communauté étendue		
Moyen		Indiquez une valeur MED pour le filtrage des itinéraires (la plage est de 0 à 4 294 967 295).
Table d'itinéraires		Indiquez la table de routage utilisée par le pare-feu lorsqu'un itinéraire correspondant doit être publié de façon conditionnelle : **unicast**, **multicast** ou **les deux**.
Préfixe d'adresse		Cliquez sur **Ajouter** le préfixe (NLRI, informations d'accessibilité à la couche réseau) exact de l'itinéraire à publier si l'itinéraire préféré est indisponible.
Saut suivant		Indiquez les routeurs ou les sous-réseaux du saut suivant pour le filtrage des itinéraires.
De l'homologue		Indiquez les routeurs d'homologues pour le filtrage des itinéraires.

Onglet Agrégation BGP

- Réseau > Routeur virtuel > BGP > Agrégation

L'agrégation d'itinéraires consiste à combiner des itinéraires spécifiques (ceux avec une longueur de préfixe plus longue) en un seul itinéraire (avec une longueur de préfixe plus courte) pour réduire les publications d'itinéraires que le pare-feu doit envoyer et avoir moins d'itinéraires dans la table de routage.

Paramètres d'agrégation BG	Configuré dans	Description
Nom	**BGP** > **Agréger**	Saisissez un nom pour la règle d'agrégation.
Préfixe		Saisissez un préfixe récapitulatif (adresse IP / longueur de préfixe) qui sera utilisé pour agréger les préfixes plus longs.
Activer		Sélectionnez cette option pour activer cette agrégation d'itinéraires.
Résumé		Sélectionnez cette option pour récapituler les itinéraires.
Définition AS		Sélectionnez cette option pour que le pare-feu, pour cette règle d'agrégation, inclue l'ensemble des numéros AS (ensemble AS) dans le chemin AS de l'itinéraire agrégé. L'ensemble AS est la

Paramètres d’agrégation BG	Configuré dans	Description
		liste non triée des numéros AS d’origine provenant des itinéraires individuels qui sont agrégés.
Nom	**BGP** > **Agréger** > **Supprimer les filtres**	Définissez les attributs qui entraîneront la suppression des itinéraires correspondants. Cliquez sur **Ajouter** et saisissez un nom pour un Filtre de suppression.
Activer		Sélectionnez cette option pour activer les Filtres de suppression.
Expression régulière du chemin AS		Indiquez une expression régulière pour que l’attribut AS_PATH filtre les itinéraires qui seront agrégés, par exemple, ^5000 suppose les itinéraires tirés de l’AS 5000.
Expression régulière de la communauté		Indiquez une expression régulière pour que les communautés filtrent les itinéraires qui seront agrégés, par exemple, 500:.* correspond aux communautés avec 500:x.
Expression régulière de la communauté étendue		Indiquez une expression régulière pour les communautés étendues afin de filtrer les itinéraires qui seront agrégés.
Moyen		Indiquez le MED qui filtre les itinéraires qui seront agrégés.
Table d'itinéraires		Indiquez la table de routage à utiliser pour les itinéraires agrégés qui doivent être supprimés (non publiés) : **unicast**, **multicast** ou **les deux**.
Préfixe d'adresse		Saisissez l’adresse IP que vous souhaitez supprimer de la publication.
Saut suivant		Saisissez l’adresse du saut suivant du préfixe BGP que vous souhaitez supprimer.
De l'homologue		Saisissez l’adresse IP de l’homologue duquel le préfixe BGP (que vous souhaitez supprimer) a été reçu.
Nom	**BGP** > **Agréger** > **Filtres de publicité**	Définissez les attributs d’un filtre de publication qui amène le pare-feu à annoncer aux homologues tout itinéraire qui correspond au filtre. Cliquez sur **Ajouter** et saisissez un nom pour le Filtre de publication.
Activer		Sélectionnez cette option pour activer ce Filtre de publication.

Paramètres d’agrégation BG	Configuré dans	Description
Expression régulière du chemin AS		Indiquez une expression régulière pour que AS_PATH filtre les itinéraires qui seront publiés.
Expression régulière de la communauté		Indiquez une expression régulière pour que la Communauté filtre les itinéraires qui seront publiés.
Expression régulière de la communauté étendue		Indiquez une expression régulière pour que la communauté étendue filtre les itinéraires qui seront publiés.
Moyen		Indiquez une valeur MED pour filtrer les itinéraires qui seront publiés.
Table d'itinéraires		Indiquez la table de routage à utiliser pour un filtre de publication des itinéraires agrégés : **unicast**, **multicast** ou **les deux**.
Préfixe d'adresse		Saisissez une adresse IP que vous souhaitez que BGP publie.
Saut suivant		Saisissez l’adresse du Saut suivant de l’adresse IP que vous souhaitez que BGP publie.
De l'homologue		Saisissez l’adresse IP de l’homologue duquel le préfixe a été reçu et que vous souhaitez que BGP publie.
	BGP > **Agréger** > **Attributs d’itinéraire agrégés**	Définissez les attributs de l’itinéraire agrégé.
Préférence locale		Préférence locale dans la plage 0 à 4 294 967 295.
Moyen		Discriminateur de sorties multiples dans la plage 0 à 4 294 967 295.
Poids		Poids dans la plage 0 à 65 535.
Saut suivant		Adresse IP du saut suivant.
Origine		Origine de l’itinéraire : **igp**, **egp** ou **incomplet**.
Limite du chemin AS		Limite du chemin AS dans la plage 1 à 255.
Chemin AS		Sélectionnez le type : **Aucun** ou **Ajouter**.

Paramètres d’agrégation BG	Configuré dans	Description
Communauté		Sélectionnez le type : **Aucun**, **Supprimer tout**, **Supprimer Regex**, **Ajouter** ou **Écraser**.
Communauté étendue		Sélectionnez le type : **Aucun**, **Supprimer tout**, **Supprimer Regex**, **Ajouter** ou **Écraser**.

Onglet Règles de redistribution BGP

- Réseau > Routeur virtuel > BGP > Règles de redistribution

Configuration des paramètres décrits dans le tableau suivant pour créer des règles pour la redistribution des itinéraires BGP.

Paramètres des règles de redistribution B	Configuré dans	Description
Autoriser la redistribution des itinéraires par défaut	**BGP** > **Règles de redistribution**	Autorise le pare-feu à redistribuer son itinéraire par défaut vers des homologues BGP.
Nom		Vous devez **Ajouter** un sous-réseau IP ou d’abord créer une règle de redistribution.
Activer		Sélectionnez cette option pour activer cette règle de redistribution.
Table d'itinéraires		Indiquez la table de routage sur laquelle l’itinéraire sera redistribué : **unicast**, **multicast** ou **les deux**.
Mesure		Saisissez une mesure dans la plage comprise entre 1 et 65 535.
Définir l'origine		Sélectionnez l’origine de l’itinéraire redistribué (**igp**, **egp** ou **incomplet**). La valeur « **incomplet** » indique un itinéraire connecté.
Définir MED		Saisissez un MED pour l’itinéraire redistribué dans la plage comprise entre 0 et 4, 294, 967, 295.
Définir les préférences locales		Saisissez une préférence locale pour l’itinéraire redistribué dans la plage comprise entre 0 et 4, 294, 967, 295.
Définir la limite de		Saisissez une limite du chemin AS pour l’itinéraire redistribué dans la plage comprise entre 1 et 255.

Paramètres des règles de redistribution B	Configuré dans	Description
chemin de l'AS		
Définir la communauté		Sélectionnez ou saisissez une valeur 32 bits au format décimal, hexadécimal ou AS:VAL ; AS et VAL sont tous deux dans la plage de 0 à 65 535. Saisissez un maximum de 10 communautés.
Définir une communauté élargie		Saisissez une valeur de 64 bits au format hexadécimal ou au format TYPE:AS:VAL ou TYPE:IP:VAL. TYPE est de 16 bits, AS ou IP sont de 16 bits et VAL est de 32 bits. Saisissez un maximum de cinq communautés étendues.

Multidiffusion IP

- Réseau > Routeur virtuel > Multicast

La définition des protocoles multicast nécessite la configuration du paramètre standard suivant :

Paramètre multicast	Description
Activer	Sélectionnez pour activer le routage multicast.

Les paramètres des onglets suivants doivent également être configurés'A0;:

- **Rendezvous Point (Point de rendez-vous)** : Voir l'Onglet Point de rendez-vous de Multicast.
- **Interfaces** : Voir Onglet Interfaces multicast.
- **SPT Threshold (Seuil SPT)** : Voir l'Onglet Seuil SPT de Multicast.
- **Source Specific Address Space (Espace d'adresses spécifique à la source)** : Voir l'Onglet Espace d'adresses spécifiques à la source de Multicast.
- **Advanced (Avancé)** : Voir Onglet avancé multicast.

Onglet Point de rendez-vous multicast

- Réseau > Routeur virtuel > Multicast > Point de rendez-vous

Utilisez les champs suivants pour configurer un point de rendez-vous IP multicast :

Paramètres multicast – Point de rendez-vous	Description
Type RP	Sélectionnez le type de point de rendez-vous (RP) qui va s'exécuter sur ce routeur virtuel. Un RP statique doit être explicitement configuré sur d'autres routeurs PIM, alors qu'un RP candidat est automatiquement élu.

Paramètres multicast – Point de rendez-vous	Description
	• **None (Aucun)** - Indiquez si aucun RP n'est en cours d'exécution sur ce routeur virtuel. • **Static (Statique)** - Indiquez une adresse IP statique pour le RP et sélectionnez des options pour **RP Interface (Interface du RP)** et **RP Address (Adresse du RP)** dans la liste déroulante. Sélectionnez **Override learned RP for the same group (Appliquer un contrôle prioritaire RP appris pour le même groupe)** si vous voulez utiliser le RP défini au lieu du RP élu pour ce groupe. • **Candidate (Candidat)** - Indiquez les informations suivantes pour le RP candidat en cours d'exécution sur ce routeur virtuel : • **RP Interface (Interface du RP)** - Sélectionnez une interface pour le RP. Les types d'interfaces valides incluent une interface en boucle, C3, VLAN, Ethernet agrégée et de tunnel. • **RP Address (Adresse du RP)** - Sélectionnez une adresse IP pour le RP. • **Priority (Priorité)** - Indiquez une priorité pour les messages RP candidats (valeur par défaut : 192). • **Advertisement interval (Intervalle de publication)** - Indiquez un intervalle entre les publications de messages RP candidats. • **Group list (Liste de groupes)** - Si vous sélectionnez **Static (Statique)** ou **Candidate (Candidat)**, cliquez sur **Add (Ajouter)** pour spécifier une liste de groupes pour lesquels ce RP candidat propose d'être le RP.
Rendez-vous Point distant	Cliquez sur **Add (Ajouter)** et indiquez les éléments suivants : • **IP address (Adresse IP)** - Indiquez une adresse IP pour le RP. • **Override learned RP for the same group (Écraser le RP appris pour le même groupe)** - Sélectionnez pour utiliser le RP défini au lieu du RP élu pour ce groupe. • **Group (Groupe)** - Indiquez une liste de groupes pour lesquels l'adresse spécifiée va servir de RP.

Onglet Interfaces multicast

- Réseau > Routeur virtuel > Multicast > Interfaces

Utilisez les champs suivants pour configurer les interfaces multicast qui partagent les paramètres IGMP, PIM et d'autorisation du groupe :

Paramètres multicast – Interfaces	Description
Name (Nom)	Saisissez un nom pour identifier un groupe d'interfaces.

Paramètres multicast – Interfaces	Description
Description	Saisissez une description (facultatif).
Interface	**Add (Ajoutez)** une ou plusieurs interfaces de pare-feu qui appartiennent au groupe d'interfaces et, par conséquence, qui partagent les paramètres d'autorisation du groupe, les paramètres IGMP et les paramètres PIM.
Autorisations du groupe	Précisez les groupes multicast qui participent à PIM Any-Source Multicast (n'importe quelle source multicast ; ASM) ou à PIM Source-Specific Multicast (multicast spécifique à la source ; SSM) : • **Any Source (N'importe quelle source)** : **Add (Ajoutez)** un **Name (Nom)** pour identifier un **Group (Groupe)** multicast autorisé à recevoir du trafic multicast de n'importe quelle source qui se trouve sur les interfaces faisant partie du groupe d'interfaces. Le groupe est **Included (Inclus)** par défaut dans la liste **Any Source (N'importe quelle source)**. Désélectionnez **Included (Inclus)** pour facilement exclure un groupe sans en supprimer la configuration. • **Source Specific (Spécifique à la source)** : **Add (Ajoutez)** un **Name (Nom)** pour un **Group (Groupe)** multicast et une paire d'adresses IP **Source** pour laquelle le trafic multicast est autorisé sur les interfaces faisant partie du groupe d'interfaces. Le Groupe et la Paire source sont **Included (Inclus)** par défaut dans la liste Source Specific (Spécifique à la source). Désélectionnez **Included(Inclus)** pour facilement exclure un groupe et une paire Source sans en supprimer la configuration.
IGMP	Indiquez les paramètres du trafic IGMP. IGMP doit être activé pour les interfaces orientées vers le récepteur multicast. • **Enable (Activer)** - Sélectionnez pour activer la configuration IGMP. • **IGMP Version (Version IGMP)** - Sélectionnez la version 1, 2 ou 3 à exécuter sur l'interface. • **Enforce Router-Alert IP Option (Appliquer l'option IP d'alerte du routeur)** - Sélectionnez pour exiger l'utilisation de l'option IP d'alerte du routeur avec IGMPv2 ou IGMPv3. Cette option doit être désactivée pour être compatible avec IGMPv1. • **Robustness (Robustesse)** - Sélectionnez un entier pour indiquer la perte de paquets sur un réseau (intervalle compris entre 1 et 7, valeur par défaut : 2). Si la perte de paquets est chose courante, sélectionnez une valeur supérieure. • **Max Sources (Sources max.)** - Indiquez le nombre maximum d'appartenances propres à la source autorisées sur ce groupe d'interfaces (intervalle compris entre 1 et 65 535 ou **unlimited (illimitées)**). • **Max Groups (Groupes max.)** - Indiquez le nombre maximum de groupes multicast autorisées sur ce groupe d'interfaces (intervalle compris entre 1 et 65 535 ou **unlimited (illimités)**).

Paramètres multicast – Interfaces	Description
	• **Query Configuration (Configuration d'une requête)** - Spécifiez les options suivantes : • **Query Interval (Intervalle de requête)** - Indiquez l'intervalle au cours duquel des requêtes générales sont envoyées à tous les récepteurs. • **Max Query Response Time (Délai max. de réponse aux requêtes)** - Indiquez le délai maximum écoulé entre une requête générale et la réponse d'un récepteur. • **Last Member Query Interval (Dernier intervalle de requête d'un membre)** - Indiquez l'intervalle entre les messages de requête d'un groupe ou spécifiques à la source (y compris ceux envoyés en réponse à des messages d'abandon de groupe). • **Immediate Leave (Quitter immédiatement)** - Sélectionnez pour quitter le groupe immédiatement lors de la réception d'un message d'abandon.
Configuration PIM	Définissez les paramètres Protocol Independent Multicast (protocole de routage multicast ; PIM) : • **Enable (Activer)** - Sélectionnez pour autoriser cette interface à recevoir et/ou à transférer des messages PIM. Vous devez procéder à l'activation pour qu'une interface transfère le trafic multicast. • **Assert Interval (Intervalle d'affirmation)** - Indiquez l'intervalle entre les messages d'affirmation PIM pour choisir un transmetteur PIM. • **Hello Interval (Intervalle Hello)** - Indiquez l'intervalle entre les messages Hello PIM. • **Join Prune Interval (Intervalle Join/Prune)** - Indiquez le nombre de secondes entre les messages de jointure (Join) PIM (et entre les messages d'élagage (Prune) PIM). La valeur par défaut est 60. • **DR Priority (Priorité du DR)** - Indiquez la priorité du routeur désigné pour cette interface. • **BSR Border (Bordure BSR)** - Sélectionnez pour utiliser l'interface en tant que bordure bootstrap. • **PIM Neighbors (Voisins PIM)** - **Add (Ajoutez)** la liste de voisins qui vont communiquer entre eux à l'aide de PIM.

Onglet Seuil SPT multicast

- Réseau > Routeur virtuel > Multicast > Seuil SPT

Le seuil Shortest Path Tree (arbre du chemin le plus court ; SPT) définit le moment où le routeur virtuel fait basculer le routage multicast d'un préfixe ou d'un groupe multicast d'une distribution en arborescence partagée (issue du point de rendez-vous) à une distribution en arborescence source également connue sous

le nom de Shortest Path Tree (arbre du chemin le plus court ; SPT). **Add (Ajoutez)** un seuil SPT à un préfixe ou un groupe multicast.

Seuil SPT	Description
Préfixe/groupe multicast	Indiquez le préfixe ou le groupe multicast pour lequel le routage multicast bascule à une distribution SPT lorsque le débit vers le groupe ou le préfixe atteint le seuil défini.
Seuil (en Kbit/s)	Sélectionnez un paramètre pour définir le moment où le routage multicast bascule à une distribution SPT pour le préfixe ou le groupe multicast correspondant : • **0 (commuter au premier paquet de données)** : (par défaut) Lorsqu'un paquet multicast destiné au groupe ou au préfixe arrive, le routeur virtuel fait basculer le routage à une distribution SPT. • **jamais (ne pas basculer vers SPT)** : le routeur virtuel continue de transférer le trafic multicast à ce groupe ou à ce préfixe via l'arbre partagé. • Saisissez le nombre total de kilobits provenant des paquets multicast qui peuvent arriver pour le préfixe ou le groupe multicast correspondant à toute interface sur une période de temps déterminée (plage comprise entre 1 et 4 294 967 295). Lorsque le débit atteint ce chiffre, le routeur virtuel passe à la distribution SPT.

Onglet Espace d'adresses spécifique à la source multicast

- Réseau > Routeur virtuel > Multicast > Espace d'adresses spécifique à la source

Add (Ajoutez) les groupes multicast qui peuvent recevoir des paquets multicast d'une source donnée uniquement. Il s'agit des mêmes noms et groupes multicast que vous avez indiqués comme Spécifique à la source à l'onglet **Multicast** > **Interfaces** > **Group Permissions (Permissions du groupe)**.

Paramètres multicast – Espace d'adresses spécifique à la source	Description
Name (Nom)	Identifiez un groupe multicast auquel le pare-feu va fournir des services Source-Specific Multicast (multicast spécifique à la source ; SSM).
Group (Groupe)	Définissez une adresse de groupe multicast qui peut accepter les paquets multicast d'une source donnée uniquement.
inclus(e)	Sélectionnez cette option pour inclure les groupes multicast dans l'espace d'adresses SSM.

Onglet Avancé multicast

- Réseau > Routeur virtuel > Multicast > Avancé

Configurez la durée pendant laquelle un itinéraire de multidiffusion reste dans la table de routage après la fin de la session.

Paramètres avancés multicast	Description
Paramètres d'expiration de l'itinéraire (sec)	Vous permet d'ajuster le délai, en secondes, pendant lequel une route multidiffusion demeure dans la table de routage sur le pare-feu à la fin de la session (intervalle compris entre 210 et 2 700 ; valeur par défaut : 210).

ECMP

- Réseau > Routeur virtuel > Paramètres de routeur > ECMP

Le traitement ECMP (Equal Cost Multiple Path/chemin multiple à coût égal) est une fonction réseau qui permet au pare-feu d'utiliser jusqu'à quatre itinéraires de coût égal vers la même destination. Sans cette fonction, s'il existe plusieurs itinéraires de coût égal vers la même destination, le routeur virtuel choisit l'un de ces itinéraires dans la table de routage et l'ajoute à sa table de transfert ; il n'utilise aucun autre itinéraire à moins qu'il n'y ait une interruption dans l'itinéraire choisi. L'activation de la fonctionnalité ECMP sur un routeur virtuel permet au pare-feu d'avoir jusqu'à quatre chemins de coût égal vers une destination dans sa table de transfert, grâce auxquels il peut :

- Équilibrer la charge des flux (sessions) vers la même destination sur plusieurs liaisons de coût égal.
- Utiliser la bande passante disponible sur toutes les liaisons vers la même destination plutôt que de laisser certains liens inutilisés.
- Déplacer le trafic de façon dynamique d’un autre membre ECMP vers la même destination en cas de défaillance d’une liaison, au lieu d’attendre que le protocole de routage ou la table RIB choisisse un autre chemin, ce qui peut aider à réduire le délai d’inactivité en cas de défaillance de la liaison.

L'équilibrage de la charge ECMP est effectué au niveau de la session et non au niveau du paquet. Le pare-feu choisit ainsi un chemin de coût égal au début d’une nouvelle session et non à chaque fois que le pare-feu reçoit un paquet.

L'activation, la désactivation ou la modification d'un routeur virtuel existant entraîne son redémarrage par le pare-feu, ce qui peut mettre fin aux sessions existantes.

Afin de configurer ECMP pour un routeur virtuel, sélectionnez un routeur virtuel et, dans **Paramètres de routeur**, cliquez sur l’onglet **ECMP** et configurez les Paramètres ECMP suivants :

Que voulez-vous faire ?	Reportez-vous à la section :
Quels sont les champs disponibles pour configurer ECMP ?	Paramètres ECMP

Que voulez-vous faire ?	Reportez-vous à la section :
Vous souhaitez en savoir plus ?	ECMP

Paramètres ECMP

- Réseau > Routeur virtuel > Paramètres de routeur > ECMP

Utilisez les champs suivants pour configurer les paramètres de chemin multiple à coût égal (ECPM).

Paramètres ECMP	Description
Activer	**Activez** ECMP. *L'activation, la désactivation ou la modification d'un routeur virtuel existant entraîne son redémarrage par le pare-feu, ce qui a parfois pour conséquence de mettre fin aux sessions existantes.*
Retour symétrique	(Facultatif) Sélectionnez l'option **Symmetric Return (Retour symétrique)** pour que les paquets de retour sortent de la même interface que celle sur laquelle les paquets d'entrée associés sont arrivés. Cela configure le pare-feu pour qu'il utilise l'interface d'entrée lorsqu'il envoie des paquets de retour, au lieu de l'interface ECMP, ce qui signifie que le paramètre **Symmetric Return (Retour symétrique)** applique un contrôle prioritaire sur l'équilibrage de la charge. Ce comportement se produit uniquement pour les flux de trafic du serveur au client.
Chemin strict d'accès source	Par défaut, le trafic IKE et IPSec en provenance du pare-feu sort d'une interface que la méthode d'équilibrage de charge ECMP détermine. Sélectionnez **Strict Source Path (Chemin d'accès source strict)** pour vous assurer que le trafic IKE et IPSec en provenance du pare-feu sort toujours de l'interface physique à laquelle appartient l'adresse IP source du tunnel IPSec. Activez le Chemin d'accès source strict lorsque le pare-feu a plus d'un ISP qui offre des chemins d'accès à coût égal vers la même destination. Les ISP effectuent généralement une vérification de Transfert de chemin d'accès inversé (RPF) (ou une vérification différente afin d'empêcher l'usurpation d'adresse IP) pour confirmer que le trafic sort de la même interface que celle sur laquelle il est arrivé. Parce que le traitement ECMP par défaut choisit une interface de sortie sur la base de la méthode ECMP configurée (au lieu de choisir l'interface source comme interface de sortie), ce n'est pas ce à quoi l'ISP s'attend et l'ISP peut bloquer le trafic de retour légitime. Dans ce cas d'utilisation, activez le **Strict Source Path (chemin d'accès strict)** afin que le pare-feu utilise l'interface de sortie correspondant à l'interface à laquelle appartient l'adresse IP source du tunnel IPSec.

Paramètres ECMP	Description
Nombre max. de chemins	Sélectionnez le nombre maximum de chemins de coût égal : (2, 3 ou 4) vers un réseau de destination qui peut être copié de la RIB à la FIB (par défaut, la valeur est 2).
Méthode	Choisissez l'un des algorithmes d'équilibrage de la charge ECMP suivants à utiliser sur le routeur virtuel. L'équilibrage de la charge ECMP est effectué au niveau de la session et non au niveau du paquet. Le pare-feu (ECMP) choisit ainsi un chemin de coût égal au début d'une nouvelle session et non à chaque fois qu'un paquet est reçu. • **IP Modulo (Modulo IP)** (par défaut) : le routeur virtuel équilibre la charge des sessions en utilisant un hachage des adresses IP source et de destination dans l'en-tête des paquets pour déterminer l'itinéraire ECMP à utiliser. • **IP Hash (Hachage IP)** : il existe deux méthodes de hachage IP qui déterminent quel itinéraire ECMP il convient d'utiliser : • Si vous sélectionnez **IP Hash (Hachage IP)**, par défaut, le pare-feu utilise un hachage des adresses IP source et de destination. • Si vous **Use Source Address Only (Utilisez l'adresse source uniquement)** (disponible dans PAN-OS 8.0.3 et dans les versions ultérieures), le pare-feu s'assure que toutes les sessions appartenant à la même adresse IP prennent toujours le même chemin. • Si vous **Use Source/Destination Ports (Utilisez les ports source/de destination)** également, le pare-feu inclut les ports dans l'un ou l'autre des calculs du hachage. Vous pouvez également saisir une **Hash Seed (Valeur initiale de hachage)** (un nombre entier) pour randomiser l'équilibrage de la charge. • **Weighted Round Robin (Pondération comparative)** - Vous pouvez utiliser cet algorithme pour prendre en compte les différentes capacités et vitesses de liaison. Lorsque vous choisissez cet algorithme, la fenêtre de dialogue de l'Interface s'ouvre. **Add (Ajoutez)** et sélectionnez une **Interface** à inclure dans le groupe Pondération comparative. Pour chaque interface, saisissez la valeur **Weight (Pondération)** à utiliser pour cette interface (plage de 1 à 255 ; par défaut la valeur est 100) Plus la valeur de pondération d'un chemin de coût égal spécifique est élevée, plus ce chemin est sélectionné pour une nouvelle session. Une liaison plus rapide doit avoir une pondération supérieure à une liaison plus lente, de manière à ce que le trafic ECMP passe par la liaison plus rapide. Vous pouvez ensuite **Add (Ajouter)** une autre interface et une autre pondération. • **Balanced Round Robin (Équilibrage comparatif)** - Distribue les sessions ECMP entrantes de manière égale entre les liaisons.

Statistiques d’exécution supplémentaires d’un routeur virtuel

Après avoir configuré des itinéraires statiques ou des protocoles de routage pour un routeur virtuel, sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et sélectionnez **More Runtime Stats (Statistiques d’exécution supplémentaires)** dans la dernière colonne pour afficher des informations détaillées sur le routeur virtuel, comme la table de routage, la table de transfert et les protocoles de routage et les itinéraires statiques que vous avez configurés. Ces fenêtres fournissent plus d’informations que ne peut en contenir un écran unique pour le routeur virtuel. La fenêtre affiche les onglets suivants :

- **Routing (Routage)** : voir Onglet Routage.
- **RIP** : voir Onglet RIP.
- **BGP** : voir Onglet BGP.
- **Multicast** : voir Onglet Multicast.
- **BFD Summary Information (Informations récapitulatives de BFP)** : voir Onglet Informations récapitulatives de BFD.

Onglet Routage

Le tableau suivant décrit les statistiques d’exécution du routeur virtuel pour la Table de routage, la Table de transfert, et la table de Surveillance des itinéraires statiques.

Statistiques d’exécution	Description
Table d'itinéraires	
Table d'itinéraires	Sélectionnez **Unicast** ou **Multicast** pour afficher la table de routage unicast ou multicast.
Afficher la famille d'adresses	Sélectionnez **IPv4 uniquement**, **IPv6 uniquement**, ou **IPv4 et IPv6** (par défaut) pour contrôler quel groupe d’adresses afficher dans le tableau.
Destination	Adresse IPv4 et masque réseau ou adresse IPv6 et longueur de préfixe des réseaux que le routeur virtuel peut atteindre.
Saut suivant	Adresse IP du périphérique au saut suivant vers le réseau de destination. Un saut suivant de 0.0.0.0 indique l'itinéraire par défaut.
Mesure	Mesure de l'itinéraire. Lorsqu’un protocole de routage comporte plus d’une route vers le même réseau de destination, il privilégie l’itinéraire avec la valeur métrique la plus basse. Chaque protocole de routage utilise un autre type de métrique, par exemple, RIP utilise le nombre de sauts.
Poids	Poids de l’itinéraire. Par exemple, lorsque BGP comporte plus d’un itinéraire vers la même destination, il préfèrera l’itinéraire avec le poids le plus élevé.
flags	• **A?B** – Actif et appris via BGP.

Statistiques d’exécution	Description
	• **A C** – Actif et résultat d’une interface interne (connectée) – Destination = réseau • **A H** – Actif et résultat d’une interface interne (connectée) – Destination = Hôte uniquement • **A R** – Actif et appris via RIP. • **A S** – Actif et statique. • **S** – Inactif (car cet itinéraire a une mesure supérieure) et statique • **O1**–OSPF externe de type 1 • **O2**–OSPF externe de type 2 • **Oi**–OSPF intra-zone • **Oo**–OSPF inter-zone
Age	Antériorité de l'entrée d'itinéraire dans la table de routage. Les itinéraires statiques n'ont aucune antériorité.
Interface	L’interface de sortie du routeur virtuel qui sera utilisée pour atteindre le saut suivant.
Actualiser	Cliquez pour actualiser les statistiques d’exécution dans le tableau.

Table de transfert

Le pare-feu choisit le meilleur itinéraire (de la table de routage (RIB) vers un réseau de destination) à placer dans la FIB.

Afficher la famille d'adresses	Sélectionnez **IPv4 uniquement**, **IPv6 uniquement**, ou **IPv4 et IPv6** (par défaut) pour contrôler la table de routage à afficher.
Destination	Meilleure adresse IPv4 et masque réseau ou adresse IPv6 et longueur de préfixe des réseaux que le routeur virtuel peut atteindre, sélectionné depuis la Table de routage.
Saut suivant	Adresse IP du périphérique au saut suivant vers le réseau de destination. Un saut suivant de 0.0.0.0 indique l'itinéraire par défaut.
flags	• **u** – L’itinéraire se dirige vers le haut. • **h** – L’itinéraire dirige vers un hôte. • **g** – L’itinéraire dirige vers une passerelle. • **e** – Le pare-feu a sélectionné cet itinéraire en utilisant le Chemin multiple à coût égal (ECMP). • ***** – L’itinéraire est le chemin privilégié vers un réseau de destination.

Statistiques d’exécution	Description
Interface	Interface de sortie du routeur virtuel qui sera utilisé pour atteindre le saut suivant.
MTU	Unité de transmission maximale (MTU) ; le nombre maximum d’octets que le pare-feu transmettra dans un seul paquet TCP vers cette destination.
Actualiser	Cliquez pour actualiser les statistiques d’exécution dans le tableau.
Surveillance des itinéraires statiques	
Destination	Adresse IPv4 et masque réseau ou adresse IPv6 et longueur de préfixe d’un réseau que le routeur virtuel peut atteindre.
Saut suivant	Adresse IP du périphérique au saut suivant vers le réseau de destination. Un saut suivant de 0.0.0.0 indique l'itinéraire par défaut.
Mesure	Mesure de l'itinéraire. Lorsqu’il y a plus d’un itinéraire statique sur le même réseau de destination, le pare-feu favorise l’itinéraire avec la valeur métrique la plus basse.
Poids	Poids de l’itinéraire.
flags	• **A?B** – Actif et appris via BGP. • **A C** – Actif et résultat d’une interface interne (connectée) – Destination = réseau • **A H** – Actif et résultat d’une interface interne (connectée) – Destination = Hôte uniquement • **A R** – Actif et appris via RIP. • **A S** – Actif et statique. • **S** – Inactif (car cet itinéraire a une mesure supérieure) et statique • **O1**–OSPF externe de type 1 • **O2**–OSPF externe de type 2 • **Oi**–OSPF intra-zone • **Oo**–OSPF inter-zone
Interface	L’interface de sortie du routeur virtuel qui sera utilisée pour atteindre le saut suivant.
Surveillance des chemins (échec)	Si la surveillance des chemins est activée pour cet itinéraire statique, l’Échec indique : • **Tout** – Le pare-feu considère l’itinéraire statique vers le bas et échoue si toutes les destinations surveillées pour l’itinéraire statique sont en panne.

Statistiques d’exécution	Description
	• **Un** – Le pare-feu considère l’itinéraire statique vers le bas et échoue si l’une des destinations surveillées pour l’itinéraire statique est en panne. Si la surveillance des chemins d’itinéraires statiques est désactivée, l’Échec indique **Désactivé**.
Status (État)	Le statut de l’itinéraire statique basé sur les requêtes pings ICMP vers les destinations surveillées : **Haut**, **Bas**, ou la surveillance des chemins pour l’itinéraire statique est **Désactivé**.
Actualiser	Actualise les statistiques d’exécution dans le tableau.

Onglet RIP

Le tableau suivant décrit les statistiques d'exécution RIP du routeur virtuel.

Statistiques d’exécution RIP	Description
Onglet Récapitulation	
Intervalle (en secondes)	Nombre de secondes dans un intervalle. RIP utilise cette valeur (une période de temps) pour contrôler ses intervalles de Mise à jour, d’Expiration et de Suppression.
Intervalles de mise à jour	Nombre d’intervalles entre les mises à jour de publication des itinéraires RIP que le routeur virtuel envoie aux homologues.
Intervalles d'expiration	Nombre d’intervalles depuis la dernière mise à jour du routeur virtuel reçue d’un homologue, après lequel le routeur virtuel marque les itinéraires de l’homologue comme inutilisables.
Intervalles de suppression	Nombre d’intervalles depuis le marquage d’un itinéraire comme inutilisable après lequel, si aucune mise à jour n’est reçue, le pare-feu supprime l’itinéraire de la table de routage.
Onglet Interface	
Adresse	Adresse IP d'une interface sur le routeur virtuel où RIP est activé.
Type d'authentification	Type d'authentification : mot de passe simple, MD5 ou aucun.
Envoi autorisé	Une coche indique que cette interface est autorisée à envoyer des paquets RIP.

Statistiques d’exécution RIP	Description
Réception autorisée	Une coche indique que cette interface est autorisée à recevoir des paquets RIP.
Publier la route par défaut	Une coche indique que RIP publiera son itinéraire par défaut sur ses homologues.
Mesure d'itinéraire par défaut	Mesure (nombre de sauts) affectée à l'itinéraire par défaut. Plus la valeur de mesure est faible, plus l'itinéraire a de chance dans la table de routage d'être sélectionné comme chemin préféré.
ID de la clé	Clé d'authentification utilisée par les homologues.
Préféré	Clé préférée pour l'authentification.
Onglet Homologue	
Adresse de l'homologue	Adresse IP d'un homologue sur l'interface RIP du routeur virtuel.
Dernière mise à jour	Date et heure auxquelles la dernière mise à jour a été reçue de cet homologue.
Version RIP	Version RIP exécutée par l'homologue.
Paquets non valides	Nombre de paquets non valides reçus de cet homologue. Raisons possibles pour lesquelles le pare-feu ne peut pas analyser le paquet RIP : x octets au-delà de la limite d'itinéraire, trop d'itinéraires dans un paquets, sous-réseau incorrect, adresse non conforme, échec de l'authentification ou mémoire insuffisante.
Itinéraires non valides	Nombre d'itinéraires non valides reçus de cet homologue. Causes possibles : itinéraire non valide, échec de l'importation ou mémoire insuffisante.

Onglet BGP

Le tableau suivant décrit les statistiques d'exécution BGP du routeur virtuel.

Statistiques d’exécution BGP	Description
Onglet Récapitulation	
ID de routeur	ID de routeur affecté à l'instance BGP.
Rejeter les itinéraires par défaut	Indique si l'option Rejeter l'itinéraire par défaut est configurée, qui permet au routeur virtuel d'ignorer les itinéraires par défaut publiés par les homologues BGP.

Statistiques d’exécution BGP	Description
Redistribuer l'itinéraire par défaut	Indique si l'option Autoriser la redistribution de l'itinéraire par défaut est configurée.
Installer un itinéraire	Indique si l'option Installer l'itinéraire est configurée, qui permet au routeur virtuel d'installer des itinéraires BGP dans la table de routage générale.
Redémarrage sans échec	Indique si l'option Redémarrage en douceur est activée (prise en charge).
Taille AS	Indique si le format AS sélectionné est de 2 ou 4 octets.
AS local	Numéro de l'AS auquel le routeur virtuel appartient.
AS membre local	Numéro de l'AS membre local (valide uniquement si le routeur virtuel se trouve dans une confédération). La valeur du champ est de 0 si le routeur virtuel n'est pas dans une confédération.
ID du cluster	Affiche l'ID du cluster de réflecteurs configuré.
Préférence locale par défaut	Affiche la préférence locale par défaut configurée pour le routeur virtuel.
Toujours comparer MED	Indique si l'option Toujours comparer MED est configurée, qui permet une comparaison afin de sélectionner un itinéraire parmi ceux des voisins dans différents systèmes autonomes.
Agréger sans tenir compte de MED	Indique si l'option Agréger MED est configurée, qui permet l'agrégation des itinéraires même lorsqu'ils ont différentes valeurs MED.
Traitement MED déterministe	Indique si l'option Comparaison MED déterministe est configurée, qui permet une comparaison afin de sélectionner un itinéraire parmi ceux qui sont publiés par des homologues IBGP (homologues BGP figurant dans le même AS).
Entrées RIB actives	Nombre d'entrées de la table RIB Out.
Pic des entrées RIB Out	Nombre maximal d'itinéraires Adj-RIB-Out qui ont été affectés à un moment donné.
Onglet Homologue	
Nom	Nom de l'homologue.
Groupe	Nom du groupe d'homologues auquel cet homologue appartient.

Statistiques d’exécution BGP	Description
IP locale	Adresse IP de l'interface BGP sur le routeur virtuel.
IP de l'homologue	Adresse IP de l'homologue.
AS Homologue	Système autonome auquel l'homologue appartient.
Mot de passe défini	Oui ou Non indique si l'authentification est définie.
État	État de l'homologue (par exemple, Actif, Connexion, Établie, Inactif, OpenConfirm ou OpenSent).
Durée de l'état (s)	Durée de l'état de l'homologue.
Onglet Groupe d'homologues	
Nom du groupe	Nom du groupe d'homologues.
Type	Type de groupe d'homologues configuré, tel que EBGP ou IBGP.
Agréger conféd. AS	Oui ou Non indique si l'option Agréger l'AS de la confédération est configurée.
Prise en charge de la réinitialisation logicielle	Oui ou Non indique si le groupe d'homologues prend en charge la réinitialisation logicielle. Lorsque les politiques de routage vers un homologue BGP sont modifiées, les mises à jour des tables de routage peuvent être affectées. Une réinitialisation logicielle est préférée plutôt qu'une réinitialisation matérielle, car elle permet la mise à jour des tables de routage sans effacer les sessions BGP.
Prochain Saut	Oui ou Non indique si cette option est configurée.
Saut suivant du tiers	Oui ou Non indique si cette option est configurée.
Supprimer l'AS privé	Indique si les numéros des AS privés seront supprimés de l'attribut AS_PATH dans les mises à jour avant leur envoi.
Onglet RIB locale	
Préfixe	Préfixe réseau et masque de sous-réseau dans la RIB locale.
Indicateur	* indique l'itinéraire choisi comme meilleur itinéraire BGP.
Saut suivant	Adresse IP du saut suivant vers le préfixe.
Homologue	Nom de l'homologue.

Statistiques d’exécution BGP	Description
Poids	Attribut de pondération affecté au préfixe. Si le pare-feu dispose de plusieurs itinéraires vers le même préfixe, l'itinéraire dont la valeur de pondération est la plus élevée est installé dans la table de routage IP.
Préf. locale	Attribut de préférence locale de l'itinéraire, qui est utilisé pour choisir le point de sortie vers le préfixe s'il existe plusieurs points de sortie. Une préférence locale élevée est préférée à une préférence locale faible.
Chemin AS	Liste des systèmes autonomes dans le chemin vers le réseau du préfixe ; la liste est publiée dans les mises à jour BGP.
Origine	Attribut d'origine du préfixe ; comment BGP a appris l'itinéraire.
MED	Attribut MED (discriminateur de sorties multiples) de l'itinéraire. Le MED est un attribut de mesure d'un itinéraire, que l'AS publiant l'itinéraire suggère à un AS externe. Un MED faible est préféré à un MED élevé.
Nombre de battements	Nombre de battements pour l'itinéraire.
Onglet RIB Out	
Préfixe	Entrée de routage réseau dans la RIB (Base d'informations de routage).
Saut suivant	Adresse IP du saut suivant vers le préfixe.
Homologue	Homologue sur lequel le routeur virtuel publiera cet itinéraire.
Préf. locale	Attribut de préférence locale pour accéder au préfixe, qui est utilisé pour choisir le point de sortie vers le préfixe s'il existe plusieurs points de sortie. Une préférence locale élevée est préférée à une préférence locale faible.
Chemin AS	Liste des systèmes autonomes dans le chemin vers le réseau du préfixe ; la liste est publiée dans les mises à jour BGP.
Origine	Attribut d'origine du préfixe ; comment BGP a appris l'itinéraire.
MED	Attribut MED (discriminateur de sorties multiples) vers le préfixe. Le MED est un attribut de mesure d’un itinéraire que l’AS publiant l’itinéraire suggère à un AS externe. Un MED faible est préféré à un MED élevé.
Adv. État	État de publication de l'itinéraire.
Aggr. État	Indique si cet itinéraire est agrégé avec d'autres itinéraires.

Onglet Multicast

Le tableau suivant décrit les statistiques d'exécution multicast IP du routeur virtuel.

Statistiques d’exécution multicast	Description
Onglet FIB	
Groupe	Entrée d'itinéraire dans la Forwarding Information Base (base d'informations de transfert ; FIB) ; adresse du groupe multicast à laquelle le routeur virtuel transfèrera les paquets.
Source	Adresse source des paquets multicast du groupe.
Interfaces trafic entrant	Interfaces où les paquets multicast du groupe arrivent.
Interfaces en cours	Interfaces desquelles le routeur virtuel transfère les paquets multicast du groupe.
Onglet Interface IGMP	
Interface	Interface sur laquelle IGMP est activé.
Version	Version 1, 2 ou 3 du protocole Internet Group Management Protocol (protocole de gestion de groupe Internet ; IGMP) exécutée sur le routeur virtuel.
Requérant	Adresse IP du requérant IGMP sur le segment multi-accès connecté à l’interface.
Délai d'activation du requérant	Nombre de secondes pendant lesquelles le requérant IGMP a été actif.
Délai d'expiration du requérant	Nombre de secondes restant avant l’expiration du minuteur Autre requérant présent.
Robustesse	Variable de robustesse de l'interface IGMP.
Limite de groupes	Nombre maximum de groupes par interface qu’IGMP peut traiter simultanément.
Limite de sources	Nombre maximum de sources par interface qu’IGMP peut traiter simultanément.
Quitter immédiatement	Oui ou Non indique si l'option Quitter immédiatement est configurée. Celle-ci permet au routeur virtuel de supprimer une interface de la table de transfert sans envoyer de requêtes spécifiques au groupe IGMP de l'interface.
Onglet Membres IGMP	

Statistiques d’exécution multicast	Description
Interface	Nom de l’interface qui appartient au groupe.
Group (Groupe)	Adresse du groupe multicast auquel l’interface appartient.
Source	Adresse IP de la source qui envoie les paquets multicast au groupe.
Délai d'activation	Nombre de secondes pendant lesquelles cette appartenance est active.
Délai d'expiration	Nombre de secondes avant l’expiration de l'appartenance.
Mode de filtrage	Inclusion ou exclusion de la source. Le routeur virtuel est configuré pour inclure l'ensemble du trafic ou uniquement le trafic de cette source (inclusion), ou bien le trafic de n'importe quelle source excepté celle-ci (exclusion).
Expiration de l'exclusion	Nombre de secondes avant l’expiration de l'état Exclure de l'interface.
Minuteur d'hôte V1	Temps restant avant que le routeur local suppose qu'il n'y a plus aucun membre IGMP Version 1 sur le sous-réseau IP associé à l'interface.
Minuteur d'hôte V2	Temps restant avant que le routeur local suppose qu'il n'y a plus aucun membre IGMP Version 2 sur le sous-réseau IP associé à l'interface.
Onglet Mappage de groupe PIM	
Groupe	Adresse IP du groupe mappé à un point de rendez-vous.
RP	Adresse IP du point de rendez-vous du groupe.
Origine	Indique si le routeur virtuel a appris le RP.
Mode PIM	ASM ou SSM.
Inactif	Indique si le mappage du groupe au RP est inactif.
Onglet Interface PIM	
Interface	Nom de l'interface participant à PIM.
Adresse	Adresse IP de l'interface.
DR	Adresse IP du routeur désigné sur le segment multi-accès connecté à l’interface.
Intervalle Hello	Intervalle Hello configurée (en secondes).

Statistiques d’exécution multicast	Description
Intervalle Join/ Prune	Intervalle configuré pour les messages Join et Prune (en secondes).
Intervalle d'affirmation	Intervalle configuré entre les messages d'affirmation PIM (en secondes) pour que le routeur virtuel envoie les messages d’affirmation. PIM utilise le mécanisme d’affirmation pour initier la sélection du transmetteur PIM pour le réseau multi-accès.
Dr priorité	Priorité configurée pour le routeur désigné sur le segment multi-accès connecté à l’interface.
Limite BSR	Oui ou Non indique si l’interface se trouve sur un routeur virtuel qui est Bootstrap Router (routeur d’amorçage ; BSR) situé à la limite du réseau local d’une entreprise.
Onglet Voisin PIM	
Interface	Nom de l'interface sur le routeur virtuel.
Adresse	Adresse IP du voisin PIM accessible sur l'interface.
Adresse secondaire	Adresse IP secondaire du voisin PIM accessible sur l'interface.
Délai d'activation	Durée pendant laquelle le voisin a été actif.
Délai d'expiration	Durée restante avant expiration du voisin, car le routeur virtuel ne reçoit pas de paquets Hello du voisin.
ID de génération	Valeur de 32-bit aléatoirement générée qui est régénérée chaque fois que la transmission PIM commence ou recommence sur l’interface (y compris lorsque le routeur lui-même est redémarré).
Dr priorité	Priorité du routeur désigné reçue par le routeur virtuel dans le dernier message Hello PIM de ce voisin.

Onglet Informations récapitulatives de BFD

Les informations récapitulatives de BFD comprennent les données suivantes.

Informations récapitulatives de BFD concernant les Statistiques d'exécution	Description
Interface	Interface qui exécute BFD.
Protocole	Itinéraire statique (famille d'adresses IP d'itinéraire statique) ou protocole de routage dynamique qui exécute BFD sur l'interface.
Adresse IP locale	Adresse IP de l'interface sur laquelle vous avez configuré BFD.
Adresse IP du voisin	Adresse IP du voisin BFD.
État	Les états BFD des homologues BFD locaux et distants : **administrateur inactif**, **inactif**, **initialisation** ou **actif**.
Temps de fonctionnement	Délai pendant lequel BFD a été activé (heures, minutes, secondes et millisecondes).
Discriminateur (local)	Discriminateur pour les homologues BFD locaux. Un discriminateur est une valeur unique et non nulle que les homologues utilisent pour distinguer plusieurs sessions BFD entre eux.
Discriminateur (distant)	Discriminateur pour les homologues BFD distants.
Erreurs	Nombre d'erreurs BFD.
Détails de la session	Cliquez sur **Détails** pour voir les informations BFD pour une session comme les adresses IP des voisins locaux et distants, le dernier code de diagnostic distant reçu, le nombre de paquets de contrôle transmis et reçus, le nombre d'erreurs, des informations sur le dernier paquet engendrant un changement d'état, etc.

Statistiques d'exécution supplémentaires d'un routeur logique

Après avoir configuré des itinéraires statiques ou des protocoles de routage pour un routeur logique, sélectionnez **Network (Réseau)** > **logical Routers (Routeurs logique)** et sélectionnez **More Runtime Stats (Statistiques d'exécution supplémentaires)** dans la dernière colonne pour afficher des informations détaillées sur le routeur logique, comme la table de routage, la table de transfert et les protocoles de routage et les itinéraires statiques que vous avez configurés. Ces fenêtres fournissent plus d'informations que ne peut en contenir un écran unique pour le routeur logique. La fenêtre affiche les onglets suivants :

- Routing (Stats for a Logical Router) (Routage Statistiques d'un routeur logique)
- BGP (Statistiques pour un routeur logique)

Statistiques d’exécution d’un routeur logique

- Routage > réseau > routeurs logiques > plus de statistiques d’exécution

Le tableau suivant décrit les statistiques d’exécution du routeur logique pour le tableau de routage, le tableau de transfert, et le tableau de Surveillance des itinéraires statiques.

Statistiques d’exécution	Description
Table d'itinéraires	
Afficher la famille d'adresses	Sélectionnez **IPv4 uniquement**, **IPv6 uniquement**, ou **IPv4 et IPv6** (par défaut) pour contrôler quel groupe d’adresses afficher dans le tableau.
Destination	Adresse IPv4 et masque réseau ou adresse IPv6 et longueur de préfixe des réseaux que le routeur logique peut atteindre.
Saut suivant	Adresse IP du périphérique au saut suivant vers le réseau de destination. Un saut suivant de 0.0.0.0 indique l'itinéraire par défaut.
Protocole	Indique que l’itinéraire est statique ou un itinéraire connecté ou hérité par BGP.
Mesure	Mesure de l'itinéraire. Lorsqu’un protocole de routage comporte plus d’une route vers le même réseau de destination, il privilégie l’itinéraire avec la valeur métrique la plus basse. Chaque protocole de routage utilise un autre type de métrique, par exemple, RIP utilise le nombre de sauts.
Sélectionné	Le champs est vrai si activé ; vide si désactivé.
Age	Antériorité de l'entrée d'itinéraire dans la table de routage.
Actif	Le champs est vrai si activé ; vide si désactivé.
Interface	L’interface de sortie du routeur logique qui sera utilisée pour atteindre le saut suivant.
Actualiser	Cliquez pour actualiser les statistiques d’exécution dans le tableau.
Table de transfert	
Le pare-feu choisit le meilleur itinéraire (de la table de routage (RIB) vers un réseau de destination) à placer dans la FIB.	

Statistiques d’exécution	Description
Destination	Meilleure adresse IPv4 et masque réseau ou adresse IPv6 et longueur de préfixe des réseaux que le routeur logique peut atteindre, sélectionné depuis la Table de routage.
Saut suivant	Adresse IP du périphérique au saut suivant vers le réseau de destination. Un saut suivant de 0.0.0.0 indique l'itinéraire par défaut.
MTU	Unité de transmission maximale (MTU) ; le nombre maximum d’octets que le pare-feu transmettra dans un seul paquet TCP vers cette destination.
flags	• **u** – L’itinéraire se dirige vers le haut. • **h** – L’itinéraire dirige vers un hôte. • **g** – L’itinéraire dirige vers une passerelle. • **e** – Le pare-feu a sélectionné cet itinéraire en utilisant le Chemin multiple à coût égal (ECMP). • ***** – L’itinéraire est le chemin privilégié vers un réseau de destination.
Interface	Interface de sortie du routeur logique qui sera utilisé pour atteindre le saut suivant.
Surveillance des itinéraires statiques	
Destination	Adresse IPv4 et masque réseau ou adresse IPv6 et longueur de préfixe d’un réseau que le routeur logique peut atteindre.
Saut suivant	Adresse IP du périphérique au saut suivant vers le réseau de destination. Un saut suivant de 0.0.0.0 indique l'itinéraire par défaut.
Mesure	Mesure de l'itinéraire. Lorsqu’il y a plus d’un itinéraire statique sur le même réseau de destination, le pare-feu favorise l’itinéraire avec la valeur métrique la plus basse.
Interface	L’interface de sortie du routeur logique qui sera utilisée pour atteindre le saut suivant.
Surveillance des chemins (échec)	Si la surveillance des chemins est activée pour cet itinéraire statique, l’Échec indique : • **Tout** – Le pare-feu considère l’itinéraire statique vers le bas et échoue si toutes les destinations surveillées pour l’itinéraire statique sont en panne.

Statistiques d’exécution	Description
	• **Un** – Le pare-feu considère l’itinéraire statique vers le bas et échoue si l’une des destinations surveillées pour l’itinéraire statique est en panne. Si la surveillance des chemins d’itinéraires statiques est désactivée, l’Échec indique **Désactivé**.
Status (État)	Le statut de l’itinéraire statique basé sur les requêtes pings ICMP vers les destinations surveillées : **Haut**, **Bas**, ou la surveillance des chemins pour l’itinéraire statique est **Désactivé**.
Actualiser	Actualise les statistiques d’exécution dans le tableau.

Statistiques BGP d’un routeur logique

Le tableau suivant décrit les statistiques d'exécution BGP du routeur logique.

Statistiques d’exécution BGP	Description
Onglet Récapitulation	
Activé	BGP activé : oui ou non.
ID du routeur	ID du routeur du routeur logique.
AS local	AS auquel appartient le routeur logique.
Appliquez le premier AS	Le champs est vrai si activé ; vide si désactivé.
Basculement externe rapide	Le champs est vrai si activé ; vide si désactivé.
Préférence locale par défaut	Préférence locale par défaut configurée
Redémarrage sans échec	Le champs est vrai si activé ; vide si désactivé.
Délai maximum de redémarrage des homologues (en sec.)	Nombre de secondes configuré pour le redémarrage en douceur du délai de redémarrage maximum des homologues.
Délai d’itinéraire obsolète (en sec.)	Nombre de secondes configuré pour le redémarrage en douceur de l’itinéraire obsolète.
Toujours comparer MED	Le champs est vrai si activé ; vide si désactivé.
Comparaison MED déterministe	Le champs est vrai si activé ; vide si désactivé.

Statistiques d’exécution BGP	Description
Onglet Homologue	
Nom	Nom de l'homologue.
Groupe d'homologues	Nom du groupe d'homologues auquel cet homologue appartient.
IP locale	Adresse IP de l'interface BGP sur le routeur logique.
AS local	AS auquel appartient le pare-feu BGP local.
IP de l'homologue	Adresse IP de l'homologue.
AS distant	AS auquel l’homologue appartient.
Haut/Bas	L’homologue est en haut ou en bas.
État	Établi
Onglet Groupe d'homologues	
Nom	Nom du groupe d'homologues.
Type	Type de groupe d'homologues configuré, tel que ebgp ou ibgp.
Rester en vie (en s)	Durée du rester en vie en secondes.
Temps d'attente (en s)	Temps d’attente en secondes.
Adresse IP	Le champs est vrai si activé ; vide si désactivé.
IPv6	Le champs est vrai si activé ; vide si désactivé.
Min. Intervalle max. de l’itinéraire (en s)	Intervalle minimum de l’itinéraire en secondes.
Unicast	Le champs est vrai si activé ; vide si désactivé.
itinéraire	
Nom	Itinéraire IPv4 ou IPv6 dans le tableau de routage : une adresse IPv4 ou IPv6 et la longueur du préfixe.
Chemin AS	AS suivant sur le chemin.
Meilleur AS	Le champs est vrai si activé ; vide si désactivé.

Statistiques d’exécution BGP	Description
Moyen	0 ou vide
Métrique	0 ou vide
Réseau	
Saut suivant	Adresse IP du saut suivant à atteindre dans le réseau identifié en tant qu’itinéraire (Nom).
Origine	Origine de l’itinéraire : IGP ou incomplet
Chemin d'accès	AS suivant dans le chemin.
Chemin depuis	Indique externe.
Nom de l’homologue	
Préfixe	
Longueur du préfixe	
Valide	Le champs est vrai si activé ; vide si désactivé.
Poids	Poids de l’itinéraire.

Réseau > Routage > Routeurs logiques

Le pare-feu a besoin d'un routeur logique pour disposer d'itinéraires vers d'autres sous-réseaux, soit via des itinéraires statiques définis manuellement, soit via l'application de protocoles de routage de couche 3 (itinéraires dynamiques). Chaque interface de Couche 3, interface en boucle et interface VLAN définie sur le pare-feu doit être associée à un routeur logique. Chacune d'entre elles ne peut appartenir qu'à un seul routeur logique.

Le routeur logique est disponible après avoir activé **Advanced Routing (Routage avancé)** dans les paramètres généraux de**Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestions)** puis validez et redémarrez le pare-feu.

Définir un routeur logique nécessite d’ajouter des interfaces Layer 3 au routeur logique et de configurer une combinaison d’itinéraires statiques et des protocoles de routage dynamique tel que l’exige votre réseau. Vous pouvez aussi configurer les autres fonctionnalités comme ECMP et BFD.

Que voulez-vous faire ?	Reportez-vous à la section
Eléments nécessaires d’un routeur logique	Paramètres généraux du routeur logique
Configurer :	Itinéraires statiques Filtres OSPF Profils de routage OSPF OSPFv3 Profils de routage OSPFv3 BGP Profils de routage BGP Multicast Profils de routage multidiffusion RIPv2 Profils de routage RIPv2 Profils de routage BFD
Consulter les informations d’un routeur logique.	Statistiques d’exécution supplémentaires d’un routeur logique

Réseau > Routage > Routeurs logiques > Généralités

Lorsque vous activez Routage Avancé (**Device (périphérique)** > **Setup (Configuration)** > **Management (Gestion)**), le pare-feu utilise un routeur logique pour le routage statique et dynamique. Un routeur logique nécessite que vous attribuiez un nom et des interfaces Layer 3 tel que cela est décrit dans le tableau suivant.

En option, vous pouvez configurer le traitement Equal Cost Multiple Path (ECMP) pour le routeur logique. Le traitement ECMP est une fonction réseau qui permet au pare-feu d'utiliser jusqu'à quatre itinéraires de coût égal vers la même destination. Sans cette fonction, s'il existe plusieurs itinéraires de coût égal vers la même destination, le routeur virtuel choisit l'un de ces itinéraires dans la table de routage et l'ajoute à sa table de transfert ; il n'utilise aucun autre itinéraire à moins qu'il n'y ait une interruption dans l'itinéraire choisi. L'activation de la fonctionnalité ECMP sur un routeur virtuel permet au pare-feu d'avoir jusqu'à quatre chemins de coût égal vers une destination dans sa table de transfert, grâce auxquels il peut :

- Équilibrer la charge des flux (sessions) vers la même destination sur plusieurs liaisons de coût égal.
- Utiliser la bande passante disponible sur toutes les liaisons vers la même destination plutôt que de laisser certains liens inutilisés.
- Déplacer le trafic de façon dynamique d’un autre membre ECMP vers la même destination en cas de défaillance d’une liaison, au lieu d’attendre que le protocole de routage ou la table RIB choisisse un autre chemin, ce qui peut aider à réduire le délai d’inactivité en cas de défaillance de la liaison.

L'équilibrage de la charge ECMP est effectué au niveau de la session et non au niveau du paquet. Le pare-feu choisit ainsi un chemin de coût égal au début d’une nouvelle session et non à chaque fois que le pare-feu reçoit un paquet.

Paramètres généraux du routeur logique	Description
Name (Nom)	Saisissez un nom pour décrire le routeur virtuel (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. N'utilisez que des lettres, chiffres, traits d'union et traits de soulignement.
Interface	
Interface	Ajoutez les interfaces Layer 3 à inclure dans le routeur logique. ces interfaces peuvent être utilisés comme interfaces sortantes dans la table de routage du routeur logique. Pour spécifier le type d’interface, reportez-vous à Réseau > Interfaces. Lorsque vous ajoutez une interface à un routeur logique, ses itinéraires connectés sont automatiquement ajoutés au RIB global.
Distances administratives	
Statique	La plage est comprise entre 1 et 255 ; la valeur par défaut est 10.
IPv6 statique	La plage est comprise entre 1 et 255 ; la valeur par défaut est 10.

Paramètres généraux du routeur logique	Description
Intra-zone OSPF	La plage est comprise entre 1 et 255 ; la valeur par défaut est 110.
Inter-zone OSPF	La plage est comprise entre 1 et 255 ; la valeur par défaut est 110.
OSPF externe	La plage est comprise entre 1 et 255 ; la valeur par défaut est 110.
Intra-zone OSPFv3	La plage est comprise entre 1 et 255 ; la valeur par défaut est 110.
Inter-zone OSPFv3	La plage est comprise entre 1 et 255 ; la valeur par défaut est 110.
OSPFv3 Externe	La plage est comprise entre 1 et 255 ; la valeur par défaut est 110.
BGP AS Interne	La plage est comprise entre 1 et 255 ; la valeur par défaut est 200.
BGP AS Externe	La plage est comprise entre 1 et 255 ; la valeur par défaut est 20.
Itinéraire local BGP	La plage est comprise entre 1 et 255 ; la valeur par défaut est 20.
RIP	La plage est comprise entre 1 et 255 ; la valeur par défaut est 120.
ECMP	
Activer	Traitement Equal Cost Multiple Path (ECMP) pour le routeur logique.
Retour symétrique	(Facultatif) Sélectionnez l'option **Symmetric Return (Retour symétrique)** pour que les paquets de retour sortent de la même interface que celle sur laquelle les paquets d'entrée associés sont arrivés. Autrement dit, le pare-feu utilisera l'interface d'entrée sur laquelle envoyer des paquets de retour, au lieu de l'interface ECMP. Ainsi, le paramètre **Symmetric Return (Retour symétrique)** applique un contrôle prioritaire sur l'équilibrage de la charge. Ce comportement se produit uniquement pour les flux de trafic du serveur au client.
Chemin strict d’accès source	Par défaut, le trafic IKE et IPSec en provenance du pare-feu sort d’une interface que la méthode d’équilibrage de charge ECMP détermine. Sélectionnez **Strict Source Path (Chemin d’accès source strict)** pour vous assurer que le trafic IKE et IPSec en provenance du pare-feu sort toujours de l’interface physique à laquelle appartient l’adresse IP source du tunnel IPSec. Vous activerez le Chemin d’accès source strict lorsque le pare-feu a plus d’un ISP qui offre des chemins d’accès à coût égal vers la même destination. Les ISP effectuent généralement une vérification de Transfert de chemin d’accès inversé (RPF) (ou une vérification différente afin d’empêcher l’usurpation d’adresse IP) pour confirmer que le trafic sort de la même interface que celle sur laquelle il est arrivé. Parce que le traitement ECMP par défaut choisira une interface de sortie sur la base de la méthode ECMP configurée (au

Paramètres généraux du routeur logique	Description
	lieu de choisir l'interface source comme interface de sortie), ce n'est pas ce à quoi l'ISP s'attend et l'ISP pourra bloquer le trafic de retour légitime. Dans ce cas d'utilisation, activez le chemin d'accès strict afin que le pare-feu utilise l'interface de sortie correspondant à l'interface à laquelle appartient l'adresse IP source du tunnel IPSec.
Nombre max. de chemins	Sélectionnez le nombre maximum d'itinéraires de coût égal : (2, 3 ou 4) vers un réseau de destination qui peut être copié de la RIB à la FIB. La valeur par défaut est 2.
Méthode d'équilibrage de charge	Choisissez l'un des algorithmes d'équilibrage de la charge ECMP suivants à utiliser sur le routeur virtuel. L'équilibrage de la charge ECMP est effectué au niveau de la session et non au niveau du paquet. Le pare-feu (ECMP) choisit ainsi un chemin de coût égal au début d'une nouvelle session et non à chaque fois qu'un paquet est reçu. • **IP Modulo (Modulo IP)**- Par défaut, le routeur virtuel équilibre la charge des sessions à l'aide de cette option, qui utilise un hachage des adresses IP source et de destination dans l'en-tête des paquets pour déterminer l'itinéraire ECMP à utiliser. • **IP Hash (Hachage IP)** : il existe deux méthodes de hachage IP qui déterminent quel itinéraire ECMP il convient d'utiliser : • Si vous sélectionnez **IP Hash (Hachage IP)**, par défaut, le pare-feu utilise un hachage des adresses IP source et de destination. • Vous pouvez également sélectionner **Use Source Address Only (Utiliser l'adresse source uniquement)** (disponible dans PAN-OS 8.0.3 et dans les versions ultérieures). Cette méthode de hachage IP garantit que toutes les sessions appartenant à la même adresse IP source prennent toujours le même chemin. • Vous pouvez éventuellement sélectionner **Use Source/ Destination Ports (Utiliser les ports source/de destination)** pour inclure les ports dans l'un ou l'autre des calculs du hachage. Vous pouvez également saisir une **Hash Seed (Valeur initiale de hachage)** (un nombre entier) pour randomiser l'équilibrage de la charge. • **Weighted Round Robin (Pondération comparative)** - Cet algorithme peut être utilisé pour prendre en compte les différentes capacités et vitesses de liaison. Lorsque vous choisissez cet algorithme, la fenêtre Interface s'ouvre. Cliquez sur **Add (Ajouter)** et sélectionnez une **Interface** à inclure dans le groupe Pondération comparative. Saisissez la valeur **Weight (Pondération)** à utiliser pour cette interface. La valeur de **Weight (Pondération)** est de 100 par défaut et l'intervalle est de 1-255. Plus la valeur de pondération d'un chemin de coût égal spécifique est élevée, plus ce chemin

Paramètres généraux du routeur logique	Description
	sera sélectionné pour une nouvelle session. Une liaison plus rapide doit avoir une pondération supérieure à une liaison plus lente, de manière à ce que le trafic ECMP passe par la liaison plus rapide. Cliquez à nouveau sur **Add (Ajouter)** pour ajouter une autre interface et une autre pondération. • **Balanced Round Robin (Équilibrage comparatif)** - Distribue les sessions ECMP entrantes de manière égale entre les liaisons.
Filtre RIB	
IPv4 - Carte d'itinéraire BGP	Sélectionnez une carte d'itinéraire de redistribution ou créez-en une nouvelle pour contrôler les itinéraires BGP IPv4 ajoutées au RIB global. Valeur par défaut : **Aucune**.
IPv4 - Carte d'itinéraire OSPFv2	Sélectionnez une carte d'itinéraire de redistribution ou créez-en une nouvelle pour contrôler les itinéraires IPv4 OSPFv2 ajoutées au RIB global. Valeur par défaut : **Aucune**.
IPv4 - Carte d'itinéraire statique	Sélectionnez une carte d'itinéraire de redistribution ou créez-en une nouvelle pour contrôler les itinéraires statiques IPv4 ajoutées au RIB global. Valeur par défaut : **Aucune**.
IPv4 - Carte d'itinéraire RIP	Sélectionnez une carte d'itinéraire de redistribution ou créez-en une nouvelle pour contrôler les itinéraires RIP ajoutés au RIB global. Valeur par défaut : **Aucune**.
IPv6 - Carte d'itinéraire BGP	Sélectionnez une carte d'itinéraire de redistribution ou créez-en une nouvelle pour contrôler les itinéraires BGP IPv6 ajoutées au RIB global. Valeur par défaut : **Aucune**.
IPv6 - Carte d'itinéraire OSPFv3	Sélectionnez une carte d'itinéraire de redistribution ou créez-en une nouvelle pour contrôler les itinéraires IPv6 OSPFv3 ajoutées au RIB global. Valeur par défaut : **Aucune**.
IPv6 - Carte d'itinéraire statique	Sélectionnez une carte d'itinéraire de redistribution ou créez-en une nouvelle pour contrôler les itinéraires statiques IPv6 ajoutées au RIB global. Valeur par défaut : **Aucune**.

Réseau > Routage > Routeurs logiques > Statique

Vous pouvez éventuellement ajouter un ou plusieurs itinéraires statiques pour un routeur logique sur un moteur de routage avancé. Sélectionnez **IPv4** ou **IPv6** et **Add (Ajoutez)** l'itinéraire utilisant une adresse IPv4 ou IPv6. Dans ce cas, vous devez généralement configurer des itinéraires par défaut (0.0.0.0/0). Ces derniers sont appliqués pour les destinations qui sont introuvables dans le tableau de routage du routeur logique.

Paramètres d’Itinéraire statique	Description
Name (Nom)	Saisissez un nom pour identifier l’itinéraire statique (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. N'utilisez que des lettres, chiffres, traits d'union et traits de soulignement.
Destination	Saisissez une adresse IP et un masque réseau en notation CIDR (Classless Inter-domaine Routing/routage inter-domaine sans classes) : *ip_address/masque* (par exemple, 192.168.2.0/24 pour IPv4 ou 2001:db8::/32 pour IPv6). Vous pouvez également créer un objet d'adresse de type Masque réseau IP.
Interface	Sélectionnez l'interface de sortie pour transférer des paquets vers leur destination et/ou configurer les paramètres du saut suivant. Indiquez une interface pour disposer d'un contrôle plus strict quant à l'interface que le pare-feu utilisera au lieu d’utiliser l'interface figurant dans la table de routage pour le saut suivant de cet itinéraire. Valeur par défaut : **Aucune**.
Saut suivant	Sélectionnez l’une des options suivantes : • **IP Address (Adresse IP)** ou **IPv6 Address (Adresse IPv6)** : sélectionnez pour saisir l’adresse IPv6 du routeur du saut suivant, ou sélectionnez ou créez un objet d’adresse de type Masque réseau IP. L’objet d’adresse doit avoir un masque réseau de /32 pour IPv4 ou de /128 pour IPv6. Vous devez **Enable IPv6 on the interface (Activer IPv6 sur l'interface)** (lorsque vous configurez des interfaces de couche 3) d sorte qu'elles utilisent une adresse IPv6 de saut suivant. • **Next LR**—Sélectionnez le prochain routeur logique en tant que saut suivant. • **FQDN**—Entrez un nom de domaine complet qui sera le saut suivant. • **Discard (Supprimer)** - Indiquez si vous voulez arrêter le trafic vers cette destination. • **None (Aucun)** : (par défaut) sélectionnez cette option s'il n'existe aucun saut suivant pour l'itinéraire. Par exemple, il n'est pas nécessaire de définir de saut suivant pour une connexion de point à point, car les paquets ne peuvent suivre qu'une direction.
Admin Dist	Indiquez la distance administrative de l'itinéraire statique (de 10 à 240, valeur par défaut : 10).
Mesure	Indiquez une mesure valide pour l'itinéraire statique (fourchette de 1 à 65 535 ; par défaut 10).
Profil BFD	Sélectionnez un profil BFD ou créez-en un nouveau à appliquer à l’itinéraire statique. Par défaut **None (disable BFD) (Aucun - BFD désactivé)**.

Paramètres d’Itinéraire statique	Description
Surveillance des chemins	Sélectionnez cette option pour procéder à la configuration de la surveillance des chemins.
Activer	**Enable (Activez)** la surveillance des chemins pour un itinéraire statique.
Condition d'échec	Sélectionnez la condition selon laquelle le pare-feu considère le chemin surveillé comme inactif et considère donc l’itinéraire statique comme inactif : • **Any (N’importe laquelle)** – Si n’importe laquelle des destinations surveillées pour l’itinéraire statique n’est pas accessible par ICMP, le pare-feu supprime l’itinéraire statique de la RIB et de la FIB et ajoute l’itinéraire dynamique ou statique dont la métrique la plus faible suivante se dirige vers la même destination que la FIB. • **Tout —**Si toutes les destinations surveillées pour la route statique sont inaccessibles par ICMP, le pare-feu supprime la route statique du RIB et du FIB et ajoute la route dynamique ou statique qui a la métrique la plus basse suivante allant à la même destination au FIB. Sélectionnez **Tout** pour éviter la possibilité qu'une seule destination surveillée signale une défaillance de route statique lorsque cette destination surveillée est simplement hors ligne pour maintenance, par exemple.
Délai de maintien préemptif	Saisissez le nombre de minutes pendant lesquelles une surveillance des chemins inactifs doit conserver l’état Active (la surveillance des chemins évalue toutes les destinations surveillées de ses membres et doit rester Active avant que le pare-feu ne réinstalle l’itinéraire statique dans la RIB). Si le minuteur expire sans que la liaison devienne inactive ou instable, la liaison est jugée stable, la surveillance des chemins peut rester Active et le pare-feu peut ajouter l’itinéraire statique à la RIB. Si la liaison devient inactive ou instable pendant le délai de maintien, la surveillance des chemins échoue et le minuteur redémarre lorsque la surveillance désactivée reprend l’état Actif. Un **Preemptive Hold Time (Délai de maintien de préemption)** de zéro permet au pare-feu de réinstaller l’itinéraire statique dans la RIB immédiatement après l’activation de la surveillance des chemins. La plage est comprise entre 0 et 1 440 ; la valeur par défaut est 2.
Nom	**Add (Ajoutez)** un nom pour la destination surveillée (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. N'utilisez que des lettres, chiffres, traits d'union et traits de soulignement.
Activer	Sélectionnez cette option pour activer la surveillance des chemins de cette destination spécifique pour l’itinéraire statique ; le pare-feu envoie des requêtes ping ICMP à cette destination.

Paramètres d’Itinéraire statique	Description
IP source	Sélectionnez l’adresse IP que le pare-feu utilisera en tant que source dans la requête ping ICMP vers la destination surveillée : • Si l’interface possède plusieurs adresses IP, sélectionnez-en une. • Si vous sélectionnez une interface, le pare-feu utilise la première adresse IP affectée à l’interface par défaut. • Si vous sélectionnez **DHCP (Use DHCP Client address) (DHCP (Utiliser l’adresse du client DHCP))**, le pare-feu utilise l’adresse que DHCP a affectée à l’interface. Pour consulter l’adresse DHCP, sélectionnez **Network (Réseau)** > **Interfaces (Interfaces)** > **Ethernet** et dans la ligne de l’interface Ethernet, cliquez sur **Dynamic DHCP Client (Client DHCP dynamique)**. L’adresse IP s’affiche dans la fenêtre Statut de l’interface IP dynamique. • **PPPOE (Use PPPoE Client Address) (Utiliser l'adresse du client PPPoE)**
IP de destination	Saisissez une adresse IP fiable et stable ou un objet d’adresse pour lequel le pare-feu surveillera les chemins. La destination surveillée et la destination de l’itinéraire statique doivent utiliser la même famille d’adresses (IPv4 ou IPv6).
Intervalle des requêtes ping (sec)	Indiquez l’intervalle de la requête ping ICMP en secondes pour déterminer la fréquence à laquelle le pare-feu surveille les chemins (effectue un test ping sur la destination surveillée) ; la plage est comprise entre 1 et 60 ; la valeur par défaut est 3.
Nombre de requêtes ping	Indiquez le nombre de paquets de requêtes ping ICMP consécutifs qui ne sont pas renvoyés par la destination surveillée avant que le pare-feu ne considère la liaison comme inactive. En fonction de la condition d’échec **Any (Indifférente)** ou **All (Toutes)**, si la surveillance des chemins est en état d’échec, le pare-feu supprime l’itinéraire statique de la RIB (la plage est comprise entre 3 et 10 et la valeur par défaut est 5). Par exemple, un Intervalle des requêtes ping de 3 secondes et un Nombre de requêtes ping de 5 requêtes ping manquées (le pare-feu ne reçoit pas de requêtes ping au cours des 15 dernières secondes) signifient que la surveillance des chemins détecte un échec de la liaison. Si la surveillance des chemins est en état d’échec et que le pare-feu reçoit une requête ping après 15 secondes, la liaison est considérée comme active ; en fonction de la condition d’échec **Any (Indifférente)** ou **All (Toutes)**, la surveillance des chemins de **Any (N’importe laquelle)** ou de **All (Toutes)** les destinations surveillées peut être considérée comme activée et le Délai de maintien de préemption commence.

Réseau > Routage > Routeurs logiques > OSPF

Le tableau décrit les paramètres permettant de configurer les zones OSPFv2 pour un routeur logique sur un moteur de routage avancé.

Paramètres OSPF	Description
Activer	Activez OSPF pour le routeur logique.
ID de routeur	Entrez un ID de routeur au format d'une adresse IPv4.
Profil BFD	Si vous souhaitez appliquer la détection de transfert bidirectionnel à OSPF, sélectionnez un profil BFD ou créez-en un nouveau. Par défaut **None (disable BFD) (Aucun - BFD désactivé)**.
Minuterie générale globale	Sélectionnez un profil Global Timer ou créez-en un nouveau à appliquer à OSPF.
Minuterie d'interface globale	Sélectionnez un minuteur d'interface OSPF ou créez-en un nouveau à appliquer à OSPF.
Profil de redistribution	Sélectionnez un profil de redistribution OSPF ou créez-en un nouveau pour redistribuer les itinéraires statiques IPv4, les itinéraires connectés, les itinéraires BGP IPv4 ou l'itinéraire IPv4 par défaut vers la base de données d'état des liens OSPF.
nominale	
ID de zone	Ajoutez une zone identifiée par son ID de zone au format x.x.x.x. Il s'agit de l'identifiant devant faire partie de la même zone et que chaque voisin doit accepter.
Type	
Authentification	Sélectionnez un profil d'authentification ou créez-en un nouveau.
Type	Sélectionnez le type de zone OSPF : • **Normal (Normal)** - Aucune restriction n'est appliquée ; la zone peut accepter tout type d'itinéraire. • **Stub (Terminale)** : il n'existe aucune sortie issue de la zone. Pour atteindre une destination en dehors de la zone, le trafic doit passer par un routeur frontalier de zone (ABR), qui se connecte à d'autres zones.

Paramètres OSPF	Description
	• **NSSA (Not-So-Stubby Area (Zone pas si terminale ; NSSA))** : le pare-feu ne peut sortir de la zone que par des itinéraires autres que des itinéraires OSPF.
pas de résumé	(Zones Stub et NSSA uniquement) Sélectionnez cette option pour empêcher la zone de recevoir des LSA sommaires de type 3 et ainsi réduire la circulation dans la zone.
Les informations par défaut proviennent	(zones NSSA uniquement) Sélectionnez cette option pour que OSPF génère un itinéraire par défaut.
Mesure	(zones NSSA uniquement) Entrez une métrique pour l'itinéraire par défaut ; la plage est comprise entre 1 et 16 777 214 ; la valeur par défaut est 10.
Type de mesure	(zones NSSA uniquement) **Type 1** ou **Type 2**
ABR	Sélectionnez si le routeur logique est un routeur de bordure de zone, ce qui permet de configurer les quatre champs suivants.
Liste d'importation	Sélectionnez une liste d'accès ou créez-en une nouvelle pour filtrer les itinéraires réseau entrant dans la zone en fonction de l'adresse source IPv4.
Liste d'exportation	Sélectionnez une liste d'accès ou créez-en une nouvelle pour filtrer les itinéraires réseau provenant de la zone, afin d'autoriser ou d'empêcher la publication des itinéraires vers d'autres zones.
Liste de filtres entrants	Sélectionnez une liste de préfixes ou créez-en une nouvelle pour filtrer les préfixes réseau entrant dans la zone.
Liste des filtres sortants	Sélectionnez une liste de préfixes ou créez-en une nouvelle pour filtrer les préfixes réseau provenant de la zone, afin d'empêcher la publication des itinéraires vers d'autres zones.
Préfixe IPv4	(zones NSSA uniquement) Si **ABR** est sélectionné et que le type de zone est **NSSA**, **ajoutez** un préfixe IPv4 pour résumer un groupe de sous-réseaux externes en un seul LSA de type 7, qui est ensuite traduit en LSA de type 5 et publié sur le backbone lorsque vous sélectionnez **Publier**.
Intervalle	
Adresse IP/Masque de réseau	Ajoutez une adresse IP/un masque de réseau. Un LSA (link-state advertisement) de type 3 Summary avec des

Paramètres OSPF	Description
	informations de routage correspondant à cette plage est annoncé dans la zone dorsale si la zone contient au moins un réseau intra-zone (c'est-à-dire décrit avec un routeur ou un réseau LSA) de cette plage).
Substituer	Entrez une adresse IP/masque de réseau de substitution afin qu'un LSA résumé de type 3 avec cette adresse IP/masque de réseau soit annoncé dans le backbone si la zone contient au moins un réseau intra-zone de l'adresse IP/masque de réseau spécifié.
Publier	Sélectionnez cette option pour envoyer des LSA qui correspondent au sous-réseau.
Interface	
Interface	Ajoutez chaque interface à inclure dans la zone.
Activer	Activez l'interface.
MTU Ignorer	Sélectionnez cette option pour ignorer les incohérences de l'unité de transmission maximale (MTU) lorsque vous essayez d'établir une contiguïté (la valeur par défaut est désactivée ; La vérification des correspondances MTU a lieu). RFC 2328 définit l'interface MTU comme « La taille en octets du plus grand datagramme IP qui peut être envoyé hors de l'interface associée, sans fragmentation ».
Passif	Sélectionnez cette option pour empêcher l'interface d'envoyer ou de recevoir des paquets OSPF ; toutefois, l'interface est toujours incluse dans la base de données d'état des liens. Vous pouvez rendre une interface passive, par exemple, si elle se connecte à un commutateur, car vous ne voulez pas envoyer de paquets Hello là où il n'y a pas de routeur.
Type de lien	Sélectionnez le type de lien : • **Broadcast (Diffusion)**: tous les voisins accessibles via l'interface sont détectés automatiquement en multidiffusant des messages Hello OSPF, comme une interface Ethernet. • **p2p** (point à point) : découvre automatiquement le voisin. • **p2mp** (point-to-multipoint/point-multipoint) : les voisins doivent être définis manuellement. Ajoutez l'adresse IP du **voisin** pour tous les voisins accessibles via cette

Paramètres OSPF	Description
	interface et la **priorité** de chaque voisin ; la plage est comprise entre 0 et 255 ; la valeur par défaut est 1.
Priorité	Entrez la priorité de l'interface ; la priorité pour que le routeur soit élu en tant que routeur désigné (DR) ou DR de sauvegarde (BDR); la plage est comprise entre 0 et 255; la valeur par défaut est 1. Lorsque la valeur 0 est configurée, le routeur ne sera pas élu en tant que DR ou BDR.
Profil de la minuterie	Sélectionnez un profil de minuterie ou créez-en un nouveau à appliquer à l'interface. Ce profil remplace le profil Global Interface Timer appliqué à OSPF.
Authentification	Sélectionnez un profil d'authentification ou créez-en un nouveau à appliquer à l'interface. Ce profil remplace le profil d'authentification appliqué sous l'onglet Type.
Profil BFD	Sélectionnez un profil BFD ou **Inherit-vr-global-setting** (par défaut) ou créez un nouveau profil BFD ou sélectionnez **Aucun (Désactiver BFD).** Ce profil remplace le profil configuré pour OSPF.
Coût	Spécifiez un coût pour l'interface; la plage est comprise entre 1 et 65 535; la valeur par défaut est 10.
Liaison virtuelle	
Nom	Donnez un Name (Nom) au câble virtuel.
Activer	Activez le lien virtuel.
nominale	
ID de routeur	
Profil de la minuterie	Sélectionnez un profil de minuterie ou créez-en un nouveau à appliquer au lien virtuel. Ce profil remplace le profil Global Interface Timer appliqué à OSPF.
Authentification	Sélectionnez un profil d'authentification ou créez-en un nouveau à appliquer au lien virtuel. Ce profil remplace le profil d'authentification appliqué sous l'onglet Type.
Avancé	
Compatibilité avec RFC 1583	Sélectionnez cette option pour appliquer la compatibilité avec la RFC 1583, qui permet une meilleure route vers

Paramètres OSPF	Description
	un routeur asbr (System Boundary Router) autonome dans la table de routage OSPF. La valeur par défaut est désactivée, ce qui signifie que la table de routage OSPF peut conserver plusieurs chemins intra-AS dans la table de routage, empêchant ainsi les boucles de routage.
Redémarrage en douceur (Graceful Restart) : activez le redémarrage en douceur.	Activez Le redémarrage progressif pour le routeur logique ; la valeur par défaut est activée.
Enable Helper Mode (Activer le mode Aide)	Activez le mode d'assistance au redémarrage progressif pour le routeur logique ; la valeur par défaut est activée.
Enable Strict LSA Checking (Activer la vérification LSA stricte)	Activez la vérification LSA stricte pour que le routeur d'assistance cesse d'exécuter le mode d'assistance et que le processus de redémarrage gracieux s'arrête si une publication sur l'état du lien indique un changement de topologie réseau ; la valeur par défaut est activée.
Période de grâce (sec)	Spécifiez le nombre de secondes pendant lesquelles le routeur logique effectuera un redémarrage en douceur si le pare-feu tombe en panne ou devient indisponible. La plage est comprise entre 5 et 1 800 ; la valeur par défaut est 120.
Heure maximale de redémarrage des voisins (sec)	La plage est comprise entre 5 et 1 800 ; la valeur par défaut est 140.

Réseau > Routage > Routeurs logiques >OSPFv3

Le tableau décrit les paramètres permettant de configurer les zones OSPFv3 pour un routeur logique sur un moteur de routage avancé.

Paramètres OSPFv3	Description
Activer	Activez OSPFv3 pour le routeur logique.
ID de routeur	Entrez un ID de routeur au format d'une adresse IPv6.
Profil BFD	Si vous souhaitez appliquer la détection de transfert bidirectionnel à OSPF, sélectionnez un profil BFD ou créez-en un nouveau. Par défaut None (disable BFD) (Aucun - BFD désactivé).
Minuterie générale globale	Sélectionnez un profil Global Timer ou créez-en un nouveau à appliquer à OSPFv3.

Paramètres OSPFv3	Description
Minuterie d’interface globale	Sélectionnez un minuteur d’interface OSPFv3 ou créez-en un nouveau à appliquer à OSPFv3.
Profil de redistribution	Sélectionnez un profil de redistribution OSPFv3 ou créez-en un nouveau pour redistribuer les itinéraires statiques IPv6, les itinéraires connectés, les itinéraires BGP IPv6 ou l’itinéraire IPv6 par défaut vers la base de données d’état des liens OSPFv3.
nominale	
ID de zone	Ajoutez une zone identifiée par son ID de zone au format d’adresse IPv4. Il s'agit de l'identifiant devant faire partie de la même zone et que chaque voisin doit accepter.
Type	
Authentification	Sélectionnez un profil d’authentification ou créez-en un nouveau.
Type	Sélectionnez le type de zone OSPFv3 : • **Normal (Normal)** - Aucune restriction n'est appliquée ; la zone peut accepter tout type d'itinéraire. • **Stub (Terminale)** : il n'existe aucune sortie issue de la zone. Pour atteindre une destination en dehors de la zone, le trafic doit passer par un routeur frontalier de zone (ABR), qui se connecte à d’autres zones. • **NSSA (Not-So-Stubby Area (Zone pas si terminale ; NSSA))** : le trafic ne peut sortir de la zone que par des itinéraires autres que des itinéraires OSPFv3.
pas de résumé	(Stub et NSSA uniquement) Sélectionnez cette option pour empêcher la zone de recevoir des LSA sommaires de type 3 et ainsi réduire le trafic dans la zone.
Les informations par défaut proviennent	(NSSA uniquement) Sélectionnez cette option pour que OSPFv3 génère un itinéraire par défaut.

Paramètres OSPFv3	Description
Mesure	(NSSA uniquement) Entrez une mesure pour l'itinéraire par défaut ; la plage est comprise entre 1 et 16 777 214 ; la valeur par défaut est 10.
Type de mesure	(NSSA uniquement) Sélectionnez **Type 1** ou **Type 2**.
ABR	Sélectionnez si le routeur logique est un routeur de bordure de zone (un routeur avec des interfaces dans plusieurs zones, y compris la zone 0), ce qui permet de configurer les quatre champs suivants.
Liste d'importation	Sélectionnez une liste d'accès ou créez-en une nouvelle pour filtrer les LSA de type 3 ; s'applique aux chemins annoncés dans la zone spécifiée en tant que LSA récapitulatifs de type 3.
Liste d'exportation	Sélectionnez une liste d'accès ou créez-en une nouvelle pour filtrer les LSA récapitulatifs de type 3 annoncés à d'autres zones provenant de chemins intra-zone de la zone spécifiée.
Liste de filtres entrants	Sélectionnez une liste de préfixes ou créez-en une nouvelle pour filtrer les LSA récapitulatifs de type 3 entrant dans la zone.
Liste des filtres sortants	Sélectionnez une liste de préfixes ou créez-en une nouvelle pour filtrer les LSA récapitulatifs de type 3 de la zone.
Préfixe IPv6	(NSSA uniquement) Si **ABR** est activé, ajoutez un préfixe IPv6 pour résumer un groupe de sous-réseaux externes en un seul LSA de type 7, qui est ensuite traduit en LSA de type 5 et publié sur le backbone lorsque vous sélectionnez **Publier**.
Intervalle	
Adresse IPv6/Masque de réseau	Ajoutez une adresse IPv6/masque de réseau. Un LSA sommaire de type 3 avec des informations de routage correspondant à cette plage est annoncé dans la zone dorsale si la zone contient au moins un réseau intra-zone (c'est-à-dire décrit avec un routeur ou un réseau LSA) de cette plage).
Publier	Sélectionnez cette option pour publier les sous-réseaux correspondants dans les LSA dans la

Paramètres OSPFv3	Description
	zone dorsale. Si **Advertise** est défini sur No, les préfixes intra-zone correspondants présents dans la zone ne seront pas publiés dans la zone dorsale.
Interface	
Interface	Ajoutez une interface à inclure dans la zone.
Activer	Activez l’interface.
MTU Ignorer	Sélectionnez cette option pour ignorer les incohérences de l’unité de transmission maximale (MTU) lorsque vous essayez d’établir une contiguïté (la valeur par défaut est désactivée ; La vérification des correspondances MTU a lieu).
Passif	Sélectionnez pour empêcher l’envoi de paquets OSPF Hello hors de cette interface et ainsi empêcher le routeur local de créer une contiguïté OSPF avec un voisin; toutefois, l’interface est toujours incluse dans la base de données d’état des liens. Vous pouvez rendre une interface passive, par exemple, si elle se connecte à un commutateur, car vous ne voulez pas envoyer de paquets Hello là où il n’y a pas de routeur.
ID d’instance	Gardez la valeur 0 car une seule instance d’OSPFv3 est autorisée ; la valeur par défaut est 0.
Type de lien	Sélectionnez le type de lien : • **Broadcast (Diffusion)** si vous voulez que tous les voisins accessibles via l'interface soient détectés automatiquement en multidiffusant des messages Hello OSPFv3, comme une interface Ethernet. • **p2p** (point à point) : découvre automatiquement le voisin. • **p2mp** (point-to-multipoint/point-multipoint) : les voisins doivent être définis manuellement. Ajoutez l’adresse IPv6 **voisine** pour tous les voisins accessibles via cette interface et la **priorité** de chaque voisin ; la plage est comprise entre 0 et 255 ; la valeur par défaut est 1.

Paramètres OSPFv3	Description
Priorité	Entrez la priorité de l'interface ; la priorité pour que le routeur soit élu en tant que routeur désigné (DR) ou DR de sauvegarde (BDR); la plage est comprise entre 0 et 255; la valeur par défaut est 1. Lorsque la valeur 0 est configurée, le routeur ne sera pas élu en tant que DR ou BDR.
Profil de la minuterie	Sélectionnez un profil de minuterie ou créez-en un nouveau à appliquer à l'interface. Ce profil remplace le profil Global Interface Timer appliqué à OSPFv3.
Authentification	Sélectionnez un profil d'authentification ou créez-en un nouveau à appliquer à l'interface. Ce profil remplace le profil d'authentification appliqué sous l'onglet Type.
Profil BFD	Sélectionnez un profil BFD ou **Inherit-vr-global-setting** (par défaut) ou créez un nouveau profil BFD ou sélectionnez **Aucun (Désactiver BFD).** Ce profil remplace le profil configuré pour OSPFv3.
Coût	Spécifiez un coût pour l'interface; la plage est comprise entre 1 et 65 535; la valeur par défaut est 10.
Liaison virtuelle	
Nom	Si l'ABR n'a pas de lien physique avec la zone dorsale, configurez une liaison virtuelle vers un ABR voisin (dans la même zone) qui a un lien physique vers la zone dorsale. Donnez un Name (Nom) au câble virtuel.
Activer	Activez le lien virtuel.
nominale	Sélectionnez la zone de transit où se trouve l'ABR voisin qui a le lien physique avec la zone dorsale.
ID de routeur	Entrez l'ID de route de l'ABR voisin à l'extrémité distante du lien virtuel.
Profil de la minuterie	Sélectionnez un profil de minuterie ou créez-en un nouveau à appliquer au lien virtuel. Ce profil remplace le profil Global Interface Timer appliqué

Paramètres OSPFv3	Description
	à OSPFv3 et le profil OSPFv3 Interface Timer appliqué à l'interface.
Authentification	Sélectionnez un profil d'authentification ou créez-en un nouveau à appliquer au lien virtuel. Ce profil remplace le profil d'authentification appliqué sous l'onglet Type et le profil d'authentification appliqué à l'interface.
Avancé	
Désactiver R-Bit et v6-Bit	Sélectionnez cette option pour effacer les LSA R-bit et V6-bit dans le routeur envoyés à partir de ce routeur logique pour indiquer que le pare-feu n'est pas actif. Lorsqu'il est dans cet état, le pare-feu participe à OSPFv3 mais n'envoie pas de trafic de transit ou de datagrammes IPv6. Dans cet état, le trafic local est transféré au pare-feu. Cela est utile lors de la maintenance sur un réseau à double interface, car le trafic peut être encore atteint lorsqu'il est réacheminé vers le pare-feu. Voir RFC 5340.
Redémarrage en douceur (Graceful Restart) : activez le redémarrage en douceur.	Activez Le redémarrage progressif pour le routeur logique ; la valeur par défaut est activée.
Enable Helper Mode (Activer le mode Aide)	Activez le mode d'assistance au redémarrage progressif pour le routeur logique ; la valeur par défaut est activée.
Enable Strict LSA Checking (Activer la vérification LSA stricte)	Activer pour que le routeur d'assistance cesse d'exécuter le mode d'assistance et pour provoquer l'arrêt du processus de redémarrage progressif si une publication d'état de liaison indique un changement de topologie réseau ; la valeur par défaut est activée.
Période de grâce (sec)	Entrez le nombre de secondes pendant lesquelles le routeur logique effectuera un redémarrage en douceur si le pare-feu tombe en panne ou devient indisponible. La plage est comprise entre 5 et 1 800 ; la valeur par défaut est 120.
Heure maximale de redémarrage des voisins (sec)	Entrez le nombre de secondes de période de grâce que le routeur logique accepte d'un voisin lorsque le routeur logique est en mode d'assistance. La

Paramètres OSPFv3	Description
	plage est comprise entre 5 et 1,800 ; la valeur par défaut est 140.

Réseau > Routage > Routeurs logiques > RIPv2

Le tableau décrit les paramètres permettant de configurer les interfaces RIPv2 pour un routeur logique sur un moteur de routage avancé.

Paramètres RIPv2	Description
Activer	Activez RIPv2 pour le routeur logique.
Origine des informations par défaut	Annoncez l'itinéraire par défaut même s'il n'existe pas dans le RIB du moteur de routage.
Profil BFD	Appliquez le profil BFD (Bidirectional Forwarding Detection) à RIPv2. Valeur par défaut : **Aucune**.
Minuterie générale globale	Sélectionnez un profil de minuteur global RIPv2 pour établir l'intervalle de mise à jour, l'intervalle d'expiration et l'intervalle de suppression. Valeur par défaut : **Aucune**.
Profil d'authentification	Sélectionnez un profil d'authentification RIPv2 pour appliquer l'authentification MD5 ou par mot de passe simple. Valeur par défaut : **Aucune**.
Profil de redistribution	Sélectionnez un profil de redistribution RIPv2 pour redistribuer les routes statiques IPv4, les routes connectées, les routes IPv4 AFI BGP ou les routes OSPFv2 vers RIPv2. Valeur par défaut : **Aucune**.
Liste globale de distribution entrante	Sélectionnez une liste de distribution pour contrôler les itinéraires entrants acceptés. La valeur par défaut est **Aucun**.
Liste globale de distribution sortante	Sélectionnez une liste de distribution pour contrôler les itinéraires qui sont annoncés aux voisins RIP. Valeur par défaut : **Aucune**.
Interface	Ajoutez une interface qui peut participer au routage RIPv2.
Activer	Activez l'interface pour utiliser RIPv2.

Paramètres RIPv2	Description
Horizon fractionné	Sélectionnez l'une des options suivantes : • **split-horizon :**n'annonce pas un itinéraire de retour sur la même interface où il a été reçu. • **no-split-horizon :**désactive l'horizon fractionné. • **no-split-horizon-with-poison-reverse :**permet à la publicité de revenir sur la même interface où elle a été reçue et définit la métrique pour ces itinéraires sur le maximum autorisé pour RIP, qui est de 16.
Mode	Sélectionnez le mode de l'interface : • **actif :**l'interface annonce les réseaux et envoie des mises à jour RIP. • **passif :**l'interface annonce les réseaux, mais n'envoie pas de mises à jour RIP. (Utile s'il n'y a pas de routeurs RIP pour le réseau, et donc aucune raison d'envoyer des mises à jour RIP sur l'interface.) • **send-only :**peut être utilisé si le pare-feu est un nœud d'extrémité et que vous souhaitez uniquement publier un préfixe en RIP, mais que vous utilisez des itinéraires statiques ou un itinéraire par défaut pour atteindre des préfixes externes.
Authentification	Sélectionnez un profil d'authentification si vous souhaitez remplacer le profil que vous avez appliqué au niveau du routeur logique.
Profil BFD	Par défaut, l'interface hérite du profil BFD que vous avez appliqué au routeur logique pour RIPv2. Vous pouvez également sélectionner un autre profil BFD (tant que BFD n'est pas désactivé pour RIPv2 sur le routeur logique) ou sélectionner **Aucun (Désactiver BFD)** pour désactiver BFD pour l'interface.
Liste de distribution entrante de l'interface : liste d'accès	Sélectionnez une liste d'accès pour contrôler les itinéraires arrivant à cette interface.
Liste de distribution entrante de l'interface - mesure	Spécifiez la mesure à appliquer aux itinéraires entrants ; la plage est comprise entre 1 et 16.

Paramètres RIPv2	Description
Liste de distribution sortante de l’interface : liste d’accès	Sélectionnez une liste d’accès pour contrôler les itinéraires annoncés sur cette interface aux voisins RIP.
Liste de distribution sortante de l’interface - mesure	Préciser la mesure à appliquer aux itinéraires annoncés; la plage est comprise entre 1 et 16.

Réseau > Routage > Routeurs logiques > BGP

Le tableau décrit les paramètres permettant de configurer BGP, les groupes d'homologues, les homologues, les réseaux, les politiques de redistribution et les routes agrégées pour un routeur logique sur un moteur de routage avancé.

Paramètres BGP	Description
Général	
Activer	Activer BGP pour le routeur logique.
ID de routeur	Affectez un ID de routeur au BGP pour le routeur logique; il s'agit généralement d'une adresse IPv4, ce qui permet de garantir que l'ID de routeur est unique.
AS local	Attribuez le système autonome local (AS) auquel le routeur logique appartient sur la base de l’ID du routeur (fourchette pour un numéro AS de 2 octets ou 4 octets de 1 à 4,294, 967, 295).
Profil BFD mondial	Sélectionnez un profil BFD ou créez un nouveau profil BFD à appliquer globalement à BGP. Par défaut **None (disable BFD) (Aucun - BFD désactivé)**.
Installer un itinéraire	Sélectionnez pour installer les itinéraires BGP apprises dans le tableau de routage globale ; par défaut est désactivé.
Basculement rapide	Sélectionnez cette option pour que BGP termine une session avec un homologue adjacent si la liaison vers cet homologue tombe en panne, sans attendre l'expiration du temps d'attente. Le basculement rapide d’EBGP est activé par défaut. Désactivez le basculement rapide EBGP si le pare-feu retire inutilement les routes BGP.
Arrêt approprié	Sélectionnez cette option pour que BGP diminue la préférence des liens d'appairage eBGP lors d'une opération de maintenance afin que BGP puisse choisir et propager des chemins alternatifs basés sur RFC 8326 ; par défaut est désactivé.

Paramètres BGP	Description
Support de multiples AS dans ECMP	Activez si vous avez configuré ECMP et que vous souhaitez exécuter ECMP sur plusieurs systèmes BGP autonomes.
Appliquez le premier AS	Sélectionnez le pare-feu pour qu'il supprime un message de Mise à jour entrant d'un homologue EBGP qui ne répertorie pas le numéro AS de l'homologue EBGP comme premier numéro AS dans l'attribut AS_PATH. (Cette option est activée par défaut.)
Préférence locale par défaut	Indiquez la préférence locale par défaut qui peut être utilisée pour déterminer des préférences entre différents chemins vers la même destination; plage de 0 à 4, 294, 967, 295 ; valeur par défaut de 100.
Activez le redémarrage en douceur	Active le redémarrage en douceur pour BGP afin que le transfert de paquets ne soit pas interrompu pendant un redémarrage BGP (défaut est activé).
Délai d'itinéraire obsolète (en sec.)	Indiquez la durée, en secondes, pendant laquelle un itinéraire peut rester dans l'état Obsolète (intervalle compris entre 1 et 3 600 ; valeur par défaut : 120).
Délai maximum de redémarrage des homologues (en sec.)	Indiquez la durée maximale (en secondes) qu'un équipement local accepte comme délai de redémarrage en période de grâce pour des périphériques homologues (plage comprise entre 1 et 3 600 ; valeur par défaut : 120).
Heure de redémarrage locale	Spécifiez la durée, en secondes, pendant laquelle le périphérique local attend pour redémarrer ; la plage est de 1 à 3 600 ; la valeur par défaut est 120. Cette valeur est annoncée aux homologues.
Sélection du chemin d'accès - Toujours comparer les MED	Activez cette comparaison afin de sélectionner des chemins provenant de voisins de différents systèmes autonomes. L'option Discriminateur à sorties multiples (MED) est une mesure externe qui permet aux voisins de connaître le chemin préféré dans un AS. Une valeur faible est préférée à une valeur élevée.
Comparaison MED déterministe	Sélectionnez un itinéraire parmi ceux qui sont publiés par des homologues iBGP (homologues BGP figurant dans le même AS). La valeur par défaut est activée.
Groupe d'homologues	
Nom	Ajoutez un groupe de pairs BGP par nom (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_), un trait d'union (-) ou un point (.) et contenir zéro ou plusieurs caractères alphanumériques, trait de soulignement, trait d'union et point. L'espace n'est pas autorisée. Le nom doit être unique dans le routeur logique et sur tous les routeurs logiques.

Paramètres BGP	Description
Activer	Activer le groupe d’homologues.
Type	Sélectionnez le type de group d’homologues en tant que **IBGP** (BGP interne, homologues dans un AS) ou **EBGP** (BGP externe, homologues dans deux systèmes autonomes).
Famille d’adresses IPv4	Sélectionnez ou créez un profil AFI IPv4 pour appliquer les paramètres du profil au groupe d’homologues ; par défaut le réglage est sur **Aucun**.
Famille d’adresses IPv6	Sélectionnez ou créez un profil AFI IPv6 pour appliquer les paramètres du profil au groupe d’homologues ; par défaut le réglage est sur **Aucun**.
Profil de filtrage IPv4	Appliquer les éléments d'un profil de filtrage BGP (pour l'IPv4 AFI) au groupe de pairs ; la valeur par défaut est **Aucun**.
Profil de filtrage IPv6	Appliquez les éléments d'un profil de filtrage BGP (pour l'IPv6 AFI) au groupe de pairs ; la valeur par défaut est **Aucun**.
Profil d'authentification	Sélectionnez ou créez un profil d'authentification pour contrôler l'authentification MD5 entre les pairs BGP du groupe de pairs ; la valeur par défaut est **Aucun**.
Profil de la minuterie	Sélectionnez ou créez un profil de minuterie BGP à appliquer au groupe d’homologues, la valeur par défaut est sur **Aucun**. Les temporisateurs affectent les messages keepalive et de mise à jour qui annoncent les itinéraires.
Plusieurs sauts	Définissez la valeur TTL (Time-To-Live) dans l’en-tête IP. La plage va de 0 à 255 ; un réglage de 0 signifie l’utilisation de la valeur par défaut de : 1 pour EBGP ; 255 pour IBGP.
Profil d'amortissement	Sélectionnez ou créez un profil d'amortissement pour déterminer comment pénaliser un itinéraire de battement pour l'empêcher d'être utilisé jusqu'à ce qu'il se stabilise. Valeur par défaut : **Aucune**.
Homologue	
Nom	Ajoutez un pair BGP par nom, qui contient un maximum de 63 caractères. Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_), un trait d’union (-) ou un point (.) et contenir zéro ou plusieurs caractères alphanumériques, trait de soulignement, trait d’union et point. L’espace n'est pas autorisée. Le nom doit être unique dans le routeur logique et sur tous les routeurs logiques.
Activer	Activez l’homologue BGP.

Paramètres BGP	Description
Passif	Sélectionnez cette option pour empêcher l'homologue d'initier une session avec ses voisins ; par défaut est désactivé.
AS Homologue	Saisissez l'AS auquel l'homologue appartient ; plage de 1 à 4, 294, 967, 295.
Adressage de l'homologue	
Hériter	• **Oui**— (par défaut) Sélectionnez cette option pour que l'homologue hérite de la configuration AFI et AFI ultérieure (SAFI) du groupe d'homologues. • **Non :**sélectionnez cette option pour remplacer les paramètres du groupe d'homologues en créant des profils AFI et de filtrage à appliquer à l'homologue.
Adresse locale – Interface	Sélectionnez l'Interface de couche 3 pour laquelle vous configurez BGP. Interfaces configurées avec une adresse IP statique et interfaces configurées en tant que client DHCP disponibles pour la sélection. Si vous sélectionnez une interface dans laquelle DHCP attribue l'adresse, l'adresse **IP** indiquera **aucune**. DHCP attribuera ensuite une adresse IP à l'interface; vous pouvez voir l'adresse lorsque vous affichez **plus de statistiques de fonctionnement** pour le routeur logique.
Adresse IP	Si l'interface possède plus d'une adresse IP, saisissez l'adresse IP et le masque réseau que vous voulez utiliser.
Adresse homologue - Type	Sélectionnez **IP** ou **FQDN** et entrez l'adresse IP ou le FQDN du pair.
Famille d'adresses IPv4	(Disponible si Hériter Non) Sélectionnez le profil **par défaut** , ou créez un profil AFI IPv4 pour appliquer les paramètres du profil au pair, ou sélectionnez **hériter (Hériter du groupe de pairs)**. La valeur par défaut est **aucune (désactiver IPv4 AFI)**.
Famille d'adresses IPv6	(Disponible si hériter non) Sélectionnez ou créez un profil AFI IPv6 pour appliquer les paramètres du profil à l'homologue ou sélectionnez **hériter (hériter du groupe d'homologues)**. La valeur par défaut est **aucune (désactiver IPv6 AFI)**.
Profil de filtrage IPv4	(Disponible si Hériter Non) Sélectionnez ou créez un profil de filtrage BGP qui spécifie l'AFI **IPv4** pour le filtrage de **monodiffusion** ou de **multidiffusion** , et appliquez-le à l'homologue. Vous pouvez également sélectionner **hériter (hériter du groupe de pairs)**. La valeur par défaut est **aucun (Désactiver le filtrage IPv4)**.
Profil de filtrage IPv6	(Disponible si Hériter Non) Sélectionnez ou créez un profil de filtrage BGP qui spécifie l' **IPv6** AFI et **Unicast**, et appliquez-le au pair. Vous pouvez

Paramètres BGP	Description
	également sélectionner **hériter (hériter du groupe de pairs)**. La valeur par défaut est **aucun (Désactiver le filtrage IPv6)**.
Homologue - Options de connexion Ces paramètres remplacent la même option que vous avez réglée pour le groupe d'homologues auquel l'homologue appartient.	
Profil d'authentification	Sélectionnez ou créer un profil d'authentification. La valeur par défaut est **hériter (hériter du groupe de pairs)**, ce qui oblige le pair à utiliser le profil d'authentification spécifié pour le groupe de pairs.
Profil de la minuterie	Sélectionnez ou créez un profil de minuterie. Le paramètre par défaut est **hériter (hériter du groupe de pairs)**, ce qui amène le pair à utiliser le profil de temporisateur spécifié pour le groupe de pairs.
Plusieurs sauts	Spécifiez la valeur TTL dans l'en-tête IP ; la plage est de 0 à 255 ; la valeur par défaut est **hériter (hériter du groupe de pairs)**.
Profil d'amortissement	Sélectionnez ou créez un profil d'amortissement, qui détermine comment pénaliser un itinéraire de battement pour l'empêcher d'être utilisé jusqu'à ce qu'il se stabilise. La valeur par défaut est **hériter (hériter du groupe de pairs)**, ce qui oblige le pair à utiliser le profil d'amortissement spécifié pour le groupe de pairs.
Homologue - avancé	
Activer la détection des boucles côté expéditeur	Sélectionnez pour faire en sorte que le pare-feu vérifie l'attribut AS_PATH d'un itinéraire dans sa base d'information à transférer avant d'envoyer l'itinéraire dans une Mise à jour afin de s'assurer que le numéro AS de l'homologue n'est pas sur la liste AS_PATH. Si c'est le cas, le pare-feu le supprime pour éviter une boucle. La valeur par défaut est activée.
Profil BFD	Sélectionnez ou créez un profil BFD à appliquer au pair ou sélectionnez **Aucun (Désactiver BFD)** pour le pair. La valeur par défaut est **Inherit-vr-global-setting (profil BFD global du protocole hérité)**.
Réseau	
Toujours annoncer l'itinéraire réseau	Sélectionnez cette option pour toujours annoncer les itinéraires réseau configurés aux homologues BGP, qu'ils soient accessibles ou non. Si cette case n'est pas cochée, le pare-feu n'annonce les routes réseau que si elles sont résolues à l'aide de la table de routage locale. La valeur par défaut est activée.
IPv4 ou IPv6	Sélectionnez **IPv4** ou **IPv6** pour spécifier le type de préfixe réseau.

Paramètres BGP	Description
Réseau	**Ajoutez** une adresse de réseau IPv4 ou IPv6 correspondante ; les sous-réseaux avec des adresses de réseau correspondantes sont publiés sur les homologues BGP du routeur logique.
Unicast	Sélectionnez pour installer les itinéraires correspondants dans le tableau de routage Unicast de tous les homologues Unicast.
Multicast	(IPv4 seulement) Sélectionnez pour installer les itinéraires correspondants dans le tableau de routage Unicast de tous les homologues Unicast.
Backdoor	(IPv4 uniquement) Sélectionnez cette option pour une connexion eBGP qui se transforme peut-être en une connexion iBGP (comme OSPF), pour empêcher BGP d'annoncer le préfixe en dehors de l'AS et à la place pour conserver la route dans l'AS. En interne, la distance administrative pour le préfixe est augmentée de sorte que le préfixe n'est pas préféré, mais reste disponible au cas où il serait nécessaire en cas de défaillance de la liaison ailleurs.
Redistribution	
Profil de redistribution IPv4	Sélectionnez ou créez un profil de redistribution BGP (spécifiant l'AFI IPv4) pour redistribuer toute combinaison de routes statiques, connectées ou OSPF vers BGP. Valeur par défaut : **Aucune**.
Profil de redistribution IPv6	Sélectionnez ou créez un profil de redistribution BGP (spécifiant l'AFI IPv6) pour redistribuer toute combinaison de routes statiques, connectées ou OSPFv3 vers BGP. Valeur par défaut : **Aucune**.
Itinéraire agrégé	
Nom	Ajoutez une stratégie d’itinéraire agrégée par nom.
Description	Entrez une description utile de la stratégie d’itinéraire agrégée.
Activer	Sélectionnez pour activer la stratégie d’itinéraire agrégée ; activé par défaut.
Résumé uniquement	Sélectionnez pour annoncer aux voisins uniquement le **préfixe récapitulatif** et non les itinéraires qui ont été récapitulés ; cela réduit le trafic et évite d'augmenter inutilement la taille des tables de routage des voisins (la valeur par défaut est désactivée). Si vous souhaitez publier à la fois l’itinéraire agrégé et les itinéraires individuels qui composent l’itinéraire agrégé, laissez décochée. ***Summary Only** et **Suppress Map** s'excluent mutuellement ; vous ne pouvez pas spécifier les deux.*

Paramètres BGP	Description
	*Si vous souhaitez utiliser **Summary Only**, mais que vous souhaitez également annoncer un itinéraire individuel, vous créez un profil de filtrage BGP qui inclut une carte d'itinéraire **Unsuppress Map** qui correspond à l'itinéraire individuel.*
Définition AS	Sélectionnez pour annoncer le préfixe avec la liste des numéros AS qui composent l'itinéraire agrégé. (La valeur par défaut est désactivée.)
Agréger le même MED uniquement	Sélectionnez cette option pour agréger uniquement les itinéraires qui ont les mêmes valeurs de discriminateur de sorties multiples (MED) ; par défaut est activé.
Type	Sélectionnez le type d'itinéraire agrégé : **IPv4** ou **IPv6**.
Préfixe de résumé	Calculez les itinéraires que vous souhaitez résumer, puis entrez le **préfixe de résumé** qui couvre ces itinéraires, en spécifiant une adresse IP/un masque de réseau ou un objet d'adresse.
Supprimer la carte	Sélectionnez une carte d'itinéraire ou créez-en une nouvelle pour empêcher l'agrégation d'itinéraires individuels ; la valeur par défaut est **Aucun**. *N'oubliez pas que le but de la carte de route Suppress est d'empêcher que certains itinéraires ne soient agrégés dans une annonce. Par conséquent, dans la carte d'itinéraire, vous **autorisez** l'agrégation des itinéraires que vous souhaitez supprimer (vous ne **refusez** pas l'agrégation des itinéraires que vous souhaitez supprimer).* ***Summary Only** et **Suppress Map** s'excluent mutuellement ; vous ne pouvez pas spécifier les deux.*
Carte des attributs	Pour définir les informations d'attribut pour le préfixe récapitulatif, sélectionnez une carte d'itinéraire BGP ou créez-en une nouvelle. N'autorise pas les critères de correspondance. La valeur par défaut est **None**, auquel cas le Summary Prefix aura des attributs par défaut.

Réseau > Routage > Routeurs logiques > Multidiffusion

Le tableau décrit les paramètres de configuration de la multidiffusion IPv4 pour un routeur logique sur un moteur de routage avancé.

Paramètres de multidiffusion IPv4	Description
activer le protocole de multidiffusion	Sélectionnez cette option pour activer le protocole de multidiffusion pour le routeur logique.
Statique	
Nom	**Ajoutez** un mroute par nom (maximum de 31 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-), et contenir zéro ou plusieurs caractères alphanumériques, trait de soulignement (_) ou trait d'union (-). Aucun point (.) ou espace n'est autorisé.
Destination	Entrez la destination (adresse/masque IPv4), qui est la source de multidiffusion vers laquelle vous effectuez une vérification RPF.
Interface	Sélectionnez l'interface de sortie pour un itinéraire de monodiffusion vers la source de multidiffusion.
Saut suivant	Entrez l'adresse IPv4 du tronçon suivant vers la source.
Préférence	Entrez une préférence pour le mroute; la plage est comprise entre 1 et 255.
PIM - Généralités	
Activer	Activez PIM.
Mode de recherche RPF	Sélectionnez le mode de recherche RPF (Reverse-Path Forwarding), qui détermine où le routeur logique cherche à trouver l'interface sortante pour atteindre l'adresse source contenue dans le paquet de multidiffusion. Si l'interface sortante stockée dans le RIB correspond à l'interface sur laquelle le paquet de multidiffusion est arrivé, le routeur logique accepte et transfère le paquet ; sinon, il laisse tomber le paquet. • **mrib-then-urib :**regardez d'abord dans le RIB de multidiffusion, puis dans le RIB de monodiffusion. • **mrib uniquement :**regardez dans le RIB de multidiffusion uniquement. • **urib-only :**regardez uniquement dans le RIB unidiffusion.
Minuterie générale de l'interface	Sélectionnez un profil de minuteur d'interface ou créez-en un nouveau.
Paramètres d'expiration de l'itinéraire (sec)	Spécifiez le nombre de secondes pendant lesquelles un itinéraire de multidiffusion reste dans la mRIB après la fin de la session entre un

Paramètres de multidiffusion IPv4	Description
	groupe de multidiffusion et une source ; la fourchette est de 210 à 7 200; la valeur par défaut est 210.
Gamme SSM multidiffusion	Pour configurer la multidiffusion spécifique à la source (SSM), sélectionnez une liste de préfixes qui spécifie les adresses sources autorisées à fournir le trafic de multidiffusion au récepteur ; la valeur par défaut est **Aucun (pas de liste de préfixes).**
Adresse du groupe	Pour configurer le seuil spt (Shortest-Path Tree) pour un groupe ou un préfixe de multidiffusion, **ajoutez** une adresse de groupe (groupe de multidiffusion ou préfixe pour lequel vous spécifiez l'arborescence de distribution) en sélectionnant une liste de préfixes ou en en créant une nouvelle.
Seuil	Spécifiez le seuil SPT pour le groupe ou le préfixe : • **0 (switch on first data packet) (commuter au premier paquet de données)** (par défaut) : la routeur virtuel bascule de l'arborescence partagée à une distribution en arborescence source pour le groupe ou le préfixe lorsque le routeur virtuel reçoit le premier paquet de données du groupe ou du préfixe. • Entrez le nombre total de kilobits par seconde qui peuvent arriver pour le groupe/préfixe de multidiffusion à n'importe quelle interface et sur n'importe quelle période de temps, sur lequel le routeur logique passe à la distribution SPT pour ce groupe/préfixe de multidiffusion ; est comprise entre 0 et 4 294 967 295. • **never (do not switch to spt) (jamais (ne pas basculer vers SPT))** : le routeur virtuel PIM continue d'utiliser l'arborescence partagée pour transférer les paquets vers le groupe ou le préfixe de multidiffusion.
PIM - Autorisations de groupe	
Liste des groupes sources	Pour accorder l'autorisation aux paquets de multidiffusion de certaines sources et/ou aux paquets de multidiffusion vers certains groupes de multidiffusion de destination de transiter par le routeur logique, sélectionnez une liste d'accès. La valeur par défaut est Aucun (pas de liste d'accès)**,, ce qui signifie qu'aucun groupe source ou multidiffusion spécifique n'est** soumis aux autorisations de groupe PIM.
PIM - Interfaces	
Nom	Entrez un nom pour l'interface (maximum de 31 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-), et contenir zéro ou plusieurs caractères

Paramètres de multidiffusion IPv4	Description
	alphanumériques, trait de soulignement (_) ou trait d'union (-). Aucun point (.) ou espace n'est autorisé.
Description	Entrez une description de l'interface.
Dr priorité	Spécifiez la priorité du routeur désigné de l'interface pour contrôler quel routeur transfère le message de jointure PIM, les messages de registre PIM et les messages d'élagage au point de rendez-vous (RP) ; est comprise entre 1 et 4 294 967 295; la valeur par défaut est 1. Parmi les périphériques PIM sur un réseau local, si la priorité de reprise après sinistre est configurée, le périphérique ayant la valeur de priorité la plus élevée est élu DR.
Envoyer BSM	Sélectionnez cette option pour autoriser la propagation des messages d'amorçage (activée par défaut).
Profil de la minuterie	Le profil de minuteur de l'interface est hérité de la section PIM général, sauf si vous le remplacez en sélectionnant un profil de minuteur pour l'interface ; la valeur par défaut est **Aucun**.
Filtre voisin	Utilisez une liste d'accès pour spécifier les préfixes des périphériques qui sont autorisés à devenir ou refusés de devenir des voisins PIM du routeur logique. La valeur par défaut est **Aucun (pas de liste d'accès).**
¨PIM - Point de rendez-vous	
Type RP	Configurer un RP statique et/ou un RP candidat ; ils ne s'excluent pas mutuellement. • **Static RP (RP Statique)** : Établit un mappage statique d'un RP à des groupes de multidiffusion. Vous devez configurer explicitement le même RP sur les autres routeurs PIM du domaine PIM. • **RP Candidat** • **None**
Interface	Sélectionnez l'interface RP où le RP reçoit et envoie des paquets de multidiffusion. Les types d'interface valides sont les interfaces Layer3 (qui incluent Ethernet, loopback, VLAN, Aggregate Ethernet (AE), tunnel et sous-interfaces).
Adresse	Sélectionnez une longueur d'adresse/préfixe de l'interface ; Les adresses IP de l'interface RP que vous avez sélectionnée remplissent la liste.
Remplacer la RP apprise pour le même groupe	(RP statique uniquement) Sélectionnez cette option pour que ce RP statique serve de RP (au lieu du RP choisi pour les groupes de la liste des groupes).

Paramètres de multidiffusion IPv4	Description
Liste des groupes	Sélectionnez ou créez une liste d'accès pour spécifier les groupes de multidiffusion pour lesquels le RP statique agit en tant que RP. La valeur par défaut est **Aucun (pas de liste d'accès).**
Priorité	(RP candidat uniquement) Spécifiez la priorité du RP candidat ; la plage est comprise entre 0 et 255 ; la valeur par défaut est 192. Une valeur de priorité inférieure indique une priorité plus élevée.
Intervalle de publicité	(RP candidat uniquement) Spécifiez la fréquence (en secondes) à laquelle le RP candidat envoie des publicités à d'autres routeurs ; la portée est comprise entre 1 et 26 214 ; la valeur par défaut est 60.
Adresse IPv4	**Ajoutez** une interface en sélectionnant **l'adresse IPv4** de l'interface.
Liste des groupes	Pour contrôler les groupes que le RP candidat accepte, sélectionnez ou créez une liste de groupes, qui est une liste d'accès IPv4. La valeur par défaut est **Aucun (pas de liste d'accès).** Si aucune liste d'accès n'est appliquée, le routeur logique commence à se présenter comme le RP pour tous les groupes.
Remplacer	Sélectionnez si vous souhaitez que le RP distant que vous avez configuré statiquement serve de RP, au lieu d'un RP qui est appris dynamiquement (élu) pour les groupes de la liste des groupes. La valeur par défaut est désactivée.
IGMP	
activer IGMP	Activez IGMP.
Dynamique	
Interface	**Ajouter** une interface
Version	Sélectionnez IGMP version **2** ou **3**.
Robustesse	Sélectionnez une valeur de robustesse; la plage est de 1 à 7; la valeur par défaut est 2. Augmentez la valeur si le sous-réseau sur lequel le pare-feu se trouve a tendance à perdre des paquets.

Paramètres de multidiffusion IPv4	Description
	*Le (Robustness * QueryInterval) + MaxQueryResponseTime détermine la durée de validité d'un message join sur le routeur logique. Si le routeur logique reçoit un message Leave Group, Robustness * LastMemberQueryInterval est la durée pendant laquelle le routeur logique attend avant de supprimer l'entrée Leave Group. Pour les messages de jointure, une valeur de robustesse de 1 est ignorée. Pour les messages Leave Group, le routeur logique utilise également la valeur Robustness comme nombre de requêtes du dernier membre.*
Filtre de groupe	Sélectionnez ou créez une liste d'accès pour contrôler les préfixes qui utilisent IGMP dynamique. La valeur par défaut est **Aucun (pas de liste d'accès).**
Nombre maximal de groupes	Entrez le nombre maximal de groupes qu'IGMP peut traiter simultanément pour l'interface ; la plage est comprise entre 1 et 65 525; la valeur par défaut est **illimitée**, ce qui signifie la valeur la plus élevée de la plage.
Nombre maximal de sources	Entrez le nombre maximal de sources qu'IGMP peut traiter simultanément pour l'interface ; la plage est comprise entre 1 et 65 525; la valeur par défaut est **illimitée**, ce qui signifie la valeur la plus élevée de la plage.
Profil de requête	Sélectionnez un profil de requête d'interface IGMP que vous avez créé ou créez-en un nouveau à appliquer à l'interface.
supprimer des paquets IGMP sans option Router Alert	Sélectionnez cette option pour exiger que les paquets IGMPv2 ou IGMPv3 entrants aient l'option d'alerte du routeur IP, RFC 2113, sinon ils seront supprimés. La valeur par défaut est désactivée.
Statique	
Nom	**Ajoutez** une interface IGMP statique par nom (maximum de 31 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-), et contenir zéro ou plusieurs caractères alphanumériques, trait de soulignement (_) ou trait d'union (-). Aucun point (.) ou espace n'est autorisé.
Interface	Sélectionnez l'interface comme interface IGMP statique.
Adresse du groupe	Entrez l'adresse du groupe de multidiffusion des membres IGMP statiques.

Paramètres de multidiffusion IPv4	Description
Adresse source	Entrez l’adresse source à partir de laquelle les membres IGMP statiques reçoivent les multidiffusions.
MSDP - Généralités	
Activer	Activez le protocole MSDP (Multicast Source Discovery Protocol) pour le routeur logique.
Minuterie globale	Sélectionnez un profil du minuteur MSDP global, sélectionnez le profil **default (par défaut)** ou créez un profil du minuteur MSDP global. Si vous sélectionnez le profil **default (par défaut)** l’intervalle Keep Alive est défini sur 60, Message Timeout est défini sur 75 et Connection Retry Interval est défini sur 30. La valeur par défaut est **None (Aucun)**, ce qui signifie que les valeurs par défaut sont appliquées.
Authentification globale	Sélectionnez un profil d’authentification ou créez-en un nouveau. Valeur par défaut : **Aucune**.
ID d’expéditeur : interface	Sélectionnez l’interface que le routeur logique utilise comme interface RP dans les messages Source Active (SA). Si vous spécifiez une adresse IP pour l’ID d’origine, vous devez configurer une interface IP d’origine. Si aucune interface n’est configurée, l’adresse IP doit rester vide.
ID d’origine : IP	Sélectionnez ou entrez l’adresse IP (avec la longueur du préfixe) que le routeur logique utilise comme adresse RP dans les messages SA. Si aucune adresse IP Originator n'est configurée, le routeur logique utilise l'adresse PIM RP pour encapsuler le message SA.
MSDP - Homologues	
Homologue	Ajoutez un nom d’homologue (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d’union (-) et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement ou de trait d’union. Aucun point (.) ou espace n’est autorisé.
Interface source	Entrez l’interface source utilisée pour établir la connexion MSDP sur TCP avec son homologue MSDP.
Interface source : IP	Sélectionnez l’adresse IP de l’interface source. Valeur par défaut : **Aucune**.
Adresse homologue - Type	Sélectionnez le type d’adresse homologue : • **IP** - (par défaut) et sélectionnez un objet d'adresse ou entrez une adresse IP.

Paramètres de multidiffusion IPv4	Description
	• **FQDN** — Sélectionnez ou saisissez le nom de domaine complet de l'homologue. La liste déroulante affiche tous les noms FQDN configurés comme objets d'adresse.
AS distant	Entrez le numéro de système autonome BGP de l'AS distant où se trouve l'homologue MSDP.
Authentification	Choisissez l'une des actions suivantes : • Sélectionnez un profil d'authentification à appliquer à ce pair, qui remplace le profil d'authentification globale que vous avez appliqué à MSDP sur la page Général. • **inherit (inherit from global authentication) (Hériter (hériter de l'authentification globale))**: profil d'authentification globale (par défaut). • **None (Aucun)** : pour désactiver l'authentification auprès de cet homologue, qui remplace le profil d'authentification global.
Max SA	Entrez le nombre maximal d'entrées Source-Active (SA) que le cache SA acceptera de cet homologue MSDP. La plage est comprise entre 0 et 1,024 ; la valeur par défaut est 0. Une fois ce maximum atteint, les nouveaux messages SA de ce pair sont supprimés.
Filtre SA entrant homologue	Sélectionnez une liste d'accès ou créez une nouvelle liste d'accès pour filtrer les messages SA entrants (bloquer les groupes indésirables) provenant de cet homologue. Valeur par défaut : **Aucune**. La liste d'accès peut spécifier des adresses source dans une paire (S,G) à filtrer, ou des adresses destination (groupe) dans une paire (S,G) à filtrer, ou les deux.
Filtre SA sortant homologue	Sélectionnez une liste d'accès ou créez une nouvelle liste d'accès pour filtrer les messages SA sortants (bloquer les groupes indésirables) propagés à cet homologue. Valeur par défaut : **Aucune**. La liste d'accès peut spécifier des adresses source dans une paire (S,G) à filtrer, ou des adresses destination (groupe) dans une paire (S,G) à filtrer, ou les deux.

Réseau > Routage > Profiles de routage

Sur un moteur de routage avancé, vous créez des profils de routage pour appliquer facilement et de manière cohérente des attributs à BGP, BFD, OSPF, OSPFv3, multidiffusion, RIPv2 et filtres.

Réseau > Routage > Profiles de routage > BGP

Pour un routeur logique, utilisez les profils de routage BGP afin d'appliquer efficacement la configuration à n'importe quels groupes d'homologues BGP, homologues ou règles de distribution. Par exemple, vous pouvez appliquer un profil de minuteur, un profil d'authentification et des profils de filtrage BGP à un groupe d'homologues BGP ou à un homologue. Vous pouvez appliquez un profil de Famille d'adresses (AFI) pour IPv4 et Ipv6 à un groupe d'homologues ou à un homologue. Vous pouvez appliquer un profil de redistribution pour IPv4 et IPv6 à la redistribution BGP.

Profils de routage BGP	Description
BGP Auth Profile (Profil d'authentification)	
Nom	Saisissez un nom pour le profil d'authentification (63 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_), un trait d'union (-) ou un point (.) et contenir zéro ou plusieurs caractères alphanumériques, trait de soulignement, trait d'union et point. L'espace n'est pas autorisée.
Phrase secrète	Saisissez la Phrase secrète et **Confirm Secret (confirmez la phrase secrète)** La phrase secrète sert de clé lors de l'authentification MD5.
Profil de la minuterie BGP	
Nom	Saisissez un nom pour le profil de minuterie (63 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_), un trait d'union (-) ou un point (.) et contenir zéro ou plusieurs caractères alphanumériques, trait de soulignement, trait d'union et point. L'espace n'est pas autorisée.
Intervalle KeepAlive (en sec.)	Saisissez l'intervalle après lequel les itinéraires d'un homologue sont supprimés conformément au paramètre de durée d'attente (intervalle compris entre 0 et 1 200 ; valeur par défaut : 30).
Temps d'attente (en sec.)	Saisissez la durée du temps, en secondes, qui peut s'écouler entre des messages Keepalive ou Update successifs émis par l'homologue avant la fermeture de la connexion (plage comprise entre 3 et 3 600 ; valeur par défaut : 90).
Intervalle de nouvelle tentative de reconnexion	Entrez le nombre de secondes à attendre à l'état Inactif avant de réessayer de vous connecter à l'homologue (plage comprise entre 1 et 3 600 ; la valeur par défaut est 15).

Profils de routage BGP	Description
Délai avant ouverture (en sec.)	Entrez le nombre de secondes de délai entre l'ouverture de la connexion TCP à l'homologue et l'envoi du premier message BGP Open pour établir une connexion BGP (plage comprise entre 0 et 240 ; la valeur par défaut est 0).
Interval de publication minimum de l'itinéraire (en sec.)	Saisissez la quantité de temps, en secondes, qui doit passer entre deux messages de mise à jour successifs (qu'un haut-parleur BGP [le pare-feu] envoie à un homologue BGP) qui publie des itinéraires ou des retraits d'itinéraires (la plage est comprise entre 1 et 600 ; valeur par défaut : 30).
BGP Address Family Profile (Profil de famille d'adresses BGP)	
Nom	Saisissez un nom pour le profil d'identifiant de la famille d'adresses (AFI) (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_), un trait d'union (-) ou un point (.) et contenir zéro ou plusieurs caractères alphanumériques, trait de soulignement, trait d'union et point. L'espace n'est pas autorisée.
AFI	Sélectionnez le type de profil AFI (**IPv4** ou **IPv6**).
unicast / multicast	Sélectionnez le type SAFI (Address Family Identifier) suivant.
Activer SAFI	Sélectionnez le profil pour activer la monodiffusion et/ou la multidiffusion SAFI. Au moins un SAFI doit être activé pour que le profil BGP soit valide ; vous pouvez activer les deux SAFI.
Reconfiguration logicielle de l'homologue avec des itinéraires stockés	Sélectionnez cette option pour que le pare-feu effectue une réinitialisation logicielle de lui-même après la mise à jour des paramètres de l'un de ses homologues BGP. (La valeur par défaut est activée.)
Publier tous les chemins d'accès aux homologues	Annoncez tous les chemins d'accès aux voisins afin de préserver les fonctionnalités multichemins au sein d'un réseau.
Annoncez le meilleur chemin pour chaque AS voisin	Activez pour vous assurer que BGP publie le meilleur chemin d'accès pour chaque AS voisin et non le chemin d'accès générique pour tous les systèmes autonomes. Désactivez si vous souhaitez publier le même chemin d'accès pour tous les systèmes autonomes.
Remplacer les ASN dans les mises à jour sortantes si AS-Path (chemin d'accès AS) est égal à Remote-AS (AS à distance)	Vous pouvez utiliser l'option de contrôle prioritaire de l'AS BGP si vous avez plusieurs sites appartenant au même AS (AS 64512, par exemple) et il y a un autre AS entre eux. Un routeur entre les deux sites reçoit une mise à jour publiant un itinéraire qui peut accéder à AS 64512. Afin d'éviter que le deuxième site annule la mise à jour parce qu'elle est aussi dans AS 64521, le routeur intermédiaire remplace AS 64512 par son propre ASN, AS 64522, par exemple.

Profils de routage BGP	Description
Client réflecteur de l’itinéraire	Permet de faire des homologues BGP un client de réflecteur de route BGP dans un réseau iBGP.
Point de départ de l’itinéraire par défaut	Sélectionnez pour publier tous les itinéraires par défaut. Désactivez si vous voulez publier uniquement les itinéraires vers une destination spécifique.
Carte d’itinéraire d’origine par défaut	Appliquez une carte d’itinéraire au champ Itinéraire par défaut d’origine, ce qui vous permet de spécifier les types d’itinéraires par défaut que vous souhaitez publier.
Autorisez AS dans	Indiquez si vous autorisez les itinéraires qui incluent le numéro du système autonome (AS) du pare-feu : • **Origin (Origine)** : Accepte les itinéraires même si l’AS du pare-feu est présent dans AS_PATH. • **Occurrence** : nombre de fois où l’AS du pare-feu peut être dans un AS_PATH. • **None (Aucun)** : (paramètre par défaut) Aucune action.
Préfixes numériques	Entrez le nombre maximal de préfixes à accepter de l’homologue ; est comprise entre 1 et 4 294 967 295; la valeur par défaut est 1 000.
Seuil (%)	Saisissez le pourcentage de seuil du nombre maximum de préfixes. Si l’homologue publie plus que le seuil, le pare-feu applique l’Action indiquée (avertissement ou redémarrage). Plage comprise entre 1 et 100.
Action	Indiquez l’action que le pare-feu prend sur la connexion BGP après que le nombre maximum de préfixes ait été ateint. **Warning Only (Avertissement uniquement)** message dans les journaux ou **Restart (Redémarrer)** la connexion d’homologue BGP.
Saut suivant	Sélectionnez le saut suivant : • **Aucun**: le tronçon suivant d’origine est conservé. • **Self (Indépendant)** : désactivez le calcul du saut suivant et publiez les itinéraires avec le saut local suivant. • **Self Force (Force indépendante)** : Force le saut suivant en mode indépendant pour les itinéraires repris.
Supprimer l'AS privé	Pour que BGP supprime des numéros d’AS privés provenant de l’attribut AS_PATH des mises à jour que le pare-feu envoie à un homologue d'un autre AS, sélectionnez parmi ce qui suit : • **All (Tous)**: Supprime tous les numéros AS. • **Replace AS (Remplacer AS)** : Remplace tous les numéros AS par le numéro AS du pare-feu.

Profils de routage BGP	Description
	• **None (Aucun)** : (paramètre par défaut) Aucune action.
Envoyez la communauté	Sélectionnez le type d'attribut de communauté BGP à envoyer dans les messages de mise à jour sortants : • **All (toutes)** : envoie toutes les communautés. • **Both (les deux)** : envoie les communautés standard et étendues. • **Extended (étendues)** : envoie les communautés étendues. • **Large (grandes)** : envoie les grandes communautés. • **Standard** : envoie les communautés standard. • **None (Aucune)**: n'envoie aucune communauté.
Liste orf	Annoncez la capacité du groupe d'homologues ou de l'homologue à envoyer une liste de préfixes et/ou à recevoir une liste de préfixes pour implémenter le filtrage de routage sortant (ORF) à la source, et ainsi minimiser l'envoi ou la réception de préfixes indésirables dans les mises à jour. Sélectionnez l'une des options suivantes : • **none**: (paramètre par défaut) Le groupe d'homologues ou l'homologue (où ce profil AFI est appliqué) n'a pas de fonctionnalité ORF. • **les deux**: annoncez que le groupe d'homologues ou l'homologue peut **envoyer** et préfixer une liste et **recevoir** une liste de préfixes pour implémenter ORF. • **recevoir** : annonce que le groupe d'homologues ou l'homologue peut recevoir une liste de préfixes pour implémenter ORF. L'homologue local reçoit la capacité ORF et la liste de préfixes de l'homologue distant, qu'il implémente en tant que filtre d'itinéraire sortant. • **envoyer** : annonce que le groupe d'homologues ou l'homologue peut envoyer une liste de préfixes pour implémenter ORF. L'homologue distant (avec capacité de réception) reçoit la fonctionnalité ORF et implémente la liste de préfixes qu'il a reçue en tant que filtre d'itinéraire sortant lors de la publicité achemine vers l'expéditeur. Mettre en œuvre ORF en procédant comme suit : **1.** Spécifiez la fonctionnalité ORF dans le profil Famille d'adresses. **2.** Pour un groupe d'homologues ou un homologue qui est un expéditeur, créez une liste de préfixes contenant l'ensemble des préfixes que le groupe d'homologues/homologues souhaite recevoir. **3.** Créez un profil de filtrage BGP et, dans la liste des préfixes entrants, sélectionnez la liste de préfixes que vous avez créée. **4.** Pour le groupe d'homologues BGP, sélectionnez le profil de famille d'adresses que vous avez créé pour l'appliquer au groupe d'homologues. Dans le cas de l'expéditeur, sélectionnez également le profil de filtrage que vous avez créé (qui indique la liste des préfixes). Si le groupe d'homologues ou l'homologue est un récepteur ORF

Profils de routage BGP	Description
	uniquement, il n’a pas besoin du profil de filtrage ; il n’a besoin que du profil Famille d’adresses pour indiquer la capacité de réception ORF.
Profil d’amortissement BGP	
Nom	Saisissez un nom pour le profil de d’amortissement (63 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_), un trait d’union (-) ou un point (.) et contenir zéro ou plusieurs caractères alphanumériques, trait de soulignement, trait d’union et point. L’espace n'est pas autorisée.
Description	Entrez une description pour le profil Amortissement.
Supprimer la limite	Entrez la valeur de suppression (valeur cumulée des pénalités pour battement), à quel point toutes les routes provenant d’un homologue sont amorties. La plage est comprise entre 1 et 20 000 ; la valeur par défaut est 2 000.
Limite de réutilisation	Entrez la valeur qui contrôle quand un itinéraire peut être réutilisé en fonction de la procédure décrite pour Half Life ; la plage est de 1 à 20 000; la valeur par défaut est 750.
Demi-vie (min)	Entrez le nombre de minutes pour la demi-vie afin de contrôler la mesure de stabilité (pénalité) appliquée à un itinéraire de battement. La plage est comprise entre 1 et 45 ; la valeur par défaut est 15. La mesure de stabilité commence à 1 000. Une fois qu’un itinéraire pénalisé s’est stabilisé, le compte à rebours half life jusqu’à son expiration, auquel cas la mesure de stabilité suivante appliquée au routeur ne représente que la moitié de la valeur précédente (500). Les coupes successives se poursuivent jusqu’à ce que la mesure de stabilité soit inférieure à la moitié de la limite de réutilisation, puis la mesure de stabilité est supprimée du routeur.
Temps maximum de suppression (min)	Entrez le nombre maximal de minutes pendant lesquelles un itinéraire peut être supprimé, quel que soit son instabilité. La plage est comprise entre 1 et 255 ; la valeur par défaut est 60.
BGP Redistribution Profile (Profil de redistribution BGP)	
Nom	Saisissez un nom pour le profil de redistribution (63 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_), un trait d’union (-) ou un point (.) et contenir zéro ou plusieurs caractères alphanumériques, trait de soulignement, trait d’union et point. L’espace n'est pas autorisée.
IPv4 ou IPv6	Sélectionnez l’identifiant de la famille d’adresses (AFI) IPv4 ou IPv6 pour indiquer le type d’itinéraire distribué.

Profils de routage BGP	Description
Statique	Sélectionnez **Statique** et **Activer** pour redistribuer des itinéraires statiques IPv4 ou IPv6 (qui correspondent à l'AFI que vous avez sélectionné) vers BGP.
Mesure	Saisissez la mesure à appliquer aux itinéraires statiques qui sont redistribués dans BGP (plage de 1 à 65 535).
Itinéraire-Carte	Sélectionnez une **carte routière pour** spécifier les critères de correspondance qui déterminent les itinéraires statiques à redistribuer. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué.
Connecté	Sélectionnez **Connecté** et **Activer** pour redistribuer les itinéraires connectés IPv4 ou IPv6 (qui correspondent à l'AFI que vous avez sélectionné) vers BGP.
Mesure	Saisissez la mesure à appliquer aux itinéraires connectés qui sont redistribués dans BGP (plage de 1 à 65 535).
Itinéraire-Carte	Sélectionnez une **carte routière** pour spécifier les critères de correspondance qui ont déterminé les itinéraires connectés à redistribuer. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué.
OSPF	(IPv4 uniquement) Sélectionnez **OSPF** et **Activer pour redistribuer les** itinéraires OSPFv2 vers BGP.
Mesure	Saisissez la mesure à appliquer aux itinéraires OSPF qui sont redistribués dans BGP (plage de 1 à 65 535).
Itinéraire-Carte	Sélectionnez une **carte routière** pour spécifier les critères de correspondance qui déterminent les itinéraires OSPF à redistribuer. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué.
RIP	(IPv4 uniquement) Sélectionnez **RIP** et **Activer** pour redistribuer les itinéraires RIP vers BGP.

Profils de routage BGP	Description
Mesure	Saisissez la mesure à appliquer aux itinéraires RIP qui sont redistribués dans BGP (plage de 1 à 65 535).
Itinéraire-Carte	Sélectionnez une **carte routière** pour spécifier les critères de correspondance qui déterminent les itinéraires RIP à redistribuer. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué.
OSPFv3	(IPv6 uniquement) Sélectionnez **OSPFv3** et **Activer pour redistribuer les** itinéraires OSPFv3 vers BGP.
Mesure	Saisissez la mesure à appliquer aux itinéraires OSPFv3 qui sont redistribués dans BGP (plage de 1 à 65 535).
Itinéraire-Carte	Sélectionnez une **carte de routage** pour spécifier les critères de correspondance qui déterminent les itinéraires OSPFv3 à redistribuer. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué.
Profil de filtrage BGP	
Nom	Entrez un nom pour le profil de filtrage BGP (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_), un trait d'union (-) ou un point (.) et contenir zéro ou plusieurs caractères alphanumériques, trait de soulignement, trait d'union et point. L'espace n'est pas autorisée.
Description	Entrez une description pour le profil de filtrage BGP.
AFI	Sélectionnez l'identifiant de la famille d'adresses (AFI) **IPv4** ou **IPv6** pour indiquer le type d'itinéraire filtré.
Liste de filtres entrants **monodiffusion**	Sélectionnez une liste d'accès AS Path ou créez-en une nouvelle pour spécifier que, lors de la réception d'itinéraires d'homologues, seuls les itinéraires ayant le même AS Path sont importés à partir du groupe d'homologues ou de l'homologue, c'est-à-dire ajoutés au RIB BGP local.
Liste de distribution entrante	Utilisez une liste d'accès (adresse source uniquement , et non adresse de destination) pour filtrer les informations de routage BGP reçues par BGP.

Profils de routage BGP	Description
	Mutuellement exclusif avec la liste de préfixes entrants dans un seul profil de filtrage.
Liste des préfixes entrants	Utilisez une liste de préfixes pour filtrer les informations de routage BGP que BGP reçoit, en fonction d'un préfixe réseau. Mutuellement exclusif avec la liste de distribution entrante dans un seul profil de filtrage.
Carte de l'itinéraire entrant	Utilisez une carte d'itinéraire pour avoir encore plus de contrôle sur les itinéraires autorisés dans le RIB BGP local (critères de correspondance) et pour définir des attributs pour les itinéraires (options définies). Par exemple, vous pouvez contrôler la préférence d'itinéraire en faisant précéder un AS du chemin AS d'un itinéraire.
Liste des filtres sortants	Sélectionnez une liste d'accès AS Path ou créez une nouvelle liste d'accès AS Path pour spécifier que seuls les itinéraires avec le même AS Path sont publiés sur un routeur homologue (groupe homologue ou homologue où ce filtre est appliqué).
Liste de distribution sortante	Utilisez une liste d'accès pour filtrer les informations de routage BGP que BGP publie, en fonction de l'adresse IP de la destination. Mutuellement exclusif avec la liste de préfixes sortants dans un seul profil de filtrage.
Liste des préfixes sortants	Utilisez une liste de préfixes pour filtrer les informations de routage BGP que BGP annonce, en fonction d'un préfixe réseau. Mutuellement exclusif avec la liste de distribution sortante dans un seul profil de filtrage.
Carte de l'itinéraire sortant	Utilisez une carte d'itinéraire pour avoir encore plus de contrôle sur les itinéraires que BGP annonce (critères de correspondance) et pour définir des attributs pour les itinéraires annoncés.
Publicité conditionnelle — Existe—Carte d'existence	Sélectionnez ou créez une carte d'itinéraire pour spécifier les critères de correspondance de la publication conditionnelle. Si ces itinéraires existent dans le RIB BGP local, les itinéraires spécifiés par la carte de publicité sont publiés. Seule la partie Match de la carte d'itinéraire dans ce champ prend effet ; la partie Définir est ignorée.
Publicité conditionnelle — Existe — Annonce de carte	Sélectionnez ou créez une carte d'itinéraire pour spécifier les itinéraires à publier dans le cas où la condition est remplie (les itinéraires de la carte Existante existent dans le RIB BGP local). Seule la partie Match de la carte d'itinéraire dans ce champ prend effet ; la partie Définir est ignorée.
Publicité conditionnelle —Non-exist—Carte inexistante	Sélectionnez ou créez une carte d'itinéraire pour spécifier les critères de correspondance de la publication conditionnelle. Si ces itinéraires n'existent pas dans le RIB BGP local, les itinéraires spécifiés par la carte de publicité sont publiés. Seule la partie Match de la carte d'itinéraire dans ce champ prend effet ; la partie Définir est ignorée.

Profils de routage BGP	Description
Publicité conditionnelle—Inexistant—Carte de publicité	Sélectionnez ou créez une carte d'itinéraire pour spécifier les itinéraires à publier dans le cas où la condition est remplie (les itinéraires de la carte inexistante n'existent pas dans le RIB BGP local). Seule la partie Match de la carte d'itinéraire dans ce champ prend effet ; la partie Définir est ignorée.
Rétablir la Carte	Sélectionnez ou créez une carte d'itinéraire des itinéraires que vous souhaitez désactiver de l'agrégation d'itinéraires ou de l'amortissement d'itinéraires et ainsi les publier.
Multidiffusion :hériter de la monodiffusion	(IPv4 AFI uniquement) Sélectionnez cette option pour hériter des paramètres de monodiffusion pour le filtrage des itinéraires de multidiffusion. Sinon, configurez les filtres de multidiffusion comme décrit dans ce tableau pour les filtres de monodiffusion.

Réseau > Routage > Profiles de routage > BFD

Créez un profil de détection de transfert bidirectionnel.

Profils de routage BFD	Description
Nom	Saisissez un nom pour le profil BFD (63 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-), et contenir zéro ou plusieurs caractères alphanumériques, trait de soulignement (_) ou trait d'union (-). Aucun point (.) ou espace n'est autorisé.
Mode	Sélectionnez le mode : • **Active (Actif)** : (par défaut) la BFD initie l'envoi de paquets de contrôle vers l'homologue. Au moins l'un des homologues BFD doit être actif ; ils peuvent être actifs tous les deux. • **Passive (Passif)** : la BFD attend que l'homologue envoie des paquets de contrôles et réponde comme il se doit.
Intervalle Tx minimum souhaité (ms)	Il s'agit de l'intervalle minimal, en millisecondes, auquel vous voulez que le protocole BFD (appelé BFD) envoie des paquets de contrôles BFD ; vous négociez ainsi l'intervalle de transmission avec l'homologue. La gamme pour les séries PA-7000,

Profils de routage BFD	Description
	PA-5200, PA-5400 et PA-3400 est comprise entre 50 et 10 000 ; la gamme pour la série PA-3200 est de 100 à 10 000; la gamme PA-400 est de 150 à 10 000; la plage pour la série VM est comprise entre 200 et 10 000 ; La valeur par défaut est 1 000.
Intervalle Rx minimum souhaité en ms).	Intervalle minimum, en millisecondes, auquel la BFD peut recevoir les paquets de contrôles BFD. La gamme pour les séries PA-7000, PA-5200, PA-5400 et PA-3400 est comprise entre 50 et 10 000 ; la gamme pour la série PA-3200 est de 100 à 10 000; la gamme PA-400 est de 150 à 10 000; la plage pour la série VM est comprise entre 200 et 10 000 ; La valeur par défaut est 1 000.
Multiplicateur de délai de détection	La plage est comprise entre 2 et 255 ; la valeur par défaut est 3. Le système local calcule le délai de détection en tant que **Multiplicateur de délai de détection** reçu du système distant multiplié par l'intervalle de transmission du système distant convenu (la valeur la plus élevée entre le **Intervalle de réception minimum requis** et le dernier **Intervalle de transmission minimum souhaité)** reçu. Si la BFD ne reçoit pas de paquet de contrôles BFD de son homologue avant l'expiration du délai de détection, c'est qu'un échec a eu lieu.
Temps d'attente (ms)	Délai, en millisecondes, entre l'apparition d'une liaison et la transmission des paquets de contrôles BFD par la BFD. Le **Hold Time (Temps d'attente)** ne s'applique qu'au mode **Actif** de la BFD. Si la BFD reçoit des paquets de contrôles BFD pendant le Hold Time (Temps d'attente), ceux-ci sont ignorés. La fourchette est de 0 à 120 000; le paramètre défini par défaut de 0 signifie qu'aucun Hold Time (Temps d'attente) n'est utilisé ; le pare-feu envoie et reçoit les paquets de contrôles BFD immédiatement après l'établissement de la liaison.
Activer les sauts multiples	Activez BFD sur BGP sauts multiples
TTL Rx minimum	Saisissez Time-to-Live minimum (nombre de sauts) que la BFD acceptera (recevra) dans un

Profils de routage BFD	Description
	paquet de contrôles BFD lorsque le protocole BGP prend en charge la BFD à sauts multiples. La plage est de 1 à 254; il n’y a pas de valeur par défaut.

Réseau > Routage > Profiles de routage > OSPF

Ajoutez des profils de routage OSPF pour configurer efficacement OSPFv2 pour un routeur logique.

Profils de routage OSPF	Description
Profil de minuterie globale OSPF	
Nom	Saisissez un nom pour le profil (63 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d’union (-) et contenir zéro ou plusieurs caractères alphanumériques, un trait de soulignement (_) ou un trait d’union(-). Aucun point (.) ou espace n’est autorisé.
Arrivée minimale LSA	Entrez la durée minimale (en secondes) entre les transmissions de deux instances du même LSA (même ID de routeur publicitaire, même type de LSA et même ID LSA). Si le même LSA arrive plus tôt que l’intervalle configuré, le LSA est supprimé. La plage est comprise entre 1 et 10 ; la valeur par défaut est 5. LSA min-arrival est équivalent à MinLSInterval dans RFC 2328. Des valeurs inférieures peuvent être utilisées pour réduire les délais de reconvergence en cas de modifications de topologie.
SPF : délai initial	Entrez le délai initial (en secondes) à partir du moment où le routeur logique reçoit un changement de topologie jusqu’à ce qu’il effectue le calcul SPF (Shortest Path First) ; la plage est comprise entre 0 et 600; la valeur par défaut est 5. Des valeurs inférieures permettent une reconvergence OSPF plus rapide. Les routeurs échangeant du trafic avec le pare-feu doivent utiliser la même valeur afin d'optimiser les délais de convergence.
Temps d’attente initial	Entrez le temps de maintien initial (en secondes) entre les calculs SPF consécutifs; la plage est comprise entre 0 et 600; la valeur par défaut est 5.
Durée d’attente maximale	Entrez le temps de maintien maximal (en secondes), qui est la valeur la plus élevée à laquelle le temps de maintien est limité

Profils de routage OSPF	Description
	jusqu’à ce qu’il reste stable ; la plage est comprise entre 0 et 600; la valeur par défaut est 5.
Profils d’authentification de l’interface OSPF	
Nom	Saisissez un nom pour le profil d’authentification (63 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d’union (-) et contenir zéro ou plusieurs caractères alphanumériques, un trait de soulignement (_) ou un trait d’union(-). Aucun point (.) ou espace n’est autorisé.
Type	Sélectionnez un type d’authentification : • **Mot de passe (Password)** : entrez un **mot de passe** (huit caractères maximum) et **confirmez le mot de passe**. • **MD5 :ajoutez** un **ID de clé MD5** (plage comprise entre 0 et 255) et une **clé** (16 caractères maximum ; tout caractère à l’exception de l’espace). Sélectionnez **Préféré** pour préférer une clé MD5 aux autres touches MD5.
Profil de la minuterie de l’interface OSPF	
Nom	Saisissez un nom pour le profil (63 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d’union (-) et contenir zéro ou plusieurs caractères alphanumériques, un trait de soulignement (_) ou un trait d’union(-). Aucun point (.) ou espace n’est autorisé.
Intervalle Hello	Entrez l’intervalle (en secondes) entre les paquets Hello que le pare-feu envoie une interface pour maintenir les relations de voisinage ; la plage est comprise entre 1 et 3600 ; la valeur par défaut est 10.
Nombre de morts	Saisissez le nombre de fois que l'intervalle Hello peut se produire pour un voisin sans qu'OSPF ne reçoive un paquet Hello du voisin, avant qu'OSPF ne considère ce voisin comme inactif ; la plage est de 3 à 20 ; la valeur par défaut est 4.
Intervalle de retransmission	Entrez le nombre de secondes entre les retransmissions LSA vers les routeurs adjacents ; la plage est comprise entre 1 et 1800; la valeur par défaut est 5.
Délai de transmission	Entrez le nombre de secondes nécessaires pour transmettre un paquet de mise à jour de l’état de liaison sur l’interface. L’âge des annonces d’état de liaison dans le paquet de mise à jour

Profils de routage OSPF	Description
	est incrémenté de ce numéro avant d'être transmis ; la plage est comprise entre 1 et 1800; la valeur par défaut est 1.
Délai de redémarrage approprié Hello (sec)	Saisissez Graceful Restart Hello Delay (en secondes) (Temporisation de redémarrage en douceur Hello) qui s'applique à une interface OSPF lorsque la haute disponibilité active / passive est configurée. La temporisation de redémarrage en douceur Hello est la durée pendant laquelle le pare-feu envoie des paquets LSA à des intervalles de 1 seconde. Pendant cette période, aucun paquet Hello n'est envoyé avant le redémarrage du pare-feu. Lors du redémarrage, le minuteur d'inactivité (qui correspond à l'Intervalle Hello multiplié par le Nombre de pertes) effectue un compte à rebours. Si la valeur du minuteur d'inactivité est trop faible, l'adjacence devient inactive pendant le redémarrage en douceur en raison de la temporisation Hello. Par conséquent, il est recommandé que la valeur du minuteur d'inactivité soit au moins quatre fois celle de la Graceful Restart Hello Delay (Temporisation de redémarrage en douceur Hello). Par exemple, un Intervalle Hello de 10 secondes et un Nombre de pertes de 4 sont égaux à une valeur de minuteur d'inactivité de 40 secondes. Si la Temporisation de redémarrage en douceur Hello est définie sur 10 secondes, la valeur du minuteur d'activité de 40 secondes est suffisante pour que l'adjacence ne devienne pas inactive. La plage est comprise entre 1 et 10 ; la valeur par défaut est 10.
Profil de redistribution OSPF	
Nom	Saisissez un nom pour le profil (63 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et contenir zéro ou plusieurs caractères alphanumériques, un trait de soulignement (_) ou un trait d'union(-). Aucun point (.) ou espace n'est autorisé.
IPv4 Statique	Sélectionnez cette option pour pouvoir configurer cette partie du profil.
Activer	Activez la redistribution d'itinéraire statique IPv4 vers OSPF.
Mesure	Précisez la mesure à appliquer aux itinéraires statiques qui sont redistribués dans OSPF (plage de 1 à 65 535).
Type de mesure	Sélectionnez : • **Type 1**

Profils de routage OSPF	Description
	• **Type 2** (par défaut)
Redistribuer la carte d’itinéraire	Sélectionnez ou créez une carte d’itinéraire de redistribution pour contrôler les routes statiques IPv4 qui sont redistribuées à OSPF et définir leurs attributs. Valeur par défaut : **Aucune**. Si la configuration de l’ensemble de cartes d’itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l’itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l’itinéraire redistribué. De même, le Type de métrique dans la configuration de l’ensemble de cartes routières a priorité sur le Type de mesure configuré dans ce profil de redistribution.
Connecté	Sélectionnez cette option pour pouvoir configurer cette partie du profil.
Activer	Activez la redistribution des itinéraires connectés vers OSPF.
Mesure	Saisissez la mesure à appliquer aux itinéraires connectés qui sont redistribués dans BGP (plage de 1 à 65 535).
Type de mesure	Sélectionnez : • **Type 1** • **Type 2** (par défaut)
Redistribuer la carte d’itinéraire	Sélectionnez ou créez une carte d’itinéraire de redistribution pour contrôler les itinéraires connectés qui sont redistribués à OSPF et définir leurs attributs. Valeur par défaut : **Aucune**. Si la configuration de l’ensemble de cartes d’itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l’itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l’itinéraire redistribué. De même, le Type de métrique dans la configuration de l’ensemble de cartes routières a priorité sur le Type de mesure configuré dans ce profil de redistribution.
RIPv2	Sélectionnez cette option pour pouvoir configurer cette partie du profil.
Activer	Activez la redistribution d’itinéraire RIPv2 vers OSPF.
Mesure	Spécifiez la métrique à appliquer aux routes RIPv2 redistribuées dans OSPF (plage comprise entre 0 et 4 294 967 295).

Profils de routage OSPF	Description
Type de mesure	Sélectionnez : • **Type 1** • **Type 2** (par défaut)
Redistribuer la carte d’itinéraire	Sélectionnez ou créez une carte d’itinéraire de redistribution pour contrôler les itinéraires RIPv2 qui sont redistribués à OSPF et définir leurs attributs. Valeur par défaut : **Aucune**. Si la configuration de l’ensemble de cartes d’itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l’itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l’itinéraire redistribué. De même, le Type de métrique dans la configuration de l’ensemble de cartes routières a priorité sur le Type de mesure configuré dans ce profil de redistribution.
BGP AFI IPv4	Sélectionnez cette option pour pouvoir configurer cette partie du profil.
Activer	Activez la redistribution de route BGP IPv4 vers OSPF.
Mesure	Spécifiez la métrique à appliquer aux routes IPv4 BGP redistribuées dans OSPF (plage comprise entre 0 et 4 294 967 295).
Type de mesure	Sélectionnez : • **Type 1** • **Type 2** (par défaut)
Redistribuer la carte d’itinéraire	Sélectionnez ou créez une carte d’itinéraire de redistribution pour contrôler les itinéraires BGP IPv4 qui sont redistribués à OSPF et définir leurs attributs. Valeur par défaut : **Aucune**. Si la configuration de l’ensemble de cartes d’itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l’itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l’itinéraire redistribué. De même, le Type de métrique dans la configuration de l’ensemble de cartes routières a priorité sur le Type de mesure configuré dans ce profil de redistribution.
Itinéraire par défaut IPv4	Sélectionnez cette option pour pouvoir configurer cette partie du profil.

Profils de routage OSPF	Description
Toujours	Sélectionnez cette option pour toujours créer et redistribuer la route par défaut IPv4 vers OSPF, même s'il n'y a pas de route par défaut sur le routeur ; la valeur par défaut est activée.
Activer	Activez la redistribution d'itinéraire par défaut IPv4 vers OSPF.
Mesure	Spécifiez la métrique à appliquer aux itinéraires IPv4 par défaut redistribués dans OSPF (plage comprise entre 0 et 4 294 967 295).
Type de mesure	Sélectionnez : • **Type 1** • **Type 2** (par défaut)

Réseau > Routage > Profiles de routage > OSPFv3

Ajoutez des profils de routage OSPFv3 pour configurer efficacement OSPFv3 pour un routeur logique.

Profils de routage OSPFv3	Description
Profil global de minuterie OSPFv3	
Nom	Saisissez un nom pour le profil (63 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et contenir zéro ou plusieurs caractères alphanumériques, un trait de soulignement (_) ou un trait d'union(-). Aucun point (.) ou espace n'est autorisé.
Arrivée minimale LSA	Entrez le plus petit intervalle auquel le pare-feu recalcule l'arborescence SPF ; la plage est de 1 à 10; la valeur par défaut est 5. Le pare-feu se recalculerait à un intervalle plus long (moins fréquemment que le paramètre).
Limitation SPF : délai initial	Entrez le délai initial (en secondes) à partir du moment où le routeur logique reçoit un changement de topologie jusqu'à ce qu'il effectue le calcul SPF (Shortest Path First) ; la plage est comprise entre 0 et 600; la valeur par défaut est 5.
Temps d'attente initial	Entrez le temps d'attente initial (en secondes) entre les deux premiers calculs SPF consécutifs; la plage est comprise entre 0 et 600; la valeur par défaut est 5. Chaque temps d'attente suivant est deux fois plus long que le temps d'attente

Profils de routage OSPFv3	Description
	précédent jusqu'à ce que le temps d'attente atteigne le temps d'attente maximal.
Durée d'attente maximale	Entrez la valeur la plus élevée à laquelle le temps d'attente augmente jusqu'à ce qu'il reste stable ; la plage est comprise entre 0 et 600; la valeur par défaut est 5.
Profil d'authentification OSPFv3	
Nom	Saisissez un nom pour le profil d'authentification (63 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et contenir zéro ou plusieurs caractères alphanumériques, un trait de soulignement (_) ou un trait d'union(-). Aucun point (.) ou espace n'est autorisé.
SPI	Entrez l'index de stratégie de sécurité, qui doit correspondre entre les deux extrémités de l'adjacence OSPFv3.
Protocole	Sélectionnez le protocole d'authentification : **ESP** (Encapsulating Security Payload) (recommandé) ou **AH** (en-tête Authentication).
Authentication Type (Type d'authentification)	Sélectionnez le type d'authentification : • **SHA1** (par défaut) - Algorithme SHA 1. • **Sha256** • **SHA384** • **SHA512** • **MD5** • **None**
Clé	Entrez la clé d'authentification au format hexadécimal: xxxxxxxx[-xxxxxxxx] ... en utilisant un total de 5 sections et **la clé de confirmation**.
Chiffrement : algorithme	(ESP uniquement) Sélectionnez l'algorithme de chiffrement : • **3des** (par défaut) • **aes-128-cbc** • **aes-192-cbc** • **aes-256-cbc** • **zéro**

Profils de routage OSPFv3	Description
Clé	(ESP uniquement) Entrez la clé de chiffrement au format hexadécimal ; utilisez le nombre correct de sections en fonction du type de chiffrement ESP et **de la clé de confirmation**: • **3des :**utilisez un total de 6 sections hexadécimales dans la clé. • **aes-128-cbc :**utilisez un total de 4 sections hexadécimales dans la clé. • **aes-192-cbc :**utilisez un total de 6 sections hexadécimales dans la clé. • **aes-256-cbc :**utilisez un total de 8 sections hexadécimales dans la clé.
Profil de minuterie d'interface OSPFv3	
Nom	Saisissez un nom pour le profil (63 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et contenir zéro ou plusieurs caractères alphanumériques, un trait de soulignement (_) ou un trait d'union(-). Aucun point (.) ou espace n'est autorisé.
Intervalle Hello	Entrez l'intervalle (en secondes) auquel OSPFv3 envoie les paquets Hello ; la plage est de 1 à 3 600; la valeur par défaut est 10.
Nombre de morts	Entrez le nombre de fois que l'intervalle Hello peut se produire à partir d'un voisin sans qu'OSPFv3 reçoive un paquet Hello du voisin, avant qu'OSPFv3 ne considère ce voisin comme descendant ; la plage est de 3 à 20; la valeur par défaut est 4.
Intervalle de retransmission	Entrez le nombre de secondes pendant lesquelles OSPFv3 attend pour recevoir un LSA d'un voisin avant qu'OSPFv3 ne retransmet le LSA : la plage est comprise entre 1 et 1 800 ; la valeur par défaut est 5.
Délai de transmission	Entrez le nombre de secondes pendant lesquelles OSPFv3 retarde la transmission d'un LSA avant d'envoyer le SLA hors d'une interface ; la plage est de 1 à 1 800; la valeur par défaut est 1.
Délai de redémarrage approprié Hello (sec)	Entrez le graceful Restart Hello Delay en secondes; la plage est de 1 à 10; la valeur par défaut est 10. Ce paramètre s'applique à une interface OSPFv3 lorsque

Profils de routage OSPFv3	Description
	la haute disponibilité active/passive est configurée. La temporisation de redémarrage en douceur Hello est la durée pendant laquelle le pare-feu envoie des paquets LSA à des intervalles de 1 seconde. Pendant cette période, aucun paquet Hello n'est envoyé avant le redémarrage du pare-feu. Lors du redémarrage, le minuteur d'inactivité (qui correspond à l'**Intervalle Hello** multiplié par le **Nombre de pertes**) effectue un compte à rebours. Si la valeur du minuteur d'inactivité est trop faible, l'adjacence devient inactive pendant le redémarrage en douceur en raison de la temporisation Hello. Par conséquent, il est recommandé que la valeur du minuteur d'inactivité soit au moins quatre fois celle de la Graceful Restart Hello Delay (Temporisation de redémarrage en douceur Hello).
Profil de redistribution OSPFv3	
Nom	Saisissez un nom pour le profil (63 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et contenir zéro ou plusieurs caractères alphanumériques, un trait de soulignement (_) ou un trait d'union(-). Aucun point (.) ou espace n'est autorisé.
IPv6 Statique	Sélectionnez cette option pour autoriser la configuration de cette partie du profil.
Activer	Activez la partie statique IPv6 du profil.
Mesure	Saisissez la mesure à appliquer aux itinéraires statiques qui sont redistribués dans OSPFv3 (plage de 1 à 65 535).
Type de mesure	Sélectionnez **Type 1** ou **Type 2**.
Redistribuer la carte d'itinéraire	Sélectionnez ou créez une carte d'itinéraire de redistribution pour contrôler les routes statiques IPv6 qui sont redistribuées vers OSPFv3 et définir leurs attributs. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué. De même, le Type de métrique dans la configuration de l'ensemble de cartes routières a priorité sur le Type de mesure configuré dans ce profil de redistribution.

Profils de routage OSPFv3	Description
Connecté	Sélectionnez cette option pour autoriser la configuration de cette partie du profil.
Activer	Activez la partie Connecté du profil.
Mesure	Saisissez la mesure à appliquer aux itinéraires connectés qui sont redistribués dans OSPFv3 (plage de 1 à 65 535).
Type de mesure	Sélectionnez **Type 1** ou **Type 2**.
Redistribuer la carte d'itinéraire	Sélectionnez ou créez une carte d'itinéraire de redistribution pour contrôler les itinéraires connectés qui sont redistribués vers OSPFv3 et définir leurs attributs. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué. De même, le Type de métrique dans la configuration de l'ensemble de cartes routières a priorité sur le Type de mesure configuré dans ce profil de redistribution.
BGP AFI IPv6	Sélectionnez cette option pour autoriser la configuration de cette partie du profil.
Activer	Activez la partie BGP AFI IPv6 du profil.
Mesure	Spécifiez la métrique à appliquer aux itinéraires IPv6 BGP redistribuées dans OSPFv3 (la plage est comprise entre 0 et 4 294 967 295).
Type de mesure	Sélectionnez **Type 1** ou **Type 2**.
Redistribuer la carte d'itinéraire	Sélectionnez ou créez une carte d'itinéraire de redistribution pour contrôler les routes BGP IPv6 redistribuées vers OSPFv3 et définir leurs attributs. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué. De même, le Type de métrique dans la configuration de l'ensemble de cartes routières a priorité sur le Type de mesure configuré dans ce profil de redistribution.

Profils de routage OSPFv3	Description
Itinéraire par défaut IPv6	Sélectionnez cette option pour autoriser la configuration de cette partie du profil.
Toujours	Sélectionnez cette option pour toujours créer et redistribuer l'itinéraire IPv6 par défaut vers OSPFv3, même s'il n'y a pas d'itinéraire par défaut sur le routeur ; la valeur par défaut est activée.
Activer	Activez la partie Itinéraire par défaut IPv6 du profil.
Mesure	Spécifiez la métrique à appliquer à l'itinéraire IPv6 par défaut redistribué dans OSPFv3 (plage comprise entre 0 et 4 294 967 295).
Type de mesure	Sélectionnez **Type 1** ou **Type 2**.

Réseau > Routage > Profiles de routage > RIPv2

Ajoutez des profils de routage RIPv2 pour configurer efficacement RIPv2 pour un routeur logique.

Profils de routage RIPv2	Description
Profil de minuterie globale RIPv2	
Nom	Saisissez un nom pour le profil (63 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et contenir zéro ou plusieurs caractères alphanumériques, un trait de soulignement (_) ou un trait d'union(-). Aucun point (.) ou espace n'est autorisé.
Intervalle de mise à jour	Entrez le nombre de secondes entre les messages de mise à jour de routage régulièrement programmés ; la plage est de 5 à 2 147 483 647 ; la valeur par défaut est 30.
Intervalle d'expiration	Entrez le nombre de secondes pendant lesquelles un itinéraire peut se trouver dans la table de routage sans être mise à jour ; la plage est de 5 à 2 147 483 647 ; la valeur par défaut est 180. Une fois l'intervalle d'expiration atteint, l'itinéraire est toujours inclus dans les messages de mise à jour jusqu'à ce que l'intervalle de suppression soit atteint.

Profils de routage RIPv2	Description
Supprimer l'intervalle	Entrez le nombre de secondes dans l'intervalle de suppression ; la plage est de 5 à 2 147 483 647 ; la valeur par défaut est 120. Lorsqu'un itinéraire expiré dans la table de routage atteint l'intervalle de suppression, il est supprimé de la table de routage.
Profil d’authentification RIPv2	
Nom	Saisissez un nom pour le profil (63 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d’union (-) et contenir zéro ou plusieurs caractères alphanumériques, un trait de soulignement (_) ou un trait d’union(-). Aucun point (.) ou espace n’est autorisé.
Type	Sélectionnez le type d'authentification : **md5 (utiliser la méthode d'authentification RIP MD5)** ou mot de **passe (authentification par mot de passe simple)**.
Mot de passe	(Authentification par mot de passe simple) Saisissez le mot de passe (16 caractères maximum) et **confirmez le mot de passe**.
MD5	(Authentification RIP MD5) Entrez l'ID de clé MD5 ; la plage est de 0 à 255.
Clé	(Authentification RIP MD5) Entrez la clé MD5 (un maximum de 16 caractères) et la **clé de confirmation**.
utiliser cette clé lors de l'envoi du paquet	(Authentification RIP MD5) Sélectionnez pour faire de cette clé la clé préférée.
Profil de redistribution RIPv2	
Nom	Saisissez un nom pour le profil (63 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d’union (-) et contenir zéro ou plusieurs caractères alphanumériques, un trait de soulignement (_) ou un trait d’union(-). Aucun point (.) ou espace n’est autorisé.

Profils de routage RIPv2	Description
IPv4 Statique	Sélectionnez pour autoriser la configuration de cette partie du profil.
Activer (par défaut) ou Désactiver	Activez la partie IPv4 statique du profil.
Mesure	Saisissez la mesure à appliquer aux itinéraires statiques qui sont redistribués dans RIPv2 (plage de 1 à 65 535).
Itinéraire-Carte	Sélectionnez ou créez une carte d'itinéraires de redistribution pour contrôler les itinéraires statiques IPv4 qui sont redistribués vers RIPv2 et définissez leurs attributs. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué.
Connecté	Sélectionnez pour autoriser la configuration de cette partie du profil.
Activer (par défaut) ou Désactiver	Activez la partie Connecté du profil.
Mesure	Saisissez la mesure à appliquer aux itinéraires connectés qui sont redistribués dans RIPv2 (plage de 1 à 65 535).
Itinéraire-Carte	Sélectionnez ou créez une carte d'itinéraires de redistribution pour contrôler les itinéraires connectés qui sont redistribués vers RIPv2 et définissez leurs attributs. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué.
BGP AFI IPv4	Sélectionnez pour autoriser la configuration de cette partie du profil.
Activer (par défaut) ou Désactiver	Activez la partie BGP AFI IPv4 du profil.

Profils de routage RIPv2	Description
Mesure	Spécifiez la métrique à appliquer aux itinéraires IPv4 BGP redistribués dans RIPv2 (la plage est comprise entre 0 et 4 294 967 295).
Itinéraire-Carte	Sélectionnez ou créez une carte d'itinéraires de redistribution pour contrôler les itinéraires IPv4 BGP qui sont redistribués vers RIPv2 et définir leurs attributs. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué.
OSPFv2	Sélectionnez pour autoriser la configuration de cette partie du profil.
Activer (par défaut) ou Désactiver	Activez la partie OSPFv2 du profil.
Mesure	Spécifiez la métrique à appliquer aux itinéraires OSPFv2 redistribuées dans RIPv2 (la plage est comprise entre 0 et 4 294 967 295).
Itinéraire-Carte	Sélectionnez ou créez une carte d'itinéraires de redistribution pour contrôler les itinéraires OSPFv2 qui sont redistribués vers RIPv2 et définissez leurs attributs. Valeur par défaut : **Aucune**. Si la configuration de l'ensemble de cartes d'itinéraires de routage inclut une action de mesure et une valeur de métrique, elles sont appliquées à l'itinéraire redistribué. Sinon, la métrique configurée sur ce profil de redistribution est appliquée à l'itinéraire redistribué.

Réseau > Routage > Profiles de routage > Filtres

Ajoutez des filtres à appliquer aux profils, par exemple, pour appliquer facilement et de manière cohérente des paramètres qui contrôlent des éléments tels que l'acceptation des routes dans le RIB, les publicités de routage vers les homologues, les publicités conditionnelles, la définition des attributs, l'agrégation des routes et la redistribution des routes.

Filtres	Description
Filtre la liste d'accès	

Filtres	Description
Nom	Entrez un nom pour la liste d'accès (63 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-), et contenir zéro ou plusieurs caractères alphanumériques, trait de soulignement (_) ou trait d'union (-). Aucun point (.) ou espace n'est autorisé.
Description	Entrez une description.
Type	Sélectionnez **IPv4** ou **IPv6**.
Suiv	**Ajoutez** une entrée (règle) et entrez le numéro de séquence de la règle dans la liste des règles pour cette liste d'accès ; la plage est de 1 à 65 535. *Laissez les numéros inutilisés entre les numéros de séquence afin de pouvoir insérer des règles supplémentaires ultérieurement.*
Action	Sélectionnez **Refuser** ou **Autoriser** pour l'entrée. La liste d'accès se termine par un **`Deny Any`**implicite.
Adresse source	(IPv4 uniquement) Sélectionnez l'une des options suivantes : • **Adresse**— Dans le champ **Adresse** suivant, entrez une adresse IPv4 et entrez un masque **générique** pour indiquer une plage d'adresses. Un zéro (0) dans le masque indique que ce bit doit correspondre au bit correspondant dans l'adresse ; un un (1) dans le masque indique un bit "indifférent". • **indifférent** • **None**
Adresse de destination	(IPv4 uniquement) Sélectionnez l'une des options suivantes : • **Adresse**— Dans le champ **Adresse** suivant, entrez une adresse IPv4 et entrez un masque **générique** pour indiquer une plage d'adresses. Un zéro (0) dans le masque indique que ce bit doit correspondre au bit correspondant dans l'adresse ; un un (1) dans le masque indique un bit "indifférent". • **indifférent** • **None**
Adresse source	(IPv6 uniquement) Sélectionnez l'une des options suivantes :

Filtres	Description
	• **Adresse**— Dans le champ **Adresse** suivant, entrez une adresse IPv6. • **indifférent** • **None**
Correspondance exacte de cette adresse	(IPv6 uniquement) Sélectionnez pour faire correspondre uniquement la correspondance exacte de l'adresse source IPv6. Non disponible si l' **adresse source** est **Any** ou **None**.
Filtres Liste des préfixes	
Nom	Entrez un nom pour la liste de préfixes (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-), et contenir zéro ou plusieurs caractères alphanumériques, trait de soulignement (_) ou trait d'union (-). Aucun point (.) ou espace n'est autorisé.
Description	Entrez une description.
Type	Sélectionnez **IPv4** ou **IPv6**.
Suiv	**Ajoutez** une entrée (règle) et entrez le numéro de séquence de la règle dans la liste des règles pour cette liste de préfixes ; la plage est de 1 à 65 535. *Laissez les numéros inutilisés entre les numéros de séquence afin de pouvoir insérer des règles supplémentaires ultérieurement.*
Action	Sélectionnez **Refuser** ou **Autoriser** pour l'entrée. La liste de préfixes se termine par un **`Deny Any`**implicite.
Préfixe	Sélectionnez l’une des options suivantes : • **Réseau n'importe lequel** • **Entrée**: saisissez un **réseau** IPv4 ou IPv6 avec une longueur de barre oblique et de préfixe. Saisissez éventuellement la longueur de préfixe à laquelle le préfixe doit être **supérieur ou égal** (la plage est comprise entre 0 et 32 pour IPv4 ; 0 à 128 pour IPv6). Saisissez éventuellement la longueur de préfixe à laquelle le préfixe doit être **inférieur ou égal** (la plage est comprise entre 0 et 32 pour IPv4 ; 0 à 128 pour IPv6). Par exemple, entrez un réseau de 192.168.3.0/24 avec une longueur de préfixe supérieure ou égale à 25 et une longueur de préfixe inférieure ou égale à 26.

Filtres	Description
	• **None**
Filtres Liste d’accès du chemin AS	
Nom	Entrez un nom pour la liste d'accès AS_Path (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-), et contenir zéro ou plusieurs caractères alphanumériques, trait de soulignement (_) ou trait d'union (-). Aucun point (.) ou espace n'est autorisé.
Description	Entrez une description.
Suiv	**Ajoutez** une entrée (règle) et entrez le numéro de séquence de la règle dans la liste des règles pour cette liste d'accès ; la plage est de 1 à 65 535. *Laissez les numéros inutilisés entre les numéros de séquence afin de pouvoir insérer des règles supplémentaires ultérieurement.*
Action	Sélectionnez **Refuser** ou **Autoriser** pour l'entrée. *Les listes d'accès AS Path se terminent par une règle implicite **Autoriser tout** . Utilisez une liste d'accès AS Path pour refuser les systèmes autonomes.*
Aspath regex	Entrez une expression régulière pour AS_PATH.
Filtres Liste des communautés	
Nom	Entrez un nom pour la liste de communauté (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-), et contenir zéro ou plusieurs caractères alphanumériques, trait de soulignement (_) ou trait d'union (-). Aucun point (.) ou espace n'est autorisé.
Description	Entrez une description de la liste de communauté.
Type	Sélectionnez Communauté **régulière**, **Grande**ou **Étendue** .
Suiv	**Ajouter** une entrée (règle) et saisir le numéro d'ordre de la règle dans la liste des règles de cette liste ; la plage est de 1 à 65 535.

Filtres	Description
	Laissez les numéros inutilisés entre les numéros de séquence afin de pouvoir insérer des règles supplémentaires ultérieurement.
Action	Sélectionnez **Refuser** ou **Autoriser**. La liste se termine par une règle **`Deny Any`** implicite.
Communauté	Sélectionnez l'une des communautés bien connues dans la liste ou entrez une communauté.
Filtres Cartes d’itinéraire BGP	
Nom	Entrez un nom pour la carte de route BGP (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-), et contenir zéro ou plusieurs caractères alphanumériques, trait de soulignement (_) ou trait d'union (-). Aucun point (.) ou espace n'est autorisé.
Description	Entrez une description de la feuille de route.
Onglet Entrée	
Suiv	**Ajoutez** une entrée (règle) et entrez le numéro de séquence de la règle dans la liste des règles pour cette feuille de route ; la plage est de 1 à 65 535. *Laissez les numéros inutilisés entre les numéros de séquence afin de pouvoir insérer des règles supplémentaires ultérieurement.*
Description	Entrez une description de l'entrée de la carte d'itinéraire.
Action	Sélectionnez **Refuser** ou **Autoriser**.
Onglet de correspondance	
Liste d’accès au chemin AS	Sélectionnez une liste d'accès AS Path.
Communauté régulière	Sélectionnez une liste de communauté pour les critères de correspondance.
Grande communauté	Sélectionnez une liste de communauté pour les critères de correspondance.

Filtres	Description
Communauté étendue	Sélectionnez une liste de communauté pour les critères de correspondance.
Mesure	Saisissez une métrique ; la plage est de 0 à 4 294 967 295.
Interface	Sélectionnez une interface.
Origine	Sélectionnez **egp**, **igp**, **incomplet**ou **aucun**.
Étiquette	Entrez une balise ; la plage est de 1 à 4 294 967 295.
Préférence locale	Entrez une préférence locale ; la plage est de 0 à 4 294 967 295.
Homologue	Sélectionnez **local (routes statiques ou redistribuées)** ou **aucun**.
IPv4 ou IPv6	Sélectionnez **IPv4** ou **IPv6** comme famille d'adresses à rechercher.
Adresse—Liste d'accès	Sélectionnez une liste d'accès que vous avez créée et qui spécifie les adresses à faire correspondre. Valeur par défaut : **Aucune**.
Adresse—Liste des préfixes	Sélectionnez une liste de préfixes que vous avez créée et qui spécifie les préfixes à faire correspondre. Il correspond au préfixe reçu d'un pair ou redistribué à partir d'un autre protocole. Valeur par défaut : **Aucune**.
Saut suivant—Liste d'accès	Sélectionnez une liste d'accès que vous avez créée et qui spécifie le saut suivant à mettre en correspondance. Valeur par défaut : **Aucune**.
Saut suivant—Liste des préfixes	Sélectionnez une liste de préfixes que vous avez créée et qui spécifie le saut suivant à mettre en correspondance. Valeur par défaut : **Aucune**.
Source de routage—Liste d'accès	(IPv4 uniquement) Sélectionnez une liste d'accès que vous avez créée et qui spécifie la source de route à faire correspondre. Valeur par défaut : **Aucune**.
Source de routage—Liste des préfixes	(IPv4 uniquement) Sélectionnez une liste de préfixes que vous avez créée et qui spécifie la source de l'itinéraire à faire correspondre. Valeur par défaut : **Aucune**.
Définir l'onglet	

Filtres	Description
Activer l’agrégat atomique BGP	Marquez l'itinéraire comme un itinéraire moins spécifique car il a été agrégé. ATOMIC_AGGREGATE est un attribut discrétionnaire bien connu qui avertit les locuteurs BGP le long d'un chemin que des informations ont été perdues en raison de l'agrégation d’itinéraires, et par conséquent, le chemin agrégé peut ne pas être le meilleur chemin vers la destination. Lorsque certains routeurs sont agrégés par un agrégateur, l'agrégateur attache son ID de routeur à l’itinéraire agrégé dans l'attribut AGGREGATOR-ID et définit ou non l'attribut ATOMIC_AGGREGATE, selon que les informations AS_PATH des routeurs agrégés ont été préservées.
Agrégateur - Agréger AS	Entrez l'agrégateur AS. L'attribut Aggregator inclut le numéro AS et l'adresse IP du routeur à l'origine de l’itinéraire agrégé. L'adresse IP est l'ID de routeur du routeur qui effectue l'agrégation d’itinéraires. Plage comprise entre 1 et 4 294 967 295.
Agrégateur—ID de routeur	Entrez l'ID de routeur de l'agrégateur (généralement une adresse de bouclage).
IPv4 ou IPv6	Sélectionnez le type d'adresse à définir.
Adresse du saut suivant global IPv6 préféré	(IPv6 uniquement) IPv6 a quatre types d'adresse : adresse de lien local, adresse de monodiffusion globale, adresse anycast et adresse de multidiffusion. **IPv6 Nexthop Prefer Global Address** oblige le pare-feu à préférer les adresses globales de monodiffusion.
Adresse source	Sélectionnez l'adresse source avec la longueur du préfixe à définir.
Saut suivant IPv4	(IPv4 uniquement) Sélectionnez **aucun**, **adresse de pair (Utiliser l'adresse de pair)**ou **inchangé**.
Saut suivant IPv6	(IPv6 uniquement) Sélectionnez **aucun** ou **adresse de pair (Utiliser l'adresse de pair)**.
Préférence locale	Entrez la préférence locale ; la plage est de 0 à 4 294 967 295.
Étiquette	Entrez la balise ; la plage est de 1 à 4 294 967 295.
Action de mesure	Sélectionnez **Aucun**, **définir**, **ajouter**ou **soustraire**.
Valeur métrique	Entrez la métrique ; la plage est de 0 à 4 294 967 295.

Filtres	Description
Poids	Entrez le poids ; la plage est de 0 à 4 294 967 295.
Origine	Sélectionnez **egp**, **igp**, **incomplet**ou **aucun**.
ID d’origine	Définissez un ID d'initiateur.
Supprimer la communauté régulière	Entrez une communauté régulière à supprimer.
Supprimer une grande communauté	Saisissez une grande communauté à supprimer.
Communauté régulière—Écraser la communauté régulière	Sélectionnez pour écraser la communauté régulière avec ce qui est ajouté dans le champ Communauté régulière.
Communauté régulière	Ajouter une communauté régulière
Grande communauté—Écraser la communauté normale	Sélectionnez pour écraser la grande communauté avec ce qui est ajouté dans le champ Grande communauté.
Grande communauté	Ajoutez une grande communauté.
Exclure ASPath	Ajoutez un AS_PATH à exclure.
Préfixe ASPath	Ajoutez un AS_PATH à préfixer.
Filtres Redistribution des cartes d’itinéraire	
Nom	Saisissez un nom pour la carte d’itinéraires de redistribution (63 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-), et contenir zéro ou plusieurs caractères alphanumériques, trait de soulignement (_) ou trait d'union (-). Aucun point (.) ou espace n'est autorisé.
Description	Entrez une description de la feuille de route.
Protocole source	Sélectionnez le protocole source redistribué.
Protocole de destination	Sélectionnez le protocole vers lequel les itinéraires sont redistribués.
Entrée	
Suiv	Entrez un numéro de séquence ; la plage est de 1 à 65 535.

Filtres	Description
	Laissez les numéros inutilisés entre les numéros de séquence afin de pouvoir insérer des règles supplémentaires ultérieurement.
Description	Entrez une description de la règle de mappage d’itinéraire.
Action	**Refuser** ou **autoriser** la redistribution des routes correspondantes.
Correspondance	
Liste d’accès au chemin AS	Sélectionnez une liste d'accès AS Path.
Communauté régulière	Entrez dans une communauté régulière.
Grande communauté	Entrez dans une grande communauté.
Communauté étendue	Entrez dans une communauté étendue
Mesure	Plage comprise entre 0 et 4 294 967 295.
Interface	Sélectionnez une interface.
Origine	Sélectionnez **egp**, **igp**, **incomplet**ou **aucun**.
Étiquette	Entrez une balise ; la plage est de 1 à 4 294 967 295.
Préférence locale	Entrez une préférence locale ; la plage est de 0 à 4 294 967 295.
Homologue	Sélectionnez local **(itinéraires statiques ou redistribués)** ou **aucun**.
Adresse—Liste d'accès	Sélectionnez une liste d'accès.
Adresse—Liste des préfixes	Sélectionnez une liste de préfixes.
Saut suivant—Liste d'accès	Sélectionnez une liste d'accès.
Saut suivant—Liste des préfixes	Sélectionnez une liste de préfixes.
Source de routage—Liste d'accès	Sélectionnez une liste d'accès.
Source de routage—Liste des préfixes	Sélectionnez une liste de préfixes.

Filtres	Description
Définir	
Action de mesure	Sélectionnez **Aucun**, **définir**, **ajouter**ou **soustraire**.
Valeur métrique	Saisissez la valeur à **laquelle définir** la métrique, l' **ajouter** à la métrique ou **la soustraire** de la métrique des itinéraires correspondants, en fonction de votre sélection pour **Metric Action**. Plage comprise entre 0 et 4 294 967 295.
Type de mesure	Sélectionnez **Type 1** ou **Type 2**.
Étiquette	Plage comprise entre 1 et 4 294 967 295.

Réseau > Routage > Profiles de routage > Multidiffusion

Ajoutez des profils de routage de multidiffusion pour configurer efficacement la multidiffusion IPv4 pour un routeur logique.

Profils de routage multidiffusion	Description
Profil de minuterie d’interface PIM IPv4 multidiffusion	
Nom	Saisissez un nom pour le profil (31 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-), et contenir zéro ou plusieurs caractères alphanumériques, trait de soulignement (_) ou trait d'union (-). Aucun point (.) ou espace n’est autorisé.
Intervalle d'affirmation	Entrez le nombre de secondes entre les messages PIM Assert que le routeur logique envoie à d’autres routeurs PIM sur le réseau multiaccess lorsqu’ils élisent un redirecteur PIM. La plage est comprise entre 1 et 65,534 ; la valeur par défaut est 177.
Intervalle Hello	Entrez le nombre de secondes entre les messages PIM Hello que le routeur logique envoie à ses voisins PIM à partir de chaque interface du groupe d’interfaces. La plage est de 1 à 180; la valeur par défaut est 30.
Intervalle Join Prune	Entrez le nombre de secondes entre les messages PIM Join (et entre les messages PIM Prune) que le routeur logique envoie en amont vers une source de multidiffusion. La plage est de 60 à 600; la valeur par défaut est 60.
Profil de requête d’interface IGMP IPv4 multidiffusion	

Profils de routage multidiffusion	Description
Nom	Saisissez un nom pour le profil (31 caractères maximum). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-), et contenir zéro ou plusieurs caractères alphanumériques, trait de soulignement (_) ou trait d'union (-). Aucun point (.) ou espace n'est autorisé.
Temps de réponse maximal à la requête	Saisissez le nombre maximal de secondes dont dispose le récepteur pour répondre à un message de requête d'adhésion IGMP avant que le routeur logique détermine que le récepteur ne souhaite plus recevoir les paquets multidiffusion pour un groupe. La plage est de 1 à 25; la valeur par défaut est 10.
Intervalle de requête	Saisissez le nombre de secondes entre les messages de requête d'adhésion IGMP que le routeur logique envoie à un récepteur pour déterminer si le récepteur souhaite toujours recevoir les paquets multicast pour un groupe. La plage est comprise entre 1 et 1,800 ; la valeur par défaut est 125.
Intervalle de requête du dernier membre	Entrez le nombre de secondes autorisées pour qu'un récepteur réponde à une requête spécifique au groupe que le routeur logique envoie après qu'un récepteur a envoyé un message Leave Group. La plage est comprise entre 1 et 25 ; la valeur par défaut est 1.
quitter le groupe immédiatement lorsqu'un message de congé est reçu	Si vous activez cette fonctionnalité lorsqu'il n'y a qu'un seul membre dans un groupe multidiffusion et que le routeur logique reçoit un message d'abandon IGMP pour ce groupe, ce paramètre entraîne la suppression par le routeur logique de ce groupe et de l'interface de sortie de la multicast routing information base (base d'informations de routage multidiffusion ; mRIB) et de la multicast forwarding information base (base d'informations de transfert multidiffusion ; mFIB) plutôt que d'attendre l'expiration du dernier intervalle de requête d'un membre. L'activation de ce paramètre permet d'économiser des ressources réseau. La valeur par défaut est désactivée.
Profil d'authentification MSDP multidiffusion	
Nom	Ajouter un profil d'authentification MSDP par nom (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement ou de trait d'union. Aucun point (.) ou espace n'est autorisé.
Phrase secrète	Entrez le Secret (les caractères alphanumériques, !, @, #, % et ^ sont autorisés). **Confirm Secret (Confirmer le code secret)**.

Profils de routage multidiffusion	Description
Profil du minuteur MSDP multidiffusion	
Nom	Ajouter un profil MSDP Timer par nom (maximum de 63 caractères). Le nom doit commencer par un caractère alphanumérique, un trait de soulignement (_) ou un trait d'union (-) et peut contenir une combinaison de caractères alphanumériques, de trait de soulignement ou de trait d'union. Aucun point (.) ou espace n'est autorisé.
Intervalle de maintien en vie	Entrez une valeur en secondes; la plage est de 1 à 60; la valeur par défaut est 60. Une fois qu'une connexion de transport MSDP est établie avec un homologue, chaque côté de la connexion envoie des messages Keepalive à l'autre côté à cet intervalle pour maintenir la session MSDP active. Si le minuteur expire, l'homologue envoie un message Keepalive et réinitialise le minuteur. Si aucun message Keepalive ou SA n'est reçu pour l'intervalle de délai d'expiration du message, la session MSDP est réinitialisée.
Message de délai d'expiration	Entrez une valeur en secondes, qui est l'intervalle auquel le pair MSDP attendra les messages Keepalive des autres pairs avant de les déclarer hors service. La plage est comprise entre 1 et 75 ; la valeur par défaut est 75.
Intervalle de nouvelle tentative de connexion	Entrez une valeur en secondes, qui est l'intervalle que les pairs attendront après la réinitialisation d'une session d'homologation avant d'essayer de rétablir la session d'homologation. La plage est comprise entre 1 et 60 ; la valeur par défaut est 30.

Réseau > Tunnels IPSec

Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)** pour établir et gérer des tunnels VPN IPSec entre les pare-feu. Il s'agit de la phase 2 de la configuration de VPN IKE/IPSec.

Que voulez-vous faire ?	Reportez-vous à la section :
Gestion des tunnels VPN IPSec.	Gestion d’un tunnel VPN IPSec
Configuration d’un tunnel IPSec.	Onglet Général Tunnel IPSec
	Onglet ID de proxy Tunnel IPSec
Affichage du statut du tunnel IPSec.	Statut du tunnel IPSec sur le pare-feu
Redémarrer ou actualiser un tunnel IPSec.	Redémarrage ou actualisation d'un tunnel IPSec
Vous souhaitez en savoir plus ?	Configuration d’un tunnel IPSec.

Gestion d’un tunnel VPN IPSec

- Réseau > Tunnels'A0;IPSec

Le tableau suivant explique comment gérer les tunnels VPN IPSec.

Champs pour gérer les tunnels VPN IPSec	
Ajouter	Cliquez pour **Ajouter** un nouveau tunnel VPN IPSec. Voir l’onglet Tunnel IPSec - Onglet Général pour des instructions sur la configuration du nouveau tunnel.
Supprimer	Cliquez pour **Supprimer** un tunnel dont vous n’avez plus besoin.
Activer	Cliquez pour **Activer** un tunnel qui a été désactivé (les tunnels sont activés par défaut).
Désactivation	Cliquez pour **Désactiver** un tunnel que vous ne voulez pas utiliser, mais qui n’est pas encore prêt à être supprimé.
PDF/CSV	Exportez la configuration des tunnels au format **PDF/CSV**. Vous pouvez appliquer des filtres pour personnaliser le tableau et n’inclure que les colonnes dont vous avez besoin. Seules les colonnes visibles dans le dialogue d’exportation sont exportées. Consultez la section Exportation des données du tableau de configuration.

Onglet Général Tunnel IPSec

- Réseau > Tunnels IPSec > Général

Utilisez les champs suivants pour configurer un tunnel IPSec.

Paramètres généraux d'un tunnel IPSec	Description
Name (Nom)	Saisissez un **Name (Nom)** pour identifier le tunnel (63 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement. La limite de 63 caractères de ce champ inclut le nom du tunnel, en plus de l'ID de proxy, séparé par deux-points.
en texte clair	Sélectionnez une interface de tunnel existante ou cliquez sur **New Tunnel Interface (Nouvelle interface de tunnel)**. Pour des informations sur la création d'une interface de tunnel, reportez-vous à Réseau > Interfaces > Tunnel.
IPv4 ou IPv6	Sélectionnez **IPv4** ou **IPv6** pour configurer le tunnel de manière à avoir des points d'extrémité avec ce type d'adresse IP.
Type	Indiquez si une clé de sécurité générée automatiquement ou saisie manuellement doit être utilisée. L'option **Auto key (Clé automatique)** est recommandée.
Clé automatique	Si vous choisissez **Auto key (Clé automatique)**, indiquez les options suivantes : • **IKE Gateway (Passerelle IKE)** – Reportez-vous à Réseau > Profils réseau > Passerelles IKE pour des descriptions des paramètres de passerelle IKE. • **IPSec Crypto Profile (Profil cryptographique IPSec)** - Sélectionnez un profil existant ou conservez le profil par défaut. Pour définir un nouveau profil, cliquez sur **New (Nouveau)** et suivez les instructions dans Réseau > Profils réseau > Crypto IPSec. • Cliquez sur **Show Advanced Options (Afficher les options avancées)** pour accéder aux champs restants. • **Enable Replay Protection (Activer la protection contre les attaques par relecture)** – Sélectionnez pour vous protéger des attaques par relecture. L'anti-rejeu est un sous-protocole d'IPSec et fait partie de la demande de commentaires (RFC) 6479 de l'Internet Engineering Task Force (IETF). Le protocole anti-rejeu est utilisé pour empêcher les pirates d'injecter ou d'apporter des modifications aux paquets qui voyagent d'une source

Paramètres généraux d’un tunnel IPSec	Description
	à une destination et utilise une association de sécurité unidirectionnelle afin d'établir une connexion sécurisée entre deux nœuds du réseau. Une fois qu'une connexion sécurisée est établie, le protocole anti-rejeu utilise des numéros de séquence de paquets pour vaincre les attaques de relecture. Lorsque la source envoie un message, elle ajoute un numéro de séquence à son paquet ; le numéro de séquence commence à 0 et est incrémenté de 1 pour chaque paquet suivant. La destination conserve la séquence de nombres dans un format de *sliding window (fenêtre glissante)*, conserve un enregistrement des numéros de séquence des paquets reçus validés et rejette tous les paquets dont le numéro de séquence est inférieur au plus petit de la fenêtre glissante (paquets trop anciens) ou des paquets qui apparaissent déjà dans la fenêtre glissante (paquets dupliqués ou rejoués). Les paquets acceptés, une fois validés, mettent à jour la fenêtre glissante, déplaçant le plus petit numéro de séquence hors de la fenêtre si elle était déjà pleine. Si vous activez la protection contre la relecture, sélectionnez la **Anti Replay Window (fenêtre Anti-relecture)** à utiliser. Vous pouvez sélectionner une taille de fenêtre anti-relecture de 64, 128, 256, 512, 1024, 2048 ou 4096. La valeur par défaut est 1024. • **Copy TOS Header (Copier l'en-tête TOS)** - Permet de copier le champ Type de service (TOS) à partir de l'en-tête IP entrant vers l'en-tête IP sortant des paquets encapsulés afin de conserver les informations TOS d'origine. Cette option copie également le champ Notification explicite de congestion (ECN). • **Mode IPSec** : spécifiez le mode IPSec. Sélectionnez le mode **Tunnel** pour chiffrer l’intégralité du paquet, y compris l’en-tête. Un nouvel en-tête IP est ajouté au paquet après le chiffrement. Sélectionnez le mode **Transport** pour chiffrer uniquement la charge utile et conserver l’en-tête IP d’origine. • **Add GRE Encapsulation (Ajouter l’encapsulation GRE)** : sélectionnez cette option pour ajouter un en-tête GRE encapsulé dans le tunnel IPSec. Le pare-feu génère un en-tête GRE après l’en-tête IPSec pour l'interopérabilité avec les points de terminaison du tunnel d’un autre fournisseur, partageant ainsi un tunnel GRE avec le tunnel IPSec.

Paramètres généraux d’un tunnel IPSec	Description
	• **Tunnel Monitor (Surveillance des tunnels)** – Sélectionnez pour informer l’administrateur de périphérique de la défaillance d’un tunnel et basculer automatiquement vers une autre interface. *Vous devez affecter une adresse IP à l'interface de tunnel à surveiller.* • **Destination IP (Adresse IP de destination)** : indiquez une adresse IP de l'autre côté du tunnel que le moniteur de tunnels va utiliser pour déterminer si le tunnel fonctionne correctement. • **Profile (Profil)** - Sélectionnez un profil existant qui déterminera les actions prises en cas de défaillance d'un tunnel. Si l'action spécifiée dans le profil de surveillance est en attente de récupération, le pare-feu attend que le tunnel devienne fonctionnel et ne cherche PAS d'autre chemin dans la table de routage. Si l'action de basculement est sélectionnée, le pare-feu recherche dans la table de routage si un autre itinéraire peut être utilisé pour atteindre la destination. Pour plus d’informations, voir Réseau > Profils réseau > Surveillance.
Clé manuelle	Si vous choisissez **Manual Key (Clé manuelle)**, indiquez les options suivantes : • **Local SPI (SPI local)** - Indiquez l'index de paramètres de sécurité (SPI) local pour le parcours du paquet entre le pare-feu local et l'homologue. SPI est un index hexadécimal ajouté à l'en-tête du tunnel IPSec permettant de différencier les flux de trafic IPSec. • **Interface** - Sélectionnez l'interface correspondant au point d'extrémité du tunnel. • **Local Address (Adresse locale)** - Sélectionnez l'adresse IP de l'interface locale correspondant au point d'extrémité du tunnel. • **Remote SPI (SPI distant)** - Indiquez l'index de paramètres de sécurité (SPI) distant pour le parcours du paquet entre le pare-feu distant et l'homologue. • **Protocol (Protocole)** - Sélectionnez le protocole utilisé pour le trafic passant par le tunnel (**ESP** ou **AH**). • **Authentication (Authentification)** - Sélectionnez le type d'authentification pour accéder au tunnel (**SHA1**, **SHA256**, **SHA384**, **SHA512**, **MD5** ou **None (Aucun)**). • **Key/Confirm Key (Clé/Confirmer la clé)** - Saisissez et confirmez une clé d'authentification. • **Encryption (Chiffrement)** - Sélectionnez une option de chiffrement pour le trafic du tunnel (**3des**, **aes-128-cbc**, **aes-192-cbc**, **aes-256-cbc**, **des** ou **null (aucun)** [aucun chiffrement]).

Paramètres généraux d’un tunnel IPSec	Description
	• **Key/Confirm Key (Clé/Confirmer la clé)** - Saisissez et confirmez une clé de chiffrement.
Satellite GlobalProtect	Si vous choisissez **GlobalProtect Satellite (Satellite GlobalProtect)**, indiquez les options suivantes : • **Name (Nom)** - Saisissez un nom pour identifier le tunnel (**31** caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement. • **Tunnel Interface (Interface de tunnel)** – Sélectionnez une interface de tunnel existante ou cliquez sur Nouvelle interface de tunnel. • **Portal Address (Adresse du portail)** – Saisissez l’adresse IP du portail GlobalProtect™. • **Interface** – Sélectionnez l’interface dans la liste déroulante correspondant à l’interface de sortie permettant d’atteindre le Portail GlobalProtect. • **Local IP Address (Adresse IP locale)** – Saisissez l’adresse IP de l’interface de sortie qui se connecte au Portail GlobalProtect. • **Options avancées** • **Publish all static and connected routes to Gateway (Publier tous les itinéraires statiques et connectés à la Passerelle)** – Sélectionnez cette option afin de publier tous les itinéraires du satellite vers la Passerelle GlobalProtect à laquelle ce satellite est connecté. • **Subnet (Sous-réseau)** - Cliquez sur **Add (Ajouter)** pour ajouter manuellement des sous-réseaux locaux à l'emplacement d'un satellite. Si d'autres satellites utilisent les mêmes informations de sous-réseau, vous devez traduire l'adresse réseau (NAT) de l'ensemble du trafic vers l'adresse IP de l'interface de tunnel. De plus, le satellite ne doit partager aucun itinéraire dans ce cas de figure, le routage entier sera alors réalisé via l'IP de tunnel. • **External Certificate Authority (Autorité de certification externe)** – Sélectionnez si vous prévoyez d’utiliser une autorité de certification (CA) externe pour gérer les certificats. Une fois vos certificats générés, vous devrez les importer dans le satellite et sélectionner le **Local Certificate (Certificat local)** et le **Certificate Profile (Profil du certificat)**.

Onglet ID de proxy Tunnel IPSec

- Réseau > Tunnels IPSec > ID Proxy

L'onglet **IPSec Tunnel Proxy IDs (ID de proxy du tunnel IPSec)** est séparé en deux sous-onglets : **IPv4** et **IPv6**. L'aide est similaire pour les deux types ; les différences entre IPv4 et IPv6 sont décrites dans les champs **Local** et **Remote (Distant)** du tableau suivant.

L'onglet **IPSec Tunnel Proxy IDs (ID de proxy du tunnel IPSec)** permet également de spécifier les sélecteurs de trafic pour IKEv2.

Paramètres d'ID de proxy IPv4 et IPv6	Description
ID de proxy	Cliquez sur **Add (Ajouter)** et saisissez un nom pour identifier le proxy. Ce champ est utilisé comme nom pour un sélecteur de trafic IKEv2.
Local	Pour IPv4 : saisissez une adresse IP ou un sous-réseau au format x.x.x.x/masque (par exemple : 10.1.2.0/24). Pour IPv6 : Saisissez une adresse IP et une longueur de préfixe au format xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/longueur-préfixe (ou par connexion IPv6, par exemple : 2001:DB8:0::/48). L'adressage IPv6 ne nécessite pas la saisie de tous les zéros ; les zéros non significatifs peuvent être omis et un groupe de zéros consécutifs peut être remplacé par deux-points adjacents (::). Ce champ est converti en adresse IP source pour un sélecteur de trafic IKEv2.
Distant	Si l'homologue l'exige : Pour IPv4, saisissez une adresse IP ou un sous-réseau au format x.x.x.x/masque (par exemple : 10.1.1.0/24). Pour IPv6, saisissez une adresse IP et une longueur de préfixe au format xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx/longueur-préfixe (ou par connexion IPv6, par exemple : 2001:DB8:55::/48). Ce champ est converti en adresse IP de destination pour un sélecteur de trafic IKEv2.
Protocole	Indiquez le protocole et les numéros de port pour les ports locaux et distants'A0;: **Number (Numéro)** - Indiquez le numéro de protocole (pour assurer l'interopérabilité avec des périphériques tiers). • **Any (Tout)** - Autorisez le trafic TCP et/ou UDP. • **TCP** - Indiquez les numéros de port TCP locaux et distants. • **UDP** - Indiquez les numéros de port UDP locaux et distants. chaque ID de proxy configuré va être inclus dans la capacité du tunnel VPN IPSec du pare-feu. Ce champ est également utilisé comme sélecteur de trafic IKEv2.

Statut du tunnel IPSec sur le pare-feu

- Réseau > Tunnels'A0;IPSec

Pour afficher le statut des tunnels VPN IPSec actuellement définis, ouvrez la page **IPSec Tunnels (Tunnels IPSec)**. Les informations suivantes concernant le statut sont signalées sur la page'A0;:

- Statut du tunnel (première colonne du statut) – La couleur verte indique un tunnel SA de phase 2 IPSec. La couleur rouge indique qu'une SA IPSec de phase 2 n'est pas disponible ou a expiré.
- Statut de la passerelle IKE – La couleur verte indique une SA de phase 1 IKE ou IKEv2 valide. La couleur rouge indique qu'une association de sécurité'A0;IKE de phase 1 n'est pas disponible ou a expiré.
- Statut de l’interface de tunnel – La couleur verte indique que l’interface du tunnel est active (car la surveillance de tunnels est désactivée ou car le statut de la surveillance de tunnels affiche ACTIF et l’adresse IP de la surveillance est accessible). La couleur rouge indique que l'interface de tunnel est inactive, car la surveillance des tunnels est activée et l'adresse IP de surveillance des tunnels ne peut pas être atteinte.

Redémarrage ou actualisation d'un tunnel IPSec

- Réseau > Tunnels'A0;IPSec

Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)** pour afficher l’état des tunnels. Dans la première colonne Statut se trouve un lien vers les informations du tunnel. Cliquez sur le tunnel que vous souhaitez redémarrer ou actualiser pour ouvrir la page **Tunnel Info (Informations du tunnel)** qui correspond à ce tunnel. Cliquez sur l’une des entrées de la liste, puis sur :

- **Restart (Redémarrer)** – Redémarre le tunnel sélectionné. Un redémarrage interrompt le trafic passant à travers le tunnel.
- **Refresh (Rafraichir)** – Affiche le statut actuel de la SA IPSec.

Réseau > Tunnels GRE

Le protocole de tunnel de Generic Routing Encapsulation (encapsulation générique de routage ; GRE) est un protocole de transport qui encapsule un protocole de charge utile. Le paquet GRE lui-même est encapsulé dans un protocole de transport (IPv4 ou IPv6). Le tunnel GRE connecte deux points de terminaison en une liaison logique de point à point entre le pare-feu et un routeur (ou un autre pare-feu). Les pare-feu Palo Alto Networks prennent en charge l'interruption du tunnel GRE.

Que voulez-vous faire ?	Reportez-vous à la section :
Blocs de construction d'un tunnel GRE	Tunnels GRE
Comment fournir l'interopérabilité avec le point de terminaison du tunnel d'un autre fournisseur	Sélectionnez **Add GRE Encapsulation (Ajouter l'encapsulation GRE)** lors de la création d'un tunnel IPSec.
Vous souhaitez en savoir plus ?	Tunnels GRE

Tunnels GRE

- Réseau > Tunnels GRE

Commencez par configurer une interface de tunnel (Réseau > Interfaces > Tunnel). Ajoutez ensuite un tunnel de generic routing encapsulation (encapsulation générique de routage ; GRE) et fournissez les renseignements suivants, en faisant référence à l'interface de tunnel que vous avez créée :

Champs du tunnel GRE	Description
Name (Nom)	Nom du tunnel GRE.
Interface	Sélectionnez l'interface à utiliser en tant que point de terminaison du tunnel GRE local (interface source), soit une interface ou une sous-interface Ethernet, une interface Aggregate Ethernet (AE), une interface de bouclage ou une interface VLAN.
Adresse locale	Sélectionnez l'adresse IP locale de l'interface à utiliser en tant qu'adresse de l'interface du tunnel.
Adresse de l'homologue	Saisissez l'adresse IP à l'extrémité opposée du tunnel GRE.
en texte clair	Sélectionnez l'interface de tunnel que vous avez configurée. (Cette interface identifie le tunnel lorsqu'il correspond au saut suivant du routage.)

Champs du tunnel GRE	Description
TTL	Saisissez la TTL du paquet IP encapsulé dans le paquet GRE (plage comprise entre 1 et 255 ; la valeur par défaut est 64).
ERSPAN	Sélectionnez cette option pour permettre au pare-feu de décapsuler les données ERSPAN (Encapsulated Remote Switched Port Analyzer) envoyées via le tunnel GRE. Vous pouvez configurer un commutateur réseau pour utiliser ERSPAN afin d'envoyer du trafic en miroir via un tunnel GRE vers le pare-feu pour une utilisation par des services de sécurité tels que IoT Security. Après avoir décapsulé les données, le pare-feu les inspecte de la même manière qu'il inspecte le trafic reçu sur un port TAP. Il crée ensuite des journaux d'application améliorés (ECL) et du trafic, des menaces, wildfire, URL, données, GTP (lorsque GTP est activé), SCTP (lorsque SCTP est activé), tunnel, authentification et journaux de déchiffrement. Le pare-feu transmet ces journaux au service de journalisation où IoT Security accède aux données et les analyse.
Copier l'en-tête ToS	Sélectionnez cette option pour copier le champ ToS (Type of Service) de l'en-tête IP entrant vers l'en-tête IP sortant des paquets encapsulés pour préserver les informations ToS d'origine.
Keep Alive	Sélectionnez cette option pour activer la fonction Keep Alive du tunnel GRE (désactivée par défaut). Si vous activez la fonction Keep Alive, il faut trois paquets keep alive non retournés (retentatives) à des intervalles de dix secondes pour que le tunnel GRE échoue, et il faut cinq intervalles Délai de maintien à des intervalles de dix secondes pour que le tunnel GRE redevienne actif.
Intervalle (s)	Définissez l'intervalle entre des paquets keepalive que l'extrémité locale du tunnel GRE envoie au tunnel homologue et l'intervalle que chaque Minuterie d'attente attend des paquets keepalive réussis avant que le pare-feu rétablit la communication avec le tunnel homologue (la plage est comprise entre 1 et 50 ; la valeur par défaut est 10).

Champs du tunnel GRE	Description
Relance	Définissez les intervalles pendant lesquels aucun paquet keepalive n’est retourné avant que le tunnel homologue considère que le tunnel homologue est inactif (la plage est comprise entre 1 et 255 ; la valeur par défaut est 3).
Minuterie d’attente	Définissez les intervalles pendant lesquels les paquets keepalive réussissent avant que le pare-feu rétablit la communication avec le tunnel homologue (la plage est comprise entre 1 et 64 ; la valeur par défaut est 5).

Réseau > DHCP

DHCP (Dynamic Host Configuration Protocol/protocole d'attribution dynamique des adresses) est un protocole normalisé qui fournit des paramètres de configuration de la couche de liaison et TCP/IP, ainsi que des adresses IP, aux hôtes configurés de façon dynamique sur un réseau TCP/IP. Une interface sur un pare-feu Palo Alto Networks peut avoir comme un serveur, un client ou un agent de relais DHCP. L'affectation de ces rôles à différentes interfaces permet au pare-feu de remplir plusieurs rôles.

Que voulez-vous faire ?	Reportez-vous à la section :
Qu'est-ce que DHCP ?	Présentation de DHCP
Comment un serveur DHCP alloue-t-il des adresses ?	Adressage DHCP
Configuration d’une interface sur le pare-feu pour agir en tant que :	
	Serveur DHCP
	Relais DHCP
	Proxy DNS
Vous souhaitez en savoir plus ?	DHCP

Présentation de DHCP

- Réseau > DHCP

DHCP utilise un modèle de communication client/serveur. Ce modèle est composé de trois rôles que le pare-feu peut remplir : client DHCP, serveur DHCP et agent de relais DHCP.

- Un pare-feu agissant comme un client (hôte) DHCP peut demander une adresse IP et d'autres paramètres de configuration auprès d'un serveur DHCP. Les utilisateurs sur les pare-feu clients gagnent ainsi du temps lors de la configuration et n'ont pas besoin de connaître le plan d'adressage du réseau ou d'autres ressources et options héritées du serveur DHCP.
- Un pare-feu agissant comme un serveur DHCP peut servir des clients. L'utilisation de l'un des trois mécanismes d'adressage DHCP permet à l'administrateur de gagner du temps lors de la configuration et de réutiliser un nombre limité d'adresses IP lorsque les clients n'ont plus besoin de connexion réseau. Le serveur peut également fournir l'adressage IP et les options DCHP à plusieurs clients.
- Un pare-feu agissant comme un agent de relais DHCP écoute les messages DHCP de diffusion et de monodiffusion, et les relais entre les clients et les serveurs DHCP.

DHCP utilise User Datagram Protocol (Protocole de datagramme utilisateur, UDP), à savoir RFC 768 comme protocole de transport. Un client envoie des messages DHCP à un serveur sur le port 67 bien connu (port UDP utilisé par BOOTP et DHCP). Un serveur envoie des messages DHCP à un client sur le port 68.

Adressage DHCP

Un serveur DHCP affecte ou envoie une adresse IP à un client de trois manières différentes :

- **Automatic allocation (Allocation dynamique)** : le serveur DHCP affecte une adresse IP permanente de ses **IP Pools (pools d'adresses IP)** à un client. Sur le pare-feu, un **Lease (Bail)** spécifié comme **Unlimited (Illimité)** signifie que l'allocation est permanente.
- **Dynamic allocation (Allocation dynamique)** : le serveur DHCP affecte une adresse IP réutilisable de ses **IP Pools (pools d'adresses IP)** à un client, pour une durée maximale, appelée *bail*. Cette méthode d'allocation d'adresse est utile lorsque le client dispose d'un nombre limité d'adresses IP ; celles-ci peuvent être affectées aux clients qui ont besoin d'un accès temporaire au réseau.
- **Static allocation (Allocation statique)** : l'administrateur réseau choisit l'adresse IP à affecter au client et le serveur DHCP l'envoie au client. Une allocation DHCP statique est permanente ; elle est effectuée en configurant un serveur DHCP et en choisissant une **Reserved Address (Adresse réservée)** correspondant à la **MAC Address (Adresse MAC)** du pare-feu client. L'allocation DHCP reste en place même si le client se déconnecte, (ferme sa session, redémarre, subit une coupure de courant, etc.).

  L'allocation statique d'une adresse IP est utile, par exemple, si vous disposez d'une imprimante sur un réseau local et que vous ne souhaitez pas que cette adresse IP change, car elle est associée à un nom d'imprimante via DNS. Un autre exemple est si un pare-feu client est utilisé pour des tâches essentielles et doit conserver la même adresse IP, même si le pare-feu est désactivé, déconnecté, redémarré ou subit une coupure de courant.

  Souvenez-vous des points suivants lors de la configuration d'une **Reserved Address (Adresse réservée)** :

  - Il s'agit d'une adresse des **IP Pools (Pools d'adresses IP)**. Vous pouvez configurer plusieurs adresses IP réservées.
  - Si vous ne configurez aucune **Reserved Address (Adresse réservée)**, les clients du serveur recevront de nouvelles allocations DHCP du pool lorsque leur bail expirera ou quand ils redémarreront, etc. (à moins que vous n'indiquiez un **Lease (Bail) Unlimited (Illimité)**).
  - Si vous affectez chaque adresse des **IP Pools (Pools d'adresses IP)** comme **Reserved Address (Adresse réservée)**, il ne reste aucune adresse dynamique à affecter au prochain client DHCP demandant une adresse.
  - Vous pouvez configurer une **Reserved Address (Adresse réservée)** sans configurer de **MAC Address (Adresse MAC)**. Dans ce cas, le serveur DHCP n'affecte la **Reserved Address (Adresse réservée)** à aucun pare-feu. Vous pouvez réserver plusieurs adresses du pool et les affecter de manière statique à une imprimante et un fax, par exemple, sans utiliser DHCP.

Serveur DHCP

- Réseau > DHCP > Serveur DHCP

La section suivante décrit chaque composant du serveur DHCP. Avant de configurer un serveur DHCP, assurez-vous d'avoir configuré une interface Ethernet ou VLAN de couche 3 et de l'avoir affectée à un routeur virtuel et une zone. Vous devez également connaître un pool valide d'adresses IP de votre plan réseau qui peut être désigné pour être affecté par votre serveur DHCP aux clients.

Lors de l'ajout d'un serveur DHCP, vous devez configurer les paramètres décrits dans le tableau ci-dessous :

Paramètres d'un serveur DHCP	Configuré dans	Description
Interface	**Serveur DHCP**	Nommez l'interface qui servira de serveur DHCP.
Mode		Sélectionnez **enabled (activé)** ou le mode **auto (automatique)**. Le mode **Auto (Automatique)** active le serveur et le désactive si un autre serveur DHCP est détecté sur le réseau. Le paramètre **disabled (désactivé)** désactive le serveur.
Envoyer une requête ping à l'adresse IP lors de l'allocation d'une nouvelle adresse IP	**Serveur DHCP** > **Crédit-bail**	Si vous cliquez sur **Ping IP when allocating new IP (Envoyer une requête ping à l'adresse IP lors de l'allocation d'une nouvelle adresse IP)**, le serveur envoie un message ping à l'adresse IP avant d'affecter cette adresse à son client. Si le message ping reçoit une réponse, cela signifie qu'un autre pare-feu dispose déjà de cette adresse ; celle-ci n'est donc pas disponible pour l'affectation. Le serveur affecte alors l'adresse suivante du pool. Si vous choisissez cette option, la colonne Sonder l'adresse IP sera cochée.
Crédit-bail		Indiquez un type de bail. • **Unlimited (Illimité)** : le pare-feu choisit de manière dynamique les adresses IP de ses pools d'adresses IP et les affecte définitivement aux clients. • **Timeout (Délai d'expiration)** : cette option détermine la durée du bail. Saisissez le nombre de **Days (Jours)**, **Hours (Heures)** et éventuellement **Minutes**.
Pools d'adresses IP		Indiquez le pool d'adresses IP dynamiques dans lequel le serveur DHCP choisit une adresse et l'affecte à un client DHCP. Vous pouvez saisir une adresse unique, une adresse/<mask length>, telle que 192.168.1.0/24, ou une plage d'adresses, telle que 192.168.1.10-192.168.1.20.
Adresse réservée		Vous pouvez indiquer une adresse IP (format x.x.x.x) des pools d'adresses IP que vous ne souhaitez pas voir affectée de façon dynamique par le serveur DHCP. Si vous spécifiez une **MAC Address (Adresse MAC)** (format xx:xx:xx:xx:xx:xx), la **Reserved Address (Adresse réservée)** est affectée au pare-feu associé à

Paramètres d'un serveur DHCP	Configuré dans	Description
		cette adresse MAC lorsqu'il demande une adresse IP via DHCP.
Source de l'héritage	**Serveur DHCP** > **Options**	Laissez **None (Aucune)** (par défaut) ou sélectionnez une interface client PPPoE ou DHCP source pour propager les divers paramètres du serveur sur le serveur DHCP. Si vous indiquez la **Inheritance Source (Source de l'héritage)**, sélectionnez une ou plusieurs options **inherited (héritées)** de cette source ci-dessous. L'un des avantages de la spécification de la source d'héritage est le transfert rapide des options DHCP du serveur qui se trouve en amont du client DHCP source. Celle-ci permet également de maintenir les options du client à jour en cas de modification sur la source de l'héritage. Par exemple, si le pare-feu source de l'héritage remplace son serveur NTP (qui a été identifié comme serveur **Primary NTP (NTP principal)**), le client héritera automatiquement de la nouvelle adresse en tant que son serveur **Primary NTP (NTP principal)**.
Vérifier l'état de la source de l'héritage		Si vous sélectionnez une **Inheritance Source (Source de l'héritage)**, cliquez sur **Check inheritance source status (Vérifier l'état de la source de l'héritage)** pour ouvrir la fenêtre Statut de l'interface IP dynamique, qui affiche les options héritées du client DHCP.
Passerelle	**Serveur DHCP** > **Options (suite)**	Adresse IP de la passerelle réseau (une interface sur le pare-feu) permettant d'accéder à chaque périphérique situé sur un autre réseau local que ce serveur DHCP.
Masque de sous-réseau		Indiquez le masque réseau qui s'applique aux adresses figurant dans le champ **IP Pools (Pools d'adresses IP)**.
Options (Options)		Pour les champs suivants, cliquez sur la liste déroulante et sélectionnez **None (Aucun)** ou **inherited (hérité)** ou saisissez l'adresse IP du serveur distant que votre serveur DHCP enverra aux clients pour accéder à ce service. Si vous sélectionnez **inherited (hérité)**, le serveur DHCP hérite des valeurs du client DHCP source indiqué comme **Inheritance Source (Source de l'héritage)**.

Paramètres d'un serveur DHCP	Configuré dans	Description
		Le serveur DHCP envoie ces paramètres à ses clients. • **Primary DNS (DNS principal)**, **Secondary DNS (DNS secondaire)** : adresse IP des serveurs Domain Name System (système de noms de domaine ; DNS) préféré et alternatif. • **Primary WINS (WINS principal)**, **Secondary WINS (WINS secondaire)** – Adresse IP des serveurs WINS (Windows Internet Name Service) préférés et alternatifs. • **Primary NIS (NIS principal)**, **Secondary NIS (NIS secondaire)** : adresse IP des serveurs Network Information Service (service d'informations réseau ; NIS) préférés et alternatifs. • **Primary NTP (NTP principal)**, **Secondary NTP (NTP secondaire)** – Adresse IP des serveurs NTP (Serveur du protocole de temps du réseau) préférés et alternatifs. • **POP3 Server (Serveur POP3)** : adresse IP du serveur POP3 (Post Office Protocol version 3). • **SMTP Server (Serveur SMTP)** : adresse IP du serveur Simple Mail Transfer Protocol (protocole simple de transfert de courrier ; SMTP). • **DNS Suffix (Suffixe DNS)** : suffixe que le client pourra utiliser localement lors de la saisie d'un nom d'hôte non qualifié irrésoluble.
Options DHCP personnalisées		Cliquez sur **Add (Ajouter)** et saisissez le **Name (Nom)** de l'option personnalisée que vous souhaitez que le serveur DHCP envoie aux clients. Saisissez un **Option Code (Code d'option)** (intervalle compris entre 1 et 254). Si un **Option Code 43 (Code d'option 43)** est saisi, le champ Identificateur de classe du fournisseur (VCI) s'affiche. Saisissez un critère de correspondance qui sera comparé au VCI provenant de l'option 60 du client. Le pare-feu examine le VCI provenant de l'option 60 du client, trouve le VCI correspondant dans la table du serveur DHCP et renvoie la valeur correspondante au client dans l'option 43. Le critère de correspondance du VCI est une chaîne ou une valeur hexadécimale. Une valeur hexadécimale doit avoir un préfixe « 0x ».

Paramètres d'un serveur DHCP	Configuré dans	Description
		Sélectionnez **Inherited from DCHP server inheritance source (Hérité de la source de l'héritage du serveur DHCP)** pour que le serveur hérite de la valeur de ce code d'option de la source de l'héritage au lieu de saisir une **Option Value (Valeur d'option)**. Vous pouvez également procéder comme suit : **Option Type (Type d'option)** : sélectionnez **IP Address (Adresse IP)**, **ASCII** ou **Hexadecimal (Hexadécimal)** pour indiquer le type de données utilisé pour la Valeur de l'option. Pour **Option Value (Valeur de l'option)**, cliquez sur **Add (Ajouter)** et saisissez la valeur de l'option personnalisée.

Relais DHCP

- Réseau > DHCP > Relais DHCP

Avant de configurer une interface de pare-feu en tant que relais DHCP, assurez-vous d'avoir configuré une interface Ethernet ou VLAN de Niveau 3 et de l'avoir affectée à un routeur virtuel et à une zone. Vous souhaitez que cette interface puisse transmettre des messages DHCP entre les clients et les serveurs. Chaque interface peut transmettre des messages à un maximum de huit serveurs DHCP IPv4 externes et de huit serveurs DHCP IPv6 externes. Un client envoie un message DHCPDISCOVER à tous les serveurs configurés, et le pare-feu relaye le message DHCPOFFER du premier serveur qui répond au client qui a effectué la demande.

Paramètres d'un relais DHCP	Description
Interface	Nommez l'interface qui servira d'agent de relais DHCP.
IPv4/IPv6	Sélectionnez le type de serveur DHCP et d'adresse IP que vous indiquerez.
Adresse IP du serveur DHCP	Saisissez l'adresse IP du serveur DHCP duquel et auquel vous relayerez les messages DHCP.
Interface	Si vous avez sélectionné IPv6 comme protocole d'adresse IP pour le serveur DHCP et spécifié une adresse multicast, vous devez également indiquer une interface sortante.

Client DHCP

- Réseau > Interfaces > Ethernet > IPv4

- Réseau > Interfaces > VLAN > IPv4

Avant de configurer une interface de pare-feu en tant que client DHCP, assurez-vous d’avoir configuré une interface Ethernet ou VLAN de Niveau 3 et de l’avoir affectée à un routeur virtuel et à une zone. Effectuez cette tâche si vous devez utiliser DHCP pour demander une adresse IPv4 pour une interface sur votre pare-feu.

Paramètres d'un client DHCP	Description
Type	Sélectionnez l'option **DHCP Client (Client DHCP)**, puis **Enable (Activer)** pour configurer cette interface en tant que client DHCP.
Créer automatiquement un itinéraire par défaut en direction de la passerelle par défaut fournie par le serveur	Le pare-feu crée un itinéraire statique vers la passerelle par défaut qui sera utile lorsque les clients tenteront d'accéder à de nombreuses destinations qui n'ont pas besoin de conserver des itinéraires dans une table de routage sur le pare-feu.
Mesure d'itinéraire par défaut	Saisissez éventuellement une **Default Route Metric (Mesure d'itinéraire par défaut)** (niveau de priorité) pour l'itinéraire entre le pare-feu et le serveur DHCP. Plus la valeur de l'itinéraire est faible, plus sa priorité de sélection est élevée. Par exemple, un itinéraire avec une valeur métrique de 10 est utilisé avant un itinéraire avec une valeur métrique de 100 (intervalle compris entre 1 et 65 535 ; aucune valeur définie par défaut).
Afficher les informations d'exécution du client DHCP	Affiche tous les paramètres reçus par le serveur DHCP, y compris le statut du bail DHCP, l'attribution de l'adresse IP dynamique, le masque de sous-réseau, la passerelle, les paramètres du serveur (DNS, NTP, domaine, WINS, NIS, POP3 et SMTP).

Réseau > Proxy DNS

Les serveurs DNS fournissent le service de résolution d'un nom de domaine en adresse IP et vice-versa. Lorsque vous configurez le pare-feu en tant que proxy DNS, il agit comme un intermédiaire entre les clients et les serveurs, et comme un serveur DNS en résolvant les requêtes du cache DNS ou en transférant les requêtes à d'autres serveurs DNS. Cette page vous permet de configurer les paramètres qui déterminent comment le pare-feu sert de proxy DNS.

Que voulez-vous savoir ?	Reportez-vous à la section :
Comment le pare-feu sert de proxy pour les requêtes DNS?	Présentation du proxy DNS
Comment puis-je configurer un proxy DNS ?	Paramètres du proxy DNS
Comment puis-je configurer les mappages d'adresse FQDN vers les IP statiques ?	
Comment puis-je gérer les proxys DNS ?	Actions de proxy DNS supplémentaires
Vous souhaitez en savoir plus ?	DNS

Présentation du proxy DNS

Vous pouvez configurer le pare-feu pour qu'il agisse en tant que serveur DNS. Tout d'abord, créez un proxy DNS et sélectionnez les interfaces auxquelles s'applique le proxy. Ensuite, spécifiez les serveurs primaires et secondaires DNS par défaut auxquels le pare-feu envoie les requêtes DNS lorsqu'il ne trouve pas le nom de domaine dans le cache du proxy DNS (et lorsque le nom de domaine ne correspond pas à une règle de proxy).

Pour diriger les requêtes DNS vers différents serveurs DNS en fonction des noms de domaine, créez des règles de proxy DNS. L'indication de plusieurs serveurs DNS peut assurer la localisation des requêtes DNS et améliorer l'efficacité. Par exemple, vous pouvez transférer toutes les requêtes DNS vers un serveur DNS d'entreprise et transférer toutes les autres requêtes vers des serveurs DNS fournisseurs de services Internet.

Utilisez les onglets suivants pour définir un proxy DNS (au-delà des serveurs DNS primaires et secondaires par défaut) :

- **Entrées statiques** – Vous permet de configurer les mappages d'adresse FQDN vers les IP statiques que le pare-feu met en cache et envoie aux hôtes en réponse aux requêtes DNS.
- **Règles de proxy DNS** – Vous permet de spécifier les noms de domaine et les serveurs DNS principaux et secondaires correspondants pour résoudre les requêtes qui correspondent à la règle. Si le nom de domaine est introuvable dans le cache du proxy DNS, le pare-feu recherche une correspondance dans le proxy DNS (sur l'interface sur laquelle la requête est parvenue) et la transmet la requête à un serveur DNS en fonction des résultats de correspondance. Si aucun résultat ne correspond, le pare-feu

envoie la requête aux serveurs DNS primaires et secondaires par défaut. Vous pouvez activer la mise en cache des domaines qui correspondent à la règle.

- **Avancé** - Vous devez activer la mise en cache (sélectionnez **Cache**) et **Cache EDNS Responses (Réponse EDNS Cache)** si l'objet proxy DNS sera utilisé pour résoudre les requêtes DNS/FQDN que le pare-feu génère. L'onglet Avancé vous permet aussi de contrôler les requêtes TCP et les nouvelles tentatives de requêtes UDP. Le pare-feu envoie des requêtes UDP DNS ou TCP par l'intermédiaire de l'interface configurée. Les requêtes UDP basculent vers TCP lorsque la réponse d'une requête DNS est trop longue pour un seul paquet UDP.

Paramètres du proxy DNS

Cliquez sur **Add (Ajouter)** et configurez le pare-feu pour qu'il agisse en tant que proxy DNS. Vous pouvez configurer jusqu'à un maximum de 256 proxys DNS sur un pare-feu.

Paramètres du proxy DNS	Configuré dans	Description
Activer	**Proxy DNS**	Sélectionnez cette option pour activer ce proxy DNS.
Name (Nom)		Saisissez un nom pour identifier un objet de proxy DNS (**31** caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Location (Emplacement)		Indiquez le système virtuel auquel l'objet de proxy DNS s'applique : • **Shared (Partagé)** : le proxy s'applique à tous les systèmes virtuels. Si vous choisissez **Shared (Partagé)**, le champ **Server Profile (Profil de serveur)** n'est pas disponible. Saisissez plutôt les objets d'adresse ou adresses IP des serveurs DNS **Primary (Principal)** et **Secondary (Secondaire)**. • Sélectionnez un système virtuel qui utilisera ce proxy DNS ; vous devez d'abord configurer un système virtuel. Sélectionnez **Device (Périphérique)** > **Virtual Systems (Systèmes virtuels)**, sélectionnez un système virtuel, puis sélectionnez un **DNS Proxy (Proxy DNS)**.
Source de l'héritage (Emplacement partagé uniquement)		Sélectionnez une source de laquelle hériter des paramètres du serveur DNS par défaut. Cette méthode est couramment utilisée dans les déploiements de bureaux de filiales dans lesquels l'interface WAN du pare-feu est prise en charge par DHCP ou PPPoE.
Vérifier l'état de la source de l'héritage		Sélectionnez cette option pour afficher les paramètres des serveurs qui sont actuellement affectés aux interfaces client DHCP et client PPPoE. Ces paramètres peuvent

Paramètres du proxy DNS	Configuré dans	Description
(Emplacement partagé uniquement)		inclure DNS, WINS, NTP, POP3, SMTP ou un suffixe DNS.
Principal/Secondaire (Emplacement partagé uniquement)		Spécifiez les adresses IP des serveurs DNS primaires et secondaires par défaut auxquels ce pare-feu (en tant que proxy DNS) envoie des requêtes DNS. Si le serveur DNS principal est introuvable, le pare-feu utilise le serveur DNS secondaire.
Profil de serveur (Emplacement du système virtuel uniquement)		Sélectionnez ou créez un nouveau profil de serveur DNS. Ce champ ne s'affiche pas si l'emplacement des systèmes virtuels a été indiqué comme Partagé.
Interface		Vous devez **Add (Ajouter)** une interface pour qu'elle fonctionne en tant que proxy DNS. Vous pouvez ajouter plusieurs interfaces. Pour supprimer le proxy DNS de l'interface, sélectionnez-le et cliquez sur **Delete (Supprimer)**. Une interface n'est pas requise si le proxy DNS est utilisé uniquement pour la fonctionnalité d'itinéraire de service. Utilisez un itinéraire de service de destination avec un proxy DNS sans interface si vous souhaitez que l'itinéraire de service de destination définisse l'adresse IP source. Sinon, le proxy DNS sélectionne une adresse IP d'interface à utiliser comme source (lorsqu'aucun itinéraire de service DNS n'est défini).
Nom	**Proxy DNS** > **Règles de proxy DNS**	Un nom est requis pour qu'une entrée puisse être référencée et modifiée via la CLI.
Activer la mise en cache des domaines résolus par ce mappage		Sélectionnez cette option pour activer la mise en cache des domaines non résolus par ce mappage.
nom de domaine		Vous devez **Ajouter** un ou plusieurs noms de domaine auxquels le pare-feu compare les FQDN entrants. Si le FQDN correspond à l'un des domaines de la règle, le pare-feu transmet la requête au serveur DNS primaire / secondaire spécifié pour ce proxy. Pour supprimer un nom de domaine, sélectionnez-le, puis cliquez sur **Supprimer**.
DNS Server Profile (profil de serveur DNS)		Sélectionnez ou ajoutez un profil de serveur DNS pour définir les paramètres DNS pour le système virtuel, y

Paramètres du proxy DNS	Configuré dans	Description
(Emplacement partagé uniquement)		compris les serveurs DNS principaux et secondaires auquel le pare-feu transmet des requêtes de noms de domaine.
Principal/Secondaire (Emplacement du système virtuel uniquement)		Saisissez le nom d'hôte ou l'adresse IP des serveurs DNS principaux et secondaires auxquels le pare-feu envoie les requêtes de noms de domaine compatibles.
Nom	**Proxy DNS** > **Entrées statiques**	Saisissez un nom pour l'entrée statique.
Nom de domaine complet		Saisissez le nom de domaine complet (FQDN) à mapper aux adresses IP statiques définies dans le champ Adresse.
Adresse		Cliquez sur **Ajouter** pour ajouter une ou plusieurs adresses IP à mapper à ce domaine. Le pare-feu inclut toutes ces adresses dans sa réponse DNS et le client choisit l'adresse IP à utiliser. Pour supprimer une adresse, sélectionnez-la et cliquez sur **Delete (Supprimer)**.
Requêtes TCP	**Proxy DNS** > **Avancé**	Sélectionnez cette option pour activer des requêtes DNS à l'aide de TCP. Indiquez le nombre maximum de requêtes simultanées DNS TCP en attente (**Max Pending Requests (Nombre max. de requêtes en attente)**) que le pare-feu prend en charge (plage comprise entre 64 et 256 ; par défaut 64).
Nouvelles tentatives de requêtes UDP	**Proxy DNS** > **Avancé**	Spécifiez des paramètres pour les nouvelles tentatives de requête UDP : • **Interval (Intervalle)** – Temps, en secondes, après lequel le proxy DNS envoie une autre requête s'il n'a pas reçu de réponse (la plage est comprise entre 1 et 30, la valeur par défaut est 30). • **Attempts (Tentatives)** – Le nombre maximum de tentatives (hormis la première) après lesquelles le proxy DNS essaie le serveur DNS suivant (plage comprise entre 1 et 30 ; par défaut 5).
Cache	**Proxy DNS** > **Avancé**	Vous devez activer la fonction **Cache** (activé par défaut) si cet objet proxy DNS est utilisé pour des requêtes que le pare-feu génère (dans la section **Device [Périphérique]** > **Setup [Configuration]** > **Services** > **DNS**, ou dans la section **Device [Périphérique]** > **Virtual Systems [Systèmes virtuels]**, vous sélectionnez un système virtuel et ensuite **General [Général]** > **DNS Proxy [Proxy DNS]**). Indiquez ensuite les options suivantes :

Paramètres du proxy DNS	Configuré dans	Description
		• **Enable TTL (Activer TTL)** – Limitez la durée pendant laquelle le pare-feu met en cache les entrées DNS pour l'objet proxy. TTL est désactivé par défaut. Ensuite, saisissez la **Time to Live (sec) (Durée de vie (sec))** – le nombre de secondes après lesquelles toutes les entrées mises en cache pour l'objet proxy sont supprimées et les nouvelles requêtes DNS doivent être résolues et remises en cache. Plage comprise entre 60 et 86 400. Il n'y a pas de TTL par défaut ; les entrées restent jusqu'à ce que le pare-feu n'ait plus de mémoire cache. • **Cache EDNS Responses (Réponses EDNS Cache)** - Vous devez activer les mécanismes d'extension de cache pour les réponses DNS (EDNS) si cet objet proxy DNS est utilisé pour les requêtes que le pare-feu génère. Le pare-feu doit pouvoir mettre en cache les réponses DNS pour que les requêtes d'objets d'adresse FQDN réussissent.

Actions de proxy DNS supplémentaires

Après configuration du pare-feu en tant que proxy DNS, vous pouvez effectuer les actions suivantes sur la page **Réseau** > **Proxy DNS** pour gérer les configurations du proxy DNS :

- **Modifier** - Pour modifier un proxy DNS, cliquez sur le nom de la configuration de proxy DNS.
- **Supprimer** - Sélectionnez une entrée de proxy DNS, cliquez sur **Supprimer** pour supprimer la configuration de proxy DNS.
- **Désactiver** - Pour désactiver un proxy DNS, cliquez sur le nom de l'entrée de proxy DNS et désélectionnez l'option **Activer**. Pour activer un proxy DNS qui a été désactivé, cliquez sur le nom de l'entrée de proxy DNS et sélectionnez **Activer**.

Proxy > réseau

La disponibilité des options de configuration du proxy dépend du type de proxy. Vous devez d'abord configure a DNS proxy object (configurer un objet proxy DNS) pour configurer un proxy.

Champs proxy	Description
Activation du proxy	
Type de proxy	Sélectionnez le type de proxy que vous souhaitez utiliser. • **None (Aucun)** : le proxy est désactivé. • **Explicite**: configurez le proxy de sorte que la demande contienne l'adresse IP de destination du proxy configuré et que le navigateur client envoie directement les demandes au proxy. • **Transparent**: configurez le proxy de sorte que la demande contienne l'adresse IP de destination du serveur Web et que le navigateur client soit redirigé vers le proxy. *Transparent Proxy requires a specific Destination NAT (Le proxy transparent nécessite une règle de stratégie NAT de destination) (DNAT)spécifique pour configurer correctement le proxy Web. Reportez-vous à la documentation du PAN-OS Networking Administrator's Guide (Guide de l'administrateur réseau PAN-OS) pour obtenir la procédure complète.*
Configuration des proxys	
Délai d'expiration de la connexion	Spécifiez (en secondes) combien de temps le proxy attend une réponse du serveur Web. La plage est comprise entre 1 et 60 secondes et la valeur par défaut est de 5 secondes. S'il n'y a pas de réponse après l'expiration du délai spécifié, le proxy ferme la connexion.
Interface d'écoute Proxy explicite uniquement	Spécifiez l'interface de couche 3 (L3) dans laquelle le pare-feu vérifie le réacheminement du trafic vers le proxy.
Interface en amont	Sélectionnez l'interface en amont.

Champs proxy	Description
	*Si vous utilisez une interface de bouclage, spécifiez cette interface comme **Upstream Interface (interface en amont)**.*
Proxy IP	Spécifiez l'adresse IP de l'interface où le pare-feu doit vérifier le trafic à rediriger vers le proxy (interface d'écoute).
Proxy DNS	Sélectionnez l'DNS proxy object (objet proxy DNS) que vous souhaitez utiliser pour la connexion proxy.
Vérifier le domaine dans CONNECT & SNI sont les mêmes Proxy explicite uniquement	Activez cette option pour empêcher les attaques frontales de domaine provoquées par la spécification de domaines différents entre la demande CONNECT et le champ SNI (Server Name Indication) dans l'en-tête HTTP.
Type de service d'authentification Proxy explicite uniquement	Sélectionnez le type de service que vous souhaitez utiliser pour authentifier les utilisateurs. • **SAML/CAS**: utilisez un service d'authentification basé sur SAML 2.0 ou le service d'authentification disponible dans Cloud Identity Engine (moteur d'identité de cloud). *Cette option nécessite Prisma Access, le plug-in Cloud Services 3.2.1 et la licence proxy Web complémentaire.* • **Kerberos Single Sign On (Authentification unique Kerberos** : utilisez le service Kerberos Single Sign-On Service (service d'authentification unique Kerberos) pour authentifier les utilisateurs. *Cette option nécessite Panorama, une licence de proxy Web et un profil d'authentification qui utilise le Kerberos Single Sign-On Service (service d'authentification unique Kerberos) sur le pare-feu.*
Profil d'authentification Proxy explicite uniquement	Sélectionnez le profil d'authentification que vous souhaitez utiliser pour le **Authentication service type (type de service d'authentification)** que vous avez sélectionné pour l'option précédente.

Réseau > QoS

Les rubriques suivantes décrivent la Qualité de service (QoS).

Que voulez-vous faire ?	Reportez-vous à la section :
Définissez les limites de bande passante pour une interface et mettez en œuvre la QoS pour le trafic sortant d'une interface.	Paramètres d'une interface de QoS
Surveiller le trafic existant sur une interface sur laquelle la QoS est activée.	Statistique de l'interface QoS
Vous souhaitez en savoir plus ?	Voir Qualité de service pour avoir accès à un flux de travail QoS complet, des concepts et des cas pratiques.
	Sélectionnez Policies > QoS (Politiques > QoS) pour affecter une classe QoS au trafic mis en correspondance ou sélectionnez Network > Network Profiles > QoS (Profils de réseau > QoS) pour définir des limites de bande passante et une priorité pour un maximum de huit classes QoS.

Paramètres d'une interface de QoS

Activez la QoS sur une interface pour définir les limites de bande passante de l'interface et/ou de permettre à l'interface de mettre en œuvre la QoS pour le trafic sortant. L'activation d'une interface de QoS inclut l'association d'un profil de QoS à l'interface. La QoS est prise en charge sur les interfaces physiques et, selon le modèle de pare-feu, également sur les sous-interfaces et les interfaces Ethernet agrégées (AE). Pour savoir si la fonction QoS est prise en charge par votre modèle de pare-feu, utilisez l'outil de comparaison de produits Palo Alto Networks.

Pour commencer, vous devez **Ajouter** ou modifier une interface de QoS, puis configurer les paramètres comme décrits dans le tableau suivant.

Paramètres d'une interface de QoS	Configuré dans	Description
Nom de l'interface	**QoS Interface > Interface physique**	Sélectionnez l'interface de pare-feu sur laquelle activer la QoS.
Sortie max. (Mbits/s)		Entrez le débit maximum (en Mbits/s) pour le trafic sortant du pare-feu via cette interface. La valeur par défaut est 0, laquelle définit la limite autorisée sur le pare-feu (60 000 Mbits/s sur PAN-OS

Paramètres d'une interface de QoS	Configuré dans	Description
		7.1.16 et les versions ultérieures ; 16 000 sur PAN-OS 7.1.15 et les versions antérieures). *Bien qu'il ne s'agisse pas d'un champ obligatoire, nous recommandons de toujours définir la valeur de **Egress Max (Sortie max.)** d'une interface de QoS.*
Activer la fonction QoS sur cette interface		Sélectionnez pour activer la QoS sur l'interface sélectionnée.
Interface de tunnel en texte clair	**QoS Interface > Interface physique > Profil par défaut**	Sélectionnez les profils de QoS par défaut pour le trafic en texte clair et par tunnel. Vous devez définir un profil par défaut pour chacun. Pour le trafic en texte clair, le profil par défaut s'applique à l'ensemble du trafic en texte clair en tant que profil agrégé. Pour le trafic par tunnel, le profil par défaut s'applique individuellement à chaque tunnel ne disposant d'aucune attribution de profil spécifique dans la section de configuration détaillée. Pour obtenir des instructions sur la définition des profils QoS, reportez-vous à Réseau > Profils réseau > QoS.
en texte clair		
Sortie garantie (Mbits/s)	**QoS Interface > Trafic en texte clair / Trafic tunnelisé**	Saisissez la bande passante garantie pour le trafic en texte clair ou par tunnel depuis cette interface.
Sortie max. (Mbits/s)		Entrez le débit maximum (en Mbits/s) pour le trafic en texte clair ou par tunnel sortant du pare-feu via cette interface. La valeur par défaut est 0, laquelle définit la limite autorisée sur le pare-feu (60 000 Mbits/s sur PAN-OS 7.1.16 et les versions ultérieures ; 16 000 sur PAN-OS 7.1.15 et les versions antérieures). La valeur de **Egress Max (Sortie max.)** du trafic en texte clair ou par tunnel ne doit pas dépasser la valeur de **Egress Max (Sortie max.)** de l'interface physique.
Ajouter		• Dans l'onglet **Clear Text Traffic (Trafic en texte clair)**, cliquez sur **Add (Ajouter)** pour définir la granularité supplémentaire au traitement du trafic en texte clair. Cliquez sur chaque entrée pour configurer les paramètres suivants : • **Name (Nom)** - Donnez un nom à ces paramètres afin de les identifier. • **QoS Profile (Profil de QoS)** - Sélectionnez le profil de QoS à appliquer à l'interface et au sous-réseau spécifiés. Pour obtenir des instructions sur la définition des profils QoS, reportez-vous à Réseau > Profils réseau > QoS.

Paramètres d'une interface de QoS	Configuré dans	Description
		• **Source Interface (Interface source)** - Sélectionnez l'interface de pare-feu. • **Destination interface (Interface de destination)** : (PA-3200 Series, PA-5200 Series, PA-5400 Series, PA-7000 Series only (série PA-3200, série PA-5200, série PA-5400, série PA-7000 uniquement)) Sélectionnez l'interface de destination à laquelle le trafic est destiné. • **Source Subnet (Sous-réseau source)** - Sélectionnez un sous-réseau pour limiter les paramètres au trafic provenant de cette source ou conservez la valeur **Indifférent** par défaut pour appliquer les paramètres à n'importe quel trafic de l'interface spécifiée. • Dans l'onglet **Tunneled Traffic (Trafic par tunnel)**, cliquez sur **Add (Ajouter)** pour appliquer un contrôle prioritaire sur l'affectation du profil par défaut de tunnels spécifiques, puis configurez les paramètres suivants : • **Tunnel Interface (Interface de tunnel)** - Sélectionnez l'interface de tunnel sur le pare-feu. • **QoS Profile (Profil de QoS)** - Sélectionnez le profil de QoS à appliquer à l'interface de tunnel spécifiée. Prenons comme exemple la configuration de deux sites, dont l'un dispose d'une connexion à 45 Mbits/s et l'autre d'une connexion T1 au pare-feu. Vous pouvez appliquer des paramètres de QoS restrictifs au site T1 afin que la connexion ne soit pas saturée, tout en autorisant des paramètres plus flexibles pour le site disposant d'une connexion à 45 Mbits/s. Pour supprimer une entrée de trafic en texte clair ou par tunnel, supprimez l'entrée et cliquez sur **Delete (Supprimer)**. Si les sections Trafic en texte clair et Trafic par tunnel ne sont pas renseignées, les valeurs définies dans la section Profil par défaut de l'onglet Interface physique sont utilisées.

Statistique de l’interface QoS

- Réseau > QoS > Statistiques

Pour une interface de QoS, sélectionnez **Statistics (Statistiques)** pour afficher les informations de bande passante, de session et d'application relatives aux interfaces de QoS.

Statistiques QoS	Description
Bande passante	Affiche les diagrammes de bande passante en temps réel pour le nœud et les classes sélectionnés. Ces informations sont mises à jour toutes les deux secondes. *les limitations Sortie max. et Sortie garantie de QoS configurées pour les classes QoS peuvent avoir une valeur légèrement différente dans l'écran Statistiques de QoS. Il s'agit d'un comportement normal qui est causé par la manière dont le moteur matériel résume les compteurs et les limites de bande passante. Il n'y a aucun problème opérationnel, car les graphiques d'utilisation de bande passante affichent les valeurs et les quantités en temps réel.*
Applications	Affiche toutes les applications actives du nœud et/ou de la classe de QoS sélectionné(e)(s).
Utilisateurs sources	Affiche tous les utilisateurs sources actifs du nœud et/ou de la classe de QoS sélectionné(e)(s).
Utilisateurs de destination	Affiche tous les utilisateurs de destination actifs du nœud et/ou de la classe de QoS sélectionné(e)(s).
Règles de sécurité	Affiche les règles de sécurité mises en correspondance et mettant en œuvre le nœud et/ou la classe de QoS.
Règles de QoS	Affiche les règles de QoS mises en correspondance et mettant en œuvre le nœud et/ou la classe de QoS.

Réseau > LLDP

LLD (Link Layer Discovery Protocol/protocole de découverte de couche liaison) fournit une méthode automatique de détection de périphériques voisins et de leurs fonctionnalités au niveau de la couche de liaison.

Que voulez-vous faire ?	Reportez-vous à la section :
Qu'est-ce que LLDP ?	Présentation de LLDP
Configuration de LLDP.	Étapes de configuration de LLDP
Configuration d’un profil LLDP.	Réseau > Profils réseau > Profil LLDP
Vous souhaitez en savoir plus ?	LLDP

Présentation de LLDP

LLDP permet au pare-feu d'envoyer et de recevoir des trames Ethernet contenant des unités de données LLDP (LLDPDU) depuis et vers les voisins. Le périphérique de réception stocke les informations dans une MIB, accessible par le protocole SNMP (Simple Network Management Protocol/protocole de gestion de réseau simple). LLDP permet aux périphériques réseau de mapper leur topologie de réseau et d’apprendre les fonctionnalités des périphériques connectés. Cela facilite la résolution des problèmes, en particulier pour les déploiements de câble virtuel où le pare-feu n’est généralement pas détecté dans une topologie de réseau.

Étapes de configuration de LLDP

Pour activer LLDP sur le pare-feu, cliquez sur Modifier, puis sur **Activer**. Vous pouvez configurer les quatre paramètres affichés dans le tableau ci-dessous, si les paramètres par défaut ne sont pas adaptés à votre environnement. Les entrées restantes du tableau décrivent l'état et les statistiques de l'homologue.

Paramètres LLDP	Configuré dans	Description
Intervalle de transmission (s)	**LLDP Général**	Précisez l'intervalle, en secondes, auquel les LLDPDU sont transmis (intervalle compris entre 1 et 3 600 ; valeur par défaut : 30).
Délai de transmission (s)		Indiquez le délai, en secondes, entre les transmissions LLDP envoyées après une modification apportée à un élément TLV (Type-Longueur-Valeur). Ce délai permet d'éviter la saturation du segment avec les LLDPDU si de nombreuses modifications réseau dépassent le nombre de modifications LLDP ou en cas de battement de l'interface. Le **délai de transmission** doit

Paramètres LLDP	Configuré dans	Description
		être inférieur à **Intervalle de transmission** (intervalle compris entre 1 et 600 ; valeur par défaut : 2).
Temps d'attente multiple		Spécifiez une valeur qui est multipliée par **intervalle de transmission** pour déterminer le temps d'attente TTL total (intervalle compris entre 1 et 100 ; valeur par défaut : 4). Le temps d'attente TTL est la durée de validité des informations de l'homologue conservées par le pare-feu. Le temps d'attente TTL maximum est de 65 535 secondes, quelle que soit la valeur du multiplicateur.
Intervalle de notification		Indiquez l'intervalle, en secondes, auquel les notifications de piège SNMP et Syslog sont transmises lorsque des modifications sont apportées à la MIB (intervalle compris entre 1 et 3 600 ; valeur par défaut : 5).
Filtre loupe	**LLDP** > **État**	Vous pouvez saisir une valeur de données dans la ligne de filtre et cliquer sur la flèche grise, pour afficher uniquement les lignes qui incluent cette valeur de données. Cliquez sur le X rouge pour effacer le filtre.
Interface		Nommez les interfaces auxquelles des profils LLDP seront affectés.
Type		Types d'interface (tels que Layer 2, Layer 3, Virtual Wire, tap, HA ou Ethernet agrégé) auxquels des profils LLDP sont affectés.
LLDP		État de LLDP : activé ou désactivé.
Pré-négociation HA		État de pré-négociation HA : activé ou désactivé. La pré-négociation LLDP facilite les basculements plus rapides dans les scénarios actifs/passifs HA.
Mode		Mode LLDP de l'interface : Transmission/Réception, Transmission uniquement ou Réception uniquement.
Profil		Nom du profil affecté à l'interface.
Total transmis		Nombre de LLDPDU transmises de l'interface.
Transmission abandonnée		Nombre de LLDPDU non transmises de l'interface en raison d'une erreur. Par exemple, une erreur de longueur lorsque le système construit une LLDPDU pour la transmission.

Paramètres LLDP	Configuré dans	Description
Total reçu		Nombre de trames LLDP reçues sur l'interface.
TLV abandonné		Nombre de trames LLDP supprimées à la réception.
Erreurs		Nombre d'éléments TLV (Type-Longueur-Valeur) reçus sur l'interface qui contiennent des erreurs. Les types d'erreurs TLV sont les suivants : un ou plusieurs éléments TLV obligatoires sont manquants, hors service, contiennent des informations en dehors de la plage admise, ou erreur de longueur.
Non reconnu		Nombre d'éléments TLV reçus sur l'interface qui ne sont pas reconnus par l'agent LLDP local, par exemple, car le type TLV se trouve dans l'intervalle TLV réservé.
Expiré		Nombre d'éléments supprimés de la MIB de réception en raison de l'expiration du TTL.
Effacement des statistiques LLDP		Sélectionnez pour effacer toutes les statistiques LLDP.
Filtre loupe	**LLDP** > **Pairs**	Vous pouvez saisir une valeur de données dans la ligne de filtre et cliquer sur la flèche grise, pour afficher uniquement les lignes qui incluent cette valeur de données. Cliquez sur le X rouge pour effacer le filtre.
Interface locale		Interface sur le pare-feu qui a détecté le périphérique voisin.
ID du châssis distant		ID de châssis de l'homologue ; l'adresse MAC est utilisée.
ID du port	**LLDP** > **Pairs (suite)**	ID de port de l'homologue.
Nom		Nom de l'homologue.
En savoir plus		Cliquez sur **Plus d'informations** pour afficher les détails de l'homologue distant, basés sur les éléments TLV obligatoires et facultatifs.
Type de châssis		Le type de châssis est l'adresse MAC.
Adresse MAC		Adresse MAC de l'homologue.
Nom du système		Nom de l'homologue.

Paramètres LLDP	Configuré dans	Description
Description du système		Description de l'homologue.
Description du port		Description du port de l'homologue.
Type de port		Nom de l'interface.
ID du port		Le pare-feu utilise l'attribut ifName de l'interface.
Fonctionnalités du système		Fonctionnalités du système. O=Other (autre), P=Repeater (répéteur), B=Bridge (pont), W=Wireless-LAN (réseau local sans fil), R=Router (routeur), T=Telephone (téléphone)
Fonctions activées		Fonctionnalités activées sur l'homologue.
Adresse de gestion		Adresse de gestion de l'homologue.

Réseau > Profils réseau

Les rubriques suivantes décrivent les profils réseau :

- Réseau > Profils réseau > Crypto IPSec GlobalProtect
- Réseau > Profils réseau > Passerelles IKE
- Réseau > Profils réseau > Crypto IPSec
- Réseau > Profils réseau > Crypto IKE
- Réseau > Profils réseau > Surveillance
- Réseau > Profils réseau > Gestion de l'interface
- Réseau > Profils réseau > Protection de zone
- Réseau > Profils réseau > QoS
- Réseau > Profils réseau > Profil LLDP
- Réseau > Profils réseau > Profil BFD
- Réseau > Profils réseau > Profil d’interface SD-WAN

Réseau > Profils réseau > Crypto IPSec GlobalProtect

La page **GlobalProtect IPSec Crypto Profiles (Profils cryptographiques IPSec GlobalProtect)** vous permet de spécifier les algorithmes d'authentification et de chiffrement dans les tunnels VPN entre des clients et une passerelle GlobalProtect. L'ordre d'ajout des algorithmes est leur ordre d'application par le pare-feu, et peut affecter la sécurité et les performances du tunnel. Pour changer l'ordre, sélectionnez un algorithme et **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)**.

Pour les tunnels VPN entre les passerelles GlobalProtect et les satellites (pare-feu), voir Réseau > Profils réseau > Crypto IPSec.

Paramètres d’un profil cryptographique IPSec GlobalProtect	
Name (Nom)	Saisissez un nom pour identifier le profil. Le nom est sensible à la casse, doit être unique et peut comporter **31** caractères maximum. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement.
Chiffrement	Cliquez sur **Add (Ajouter)** et sélectionnez les algorithmes de chiffrement de votre choix. Pour une sécurité maximale, changez l'ordre (de haut en bas) en : **aes-256-gcm**, **aes-128-gcm**, **aes-128-cbc**.
Authentification	Cliquez sur **Add (Ajouter)** et sélectionnez l'algorithme d'authentification. Actuellement, la seule option est **sha1**.

Réseau > Profils réseau > Passerelles IKE

Utilisez cette pour gérer ou définir une passerelle contenant les informations de configuration nécessaires à la négociation du protocole IKE (Internet Key Exchange / échange de clés Internet) avec une passerelle homologue. Il s'agit de la phase 1 de la configuration de VPN IKE/IPSec.

Pour gérer, configurer, redémarrer ou actualiser une passerelle IKE, reportez-vous aux sections suivantes :

- Gestion de la passerelle IKE
- Passerelle IKE - Onglet Général
- Passerelle IKE - Onglet Options avancées
- Redémarrage ou actualisation d'une passerelle IKE

Gestion de la passerelle IKE

- Réseau > Profils réseau > Passerelles'A0;IKE

Le tableau suivant explique comment gérer les passerelles IKE.

Gestion des passerelles IKE	Description
Ajouter	Pour créer une nouvelle passerelle IKE, cliquez sur **Add (Ajouter)**. Voir Passerelle IKE – Onglet Général et Passerelle IKE – Onglet Options avancées pour obtenir des instructions sur la configuration de la nouvelle passerelle.
Supprimer	Pour supprimer une passerelle, sélectionnez-la et cliquez sur **Delete (Supprimer)**.
Activer	Pour activer une passerelle qui a été désactivée, sélectionnez-la et cliquez sur **Enable (Activer)**, qui est le paramètre par défaut.
Désactivation	Pour désactiver une passerelle, sélectionnez-la et cliquez sur **Disable (Désactiver)**.
PDF/CSV	Les rôles administrateur qui sont au moins dotés de l’accès en lecture seule peuvent exporter le tableau de configuration de l’objet au format **PDF/ CSV**. Vous pouvez appliquer des filtres pour créer des sorties du tableau de configuration plus précises, par exemple, pour effectuer des audits. Seules les colonnes qui sont visibles dans l’interface Web seront exportées. Reportez-vous à la section Exportation du tableau de configuration.

Passerelle IKE - Onglet Général

- Réseau > Profils réseau > Passerelles IKE > Général

Le tableau suivant décrit les premiers paramètres de configuration d'une passerelle IKE. IKE est la phase 1 du processus de configuration de VPN IKE/IPSec. Après avoir configuré ces paramètres, reportez-vous à la section Onglet Options avancées de passerelle IKE.

Paramètres généraux d’une passerelle IKE	Description
Name (Nom)	Saisissez un **Name (Nom)** pour identifier la passerelle (31 caractères maximum). Celui-ci est sensible aux majuscules et minuscules et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement.
Version	Sélectionnez la version IKE que la passerelle prend en charge et doit accepter d'utiliser avec la passerelle homologue : **IKEv1 only mode (Mode IKEv1 uniquement)**, **IKEv2 only mode (Mode IKEv2 uniquement)** ou **IKEv2 preferred mode (Mode IKEv2 préféré)**. Le mode IKEv2 préféré entraîne la négociation IKEv2 par la passerelle, et c'est ce mode qu'elles utiliseront si la passerelle homologue prend également en charge IKEv2 ; sinon, la passerelle revient à IKEv1.
Type d'adresse	Sélectionnez le type d'adresse IP que la passerelle utilise. **IPv4** ou **IPv6**.
Interface	Spécifiez l'interface de tunnel VPN sortante sur le pare-feu.
Adresse IP locale	Sélectionnez ou saisissez l'adresse IP de l'interface locale correspondant au point d'extrémité du tunnel.
Type d’ Adresse IP de l'homologue	Sélectionnez l’un des paramètres suivants et saisissez les informations correspondantes de l’homologue : • **Dynamic (Dynamique)** : sélectionnez cette option si l’adresse IP ou la valeur FQDN de l'homologue est inconnue. Lorsque le type d’adresse IP de l’homologue est défini sur Dynamique, il revient à l’homologue de lancer la négociation de la passerelle IKE. • **IP** : saisissez la **Peer Address (Adresse de l'homologue)** en tant qu'adresse IPv4 ou IPv6 ou qu’objet d'adresse correspondant à une adresse IPv4 ou IPv6. • **FQDN** : saisissez la **Peer Address (Adresse de l'homologue)** sous forme de FQDN ou d’objet d'adresse utilisant un FQDN. Si vous saisissez un FQDN ou un objet d'adresse FQDN qui se résout en plus d’une adresse IP, le pare-feu choisit l’adresse préférée dans

Paramètres généraux d’une passerelle IKE	Description
	l’ensemble d’adresses qui correspondent au Type d’adresse (IPv4 ou IPv6) de la passerelle IKE, comme suit : • Si aucune Security Association (association de sécurité ; SA) IKA n’a été négotiée, l’adresse préférée correspond à l’adresse IP qui possède la plus faible valeur. • Si une adresse est utilisée par la passerelle IKE et qu’elle figure dans l’ensemble d’adresses renvoyées, celle-ci est utilisée (qu’elle possède la plus faible valeur ou non). • Si une adresse est utilisée par la passerelle IKE, mais qu’elle ne figure pas dans l’ensemble d’adresses renvoyées, une nouvelle adresse est sélectionnée : celle qui possède la plus faible valeur.  *L’utilisation d’un FQDN ou d’un objet d'adresse FQDN réduit les problèmes d’environnements où l’homologue est soumis aux changements des adresses IP dynamiques (ce qui autrement vous obligerez à reconfigurer l’adresse de cette passerelle IKE homologue).*
Authentification	Sélectionnez le type d'authentification : **Pre-Shared Key (Clé pré-partagée)** ou **Certificate (Certificat)**) qui se produira sur la passerelle homologue. En fonction de la sélection, voir Champs de Clé pré-partagée ou Champs de certificat.
Champs de l’option Clé pré-partagée	
Clé pré-partagée / Confirmer la clé pré-partagée	Si vous sélectionnez **Pre-Shared Key (Clé pré-partagée)**, saisissez une clé de sécurité unique à utiliser pour l’authentification symétrique via le tunnel. La valeur de la **Pre-Shared Key (Clé pré-partagée)** est une chaîne créée par l'administrateur à l'aide d’un maximum de 255 caractères ASCII ou autres. Générez une clé difficile à décoder par des attaques par dictionnaire ; utilisez un générateur de clés pré-partagées, si nécessaire.
Identification locale	Définit le format et l'identification de la passerelle locale, qui sont utilisés avec la clé pré-partagée pour l'établissement d'une SA IKEv1 de phase 1 et d'une SA IKEv2. Sélectionnez l'un des types suivants et saisissez une valeur : **FQDN (Nom de domaine complet)** (nom d'hôte), **IP address (Adresse IP)**, **KEYID** (chaîne d'ID au format binaire hexadécimal), **FQDN (Nom de domaine complet de l'utilisateur)** (adresse e-mail). Si vous n’indiquez aucune valeur, la passerelle utilisera l'adresse IP locale comme valeur de **Local Identification (Identification locale)**.

Paramètres généraux d’une passerelle IKE	Description
Identification de l'homologue	Définit le type et l'identification de la passerelle homologue, qui sont utilisés avec la clé pré-partagée lors de l'établissement d'une SA IKEv1 de phase 1 et d'une SA IKEv2. Sélectionnez l'un des types suivants et saisissez une valeur : **FQDN (Nom de domaine complet)** (nom d'hôte), **IP address (Adresse IP)**, **KEYID** (chaîne d'ID au format binaire hexadécimal), **FQDN (Nom de domaine complet de l'utilisateur)** (adresse e-mail). Si vous n’indiquez aucune valeur, la passerelle utilisera l'adresse IP de l’homologue comme valeur de **Peer Identification (Identification de l'homologue)**.
Champs de l’option Certificat	
Certificat local	Si l'option **Certificate (Certificat)** est sélectionnée comme type d'**Authentication (Authentification)**, choisissez un certificat qui est déjà sur le pare-feu dans la liste déroulante. Sinon, vous pouvez **Import (Importer)** un certificat ou **Generate (Générer)** un nouveau certificat, comme suit : **Import (Importer)** : • **Certificate Name (Nom du certificat)** - Saisissez un nom pour le certificat que vous importez. • **Shared (Partagé)** - Sélectionnez cette option si le certificat sera partagé par plusieurs systèmes virtuels. • **Certificate File (Fichier de certificat)** - Cliquez sur **Browse (Parcourir)** pour accéder à l'emplacement où se trouve le fichier de certificat. Cliquez sur le fichier et sélectionnez **Open (Ouvrir)**. • **File Format (Format de fichier)** - Sélectionnez l'un des formats suivants : • **Base64 Encoded Certificate (PEM) (Certificat codé en Base64 (PEM))** - Contient le certificat mais pas la clé. Texte en clair. • **Encrypted Private Key and Certificate (PKCS12) (Clé privée et certificat cryptés (PKCS12))** - Contient le certificat et la clé. • **Private key resides on Hardware Security Module (La clé privée se trouve sur le module de sécurité matériel)** - Sélectionnez cette option si le pare-feu est un client d'un serveur de module de sécurité matériel où la clé réside.

Paramètres généraux d’une passerelle IKE	Description
	• **Import Private Key (Importer la clé privée)** - Cliquez sur cette option si une clé privée sera importée car celle-ci se trouve dans un autre fichier que le fichier de certificat. • **Block Private Key Export (Bloquer l’exportation de clé privée)** : Lorsque vous sélectionnez **Import Private Key (Importer la clé privée)**, cela empêche les administrateurs, y compris les super utilisateurs, d’exporter la clé privée. • **Key File (Fichier de clé)** - Cliquez sur Parcourir et accédez au fichier de clé à importer. Cette entrée est disponible si vous avez choisi PEM comme format de fichier. • **Passphrase (Phrase secrète)** et **Confirm Passphrase (Confirmer la phrase secrète)** - Saisissez-la pour accéder à la clé.
Certificat local (suite)	**Generate (Générer)** : • **Certificate Name (Nom du certificat)** - Saisissez un nom pour le certificat que vous créez. • **Common Name (Nom commun)** - Saisissez le nom commun, qui est l'adresse IP ou le nom de domaine complet à apparaître sur le certificat. • **Shared (Partagé)** - Sélectionnez cette option si le certificat sera partagé par plusieurs systèmes virtuels. • **Signed By (Signé par)** - Sélectionnez Autorité externe (demande de signature de certificat) ou saisissez l'adresse IP du pare-feu. Cette entrée doit être une autorité de certification. • **Certificate Authority (Autorité de certification)** - Sélectionnez cette option si le pare-feu est l'autorité de certification racine. • **Block Private Key Export (Bloquer l’exportation de clé privée)** : empêche les administrateurs, y compris les super utilisateurs, d’exporter la clé privée. • **OCSP Responder (Répondeur OCSP)** – Saisissez le répondeur OSCP qui suit si le certificat est valide ou révoqué. • **Algorithm (Algorithme)** - Sélectionnez RSA ou ECDSA pour générer la clé du certificat. • **Number of Bits (Nombre de bits)** - Sélectionnez 512, 1024, 2048 ou 3072 comme nombre de bits de la clé. • **Digest (Résumé)** - Sélectionnez md5, sha1, sha256, sha384, ou sha512 comme méthode pour rétablir la chaîne à partir du hachage. • **Expiration (days) (Expiration (jours))** - Saisissez le nombre de jours pendant lequel le certificat est valide. • **Certificate Attributes (Attributs du certificat)** : **Type** - Vous pouvez éventuellement sélectionner des types d'attributs de certificat supplémentaires dans la liste déroulante.

Paramètres généraux d’une passerelle IKE	Description
	• **Value (Valeur)** - Saisissez une valeur pour l'attribut.
Échange des certificats HTTP	Cliquez sur **HTTP Certificate Exchange (Échange des certificats HTTP)** et saisissez le **Certificate URL (URL du certificat)** afin d'utiliser la méthode Hachage et URL pour informer l'homologue de l'emplacement du certificat. L'URL du certificat est l'URL du serveur distant où vous stockez votre certificat. Si l'homologue indique qu'il prend également en charge la méthode Hachage et URL, les certificats sont alors échangés via le hachage SHA1 et l'échange d'URL. Lorsque l'homologue reçoit les données utiles du certificat IKE, il voit l'URL HTTP et récupère le certificat sur ce serveur. L’homologue utilise ensuite le hachage spécifié dans les données utiles du certificat pour vérifier les certificats téléchargés sur le serveur HTTP.
Identification locale	Identifie comment l'homologue local est identifié dans le certificat. Sélectionnez l'un des types suivants et saisissez une valeur : **Distinguished Name (Nom unique)** (objet), **FQDN (Nom de domaine complet)** (nom d'hôte), **IP address (Adresse IP)** ou **User FQDN (Nom de domaine complet de l'utilisateur)** (adresse e-mail).
Identification de l'homologue	Identifie comment l'homologue distant est identifié dans le certificat. Sélectionnez l'un des types suivants et saisissez une valeur : **Distinguished Name (Nom unique)** (objet), **FQDN (Nom de domaine complet)** (nom d'hôte), **IP address (Adresse IP)** ou **User FQDN (Nom de domaine complet de l'utilisateur)** (adresse e-mail).
Vérification de l'ID de l'homologue	Sélectionnez **Exact** ou **Wildcard (Caractère générique)**. Ce paramètre s'applique à l'identification de l'homologue qui est examinée pour valider le certificat. Par exemple, si l'Identification de l'homologue est un nom égal à domain.com, vous sélectionnez l'option **Exact**, et si le nom qui figure dans les données utiles du certificat IKE est mail.domain2.com, la négociation IKE échouera. Mais si vous avez sélectionnez l'option **Wildcard (Caractère générique)**, alors seuls les caractères qui figurent dans la chaîne Nom avant l'astérisque (*) doivent correspondre et tout caractère après l'astérisque peut différer.
Autoriser la non-correspondance de l'identification d'homologue et de l'identification des données utiles du certificat	Sélectionnez si vous souhaitez avoir la possibilité d’une SA IKE réussie même si l’identification de l’homologue ne correspond pas aux données utiles du certificat.

Paramètres généraux d’une passerelle IKE	Description
Profil du certificat	Sélectionnez ou créer un nouveau **Certificate Profile (Profil de certificat)** qui configure les options de certificat s'appliquant au certificat que la passerelle locale envoie à la passerelle homologue. Voir Périphérique > Gestion des certificats > Profil de certificat.
Activer la validation stricte de l'utilisation de la clé étendue de l'homologue	Sélectionnez si vous souhaitez contrôler strictement l’utilisation de la clé.

Passerelle IKE - Onglet Options avancées

- Réseau > Profils réseau > Passerelles IKE > Options avancées

Configurez les paramètres avancés de la passerelle IKE tels que le mode passif, le parcours NAT et les réglages IKEv1 comme la détection des homologues qui ne répondent pas.

Options avancées d’une passerelle IKE	Description
Activer le mode passif	Sélectionnez cette option pour que le pare-feu réponde uniquement aux connexions IKE sans jamais les initier.
Activer le parcours NAT	Sélectionnez cette option pour utiliser l'encapsulation UDP sur les protocoles IKE et UDP, en les autorisant à passer par des périphériques NAT intermédiaires. Activez le parcours NAT si la traduction d'adresses réseau (NAT) est configurée sur un périphérique entre les points de terminaison VPN IPSec.
Onglet'A0;IKEv1	
Mode d'échange	Sélectionnez **auto (automatique)**, **aggressive (agressif)** ou **main (principal)**. En mode **auto (automatique)** (le mode par défaut), le périphérique peut accepter des demandes de négociation en mode **main (principal)** et en mode **aggressive (agressif**. Toutefois, chaque fois que cela est possible, il initie une négociation et autorise des échanges en mode **main (principal)**. Vous devez configurer le périphérique homologue avec le même mode d'échange afin qu'il puisse accepter des demandes de négociation initiées à partir du premier périphérique.
Profil crypto IKE	Sélectionnez un profil existant, conservez le profil par défaut ou créez un nouveau profil. Les profils sélectionnés pour IKEv1et IKEv2 peuvent différer.

Options avancées d'une passerelle IKE	Description
	Pour plus d'informations sur les profils Crypto IKE, voir Réseau > Profils réseau > Crypto IKE.
Activer la fragmentation	Sélectionnez cette option pour autoriser la passerelle locale à recevoir des paquets IKE fragmentés. La taille maximale des paquets fragmentés est de 576 octets.
Détection des homologues arrêtés	Cliquez pour activer et entrer un intervalle (2 à 100 secondes) et un nombre de nouvelles tentatives (2 à 100). La détection des homologues arrêtés identifie les homologues IKE inactifs ou indisponibles et permet de restaurer des ressources perdues en cas d'indisponibilité d'un homologue.
Onglet IKEv2	
Profil cryptographique IKE	Sélectionnez un profil existant, conservez le profil par défaut ou créez un nouveau profil. Les profils sélectionnés pour IKEv1et IKEv2 peuvent différer. Pour plus d'informations sur Profil cryptographique IKE, voir Réseau > Profils réseau > Crypto IKE.
Validation stricte du cookie	Cochez cette case pour activer l'option **Strict Cookie Validation (Validation stricte du cookie)** sur la passerelle IKE. • Lorsque vous activez l'option **Strict Cookie Validation (Validation stricte du cookie)**, la validation du cookie IKEv2 est toujours mise en œuvre ; l'initiateur doit envoyer un message IKE_SA_INIT contenant un cookie. • Lorsque vous désactivez l'option **Strict Cookie Validation (Validation stricte du cookie)** (le paramètre par défaut), le système compare le nombre de SA à moitié ouvertes au **Cookie Activation Threshold (Seuil d'activation du cookie)**, qui est un paramètre des sessions VPN. Si le nombre de SA à moitié ouvertes dépasse le **Cookie Activation Threshold (Seuil d'activation du cookie)**, l'initiateur doit envoyer un message IKE_SA_INIT contenant un cookie.
Vérification de l'activité	L'option **Liveness Check (Vérification de l'activité)** IKEv2 est toujours activée ; tous les paquets IKEv2 permettent d'effectuer une vérification de l'activité. Cochez cette case pour que le système envoie des paquets d'information vides après que l'homologue a été inactif pendant un nombre de secondes spécifié. Plage entre 2 et 100. Par défaut : 5. Si nécessaire, le côté qui essaie d'envoyer des paquets IKEv2 effectue la vérification d'activité 10 fois maximum (tous les paquets IKEv2 sont pris en compte dans le paramètre de retransmission). S'il ne reçoit aucune réponse, l'expéditeur ferme et supprime les IKE_SA et CHILD_SA. L'expéditeur envoie un autre message IKE_SA_INIT.

Redémarrage ou actualisation d'une passerelle IKE

- Réseau > Tunnels IPSec

Sélectionnez **Network (Réseau)** > **IPSec Tunnels (Tunnels IPSec)** pour afficher l'état des tunnels. Dans la deuxième colonne Statut se trouve un lien vers les Informations IKE. Cliquez sur la passerelle que vous souhaitez redémarrer ou actualiser. La page Informations IKE s'ouvre. Cliquez sur l'une des entrées de la liste, puis sur :

- **Restart (Redémarrer)** – Redémarre la passerelle sélectionnée. Un redémarrage interrompt le trafic passant à travers le tunnel. Les comportements de redémarrage sont différents pour IKEv1 et IKEv2, comme suit :
  - **IKEv1** - Vous pouvez redémarrer (effacer) une SA de phase 1 ou de phase 2 de façon indépendante. Seule cette SA est affectée.
  - **IKEv2** - Entraîne l'effacement de toutes les SA enfants (tunnels IPSec) lorsque la SA IKEv2 est redémarrée.

    Si vous redémarrez la SA IKEv2, tous les tunnels IPSec sous-jacents sont également effacés.

    Si vous redémarrez le tunnel IPSec (SA enfant) associé à une SA IKEv2, le redémarrage n'affecte pas la SA IKEv2.
- **Refresh (Rafraichir)** – Affiche le statut actuel de la SA IKE.

Réseau > Profils réseau > Crypto IPSec

Sélectionnez **Network (Réseau)** > **Network Profiles (Profils réseau)** > **IPSec Crypto (Crypto IPSec)** pour définir des protocoles Crypto IPSec qui indiquent les protocoles et les algorithmes pour l'identification, l'authentification et le cryptage dans les tunnels VPN en fonction de la négociation SA IPSec (Phase 2).

Pour les tunnels VPN entre les passerelles GlobalProtect et les clients, voir Réseau > Profils réseau > Crypto IPSec GlobalProtect.

Paramètres d'un profil crypto IPSec	Description
Name (Nom)	Saisissez un **Name (Nom)** pour identifier le profil (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Protocole IPSec	Sélectionnez un protocole pour sécuriser les données qui traversent le tunnel VPN : • **ESP** - Le protocole ESP (Encapsulating Security Payload/Encapsulation sécurisée de la charge utile) crypte les données, authentifie la source et vérifie l'intégrité des données. • **AH** - Le protocole AH (Authentication Header/En-tête d'authentification) authentifie la source et vérifie l'intégrité des données.

Paramètres d'un profil crypto IPSec	Description
	*Utilisez le protocole **ESP**, car il assure la confidentialité de la connexion (chiffrement) et procure l'authentification.*
Chiffrement (protocole ESP uniquement)	Cliquez sur **Add (Ajouter)** et sélectionnez les algorithmes de chiffrement de votre choix. Pour une sécurité optimale, utilisez **Move Up (Déplacer vers le haut)** et **Move Down (Déplacer vers le bas)** pour modifier l'ordre (du haut vers le bas) comme suit : **aes-256-gcm**, **aes-256-cbc**, **aes-192-cbc**, **aes-128-gcm**, **aes-128-ccm** (le pare-feu VM-Series ne prend pas en charge cette option), **aes-128-cbc**, et **3des**. Vous pouvez également sélectionner **null (aucun)** (aucun chiffrement). *Utilisez une forme de chiffrement **AES**. (3DES est un algorithme faible et vulnérable.)*
Authentification	Cliquez sur **Add (Ajouter)** et sélectionnez les algorithmes d'authentification de votre choix. Pour une sécurité maximale, utilisez **Move Up (Monter)** ou **Move Down (Descendre)** afin d'obtenir l'ordre (de haut en bas) suivant : **sha512**, **sha384**, **sha256**, **sha1**, **md5**. Si le **protocole IPSec** est **ESP**, vous pouvez également sélectionner **none (aucune)** (aucune authentification). *Utilisez **sha256** ou une authentification plus forte, car **md5** et **sha1** ne sont pas sûrs. Utilisez **sha256** pour les sessions de courte durée et **sha384** ou plus pour le trafic qui exige l'authentification la plus sécuritaire, comme les transactions financières.*
Groupe DH	Sélectionnez le groupe DH Diffie-Hellman pour IKE (Internet Key Exchange/échange de clés Internet) : **group1 (groupe1)**, **group2 (groupe2)**, **group5 (groupe5)**, **group14 (groupe14)**, **group15 (groupe15)**, **group16 (groupe16)**, **group19 (groupe19)**, **group20 (groupe20)**, ou **group21 (groupe21)**. Pour une sécurité maximale, choisissez le groupe dont le nombre est le plus élevé. Si vous ne souhaitez pas renouveler la clé créée par le pare-feu lors de la négociation IKE de phase 1, sélectionnez **no-pfs (Mode PFS (Perfect Forward Secrecy) désactivé)** ; le pare-feu réutilise la clé actuelle pour les négociations SA IPSec.
Durée de vie	Sélectionnez les unités et saisissez la durée (le paramètre par défaut est une heure) pendant laquelle la clé négociée restera active.
Taille réelle	Sélectionnez des unités facultatives et saisissez la quantité de données qu'une clé peut utiliser pour le chiffrement.

Réseau > Profils réseau > Crypto IKE

Utilisez la page **IKE Crypto Profiles (Profils cryptographiques IKE)** pour définir des protocoles et des algorithmes pour l'identification, l'authentification et le cryptage (IKEv1 ou IKEv2, Phase 1).

Pour modifier l'ordre d'affichage d'un algorithme ou d'un groupe, sélectionnez un élément, puis cliquez sur **Move Up (Monter)** ou **Move Down (Descendre)**. L'ordre détermine le premier choix lors de la négociation des paramètres avec un homologue distant. Un essai du paramètre situé en tête de liste est réalisé en premier, puis en descendant dans la liste jusqu'à ce qu'un essai soit réussi.

Paramètres d'un profil cryptographique IKE	Description
Name (Nom)	Saisissez un Name (Nom) pour le profil.
Groupe DH	Indiquez la priorité des groupes Diffie-Hellman (DH). Cliquez sur **Ajouter** et sélectionnez les groupes : **group1**, **group2**, **group5**, **group14**,**group15**, **group16**,**group19**, **group20**ou **group21**. Pour une sécurité maximale, sélectionnez un élément, puis cliquez sur **Move Up (Monter)** ou **Move Down (Descendre)** pour déplacer les groupes dont les identifiants numériques sont les plus élevés en tête de liste. Par exemple, déplacez **group14 (groupe14)** au-dessus de **group2 (groupe2)**.
Authentification	Indiquez la priorité des algorithmes de hachage. Cliquez sur **Add (Ajouter)** et sélectionnez des algorithmes. Pour une sécurité maximale, sélectionnez un élément, puis cliquez sur **Move Up (Monter)** ou **Move Down (Descendre)** afin d'obtenir l'ordre (de haut en bas) suivant : • **SHA512** • **sha384** • **sha256** • **sha1** • **md5** • **aucun** *Si vous sélectionnez un algorithme AES-GCM pour le cryptage, vous devez sélectionner le paramètre d'authentification **aucun**. Le hachage est automatiquement sélectionné sur la base du groupe DH sélectionné. Le groupe DH 19 et en-dessous utilise **sha256** ; le groupe DH 20 utilise **sha384**.*
Chiffrement	Sélectionnez les options appropriées d'authentification ESP (Encapsulating Security Payload/Encapsulation sécurisée de la charge utile). Cliquez sur **Add (Ajouter)** et sélectionnez des algorithmes. Pour une sécurité maximale, sélectionnez un élément, puis cliquez sur **Move Up (Monter)** ou **Move Down (Descendre)** afin d'obtenir l'ordre (de haut en bas) suivant :

Paramètres d'un profil cryptographique IKE	Description
	• **aes-256-gcm** (nécessite IKEv2 ; le groupe DH doit être défini sur **group20**) • **aes-128-gcm** (nécessite IKEv2 et groupe DH défini sur **group19**) • **aes-256-cbc** • **aes-192-cbc** • **aes-128-cbc** • **3des** *Les algorithmes **aes-256-gcm** et **aes-128-gcm** ont une authentification intégrée ; par conséquent, dans ces cas, vous devez sélectionner pour **Authentication (authentification)** le paramètre **none (aucun)**.*
Durée de vie de la clé	Sélectionnez l'unité de temps et saisissez la durée pendant laquelle la clé IKE de phase 1 négociée sera effective. • IKEv2 - Avant que la durée de vie de la clé expire, la SA doit être renouvelée ou sinon, lors de l'expiration, la SA doit démarrer une nouvelle négociation de clé de phase 1. • IKEv1 - Le renouvellement de clé de phase 1 n'est pas effectué de manière active avant l'expiration. Le renouvellement de clé de phase 1 IKEv1 est déclenché uniquement lors de l'expiration de la SA IPSec IKEv1.
Authentification à facteurs multiples IKEv2	Spécifiez une valeur (intervalle : 0-50, valeur par défaut : 0) qui est multipliée par la durée de vie de la clé pour déterminer le nombre d'authentifications. Le nombre d'authentifications est le nombre de fois que la passerelle peut effectuer un renouvellement de clé SA IKE IKEv2 avant la réauthentification IKEv2. Une valeur de 0 désactive la fonction de réauthentification.

Réseau > Profils réseau > Surveillance

Un profil de surveillance permet de surveiller des tunnels IPSec et le périphérique du saut suivant dans le cadre de règles de transfert basé sur une politique (PBF). Dans les deux cas, le profil de surveillance permet de définir une action à appliquer lorsqu'une ressource (tunnel IPSec ou périphérique d'un saut suivant) devient indisponible. Les profils de surveillance sont facultatifs, mais peuvent être très utiles pour maintenir la connectivité entre des sites et s'assurer que les règles'A0;PBF sont également maintenues. Les paramètres suivants permettent de configurer un profil de surveillance.

Champ	Description
Name (Nom)	Saisissez un nom pour identifier le profil de surveillance (**31** caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Action (Action)	Indiquez une action à appliquer en cas d'indisponibilité du tunnel. Si le seuil du nombre de pulsations est perdu, le pare-feu applique l'action définie. • **wait-recover (en attente de récupération)** - Attendez que le tunnel récupère ; n'appliquez aucune action supplémentaire. Les paquets vont continuer à être envoyés conformément à la règle PBF. • **fail-over (basculement)** - Le trafic va basculer vers un chemin de secours, à condition qu'il soit disponible. Le pare-feu utilise la recherche de tables de routage afin de déterminer le routage à appliquer pendant toute la durée de cette session. Dans les deux cas, le pare-feu essaie de négocier de nouvelles clés IPSec afin d'accélérer la récupération.
Intervalle	Indiquez un délai entre les pulsations (intervalle compris entre 2 et 10, valeur par défaut : 3).
Seuil	Indiquez le nombre de pulsations devant être perdues avant que le pare-feu n'applique l'action définie (intervalle est compris entre 2 et 10 ; la valeur par défaut est 5).

Réseau > Profils réseau > Gestion de l'interface

Un profil de gestion de l'interface protège le pare-feu contre un accès non autorisé en définissant les services et les adresses IP qu'une interface du pare-feu autorise. Vous pouvez assigner un profil de gestion aux interfaces Ethernet de couche 3 (y compris les sous-interfaces) et aux interfaces logiques (groupe d'interfaces agrégées, interfaces VLAN, interfaces en boucle et interfaces de tunnel). Pour affecter un profile de gestion d'interface, voir Réseau > Interfaces.

N'affectez pas un profil de gestion de l'interface qui autorise Telnet, SSH, HTTP ou HTTPS à une interface qui autorise l'accès aux zones sécurisées de votre entreprise depuis l'Internet ou d'autres zones non sécurisées. Il s'agit entre autres de l'interface sur laquelle vous avez configuré un portail ou une passerelle GlobalProtect ; GlobalProtect n'a pas besoin d'un profil de gestion de l'interface pour autoriser l'accès au portail ou à la passerelle. Reportez-vous à la section Bonnes pratiques d'accès administratif *pour obtenir des précisions sur la manière de protéger l'accès à vos pare-feu et à Panorama.*

N'affectez pas un profil de gestion de l'interface qui autorise Telnet, SSH, HTTP ou HTTPS à une interface sur laquelle vous avez configuré un portail ou une passerelle GlobalProtect, car ce faisant vous exposeriez l'interface de gestion à l'Internet.

Champ	Description
Name (Nom)	Saisissez un nom pour le profil (**31** caractères maximum). Ce nom apparaît dans la liste des profils des Interface de gestion lors de la configuration d'interfaces. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Services de gestion administrative	• **Telnet** - Utilisez cette fonction pour accéder à la CLI du pare-feu. Telnet utilise du texte en clair, ce qui n'est pas aussi sécuritaire que le protocole SSH. *Activez le protocole SSH plutôt que le protocole de Telnet pour le trafic de gestion sur l'interface.* • **SSH** - Utilisez ce protocole pour obtenir un accès sécurisé à la CLI du pare-feu. • **HTTP** - Utilisez ce protocole pour accéder à l'interface Web du pare-feu. HTTP utilise du texte en clair, ce qui n'est pas aussi sécuritaire que le protocole HTTPS. *Activez le protocole **HTTPS** plutôt que le protocole HTTP pour le trafic de gestion sur l'interface.* • **HTTPS** - Utilisez ce protocole pour obtenir un accès sécurisé à l'interface Web du pare-feu.
Services du réseau	• **Ping** - Utilisez cette fonction pour tester la connectivité avec des services externes. Par exemple, vous pouvez envoyer un ping à l'interface pour vérifier qu'elle reçoit les mises à jour logicielles et de contenu de PAN-OS du serveur de mises à jour Palo Alto Networks. • **HTTP OCSP** - Utilisez ce protocole pour configurer le pare-feu en tant que répondeur du protocole OCSP (Online Certificate Status Protocol). Pour plus d'informations, voir Périphérique > Gestion des certificats > Répondeur OCSP. • **SNMP** - Utilisez ce protocole pour traiter les requêtes de statistiques du pare-feu à partir d'un gestionnaire SNMP. Pour plus de détails, voir Activation de la surveillance SNMP. • **Response Pages (Pages de réponse)** - Utilisez cette fonction pour activer des pages de réponse du portail captif. • **Authentication Portal (Portail d'authentification** - Les ports utilisés pour fournir les pages de réponses du portail d'authentification sont laissées ouverts sur les interfaces de couche 3 : le port 6080 pour NTLM, 6081 pour le portail d'authentification sans profil de serveur SSL/TLS et 6082 pour le portail d'authentification avec un profil de serveur SSL/TLS. Pour plus de détails, consultez Device > User Identification > Authentication Portal Settings (Périphérique > Identification utilisateur > Paramètres du portail d'authentification).

Champ	Description
	• **URL Admin Override (Contrôle prioritaire de l'URL par l'administrateur)** – Pour plus d'informations, voir Périphérique > Configuration > Content-ID. • **User-ID** – Utilisez pour activer la data redistribution (redistribution des données) des mappages d'utilisateurs sur les pare-feu. • **User-ID Syslog Listener-SSL (Écouteur Syslog User-ID-SSL)** - Est utilisé pour permettre à l'agent User-ID intégré à PAN-OS de recueillir les messages Syslog via SSL. Pour plus de détails, voir Configuration de l'accès aux serveurs surveillés. • **User-ID Syslog Listener-UDP (Écouteur Syslog User-ID-UDP)** - Est utilisé pour permettre à l'agent User-ID intégré à PAN-OS de recueillir les messages Syslog via UDP. Pour plus de détails, voir Configuration de l'accès aux serveurs surveillés.
Adresses IP autorisées	Saisissez la liste d'adresses IPv4 ou IPv6 à partir desquelles le pare-feu autorise l'accès.

Réseau > Profils réseau > Protection de zone

Un Profil de protection de zone appliqué à une zone offre une protection contre les attaques par saturation et les attaques de reconnaissance les plus fréquentes, les autres attaques basées sur les paquets et l'utilisation de protocoles non IP et les en-têtes avec 802.1Q (Ethertype 0x8909) qui ont des étiquettes de groupe de sécurité spécifiques (SGTs). Un profil de protection de zone est conçu pour fournir une protection renforcée de la zone d'entrée (la zone où le trafic entre sur le pare-feu) ; il ne permet pas de protéger un hôte spécifique ou du trafic vers une zone de destination particulière. Vous pouvez attacher un profil de protection de zone à une zone.

Appliquez un profil de protection de zone à chaque zone pour ajouter des couches de protection supplémentaire contre les attaques par saturation, les attaques de reconnaissance, les attaques basées sur les paquets et les attaques par utilisation de protocoles non IP. La protection de zone sur le pare-feu doit être une deuxième couche de protection après un périphérique DDoS dédié au périmètre Internet.

Pour améliorer les fonctions de protection de zone sur le pare-feu, configurez une politique de protection DoS (Politiques > Protection DoS) pour la mise en correspondance avec une zone, une interface, une adresse IP ou un utilisateur spécifique.

La protection de zone est uniquement mise en œuvre lorsque le paquet ne correspond à aucune session existante, car la protection de zone est basée sur de nouvelles connexions par seconde (cps) et non sur des paquets par seconde (pps). Dans le cas contraire, le paramètre de protection de zone est ignoré.

Que voulez-vous faire ?	Reportez-vous à la section :
Comment puis-je créer un profil de Protection de zone ?	Blocs de construction des profils de protection de zone Protection contre le flooding Protection contre la reconnaissance Protection contre les attaques basées sur les paquets Protection du protocole Protection SGT Ethernet l'inspection des en-têtes L3 et L4

Blocs de construction des profils de protection de zone

Pour créer un profil de Protection de zone, il faut **Ajouter** un profil et lui donner un nom.

Paramètres d'un profil de protection de zone	Configuré dans	Description
Nom	**Réseau** > **profils réseaux** > **protection de zones**	Saisissez un nom pour le profil (31 caractères maximum). Ce nom apparaît dans la liste des profils de Protection de Zone lors de la configuration des zones. Celui-ci est sensible à la casse et doit être unique. Vous pouvez uniquement utiliser des lettres, des nombres, des espaces et des caractères de soulignement.
Description		Saisissez une description facultative du profil de Protection de Zone.

Continuez la création d'un profil de Protection de zone en configurant toutes les combinaisons de paramètres qui correspondent aux types de protections dont votre zone a besoin :

- Protection contre la saturation
- Protection contre la reconnaissance
- Protection contre les attaques basées sur les paquets
- Protection du protocole
- Protection SGT Ethernet

Si vous disposez d'un environnement de systèmes virtuels multiples et que vous avez activé'A0;:

- *Les zones externes pour permettre la communication entre les systèmes virtuels*
- *Les passerelles partagées pour permettre aux systèmes virtuels de partager une interface commune et une adresse IP unique pour les communications externes*

Les mécanismes de protection de Zone et DoS suivants seront désactivés dans la zone externe :

- *Cookies SYN*
- *Fragmentation IP*
- *ICMPv6*

Pour activer la fragmentation IP et la protection ICMPv6 pour la passerelle partagée, vous devez créer un profil de Protection de zone distinct pour la passerelle partagée.

Pour protéger la passerelle partagée contre la saturation SYN, vous pouvez appliquer un profil de protection contre la saturation SYN avec l'abandon anticipé aléatoire ou les cookies SYN ; dans une zone externe, seule l'abandon anticipé aléatoire est disponible pour la protection contre la saturation SYN.

Protection contre la saturation

- Réseau > Profils réseau > Protection de zone > Protection contre la saturation

Configurez un profil qui fournit une protection contre la saturation relative aux paquets SYN, ICMP, ICMPv6, SCTP INIT et UDP, ainsi qu'une protection contre la saturation provenant d'autres types de paquets IP. Les taux correspondent à des connexions par seconde ; par exemple, un paquet SYN entrant qui ne correspond par à une session existante est considéré comme une nouvelle connexion.

Paramètres d'un profil de protection de zone – Protection contre la saturation	Configuré dans	Description
SYN	**Réseau** > **profils réseaux** > **protection**	Sélectionnez cette option pour activer la protection contre les saturations SYN.

Paramètres d’un profil de protection de zone – Protection contre la saturation	Configuré dans	Description
Action (Action)	**de zones** > **Protection contre la saturation**	Sélectionnez l'action à appliquer en réponse à une attaque par saturation SYN. • **Random Early Drop (RED)** - Supprime des paquets SYN afin d’atténuer une attaque par saturation : • Lorsque le flux dépasse le seuil du taux **Alert (Alerte)**, une alarme est générée. • Lorsque le flux dépasse le seuil du taux **Activate (Activation)**, le pare-feu supprime des paquets SYN individuels de façon aléatoire afin de restreindre le flux. • Lorsque le flux dépasse le seuil du taux **Maximum**, 100 % des paquets SYN entrants sont supprimés. • **SYN Cookies (Cookies SYN)** – Ils permettent au pare-feu d’agir comme un proxy, interceptent le SYN, génèrent un cookie au nom du serveur vers lequel le SYN a été dirigé et envoient un SYN-ACK avec le cookie à la source d’origine. C’est uniquement lorsque la source renvoie un ACK avec le cookie au pare-feu que ce dernier considère la source valide et renvoie le SYN au serveur. Cette Action est recommandée. Lorsque **SYN Cookies (cookies SYN)** sont activés, le pare-feu n’honore pas les options TCP envoyées par le serveur car il ne connaît pas ces valeurs au moment où il effectue le proxy SYN/ACK. Par conséquent, des valeurs telles que la taille de la fenêtre du serveur TCP et les valeurs MSS ne peuvent pas être négociées pendant la négociation TCP et le pare-feu utilisera ses propres valeurs par défaut. Dans le scénario où le MSS du chemin d’accès au serveur est plus petit que la

Paramètres d'un profil de protection de zone – Protection contre la saturation	Configuré dans	Description
		valeur MSS par défaut du pare-feu, le paquet devra être fragmenté. *Le trafic légitime traite les cookies SYN équitablement, mais consomme plus de ressources du pare-feu que RED. Si les syncookies consomment trop de ressources, basculez sur RED. Si vous ne disposez pas d'un périphérique de prévention DDoS devant le pare-feu (au périmètre Internet), utilisez toujours RED.*
Taux d'alarmes (connexions/s)	**Network (Réseau) > Network Profiles (Profils de réseau) > Zone Protection (Protection de zone) > Flood Protection (Protection contre la saturation)** (suite)	Saisissez le nombre de paquets SYN (ne correspondant pas à une session existante) que la zone reçoit par seconde et qui déclenche une alarme. Vous pouvez consulter ces alarmes sur le Tableau de bord et dans le journal des menaces (Surveillance > Capture de paquets). La plage est comprise entre 0 et 2 000 000 ; la valeur par défaut est 10 000. *Fixez le seuil de 15 à 20 % au-dessus du taux de CPS moyen de la zone afin de composer avec les fluctuations normales et à ajuster le seuil si vous recevez un trop grand nombre d'alarmes.*
Activer (connexions/s)		Saisissez le nombre de paquets SYN (ne correspondant pas à une session existante) que la zone reçoit par seconde et qui déclenche l'Action spécifiée dans ce Profil de protection de zone. Le pare-feu utilise un algorithme pour supprimer progressivement plus de paquets au fur et à mesure que le taux d'attaque augmente, jusqu'à ce que ce dernier atteigne le taux Maximal. Le pare-feu empêche la suppression des paquets SYN si le taux entrant descend sous le seuil d'Activation. Pour RED, la plage est comprise entre 1 et 2 000 000 et la valeur par défaut est 10 000. Pour les cookies SYN, la plage est comprise entre 0 et 2 000 000 et la valeur par défaut est 0.

Paramètres d’un profil de protection de zone – Protection contre la saturation	Configuré dans	Description
		Définissez le seuil juste au-dessus du taux de CPS de pointe de la zone pour éviter de limiter le trafic légitime et ajuster le seuil, au besoin.
Maximum (connexions/s)		Saisissez le nombre maximum de paquets SYN (ne correspondant pas à une session existante) que la zone reçoit par seconde, avant que les paquets dépassant le maximum ne soient supprimés. La valeur doit être comprise entre 1 et 2 000 000. La valeur par défaut est 40 000 pour RED ; la valeur par défaut est 1 000 000 pour les cookies SYN. Franchir le seuil bloque de nouvelles connexions jusqu'à ce que le taux de CPS repasse sous le seuil. *Définissez le seuil à une valeur allant de 80 à 90 % de la capacité du pare-feu, tenant compte des autres fonctions qui consomment les ressources du pare-feu.*
ICMP	**Network (Réseau)** > **Network Profiles (Profils de réseau)** > **Zone Protection (Protection de zone)** > **Flood Protection (Protection contre la saturation)** (suite)	Sélectionnez cette option pour activer la protection contre les saturations ICMP.
Taux d'alarmes (connexions/s)		Saisissez le nombre de demandes d’écho ICMP (pings ne correspondant pas à une session existante) que la zone reçoit par seconde et qui déclenche une alarme contre les attaques. Plage de 0 à 2 000 000 ; valeur par défaut : 10 000. *Fixez le seuil de 15 à 20 % au-dessus du taux de CPS moyen de la zone afin de composer avec les fluctuations normales et à ajuster le seuil si vous recevez un trop grand nombre d’alarmes.*
Activer (connexions/s)		Saisissez le nombre de paquets ICMP (ne correspondant pas à une session existante) que la zone reçoit par seconde, avant que les paquets ICMP subséquents ne soient supprimés. Le pare-feu utilise un algorithme pour supprimer progressivement plus de paquets au fur et à

Paramètres d'un profil de protection de zone – Protection contre la saturation	Configuré dans	Description
		mesure que le taux d'attaque augmente, jusqu'à ce que ce dernier atteigne le taux Maximal. Le pare-feu empêche la suppression des paquets ICMP si le taux entrant descend sous le seuil d'Activation. La plage est comprise entre 1 et 2 000 000 ; la valeur par défaut est 10 000. *Définissez le seuil juste au-dessus du taux de CPS de pointe de la zone pour éviter de limiter le trafic légitime et ajuster le seuil, au besoin.*
Maximum (connexions/s)		Saisissez le nombre maximum de paquets ICMP (ne correspondant pas à une session existante) que la zone reçoit par seconde, avant que les paquets dépassant le maximum ne soient supprimés. La plage est comprise entre 1 et 2 000 000 ; la valeur par défaut est 40 000. *Définissez le seuil à une valeur allant de 80 à 90 % de la capacité du pare-feu, tenant compte des autres fonctions qui consomment les ressources du pare-feu.*
SCTP INIT	**Network (Réseau) > Network Profiles (Profils de réseau) > Zone Protection (Protection de zone) > Flood Protection (Protection contre la saturation)** (suite)	Sélectionnez cette option pour activer la protection contre la saturation des paquets de Stream Control Transmission Protocol (protocole de contrôle de transmission des flux ; SCTP) qui contiennent un bloc d'initiation (INIT). Un bloc INIT ne peut être groupé avec d'autres blocs ; le paquet est alors appelé paquet SCTP INIT.
Taux d'alarmes (connexions/s)		Saisissez le nombre de paquets SCTP INIT (ne correspondant pas à une session existante) que la zone reçoit par seconde et qui déclenchent une alarme contre les attaques. La plage est comprise entre 0 et 2 000 000. La valeur par défaut selon le modèle de pare-feu est la suivante : • **PA-5280** : 10 000 • **PA-5260** : 7 000 • **PA-5250** : 5 000 • **PA-5220** : 3 000

Paramètres d'un profil de protection de zone – Protection contre la saturation	Configuré dans	Description
		• **VM-700** : 1 000 • **VM-500** : 500 • **VM-300** : 250 • **VM-100** : 200 • **VM-50** : 100
Activer (connexions/s)		Saisissez le nombre de paquets SCTP INIT (ne correspondant pas à une session existante) que la zone reçoit par seconde, avant que les paquets SCTP INIT subséquents ne soient supprimés. Le pare-feu utilise un algorithme pour supprimer progressivement plus de paquets au fur et à mesure que le taux d'attaque augmente, jusqu'à ce que ce dernier atteigne le taux Maximal. Le pare-feu empêche la suppression des paquets SCTP INIT si le taux entrant descend sous le seuil d'Activation. La valeur doit être comprise entre 1 et 2 000 000. La valeur par défaut selon le modèle de pare-feu est identique à la valeur par défaut du taux d'alarmes.
Maximum (connexions/s)	**Network (Réseau)** > **Network Profiles (Profils de réseau)** > **Zone Protection (Protection de zone)** > **Flood Protection (Protection contre la saturation)** (suite)	Saisissez le nombre maximum de paquets SCTP INIT (ne correspondant pas à une session existante) que la zone reçoit par seconde, avant que les paquets dépassant le maximum ne soient supprimés. La valeur doit être comprise entre 1 et 2 000 000. La valeur par défaut selon le modèle de pare-feu est la suivante : • **PA-5280** : 20 000 • **PA-5260** : 14 000 • **PA-5250** : 10 000 • **PA-5220** : 6 000 • **VM-700** : 2 000 • **VM-500** : 1 000 • **VM-300** : 500 • **VM-100** : 400 • **VM-50** : 200

Paramètres d’un profil de protection de zone – Protection contre la saturation	Configuré dans	Description
UDP	**Network (Réseau)** > **Network Profiles (Profils de réseau)** > **Zone Protection (Protection de zone)** > **Flood Protection (Protection contre la saturation)** (suite)	Sélectionnez cette option pour activer la protection contre les saturations UDP.
Taux d'alarmes (connexions/s)		Saisissez le nombre de paquets UDP (ne correspondant pas à une session existante) que la zone reçoit par seconde et qui déclenchent une alarme contre les attaques. Plage de 0 à 2 000 000 ; valeur par défaut : 10 000. *Fixez le seuil de 15 à 20 % au-dessus du taux de CPS moyen de la zone afin de composer avec les fluctuations normales et à ajuster le seuil si vous recevez un trop grand nombre d’alarmes.*
Activer (connexions/s)		Saisissez le nombre de paquets UDP (ne correspondant pas à une session existante) que la zone reçoit par seconde et qui déclenchent la suppression aléatoire de paquets UDP. Le pare-feu utilise un algorithme pour supprimer progressivement plus de paquets au fur et à mesure que le taux d’attaque augmente, jusqu’à ce que ce dernier atteigne le taux Maximal. Le pare-feu empêche la suppression des paquets UDP si le taux entrant descend sous le seuil d’Activation. La plage est comprise entre 1 et 2 000 000 ; la valeur par défaut est 10 000. *Définissez le seuil juste au-dessus du taux de CPS de pointe de la zone pour éviter de limiter le trafic légitime et ajuster le seuil, au besoin.*
Maximum (connexions/s)		Saisissez le nombre maximum de paquets UDP (ne correspondant pas à une session existante) que la zone reçoit par seconde, avant que les paquets dépassant le maximum ne soient supprimés. La plage est comprise entre 1 et 2 000 000 ; la valeur par défaut est 40 000.

Paramètres d'un profil de protection de zone – Protection contre la saturation	Configuré dans	Description
		Définissez le seuil à une valeur allant de 80 à 90 % de la capacité du pare-feu, tenant compte des autres fonctions qui consomment les ressources du pare-feu.
ICMPv6	**Network (Réseau)** > **Network Profiles (Profils de réseau)** > **Zone Protection (Protection de zone)** > **Flood Protection (Protection contre la saturation)** (suite)	Sélectionnez cette option pour activer la protection contre les saturations ICMPv6.
Taux d'alarmes (connexions/s)		Saisissez le nombre de demandes d'écho ICMPv6 (pings ne correspondant pas à une session existante) que la zone reçoit par seconde et qui déclenche une alarme contre les attaques. Plage de 0 à 2 000 000 ; valeur par défaut : 10 000. *Fixez le seuil de 15 à 20 % au-dessus du taux de CPS moyen de la zone afin de composer avec les fluctuations normales et à ajuster le seuil si vous recevez un trop grand nombre d'alarmes.*
Activer (connexions/s)		Saisissez le nombre de paquets ICMPv6 (ne correspondant pas à une session existante) que la zone reçoit par seconde, avant que les paquets ICMPv6 subséquents ne soient supprimés. Le pare-feu utilise un algorithme pour supprimer progressivement plus de paquets au fur et à mesure que le taux d'attaque augmente, jusqu'à ce que ce dernier atteigne le taux Maximal. Le pare-feu empêche la suppression des paquets ICMPv6 si le taux entrant descend sous le seuil d'Activation. La plage est comprise entre 1 et 2 000 000 ; la valeur par défaut est 10 000. *Définissez le seuil juste au-dessus du taux de CPS de pointe de la zone pour éviter de limiter le trafic légitime et ajuster le seuil, au besoin.*
Maximum (connexions/s)		Saisissez le nombre maximum de paquets ICMPv6 (ne correspondant pas à une session existante) que la zone reçoit par seconde, avant que les paquets dépassant le

Paramètres d'un profil de protection de zone – Protection contre la saturation	Configuré dans	Description
		maximum ne soient supprimés. La plage est comprise entre 1 et 2 000 000 ; la valeur par défaut est 40 000. *Définissez le seuil à une valeur allant de 80 à 90 % de la capacité du pare-feu, tenant compte des autres fonctions qui consomment les ressources du pare-feu.*
Autre IP	**Network (Réseau)** > **Network Profiles (Profils de réseau)** > **Zone Protection (Protection de zone)** > **Flood Protection (Protection contre la saturation)** (suite)	Sélectionnez pour activer la protection contre d'autres attaques par saturation d'IP (non TCP, non ICMP, non ICMPv6, non SCTP et non UDP).
Taux d'alarmes (connexions/s)		Saisissez le nombre d'autres paquets IP (paquets non TCP, non ICMP, non ICMPv6, non SCTP et non UDP) (ne correspondant pas à une session existante) reçu par la zone par seconde et qui déclenche une alarme contre les attaques. Plage de 0 à 2 000 000 ; valeur par défaut : 10 000. *Fixez le seuil de 15 à 20 % au-dessus du taux de CPS moyen de la zone afin de composer avec les fluctuations normales et à ajuster le seuil si vous recevez un trop grand nombre d'alarmes.*
Activer (connexions/s)		Saisissez le nombre d'autres paquets IP (paquets non TCP, non ICMP, non ICMPv6 et non UDP) (ne correspondant pas à une session existante) reçu par la zone par seconde et qui déclenche la suppression aléatoire de paquets d'autres IP. Le pare-feu utilise un algorithme pour supprimer progressivement plus de paquets au fur et à mesure que le taux d'attaque augmente, jusqu'à ce que ce dernier atteigne le taux Maximal. Le pare-feu empêche la suppression des paquets d'autres IP si le taux entrant descend sous le seuil d'Activation. La plage est comprise entre 1 et 2 000 000 ; la valeur par défaut est 10 000.

Paramètres d'un profil de protection de zone – Protection contre la saturation	Configuré dans	Description
		Définissez le seuil juste au-dessus du taux de CPS de pointe de la zone pour éviter de limiter le trafic légitime et ajuster le seuil, au besoin.
Maximum (connexions/s)		Saisissez le nombre maximum d'autres paquets IP (paquets non TCP, non ICMP, non ICMPv6 et non UDP) (ne correspondant pas à une session existante) reçu par la zone par seconde avant que les paquets qui dépassent le maximum ne soient supprimés. La plage est comprise entre 1 et 2 000 000 ; la valeur par défaut est 40 000. *Définissez le seuil à une valeur allant de 80 à 90 % de la capacité du pare-feu, tenant compte des autres fonctions qui consomment les ressources du pare-feu.*

Protection contre la reconnaissance

- Réseau > Profils réseau > Protection de zone > Protection contre la reconnaissance

Les paramètres suivants définissent la protection de reconnaissance :

Paramètres d'un profil de protection de zone – Protection de la reconnaissance	Configuré dans	Description
Balayage des ports TCP	**Réseau** > **profils réseaux** > **protection de zones** > **Protection contre la reconnaissance**	**Enable (Activer)** - Configure le profil de façon à activer la protection contre le balayage des ports TCP.
Balayage de port UDP		**Enable (Activer)** - Configure le profil de façon à activer la protection contre le balayage des ports UDP.
Balayage de l'hôte		**Enable (Activer)** - Configure le profil de façon à activer la protection contre le balayage de l'hôte.

Paramètres d'un profil de protection de zone – Protection de la reconnaissance	Configuré dans	Description
Action (Action)		Action que le système va appliquer en réponse à la tentative de reconnaissance correspondante : • **Allow (Autoriser)** - Autorise la reconnaissance par l'analyse de ports ou le balayage d'hôtes. • **Alert (Alerter)**- Génère une alerte pour chaque analyse de ports ou balayage d'hôtes correspondant au seuil et dans l'intervalle de temps spécifié (l'action par défaut). • **Block (Bloquer)** - Supprime tous les paquets suivants entre la source et la destination pendant l'intervalle de temps restant spécifié. • **Block IP (Blocage IP)** - Supprime tous les paquets suivants pour la **Duration (Durée)** indiquée, en secondes (plage comprise entre 1 et 3 600). **Track By (Suivre en fonction de)** détermine s'il faut bloquer le trafic source ou le trafic source et de destination. Par exemple, bloque les tentatives qui dépassent le seuil établi par intervalle provenant d'une seule source (plus stricte) ou les tentatives qui disposent d'une paire source et de destination (moins stricte). *Bloquez tous les balayages de reconnaissance, sauf vos balayages de vulnérabilité interne.*
Intervalle (s)		Intervalle de temps, en secondes, pour la détection du balayage des ports TCP ou UDP (plage comprise entre 2 et 65 535 ; par défaut 2). Intervalle de temps, en secondes, pour la détection du balayage de l'hôte (plage comprise entre 2 et 65 535 ; par défaut 10).
Seuil (événements)		Nombres d'événements relatifs à un balayage de ports ou à un balayage d'hôtes survenus au cours de l'intervalle de temps précisé qui ont déclenché l'Action (intervalle compris entre 2 et 65 535 ; valeur par défaut : 100). *Utilisez le seuil d'événement par défaut pour journaliser quelques paquets à des fins d'analyse avant de bloquer les tentatives de reconnaissance.*

Paramètres d’un profil de protection de zone – Protection de la reconnaissance	Configuré dans	Description
Exclusion de l'adresse source		Adresses IP que vous voulez exclure de la protection de reconnaissance. La liste prend en charge un maximum de 20 adresses IP ou objets d’adresse Netmask. • **Name (Nom)** : Saisissez un nom descriptif pour l’adresse à exclure. • **Address Type (type d’adresse)** : Sélectionnez IPv4 ou IPv6 dans la liste déroulante. • **Address (Adresse)** : Sélectionnez une adresse ou un objet d’adresse dans la liste déroulante ou saisissez-en un manuellement. *Excluez uniquement les adresses IP des groupes internes de confiance qui effectuent des tests de vulnérabilité.*

Protection contre les attaques basées sur les paquets

- Réseau > Profils réseau > Protection de zone > Protection contre les attaques basées sur les paquets

Vous pouvez configurer la protection contre les attaques basées sur les paquets pour supprimer les types de paquets suivants :

- Blocage de l’IP
- Blocage TCP
- Blocage ICMP
- Blocage IPv6
- Blocage ICMPv6

Blocage de l’IP

Pour indiquer au pare-feu ce qu’il doit faire de certains paquets IP qu’il reçoit dans la zone, précisez les paramètres suivants :

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
Adresse IP usurpée	**Réseau** > **profils réseaux** > **protection de zones** > **Protection contre les attaques basées sur les paquets** > **Blocage de l'IP**	Vérifiez que l'adresse IP source du paquet d'entrée est routable et que l'interface de routage est dans la même zone que l'interface d'entrée. Si l'une de ces conditions n'est pas vraie, supprimez le paquet. *Le pare-feu ne prend pas en compte les règles PBF (Policy Based Forwarding) lors de cette vérification ; il considère uniquement les itinéraires répertoriés dans la table de routage (RIB), c'est-à-dire les itinéraires répertoriés sous la sortie CLI pour* `show routing route (afficher l'itinéraire de routage)`. *Suru les zones internes uniquement, abandonnez les paquets d'adresses IP usurpées pour veiller à ce qu'à l'entrée l'adresse source correspond à la table de routage du pare-feu.*
Stricte vérification de l'adresse IP		Vérifiez que les deux conditions sont vraies : • L'adresse IP source n'est pas l'adresse IP de diffusion de sous-réseau de l'interface d'entrée. • L'adresse IP source est routable sur l'interface d'entrée exacte. Si l'une de ces conditions n'est pas vraie, supprimez le paquet. *Le pare-feu ne prend pas en compte les règles PBF (Policy Based Forwarding) lors de cette vérification ; il considère uniquement les itinéraires répertoriés dans la table de routage (RIB), c'est-à-dire les itinéraires répertoriés sous la sortie CLI pour* `show routing route (afficher l'itinéraire de routage)`. Si le pare-feu est en mode CC (Common Criteria/critères communs), vous pouvez activer la journalisation des paquets supprimés. Sur l'interface Web du pare-feu, sélectionnez **Device (Périphérique)** > **Log Settings (Paramètres du journal)**. À la section Gestion des journaux, sélectionnez **Selective Audit (Audit**

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
		sélectif), puis activez la **Packet Drop Logging (Consignation dans les journaux des paquets abandonnés)**.
Trafic fragmenté		Supprime des paquets IP fragmentés.
Abandon de l'option IP		Sélectionnez les paramètres dans ce groupe pour permettre au pare-feu de supprimer les paquets contenant ces Options IP.
Routage source strict		Supprime des paquets dans lesquels l'option IP de routage source strict est définie. Le Routage de source strict est une option qui permet à une source d'un datagramme de fournir les informations de routage par l'intermédiaire desquelles une passerelle ou un hôte doit envoyer le datagramme. *Abandonnez les paquets dotés d'un routage de source strict, car le routage de source permet aux adversaires de contourner les règles de politique de sécurité qui utilisent l'adresse IP de destination en tant que critère de correspondance.*
Routage source vague		Supprime des paquets dans lesquels l'option IP de routage source vague est définie. Le routage de source souple est une option qui permet à une source d'un datagramme de fournir des informations de routage, et une passerelle ou un hôte est autorisé à choisir n'importe quelle route composée d'un certain nombre de passerelles intermédiaires pour router le datagramme vers l'adresse suivante dans l'itinéraire. *Abandonnez les paquets dotés d'un routage de source vague, car le routage de source permet aux adversaires de contourner les règles de politique de sécurité qui utilisent l'adresse IP de destination en tant que critère de correspondance.*
Horodatage		Supprime des paquets dans lesquels l'option IP Horodatage est définie.

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
Itinéraire d'enregistrement		Supprime des paquets dans lesquels l'option IP de l'itinéraire d'enregistrement est définie. Lorsqu'un datagramme comporte cette option, chaque routeur qui route le datagramme ajoute sa propre adresse IP à l'en-tête, fournissant ainsi le chemin d'accès au destinataire.
Sécurité		Supprime des paquets, à condition que l'option de sécurité soit définie.
ID du flux		Supprime des paquets, à condition que l'option ID du flux soit définie.
inconnue		Supprime des paquets, à condition que la classe et le numéro soient inconnus.  *Supprime les paquets inconnus.*
Incorrect		Supprime des paquets, à condition que leurs combinaisons de classes, de nombres et de longueurs basés sur RFC 791, 1108, 1393 et 2113 soient incorrectes.  *Supprimer les paquets mal formés.*

Abandon de TCP

Pour indiquer au pare-feu ce qu'il doit faire de certains paquets TCP qu'il reçoit dans la zone, précisez les paramètres suivants.

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
Segments TCP superposés différents	**Réseau** > **profils réseaux** > **protection de zones** > **Protection contre les attaques basées sur les paquets** > **Abandon de TCP**	Les pirates peuvent établir des connexions avec des données qui se recoupent, mais différentes, pour essayer d'induire une interprétation erronée de la connexion. Les pirates peuvent utiliser l'usurpation d'adresse IP et la prédiction du numéro de séquence pour intercepter la connexion d'un utilisateur et y injecter leurs propres données. Utilisez ce paramètre pour signaler une non-concordance de superposition et abandonner le paquet lorsque les données du segment ne correspondent pas dans ces cas : • Le segment est dans un autre segment. • Le segment et une partie d'un autre segment sont superposés. • Le segment couvre un autre segment. Ce mécanisme de protection utilise des numéros de séquence pour déterminer l'emplacement des paquets dans le flux de données'A0;TCP. *Abandonne des paquets dont les segments TCP superposés sont différents.*
Établissement de liaison de segmentation		Empêche l'établissement d'une session TCP si la procédure d'établissement de session n'utilise pas l'établissement de la connexion en trois étapes bien connues. Une procédure d'établissement de liaison de segmentation en quatre ou cinq étapes ou une procédure d'ouverture de sessions simultanées sont des exemples de variations qui ne seraient pas autorisées. Le pare-feu Palo Alto Networks de dernière génération gère correctement les sessions et tous les processus de couche 7 pour l'établissement de liaison de segmentation et d'ouverture de sessions simultanées sans configurer l'**Établissement de liaison de segmentation**. Lorsque cette option est configurée pour un profil de protection de zone et que celui-ci est appliqué à une zone, les sessions TCP des interfaces de cette zone doivent être établies à l'aide de l'établissement de la connexion en trois étapes ; les variations ne sont pas autorisées. *Abandonne des paquets avec établissement de liaison de segmentation.*

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
Paquet TCP SYN avec les données		Empêche qu'une session TCP soit ouverte si le paquet TCP SYN contient des données lors d'une connexion en trois étapes. Cette option est activée par défaut.
Paquet TCP SYN/ ACK avec les données		Empêche qu'une session TCP soit ouverte si le paquet TCP SYN-ACK contient des données lors d'une connexion en trois étapes. Cette option est activée par défaut.
Rejeter le protocole TCP non-SYN		Détermine si un paquet doit être rejeté ou pas, à condition que le premier paquet pour la configuration d'une session TCP ne soit pas un paquet SYN : • **global** - Utilisez un paramètre système qui est attribué via l'interface CLI. • **yes (oui)** - Rejetez le protocole TCP non-SYN. • **no (non)** - Acceptez le protocole TCP non-SYN. *L'autorisation du trafic TCP non-SYN peut empêcher le fonctionnement normal des politiques de blocage des fichiers, lorsque la connexion client et/ou serveur n'est pas définie après l'occurrence du blocage.* *Si vous configurez l'inspection du contenu du tunnel sur une zone et activez l'option **Rematch Sessions (Revérifier les sessions)**, puis, pour cette zone uniquement, désactivez **Reject Non-SYN TCP (Rejeter le protocole TCP non-SYN)** pour que l'activation ou la modification d'une politique d'inspection du contenu du tunnel n'entraîne pas l'abandon des sessions de tunnel existantes de la part du tunnel.*
Chemin asymétrique		Détermine si des paquets contenant des ACK désynchronisés ou des numéros de séquence hors de la fenêtre doivent être supprimés ou ignorés : • **global** - Utilisez un paramètre système qui est attribué via **TCP Settings (Paramètres TCP)** ou l'interface CLI.

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
		• **drop (supprimer)** - Supprimez des paquets contenant un chemin asymétrique. • **bypass (ignorer)** - Ignorez l'analyse de paquets contenant un chemin asymétrique.
Extraire les options TCP		Détermine s'il faut supprimer l'option Horodatage TCP ou l'option TCP Fast Open des paquets TCP.
Horodatage TCP	**Réseau** > **profils réseaux** > **protection de zones** > **Protection contre les attaques basées sur les paquets** > **Abandon de TCP**	Détermine si l'en-tête du paquet contient un horodatage TCP et, le cas échéant, le supprime. *Supprime l'horodatage TCP des paquets qui le contiennent pour empêcher une attaque DoS par horodatage.*
TCP Fast Open		Supprime l'option TCP Fast Open (et la charge utile de données, le cas échéant) du paquet TCP SYN ou du paquet SYN-ACK lors d'une connexion TCP en trois étapes. Lorsque cette option est décochée (désactivée), l'option TCP Fast Open est autorisée, ce qui préserve la vitesse d'une configuration de connexion en incluant la livraison des données. Cela fonctionne indépendamment du paquet TCP SYN avec les données et du paquet TCP SYN-ACK avec les données. Cette option est désactivée par défaut.
Options MPTCP (Multipath TCP)		MPTCP est une extension de TCP qui permet à un client de maintenir une connexion en utilisant simultanément plusieurs chemins pour se connecter à l'hôte de destination. Par défaut, la prise en charge de MPTCP est désactivée, en fonction du paramètre MPTCP global. Vérifiez ou ajustez les paramètres MPTCP pour les zones de sécurité associées à ce profil :

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
		• **Non** – Active la prise en charge MPTCP (ne supprime pas l'option MPTCP). • **Oui** – Désactive la prise en charge MPTCP (supprime l'option MPTCP). Avec cette configuration, les connexions MPTCP sont converties en connexions TCP standards, car MPTCP est rétrocompatible avec TCP. • **(Par défaut) global** – Prise en charge MPTCP basée sur le paramètre MPTCP global. Par défaut, le paramètre MPTCP global est défini sur oui pour que l'option MPTCP soit désactivée (l'option MPTCP est supprimée du paquet). Vous pouvez vérifier ou ajuster le paramètre MPTCP global en utilisant la commande de la CLI suivante : `# set deviceconfig setting tcp strip-mptcp-option <yes|no>`

Drop de ICMP

Pour indiquer au pare-feu qu'il doit supprimer certains paquets ICMP qu'il reçoit dans la zone, sélectionnez les paramètres suivants pour les activer.

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
ID ping ICMP 0	**Réseau** > **profils réseaux** > **protection de zones** > **Protection contre les attaques**	Supprime des paquets, à condition que le paquet de pings ICMP affiche une valeur d'identifiant égale à 0.
Fragment ICMP		Supprime des paquets composés de fragments ICMP.

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
Paquet volumineux ICMP (>1024)	**basées sur les paquets** > **Blocage ICMP**	Supprime des paquets ICMP supérieurs à 1 024 octets.
Supprimer ICMP incorporé dans un message d'erreur		Supprime des paquets ICMP incorporés dans un message d'erreur.
Supprimer l'erreur d'expiration ICMP TTL		Arrête l'envoi de messages ICMP TTL arrivés à expiration.
Supprimer la fragmentation ICMP requise		Arrête l’envoi de messages de fragmentation ICMP requis en réponse à des paquets qui dépassent la valeur MTU de l’interface et dont l’octet DF (Do not Fragment/ne pas fragmenter) est défini. Ce paramètre va interférer avec le processus PMTUD exécuté par les hôtes situés derrière le pare-feu.

Abandon d'IPv6

Pour indiquer au pare-feu qu’il doit supprimer certains paquets IPv6 qu’il reçoit dans la zone, sélectionnez les paramètres suivants pour les activer.

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
En-tête de routage de type 0	**Réseau** > **profils réseaux** > **protection**	Supprime les paquets IPv6 contenant un en-tête de routage de type 0. Voir RFC 5095 pour des informations d’en-tête de routage de type 0.

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
Adresse compatible IPv4	**de zones** > **Protection contre les attaques basées sur les paquets** > **Blocage IPv6**	Supprime les paquets IPv6 définis comme adresse IPv6 compatible IPv4 selon le document RFC 4291.
Adresse source anycast		Supprime les paquets IPv6 qui contiennent une adresse source anycast.
En-tête de fragment inutile		Supprime les paquets IPv6 qui disposent de l'indicateur de dernier fragment (M=0) et d'un décalage de zéro.
MTU dans ICMP (paquet trop volumineux) inférieure à 1 280 octets		Supprime les paquets IPv6 qui contiennent un message Paquet ICMPv6 trop volumineux lorsque l'unité de transmission maximale (MTU) est inférieure à 1 280 octets.
Extension saut par saut		Supprime les paquets IPv6 qui contiennent l'en-tête d'extension Options saut par saut.
Extension de routage		Supprime les paquets IPv6 qui contiennent l'en-tête d'extension Routage, qui dirige les paquets vers un ou plusieurs nœuds intermédiaires en chemin vers sa destination.
Extension de destination		Supprime les paquets IPv6 qui contiennent l'en-tête d'extension Options de destination incluant des options destinées uniquement à la destination du paquet.
Options IPv6 non valides dans l’en-tête d’extension		Supprime les paquets IPv6 qui contiennent des options IPv6 non valides dans un en-tête d'extension.
Valeur de champ réservé non nulle		Supprime les paquets IPv6 qui contiennent un en-tête dont la valeur de champ réservé n'est pas définie sur zéro.

Abandon d'ICMPv6

Pour indiquer au pare-feu ce qu'il doit faire de certains paquets ICMPv6 qu'il reçoit dans la zone, sélectionnez les paramètres suivants pour les activer.

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
Erreur ICMPv6 - Destination inaccessible - Exiger la correspondance explicite de la règle de sécurité	**Réseau** > **profils réseaux** > **protection de zones** > **Protection contre les attaques basées sur les paquets** > **Blocage ICMPv6**	Exige une correspondance explicite de la politique de Sécurité pour les messages ICMPv6 de destination inaccessibles, même lorsque le message est associé à une session existante.
ICMPv6 de paquet trop volumineux - Exiger la correspondance explicite de la règle de sécurité		Exige une correspondance explicite de la politique de Sécurité pour les messages ICMPv6 de paquet trop volumineux, même lorsque le message est associé à une session existante.
ICMPv6 de délai dépassé - Exiger la correspondance explicite de la règle de sécurité		Exige une correspondance explicite de la politique de Sécurité pour les messages ICMPv6 de délai dépassé, même lorsque le message est associé à une session existante.
ICMPv6 de problème de paramètre - Exiger la correspondance explicite de la règle de sécurité		Exige une correspondance explicite de la politique de Sécurité pour les messages ICMPv6 de problème de paramètre, même lorsque le message est associé à une session existante.

Paramètres de profil de protection de zone – Protection contre les attaques basées sur les paquets	Configuré dans	Description
ICMPv6 de redirection - Exiger la correspondance explicite de la règle de sécurité		Exige une correspondance explicite de la politique de Sécurité pour les messages ICMPv6 de redirection, même lorsque le message est associé à une session existante.

Protection du protocole

- Réseau > Profils réseau > Protection de zone > Protection de protocole

Le pare-feu autorise normalement des protocoles non-IP entre les zones de couche 2 et entre les zones à câble virtuel. La protection du protocole vous permet de contrôler les protocoles non-IP qui sont autorisés (inclure) ou refusés (exclure) entre ou au sein des zones de sécurité sur un VLAN de couche 2 ou un câble virtuel. Parmi les exemples de protocoles non-IP se trouvent des systèmes AppleTalk, Banyan VINES, Novell, NetBEUI et Contrôle de supervision et Acquisition de données (SCADA), tels qu'un Evénement de Sous-poste Orienté objet Générique (GOOSE).

Après avoir configuré la protection du protocole dans un profil de Protection de zone, appliquez le profil à une zone de sécurité d'entrée sur un VLAN de niveau 2 ou un câble virtuel.

Activez la protection du protocole sur les zones Internet pour empêcher le trafic de couche 2 des protocoles que vous n'utilisez pas à accéder au réseau.

Paramètres d'un profil de protection de zone – Protection du protocole	Configuré dans	Description
Rule Type (Type de règle)	**Réseau** > **profils réseaux** > **protection de zones** > **Protection du protocole**	Spécifiez le type de liste que vous créez pour la protection du protocole : • **Inclure la liste** – Seuls les protocoles de la liste sont autorisés, en plus des trames étiquetées IPv4 (0x0800), IPv6 (0x86DD), ARP (0x0806) et VLAN (0x8100). Tous les autres protocoles sont implicitement refusés (bloqués).

Paramètres d'un profil de protection de zone – Protection du protocole	Configuré dans	Description
		• **Exclure la liste** – Seuls les protocoles de la liste sont refusés. Tous les autres protocoles sont implicitement autorisés. Vous ne pouvez pas exclure les trames étiquetées IPv4 (0x0800), IPv6 (0x86DD), ARP (0x0806) ou VLAN (0x8100).  *Utilisez la liste d'inclusion pour autoriser uniquement les protocoles de couche 2 que vous utilisez et pour refuser tous les autres protocoles. Cela réduit la surface d'attaque en refusant les protocoles que vous n'utilisez pas sur le réseau. Le pare-feu refuse uniquement les protocoles que vous ajoutez à la Liste d'exclusion et autorise tous les autres protocoles qui ne sont pas sur la liste. Si vous ne configurez pas de Protection de Protocole, tous les protocoles de couche 2 sont autorisés.*
Nom du protocole		Saisissez le nom du protocole qui correspond au code Ethertype que vous ajoutez à la liste. Le pare-feu ne vérifie pas que le nom du protocole correspond au code Ethertype, mais le code Ethertype détermine le filtre de protocole.
Activer		Vous pouvez **Activer** le code Ethertype sur la liste. Si vous souhaitez désactiver un protocole à des fins de test, mais pas le supprimer, désactivez-le plutôt.
EtherType (format hexadécimal)		Saisissez un code Ethertype (protocole) précédé de 0x pour indiquer l'hexadécimal (la plage est de 0x0000 à 0xFFFF). Une liste peut avoir un maximum de 64 Ethertypes. Certaines sources de codes Ethertype sont : • IEEE hexadécimal Ethertype • standards.ieee.org/develop/regauth/ethertype/eth.txt • http://www.cavebear.com/archive/cavebear/Ethernet/type.html

Protection SGT Ethernet

- Réseau > Profils réseau > Protection de zone > Protection SGT Ethernet

Pour un pare-feu sur un réseau Cisco TrustSec, créez un Profil de protection de zone avec une liste d'étiquettes de groupe de sécurité (SGT) de couche 2 que vous voulez exclure. Appliquez le profil de protection de zone à une Couche 2, câble virtuel ou interface TAP. Si un paquet entrant avec un en-tête

802.1Q (Ethertype 0x8909) a une SGT qui correspond à une SGT de votre liste, le pare-feu supprime la paquet.

Paramètres d'un profil de protection de zone	Configuré dans	Description
Liste d'exclusion SGT de couche 2.	**Réseau** > **profils réseaux** > **protection de zones** > **Protection SGT Ethernet**	Saisissez un nom pour la liste d'étiquettes du groupe de sécurité (SGT).
Étiquette		Saisissez les SGT de Couche 2 dans les en-têtes des paquets que vous voulez exclure (supprimer) lorsque la SGT correspond à la liste dans le profil de protection de zone appliqué à une zone (plage de 0 à 65 535).
Activer		**Enable (Activez)** (par défaut) cette liste d'exclusion pour la protection SGT Ethernet. Désélectionnez l'option **Enable (Activer)** pour désactiver la liste d'exclusion.

l'inspection des en-têtes L3 et L4

- Profils réseau > réseau > protection de zone > inspection des en-têtes L3 et L4

Lorsque l'inspection des en-têtes L3 et L4 est activée globalement, le pare-feu est capable de détecter et de prévenir les vulnérabilités dans les protocoles pris en charge (IP/IPv6, ICMP/ICMPv6, TCP et UDP) et d'enregistrer et/ou de bloquer les paquets qui correspondent aux règles personnalisées spécifiées par l'utilisateur. En outre, vous devez Enable Net Inspection (activer Net Inspection) (**Network (Réseau)** > **Zones**) pour chaque zone de sécurité à l'aide de règles personnalisées d'inspection d'en-tête.

Vous pouvez ajouter, supprimer et cloner des règles existantes, ainsi que définir la priorité et l'état opérationnel des règles personnalisées telles qu'évaluées par le profil Protection de zone.

Après avoir configuré l'inspection des en-têtes L3 et L4 dans un profil de protection de zone, appliquez le profil à une zone de sécurité d'entrée.

Palo Alto Networks recommande de configurer et d'activer L3 & L4 Header Inspection uniquement dans les zones de sécurité susceptibles de rencontrer et de traiter des paquets correspondant aux règles personnalisées, car il existe un nombre limité de zones pouvant fonctionner simultanément lorsque cette fonctionnalité est activée.

Paramètres du profil de protection de zone : inspection des en-têtes L3 et L4	Configuré dans	Description
Onglet Configuration		
Général		
rule	**Réseau** > **profils réseaux** > **protection de zones** > **l'inspection des en-têtes L3 et L4**	Saisissez un nom pour identifier la règle personnalisée (31 caractères maximum).
ID de menace		Spécifiez un numéro d'ID de menace pour la configuration de la règle personnalisée (la plage de signatures de vulnérabilité est 41000-45000 et 6800001-6900000).
Commentaire		Entrez un commentaire facultatif pour décrire la règle personnalisée.
Capture de paquets		Active une capture de paquets lors de la détection d'une vulnérabilité correspondant à la règle personnalisée. Dans la liste déroulante, sélectionnez **single-packet (paquet unique)** ou **extended-capture (capture étendue)**, ou **disable (désactiver)** si vous ne souhaitez pas que le pare-feu enregistre les captures de paquets. Vous pouvez également **send icmp unreachable packets if packet is dropped (envoyer des paquets icmp inaccessibles si le paquet est abandonné)** pour informer le client qu'une session n'est pas autorisée.
IP d'exemption		Entrez la ou les adresses IP auxquelles vous ne souhaitez pas que la règle personnalisée s'applique.
Propriétés		
Gravité des journaux	**Réseau** > **profils réseaux** > **protection de zones** > **l'inspection des en-têtes L3 et L4**	Spécifiez le niveau de gravité de la journalisation enregistré lorsque le pare-feu détecte une vulnérabilité correspondant à la règle personnalisée.
Intervalle de journalisation		Spécifiez la fréquence de journalisation maximale (en secondes) d'un événement correspondant.
Action		Spécifiez l'action de stratégie à exécuter lorsqu'une vulnérabilité correspondant à la règle personnalisée est détectée dans l'en-tête. Les options disponibles sont les suivantes'A0;:

Paramètres du profil de protection de zone : inspection des en-têtes L3 et L4	Configuré dans	Description
		• allow (autoriser) • alert (alerter) • blocage • réinitialiser le client • réinitialiser le serveur • réinitialiser les deux
Référence		
CVE	**Réseau** > **profils réseaux** > **protection de zones** > **l'inspection des en-têtes L3 et L4**	Identificateur de vulnérabilité de sécurité connu publiquement associé à la menace. L'identifiant des Failles et vulnérabilités communes (CVE) est l'identifiant le plus utile pour trouver des informations sur une vulnérabilité unique, car les ID spécifiques aux fournisseurs incluent généralement de multiples vulnérabilités.
Bugtraq		Identificateur bugtraq (similaire à CVE) associé à la vulnérabilité. Peut être utilisé comme référence externe pour des informations générales et des détails d'analyse supplémentaires.
Constructeur		L'identifiant spécifique au fournisseur d'une vulnérabilité.
Référence		Liens vers une analyse supplémentaire ou des informations contextuelles.
Onglet Signature		
Commentaire	**Réseau** > **profils réseaux** > **protection de zones** > **l'inspection des en-têtes L3 et L4**	Entrez un commentaire facultatif pour décrire les détails de la signature de la règle personnalisée.
Ou condition		Spécifiez une **Or condition (condition Ou)** pour la signature personnalisée.
Condition And		Ajoutez une **And condition (condition ET)** pour la signature personnalisée en configurant les éléments suivants : • **And condition (Condition Et)** spécifiez une valeur de condition Et pour la signature personnalisée. • **Operator (opérateur)** définit le type de condition qui doit être vrai pour que la signature personnalisée

Paramètres du profil de protection de zone : inspection des en-têtes L3 et L4	Configuré dans	Description
		corresponde au trafic. Choisissez parmi les opérateurs Supérieur à, Inférieur à, Égal à, Plage ou Événement. • **Context (Contexte)** - Choisissez parmi les options de contexte disponibles. Selon votre sélection, vous pouvez avoir d'autres champs liés au contexte et/ou à l'opérateur qui doivent être spécifiés pour activer la condition. *Les conditions d'ajout sont ajoutées en tant qu'entrée de deuxième niveau sous **Or Condition (Condition Ou)**.*

Réseau > Profils réseau > QoS

Vous devez **Ajouter** un profil QoS pour définir les limites de bande passante et les priorités d'un maximum de huit classes de services. Il est possible de définir des limites de bande passante garanties et maximales pour chacune des classes ou pour l'ensemble des classes. Ces priorités déterminent la méthode de traitement du trafic en cas de contention.

Pour permettre au pare-feu de fournir une QoS, effectuez également les actions suivantes :

- Définissez le trafic qui doit recevoir le traitement QoS (sélectionnez Politiques > QoS pour ajouter ou modifier une politique QoS).
- Activez la QoS sur une interface (sélectionnez Réseau > QoS).

Voir Qualité de service pour avoir accès à un flux de travail QoS complet, des concepts et des cas pratiques.

Paramètres d'un profil QoS	
Nom du profil	Saisissez un nom pour identifier le profil (**31** caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Trafic sortant max.	Entrez le débit maximum (en Mbits/s) pour le trafic sortant du pare-feu via cette interface. La valeur par défaut est 0, laquelle définit la limite autorisée sur le pare-feu (60 000 Mbits/s sur PAN-OS 7.1.16 et les versions ultérieures ; 16 000 sur PAN-OS 7.1.15 et les versions antérieures).

Paramètres d’un profil QoS	
	La valeur de **Egress Max (Sortie max.)** d'un profil de QoS ne doit pas dépasser la valeur de **Egress Max (Sortie max.)** définie pour l'interface physique sur laquelle la QoS est activée. Voir Réseau > QoS. *Bien qu'il ne s'agisse pas d'un champ obligatoire, il est recommandé de toujours définir la valeur de **Egress Max** (Sortie max.) d'un profil QoS.*
Trafic sortant garanti	Saisissez la bande passante garantie pour ce profil (Mbits/s). Dans l'éventualité où le trafic dépasse la bande passante de sortie garantie, le pare-feu achemine le trafic dans la mesure du possible. Vous pouvez configurer les valeurs **Egress Guaranteed (Sortie garantie)** et **Egress Max (Sortie maximale)** en Mbits/s ou en pourcentages. Les considérations suivantes doivent être prises en compte lors de la configuration de ces valeurs en pourcentages : • La **Egress Guaranteed (sortie garantie)** en (%) par classe est calculée à l’aide de la valeur **Egress Max (Sortie maximale)** et non de la valeur **Egress Guaranteed (Sortie garantie)**. • **Egress Guaranteed (sortie garantie)** de profil égale à la somme de**Egress Guaranteed (sortie garantie)** en (%) par catégorie multipliée par **Egress Max (Sortie max.)**. Par exemple : **Egress Max (sortie max.)** est configuré sur 100 Mbps. Le pourcentage garanti configuré pour la classe 1 est de 30%, pour la classe 2 il est de 20%, pour la classe 3 il est de 5% et pour la classe 4 il est de 1%. Cette configuration se traduit par un pourcentage total garanti de 56%. Dans ce cas, le profil **Egress Guaranteed (Sortie garantie)** est de 56 Mbit/s (56 % x **Egress Max (Sortie Max)**). Cela signifie également que la **Egress Guaranteed (sortie garantie)** de classe 1 est de 30 Mbps, la **Egress Guaranteed (sortie garantie)** de classe 2 est de 20 Mbps, et ainsi de suite.
Classes	**Ajouter** et indiquer la méthode de traitement des classes de QoS individuelles. Vous pouvez sélectionner une ou plusieurs classes à configurer : • **Class**: si vous ne configurez pas une classe, vous pouvez toujours l’inclure dans une stratégie QoS. Dans ce cas, le trafic est soumis à des limites de QoS globales. Le trafic qui ne correspond pas à une politique de QoS sera assigné à la classe 4.

Paramètres d’un profil QoS	
	• **Priorité (Priority**) : cliquez sur une priorité et sélectionnez-la pour l’affecter à une classe : • **temps** • **réel** • **élevé** • **moyen** • **faible** En cas de conflit, le trafic auquel une priorité inférieure est attribuée est supprimé. La priorité en temps réel utilise sa propre file d’attente distincte. • **Egress Max (**Cliquez et entrez le débit maximal (en Mbps) pour cette classe. La valeur par défaut est 0, laquelle définit la limite autorisée sur le pare-feu (60 000 Mbits/s sur PAN-OS 7.1.16 et les versions ultérieures ; 16 000 sur PAN-OS 7.1.15 et les versions antérieures). Le **maximum de sortie** pour une classe QoS doit être inférieur ou égal au maximum de sortie pour le profil QoS. *Bien qu’il ne s’agisse pas d’un champ obligatoire, nous vous recommandons de toujours définir la **valeur Egress Max** pour un profil QoS.* • **Sortie garantie**: cliquez et entrez la bande passante garantie (Mbps) pour cette classe. La bande passante garantie attribuée à une classe n'est pas réservée à cette classe ; la bande passante qui n'est pas utilisée demeure disponible pour l'acheminement de tout trafic. Toutefois, lorsque le trafic dépasse la bande passante de sortie garantie attribuée à une classe de trafic, le pare-feu achemine le trafic dans la mesure du possible.

Réseau > Profils réseau > Profil LLDP

Un profil LLDP (Link Layer Discovery Protocol/protocole de découverte de couche liaison) vous permet de configurer le mode LLDP du pare-feu, d'activer les notifications SNMP et Syslog, ainsi que de configurer les éléments TLV (Type-Longueur-Valeur) que vous souhaitez transmettre aux homologues LLDP. Une fois le profil LLDP configuré, affectez-le à une ou plusieurs interfaces.

En savoir plus sur LLDP, y compris la façon de configurer et de surveiller LLDP.

Paramètres d’un profil LLDP	Description
Name (Nom)	Donnez un nom au profil LLDP.

Paramètres d’un profil LLDP	Description
Mode	Sélectionnez le mode dans lequel LLDP fonctionnera : **transmit-receive (transmission/réception)**, **transmit-only (transmission uniquement)** ou **receive-only (réception uniquement)**.
Notifications SNMP et Syslog	Active les notifications de piège SNMP et Syslog, qui se produiront au **Notification Interval (Intervalle de notification)** global. Si cette option est activée, le pare-feu envoie des événements de piège SNMP et Syslog, tel que configuré dans **Device (Périphérique)** > **Log Settings (Paramètres des journaux)** > **System (Système)** > **SNMP Trap Profile (Profil de déroutement SNMP)** et **Syslog Profile (Profil Syslog)**.
Description du port	Permet l'envoi de l'objet ifAlias du pare-feu dans l'élément TLV Description du port.
Nom du système	Permet l'envoi de l'objet sysName du pare-feu dans l'élément TLV Nom du système.
Description du système	Permet l'envoi de l'objet sysDescr du pare-feu dans l'élément TLV Description du système.
Fonctionnalités du système	Permet l'envoi du mode de déploiement (C3, C2 ou câble virtuel) de l'interface, via le mappage suivant, dans l'élément TLV Fonctionnalités du système. • Si celui-ci est C3, le pare-feu publie la fonctionnalité de routeur (bit 6) et l'autre bit (bit 1). • Si celui-ci est C2, le pare-feu publie la fonctionnalité de pont MAC (bit 3) et l'autre bit (bit 1). • Si celui-ci est C3, le pare-feu publie la fonctionnalité de répéteur (bit 2) et l'autre bit (bit 1). La MIB SNMP combinera les fonctionnalités configurées sur les interfaces en une entrée unique.
Adresse de gestion	Permet l'envoi de la **Management Address (Adresse de gestion)** dans l'élément TLV Adresse de gestion. Vous pouvez saisir jusqu'à quatre adresses de gestion, qui sont envoyées dans l'ordre spécifié. Pour modifier l'ordre, cliquez sur **Move Up (Monter)** ou **Move Down (Descendre)**.
Name (Nom)	Donnez un nom à l'adresse de gestion.
Interface	Sélectionnez une interface dont l'adresse IP sera l'adresse de gestion. Si vous sélectionnez **None (Aucune)**, vous pouvez saisir une adresse IP dans le champ en regard de la sélection IPv4 ou IPv6.

Paramètres d’un profil LLDP	Description
Choix IP	Sélectionnez **IPv4** ou **IPv6**, puis, dans le champ adjacent, choisissez ou saisissez l'adresse IP à transmettre comme adresse de gestion. Au moins une adresse est requise si l'élément TLV **Management Address (Adresse de gestion)** est activé. Si aucune adresse IP de gestion n'est configurée, le système utilise l'adresse MAC de l'interface de transmission comme adresse de gestion transmise.

Réseau > Profils réseau > Profil BFD

La BFD (Bidirectional Forwarding Detection/détection de transmission bidirectionnelle) contribue à une détection extrêmement rapide d'un échec de la liaison, ce qui accélère le basculement vers un itinéraire différent.

Que voulez-vous faire ?	Reportez-vous à la section :
Qu'est ce que la BFD?	Présentation de la BFD
Quels champs sont disponibles pour la création d'un profil BFD?	Blocs de construction d’un profil BFD
Affichage du statut BFD pour un routeur virtuel.	Affichage du récapitulatif et des détails BFD
Vous souhaitez en savoir plus ?	En savoir plus sur la BFD et la configurer. Configurez la BFD pour : Itinéraires statiques BGP OSPF OSPFv3 RIP

Présentation du BFD

Le BFD est un protocole qui reconnaît un échec d'un chemin bidirectionnel entre deux moteurs d'acheminement, comme des interfaces, des liaisons de données ou les moteurs d'acheminement en tant que tel. Dans l'implémentation PAN-OS, l'un des moteurs d'acheminement est une interface sur le pare-feu et l'autre est un homologue BFD adjacent qui a été configuré. La détection de l'échec BFD entre deux moteurs est extrêmement rapide, ce qui assure un basculement plus rapide que ce que l'on pourrait atteindre en surveillant les liaisons ou en effectuant fréquemment des vérifications de l'état santé du routage dynamique, comme des pulsations ou des paquets Hello.

Une fois que le BFD a détecté un échec, elle avise le protocole de routage d'utiliser un autre chemin vers l'homologue. Si le BFD est configuré pour l'utilisation d'un itinéraire statique, le pare-feu supprime les itinéraires attribués dans les tables RIB et FIB.

Le BFD est prise en charge sur les types d'interface suivants : ethernet physique, ethernet agrégé, VLAN, de tunnel (VPN de site à site et LSVPN) ainsi que sur les sous-interfaces des interfaces de couche 3. Pour chaque itinéraire statique ou protocole de routage dynamique, vous pouvez activer ou désactiver le BFD, sélectionner le profil BFD par défaut ou configurer un profil BFD.

Blocs de construction d’un profil BFD

- Réseau > Profils réseau > Profil BFD

Vous pouvez activer la BFD pour un itinéraire statique ou un protocole de routage dynamique en appliquant le profil BFD par défaut ou un profil BFD que vous avez créé. Le profil par défaut se sert des paramètres BFD par défaut et ne peut être modifié. Vous pouvez cliquer sur **Ajouter** pour ajouter un nouveau profil BFD et précisez les informations suivantes.

Paramètres d'un profil BFD	Description
Nom	Nom du profil BFD (31 caractères maximum). Celui-ci est sensible aux majuscules et minuscules et doit être unique sur le pare-feu. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement.
Mode	Mode sous lequel la BFD fonctionne : • **Actif** - La BFD initie l'envoi de paquets de contrôle (par défaut). Au moins l'un des homologues BFD doit être actif ; ils peuvent être actifs tous les deux. • **Passif** - La BFD attend que l'homologue envoie des paquets de contrôles et répond comme il se doit.
Intervalle Tx minimum souhaité (ms)	Intervalle minimum (en millisecondes) auquel vous souhaitez que le protocole BFD envoie des paquets de contrôles BFD. La valeur minimale des séries PA-7000, PA-5450, PA-5430, PA-5420, PA-5410 et PA-3400 est de 50; la valeur minimale des séries PA-3200 est de 100; la valeur minimale des séries PA-400 est de 150; la valeur minimale des séries VM est de 200 (la valeur maximale est de 10 000; la valeur par défaut est de 1000). *Si vous disposez de plusieurs protocoles qui utilisent des profils BFD différents sur la même interface, configurez les profils BFD avec le même **Desired Minimum Tx Interval (Intervalle Tx minimum souhaité)**.*
Intervalle Rx minimum souhaité (ms)	Intervalle minimum (en millisecondes) auquel la BFD peut recevoir les paquets de contrôles BFD. La valeur minimale des séries PA-7000, PA-5450, PA-5430, PA-5420, PA-5410 et PA-3400 est de 50; la valeur minimale des séries PA-3200 est de 100; la valeur minimale des séries PA-400 est de 150; la valeur minimale des séries VM est de 200 (la valeur maximale est de 10 000; la valeur par défaut est de 1000).

Paramètres d'un profil BFD	Description
Multiplicateur de délai de détection	Le système local calcule le délai de détection en tant que **Multiplicateur de délai de détection** reçu du système distant multiplié par l'intervalle de transmission du système distant convenu (la valeur la plus élevée entre le **Intervalle de réception minimum requis** et le dernier **Intervalle de transmission minimum souhaité)** reçu. Si la BFD ne reçoit pas de paquet de contrôles BFD de son homologue avant l'expiration du délai de détection, c'est qu'un échec a eu lieu (intervalle compris entre 2 et 50 ; valeur par défaut : 3).
Temps d'attente (ms)	Délai (en millisecondes) entre l'apparition d'une liaison et la transmission des paquets de contrôles BFD par le pare-feu. Le **Temps d'attente** ne s'applique qu'au mode Actif de la BFD. Si le pare-feu reçoit des paquets de contrôles BFD pendant le **Temps d'attente**, il les ignore (intervalle compris entre 0 et 120 000 ; valeur par défaut : 0). Le paramètre défini par défaut de 0 signifie qu'aucun **Temps d'attente** n'est utilisé ; le pare-feu envoie et reçoit les paquets de contrôles BFD immédiatement après l'établissement de la liaison.
Activer les sauts multiples	Active la BFD à sauts multiples. Ne s'applique que dans le cas d'une implémentation BGP.
TTL Rx minimum	Valeur TTL minimale (nombre de sauts) la BFD acceptera (recevra) lorsqu'elle prend en charge la BFD à sauts multiples. Ne s'applique que dans le cas d'une implémentation BGP (intervalle compris entre 1 et 254 ; aucune valeur par défaut).

Affichage du récapitulatif et des détails BFD

- Réseau > Routeurs virtuels

Le tableau suivant décrit les informations récapitulatives de BFD.

Voir des informations sur la BFD	
Voir le récapitulatif de la BFD.	Sélectionnez **Network (Réseau)** > **Virtual Routers (Routeurs virtuels)** et, dans la rangée du routeur virtuel qui vous intéresse, cliquez sur **More Runtime Stats (Statistiques d'exécution supplémentaires)**. Sélectionnez l'onglet **BFD Summary Information (Informations récapitulatives de BFP)** sur la BFD.
Voir des informations sur la BFD	Sélectionnez **details (détails)** dans la rangée de l'interface qui vous intéresse pour afficher les Détails de la BFD.

Réseau > Profils réseau > Profil d’interface SD-WAN

Créez un profil d’interface SD-WAN pour regrouper les liens physiques par Link Tag (étiquette de liens) et pour contrôler la vitesse des liens et la fréquence à laquelle le pare-feu surveille les liens.

	Profil d’interface SD-WAN
Name (Nom)	Saisissez un nom pour le profil d’interface SD-WAN en utilisant un maximum de 31 caractères alphanumériques. Le nom doit commencer par un caractère alphanumérique et peut contenir des lettres, des nombres, des traits de soulignement (_), des traits-d’union (-), des points (.) et des espaces.
Emplacement	Sélectionnez un système virtuel pour un périphérique multi-vsys.
Étiquette de liens	Sélectionnez l’étiquette de liens que ce profil attribuera à l’interface ou ajoutez une nouvelle étiquette. Une étiquette de liens regroupe les liens physiques (de différents ISP) pour que le pare-feu puisse sélectionner parmi ceux-ci lors de la sélection du chemin d’accès et du basculement.
Description	Il est conseillé de saisir une description conviviale pour le profil.
Type de lien	Sélectionnez le type de lien physique dans la liste prédéfinie (**ADSL/DSL**, **Cable Modem [Modem câble]**, **Ethernet**, **Fiber [Fibre]**, **LTE/3G/4G/5G**, **MPLS**, **Microwave/Radio [micro-onde/radio]**, **Satellite**, **WiFi**, ou **Other [Autre]**). Le pare-feu est compatible avec n’importe quel périphérique CPE qui se termine par une connexion Ethernet sur le pare-feu ; par exemple, les points d’accès WiFi, des modems LTE, des CPE laser/micro-onde peuvent tous se terminer par un raccord Ethernet.

	Profil d’interface SD-WAN
	Pour les déploiements PAN-OS existants dont les zones sont définies sur les interfaces qui seront utilisées pour prendre en charge le PAN-OS SD-WAN, Panorama peut configurer automatiquement le nom de la zone de l’interface sur l’une des zones SD-WAN prédéfinies dans les conditions suivantes : *1. L’interface SD-WAN est configurée en tant que type de liaison privée point à point (**MPLS**, **satellite**, ou **micro-ondes**) dans son profil d’interface.* *2. La case**Assistance du tunnel de données VPN** est désactivée (décochée) sur le profil d’interface SD-WAN. Cela indique à PAN-OS de transférer le trafic en texte clair en dehors du tunnel VPN SD-WAN.* *Sur le pare-feu Hub, le nom de la zone est configuré comme «`zone-à-branche`» lorsque la condition #1 est remplie. Sur le pare-feu de la succursale, le nom de la zone est configuré comme «`zone-à-hub`» lorsque la condition #1 et la condition #2 sont remplies. Panorama automatise cette étape pour simplifier la configuration afin d’assurer une communication correcte entre le hub et les pare-feu des succursales. Si vous avez des stratégies de pare-feu préexistantes qui référençaient l’ancien nom de zone, vous devez mettre à jour les stratégies pour refléter le nouveau nom de zone SD-WAN prédéfini.*
Téléchargement maximum (Mbps)	Spécifiez la vitesse de téléchargement maximum de l’ISP en mégabits par seconde (Mbps) ; la plage est comprise entre 1 et 100 000 ; il n’y a pas de valeur par défaut. Demandez à votre ISP la vitesse du lien ou prenez un échantillon des vitesses maximales du lien à l’aide d’un outil comme speedtest.net et prenez la moyenne des maximales sur une bonne durée de temps.
Upload maximum (Mbps)	Spécifiez la vitesse de mise en téléchargement maximum de l’ISP en mégabits par seconde (Mbps) (la plage est comprise entre 1 et 100 000 ; il n’y a pas de valeur par défaut). Demandez à votre ISP la vitesse du lien ou prenez un échantillon des vitesses maximales du lien à l’aide d’un outil comme speedtest.net et prenez la moyenne des maximales sur une bonne durée de temps.
Eligible à la sélection d’interface de	Sélectionnez ce paramètre pour que les interfaces (lorsque vous appliquez ce profil) soient éligibles pour que le pare-feu d’encodage les sélectionne pour le Transfert de correction des erreurs (FEC) ou la duplication de paquet. Vous désélectionnez ce paramètre afin que la méthode FEC ou de duplication de paquet onéreuse ne soit jamais utilisée sur un lien onéreux (interface) auquel vous

	Profil d’interface SD-WAN
profil de correction des erreurs	appliquez le profil. Le**Link Type (type de lien)** indiqué pour le profil détermine si le paramètre par défaut de **Eligible for Error Correction Profile interface selection (éligible pour la sélection d’interface de profil de correction des erreurs)** est sélectionné ou non. Pour configurer FEC ou la duplication de paquet, créez un Error Correction Profile (Profil de correction ds erreurs) SD-WAN.
Assistance du tunnel de données VPN	Détermine si le trafic de la branche vers le hub et le trafic de retour passent par un tunnel VPN pour plus de sécurité (option activée par défaut) ou passe en dehors du tunnel VPN afin d’éviter la surcharge du cryptage. • Laissez **VPN Data Tunnel Support** (Assistance du tunnel de données VPN) activé pour les types de liens publics qui ont des connexions internet directes ou une capacité d’interruption d’internet, comme le modem câble, l’ADSL et les autres connexions internet. • Vous pouvez désactiver **VPN Data Tunnel Support** (Assistance du tunnel de données VPN) pour les types de liens privés comme MPLS, satellite, ou micro-onde qui n’ont pas de capacité de sortie internet. Cependant, vous devez d’abord vous assurer que le trafic ne peut pas être intercepté parce qu’il sera envoyé en dehors du tunnel VPN. • La branche peut avoir un trafic DIA qui nécessite de basculer sur le lien MPLS privé se connectant au hub et atteindre internet depuis le hub. Le réglage de **VPN Data Tunnel Support (Assistance du tunnel de données VPN)** détermine si les données privées passent par le tunnel VPN ou en dehors du tunnel et le trafic qui a basculé utilise l’autre connexion (que le flux de données privées n’utilise pas). Le pare-feu utilise des zones pour segmenter le trafic qui a basculé en DIA depuis le trafic MPLS privé.
Mesure de basculement VPN	(PAN-OS 10.0.3 and later releases (PAN-OS 10.0.3 et versions 10.0 ultérieures)) Lorsque vous configurez DIA AnyPath, vous avez besoin d’un moyen d’indiquer l’ordre de basculement des tunnels VPN individuels rassemblés sur une interface virtuelle de plate-forme ou de branche sur laquelle le DIA bascule. Indiquez la mesure de basculement VPN pour le tunnel VPN (lien) ; plage de 1 à 65 535 ; valeur par défaut 10. Plus la valeur de la mesure est faible, plus la priorité du tunnel est élevée (lien auquel vous appliquez ce profil) afin qu’il soit choisi lors du basculement. Par exemple, réglez la mesure sur une valeur faible et appliquez le profil à une interface de bande passante ; ensuite créez un profil différent qui définit une mesure élevée à appliquer à une interface LTE onéreuse afin de garantir qu’elle est utilisée uniquement après le basculement de bande passante.

	Profil d’interface SD-WAN
	*Si vous n’avez qu’un seul lien sur le hub, ce lien prend en charge toutes les interfaces virtuelles et le trafic DIA. Si vous souhaitez utiliser les types de liens dans un ordre spécifique, vous devez appliquer un profil de distribution du trafic au hub qui spécifie la **Top Down Priority (priorité descendante)** puis ordonner aux balises de lien de spécifier l’ordre préféré. Si vous appliquez un profil de distribution du trafic qui spécifie à la place **Best Available Path (meilleur chemin disponible)**, le pare-feu utilisera le lien, quel qu’en soit le coût, pour choisir le chemin d’accès le plus performant à la branche. En résumé, Lier des balises dans un profil de distribution du trafic. la balise link appliquée à une hub virtual interface (interface virtuelle hub) et une VPN Failover Metric (métrique de basculement VPN) fonctionnent uniquement lorsque le profil de distribution du trafic spécifie la **Top Down Priority (priorité descendante)**.*
Surveillance des chemins	Sélectionnez le mode de surveillance des chemins dans lequel le pare-feu surveille les interfaces auxquelles vous appliquez le profil d’interface SD-WAN. • **Aggressive (mode agressif)** — (Par défaut pour tous les types sauf LTE et Satellite) - Le pare-feu sonde les paquets à l’extrémité opposée du lien SD-WAN à une fréquence constante. *Utilisez le mode Agressif si vous avez besoin d’une détection rapide et d’un basculement dans des conditions de dégradation et de panne générale.* • **Relaxed (Mode souple)** —(Par défaut pour les types de lient LTE et Satellite) Le Pare-feu patiente quelques secondes (le**Probe Idle Time**) (délai d’attente de la sonde) entre l’envoi d’ensemble de paquets de sondage, ce qui rend la surveillance des chemins moins fréquente. Lorsque le délai d’attente de la sonde expire, le pare-feu envoie des sondes pendant sept secondes selon la **Probe Frequency (Fréquence de sondage)** configurée. *Utilisez le mode Souple lorsque vous avez des liens de bande passante faibles, des liens qui chargent en fonction de l’usage (comme LTE) ou lorsque la détection rapide n’est pas aussi importante que la préservation du coût et de la bande passante.*
Fréquence de sondage (par seconde)	Réglez la fréquence de sondage, qui correspond au nombre de fois par seconde où le pare-feu envoie un paquet de sondage à l’extrémité opposée du lien SD-WAN (la plage est comprise entre 1 et 5 ; la valeur par défaut est de 5).
Délai d’attente de la sonde (secondes)	Si vous sélectionnez le mode de surveillance des chemins **Relaxed (Souple)**, vous pouvez régler le délai d’attente de la sonde (en secondes) pendant lequel le pare-feu attend entre des ensembles de paquets de sondage (la plage est comprise entre 1 et 60 ; la valeur par défaut est 60).

	Profil d’interface SD-WAN
Délai d’attente avant basculement (secondes)	Saisissez le délai d’attente avant basculement (en secondes) pendant lequel le pare-feu attend qu’un lien récupéré soit qualifié avant que le pare-feu réaffecte ce lien en tant que lien préféré après le basculement (la plage est comprise entre 20 et 120 ; la valeur par défaut est 120). Le délai d’attente avant basculement empêche un lien récupéré d’être rétabli comme lien préféré trop rapidement et d’échouer de nouveau immédiatement.

Périphérique

Les sections suivantes servent de référence lors de la réalisation de tâches de maintenance et de configuration du système de base sur le pare-feu :

- Périphérique > Configuration
- Périphérique > Haute disponibilité
- Périphérique > Carte de transfert des journaux
- Périphérique > Audit de configuration
- Périphérique > Profils de mot de passe
- Périphérique > Administrateurs
- Périphérique > Rôles admin
- Périphérique > Domaine d'accès
- Périphérique > Profil d'authentification
- Périphérique > Séquence d'authentification
- Périphérique > Authentification de l’Utilisateur
- Périphérique > IoT > Serveur DHCP
- Périphérique > Redistribution des données
- Périphérique > Quarantaine du périphérique
- Périphérique > Sources d'informations de machine virtuelle
- Périphérique > Résolution des problèmes
- Périphérique > Systèmes virtuels
- Périphérique > Passerelles partagées
- Périphérique > Gestion des certificats
- Périphérique > Pages de réponse
- Périphérique > Paramètres des journaux
- Périphérique > Profils de serveur
- Périphérique > Base de données d'utilisateurs locale > Utilisateurs
- Périphérique > Base de données d'utilisateurs locale > Groupes d'utilisateurs
- Périphérique > Exportation programmée des journaux
- Périphérique > Logiciel
- Périphérique > Client GlobalProtect
- Périphérique > Mises à jour dynamiques
- Périphérique > Licences
- Périphérique > Support
- Périphérique > Clé principale et diagnostics

- Périphérique > Recommandation de politique

Périphérique > Configuration

- Périphérique > Configuration > Gestion
- Périphérique > Configuration > Opérations
- Périphérique > Configuration > Module de sécurité matériel
- Périphérique > Configuration > Services
- Périphérique > Configuration > Interfaces
- Périphérique > Configuration > Télémesure
- Périphérique > Configuration > Content-ID
- Périphérique > Configuration > WildFire
- Périphérique > Configuration > Session
- Périphérique > Configuration > DLP

Périphérique > Configuration > Gestion

- **Périphérique** > **setup** > **Gestion**
- **Panorama** > **setup** > **Gestion**

Sur un pare-feu, sélectionnez **Périphérique** > **Configuration** > **Gestion** pour configurer les paramètres de gestion.

Sur Panorama™, sélectionnez **Périphérique** > **Configuration** > **Gestion** pour configurer les pare-feu que vous gérez à l'aide des modèles Panorama. Sélectionnez **Panorama** > **Configuration** > **Gestion** pour configurer les paramètres de gestion de Panorama.

Sauf mention contraire, les paramètres de gestion suivants s'appliquent à la fois au pare-feu et à Panorama.

- Paramètres généraux
- Paramètres d'authentification
- Paramètres de la base de règles de politique
- Paramètres de Panorama : Périphérique > Configuration > Gestion (paramètres configurés sur le pare-feu pour se connecter à Panorama)
- Paramètres de Panorama : Panorama > Configuration > Gestion (paramètres configurés sur Panorama pour les connexions aux pare-feu)
- Paramètres de journalisation et de génération de rapports
- Interface de journal (PA-5450 uniquement)
- Bannières et messages
- Complexité minimale des mots de passe
- AutoFocus™
- Cortex Data Lake
- Paramètres des profils de gestion SSH
- Paramètres du service Edge PAN-OS

Élément	Description
Paramètres généraux	
Nom d'hôte	Saisissez un nom d'hôte (31 caractères maximum). Le nom est sensible à la casse, doit être unique et peut inclure uniquement des lettres, chiffres, virgules, traits d'union et traits de soulignement. Si vous ne saisissez rien, PAN-OS® utilise le modèle de pare-feu (par exemple, PA-5220_2) comme valeur par défaut. Vous pouvez éventuellement configurer le pare-feu afin d'utiliser un nom d'hôte fourni par un serveur DHCP. Reportez-vous à la section Accepter le Nom d'hôte fourni par le serveur DHCP (pare-feu uniquement).

Élément	Description
	Configurez un nom d'hôte unique pour facilement identifier le périphérique que vous gérez.
Domain (Domaine)	Saisissez le nom de domaine du réseau pour le pare-feu (31 caractères maximum). Vous pouvez éventuellement configurer les pare-feu et Panorama afin d'utiliser un domaine fourni par un serveur DHCP. Reportez-vous à la section Accepter le Domaine fourni par le serveur DHCP (pare-feu uniquement).
Accepter le Nom d'hôte fourni par le serveur DHCP (Pare-feu uniquement)	(S'applique uniquement lorsque le Type d'adresse IP de l'interface de gestion est Client DHCP)Sélectionnez cette option pour que l'interface de gestion accepte le nom d'hôte qu'elle reçoit du serveur DHCP. Le nom d'hôte obtenu du serveur (s'il est valide) remplace toute valeur spécifiée dans le champ Nom d'hôte.
Accepter le Domaine fourni par le serveur DHCP (Pare-feu uniquement)	(S'applique uniquement lorsque le Type d'adresse IP de l'interface de gestion est Client DHCP)Sélectionnez cette option pour que l'interface de gestion accepte le domaine (suffixe DNS) qu'elle reçoit du serveur DHCP. Le domaine obtenu du serveur remplace toute valeur spécifiée dans le champ **Domain (Domaine)**.
Bannière de connexion	Saisissez le texte (jusqu'à 3 200 caractères) que vous souhaitez afficher sur la page de connexion de l'interface Web en dessous des champs **Nom** et **Mot de passe**.
Forcer les administrateurs à accuser réception de la bannière de connexion	Sélectionnez cette option pour afficher et forcer les administrateurs à sélectionner **J'accepte et accuse réception de l'énoncé ci-dessous** (au-dessus de la bannière de connexion figurant sur la page de connexion), ce qui force les administrateurs à reconnaître qu'ils comprennent et acceptent le contenu du message avant de pouvoir **Se connecter**.
Mode TLS de gestion	Spécifiez les versions de protocole et les suites de chiffrement que votre interface de gestion négocie en sélectionnant l'un des modes TLS suivants. • **tlsv1.3_only**— Limite l'accès à l'interface de gestion aux connexions sécurisées par TLSv1.3 et les suites de chiffrement associées. Si un client ne peut pas négocier les chiffrements TLSv1.3, la connexion échoue. • **mixed mode (mode mixte)**Autorise l'accès de l'interface de gestion aux connexions sécurisées par n'importe quelle

Élément	Description
	version de TLS (TLSv1.0-TLSv1.3) et les suites de chiffrement associées. *TLSv1.1 est la première version TLS prise en charge par les pare-feu en mode FIPS-CC.* • (Default (Par défaut)) **exclude_tlsv1.3**— Limite l'accès à l'interface de gestion aux connexions sécurisées par TLSv1.0, TLSv1.1 ou TLSv1.2 et les suites de chiffrement associées.
certificate	Sélectionnez le certificat que votre serveur de gestion utilise pour sécuriser l'accès administratif à l'interface de gestion. *Ce paramètre est uniquement disponible pour les modes qui fournissent la prise en charge de TLSv1.3 (`tlsv1.3_only` et `mixed-mode (mode mixte)`). Pour restreindre les versions de protocole TLS, les suites de chiffrement et spécifier manuellement les certificats en mode **exclude_tlsv1.3***, configure an SSL/TLS service profile (configurez un profil de service SSL/TLS).
Profil de service SSL/TLS	Affectez un profil de service SSL/TLS existant ou créez-en un nouveau pour indiquer un certificat et les paramètres de protocole SSL/TLS autorisés sur l'interface de gestion (voir Device > Certificate Management > SSL/TLS Service Profile (Périphérique > Gestion des certificats > Profil de service SSL/TLS)). Le pare-feu ou Panorama utilise ce certificat pour authentifier les administrateurs qui accèdent à l'interface Web via l'interface de gestion (MGT) ou toute autre interface prenant en charge le trafic de gestion HTTP/HTTPS (voir Réseau > Profils réseau> Gestion de l'interface). Si vous sélectionnez **aucun** (par défaut), le pare-feu ou Panorama utilise le certificat prédéfini. *Le certificat prédéfini est fourni pour plus de commodité. Pour une meilleure sécurité, affectez un profil de service SSL/TLS. Pour garantir la fiabilité, le certificat doit être signé par un certificat d'autorité de certification (AC) qui se trouve dans le magasin de certificats racines approuvés des systèmes clients.*
Fuseau horaire	Sélectionnez le fuseau horaire du pare-feu.
Lieu	Sélectionnez la langue des rapports PDF dans la liste déroulante. Voir Surveillance > Rapports PDF > Gérer le récapitulatif PDF.

Élément	Description
	Même si une préférence de langue spécifique est définie pour l'interface Web, les rapports PDF utiliseront tout de même la langue indiquée dans ces **Paramètres locaux**.
Date	Définissez la date sur le pare-feu ; saisissez la date du jour (au format AAAA/MM/JJ) ou sélectionnez la date dans le menu déroulant. *Vous pouvez également définir un serveur NTP (**Périphérique** > **Configuration** > **Services**).*
Période	Définissez l'heure sur le pare-feu ; saisissez l'heure actuelle (en format 24 heures) ou sélectionnez l'heure dans le menu déroulant. *Vous pouvez également définir un serveur NTP (**Périphérique** > **Configuration** > **Services**).*
Numéro de série (Appareils virtuels Panorama uniquement)	Saisissez le numéro de série de Panorama. Vous pouvez trouver le numéro de série dans l'e-mail de confirmation de commande qui vous a été envoyé par Palo Alto Networks®.
Latitude	Saisissez la latitude (de -90,0 à 90,0) du pare-feu.
Longitude	Saisissez la longitude (de -180,0 à 180,0) du pare-feu.
Appliquer automatiquement un verrou de validation	Sélectionnez cette option pour appliquer automatiquement un verrou de validation lors de la modification de la configuration candidate. Pour plus d'informations, reportez-vous à la section Verrouillage des configurations. *Activez **Appliquer automatiquement un verrou de validation** afin d'éviter que d'autres administrateurs puissent apporter des changements de configuration avant que le premier administrateur ait valider ses changements.*
Vérification de la date d'expiration du certificat	Configurez le pare-feu pour qu'il renvoie des messages d'avertissement lorsque des certificats inclus approchent de leur date d'expiration.

Élément	Description
	*Activez la **Vérification de la date d'expiration du certificat** pour générer un message d'avertissement lorsque des certificats inclus approchent de leur date d'expiration.*
Fonction de systèmes virtuels multiples	Permet d'utiliser plusieurs systèmes virtuels sur les pare-feu prenant en charge cette fonctionnalité (voir Périphérique > Systèmes virtuels). *Pour activer plusieurs systèmes virtuels sur un pare-feu, les politiques du pare-feu doivent faire référence à un maximum de 640 groupes d'utilisateurs distincts. Si nécessaire, réduisez le nombre de groupes d'utilisateurs référencés. Puis, après avoir activé et ajouté plusieurs systèmes virtuels, les politiques peuvent ensuite référencer à nouveau 640 groupes d'utilisateurs pour chaque système virtuel supplémentaire.*
Base de données de filtrage des URL (Panorama uniquement)	Sélectionnez un fournisseur de filtrage des URL à utiliser avec Panorama : **brightcloud** ou **paloaltonetworks** (PAN-DB).
Utiliser les adresses MAC attribuées par l'hyperviseur (Pare-feu VM-Series uniquement)	Sélectionnez cette option pour que le pare-feu VM-Series utilise l'adresse MAC affectée par l'hyperviseur au lieu de générer une adresse MAC à l'aide du schéma personnalisé de PAN-OS. Si vous activez cette option et que vous utilisez une adresse IPv6 pour l'interface, l'ID d'interface ne doit pas être au format EUI-64 qui dérive l'adresse IPv6 de l'adresse MAC de l'interface. Dans une configuration (haute disponibilité ; HD) active/passive, une erreur de validation se produit si vous utilisez le format EUI-64.
Sécurité GTP	Sélectionnez cette option pour permettre l'inspection des messages du plan de contrôle et du plan de données utilisateur dans le trafic du GPRS Tunneling Protocol (protocole tunnel GPRS ; GTP). Voir Objets > Profils de sécurité > Protection de réseau mobile pour configurer un profil de protection de réseau mobile afin que vous puissiez appliquer la politique sur le trafic GTP.
Sécurité SCTP	Sélectionnez cette option pour permettre l'inspection et le filtrage des paquets et des blocs Stream Control Transmission Protocol (protocole de contrôle de transmission des flux ; SCTP) et pour appliquer la protection contre la saturation initiation (INIT) SCTP. Reportez-vous à la section Objets > Profils de sécurité >

Élément	Description
	Protection SCTP. Pour la protection contre la saturation SCTP INIT flood protection, reportez-vous à la section Configuration de la protection contre la saturation SCTP INIT.
Routage avancé	Sélectionnez cette option pour activer le moteur de routage avancé, qui prend en charge les itinéraires statiques, BGP, OSPFv2, OSPFv3, la multidiffusion IPv4 et RIPv2 sur les routeurs logiques. Vous devez valider et redémarrer le pare-feu pour que la modification vers le nouveau moteur de routage prenne effet (ou pour revenir au moteur d'itinéraire hérité).
Accélération du tunnel	Sélectionnez cette option pour améliorer la performance et la production pour le trafic qui passe par les tunnels GRE, les tunnels VXLAN et les tunnels GTP-U. Cette option est activée par défaut. • **accélération des tunnels GRE et VXLAN**: compatible avec les pare-feux de la série PA-3200et série PA-7000 avec PA-7000-NPC et SMC-B. • **accélération des tunnels GTP-U**: compatible avec les pare-feux de la série PA-7000-NPC et SMC-B. Pour que le trafic des tunnels GTP-U accélère, l'accélération des tunnels doit être activée, GTP doit être activé, aucune règle de politique d'inspection du contenu du tunnel (TCI) pour le protocole GTP-U ne peut être configuré et une règle de politique de sécurité avec un profil de protection de réseau mobile lié ne doit autoriser le trafic GTP. *Si vous désactivez ou ré-activer l'accélération des tunnels et que vous validez, vous devez redémarrer le pare-feu.*
Certificat du périphérique	
Obtenir un certificat	Cliquez afin de saisir le mot de passe à usage unique généré par le Portail Support Client. Le certificat du périphérique est nécessaire pour réussir à authentifier Panorama sur le CSP et d'exploiter les services cloud comme Zero Touch Provisioning (ZTP), IoT, Device Telemetry, et Enterprise Data Loss Prevention (prévention des pertes de données - DLP). Après avoir réussi l'installation du certificat de périphérique, les éléments suivants s'affichent : • **État du certificat de périphérique actuel** - L'état actuel du certificat de périphérique (`Valide`, `Invalide` ou `Expiré`) • **Valide à partir de** - L'horodotage indiquant le moment où la validité du certificat de périphérique commence.

Élément	Description
	• **Valide jusqu'à** - L'horodotage indiquant le moment où la validité du certificat de périphérique expire et le certificat de périphérique devient donc `invalide` ou `expiré`. • **Dernier message extrait** - Message indiquant si le certificat de périphérique est correctement installé ou si l'installation du certificat de périphérique a échoué. • **Dernier état extrait** - L'état de l'extraction du certificat de périphérique (`réussite` ou `échec`). • **Last Fetched Timestamp (Dernier horodatage extrait)** - L'horodatage de la dernière tentative d'installation du certificat de périphérique.
Paramètres d'authentification	
Profil d'authentification	Sélectionnez le profil d'authentification (ou la séquence) utilisé par le pare-feu pour authentifier les comptes administratifs que vous définissez sur un serveur externe plutôt que localement sur le pare-feu (voir Périphérique > Profil d'authentification). Lorsque des administrateurs externes se connectent, le pare-feu requiert l'authentification et demande des informations relatives aux autorisations (notamment le rôle administratif) au serveur externe. L'activation de l'authentification pour les administrateurs externes requiert des étapes supplémentaires en fonction du type de serveur indiqué par le profil d'authentification, qui doit être l'un des éléments suivants : • RADIUS • TACACS+ • SAML *Les administrateurs peuvent utiliser SAML pour s'authentifier sur l'interface Web, mais pas sur la CLI.* Sélectionnez **Aucun** pour désactiver l'authentification pour les administrateurs externes. Pour les comptes administratifs que vous définissez localement (sur le pare-feu), le pare-feu s'authentifie à l'aide du profil d'authentification attribué à ces comptes (voir Périphérique > Administrateurs).
Profil du certificat	Sélectionnez un profil de certificat pour vérifier les certificats clients des administrateurs qui sont configurés pour pouvoir accéder à l'interface Web du pare-feu grâce à un certificat.

Élément	Description
	Pour obtenir des instructions sur la configuration des profils de certificat, voir Périphérique > Gestion des certificats > Profil du certificat. *Configurez un profil de certificat pour vous assurer que la machine qui héberge l'administrateur possède les bons certificats pour authentifier le certificat CA racine défini dans le profil de certificat.*
Délai d'inactivité	Saisissez, pour l'interface Web ou la CLI, le délai d'inactivité maximum (en minutes) avant qu'un administrateur ne soit automatiquement déconnecté (la plage est comprise entre 0 et 1 440, la valeur par défaut est 60). Une valeur égale à 0 signifie que l'inactivité n'entraîne pas une déconnexion automatique. *L'actualisation manuelle et automatique des pages de l'interface Web (telles que l'onglet **Tableau de bord** et la boîte de dialogue Alarmes système) réinitialise le compteur **Délai d'inactivité**. Pour permettre au pare-feu d'appliquer le délai d'inactivité lorsque vous êtes sur une page qui prend en charge l'actualisation automatique, définissez l'intervalle d'actualisation sur **Manuel** ou sur une valeur supérieure au **Délai d'inactivité**. Vous pouvez également désactiver l'**Actualisation automatique** dans l'onglet **ACC**.* *Définissez un **Délai d'inactivité** de 10 minutes pour empêcher les utilisateurs non autorisés d'accéder au pare-feu si un administrateur laisse une session du pare-feu ouverte.*
Délai de vie de la clé API	Saisissez la durée, en minutes, pendant lesquelles la clé API est valide (plage comprise entre 0 et 525 600 ; par défaut 0). Une valeur de 0 signifie que la clé API n'expire jamais. Sélectionnez **Expirer toutes les clés API** pour invalider toutes les clés API précédemment générées. Utilisez cette option avec parcimonie, car toutes les clés existantes deviennent inutiles et les opérations pour lesquelles vous utilisez ces clés API cessent de fonctionner.

Élément	Description
	Effectuez cette opération lors d'une maintenance pour que vous puissiez remplacer les clés sans perturber les applications actuelles où les clés API sont référencées.
Les dernières clés API arrivées à expiration	Affiche l'horodatage de la dernière expiration de clés API Ce champ ne comporte aucune valeur si vous n'avez jamais réinitialisé vos clés.
Tentatives échouées	Saisissez le nombre d'échecs de tentatives de connexion (de 0 à 10) autorisées par le pare-feu pour l'interface Web et la CLI avant le verrouillage du compte administrateur. Une valeur de 0 indique un nombre illimité de tentatives de connexion. La valeur par défaut est de 0 pour les pare-feu en mode opérationnel normal et de 10 pour les pare-feu en mode FIPS-CC. Limiter les tentatives de connexion peut vous permettre de protéger le pare-feu contre les attaques en force. (Panorama managed firewalls only (Pare-feu gérés par Panorama uniquement)) La valeur minimale prise en charge est 1 lorsque vous gérez le paramètre de tentatives infructueuses à partir d'un modèle ou d'une configuration de pile de modèles sur Panorama. *Si vous définissez les **Tentatives échouées** sur une valeur autre que 0 mais que vous conservez la valeur **Durée de verrouillage** de 0, les **Tentatives échouées** sont ignorées et l'utilisateur n'est jamais verrouillé.* *Définissez le nombre de **Tentatives échouées** sur 5 ou moins pour permettre un nombre raisonnable de nouvelles tentatives en cas de fautes de frappe, tout en empêchant les systèmes malveillants de tenter des méthodes d'attaque par force pour se connecter au pare-feu.*
Durée de verrouillage	Saisissez le nombre de minutes (plage de 0 à 60) pendant lesquelles l'accès d'un administrateur à l'interface Web et la CLI est verrouillé par le pare-feu si la limite de **Tentatives échouées** est atteinte. Une valeur de 0 (par défaut) signifie que le verrouillage s'applique jusqu'à ce qu'un autre administrateur déverrouille manuellement le compte.

Élément	Description
	*Si vous définissez le champ **Tentatives échouées** sur une valeur non nulle, mais que vous laissez le champ **Durée de verrouillage** sur 0, l'utilisateur est verrouillé une fois le nombre défini de tentatives de connexion atteint et jusqu'à ce qu'un autre administrateur déverrouille manuellement le compte.* *Définissez la **Durée de verrouillage** sur au moins 30 minutes pour empêcher les tentatives de connexion continues d'un acteur malveillant.*
Compte de session max.	Saisissez le nombre de sessions simultanées max. autorisé pour tous les comptes administrateur et utilisateur (la plage est de 0 à 4). une valeur de 0 (par défaut) signifie qu'un nombre illimité de sessions simultanées est autorisé. *En mode FIPS-CC, la plage est de 0 à 4 avec une valeur par défaut de 4. Entrez une valeur de **0** pour autoriser un nombre illimité de sessions simultanées.*
Durée de session max.	Saisissez le nombre de minutes (la plage est de 60 à 1 499) pendant lesquelles un administrateur, actif, non passif peut rester connecté. Une fois que cette durée de session max est atteinte, la session est arrêtée et nécessite une nouvelle authentification pour commencer une autre session. La valeur par défaut est de 0 (30 jours) et ne peut pas être saisie manuellement. Si aucune valeur n'est saisie, la **durée de session max** est de 0 par défaut. *En mode FIPS-CC, la plage est de 60 à 1,499 avec une valeur par défaut de 720. Si aucune valeur n'est saisie, la **durée de session max** est de 720 par défaut.*
Paramètres de la base de règles de politique	
Étiquette exigée dans les politiques	Exige la présence d'au moins une étiquette lors de la création d'une nouvelle règle de politique. Si une règle de politique existe déjà lorsque vous activez cette option, vous devez ajouter au moins une étiquette lors de votre prochaine modification de la règle.
Description exigée dans les politiques	Vous devez ajouter une **Description** lors de la création d'une nouvelle règle de politique. Si une règle de politique existe

Élément	Description
	déjà lorsque vous activez cette option, vous devez ajouter une **Description** lors de votre prochaine modification de la règle.
Échec de validation si les politiques ne possèdent aucune étiquette ou description	Force l'échec de votre validation si vous n'ajoutez aucune étiquette ou description à la règle de politique. Si une règle de politique existe déjà lorsque vous activez cette option, la validation échouera si vous n'ajoutez aucune étiquette ou description lors de votre prochaine modification de la règle. Pour que la validation échoue, vous devez sélectionner les options **Étiquette exigée dans les politiques** ou **Description exigée dans les politiques**.
Commentaire d'audit exigé dans les politiques	Exige la présence d'un **Commentaire d'audit** lors de la création d'une nouvelle règle de politique. Si une règle de politique existe déjà lorsque vous activez cette option, vous devez ajouter un **Commentaire d'audit** lors de votre prochaine modification de la règle.
Expression régulière de commentaire d'audit	Précisez les exigences de paramètres pour le format des commentaires dans les commentaires d'audit.
Mode de correspondance descendante générique (pare-feu uniquement)	(PAN-OS 10.2.1 et versionsultérieures 10.2) Lorsque le mode de correspondance descendante générique est activé, lorsqu'un paquet correspond aux règles de stratégie de sécurité qui utilisent une adresse IP source ou de destination avec masque générique et que les masques se chevauchent, le pare-feu choisit la première de ces règles correspondantes (dans l'ordre descendant) qui correspond entièrement à tous les bits d'adresse basés sur le masquage. La valeur par défaut est désactivée ; en cas de correspondance de masques génériques qui se chevauchent, le pare-feu choisit la règle avec le préfixe correspondant le plus long dans le masque générique.
Nombre de correspondance à la règle de politique	Suivez la fréquence à laquelle le trafic est mis en correspondance avec des règles de politique que vous avez configurées sur le pare-feu. Lorsque cette option est activée, vous pouvez afficher le Nombre de correspondances total entre le trafic et chacune des règles, ainsi que la date et l'heure de création et de modification de la règle, et de la première correspondance et de la dernière correspondance.
Utilisation de l'application de la politique	

Panorama Settings Paramètres de Panorama): Périphérique > Configuration > Gestion

Configurez les paramètres suivants sur le pare-feu ou dans un modèle sur Panorama. Ces paramètres permettent d'établir une connexion entre le pare-feu et Panorama.

Élément	Description
Vous devez également configurer les paramètres de connexion et de partage d'objet sur Panorama (voir Paramètres de Panorama : Panorama > Configuration > Gestion). *Le pare-feu utilise une connexion SSL avec cryptage AES256 pour s'enregistrer sur Panorama. Par défaut, Panorama et le pare-feu s'authentifient mutuellement à l'aide de certificats 2 048 bits prédéfinis et utilisent la connexion SSL pour la gestion de la configuration et la collecte des journaux. Pour sécuriser davantage les connexions SSL entre Panorama, les pare-feu et les collecteurs de journaux, veuillez vous référer à la section* Sécurisation des communications avec le client *pour configurer des certificats personnalisés entre le pare-feu et Panorama ou un collecteur de journaux.*	
Managed By (Géré par)	Spécifiez si le pare-feu est géré par **Panorama** ou par un **Cloud Service (Service Cloud)**.
(Managed By Panorama only (Géré par Panorama uniquement)) Serveurs Panorama	Saisissez l'adresse IP ou le nom de domaine complet du serveur Panorama Si Panorama est dans une configuration haute disponibilité (HD), saisissez l'adresse IP ou le nom de domaine complet du serveur Panorama secondaire dans le second champ **Serveurs Panorama**.
Clé d'authentification	Entrez la device registration auth key (clé d'autorisation d'enregistrement de l'appareil) générée sur Panorama..
Délai d'attente en réception pour la connexion à Panorama	Saisissez le délai (en secondes) de réception des messages TCP de Panorama (plage de 1 à 240 ; par défaut 240).
Délai d'attente à l'envoi pour la connexion à Panorama	Saisissez le délai (en secondes) d'envoi des messages TCP à Panorama (plage de 1 à 240 ; par défaut 240).
Nombre de relances pour les envois SSL à Panorama	Saisissez le nombre de tentatives autorisées lors de l'envoi de messages SSL (Secure Socket Layer) à Panorama (plage de 1 à 64 ; par défaut 25).
Activation de la récupération automatique de la validation	Activez pour permettre au pare-feu de vérifier automatiquement sa connexion au serveur de gestion Panorama lorsqu'une configuration est validée et transmise au pare-feu et à des intervalles configurés après qu'une configuration a été transmise avec succès. Lorsque cette option est activée et que le pare-feu ne réussit pas à vérifier sa connexion avec le serveur de gestion Panorama, le pare-feu et la gestion Panorama reviennent à leur dernière configuration fonctionnelle afin de restaurer la connectivité.
Nombre de tentatives de vérification de la connectivité Panorama	Lorsque l'option **Activation de la récupération automatique de la validation** est activée, configurez le nombre de fois que le pare-feu teste sa connexion avec le serveur de gestion Panorama.

Élément	Description
Intervalle entre les tentatives (sec)	Lorsque l’option **Activation de la récupération automatique de la validation** est activée, configurez la durée en secondes entre les tentatives de connexion du pare-feu au serveur de gestion Panorama.
Communication sécurisée avec le client	Activez la **Sécurisation des communications avec le client** pour vous assurer que le pare-feu utilise des certificats personnalisés configurés (plutôt que le certificat par défaut) pour authentifier les connexions SSL avec Panorama ou les collecteurs de journaux. • **Aucun** (par défaut) – Si aucun certificat de périphérique n’est configuré et que le certificat prédéfini par défaut est utilisé. • **Local** – Le pare-feu utilise un certificat de périphérique local et la clé privée correspondante générée sur le pare-feu ou importée à partir d’un serveur PKI d’entreprise existant. • **Certificat** – Sélectionnez le certificat de périphérique local que vous avez généré ou importé. Ce certificat peut être unique au pare-feu (en fonction d’un hachage du numéro de série du pare-feu) ou il peut s’agir d’un certificat de périphérique commun utilisé par tous les pare-feu qui se connectent à Panorama. • **Profil de certificat** – Sélectionnez le Profil de certificat dans le menu déroulant. Le Profil de certificat définit le certificat CA à utiliser pour vérifier les certificats clients et comment vérifier l’état de révocation des certificats. • **SCEP** – Le pare-feu utilise un certificat de périphérique et une clé privée générée par un serveur SCEP (Protocole d’inscription de certificats simple). • **Profil SCEP** : Sélectionnez un Périphérique > Gestion de Certificat >SCEP dans le menu déroulant. Le Profil SCEP fournit à Panorama les informations nécessaires pour authentifier les périphériques clients auprès d’un serveur SCEP de votre PKI d'entreprise. • **Profil de certificat**: sélectionnez lePériphérique > Gestion de certificat dans le menu déroulant. Le Profil de certificat définit le certificat CA à utiliser pour vérifier les certificats clients et comment vérifier l’état de révocation des certificats.

Élément	Description
	• **Personnaliser la communication** – Le pare-feu utilise son certificat personnalisé configuré pour s'authentifier auprès des périphériques sélectionnés. • **Communication avec Panorama** – Le pare-feu utilise le certificat client configuré pour communiquer avec Panorama. • **Communication avec PAN-DB** – Le pare-feu utilise le certificat client configuré pour communiquer avec un appareil PAN-DB. • **Communication avec WildFire** – Le pare-feu utilise le certificat client configuré pour communiquer avec un appareil WildFire®. • **Communication avec le Collecteur de journaux** – Le pare-feu utilise le certificat client configuré pour communiquer avec le Collecteur de journaux. • **Vérification de l'identité du serveur** – (Communication avec Panorama et avec le Collecteur de journaux) Le pare-feu confirme l'identité du serveur en faisant correspondre le Common Name (nom commun ; CN) avec l'adresse IP ou le FQDN du serveur.
Activer/Désactiver les politiques et objets Panorama	Cette option s'affiche uniquement lorsque vous modifiez les **Paramètres de Panorama** sur un pare-feu (et non dans un modèle sur Panorama). **Désactiver les politiques et objets Panorama** désactive la propagation des politiques et objets de groupe de périphériques sur le pare-feu. Par défaut, cette action supprime également ces politiques et objets du pare-feu. Pour conserver une copie locale des politiques et objets sur le pare-feu, cochez **Importer les politiques et objets Panorama avant la désactivation dans la boîte de dialogue qui s'affiche lorsque vous cliquez sur cette option**. Une fois validés, ces politiques et objets font partie de la configuration du pare-feu et Panorama ne les gère plus. *Pour les pare-feu multi-vsys, vous devez d'abord importer la configuration du modèle, puis importer la configuration du groupe de périphériques pour désactiver avec succès la configuration transmise de Panorama.* Dans des conditions d'exploitation normales, la désactivation de la gestion Panorama est inutile et peut compliquer la configuration et la maintenance des pare-feu. Cette option s'applique généralement à des situations dans lesquelles les pare-feu nécessitent des règles et des valeurs d'objet différentes de

Élément	Description
	celles définies dans le groupe de périphériques. Un exemple type est lorsque vous déplacez un pare-feu hors de la production dans un environnement de laboratoire afin de le tester. Pour rétablir la gestion des politiques et des objets Panorama, cliquez sur le lien **Activer les politiques et objets Panorama**.
Activer/Désactiver le modèle de réseau et de périphérique	Cette option s'affiche uniquement lorsque vous modifiez les **Paramètres de Panorama** sur un pare-feu (et non dans un modèle sur Panorama). **Désactiver le modèle de réseau et de périphérique** désactive la propagation des informations relatives au modèle (configuration de périphérique et réseau) sur le pare-feu. Par défaut, cette action supprime également les informations de modèle du pare-feu. Pour conserver une copie locale des informations de modèle sur le pare-feu, cochez **Importer les modèles de réseau et de périphérique avant la désactivation** dans la boîte de dialogue qui s'affiche lorsque vous sélectionnez cette option. Une fois validés, les informations de modèle font partie de la configuration du pare-feu et Panorama ne les gère plus. *Pour les pare-feu multi-vsys, vous devez d'abord importer la configuration du modèle, puis importer la configuration du groupe de périphériques pour désactiver avec succès la configuration transmise de Panorama.* *Dans des conditions d'exploitation normales, la désactivation de la gestion Panorama est inutile et peut compliquer la configuration et la maintenance des pare-feu. Cette option s'applique généralement à des situations dans lesquelles les pare-feu nécessitent des valeurs de configuration de périphérique et réseau différentes de celles définies dans le modèle. Un exemple type est lorsque vous déplacez un pare-feu hors de la production dans un environnement de laboratoire afin de le tester.* Pour configurer le pare-feu afin qu'il recommence à accepter les modèles, cliquez sur **Activer/Désactiver les modèles de réseau et de périphérique**.

Panorama Settings Paramètres de Panorama): Panorama > Configuration > Gestion

Si vous utilisez Panorama pour gérer les pare-feu, configurez les paramètres suivants sur Panorama. Ces paramètres déterminent les délais d'expiration et les tentatives de message SSL des connexions entre Panorama et les pare-feu gérés, ainsi que les paramètres de partage d'objet.

Élément	Description
Vous devez également configurer les paramètres de connexion Panorama sur le pare-feu ou dans un modèle sur Panorama voir Paramètres de Panorama : Périphérique > Configuration > Gestion. *Le pare-feu utilise une connexion SSL avec cryptage AES256 pour s'enregistrer sur Panorama. Par défaut, Panorama et le pare-feu s'authentifient mutuellement à l'aide de certificats 2 048 bits prédéfinis et utilisent la connexion SSL pour la gestion de la configuration et la collecte des journaux. Pour sécuriser davantage ces connexions SSL, veuillez vous référer à la section* Personnaliser la communication sécurisée avec le serveur *pour configurer des certificats personnalisés entre Panorama et ses clients.*	
Délai d'attente en réception pour connexion au périphérique	Saisissez le délai (en secondes) de réception des messages TCP provenant de tous les pare-feu gérés (plage de 1 à 240 ; par défaut 240).
Délai d'attente à l'envoi pour la connexion au périphérique	Saisissez le délai (en secondes) d'envoi des messages TCP à tous les pare-feu gérés (plage de 1 à 240 ; par défaut 240).
Nombre de relances pour le périphérique SSL destinataire	Saisissez le nombre de tentatives autorisées lors de l'envoi de messages SSL (Secure Socket Layer) aux pare-feu gérés (plage de 1 à 64 ; par défaut 25).
Partager les objets de service et d'adresse inutilisés avec les périphériques	Sélectionnez cette option (activée par défaut) pour partager tous les objets partagés et les objets spécifiques à un groupe de périphériques Panorama avec les pare-feu gérés. Si vous désactivez cette option, l'appareil recherche des objets d'adresse, de groupe d'adresses, de services ou de groupes de services dans les politiques Panorama et ne partage aucun objet non référencé. Cette option permet de réduire le nombre total d'objets en s'assurant que l'appareil envoie uniquement les objets nécessaires aux pare-feu gérés. Si vous avez une règle de politique qui cible des appareils spécifiques dans un groupe d'appareils, alors les objets utilisés dans cette politique sont considérés comme utilisés dans ce groupe d'appareils.
Les objets définis dans la section ancienne ont une priorité supérieure.	Sélectionnez cette option (désactivée par défaut) pour indiquer que les valeurs d'objet dans les anciens groupes ont priorité sur celles des groupes descendants lorsque les groupes de périphériques à différents niveaux dans la hiérarchie ont des objets du même type et du même nom, mais avec des valeurs différentes. Cela signifie que lorsque vous validez un groupe de périphériques, les anciennes valeurs appliquent un contrôle prioritaire sur toutes les valeurs de contrôle prioritaire. De même, cette option entraîne le fait que la valeur d'un objet partagé remplace les valeurs d'objets du même type et du même nom dans les groupes de périphériques.

Élément	Description
	Si vous sélectionnez cette option, le lien Recherche d’objets remplacés s’affiche.
Recherche d’objets remplacés	Sélectionnez cette option (en bas de la boîte de dialogue Paramètres de Panorama) pour énumérer tous les objets *grisés*. Un objet ombré est un objet dans l’Emplacement partagé qui a le même nom, mais une valeur différente dans un groupe de périphériques. Le lien ne s’affiche que si vous indiquez que les objets définis dans les anciens emplacements auront préséance.
Activation des rapports et du filtrage sur les groupes	Sélectionnez cette option (désactivée par défaut) pour permettre à Panorama de stocker localement les noms d’utilisateur, les noms des groupes d’utilisateurs et les informations de mappage de nom d’utilisateur / groupe qu’il reçoit des pare-feu. Cette option est universelle pour tous les groupes de périphériques de Panorama. Cependant, vous devez également activer le stockage local au niveau de chaque groupe de périphériques en indiquant un Périphérique principal et en configurant la pare-feu pour le Stockage des utilisateurs et des groupes à partir du périphérique principal.
Paramètres de communication sécurisée: Panorama > Configuration > Gestion	
Personnaliser la communication sécurisée avec le serveur	• **Certificat personnalisé uniquement** – Lorsque cette option est activée, Panorama accepte uniquement des certificats personnalisés pour l’authentification avec des pare-feu et des Collecteurs de journaux gérés. • **Profil de service SSL/TLS** – Sélectionnez un profil de service SSL/TLS à partir du menu déroulant. Ce profil définit le certificat et les versions SSL/TLS compatibles que le pare-feu peut utiliser pour communiquer avec Panorama. • **Profil de certificat** – Sélectionnez un profil de certificat dans le menu déroulant. Ce profil de certificat définit le comportement de la vérification de la révocation du certificat et le certificat CA racine utilisé pour authentifier la chaîne de certificats présentée par le client. • **Liste d'autorisations** – **Ajoutez** et configurez un nouveau profil d’autorisation en utilisant les champs suivants pour définir les critères d’autorisation des périphériques cliens qui peuvent se connecter à Panorama. La Liste d’autorisations prend en charge un maximum de 16 entrées de profil. • **Identifier (Identifiant)** – Sélectionnez **Objet** ou **Autre nom d’objet** en tant qu’identifiant d’autorisation. • **Type** – Si vous avez choisi **Autre objet** en tant qu’identifiant, puis sélectionnez **IP**, **nom d’hôte** ou **e-mail** comme type de l’identifiant. Si vous avez sélectionné

Élément	Description
	Objet, vous devez utiliser le **nom commun** comme type d'identifiant. • **Valeur** – Saisissez la valeur d'identifiant. • **Autorisation des clients en fonction du numéro de série** – Panorama autorise les périphériques clients en fonction du hachage du numéro de série du périphérique. • **Vérifier la liste d'autorisations** – Panorama vérifie l'identité des périphériques clients par rapport à la liste d'autorisations. Un appareil ne doit correspondre qu'à un seul critère de la liste à autoriser. Si aucune correspondance n'est trouvée, le périphérique n'est pas autorisé. • **Délai d'attente de déconnexion (min)** – Période (en minutes) pendant laquelle Panorama attend avant de mettre fin à la connexion actuelle avec ses périphériques gérés. Panorama rétablit alors les connexions avec ses périphériques gérés en utilisant les paramètres de communication du serveur sécurisé et configuré. Le délai d'attente commence après que vous avez validé la configuration des communications sécurisées avec le serveur.
Communications sécurisées avec le client	L'utilisation de la **Communication sécurisée avec le client** permet de s'assurer que le client Panorama utilise des certificats personnalisés configurés (plutôt que le certificat prédéfini par défaut) pour authentifier les connexions SSL avec un autre appareil Panorama dans une paire HA ou avec un autre appareil WildFire. • **Prédéfini** (par défaut) – Aucun certificat de périphérique n'est configuré est Panorama utilise le certificat prédéfini par défaut. • **Local** – Panorama utilise un certificat de périphérique local et la clé privée correspondante générée sur le pare-feu ou importée à partir d'un serveur PKI d'entreprise existant. • **Certificat** – Sélectionnez le certificat de périphérique local. • **Profil de certificat** – Sélectionnez le Profil de certificat dans le menu déroulant. • **SCEP** – Panorama utilise un certificat de périphérique et une clé privée générée par un serveur Simple Certificate Enrollment Protocol (Protocole d'inscription de certificats simple ; SCEP). • **Profil SCEP** – Sélectionnez le Profil SCEP dans le menu déroulant.

Élément	Description
	• **Profil de certificat** – Sélectionnez le Profil de certificat dans le menu déroulant. • **Personnaliser la communication** • **Communication HA** – Panorama utilise le certificat client configuré pour assurer la communication HA avec son homologue HA. • **WildFire Communication (Communication avec WildFire)** – Panorama utilise le certificat client configuré pour communiquer avec un appareil WildFire.
Paramètres de journalisation et de génération de rapports Utilisez cette section pour modifier : • Les périodes d'expiration et les quotas de stockage des rapports et des types de journaux suivants. Les paramètres sont synchronisés entre les paires haute disponibilité. • Journaux de tous types qui sont générés par le pare-feu et qui sont stockés localement (**Périphérique** > **Configuration** > **Gestion**). Les paramètres s'appliquent à tous les systèmes virtuels sur le pare-feu. • Journaux qui sont générés par un appareil M-Series ou un appareil virtuel Panorama en mode Panorama et qui sont stockés localement : journaux système, journaux de configuration, journaux de statistiques d'application et journaux User-ID™ (**Panorama** > **Configuration** > **Gestion**). • Journaux de tous types qui sont générés localement par l'appareil virtuel Panorama en Mode hérité ou qui sont rassemblés à partir des pare-feu (**Panorama** > **Configuration** > **Gestion**). *Pour les journaux qui sont envoyés aux collecteurs de journaux Panorama par les pare-feu, vous pouvez définir des quotas de stockage et des périodes d'expiration pour chaque groupe de collecteurs (voir* Panorama > Groupes de collecteurs*).* • Attributs permettant le calcul et l'exportation de rapports d'activité des utilisateurs. • Rapports prédéfinis créés sur le pare-feu ou sur Panorama.	
Onglet Stockage des journaux (Le serveur de gestion de Panorama et tous les modèles de pare-feu, à l'exception des pare-feu de la série PA-5200 et de la série PA-7000)	Pour chaque type de journal, indiquez : • **Quota** – Le **Quota**, en pourcentage, attribué sur le disque dur pour le stockage des journaux. Lorsque vous modifiez une valeur de **Quota**, l'allocation du disque associée change automatiquement. Si le total de toutes les valeurs est supérieur à 100 %, un message s'affiche en rouge et un message d'erreur s'affiche lorsque vous tentez d'enregistrer les

Élément	Description
*Panorama affiche cet onglet si vous modifiez les paramètres de journalisation et de génération de rapports (**Panorama** > **Configuration** > **Gestion**). Si vous utilisez un modèle Panorama pour configurer les paramètres des pare-feu (**Périphérique** > **Configuration** > **Gestion**), veuillez vous référer aux onglets* Stockage à disque unique et Stockage à disque multiple.	paramètres. Dans ce cas, ajustez les pourcentages afin que le total soit inférieur ou égal à 100 %. *Par défaut, les pare-feu VM-Series dispose d'un quota de 0 % alloué au stockage du journal**SCTP**, au **Récapitulatif SCTP**, au **Récapitulatif SCTP horaire**, au **Récapitulatif SCTP quotidien** et au **Récapitulatif SCTP hebdomadaire**. Vous devez donc allouer un certain pourcentage à la journalisation de ces informations SCTP par ces pare-feu.* • **Max Days (Jours max)** – La durée (en jours) de la période d'expiration du journal (plage comprise entre 1 et 2 000). Le pare-feu ou l'appareil Panorama supprime automatiquement les journaux qui ont atteint la période spécifiée. Par défaut, il n'existe aucune période d'expiration, ce qui signifie que les journaux n'expirent jamais. Le pare-feu ou l'appareil Panorama évalue les journaux lors de leur création, puis supprime les journaux ayant atteint la période d'expiration ou la taille du quota. *Les journaux récapitulatifs hebdomadaires peuvent dépasser le seuil avant la suppression suivante s'ils atteignent le seuil d'expiration entre les intervalles de suppression des journaux par le pare-feu. Lorsqu'un quota de journal atteint la taille maximale, les nouvelles entrées du journal commencent à remplacer les entrées du journal les plus anciennes. Si vous réduisez la taille d'un quota de journal, le pare-feu ou Panorama supprime les journaux les plus anciens lorsque vous validez les modifications. Dans une configuration haute disponibilité, l'homologue passif ne reçoit pas les journaux et ne les supprime donc pas, sauf en cas de basculement et si l'homologue passif devient de fait actif.*
	• **Fichiers noyau** – Si votre pare-feu connaît une défaillance du système fonctionnel, il générera un fichier noyau qui contient des détails sur le processus et sur la raison de l'échec. Si un fichier noyau est trop lourd pour l'emplacement de stockage du fichier noyau par défaut (`/var/cores` partition), vous pouvez activer l'option de fichier **`large-core`** pour attribuer un emplacement de stockage alternatif et plus grand (`/opt/panlogs/cores`). Un ingénieur d'assistance de

Élément	Description

	Palo Alto Networks peut augmenter le stockage attribué si nécessaire.
	
	Pour activer ou désactiver l'option **de fichier à gros cœur** entrez la commande CLI suivante à partir du mode de configuration, puis **validez** la configuration :
	
	`# set deviceconfig setting management large-core [yes|no]`
	
	Le fichier noyau est supprimé si vous désactivez cette option.
	
	Vous devez utiliser le protocole SCP du mode opérationnel pour exporter le fichier noyau :
	
	`> scp export core-file large-corefile`
	
	Seul un ingénieur d'assistance de Palo Alto Networks peut interpréter le contenu des fichiers noyaux.
	
	• **Rétablir les valeurs par défaut** – Sélectionnez cette option pour revenir aux valeurs par défaut.

Onglets **Stockage du journal de session** et **Stockage du journal de gestion** (Uniquement les pare-feu des séries PA-5200 et PA#7000)	Les pare-feu de la série PA-5200 et de la série PA-7000 enregistrent les journaux de gestion et les journaux de sessions sur des disques séparés. Sélectionnez l'onglet pour chaque ensemble de journaux et configurez les paramètres décrits dans l'Onglet Stockage des journaux : • **Stockage des journaux de sessions** – Sélectionnez **Quota de journal de sessions** et définissez des quotas et des périodes d'expiration pour les journaux de trafic, de menaces, de filtrage des URL, de correspondance HIP, d'User-ID, GTP / Tunnel, SCTP et d'authentification, ainsi que les PCAPs de menaces étendues. • **Stockage des journaux de gestion** – Définissez des quotas et des périodes d'expiration pour les journaux système, les journaux de configuration et les journaux de statistiques de l'application, ainsi que pour les rapports HIP, les captures de filtrage de données, les PCAP d'application et les PCAP de filtrage de débogage.
Onglets **Stockage à disque unique** et **Stockage à disque multiple**	Si vous utilisez un modèle Panorama pour configurer les quotas de journal et les périodes d'expiration, configurez les paramètres

Élément	Description
(Modèle Panorama uniquement)	dans l'un ou dans les deux onglets suivants en fonction des pare-feu affectés au modèle : • **Pare-feu de la série PA-5200 et de la série PA-7000** – Sélectionnez **Stockage à disque multiple** et configurez les paramètres dans les onglets Stockage des journaux de session et Stockage des journaux de gestion. *Par défaut, les pare-feu de la série PA-5200 dispose d'un quota de 0 % alloué au stockage du journal**SCTP**, au **Récapitulatif SCTP**, au **Récapitulatif SCTP horaire**, au **Récapitulatif SCTP quotidien** et au **Récapitulatif SCTP hebdomadaire**. Vous devez donc allouer un certain pourcentage à la journalisation de ces informations SCTP par ces pare-feu.* • **Tous les autres modèles de pare-feu** – Sélectionnez **Stockage à disque unique**, sélectionnez **Quota de journal de session** et configurez les paramètres sur l'onglet Stockage des journaux.
Onglet Exportation des journaux et génération de rapports	Configurez les paramètres d'exportation et de rapport des journaux suivants au besoin : • **Nombre de versions d'audit de configuration** : saisissez le nombre de versions de configuration à enregistrer avant de supprimer les plus anciennes (par défaut 100). Vous pouvez utiliser ces versions enregistrées pour contrôler et comparer les modifications apportées à la configuration. • **Nombre de versions de sauvegarde de configuration** – (Panorama uniquement) Saisissez le nombre de sauvegardes de configuration à enregistrer avant de supprimer les plus anciennes (la valeur par défaut est 100). • **Nombre max. de lignes exportées au format CSV** – Saisissez le nombre maximum de lignes qui s'affichent dans les rapports CSV générés en cliquant sur **Export to CSV (Exporter vers un fichier CSV)** dans la vue des journaux du trafic (plage de 1 à 1 048 576 ; par défaut 65 535). • **Nombre max. de lignes dans le rapport d'activité des utilisateurs** – Saisissez le nombre maximum de lignes pris en charge pour les rapports d'activité des utilisateurs détaillés (plage de 1 à 1 048 576 ; par défaut 5 000).
Onglet Exportation des journaux et génération de rapports (suite)	• **Durée de navigation moyenne (secondes)** – Configurez cette variable pour ajuster la manière dont la durée de navigation est calculée en secondes pour Surveillance > Rapports au

Élément	Description
	format PDF > Rapport d’activité des utilisateurs (plage de 0 à 300 secondes ; par défaut 60). Le calcul ignore les sites classés comme des publicités Web et des réseaux de distribution de contenu. Le calcul de la durée de navigation est basé sur les pages de conteneur consignées dans les journaux de filtrage des URL. Les pages de conteneur servent de base au calcul car de nombreux sites chargent du contenu de sites externes qui ne doit pas être pris en compte. Pour plus d’informations sur la page de conteneur, reportez-vous à la section Pages de conteneur. Le paramètre de durée de navigation moyenne correspond à la durée moyenne jugée nécessaire par l’administrateur à la navigation d’une page Web par un utilisateur. Toute requête formulée une fois la durée de navigation moyenne écoulée sera considérée comme une nouvelle activité de navigation. Le calcul ignore les nouvelles pages Web chargées entre la première requête (heure de début) et la durée de navigation moyenne. Ce comportement a été conçu afin d’exclure des sites externes et chargés depuis la page Web consultée. Exemple : si la durée de navigation moyenne est définie sur 2 minutes et qu’un utilisateur ouvre une page Web et la consulte pendant 5 minutes, la durée de navigation de cette page sera toujours de 2 minutes. Ceci est dû au fait qu’il est impossible de déterminer la durée de consultation d’une page donnée par un utilisateur • **Seuil de chargement de page (secondes)** – Vous permet de régler la durée supposée (en secondes) de chargement des éléments sur la page (plage de 0 à 60 ; par défaut 20). Toute requête formulée entre le premier chargement de page et le seuil de chargement de page est considérée comme des éléments de la page. Toute requête formulée en dehors du seuil de chargement de page est supposée correspondre à un clic de l’utilisateur sur un lien dans la page. Le seuil de chargement de page est également utilisé dans les calculs pour Surveillance > Rapports PDF > Rapport d’activité des utilisateurs. • **Format NOM D’HÔTE Syslog** – Choisissez le FQDN, le nom d’hôte ou l’adresse IP (IPv4 ou IPv6) à utiliser dans l’en-tête du message Syslog. Cet en-tête identifie le serveur de gestion du pare-feu ou de Panorama d’où le message est originaire. • **Temps d’exécution du rapport** – Sélectionnez l’heure (la valeur par défaut est 2 heures) à laquelle le pare-feu ou l’appareil Panorama commence à générer des rapports quotidiens programmés.

Élément	Description
	• **Période d’expiration du rapport** – Définissez la période d’expiration (en jours) des rapports (plage de 1 à 2 000). Par défaut, il n’existe aucune période d’expiration, ce qui signifie que les rapports n’expirent jamais. Le pare-feu ou l’appareil Panorama supprime les rapports expirés chaque nuit à 2 h, en fonction de l’heure du système.
	• **Arrêter le trafic lorsque la base de données des journaux est saturée** (pare-feu uniquement ; désactivée par défaut) – Sélectionnez cette option si vous souhaitez que le trafic via le pare-feu soit arrêté lorsque la base de données des journaux est saturée. • **Activer l’accès à l’archivage sécurisé des menaces** (activé par défaut) – Permet au pare-feu d’accéder à l’Archivage sécurisé des menaces pour recueillir les dernières informations sur les menaces détectées. Cette information est disponible pour les journaux de menaces et pour les principales activités de menaces inscrites sur l’ACC. • **Activer la journalisation de la charge DP** (pare-feu uniquement ; désactivée par défaut) – Sélectionnez cette option pour indiquer qu’une entrée du journal système est générée lorsque la charge de traitement des paquets sur le pare-feu utilise le processeur à 100 %.  *L’option **Activer la journalisation de la charge DP** permet aux administrateurs d’enquêter et d’identifier la cause de la forte utilisation du processeur.* *Une charge processeur élevée peut altérer le fonctionnement du système, car le nombre de cycles du processeur n’est pas suffisant pour traiter tous les paquets. Le journal système vous informe de ce problème (une entrée est générée dans le journal à chaque minute) et vous permet d’en déterminer la cause.* • **Activer le transfert de données à grande vitesse** (pare-feu de la série PA-5200, PA-5450 et de la série PA-7000 uniquement ; désactivé par défaut) – En tant que meilleure pratique, sélectionnez cette option pour transférer des journaux vers Panorama avec un débit maximal de 7000 journaux/seconde. Lorsque cette option est désactivée,

Élément	Description
	le pare-feu transmet des journaux à Panorama avec un débit maximal de seulement 80 000 journaux par seconde. Si vous activez cette option, le pare-feu ne stocke pas les journaux localement ou ne les affiche pas dans les onglets **Tableau de bord**, **ACC**, ou **Surveillance**. De plus, vous devez configurer le transfert de journal vers Panorama pour utiliser cette option. • **État du collecteur de journaux** : affiche l'état du pare-feu, à savoir s'il a établi avec succès une connexion à l'architecture de Collecte de journaux distribuée et s'il lui envoie des journaux. Si le pare-feu est également configuré pour envoyer des journaux au service de journalisation, vérifiez l'état du , dans la section Service de journalisation.
(Panorama uniquement)	• **Transfert des journaux mis en mémoire tampon depuis le périphérique** (activé par défaut) – Permet au pare-feu de mettre en mémoire tampon les entrées de journal sur son disque dur (stockage local) lorsqu'il perd la connectivité à Panorama. Lorsque la connexion à Panorama est rétablie, le pare-feu transfère les entrées de journal à Panorama ; l'espace disque disponible pour la mise en mémoire tampon dépend du quota de stockage des journaux sur le modèle du pare-feu et du volume des journaux en attente de transfert. Si l'espace disque disponible est utilisé, les entrées les plus anciennes sont supprimées pour permettre la journalisation des nouveaux événements. *Activez l'option **Transfert des journaux mis en mémoire tampon depuis le périphérique** pour empêcher la perte des journaux en cas d'échec de la connexion à Panorama.* • **Obtenir uniquement les nouveaux journaux lors de la conversion vers le périphérique principal** (désactivé par défaut) – Cette option s'applique uniquement à un appareil virtuel Panorama en mode hérité qui écrit des journaux dans un système de fichiers réseau (NFS). Avec la journalisation NFS, seul le serveur Panorama principal est monté sur le NFS. Par conséquent, les pare-feu envoient des journaux uniquement à l'appareil Panorama principal actif. Cette option vous permet de configurer les pare-feu de manière à ce qu'ils envoient les nouveaux journaux générés uniquement à Panorama, lorsqu'un basculement HD se produit et que le serveur Panorama secondaire reprend la journalisation sur le NFS (après avoir été promu serveur principal). Cette option est généralement activée pour éviter

Élément	Description
	aux pare-feu d’envoyer de gros volumes de journaux placés en mémoire tampon une fois la connectivité vers Panorama restaurée après une période significative. • **Seulement les journaux actifs sur le disque local** (désactivé par défaut) – Cette option s’applique uniquement à un appareil virtuel Panorama en mode hérité. Cette option vous permet de configurer uniquement le Panorama actif pour enregistrer les journaux sur le disque local.
	• **Rapports prédéfinis** (activé par défaut) – Des rapports prédéfinis relatifs aux applications, au trafic, aux menaces, au filtrage des URL et au Stream Control Transmission Protocol (protocole de contrôle de transmission des flux ; SCTP) sont disponibles sur le pare-feu et sur Panorama. Les rapports prédéfinis relatifs à SCTP sont disponibles sur le pare-feu et sur Panorama une fois que la Sécurité SCTP est activée sous **Périphérique** > **Configuration** > **Gestion** > **Paramètres généraux**. Comme les pare-feu consomment des ressources mémoires lors de la génération des résultats toutes les heures (et de leur transfert à Panorama où ils sont agrégés et compilés pour affichage), pour réduire l’utilisation de la mémoire, vous pouvez désactiver les rapports qui ne vous sont pas utiles. Pour désactiver un rapport, désactivez cette option en regard du rapport. Cliquez sur **Select All (Sélectionner tout)** ou **Deselect All (Désélectionner tout)** pour activer ou de désactiver la génération de rapports prédéfinis. *Avant de désactiver un rapport, assurez-vous qu’aucun Rapport de groupe ou Rapport au format PDF ne l’utilise. Si vous désactivez un rapport prédéfini attribué à un ensemble de rapports, l’ensemble des rapports ne contiendra plus aucune donnée.* • **Log Admin Activity (Activité d’administrateur de connexion)** (désactivé par défaut) : indiquez s'il faut générer un journal d'audit lorsqu'un administrateur exécute une commande opérationnelle dans la CLI du pare-feu ou navigue via l'interface Web. Vous devez d'abord configurer avec succès un serveur syslog avant de pouvoir générer et transmettre un journal d'audit. • **Operational Commands (Commandes opérationnelles)** : générez un journal d'audit lorsqu'un administrateur exécute une commande opérationnelle ou de débogage

Élément	Description
	dans la CLI ou une commande opérationnelle déclenchée à partir de l'interface Web. Consultez la CLI Operational Command Hierarchy (hiérarchie des commandes opérationnelles) de l'interface de ligne de commande pour obtenir la liste complète des commandes opérationnelles et de débogage de PAN-OS. • **UI Actions (Actions de l'interface utilisateur)** : générez un journal d'audit lorsqu'un administrateur navigue dans l'interface Web. Cela inclut la navigation entre les onglets de configuration, ainsi qu'entre les objets individuels au sein d'un onglet. Par exemple, un journal d'audit est généré lorsqu'un administrateur navigue de l'**ACC** vers l'onglet **Policies (Politiques)**. De plus, un journal d'audit est généré lorsqu'un administrateur navigue depuis **Objects (Objets)** > **Addresses (Adresses)**vers **Objects (Objets)** > **Tags (Etiquettes)**. • **Syslog Server (Serveur Syslog)** : sélectionnez le profil de serveur syslog cible pour transférer les journaux d'audit.
Interface de journal (PA-5450 uniquement)	
Adresse IP	Entrez l'adresse IP du port de l'interface du journal. *Lorsque les interfaces de journal sont configurées avec une adresse IP, tout transfert de journal passe automatiquement de la gestion par l'interface de gestion (par défaut) à l'interface de journal, sauf si un itinéraire de service est spécifié pour un service particulier. Les itinéraires de service spécifiques sont hiérarchisés par l'interface du journal.*
netmask	Spécifiez le masque réseau pour l'adresse IP de l'interface du journal.
Passerelle par défaut	Entrez l'adresse IP de la passerelle par défaut pour activer le chemin d'accès des journaux sortants.
Adresse IPv6	Si votre réseau utilise IPv6, définissez les options suivantes : • **Adresse IPv6 : adresse**IPv6 du port de l'interface du journal. • **Default Gateway (Passerelle par défaut)** - Adresse IPv6 de la passerelle par défaut du port.
Vitesse de liaison	Sélectionnez la vitesse de l'interface en Mbits/s ou sélectionnez **Auto** (par défaut) pour que le pare-feu détermine

Élément	Description
	automatiquement la vitesse en fonction de la connexion. **Auto** est la seule option possible pour les interfaces dont la vitesse ne peut être configurée.
Mode duplex de la liaison	Indiquez si le mode de transmission de l'interface est en duplex intégral (**full (intégral)**), semi-duplex (**half (semi)**) ou automatiquement négocié (**auto**).
état des liaisons	Indiquez si l'état de l'interface est activé (**up (actif)**), désactivé **down (inactif)**) ou automatiquement déterminé en fonction de la connexion (**auto**). La valeur par défaut est **auto**.
Statistiques de l’interface de journalisation	Sélectionnez **Afficher les statistiques** pour afficher les statistiques et les erreurs de paquets.

Bannières et messages

Pour afficher tous les messages dans une boîte de dialogue Message du jour, reportez-vous à la section Message du jour.

*Une fois que vous avez configuré le Message du jour et cliqué sur **OK**, les administrateurs qui se connectent ensuite ainsi que les administrateurs actifs qui actualisent leur navigateur verront immédiatement le nouveau message ou le message mis à jour ; une validation n’est pas requise. Cela vous permet d’avertir les autres administrateurs qu’une validation est imminente juste avant que vous l’effectuiez.*

Message du jour (case à cocher)	Sélectionnez cette option pour afficher la boîte de dialogue Message du jour lorsqu’un administrateur se connecte à l’interface Web.
Message du jour (champ de saisie de texte)	Saisissez le texte (jusqu’à 3 200 caractères) de la boîte de dialogue Message du jour.
Autoriser l’option Ne plus afficher	Sélectionnez cette option (désactivée par défaut) pour inclure la case à cocher **Do not show again (Ne plus afficher)** dans la boîte de dialogue Message du jour. Cette option offre aux administrateurs la possibilité de ne pas revoir ce même message lors de leurs prochaines connexions.

Élément	Description
	*Si vous modifiez le texte du **Message of the Day (Message du jour)**, le message s'affichera même pour les administrateurs qui ont sélectionné **Do not show again (Ne plus afficher)**. Les administrateurs doivent resélectionner cette option pour éviter de voir le message modifié lors de sessions ultérieures, à moins que le message soit modifié de nouveau.*
Title	Saisissez le texte de l'en-tête du Message du jour (par défaut `Message du jour`).
Couleur d'arrière-plan	Sélectionnez une couleur de fond pour la boîte de dialogue Message du jour. Par défaut (**None (Aucune)**), la couleur de fond est un gris clair.
Icône	Sélectionnez une icône prédéfinie qui apparaîtra au-dessus du texte dans la boîte de dialogue Message du jour : • **None (Aucune)** (par défaut) • **Erreur**  • **Aide**  • **Information**  • **Avertissement** 
Bannière de l'en-tête	Saisissez le texte qu'affiche la bannière de l'en-tête (jusqu'à 3 200 caractères).
Couleur de l'en-tête	Sélectionnez une couleur de fond pour l'en-tête. Par défaut (**None (Aucune)**), il n'y a aucune couleur de fond (transparent).
Couleur de texte de l'en-tête	Sélectionnez une couleur pour le texte de l'en-tête. Par défaut (**None (Aucune)**), la couleur de fond est noire.
Même bannière pour l'en-tête et le pied de page	Sélectionnez cette option (activée par défaut) si vous voulez que la bannière du pied de page possède le même texte et les mêmes couleurs que la bannière de l'en-tête. Lorsque cette option est activée, les champs pour le texte et les couleurs de la bannière du pied de page sont grisés.
Bannière du pied de page	Saisissez le texte qu'affiche la bannière du pied de page (jusqu'à 3 200 caractères).

Élément	Description
Couleur du pied de page	Sélectionnez une couleur de fond pour le pied de page. Par défaut (**None (Aucune)**), il n'y a aucune couleur de fond (transparent).
Couleur de texte du pied de page	Sélectionnez une couleur pour le texte du pied de page. Par défaut (**None (Aucune)**), la couleur de fond est noire.
Complexité minimale des mots de passe	
Activé	Activez les exigences minimales des mots de passe pour les comptes locaux. Cette fonction garantit que les comptes administrateur locaux sur le pare-feu sont conformes à un ensemble d'exigences des mots de passe. Vous pouvez également créer un profil de mot de passe contenant un sous-ensemble de ces options qui appliqueront un contrôle prioritaire sur ces paramètres et qui peut être appliqué à des comptes spécifiques. Pour plus d'informations, voir Périphérique > Profils de mot de passe et reportez-vous à la section Exigences relatives au nom d'utilisateur et au mot de passe pour obtenir des informations sur les caractères valides qui peuvent être utilisés pour les comptes. *La longueur maximale du mot de passe est de 64 caractères.* Si la haute disponibilité (HD) est configurée, utilisez toujours l'homologue principal lors de la configuration des options de complexité des mots de passe et validez immédiatement après l'apport de modifications. Les paramètres de complexité minimale du mot de passe ne s'appliquent pas aux comptes de bases de données locales pour lesquelles vous avez indiqué un **Hachage du mot de passe** (voir Périphérique > Base de données locale des utilisateurs > Utilisateurs).

Élément	Description
	Exigez des mots de passe forts pour aider à prévenir les attaques par force brute d'accès au réseau. Exigez une longueur minimale et l'utilisation d'au moins un de chacun des éléments suivants : lettre majuscule, lettre minuscule, valeur numérique et caractère spécial. De plus, évitez les répétitions excessives de caractères et de noms d'utilisateur dans les mots de passe, définissez les limites sur la fréquences de réutilisation des mots de passe et définissez les périodes régulières de modification des mots de passe, afin d'éviter que les mots de passe soient utilisés trop longtemps. Plus les exigences en matière de mot de passe sont élevées, plus il est difficile pour les pirates de pirater un mot de passe. Veillez à respecter les pratiques exemplaires en matière de robustesse des mots de passe *pour vous assurer de créer un mot de passe fort.*
Longueur minimale	Une longueur minimale de mot de passe est requise (plage de 1 à 16 caractères). *En mode FIPS-CC, la longueur minimale du mot de passe est comprise entre 8 et 16 caractères.*
Nombre minimum de lettres en majuscules	Un nombre minimum de lettres en majuscules est requis (plage de 0 à 16 caractères).
Nombre minimum de lettres en minuscule	Un nombre minimum de lettres en minuscules est requis (plage de 0 à 16 caractères).
Nombre minimum de chiffres	Un nombre minimum de chiffres est requis (plage de 0 à 16 chiffres).
Nombre minimum de caractères spéciaux	Un nombre minimum de caractères spéciaux (non alphanumériques) est requis (plage de 0 à 16 caractères).
Bloquer les caractères récurrents	Indiquez le nombre de caractères en double séquentiels qui sont autorisés dans un mot de passe (plage de 3 à 16). Si vous définissez la valeur 3, le mot de passe peut comporter le même caractère séquentiel trois fois, mais si le même caractère est utilisé quatre fois ou plus dans une séquence, le mot de passe n'est pas autorisé.

Élément	Description
	Par exemple, si la valeur est définie sur 3, le système acceptera le mot de passe test111 ou 111test111, mais pas test1111, car le chiffre 1 apparaît quatre fois dans la séquence.
Bloquer l’intégration du nom d’utilisateur (inversé inclus)	Sélectionnez cette option pour empêcher l’utilisation du nom d’utilisateur du compte (ou une version inversée du nom) dans le mot de passe.
Les caractères du nouveau mot de passe sont différents	Lorsque les administrateurs changent leurs mots de passe, les caractères doivent être différents de la valeur définie.
Changement de mot de passe exigé à la première ouverture de session	Sélectionnez cette option pour demander aux administrateurs de changer leurs mots de passe à la prochaine connexion au pare-feu.
Empêcher la limite de réutilisation du mot de passe	Demandez à ce qu’un mot de passe précédent ne soit pas réutilisé en fonction du nombre défini. Par exemple, si la valeur est définie sur 4, vous ne pouvez pas réutiliser l’un de vos 4 derniers mots de passe (plage de 0 à 50).
Blocage de la période de modification du mot de passe (jours)	L’utilisateur ne peut pas changer son mot de passe avant le nombre de jours défini (plage de 0 à 365 jours).
Période de modification du mot de passe requise (jours)	Requiert que les administrateurs modifient régulièrement leur mot de passe (plage de 0 à 365 jours). Par exemple, si la valeur est définie sur 90, les administrateurs sont invités à modifier leur mot de passe tous les 90 jours. Vous pouvez également définir un message d’avertissement d’expiration de 0 à 30 jours et indiquer un délai supplémentaire.
Avertissement avant la date d’expiration (jours)	Si une **Required Password Change Period (Période de modification du mot de passe requise)** est définie, vous pouvez utiliser cet **Expiration Warning Period (Avertissement avant expiration)** pour demander à l’utilisateur de modifier son mot de passe lorsqu’il reste moins qu’un certain nombre de jours indiqués avant la date de modification du mot de passe requise (plage de 0 à 30).
Nombre d'ouvertures de session Administrateur après expiration (nombre)	Autorise l’administrateur à se connecter un certain nombre de fois après la date de modification requise (plage de 0 à 3). Par exemple, si vous définissez cette valeur sur 3 et que le compte est arrivé à expiration, l’administrateur peut se connecter encore trois fois sans modifier son mot de passe avant que le compte ne soit verrouillé.

Élément	Description
Période de grâce après expiration (jours)	Autorise l'administrateur à se connecter un certain nombre de jours une fois le compte arrivé à expiration (plage de 0 à 30).
AutoFocus™	
Activé	Activez le pare-feu pour qu'il se connecte à un portail AutoFocus afin de récupérer des données de renseignement sur la menace et de permettre des recherches intégrées entre le pare-feu et AutoFocus. Lorsque le pare-feu est connecté à AutoFocus, il affiche les données AutoFocus associées aux entrées de journal en ce qui concerne le Trafic, la Menace, le Filtrage des URL, les Envois WildFire et le Filtrage des données (**Surveillance** > **Journaux**). Vous pouvez cliquer sur un artefact dans ces types d'entrées de journal (comme une adresse IP ou une URL) pour afficher un récapitulatif des résultats et des statistiques AutoFocus pour cet artefact. Vous pouvez ensuite lancer une recherche AutoFocus élargie pour l'artefact directement à partir du pare-feu. *Vérifiez que votre licence AutoFocus est active sur le pare-feu (**Device (Périphérique)** > **Licenses (Licences)**). Si la licence AutoFocus n'est pas affichée, utilisez l'une des options de **License Management (Gestion des licences)** pour activer la licence.*
URL AutoFocus	Saisissez l'URL AutoFocus : **`https://autofocus.paloaltonetworks.com:10443`**
Délai d'expiration de la requête (secondes)	Réglez la durée (en secondes) pendant laquelle le pare-feu peut tenter d'effectuer une requête auprès d'AutoFocus pour obtenir les données de renseignement sur la menace. Si le portail AutoFocus ne répond pas avant la fin de la période spécifiée, le pare-feu met fin à la connexion.

Cortex Data Lake

Utilisez cette section pour configurer les pare-feu VM-Series et matériels pour le transfert des journaux au Cortex Data Lake. Voici le flux de travail complet pour configurer les options décrites ci-dessous :

- Start Logging to Cortex Data Lake (without Panorama) (Commencer la journalisation dans Cortex Data Lake [sans Panorama])
- Start Logging to Cortex Data Lake (for Panorama-managed firewalls) (Commencer la journalisation dans Cortex Data Lake [pour les pare-feux gérés par Panorama])

Élément	Description
Le service de journalisation se nomme désormais Cortex Data Lake. Cependant, certaines fonctionnalités et certains boutons du pare-feu continuent d'afficher le nom Logging Service (service de journalisation).	
Activer Cortex Data Lake	Choisissez cette option pour permettre au pare-feu (ou, si vous utilisez Panorama, aux pare-feu appartenant au modèle sélectionné **) de transférer les journaux vers Cortex Data Lake (Cortex Data Lake s'appelait auparavant le service de journalisation).**Après avoir configuré le transfert de journal (objets > transfert dejournal), le pare-feu transfère les journaux directement à Cortex Data Lake, ce qui est vrai même pour les pare-feu gérés par Panorama.
Activer la journalisation double (pour les pare-feux gérés par Panorama uniquement)	**Enable Duplicate Logging (Activer la journalisation double)** pour continuer d'envoyer les journaux à Panorama et aux collecteurs de journaux distribués, en plus d'envoyer les journaux au Cortex Data Lake. Cette option est très utile lorsque vous évaluez Cortex Data Lake ; lorsque cette option est activée, les pare-feux qui appartiennent au modèle sélectionné enregistrent une copie des journaux auprès du Cortex Data Lake et de votre Panorama ou de l'architecture de collecte de journaux distribuée.
Activer la journalisation améliorée des applications	**Enable Enhanced Application Logging (Activez la journalisation améliorée des applications)** si vous voulez que le pare-feu recueille des données qui accroissent la visibilité des applications de Palo Alto Networks. Par exemple, cette visibilité accrue du réseau permet aux applications Palo Alto Networks Cortex XDR de mieux catégoriser et établir une base de référence pour l'activité réseau normale afin que le pare-feu puisse détecter un comportement inhabituel pouvant indiquer une attaque. La journalisation améliorée des applications nécessite une licence de service de journalisation (Cortex Data Lake). Vous ne pouvez afficher ces journaux ; ils sont conçus pour n'être utilisés que par les applications de Palo Alto Networks.
Région	Sélectionnez la région géographique de l'instance de Cortex Data Lake (service de journalisation) à laquelle le pare-feu transférera les journaux. Connectez-vous au Cortex hub (concentrateur Cortex) pour confirmer la région dans laquelle l'instance Cortex Data Lake est déployée (dans le concentrateur, sélectionnez l'engrenage des paramètres dans la barre de menu supérieure et **Manage Apps (gérer les applications)**.

Élément	Description
Compte de connexions à Cortex Data Lake pour les pare-feux des séries PA-7000 et PA-5200.	(Pare-feux PA-7000 Series et PA-5200 Series uniquement) Spécifiez le nombre de connexions pour envoyer des journaux depuis les pare-feux vers Cortex Data Lake (la plage est comprise entre 1 et 20 ; la valeur par défaut est 5). Vous pouvez utiliser la commande de la CLI **`request logging-service-forwarding status`** sur le pare-feu pour vérifier le nombre de connexions actives entre le pare-feu et Cortex Data Lake.
Embarqué sans Panorama (pour les pare-feu qui ne sont pas gérés par Panorama)	Vous pouvez permettre aux pare-feux qui ne sont pas gérés par Panorama d'envoyer des journaux à Cortex Data Lake. Pour ce faire, vous devez d'abord générer une clé dans l'application Cortex Data Lake. Cette clé permet au pare-feu de s'authentifier et de se connecter en toute sécurité à Cortex Data Lake. Après avoir généré la clé, saisissez-là et enable the firewall to start forwarding logs (autorisez le pare-feu à commencer à transférer les journaux) à Cortex Data Lake.
État du service de journalisation	Affichez l'état de la connexion à Cortex Data Lake. **Show Status (Montrer l'état)** pour afficher les détails des contrôles suivants : • **Licence** : `OK` ou `Error (Erreur)` pour indiquer si le pare-feu dispose d'une licence valide pour transférer les journaux au Cortex Data Lake. • **Certificat** : `OK` ou `Error (Erreur)` pour indiquer si le pare-feu a bien récupéré le certificat nécessaire pour s'authentifier auprès de Cortex Data Lake.. • **Info client** : `OK` ou `Erreur` pour indiquer si le pare-feu dispose du numéro d'identification du client nécessaire pour utiliser Cortex Data Lake. Lorsque l'état correspond à `OK`, vous pouvez également voir le numéro d'identification du client. • **Connectivité du périphérique** : indique si le pare-feu s'est bien connecté au Cortex Data Lake.
Paramètres des profils de gestion SSH	
Profil de serveur	Un type de profil de service SSH qui s'applique aux sessions SSH pour les connexions de gestion CLI sur votre réseau. Pour appliquer un profil de serveur existant, sélectionnez un profil, cliquez sur **OK**, et **Commit (validez)** votre modification. *Vous devez effectuer un redémarrage de service SSH depuis le CLI pour activer le profil.* Pour plus d'informations, consultez Device > Certificate Management >SSH Service Profile.

Élément	Description
Paramètres du service Edge PAN-OS	
Activer les verdicts d’appareils tiers	Cette option est réservée pour une version ultérieure. Si vous activez cette option, il n’y a aucune fonctionnalité.
État de la connexion	Affiche l’état (connecté ou déconnecté) de la connexion du pare-feu au service Edge.
Activer le service cloud de contexte utilisateur	Sélectionnez cette option pour connecter le pare-feu au service cloud User Context, ce qui vous permet d'utiliser Cloud Identity Engine pour afficher et gérer la redistribution d'informations telles que les mappages et les balises entre vos pare-feux et appareils.
État de la connexion	Affiche l’état (connecté ou déconnecté) de la connexion du pare-feu au service Edge.

Périphérique > Configuration > Opérations

Vous pouvez exécuter les tâches suivantes pour gérer les configurations candidate et active du pare-feu et de Panorama™. Si vous utilisez un appareil virtuel Panorama, vous pouvez également utiliser les paramètres de cette page pour configurer les Partitions de stockage de journaux pour un appareil virtuel Panorama en mode hérité.

Vous devez Valider les modifications *que vous apportez dans la configuration candidate pour activer ces changements, afin qu'ils fassent partie de la configuration en cours d'exécution. Comme pratique exemplaire, nous vous recommandons d'*Enregistrer les configurations candidates*, et ce, régulièrement.*

Vous pouvez utiliser les commandes SCP (Secure Copy) à partir de la CLI *pour exporter des fichiers de configuration, des journaux, des rapports ainsi que d'autres fichiers vers un serveur SCP et importer les fichiers vers un autre pare-feu ou vers un appareil Panorama M-Series ou vers un appareil virtuel. Cependant, parce que la base de données des journaux est trop grande pour l'exporter ou l'importer afin qu'elle puisse être utilisée, les modèles suivants ne prennent pas en charge l'exportation ou l'importation de la base de données des journaux en entier : Pare-feu PA-7000 Series (toutes les versions de PAN-OS®), appareils virtuels Panorama exécutant Panorama 6.0 ou versions ultérieures, et appareils Panorama M-Series (toutes les versions de Panorama).*

Fonction	Description
Gestion de la configuration	
Rétablir la dernière configuration enregistrée	Restaure l'instantané par défaut (.snapshot.xml) de la configuration candidate (l'instantané que vous créez ou que vous remplacez lorsque vous sélectionnez **Configuration** > **Enregistrer les modifications** dans le coin supérieur droit de l'interface Web). (Panorama uniquement) **Sélectionnez les groupes de périphériques et les modèles** pour sélectionner des configurations de groupes de périphériques, de modèles ou de piles de modèles spécifiques à annuler. Les administrateurs des groupes de périphériques et des modèles peuvent uniquement sélectionner les groupes de périphériques, les modèles ou les piles de modèles qui leur sont attribués dans le domaine d'accès qui leur est affecté.
Revenir à la configuration en cours d'exécution	Restaure la configuration active actuelle. Cette opération annule toutes les modifications apportées par chaque administrateur à la configuration candidate depuis la dernière validation. Pour annuler uniquement les changements d'administrateurs spécifiques, voir Annuler les changements. (Panorama uniquement) **Sélectionnez les groupes de périphériques et les modèles** pour sélectionner des configurations de groupes de périphériques, de modèles ou de piles de modèles spécifiques à annuler. Les administrateurs des groupes de périphériques et des modèles peuvent

Fonction	Description
	uniquement sélectionner les groupes de périphériques, les modèles ou les piles de modèles qui leur sont attribués dans le domaine d'accès qui leur est affecté.
Sauvegarder le cliché de la configuration nommée	Crée un instantané de la configuration candidate qui ne remplace pas l'instantané par défaut (.snapshot.xml). Saisissez un **Nom** pour l'instantané ou sélectionnez un instantané nommé existant à remplacer. (Panorama uniquement) **Sélectionnez les groupes de périphériques et les modèles** pour sélectionner des configurations de groupes de périphériques, de modèles ou de piles de modèles spécifiques à enregistrer. Les administrateurs des groupes de périphériques et des modèles peuvent uniquement sélectionner les groupes de périphériques, les modèles ou les piles de modèles qui leur sont attribués dans le domaine d'accès qui leur est affecté.
Sauvegarder la configuration candidate	Crée ou remplace l'instantané par défaut de la configuration candidate (.snapshot.xml) par la configuration candidate actuelle. Il s'agit de la même action que lorsque vous sélectionnez **Configuration** > **Enregistrer les modifications** dans le coin supérieur droit de l'interface Web. Pour sauvegarder uniquement les modifications d'administrateurs spécifiques, voir Enregistrer les configurations candidates. (Panorama uniquement) **Sélectionnez les groupes de périphériques et les modèles** pour sélectionner des configurations de groupes de périphériques, de modèles ou de piles de modèles spécifiques à enregistrer. Les administrateurs des groupes de périphériques et des modèles peuvent uniquement sélectionner les groupes de périphériques, les modèles ou les piles de modèles qui leur sont attribués dans le domaine d'accès qui leur est affecté.
Charger l'instantané de la configuration (pare-feu) OU Charger l'instantané de la configuration nommé Panorama	Remplace la configuration candidate actuelle par l'une des options suivantes : • Instantané au nom personnalisé de la configuration candidate (plutôt que l'instantané par défaut). • Configuration active au nom personnalisé que vous avez importé. • Configuration active actuelle. La configuration doit demeurer sur le pare-feu ou sur le Panorama sur lequel vous le chargez. Sélectionnez le **Nom** de la configuration et saisissez la **Clé de déchiffrement)** qui est la clé principale du pare-feu ou de Panorama (voir Périphérique > Clé principale et diagnostics). La clé principale est requise pour déchiffrer tous les mots de passe et les clés privées de la configuration. Si vous chargez une configuration importée, vous devez saisir la clé principale du pare-feu ou de Panorama à partir duquel vous réalisez l'importation. Une fois l'opération de chargement terminée, la clé

Fonction	Description
	principale du pare-feu ou de Panorama sur laquelle vous avez chargé la configuration rechiffre les mots de passe et les clés privées. Pour générer de nouveaux UUID pour toutes les règles de la configuration (par exemple, si vous chargez une configuration d'un autre pare-feu tout en souhaitant préserver les règles uniques lors du chargement de cette configuration), le super utilisateur doit **Régénérer les UUID de la règle pour la configuration nommée qui est sélectionnée** afin de générer de nouveaux UUID pour toutes les règles. (Panorama uniquement) Précisez les configurations d'objet, de politique, de groupe de périphériques ou de modèles pour charger partiellement les configurations à partir des configurations nommées en faisant votre sélection à partir de ce qui suit : • **Charger les objets partagés** : Chargez uniquement les objets partagés ainsi que toutes les configurations des groupes de périphériques et des modèles. • **Charger les politiques partagées** : Chargez uniquement les politiques partagées ainsi que toutes les configurations des groupes de périphériques et des modèles. • **Sélectionnez les groupes de périphériques et les modèles** : Sélectionnez les configurations de groupes de périphériques, de modèles ou de piles de modèles à charger. Les administrateurs des groupes de périphériques et des modèles peuvent uniquement sélectionner les groupes de périphériques, les modèles ou les piles de modèles qui leur sont attribués dans le domaine d'accès qui leur est affecté. • **Préserver les UUID de la règle** : Conservez les UUID de la configuration active.
Charger la version de la configuration (pare-feu) OU Charger la version de la configuration Panorama	Remplace la configuration candidate actuelle par une version précédente de la configuration en cours d'exécution qui est stockée sur le pare-feu ou sur Panorama. Sélectionnez le **Nom** de la configuration et saisissez la **Clé de déchiffrement** qui est la clé principale du pare-feu ou de Panorama (voir Périphérique > Clé principale et diagnostics). La clé principale est requise pour déchiffrer tous les mots de passe et les clés privées de la configuration. Une fois l'opération de chargement terminée, la clé principale rechiffre les mots de passe et les clés privées. (Panorama uniquement) Précisez les configurations d'objet, de politique, de groupe de périphériques ou de modèles pour charger partiellement les configurations à partir des configurations nommées en faisant votre sélection : • **Charger les objets partagés** : Chargez uniquement les objets partagés ainsi que toutes les configurations des groupes de périphériques et des modèles.

Fonction	Description
	• **Charger les politiques partagées** : Chargez uniquement les politiques partagées ainsi que toutes les configurations des groupes de périphériques et des modèles. • **Sélectionnez les groupes de périphériques et les modèles** : Sélectionnez les configurations de groupes de périphériques, de modèles ou de piles de modèles à charger. Les administrateurs des groupes de périphériques et des modèles peuvent uniquement sélectionner les groupes de périphériques, les modèles ou les piles de modèles qui leur sont attribués dans le domaine d'accès qui leur est affecté.
Exporter l'instantané de la configuration	Exporte la configuration active actuelle, un instantané de la configuration candidate ou une configuration précédemment importée (candidate ou active). Le pare-feu exporte la configuration sous la forme d'un fichier XML avec le nom spécifié. Vous pouvez enregistrer l'instantané dans n'importe quel emplacement réseau. (Panorama uniquement) **Sélectionnez les groupes de périphériques et les modèles** pour sélectionner des configurations de groupes de périphériques, de modèles ou de piles de modèles spécifiques à exporter. Les administrateurs des groupes de périphériques et des modèles peuvent uniquement sélectionner les groupes de périphériques, les modèles ou les piles de modèles qui leur sont attribués dans le domaine d'accès qui leur est affecté.
Exporter la version de la configuration	Exporte une **Version** de la configuration active sous la forme d'un fichier XML. (Panorama uniquement) **Sélectionnez les groupes de périphériques et les modèles** pour sélectionner des configurations de groupes de périphériques, de modèles ou de piles de modèles spécifiques à exporter. Les administrateurs des groupes de périphériques et des modèles peuvent uniquement sélectionner les groupes de périphériques, les modèles ou les piles de modèles qui leur sont attribués dans le domaine d'accès qui leur est affecté.
Exporter la solution de configuration des périphériques et de Panorama (Panorama uniquement)	Génère et exporte les dernières versions de la configuration de secours en cours d'exécution de Panorama et de chaque pare-feu géré. Pour automatiser le processus de création et exporter la solution de configuration quotidienne vers un serveur SCP ou FTP, voir Panorama > Exportation de config planifiée.
Exporter ou appliquer la solution de configuration des périphériques (Panorama uniquement)	Vous invite à sélectionner un pare-feu et à effectuer l'une des actions suivantes sur la configuration de pare-feu stockée sur Panorama : • **Appliquez et validez** la configuration sur le pare-feu. Cette action nettoie le pare-feu (supprime toute configuration locale de celui-ci) et applique la configuration de pare-feu stockée sur Panorama. Après

Fonction	Description
	l'importation d'une configuration de pare-feu, utilisez cette option pour nettoyer le pare-feu pour pouvoir le gérer à l'aide de Panorama. • **Exportez** la configuration vers le pare-feu sans la charger. Pour charger la configuration, vous devez accéder à la CLI du pare-feu et exécuter la commande de mode de configuration **load device-state**. Cette commande nettoie le pare-feu comme l'option **Push & Commit (Appliquer & valider)**. • **Use FW Master Key (Utilisez la clé principale FW)** pour chiffrer l'ensemble de configuration de périphérique exporté avec la clé principale déployée sur le pare-feu géré. Saisissez la **FW Master Key (clé principale FW)**, puis **Confirm FW Master Key (confirmez la clé principale FW)**.
Exporter l'état du périphérique (Pare-feu uniquement)	Exporte les informations relatives à l'état du pare-feu sous la forme d'un module. En plus de la configuration active, les informations relatives à l'état comprennent le groupe de périphériques et les paramètres du modèle poussés par Panorama. Si le pare-feu est un portail GlobalProtect™, le module comprend également des informations relatives au certificat, une liste des satellites que le portail gère et les informations d'authentification des satellites. Si vous remplacez un pare-feu ou un portail, vous pouvez restaurer les informations exportées relatives au remplacement en important le module d'état. *Vous pouvez exécuter manuellement l'exportation de l'état du pare-feu ou créer un script d'API XML planifié afin d'exporter le fichier sur un serveur distant. Cette tâche doit être régulièrement exécutée puisque les certificats des satellites font fréquemment l'objet de modifications.* Pour créer le fichier d'état du pare-feu à partir de la CLI, en mode de configuration, exécutez la commande **`save device state`**. Le nom du fichier sera `device_state_cfg.tgz` et il sera stocké dans `/opt/pancfg/mgmt/device-state`. La commande opérationnelle pour exporter le fichier d'état du pare-feu est **`scp export device-state`** (vous pouvez aussi utiliser **`tftp export device-state`**). Pour plus d'informations sur l'utilisation de l'API XML ou REST, consultez la section Guide de l'API de Panorama et de PAN-OS .
Importer l'instantané de la configuration	Importe une configuration active ou candidate à partir d'un emplacement réseau. Cliquez sur **Parcourir** et sélectionnez le fichier de configuration à importer.
Importer l'état du périphérique (Pare-feu uniquement)	Permet d'importer le module d'informations relatives à l'état que vous avez exporté d'un pare-feu lorsque vous avez décidé de **Exporter l'état du périphérique**. Outre la configuration active, les informations relatives à l'état comprennent le groupe de périphériques et les paramètres du

Fonction	Description
	modèle poussés par Panorama. Si le pare-feu est un portail GlobalProtect, le module comprend également des informations relatives au certificat, une liste des satellites et les informations d'authentification des satellites. Si vous remplacez un pare-feu ou un portail, vous pouvez restaurer les informations relatives au remplacement en important le module d'état.
Importer la configuration de périphérique vers Panorama (Panorama uniquement)	Permet d'importer une configuration de pare-feu vers Panorama. Panorama crée automatiquement un modèle contenant les configurations réseau et de périphérique. Pour chaque système virtuel (vsys) sur le pare-feu, Panorama crée automatiquement un groupe de périphériques qui contiendra les configurations de politique et d'objet. Les groupes de périphériques se situeront un niveau en dessous de l'emplacement Partagé dans la hiérarchie, même si vous pouvez les réaffecter à un autre groupe de périphériques parent une fois l'importation terminée (voir Panorama > VMware NSX). *Les versions de contenu sur Panorama (la base de données d'applications et de menaces par exemple) doivent être supérieures ou égales aux versions sur le pare-feu duquel vous importerez une configuration.* Configurez les options d'importation suivantes : • **Périphérique** : sélectionnez le pare-feu duquel Panorama importera les configurations. Le menu déroulant comprend uniquement les pare-feu connectés à Panorama et non affectés à un autre groupe de périphériques ou modèle. Vous pouvez ne sélectionner qu'un pare-feu dans son ensemble, et non un système virtuel individuel. • **Use FW Master Key (Utiliser la clé principale FW)** : activez cette option pour déchiffrer la configuration de pare-feu importée à l'aide de la clé principale déployée sur le pare-feu géré. Saisissez la **FW Master Key (clé principale FW)**, puis **Confirm FW Master Key (confirmez la clé principale FW)**. Si vous déchiffrez la configuration importée de plusieurs pare-feu, les pare-feu doivent tous utiliser la même clé principale. • **Nom du modèle** : donnez un nom au modèle qui contiendra les paramètres de périphérique et réseau importés. Pour un pare-feu à plusieurs systèmes virtuels, ce champ est vide. Pour les autres pare-feu, la valeur par défaut est le nom du pare-feu. Vous ne pouvez pas utiliser le nom d'un modèle existant. • **Préfixe de nom du groupe de périphériques** (pare-feu à plusieurs systèmes virtuels uniquement) : facultativement, ajoutez une chaîne de caractères comme préfixe pour chaque nom de groupe de périphériques. • **Nom du groupe de périphériques** : pour un pare-feu à plusieurs systèmes virtuels, chaque groupe de périphérique comporte un nom de système virtuel par défaut. Pour les autres pare-feu, la valeur par défaut est le nom du pare-feu. Vous pouvez modifier les noms par défaut,

Fonction	Description
	mais vous ne pouvez pas utiliser le nom d'un groupe de périphériques existant. • **Importer les objets partagés des périphériques vers le contexte partagé de Panorama** (activé par défaut) – Panorama importe des objets appartenant à Partagé sur le pare-feu vers Partagé sur Panorama.  *Panorama prend en considération tous les objets partagés sur un pare-feu sans avoir besoin de plusieurs systèmes virtuels. Si vous désactivez cette option, Panorama copie les objets de pare-feu partagés dans des groupes de périphériques au lieu de Partagé. Ce paramètre inclut les exceptions suivantes :* • Si un objet de pare-feu partagé a le même nom et la même valeur qu'un objet Panorama partagé existant, l'importation exclut cet objet pare-feu. • Si le nom ou la valeur de l'objet de pare-feu partagé est différent de l'objet Panorama partagé, Panorama importe l'objet de pare-feu dans chaque groupe de périphériques. • Si une configuration importée dans un modèle fait référence à un objet de pare-feu partagé, Panorama importe cet objet dans Partagé que vous sélectionniez l'option ou non. • Si un objet de pare-feu partagé fait référence à une configuration importée dans un modèle, Panorama importe l'objet dans un groupe de périphériques que vous sélectionniez l'option ou non. • **Emplacement d'importation de règle** : sélectionnez si Panorama importera les politiques en tant que pré ou post-règles. Quel que soit votre choix, Panorama importe les règles de sécurité par défaut (défaut intrazone et interzone) dans la post-règle de base.  *Si Panorama comporte une règle portant le même nom qu'une règle de pare-feu que vous importez, Panorama affiche les deux règles. Les noms de règles doivent toutefois être uniques : supprimez une des règles avant de valider sur Panorama, sinon la validation échouera.*
Opérations périphérique	
Redémarrer	Pour redémarrer le pare-feu ou Panorama, **Redémarrez le périphérique**. Le pare-feu ou Panorama vous déconnecte, recharge le logiciel (PAN-OS ou Panorama) et la configuration active, ferme et consigne les sessions existantes, et crée une entrée de journal système pour noter le nom de l'administrateur à l'origine de l'arrêt. Toutes les modifications apportées à la configuration et non enregistrées ou validées sont perdues (voir Périphérique > Configuration > Opérations).

Fonction	Description
	Si l'interface Web n'est pas disponible, utilisez la commande opérationnelle de la CLI suivante : **`request restart system`**
Arrêter	Pour procéder à un arrêt progressif du pare-feu ou de Panorama, **Arrêtez le périphérique** ou **Arrêtez Panorama**, puis cliquez sur **Oui** lorsque vous êtes invité à le faire. Toutes les modifications apportées à la configuration et non enregistrées ou validées sont perdues. Tous les administrateurs sont déconnectés et le processus suivant se produit: • Toutes les sessions de connexion sont fermées. • Les interfaces sont désactivées. • Tous les processus du système sont arrêtés. • Les sessions en cours sont fermées et consignées. • Des journaux système indiquant le nom de l'administrateur à l'origine de l'arrêt sont créés. Si cette entrée du journal ne peut pas être écrite, un avertissement s'affiche et le système n'est pas arrêté. • Les lecteurs de disques sont démontés de manière appropriée et le pare-feu ou Panorama est mis hors tension. Vous devez débrancher la source d'alimentation puis la rebrancher avant de remettre le pare-feu ou Panorama sous tension. *Si l'interface Web n'est pas disponible, utilisez la commande de la CLI :* **`request shutdown system`**
Redémarrer le panneau de données	**Redémarrez le panneau de données** pour relancer les fonctions de données du pare-feu sans redémarrer. Cette option n'est pas disponible sur les pare-feu Panorama ou PA-220, PA-800 ou VM.T. *Si l'interface Web n'est pas disponible, utilisez la commande CLI suivante :* ***`request restart dataplane`*** Sur un pare-feu de la série PA-7000, chaque PNJ dispose d'un plan de données afin que vous puissiez redémarrer le PNJ pour effectuer cette opération en exécutant l'emplacement **`de redémarrage du châssis de demande de commande`**.
Divers	
Personnaliser les logos	Utilisez **Personnaliser les logos** pour personnaliser les éléments suivants :

Fonction	Description
	• Image de l’arrière-plan du **Écran de connexion** • Image de l’en-tête de la **interface utilisateur principale** (interface Web) • Image de la **Page de titre du rapport PDF**. Voir Surveillance > Rapports PDF > Gérer le récapitulatif PDF. • Image du **Pied de page du rapport PDF**.  Chargez (<image>) un fichier image  pour la prévisualiser ou pour supprimer () une image précédemment chargée. Pour rétablir le logo par défaut, supprimez votre entrée et **Validez**. Pour le **Écran de connexion** et la **Interface utilisateur principale**, vous pouvez afficher () l’image comme elle apparaîtra ; au besoin, le pare-feu recadre l’image aux dimensions de la page. Pour les rapports PDF, le pare-feu redimensionne automatiquement les images pour qu’elles correspondent aux dimensions de la page sans rognage. Dans tous les cas de figure, l’aperçu présente les dimensions recommandées pour l’image. La taille maximale d’image d’un logo est de 128 Ko. Les types de fichiers pris en charge sont png et jpg. Le pare-feu ne prend pas en charge les fichiers d'image qui sont entrelacés, les images qui contiennent des canaux alpha et les types de fichier gif car ces fichiers interfèrent avec la génération de rapports PDF. Il se peut que vous deviez contacter l’illustrateur qui a créé l’image pour en supprimer les canaux alpha, ou vous assurer que le grapheur utilisé n’enregistre pas les fichiers avec la fonction de canal alpha. Pour plus d’informations sur la génération de rapports PDF, voir Surveillance > Rapports PDF > Gérer le résumé PDF.
Réglage SNMP	Activation de la surveillance SNMP.
Configuration de la partition de stockage (uniquement sur Panorama)	Partitions de stockage des journaux pour un appareil virtuel Panorama en mode hérité.

Activation de la surveillance SNMP

- Périphérique > Configuration > Opérations

SNMP (Simple Network Management Protocol) est un protocole standard permettant la surveillance des périphériques sur votre réseau. Sélectionnez **Operations (Opérations)** pour configurer le pare-feu afin qu'il utilise la version SNMP prise en charge par votre gestionnaire SNMP (SNMPv2c ou SNMPv3). Pour obtenir la liste des MIB que vous devez charger dans le gestionnaire SNMP afin qu'il puisse interpréter les statistiques qu'il collecte sur le pare-feu, reportez-vous à MIB prises en charge. Pour configurer le profil de serveur permettant au pare-feu de communiquer avec les destinations de pièges SNMP sur votre réseau, reportez-vous à la section Périphérique > Profils de serveur > Piège SNMP. Les MIB SNMP définissent tous les objets SNMP et événements générés par le pare-feu. Un piège SNMP identifie un événement par un ID d'objet (OID) unique et chaque champ est défini comme liste de liaisons de variables. Cliquez sur **Configuration SNMP** et définissez les paramètres suivants pour autoriser les requêtes SNMP GET de votre gestionnaire SNMP :

Champ	Description
Emplacement physique	Indiquez l'emplacement physique du pare-feu. Lorsqu'un journal ou un piège est généré, ces informations vous permettent d'identifier (dans un gestionnaire SNMP) le pare-feu qui a généré la notification.
Contact	Saisissez le nom ou l'adresse de courrier électronique de la personne en charge de la gestion du pare-feu. Ce paramètre est rapporté dans le MIB d'informations du système standard.
Utiliser les définitions des pièges spécifiques	Cette option est sélectionnée par défaut, ce qui signifie que le pare-feu utilise un OID unique pour chaque piège SNMP en fonction du type d'événement. Si vous désélectionnez cette option, tous les pièges porteront le même OID.
Version	Sélectionnez la version de SNMP : **V2c** (par défaut) ou **V3**. Votre sélection détermine les autres champs affichés dans la boîte de dialogue.
Pour SNMP V2c	
Chaîne de communauté SNMP	Saisissez la chaîne de communauté qui identifie une *communauté* SNMP de gestionnaires SNMP et de périphériques surveillés, et qui sert également de mot de passe pour authentifier les membres de la communauté entre eux lorsqu'ils échangent des messages SNMP get (requêtes de statistiques) et de pièges. La chaîne peut comporter 127 caractères maximum, accepte tous les caractères et est sensible à la casse. *Il convient de ne pas utiliser la chaîne de communauté **publique** définie par défaut. Les messages SNMP contenant des chaînes de communautés en clair, tenez compte des exigences de sécurité de votre réseau lors de la définition de l'appartenance à la communauté (accès administrateur).*
Pour SNMP V3	
Nom / Vue	Vous pouvez affecter un groupe d'une ou plusieurs vues à l'utilisateur d'un gestionnaire SNMP afin de contrôler les objets MIB (statistiques) que

Champ	Description
	l'utilisateur peut obtenir du pare-feu. Chaque vue est constituée d'une paire OID/masque de niveau bit : l'OID définit un MIB et le masque (au format hexadécimal) définit les objets qui sont accessibles à l'intérieur (inclure correspondance) ou à l'extérieur (exclure correspondance) de ce MIB. Par exemple, si l'**OID** est 1.3.6.1, que l'**Option** de correspondance est définie sur **inclure** et le **Masque** est 0xf0, les OID des objets demandés par l'utilisateur doivent correspondre aux quatre premiers nœuds (f = 1111) de 1.3.6.1. Les objets ne doivent pas nécessairement correspondre aux nœuds restants. Dans cet exemple, 1.3.6.1.2 correspond au masque et 1.4.6.1.2 n'y correspond pas. Pour chaque groupe de vues, cliquez sur **Add (Ajouter)**, donnez un **Name (Nom)** au groupe, puis configurez les paramètres suivants pour chaque vue que vous **Add (Ajouter)** au groupe : • **View (Vue)** : donnez un nom à la vue. Ce nom peut comporter jusqu'à 31 caractères, à savoir des caractères alphanumériques, des points, des traits de soulignement ou des traits d'union. • **OID** : indiquez l'OID du MIB. • **Option** : sélectionnez la logique de correspondance à appliquer au MIB. • **Mask (Masque)** : indiquez le masque au format hexadécimal. *Pour pouvoir accéder à toutes les informations de gestion, utilisez l'**OID** de niveau supérieur 1.3.6.1, et définissez le **Mask (Masque)** sur 0xf0 et l'**Option** de correspondance sur **include (inclure)**.*
Users (Utilisateurs)	Les comptes utilisateur SNMP fournissent l'authentification, la confidentialité et le contrôle d'accès lorsque des pare-feu transfèrent des pièges et que des gestionnaires SNMP obtiennent des statistiques de pare-feu. Pour chaque utilisateur, cliquez sur **Add (Ajouter)** et configurez les paramètres suivants : • **Users (Utilisateurs)** : indiquez un nom d'utilisateur pour identifier le compte utilisateur SNMP. Le nom d'utilisateur que vous configurez sur le pare-feu doit correspondre au nom d'utilisateur configuré sur le gestionnaire SNMP. Le nom d'utilisateur peut comporter 31 caractères maximum. • **View (Vue)** : affectez un groupe de vues à l'utilisateur. • **Auth Password (Mot de passe d'authentification)** : indiquez le mot de passe d'authentification de l'utilisateur. Le pare-feu utilise le mot de passe pour s'authentifier auprès du gestionnaire SNMP lors du transfert de pièges et de la réponse à des requêtes de statistiques. Le mot de passe doit comporter entre 8 et 256 caractères et tous les caractères sont autorisés. • **Priv Password (Mot de passe privé)** : indiquez le mot de passe privé de l'utilisateur. Le mot de passe doit comporter entre 8 et 256 caractères et tous les caractères sont autorisés.

Champ	Description
	• **Authentication Protocol (Protocole d’authentification) :**le pare-feu utilise l’algorithme sha (Secure Hash Algorithm) pour hacher le mot de passe. • **SHA-1**, **SHA-224**, **SHA-256**, **SHA-384**, **SHA-512** • **Privacy Protocol (protocole de confidentialité) :**Le pare-feu utilise le mot de passe et la norme Advanced Encryption Standard (AES) pour crypter les pièges SNMP et les réponses aux requêtes de statistiques. • **AES-128**, **AES-192**, **AES-256**

Périphérique > Configuration > Module de sécurité matériel

Sélectionnez **Périphérique** > **Configuration** > **HSM** module de sécurité matériel ; HSM), pour effectuer des opérations et pour afficher le statut du HSM.

Que voulez-vous faire ?	Reportez-vous à la section :
Quel est le but d'un module de sécurité matériel (HSM) et où puis-je trouver des procédures de configuration détaillées ?	Sécurisation des clés avec un module de sécurité matériel (HSM)
Configurer :	Paramètres du fournisseur du module matériel de sécurité
	Authentication HSM
Effectuer des opérations matérielles de sécurité	Opérations matérielles de sécurité
Comment puis-je afficher le statut du HSM ?	Configuration et état du fournisseur du module matériel de sécurité matériel
	Statut du module matériel de sécurité

Paramètres du fournisseur du module matériel de sécurité

Pour configurer un module de sécurité matériel sur le pare-feu, modifiez les paramètres du module de sécurité matériel.

Paramètres du fournisseur du module matériel de sécurité	Description
Fournisseur configuré	Sélectionnez le fournisseur HSM : • **None (Aucun)** (par défaut) : le pare-feu ne se connecte à aucun module de sécurité matériel. • **HSM Réseau SafeNet** • **nCipher nShield Connect** *La version du serveur HSM doit être compatible avec la* version du client HSM *installée sur le pare-feu.*

Paramètres du fournisseur du module matériel de sécurité	Description
Nom du module	Ajoutez un nom au module de sécurité matériel. Il peut s'agir de n'importe quelle chaîne'A0;ASCII de 31caractères maximum. Ajoutez un maximum de 16 noms de module si vous configurez des modules de sécurité matériels SafeNet haute disponibilité ou indépendants.
Adresse du serveur	Indiquez une adresse IPv4 pour chaque module de sécurité matériel configuré.
Haute disponibilité (Réseau SafeNet uniquement)	(Facultatif) Sélectionnez cette option si vous définissez des modules de sécurité matériels SafeNet dans une configuration haute disponibilité. Vous devez configurer le nom du module et l'adresse du serveur de chaque module de sécurité matériel.
Tentative de rétablissement automatique (Réseau SafeNet uniquement)	Indiquez le nombre de fois que le pare-feu tente de rétablir la connexion à un module de sécurité matériel avant de basculer vers un autre dans une configuration de module de sécurité matériel haute disponibilité (plage de 0 à 500 ; valeur par défaut de 0).
Nom du groupe de haute disponibilité (Réseau SafeNet uniquement)	Donnez un nom au groupe de modules de sécurité matériels haute disponibilité. Ce nom est utilisé en interne par le pare-feu. Il peut s'agir de n'importe quelle chaîne'A0;ASCII de 31caractères maximum.
Supprimer l’adresse du système de fichiers (nCipher nShield Connect uniquement)	Configurez l'adresse IPv4 du système de fichiers distant utilisé dans la configuration du module de sécurité matériel nShield Connect.

Authentication HSM

Sélectionnez **Setup Hardware Security Module (Paramétrer le module de sécurité matériel)** et configurez les paramètres suivants pour authentifier le pare-feu sur le module de sécurité matériel.

Authentification du module HSM	
Nom du serveur	Sélectionnez un nom de serveur HSM dans le menu déroulant puis sélectionnez si vous voulez authentifier et définir la fiabilité à l’aide de certificats générés automatiquement ou manuellement. • **Automatiquement**

Authentification du module HSM	
	• **Manuellement** Si vous sélectionnez **Manual (Manuellement)**, vous devez importer et installer le certificat du serveur HSM généré manuellement. Exportez le certificat client HSM pour l'installer sur le serveur HSM.
Mot de passe de l'administrateur	Saisissez le mot de passe administrateur du module de sécurité matériel pour authentifier le pare-feu sur le module de sécurité matériel.

Opérations matérielles de sécurité

Pour effectuer une opération sur le module de sécurité matériel (HSM) ou le pare-feu connecté au HSM, sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **HSM (Module de sécurité matériel)**, puis sélectionnez l'une des opérations de matérielles de sécurité suivantes :

Opérations matérielles de sécurité	
Configurer le module matériel de sécurité	Configure le pare-feu pour qu'il s'authentifie auprès d'un HSM.
Afficher les informations détaillées	Affiche des informations sur les serveurs HSM, sur l'état de la haute disponibilité HSM et sur le matériel HSM.
Synchroniser avec le système de fichiers distants (nCipher nShield Connect uniquement)	Synchronise les données de clés provenant du système de fichiers distants de nShield Connect avec le pare-feu.
Réinitialiser la configuration	Supprime toutes les connexions HSM au pare-feu. Vous devez répéter toutes la procédures d'authentification avant de réinitialiser la configuration HSM.
Sélectionner la version du client HSM (Réseau SafeNet uniquement))	Vous permet de choisir la version du logiciel qui s'exécute sur le client HSM (le pare-feu). La version du client HSM doit être compatible avec la version du serveur HSM. Reportez-vous à la documentation du fournisseur HSM pour une matrice de compatibilité de la version client/serveur.

Configuration et état du fournisseur du module matériel de sécurité matériel

La section Fournisseur du module de matériel de sécurité vous permet de visualiser les paramètres de configuration HSM et l'état de connectivité du HSM.

Statut du fournisseur du module matériel de sécurité	
Fournisseur configuré	Sélectionnez le fournisseur HSM configuré sur le pare-feu : • **None** • **HSM Réseau SafeNet** • **nCipher nShield Connect**
Haute disponibilité	(Réseau SafeNet uniquement) La haute disponibilité du module de sécurité matériel est configurée.
Nom du groupe de haute disponibilité	(Réseau SafeNet uniquement) Nom du groupe configuré sur le pare-feu pour la haute disponibilité du module de sécurité matériel.
Adresse du système de fichiers distant	(nShield Connect uniquement) L'adresse du système de fichiers distant.
Adresse source du pare-feu	Adresse du port utilisé pour le module de sécurité matériel. Il s'agit par défaut de l'adresse du port de gestion. Toutefois, une autre adresse de port peut être spécifiée dans la fenêtre Services Route Configuration (Configuration de l'itinéraire de service) en sélectionnant **Device (Périphérique)** > **Setup (Configuration)** > **Services**.
Version client HSM sur pare-feu	Affiche la Version client HSM installée
Clé principale sécurisée par HSM	Cochez cette case pour sécuriser la clé principale par le module de sécurité matériel.
Status (État)	S'affiche en vert si le pare-feu est connecté et authentifié au HSM et s'affiche en rouge si le pare-feu n'est pas authentifié ou si la connectivité réseau vers le HSM est désactivée. Vous pouvez également voir l'État du module du matériel de sécurité pour plus de détails sur la connexion HSM.

Statut du module matériel de sécurité

L'État du module de sécurité matériel comprend les informations suivantes sur les modules de sécurité matériels qui ont été authentifiés avec succès. L'affichage diffère en fonction du fournisseur de modules de sécurité matériels configuré (SafeNet ou nCipher).

Statut du module matériel de sécurité	
HSM Réseau SafeNet	• **Numéro de série** – Le numéro de série de la partition du module de sécurité matériel s'affiche si celle-ci a été authentifiée avec succès.

Statut du module matériel de sécurité	
	• **Partition** – Le nom de la partition du module de sécurité matériel qui a été affectée sur le pare-feu. • **État du module** – L'état de fonctionnement actuel du module de sécurité matériel. Le champ affiche **Authentifié** si le HSM s'affiche dans ce tableau.
nCipher nShield Connect HSM	• **Nom** – Le nom du Serveur du HSM. • **Adresse IP** – L'adresse IP du HSM qui a été affecté sur le pare-feu. • **État du module** – L'état de fonctionnement actuel du module de sécurité matériel. Ce paramètre affiche **Authentifié** si le pare-feu a été authentifié avec succès au HSM et affiche **Non authentifié** si l'authentification a échoué.

Périphérique > Configuration > Services

Les rubriques suivantes décrivent les paramètres des services de système globaux et virtuels sur le pare-feu :

- configuration des services pour les systèmes globaux et virtuels ;
- Paramètres des services globaux
- Prise en charge des protocoles IPv4 et IPv6 pour la configuration de l’itinéraire de service
- Route pour le service de destination

configuration des services pour les systèmes globaux et virtuels ;

Sur un pare-feu sur lequel plusieurs systèmes virtuels sont activés, sélectionnez **Services** pour afficher les onglets **Global** et **Systèmes virtuels** sur lesquels vous définissez des services utilisés respectivement par le pare-feu ou ses systèmes virtuels pour fonctionner efficacement. (Si le pare-feu comporte un seul système virtuel ou si plusieurs systèmes virtuels sont désactivés, l’onglet **Systèmes virtuels** ne s’affiche pas.)

Sélectionnez **Global** pour définir des services pour l'ensemble du pare-feu. Ces paramètres sont également utilisés comme valeurs par défaut pour les systèmes virtuels pour lesquels aucun paramètre personnalisé n'est défini pour un service.

- Modifiez **Services** pour définir les adresses IP de destination des serveurs DNS, du Serveur de mises à jour et du Serveur proxy. L'onglet **NTP** vous permet de configurer les paramètres NTP (Network Time Protocol). Pour obtenir une description des options Services disponibles, reportez-vous à la section Table 12.
- Dans **Fonctions de service**, cliquez sur **Configuration de l'itinéraire de service** pour définir comment le pare-feu communiquera avec les autres serveurs/périphériques pour des services tels que DNS, messagerie, LDAP, RADIUS, Syslog, et bien d'autres encore. Deux méthodes de configuration des itinéraires de service sont possibles :
  - L'option **Utiliser l'interface de gestion pour tous** force toutes les communications de services du pare-feu avec des serveurs externes via l'interface de gestion (MGT). Si vous sélectionnez cette option, vous devez configurer l'interface MGT pour qu'elle autorise les communications entre le pare-feu et les serveurs/périphériques qui proposent des services. Pour configurer l’interface MGT, sélectionnez Périphérique > Configuration > Gestion et modifiez les paramètres.
  - L'option **Personnaliser** vous permet de contrôler de manière granulaire la communication du service en configurant une interface source spécifique et une adresse IP utilisées par le service comme interface de destination et adresse IP de destination dans sa réponse. (Par exemple, vous pouvez configurer une adresse IP / interface source spécifique pour la messagerie entre le pare-feu et un serveur de messagerie et utiliser une autre adresse IP / interface source pour les Services Palo Alto.) Sélectionnez le ou les services que vous souhaitez personnaliser sur les mêmes paramètres, puis cliquez sur **Définir les itinéraires de service sélectionnés**. Les services sont répertoriés dans la Table 13, qui indique si un service peut être configuré pour le pare-feu **Global** ou des **Systèmes virtuels** et si le service prend en charge une adresse source IPv4 et/ou IPv6.

L'onglet **Destination** est une autre fonction d'itinéraire de service Global que vous pouvez personnaliser. Cet onglet s’affiche dans la fenêtre Configuration de l’itinéraire de service et est décrit dans la section Itinéraire de service de destination.

Utilisez l'onglet **Systèmes virtuels** pour définir les itinéraires de service d'un système virtuel unique. Sélectionnez un Emplacement (système virtuel), puis cliquez sur **Configuration de l'itinéraire de service)**. Sélectionnez **Hériter de la configuration d'itinéraire de service global** ou **Personnaliser** des itinéraires de service pour un système virtuel. Si vous choisissez de personnaliser des paramètres, sélectionnez **IPv4** ou **IPv6**. Sélectionnez le ou les services que vous souhaitez personnaliser sur les mêmes paramètres, puis cliquez sur **Définir les itinéraires de service sélectionnés**. Reportez-vous à la Table 13 pour les services pouvant être personnalisés.

Pour contrôler et rediriger des requêtes DNS entre des systèmes virtuels partagés et spécifiques, vous pouvez utiliser un proxy DNS et un profil de Serveur DNS.

Paramètres des services globaux

- Périphérique > Configuration > Services

Pour contrôler et rediriger des requêtes DNS entre des systèmes virtuels partagés et spécifiques, vous pouvez utiliser un proxy DNS et un profil de Serveur DNS.

Paramètres des services globaux	Description
Services	
Serveur de mises à jour	Correspond à l'adresse IP ou au nom d'hôte du serveur à partir duquel télécharger les mises à jour de Palo Alto Networks. La valeur actuelle est **updates.paloaltonetworks.com**. Ne modifiez ce paramètre que si le support technique vous demande de le faire.
Vérifier l'identité du serveur de mises à jour	Si vous activez cette option, le pare-feu ou Panorama vérifie que le serveur sur lequel est téléchargé le module logiciel ou de contenu dispose d'un certificat SSL signé par une autorité de confiance. Cette option ajoute un niveau de sécurité supplémentaire à la communication entre les pare-feu ou les serveurs Panorama et le serveur de mises à jour. *Vérifiez l'identité du serveur de mise à jour afin de valider que le serveur dispose d'un certificat SSL signé par une autorité de confiance.*
Paramètres DNS	Choisissez le type de service DNS (**Servers (Serveurs)** ou **DNS Proxy Object (Objet de proxy DNS)**) pour toutes les requêtes DNS provenant du pare-feu afin de prendre en charge des objets d'adresse FQDN, la journalisation et la gestion du pare-feu. Les options disponibles sont les suivantes'A0;: • Serveurs DNS principal et secondaire pour permettre la résolution du nom de domaine. • Un proxy DNS configuré sur le pare-feu constitue une autre méthode de configuration des serveurs DNS. Si vous activez un proxy DNS, vous devez activer **Cache** et **EDNS Cache Responses (Réponses EDNS Cache)** (**Network (Réseau)** > **DNS Proxy (Proxy DNS)** > **Advanced (Avancé)**).

Paramètres des services globaux	Description
Serveur DNS principal	Saisissez l'adresse IP du serveur DNS principal à utiliser pour la résolution des requêtes DNS provenant du pare-feu. Par exemple, pour trouver le serveur de mise à jour, pour résoudre des entrées DNS dans des journaux ou pour résoudre des objets d'adresse FQDN.
Serveur DNS secondaire	(Facultatif) Saisissez l'adresse IP d'un serveur DNS secondaire à utiliser si le serveur principal n'est pas disponible.
Fréquence d'actualisation minimale du FQDN (sec)	Définissez une limite quant à la vitesse d'actualisation par le pare-feu des FQDN qu'il reçoit d'un DNS. Le pare-feu actualise un FQDN en fonction de la TTL du FQDN tant que la TTL est supérieure ou égale à ce **Minimum FQDN Refresh Time (Fréquence d'actualisation minimale du FQDN)** (en secondes). Si la TTL est inférieure à cette fréquence d'actualisation minimale du FQDN, le pare-feu actualise le FQDN en fonction de la fréquence d'actualisation minimale du FQDN (c'est-à-dire que le pare-feu ne respecte pas les TTL qui sont plus rapides que ce paramètre). La minuterie commence lorsque le pare-feu reçoit une réponse DNS d'un serveur DNS ou d'un objet de proxy DNS pour résoudre le FQDN (plage comprise entre 0 et 14 400 ; la valeur par défaut est 30). Si le paramètre est défini sur 0, le pare-feu actualisera le FQDN en fonction de la valeur TTL du DNS et n'applique pas une fréquence d'applications minimale du FQDN. *Si la TTL du FQDN du DNS est courte, mais que les résolutions FQDN ne changent pas aussi souvent que le délai TTL, une fréquence d'actualisation plus rapide n'est pas nécessaire. Vous devriez donc définir une fréquence d'actualisation minimale du FQDN pour éviter des tentatives d'actualisation du FQDN non nécessaires.*
Délai de temporisation des entrées obsolètes du FQDN (min.)	Précisez la durée de temps (en minutes) pendant laquelle le pare-feu continue à utiliser des résolutions FQDN obsolètes en cas d'échec du réseau ou d'un serveur DNS inaccessible — lorsqu'un FQDN n'est pas actualisé (la plage est comprise entre 0 et 10 080 ; la valeur par défaut est 1 440). Une valeur nulle indique que le pare-feu ne continue pas d'utiliser une entrée obsolète. Si le serveur DNS demeure inaccessible à la fin du délai de temporisation de l'état, l'entrée FQDN devient non résolue (les résolutions d'état sont supprimées). *Assurez-vous que la valeur de **FQDN Stale Entry Timeout (Délai de temporisation des entrées obsolètes du FQDN)** est suffisamment courte pour ne pas autoriser le transfert incorrect de trafic (qui présente un risque à la sécurité), mais suffisamment longue pour permettre la continuité du trafic sans causer de panne réseau non planifiée.*
Section Serveur proxy	

Paramètres des services globaux	Description
Serveur	Si le pare-feu doit utiliser un serveur proxy pour accéder aux services de mises à jour Palo Alto Networks, saisissez l'adresse IP ou le nom d'hôte du serveur proxy.
Port	Saisissez le port du serveur proxy
Utilisateur	Saisissez le nom d’utilisateur que l’administrateur doit entrer lorsqu’il accède au serveur proxy.
Mot de passe/ Confirmer le mot de passe	Saisissez et confirmez le mot de passe que l’administrateur doit entrer pour accéder au serveur proxy.
Utilisez un proxy pour envoyer les journaux vers Cortex Data Lake	Activez le pare-feu pour envoyer les journaux vers Cortex Data Lake via le serveur proxy.
NTP	
Adresse du serveur NTP	Saisissez l'adresse IP ou le nom d'hôte d'un serveur NTP que vous utiliserez pour synchroniser l'horloge du pare-feu. Vous pouvez éventuellement saisir l'adresse IP ou le nom d'hôte d'un second serveur NTP à utiliser pour synchroniser l'horloge du pare-feu, si le serveur principal devient indisponible. *Lorsqu'un serveur NTP conserve la synchronisation de toutes les horloges du pare-feu réseau, les travaux planifiés sont exécutés comme prévu et les horodatages peuvent permettre d’identifier les causes profondes des problèmes touchant plusieurs pare-feu. Configurez un serveur NTP principal et un serveur NTP secondaire, au cas où le serveur NTP principal devienne inaccessible.*
Authentication Type (Type d’authentification)	Vous pouvez permettre au pare-feu d'authentifier les mises à jour de l'heure provenant d'un serveur'A0;NTP. Pour chaque serveur'A0;NTP, sélectionnez le type d'authentification à utiliser'A0;: • **None (Aucune)** (par défaut) : sélectionnez cette option pour désactiver l'authentification NTP. • **Symmetric Key (Clé symétrique)** : sélectionnez cette option pour que le pare-feu utilise un échange de clés symétriques (secrets partagés) pour authentifier les mises à jour de l’heure du serveur NTP. Si vous sélectionnez l''option Clé symétrique, poursuivez en indiquant les valeurs suivantes : • **Key ID (ID de clé)**– Saisissez l'ID de la clé (1 à -65534). • **Algorithm (Algorithme)** : sélectionnez l’algorithme MD5 ou SHA1 à utiliser pour l’authentification NTP.

Paramètres des services globaux	Description
	• **Authentication Key/Confirm Authentication Key (Clé d'authentification/ Confirmer la clé)** : saisissez et confirmez la clé d'authentification de l'algorithme d'authentification. • **Autokey (Clé automatique)** : sélectionnez cette option pour que le pare-feu utilise une clé automatique (chiffrement à clé publique) pour authentifier les mises à jour de l'heure du serveur NTP. *Activez l'authentification du serveur NTP pour que le serveur NTP approuve le client et fournisse des mises à jour synchronisées.*

Prise en charge des protocoles IPv4 et IPv6 pour la configuration de l'itinéraire de service

Le tableau suivant présente la prise en charge IPv4 et IPv6 pour les configurations de l'itinéraire de service sur les systèmes globaux et virtuels.

Paramètres de configuration de l'itinéraire de service	Globale		Virtual System (système virtuel - vsys)	
	IPv4	IPv6	IPv4	IPv6
AutoFocus : serveur AutoFocus™	✓	—	—	—
État CRL : serveur Certificate Revocation List (liste de révocation du certificat ; CRL).	✓	✓	—	—
Data Services (Services de données) : envoyez des données aux services cloud de Palo Alto Networks à partir du plan de données du pare-feu. Optimisé pour un transfert de données plus rapide et empêche la perte de données. Requis pour la sécurité IoT, Enterprise DLP et SaaS Security.	✓	✓	✓	✓
DDNS : Service DNS dynamique.	✓	✓	✓	✓
Mises à jour transmises à Panorama : mises à jour de contenu et logiciels déployées depuis Panorama™.	✓	✓	—	—

Paramètres de configuration de l’itinéraire de service	Globale		Virtual System (système virtuel - vsys)	
	IPv4	IPv6	IPv4	IPv6
DNS : serveur Domain Name System. * Pour les systèmes virtuels, le DNS est inclus dans le profil de serveur DNS.	✓	✓	✓ *	✓ *
Listes dynamiques externes : mises à jour pour les listes dynamiques externes.	✓	✓	—	—
Messagerie : serveur de messagerie électronique.	✓	✓	✓	✓
HSM : serveur Hardware Security Module.	✓	—	—	✓
HTTP - Transfert HTTP.	✓	✓	✓	✓
Kerberos : serveur d'authentification Kerberos.	✓	—	✓	✓
LDAP : serveur Lightweight Directory Access Protocol.	✓	✓	✓	✓
MDM : serveur Mobile Device Management.	✓	✓	—	—
Authentification multi-facteur : serveur d’authentification multi-facteur (MFA).	✓	✓	✓	✓
NetFlow : le collecteur Netflow pour la collecte des statistiques de trafic réseau.	✓	✓	✓	✓
NTP : serveur Network Time Protocol.	✓	✓	—	—
Services Palo Alto Networks : mises à jour depuis Palo Alto Networks® et le serveur public WildFire®. Il s’agit également de l’itinéraire de service pour la transmission des pre-10.0 telemetry data (données de télémétrie antérieures à 10.0) vers Palo Alto Networks. (La télémétrie actuelle permet le transfert de ses données à Cortex Data Lake. Cet itinéraire de service n’est pas utilisé dans ce cas.)	✓	—	—	—

Paramètres de configuration de l'itinéraire de service	Globale		Virtual System (système virtuel - vsys)	
	IPv4	IPv6	IPv4	IPv6
Panorama : serveur de gestion de Panorama.	✓	✓	—	—
Transfert des journaux de Panorama (Les pare-feu de la Série PA-5200 uniquement**)** : transfert des journaux depuis le pare-feu vers les collecteurs de journaux.	✓	✓	—	—
Proxy : serveur agissant en tant que proxy sur le pare-feu.	✓	✓	—	—
RADIUS : serveur Remote Authentication Dial-in User Service.	✓	✓	✓	✓
SCEP : protocole Simple Certificate Enrollment Protocol pour la demande et la distribution de certificats clients.	✓	✓	✓	—
Piège SNMP : serveur de pièges Simple Network Management Protocol.	✓	—	✓	—
Syslog : serveur de journalisation des messages système.	✓	✓	✓	✓
TACACS+ : Serveur Terminal Access Controller Access-Control System Plus (TACACS+) pour les services d'authentification, d'autorisation et de comptabilité (AAA).	✓	✓	✓	✓
Agent UID : serveur d'agent User-ID.	✓	✓	—	✓
Mises à jour d'URL : serveur de mises à jour Uniform Resource Locator (localisateur uniforme de ressource ; URL).	✓	✓	—	—
Surveillance des machines virtuelles : surveillance des informations des machines virtuelles, lorsque vous avez activé Périphérique > Sources d'informations de machine virtuelle.	✓	✓	✓	✓

Paramètres de configuration de l’itinéraire de service	Globale		Virtual System (système virtuel - vsys)	
	IPv4	IPv6	IPv4	IPv6
Les pare-feu VM-Series dans des déploiements de cloud public qui surveillent des machines virtuelles doivent utiliser l’interface MGT. Vous ne pouvez pas utiliser une interface de plan de données comme itinéraire de service.				
Wildfire privé : serveur WildFire privé de Palo Alto Networks.	✓	—	—	—

Lors de la personnalisation d’un itinéraire de service **Global**, sélectionnez **Service Route Configuration (Configuration de l'itinéraire de service)** et, à l’onglet **IPv4** ou **IPv6**, sélectionnez un service dans la liste des services disponibles ; vous pouvez également sélectionner plusieurs services et **Set Selected Service Routes (Définir les itinéraires de service sélectionnés)** pour configurer plusieurs itinéraires de service en même temps. Pour restreindre les choix qui apparaissent dans la liste déroulante **Source Address (Adresse source)**, sélectionnez une **Source Interface (Interface source)** puis une **Source Address (Adresse source)** (correspondant à cette interface). Une interface source définie sur **Any (Tout)** vous permet de sélectionner une Adresse source parmi toutes les interfaces disponibles. Le champ Adresse source affiche l'adresse IPv4 ou IPv6 affectée à l'interface sélectionnée ; l'adresse IP sélectionnée est la source du trafic du service. Vous pouvez sélectionner **Use Default (Utiliser les paramètres par défaut)** si vous voulez que le pare-feu utilise l'interface de gestion pour l'itinéraire de service. Cependant, si l'adresse IP de destination du paquet correspond à l'adresse IP de destination configurée, l'adresse IP source est définie par l'Adresse Source configurée pour la Destination. Vous n'avez pas besoin de définir une adresse de destination car la destination est configurée lorsque vous configurez chaque service. Par exemple, lorsque vous définissez vos serveurs DNS (**Device (Périphérique)** > **Setup (Configuration)** > **Services**), vous définissez la destination des requêtes DNS. Vous pouvez spécifier une adresse IPv4 et une adresse IPv6 pour un service.

Une autre façon de personnaliser un itinéraire de service **Global** consiste à sélectionner **Service Route Configuration (Configuration de l'itinéraire de service)**, puis à sélectionner **Destination**. Définissez une adresse IP de **Destination** à laquelle un paquet entrant est comparé. Si l’adresse de destination du paquet correspond à l’Adresse IP de destination configurée, l’adresse IP source est définie sur l’Adresse source configurée pour la Destination. Pour restreindre les choix qui apparaissent dans la liste déroulante **Source Address (Adresse source)**, sélectionnez une **Source Interface (Interface source)** puis une **Source Address (Adresse source)** (correspondant à cette interface). Une interface source définie sur **Any (Tout)** vous permet de sélectionner une adresse source parmi toutes les interfaces disponibles. L’interface **MGT** source entraîne l'utilisation par le pare-feu de l'interface de gestion pour l'itinéraire de service.

Lorsque vous configurez des itinéraires de service pour un **Virtual System (Système virtuel)**, le choix de l’option **Inherit Global Service Route Configuration (Hériter de la configuration d'itinéraire de service globale)** implique que tous les services du système virtuel hériteront des paramètres de l'itinéraire

de service global. Vous pouvez plutôt choisir **Customize (Personnaliser)**, sélectionner **IPv4** ou **IPv6**, puis sélectionner un service ; vous pouvez également sélectionner plusieurs services et **Set Selected Service Routes (Définir les itinéraires de service sélectionnés)**. La **Source Interface (Interface source)** propose les trois choix suivants :

- **Inherit Global Setting (Hériter du paramètre global)** : les services sélectionnés héritent des paramètres globaux de ces services.
- **Any (Tout)** : vous permet de sélectionner une adresse source parmi toutes les interfaces disponibles (interfaces du système virtuel spécifique).
- **Une interface qui figure dans la liste déroulante** : restreint les choix de la liste déroulante **Source Address (Adresse source)** aux adresses IP de cette interface.

Pour la **Source Address (Adresse source)**, sélectionnez une adresse dans la liste déroulante. Pour les services sélectionnés, les réponses du serveur sont envoyées à cette adresse source.

Route pour le service de destination

- Périphérique > Configuration > Services > Global

À l'onglet **Global**, lorsque vous cliquez sur **Configuration de l'itinéraire de service**, puis sur **Personnaliser**, l'onglet **Destination** s'affiche. Les routes de service de destination sont disponibles dans l'onglet **Global** uniquement (et non dans l'onglet **Systèmes virtuels**), de sorte que le service de route d'un système virtuel ne peut pas appliquer un contrôle prioritaire sur les entrées de table de routage non associées à ce système virtuel.

Vous pouvez utiliser un itinéraire de service de destination pour ajouter une redirection personnalisée d'un service non pris en charge dans la liste de services **Personnaliser**. Un itinéraire de service de destination constitue une méthode de configuration du routage pour appliquer un contrôle prioritaire sur la table d'itinéraire de base d'informations de transfert (FIB). Tous les paramètres des itinéraires de service de destination appliqueront un contrôle prioritaire sur les entrées de la table d'itinéraire. Ils peuvent être liés ou non à n'importe quel service.

L'onglet **Destination** s'applique aux cas pratiques suivants :

- Lorsqu'un service ne comporte pas d'itinéraire de service d'application.
- Dans un système virtuel, lorsque vous souhaitez utiliser plusieurs routeurs virtuels ou une combinaison routeur virtuel/port de gestion.

Paramètres d’itinéraire de service de destination	Description
Destination	Saisissez l'adresse IP de **Destination**. Un paquet entrant dont l'adresse de destination correspond à cette adresse utilisera comme source l’adresse source que vous avez spécifié pour cette route de service.
Interface source	Pour restreindre la liste déroulante Adresse source, sélectionnez une **Interface source**. Si vous sélectionnez **tout**, toutes les adresses IP de toutes les interfaces seront disponibles dans la liste déroulante Adresse source. Le fait de sélectionner **MGT** entraîne

Paramètres d’itinéraire de service de destination	Description
	l'utilisation par le pare-feu de l'interface MGT pour l'itinéraire de service.
Adresse source	Sélectionnez la **Adresse source** de la route de service ; cette adresse servira aux paquets qui reviennent de la destination. Vous n'avez pas besoin de saisir le sous-réseau de l'adresse de destination.

Périphérique > Configuration > Interfaces

Utilisez cette page pour configurer les paramètres de connexion, les services autorisés et l'accès administratif pour l'interface de gestion (MGT) sur tous les modèles de pare-feu et pour les interfaces auxiliaires (AUX-1 et AUX-2) sur les pare-feu de la série PA-5200.

Palo Alto Networks vous recommande de toujours indiquer l'adresse IP et le masque de réseau (pour IPv4) ou la longueur de préfixe (pour IPv6) et la passerelle par défaut pour chaque interface. Si vous omettez l'un de ces paramètres pour l'interface MGT (comme la passerelle par défaut), vous pouvez uniquement accéder au pare-feu via le port de la console pour les modifications de configuration futures.

Pour configurer l'interface MGT sur l'appareil M-500 ou sur l'appareil virtuel Panorama, voir Panorama > Configuration > Interfaces.

*Vous pouvez utiliser une interface en boucle en tant qu'alternative à l'interface MGT pour la gestion des pare-feu (*Réseau > Interfaces > En boucle*).*

Élément	Description
Type (Interface MGT uniquement)	Sélectionnez parmi les choix suivants : • **Static (Statique)**: vous devez entrer manuellement l'adresse IPv4 ou IPv6 (ou les deux) et la ou les passerelles par défaut, qui sont décrites plus bas dans ce tableau. • **Client DHCP** : Configure l'interface MGT en tant que client DHCP afin que le pare-feu puisse envoyer des messages de Découverte ou de Demande de serveur DHCP pour trouver un serveur DHCP. Le serveur répond en fournissant une adresse IP (IPv4), un masque réseau (IPv4) et une passerelle par défaut pour l'interface MGT. Le serveur DHCP sur l'interface MGT est désactivé par défaut pour le pare-feu VM-Series (sauf pour le pare-feu VM-Series à AWS et Azure). Si vous sélectionnez **Client DHCP**, vous pouvez sélectionnez une ou les deux Options clientes suivantes : • **Envoyer le nom d'hôte** – Permet à l'interface MGT d'envoyer son nom d'hôte au serveur DHCP dans le cadre de l'Option DHCP 12. • **Envoyer l'ID du client** – Permet à l'interface MGT d'envoyer son identifiant client dans le cadre de l'Option DHCP 61. Si vous sélectionnez **Client DHCP**, vous pouvez cliquer sur **Afficher l'information concernant l'exécution du client DHCP** pour afficher l'état dynamique de l'interface IP : • Interface – Indique l'interface MGT. • Adresse IP : Adresse IP de l'interface MGT. • Masque réseau – Masque du sous-réseau pour l'adresse IP qui indique quels bits représentent le réseau ou le sous-réseau et lesquels représentent l'hôte. • Passerelle : Passerelle par défaut pour le trafic sortant de l'interface MGT.

Élément	Description
	• NTP primaire/secondaire : L'adresse IP d'un maximum de deux serveurs NTP desservant l'interface de gestion. Si le serveur DHCP renvoie les adresses du serveur NTP, le pare-feu les considère seulement si vous n'avez pas configuré manuellement les adresses du serveur NTP. Si vous avez configuré manuellement les adresses du serveur NTP, le pare-feu ne les remplace pas par celles du serveur DHCP. • Durée d'attribution : Nombre de jours, d'heures, de minutes et de secondes pendant lesquels l'adresse IP du serveur DHCP est attribuée. • Moment d'expiration : La date (année/mois/jour), l'heure (heures/minutes/secondes) et le fuseau horaire indiquant le moment où expirera l'attribution du serveur DHCP. • Serveur DHCP – Adresse IP du serveur DHCP répondant au Client DHCP de l'interface MGT. • Domaine : Nom de domaine auquel appartient l'interface MGT. • Serveur DNS : Adresse IP d'un maximum de deux serveurs DNS desservant l'interface de gestion. Si le serveur DHCP renvoie les adresses du serveur DNS, le pare-feu les considère seulement si vous n'avez pas configuré manuellement les adresses du serveur DNS. Si vous avez configuré manuellement les adresses du serveur DNS, le pare-feu ne les remplace pas par celles du serveur DHCP. Vous pouvez éventuellement **Renouveler** le bail DHCP pour l'adresse IP affectée à l'interface MGT. Sinon, cliquez sur **Fermer** pour fermer la fenêtre.
Aux 1 / Aux 2 (Pare-feu de la série PA-5200 uniquement)	Sélectionnez l'une des options suivantes pour activer une interface auxiliaire. Ces interfaces assurent un débit de 10 Gbit/s (SFP+) pour : • Trafic de gestion du pare-feu – Vous devez activer les Services réseau (protocoles) qui seront utilisés par les administrateurs lorsqu'ils accéderont à l'interface Web et à la CLI pour gérer le pare-feu. *Activez HTTPS au lieu de HTTP pour l'interface Web et activez SSH au lieu de Telnet pour la CLI.* • Synchronisation de la haute disponibilité (HD) entre les pare-feu homologues – Après avoir configuré l'interface, vous devez la sélectionner en tant que Liaison de contrôle HD **Périphérique** > **Haute disponibilité** > **Général**). • Transfert des journaux vers Panorama – Vous devez configurer un itinéraire de service avec le service activé **Transfert des journaux Panorama** (Périphérique > Configuration > Services).
Adresse IP (IPv4)	Si votre réseau utilise IPv4, affectez une adresse IPv4 à l'interface. Vous pouvez éventuellement affecter l'adresse IP d'une interface en boucle pour la gestion du pare-feu (voir Réseau > Interfaces > En boucle). Par défaut,

Élément	Description
	l'adresse IP que vous saisissez correspond à l'adresse source pour le transfert des journaux.
Masque réseau (IPv4)	Si vous avez affecté une adresse IPv4 à l'interface, vous devez également saisir un masque réseau (par exemple, 255.255.255.0).
Passerelle par défaut	Si vous avez affecté une adresse IPv4 à l'interface, vous devez également affecter une adresse IPv4 à la passerelle par défaut (elle doit se trouver sur le même sous-réseau que l'interface).
Longueur du préfixe / de l'adresse IPv6	Si votre réseau utilise IPv6, affectez une adresse IPv6 à l'interface. Pour indiquer le masque réseau, saisissez une longueur de préfixe IPv6 (par exemple, 2001:db8::300::1/64).
Passerelle IPv6 par défaut	Si vous avez affecté une adresse IPv6 à l'interface, vous devez également affecter une adresse IPv6 à la passerelle par défaut (elle doit se trouver sur le même sous-réseau que l'interface); par exemple, 2001:db8:300::5.
Vitesse	Configurez un débit de données et une option de duplex pour l'interface. Les choix possibles sont : 10 Mbits/s, 100 Mbits/s et 1 Gbit/s en duplex intégral ou semi-duplex. Utilisez le paramètre de négociation automatique par défaut pour que le pare-feu détermine la vitesse de l'interface. *Ce paramètre doit correspondre aux paramètres de port de l'équipement réseau voisin. Pour assurer les paramètres de mappage, sélectionnez la négociation automatique si l'équipement voisin prend en charge cette option.*
MTU	Saisissez l'unité de transmission maximale (MTU) en octets par paquet envoyé sur cette interface (plage de 576 à 1 500 ; par défaut 1 500).
Services de gestion administrative	• **HTTP** – Utilisez ce service pour accéder à l'interface Web du pare-feu. *HTTP utilise du texte en clair, ce qui n'est pas aussi sécuritaire que le protocole HTTPS. Par conséquent, Palo Alto Networks vous recommande d'activer le protocole **HTTPS** au lieu du protocole HTTP pour le trafic de gestion sur l'interface.* • **Telnet** – Utilisez ce service pour accéder au mode CLI du pare-feu. *Telnet utilise du texte en clair, ce qui n'est pas aussi sécuritaire que le protocole SSH. Par conséquent, Palo Alto Networks vous recommande d'activer le protocole SSH au lieu du protocole Telnet pour le trafic de gestion sur l'interface.*

Élément	Description
	• **HTTPS** – Utilisez ce service pour obtenir un accès sécurisé à l'interface Web du pare-feu. • **SSH** – Utilisez ce service pour obtenir un accès sécurisé à la CLI du pare-feu.
Services du réseau	Sélectionnez les services que vous souhaitez activer sur l'interface : • **HTTP OCSP** – Utilisez ce service pour configurer le pare-feu en tant que répondeur du protocole OCSP (Online Certificate Status Protocol). Pour plus d'informations, voir Périphérique > Gestion des certificats > Répondeur OCSP. • **Ping** – Utilisez ce service pour tester la connectivité avec des services externes. Par exemple, vous pouvez envoyer un ping à l'interface pour vérifier qu'elle reçoit les mises à jour logicielles et de contenu de PAN-OS du serveur de mises à jour Palo Alto Networks. Dans un déploiement haute disponibilité (HD), les pairs HA utilisent l'envoi de ping pour échanger de l'information sur la sauvegarde de pulsation. • **SNMP** – Utilisez ce service pour traiter les requêtes de statistiques du pare-feu à partir d'un gestionnaire SNMP. Pour plus de détails, voir Activation de la surveillance SNMP. • **User-ID** – Utilisez ce service pour Activer la redistribution des associations d'utilisateurs sur les pare-feu. • **SSL de l'écouteur Syslog de User-ID** – Utilisez ce service pour permettre à l'agent User-ID™ intégré à PAN-OS de collecter les messages Syslog sur SSL. Pour plus de détails, voir Configuration de l'accès aux serveurs surveillés. • **Ecoute UDP Syslog de User-ID** – Utilisez ce service pour permettre à l'agent User-ID intégré à PAN-OS de collecter les messages Syslog sur UDP. Pour plus de détails, voir Configuration de l'accès aux serveurs surveillés.
Adresses IP autorisées	Saisissez les adresses IP à partir desquelles les administrateurs peuvent accéder au pare-feu via l'interface. Une liste vide (par défaut) indique que l'accès est possible à partir de n'importe quelle adresse IP.  *Ne laissez pas la liste vide. Indiquez uniquement les adresses IP des administrateurs de pare-feu pour empêcher tout accès non autorisé.*

Périphérique > Configuration > Télémétrie

La télémétrie est la procédure consistant à collecter et transmettre les données de menaces et d'en fournir une analyse et à activer la logique de l'application. pour collecter et transmettre les données de télémétrie à Palo Alto Networks, vous devez d'abord sélectionner une région de destination. Si votre organisation possède actuellement une licence de Cortex Data Lake, votre région de destination est limitée à la même région que celle où réside votre instance Cortex Data Lake.

Les données de télémétrie sont utilisées pour renforcer les applications qui augmentent votre capacité à gérer et configurer vos produits et services Palo Alto Networks. Ces applications vous offrent une meilleure visibilité sur la santé, les performances, la planification des capacités et la configuration des périphériques. Palo Alto Networks utilise aussi en permanence ces données pour améliorer la prévention des menaces et vous aider à rentabiliser au maximum les avantages de votre produit.

Sélectionnez **Périphérique** > **Configuration** > **Télémétrie** pour voir les catégories de télémétrie actuellement collectées. Pour changer ces catégories, éditez le widget Télémétrie. Désélectionnez les catégories que vous ne voulez pas que le pare-feu collecte, puis validez la modification.

Générez un fichier de télémétrie pour obtenir un exemple en temps réel des données que le pare-feu enverra à Palo Alto Networks lors de l'intervalle de transmission de télémétrie) suivant.

Pour désactiver totalement la transmission de télémétrie, veillez à ce que **Activer la télémétrie** ne soit pas coché et validez votre modification.

Périphérique > Configuration > Content-ID

Utilisez l'onglet **Content-ID™** pour définir des paramètres de URL Filtering, de protection des données et de pages de conteneur.

Paramètres Content-ID	Description
Filtrage d'URL	
Délai de maintien des URL	Indiquez l'intervalle suivant une action **Continuer** d'un utilisateur avant que celui-ci ne doive de nouveau appuyer sur continuer pour des URL de même catégorie (plage de 1 à 86 400 minutes, par défaut 15).
Délai de contrôle prioritaire sur l'URL par l'administrateur	Indiquez l'intervalle suivant la saisie du mot de passe de **Administrateur outrepasser** par l'utilisateur avant que celui-ci ne doive de nouveau saisir le mot de passe pour des URL de même catégorie (plage de 1 à 86 400 minutes ; par défaut 15).
Garder en mémoire la demande du client pour la recherche de catégorie	Activez cette option pour indiquer que lorsque le pare-feu ne peut trouver les informations sur les catégories pour un URL dans son cache local, il garde en mémoire la requête Web pendant la requête PAN-DB. *Cette option est désactivée par défaut. Activez-la pour respecter les*bonnes pratiques du profil de URL Filtering .
Ajouter une barre oblique de fin	Activez le pare-feu pour ajouter une barre oblique de fin (/) aux entrées de domaine (par exemple, **`paloaltonetworks.com`**) dans des catégories d'URL personnalisées et des listes dynamiques externes de type de Listes d'URL qui ne se *terminent* pas par une barre oblique ou un astérisque de substitution (*). La barre oblique de fin limite les URL que le pare-feu considère comme correspondant à l'entrée et sur lesquelles il peut appliquer des règles de stratégie de filtrage d'URL. • Pour les entrées de domaine sans caractères génériques (* ou ^), les limites de barre oblique de fin correspondent au domaine spécifié et à ses sous-répertoires. • Pour les entrées de domaine comportant des caractères génériques, les limites de barre oblique de fin correspondent aux URL conformes au modèle spécifié. URL Category Exceptions (Exceptions de catégorie d'URL) décrit la barre oblique de fin plus en détail et inclut des instructions de mise en forme de liste d'URL.

Paramètres Content-ID	Description
	Cette option est activée par défaut.
Délai d'expiration pour le recherche de catégorie (secondes)	Précisez la période de temps, en secondes, pendant laquelle le pare-feu essaiera de trouver la catégorie d'un URL avant de déterminer que la catégorie est `non résolue` (plage comprise entre 1 et 60 secondes ; par défaut : 2).
Délai de verrouillage de l'URL par l'administrateur	Indiquez l'intervalle pendant lequel un utilisateur ne peut pas utiliser le mot de passe de Contrôle prioritaire administratif des URL après trois échecs (plage de 1 à 86 400 minutes ; par défaut 30).
Serveur PAN-DB (Obligatoire pour la connexion à un serveur PAN-DB privé)	Indiquez l'adresse IPv4, l'adresse IPv6 ou le nom de domaine complet des serveurs PAN-DB privés sur votre réseau. Vous pouvez ajouter jusqu'à 20 entrées. Le pare-feu se connecte par défaut au cloud PAN-DB public. La solution PAN-DB privé est conçue pour les entreprises qui interdisent aux pare-feux d'accéder directement aux serveurs PAN-DB du cloud public. Les pare-feu accèdent aux serveurs figurant dans cette liste de serveurs PAN-DB pour la base de données d'URL, les mises à jour des URL et les recherches d'URL afin de classer les pages Web.
Contrôle prioritaire sur l'URL par l'administrateur	
Paramètres de contrôle prioritaire de l'URL par l'administrateur	Pour chaque système virtuel que vous souhaitez configurer pour le contrôle prioritaire de l'URL par l'administrateur, cliquez sur **Add (Ajouter)** et indiquez les paramètres qui s'appliquent lorsqu'un profil de URL Filtering bloque une page et que l'action **Override (Contrôle prioritaire)** est spécifiée. Pour plus de détails, consultez Objects > Security Profiles > URL Filtering (Objets > Profiles de sécurité > Filtrage des URL). • **Emplacement** - (pare-feu comportant plusieurs systèmes virtuels uniquement) Sélectionnez le système virtuel dans le menu déroulant. • **Mot de passe/Confirmer le mot de passe** - Saisissez le mot de passe que l'utilisateur doit entrer pour appliquer un contrôle prioritaire sur la page de blocage. • **SSL/TLS Service Profile (Profil de service SSL/TLS)** - Pour préciser un certificat et les versions du protocole TLS autorisées pour sécuriser les communications lors d'une redirection via le serveur indiqué, sélectionnez un profil de service SSL/TLS. Pour plus d'informations, voir Périphérique > Gestion des certificats > Profil de service SSL/TLS. • **Mode** - Déterminez si la page de blocage est distribuée de manière transparente (elle semble provenir du site Web bloqué) ou si elle est redirige l'utilisateur vers le serveur défini. Si vous choisissez **Rediriger**, saisissez ensuite l'adresse IP de redirection.

Paramètres Content-ID	Description
	Vous pouvez aussi **Delete (Supprimer)** une entrée.
Paramètres HTTP/2	
Journalisation des connexions	Permet au pare-feu d'enregistrer les sessions de connexion HTTP/2 en tant qu'entrées de journal d'inspection de tunnel.
Paramètres du cloud de contenu	
URL du service	URL du serveur Cloud-Delivered Security Services. • **APAC—apac.hawkeye.services-edge.paloaltonetworks.com** • **Europe—eu.hawkeye.services-edge.paloaltonetworks.com** • **Royaume-Uni—uk.hawkeye.services-edge.paloaltonetworks.com** • **United States—us.hawkeye.services-edge.paloaltonetworks.com**
URL de Catégorisation du cloud en ligne	
Latence maximale (s)	Spécifiez la durée de traitement maximale acceptable, en secondes, pour que Inline Cloud Categorization renvoie un résultat.
Autoriser la latence maximale	Permet au pare-feu de prendre l'action d'autoriser, lorsque la latence maximale est atteinte. La désélection de cette option définit l'action du pare-feu sur bloquer.
Enregistrer le trafic non analysé	Permet au pare-feu d'enregistrer les demandes de catégorisation d'URL qui présentent la présence de certaines menaces de pages Web avancées, mais qui n'ont pas été traitées par Inline Cloud Categorization.
Paramètres Content-ID	
Autoriser le transfert du contenu déchiffré	Activez cette option pour configurer le pare-feu pour qu'il transfère du contenu déchiffré à un service externe lors de la mise en miroir du port ou de l'envoi de fichiers WildFire® pour analyse. *Activez cette option et envoyez tous les fichiers inconnus du trafic déchiffré à WildFire à des fins d'analyse.* Pour un pare-feu doté de la fonctionnalité de systèmes virtuels multiples (plusieurs systèmes virtuels), vous activez cette option individuellement pour chaque système virtuel. Sélectionnez **Périphérique** > **Systèmes virtuels** et sélectionnez le système virtuel sur lequel vous souhaitez activer

Paramètres Content-ID	Description
	le transfert du contenu décrypté. Cette option est disponible dans la boîte de dialogue Système virtuel.
Longueur de capture étendue des paquets	Définissez le nombre de paquets à capturer lorsque l'option de capture étendue est activée dans les profils antispyware et de Protection contre les vulnérabilités (plage de 1 à 50 ; par défaut 5).
Transférer les segments excédant le nombre permis par la file d'attente d'inspection de l'App-ID™ TCP	Activez cette option pour transférer les segments et enregistrer une application comme `tcp-inconnu` lorsque la file d'attente de l'App-ID dépasse la limite de 64 segments. Utilisez le compteur global suivant pour afficher le nombre de segments excédant le nombre permis par cette file d'attente indépendamment du fait que vous ayez activé ou désactivé cette option : `appid_exceed_queue_limit` Désactivez cette option pour empêcher le pare-feu de transférer les segments TCP et de sauter l'inspection de l'App-ID lorsque la file d'attente d'inspection de l'App-ID est pleine. *Cette option est désactivée par défaut et doit rester désactivée pour une sécurité maximale.* *Lorsque vous désactivez cette option, il est possible de constater une augmentation de la latence sur les flux où plus de 64 segments attendent le traitement de l'App-ID.*

Transférer les segments excédant le nombre permis par la file d'attente d'inspection du contenu TCP	Activez cette option pour transférer des segments TCP et sauter l'inspection du contenu lorsque la file d'attente d'inspection du contenu TCP est pleine. Le pare-feu peut mettre en file d'attente jusqu'à 64 segments lorsqu'il attend une réponse du moteur de contenu. Lorsque le pare-feu transmet un segment et ignore l'inspection du contenu en raison de la file d'attente d'inspection de l'ensemble du contenu, il incrémente le compteur global suivant :
	`ctd_exceed_queue_limit`
	Désactivez cette option pour empêcher le pare-feu de transférer les segments TCP et de sauter l'inspection du contenu lorsque la file d'attente d'inspection du contenu est pleine. Lorsque vous désactivez cette option, le pare-feu supprime tous les segments qui dépassent la limite de la file d'attente et incrémente le compteur global suivant :
	`ctd_exceed_queue_limit_drop`

Paramètres Content-ID	Description
	Cette paire de compteurs globaux s'applique à la fois aux paquets TCP et UDP. Si, après avoir affiché les compteurs généraux, vous décidez de modifier les paramètres, vous pouvez les modifier au sein de la CLI à l'aide de la commande suivante : **`set deviceconfig setting ctd tcp-bypass-exceed-queue`** *Cette option est activée par défaut, mais Palo Alto Networks vous recommande de désactiver cette option pour une sécurité maximale. Cependant, en raison des retransmissions TCP du trafic abandonné, la désactivation de cette option peut entraîner une dégradation des performances et une perte de fonctionnalité pour certaines applications, en particulier dans les environnements de trafic à fort volume.*

Transférer les datagrammes excédant le nombre permis par la file d'attente d'inspection du contenu UDP	Activez cette option pour transférer des datagrammes UDP et sauter l'inspection du contenu lorsque la file d'attente d'inspection du contenu UDP est pleine. Le pare-feu peut mettre en file d'attente jusqu'à 64 datagrammes lorsqu'il attend une réponse du moteur de contenu. Lorsque le pare-feu transmet un datagramme et ignore l'inspection du contenu en raison d'un débordement de la file d'attente d'inspection du contenu UDP, il incrémente le compteur global suivant :
	`ctd_exceed_queue_limit`
	Désactivez cette option pour empêcher le pare-feu de transférer les datagrammes et de sauter l'inspection du contenu lorsque la file d'attente d'inspection du contenu UDP est pleine. Lorsque cette option est désactivée, le pare-feu supprime tous les datagrammes qui dépassent la limite de la file d'attente et incrémente le compteur global suivant :
	`ctd_exceed_queue_limit_drop`
	Cette paire de compteurs globaux s'applique à la fois aux paquets TCP et UDP. Si, après avoir affiché les compteurs généraux, vous décidez de modifier les paramètres, vous pouvez les modifier au sein de la CLI à l'aide de la commande suivante :
	`set deviceconfig setting ctd udp-bypass-exceed-queue`

Paramètres Content-ID	Description
	Cette option est activée par défaut, mais Palo Alto Networks vous recommande de désactiver cette option pour une sécurité maximale. Cependant, en raison des paquets abandonnés, la désactivation de cette option peut entraîner une dégradation des performances et une perte de fonctionnalité pour certaines applications, en particulier dans les environnements de trafic à fort volume.
Autoriser les réponses HTTP partielles	Activez cette option de réponse partielle HTTP pour permettre à un client d'extraire seulement une partie d'un fichier. Lorsqu'un pare-feu de nouvelle génération identifie et supprime un fichier malveillant dans le chemin d'accès d'un transfert, il met fin à la session TCP à l'aide d'un paquet RST. Si le navigateur Web implémente l'option de plage HTTP, il peut commencer une nouvelle session pour extraire uniquement la partie restante du fichier. Cela empêche le pare-feu de déclencher à nouveau la même signature en raison de l'absence de contexte dans la session initiale, tout en permettant au navigateur Web de réassembler le fichier et de livrer le contenu malveillant ; pour éviter cette situation, assurez vous de désactiver cette option.

Paramètres Content-ID	Description
	***Autoriser la réponse** partielle HTTP est activé sur le pare-feu par défaut. Cela offre une disponibilité maximale mais augmente le risque d'une cyberattaque réussie. Pour une sécurité maximale, désactivez cette option pour empêcher le navigateur Web de démarrer une nouvelle session pour récupérer le reste d'un fichier après que le pare-feu a mis fin à la session d'origine en raison d'une activité malveillante. La désactivation de la réponse partielle HTTP affecte les transferts de données HTTP qui utilisent l'en-tête RANGE, ce qui peut entraîner des anomalies de service pour certaines applications. Après avoir désactivé la réponse partielle HTTP, validez le fonctionnement de vos applications stratégiques.* *Si vous rencontrez une interruption du transfert de données HTTP sur une application stratégique, vous pouvez créer une stratégie de remplacement d'application pour cette application spécifique. Étant donné que application Override contourne App-ID (y compris l'inspection des menaces et du contenu), créez une stratégie Application Override uniquement pour l'application critique spécifique et spécifiez les sources et les destinations pour limiter la règle (principe de l'accès au moindre privilège). Ne créez pas de stratégie de remplacement d'application, sauf si vous le devez. Pour plus d'informations sur les stratégies de remplacement d'application, reportez-vous à* https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVLCA0.
Recherche de signatures en temps réel	
Délai d'expiration de la recherche de signature DNS (ms)	Précisez la durée de temps, en millisecondes, avant que le pare-feu interroge le service de Sécurité DNS. Si le nuage ne répond pas avant la fin de la période précisée, le pare-feu communique la réponse DNS associée au client effectuant la demande (la plage est comprise entre 0 et 60 000 ; la valeur par défaut est 100).
En-têtes X-Forwarded-For	
Utilisez l'en-tête X-Forwarded-For	*Vous ne pouvez pas activer X-Forwarded-For pour une ID-Utilisateur et une Politique de sécurité en même temps.* • **désactivé** : lorsqu'il est désactivé, le pare-feu ne peut pas lire les adresses IP de l'en-tête X-Forwarded-For (XFF) dans les requêtes de client.

Paramètres Content-ID	Description
	• **Activez pour l'ID-Utilisateur**Activez cette option pour indiquer que User-ID lit les adresses IP de l'en-tête X-Forwarded-For (XFF) dans les demandes client de services Web lorsque le pare-feu est déployé entre internet et un serveur proxy qui masquerait autrement les adresses IP des clients. User-ID met en correspondance les adresses IP qu'il lit avec les noms d'utilisateur référencés dans vos politiques afin que ces politiques puissent contrôler et consigner l'accès des utilisateurs et groupes associés. Si l'en-tête comporte plusieurs adresses IP, User-ID utilise la première entrée à gauche. Dans certains cas, la valeur d'en-tête est une chaîne de caractères au lieu d'être une adresse IP. Si la chaîne correspond à un nom d'utilisateur que l'User-ID a mappé à une adresse IP, le pare-feu utilise ce nom d'utilisateur pour les références de mappage de groupe dans les politiques. Si aucun mappage d'adresse IP n'existe pour la chaîne, le pare-feu invoque les règles de politique dans lesquelles l'utilisateur source est configuré sur **tout** ou **inconnu**. Les journaux de filtrage des URL affichent les noms d'utilisateur correspondants dans le champ Utilisateur source. Si User-ID ne parvient pas à effectuer la correspondance ou s'il n'est pas activé pour la zone associée à l'adresse IP, le champ Utilisateur source indique l'adresse IP XFF avec le préfixe **`x-fwd-for`**. *Activez l'utilisation de l'en-tête XFF dans User-ID pour que l'adresse IP du client d'origine apparaisse dans les journaux pour vous aider à enquêter sur des problèmes.* • **Activez pour la politique de sécurité** : Activez cette option pour indiquer que le pare-feu lit les adresses IP de l'en-tête X-Forwarded-For (XFF) dans les demandes client de services Web lorsqu'un périphérique en amont, comme un serveur proxy ou un équilibreur de charge, est déployé entre le client et le pare-feu. L'adresse IP du serveur proxy ou de l'équilibreur de charge remplace l'adresse IP client en tant que IP source de la requête. Le pare-feu peut ensuite utiliser les adresses IP dans l'en-tête XFF pour appliquer la stratégie. *Le pare-feu utilise l'adresse IP la plus récemment ajoutée au champ XFF. Si la requête passe par plusieurs périphériques en amont, le pare-feu applique la politique sur la base de laquelle l'adresse IP a été ajoutée en dernier.*
En-tête Strip-X-Forwarded-For	Activez cette option pour supprimer l'en-tête X-Forwarded-For (XFF), qui contient l'adresse IP d'un client demandant un service Web lorsque le pare-feu est déployé entre internet et un serveur proxy. Le pare-feu réinitialise la valeur de l'en-tête avant de transférer la requête : les paquets transférés ne contiennent aucune information sur l'adresse IP source interne.

Paramètres Content-ID	Description
	L'activation de cette option ne désactive pas l'utilisation d'en-têtes XFF pour l'attribution d'utilisateur dans des politiques ; le pare-feu réinitialise la valeur XFF uniquement après l'avoir utilisée pour l'attribution d'utilisateur. *Lorsque vous activez l'utilisation d'en-têtes XFF dans User-ID, activez également la suppression de l'en-tête XFF avant le transfert du paquet pour protéger la confidentialité des utilisateurs sans perdre la capacité de les suivre. L'activation des deux options vous permet de journaliser et de faire le suivi des adresses IP des utilisateurs initiaux tout en protégeant leur confidentialité en évitant de transférer leur adresse IP d'origine.*
ID de contenu - Caractéristiques	
Gérer la protection des données	Ajoutez une protection supplémentaire à l'accès aux journaux pouvant contenir des informations sensibles, des numéros de carte de crédit ou de sécurité sociale par exemple. Cliquez sur **Gérer la protection des données** pour effectuer les tâches suivantes : • **Définir le mot de passe** - Si aucun mot de passe n'a déjà été configuré, saisissez et confirmez-en un nouveau. • **Modifier le mot de passe** - Saisissez l'ancien mot de passe, puis saisissez et confirmez-en un nouveau. • **Supprimer le mot de passe** - Supprime le mot de passe et les données protégées.
Pages de conteneur	Utilisez ces paramètres pour préciser les types d'URL qui sont suivis ou consignés par le pare-feu en fonction du type de contenu, application/pdf, application/soap+xml, application/xhtml+, texte/html, texte/brut et texte/xml par exemple. Les pages de conteneur sont définies par système virtuel que vous sélectionnez dans le menu déroulant **Location (Emplacement)**. Si une page de conteneur n'est pas explicitement définie pour un système virtuel, le pare-feu utilise les types de contenu par défaut. **Ajoutez** et saisissez un type de contenu ou sélectionnez un type de contenu existant. L'ajout de nouveaux types de contenu pour un système virtuel applique un contrôle prioritaire sur la liste des types de contenu par défaut. Si aucun type de contenu n'est associé à un système virtuel, la liste des types de contenu par défaut est utilisée.
Threat Prevention de l'analyse cloud en ligne	

Paramètres Content-ID	Description
Latence maximale (s)	Spécifiez la durée de traitement maximale, en secondes, pour que Advanced Threat Prevention Inline Cloud Analysis renvoie un résultat.
Autoriser la latence maximale	Permet au pare-feu de prendre l’action d’autoriser, lorsque la latence maximale est atteinte. La désélection de cette option définit l’action du pare-feu sur bloquer.
Enregistrer le trafic non analysé	Permet au pare-feu d’enregistrer les demandes de trafic qui présentent des caractéristiques anormales indiquant la présence de menaces C2 (Command and Control) avancées et évasives, mais qui n’ont pas été traitées par les analyseurs Threat Prevention Inline Cloud.

Périphérique > Configuration > WildFire

Sélectionnez **Périphérique** > **Configuration** > **WildFire** pour configurer les paramètres WildFire sur le pare-feu et sur Panorama. Vous pouvez activer le cloud WildFire et un appareil WildFire pour les utiliser afin d'analyser des fichiers. Vous pouvez également définir des limites de taille de fichier et des informations de session à signaler. Après avoir renseigné des paramètres WildFire, vous pouvez indiquer les fichiers à transférer au cloud WildFire ou à l'appareil WildFire en créant un profil d'**Analyse WildFire** (**Objets** > **Profils de sécurité** > **Analyse WildFire**).

Pour transférer le contenu déchiffré à WildFire, reportez-vous à la section Transfert du trafic déchiffré pour analyse WildFire.

Paramètres WildFire	Description
Paramètres généraux	
Cloud public WildFire	Saisissez **`wildfire.paloaltonetworks.com`** pour envoyer des fichiers sur le Cloud mondial WildFire, hébergé aux États-Unis (U.S.), pour qu'ils fassent l'objet d'une analyse. Par ailleurs, vous pouvez, à la place, envoyer des fichiers à un Cloud régional WildFire pour qu'ils fassent l'objet d'une analyse. Les Cloud régionaux sont conçus pour adhérer à vos attentes en matière de confidentialité des données en fonction de votre emplacement.

Paramètres WildFire	Description
	Transmettez les échantillons à un cloud régional WildFire pour veiller au respect des normes en matière de conformité et de confidentialité des données propres à votre région. Les clouds régionaux sont les suivants : • *Europe :* ***eu.wildfire.paloaltonetworks.com*** • *Japon :* ***jp.wildfire.paloaltonetworks.com*** • *Singapour :* ***sg.wildfire.paloaltonetworks.com*** • *Royaume-Uni —****uk.wildfire.paloaltonetworks.com*** • *Canada—****ca.wildfire.paloaltonetworks.com*** • *Australie :* ***au.wildfire.paloaltonetworks.com*** • *Allemagne —****de.wildfire.paloaltonetworks.com*** • *Inde—****in.wildfire.paloaltonetworks.com***
Cloud WildFire privé	Indiquez l'adresse IPv4/IPv6 ou le nom de domaine complet de l'appareil WildFire. Le pare-feu envoie des fichiers pour analyse à l'appareil WildFire spécifié. Panorama collecte des ID de menace depuis l'appareil WildFire pour permettre l'ajout d'exceptions de menace dans les profils antispyware (uniquement pour les signatures DNS) et les profils antivirus que vous configurez dans les groupes de périphériques. Panorama collecte également des informations provenant de l'appareil WildFire pour remplir les champs manquants dans les journaux des envois WildFire reçus de la part des pare-feu exécutant des versions de logiciels antérieures à PAN-OS 7.0.
Limites de taille de fichier	Indiquez la taille de fichier maximale à transférer au serveur WildFire. Pour toutes les recommandations relatives aux tailles de fichiers, si la limite est trop grande et empêche le pare-feu de transférer en même temps plusieurs fichiers du jour zéro de grande taille, réduisez et affinez la limite maximale à la taille d'espace tampon disponible sur le pare-feu. Si de l'espace tampon supplémentaire est disponible, vous pouvez accroître la limite de taille du

Paramètres WildFire	Description
	fichier au-dessus de la recommandation. Les recommandations sont un bon point de départ pour définir des limites efficaces qui ne surchargent pas les ressources du pare-feu. Les intervalles disponibles sont: • **pe** (Portable Executable) – La plage est comprise entre 1 et 50 Mo ; 16 Mo par défaut.  *Définissez la taille des fichiers PE sur 16 Mo.* • **apk** (Application Android) – La plage est comprise entre 1 et 50 Mo ; 10 Mo par défaut.  *Définissez la taille des fichiers APK sur 10 Mo.* • **pdf** (Portable Document Format) – La plage est comprise entre 100 Ko et 51 200 Ko ; 3 072 Ko par défaut.  *Définissez la taille des fichiers PDF sur 3 072 Ko.* • **ms-office** (Microsoft Office) – La plage est comprise entre 200 Ko et 51 200 Ko ; 16 384 Ko par défaut.  *Définissez la taille des fichiers ms-office sur 16 384 Ko.* • **jar** (Packaged Java class file) – La plage est comprise entre 1 et 20 Mo ; 5 Mo par défaut.  *Définissez la taille des fichiers jar sur 5 Mo.* • **Flash** (Adobe Flash) – La plage est comprise entre 1 et 10 Mo ; 5 Mo par défaut.  *Définissez la taille des fichiers flash sur 5 Mo.* • **Mac OS X** (Fichiers DMG / MAC-APP / MACH-O PKG) – Plage comprise entre 1 et 50 Mo ; la valeur par défaut est de 10 Mo.  *Définissez la taille des fichiers MacOSX sur 1 Mo.* • **archive** (Fichiers RAR et 7z) – La plage est comprise entre 1 et 50 Mo ; 50 Mo par défaut.  *Définissez la taille des fichiers d'archive sur 50 Mo.*

Paramètres WildFire	Description
	• **linux** (Fichiers ELF) – La plage est comprise entre 1 et 50 Mo ; 50 Mo par défaut. *Définissez la taille des fichiers linux sur 50 Mo.* • **script** (fichiers JScript, VBScript, PowerShell et Shell Script) – La plage est comprise entre 10 et 4 096 Ko; 20 Ko par défaut. *Définissez la taille des fichiers script sur 20 Ko.* *Les valeurs précédentes peuvent varier en fonction de la version actuelle de PAN-OS ou de la version du contenu. Pour afficher les plages valides, cliquez sur le champ **Taille maximale**. Une fenêtre contextuelle indiquant la plage disponible et la valeur par défaut s'affiche.*
Signaler des fichiers bénins	Lorsque cette option (désactivée par défaut) est activée, les fichiers analysés par WildFire déterminés comme bénins s'affichent dans le journal des envois WildFire dans **Surveillance** > **Envois WildFire**. même si cette option est activée sur le pare-feu, les liens contenus dans les e-mails que WildFire considère comme bénins ne sont pas consignés en raison de la quantité possible de liens traités.
Signaler des fichiers Grayware	Lorsque cette option (désactivée par défaut) est activée, les fichiers analysés par WildFire déterminés comme indésirables s'affichent dans le journal des envois WildFire dans **Monitor (Surveillance)** > **WildFire Submissions (Envois WildFire)**. *même si cette option est activée sur le pare-feu, les liens contenus dans les e-mails que WildFire considère comme « grayware » ne sont pas consignés en raison de la quantité possible de liens traités.* *Activez le signalement des fichiers bénins pour journaliser les informations de session, l'activité réseau, l'activité des hôtes et les autres informations qui aident les analyses.*
Paramètres des informations de session	
Paramètres	Indiquez les informations à transférer au serveur'A0;WildFire. Par défaut, toutes les options sont sélectionnées. Il est recommandé de transférer toutes les informations de session pour fournir des statistiques et d'autres mesures qui vous permettent de prendre des mesures pour empêcher les événements des menaces :

Paramètres WildFire	Description
	• **Adresse IP source** : adresse IP source ayant envoyé le fichier suspect. • **Port source** : port source ayant envoyé le fichier suspect. • **Adresse IP de destination** : adresse IP de destination ayant envoyé le fichier suspect. • **Port de destination** : port de destination ayant envoyé le fichier suspect. • **Vsys** : système virtuel de pare-feu ayant identifié le logiciel malveillant possible. • **Application** : application utilisateur utilisée pour transmettre le fichier. • **Utilisateur** : utilisateur ciblé. • **URL** : URL associée au fichier suspect. • **Nom du fichier** : nom du fichier envoyé. • **Expéditeur de l'e-mail** : indique le nom de l'expéditeur dans les journaux et les rapports détaillés WildFire lorsqu'un lien contenu dans un e-mail est détecté dans le trafic SMTP et POP3. • **Destinataire de l'e-mail** : indique le nom du destinataire dans les journaux et les rapports détaillés WildFire lorsqu'un lien contenu dans un e-mail est détecté dans le trafic SMTP et POP3. • **Objet de l'e-mail** : indique l'objet de l'e-mail dans les journaux et les rapports détaillés WildFire lorsqu'un lien contenu dans un e-mail est détecté dans le trafic SMTP et POP3.

Périphérique > Configuration > Session

Sélectionnez **Périphérique** > **Configuration** > **Session** pour configurer les paramètres d'expiration de session, les paramètres de certificat de déchiffrement et les paramètres généraux relatifs à la session, comme la protection par pare-feu du trafic IPv6 et la revérification de la politique de Sécurité sur les sessions existantes en cas de modification de la politique. Cet onglet contient les sections suivantes:

- Paramètres de session
- Délais d'expiration de session
- Paramètres TCP
- Paramètres de décryptage : Vérification de la révocation du certificat
- Paramètres de décryptage : Paramètres de certificat du serveur proxy de transfert
- Paramètres de décryptage : Paramètres de décryptage SSL
- Paramètres de session VPN

Paramètres de session

Le tableau suivant décrit les paramètres de session.

Paramètres de session	Description
Revérifier les sessions	Cliquez sur **Edit (Modifier)** et sélectionnez **Rematch Sessions (Revérifier les sessions)** pour que le pare-feu applique les nouvelles règles de politique de sécurité configurées aux sessions en cours. Cette option est activée par défaut. Si ce paramètre est désactivé, une fois validée, toute modification d'une règle de politique s'applique uniquement aux sessions initiées après la réalisation de la modification. Par exemple, si une session Telnet commence alors qu'une règle de politique associée a été configurée pour autoriser Telnet et que vous validez par la suite une modification de règle de politique pour refuser Telnet, le pare-feu applique la règle de politique révisée à la session en cours et la bloque. *Activez **Rematch Sessions (Revérifier les sessions)** pour appliquer vos dernières règles de politique de sécurité aux sessions actuellement actives.*
ICMPv6, jeton - Taille du compartiment	Saisissez la taille du jeton pour la limitation des messages d'erreur ICMPv6. La taille du jeton est un paramètre de l'algorithme du jeton qui contrôle la distribution en paquets des erreurs ICMPv6 (plage de 10 à 65 535 paquets ; par défaut 100).
Erreur ICMPv6 - Débit du paquet	Saisissez le nombre moyen de paquets d'erreur ICMPv6 par seconde autorisés globalement sur le pare-feu (plage de 10 à 65 535 paquets/seconde ; par défaut 100). Cette valeur s'applique à toutes les interfaces. Si le pare-

Paramètres de session	Description
	feu atteint le nombre moyen de paquets d'erreur ICMPv6, le sceau à jetons permet la limitation des messages d'erreur ICMPv6.
Activer le pare-feu IPv6	Pour activer les fonctions du pare-feu pour IPv6, cliquez sur **Edit (Modifier)** et sélectionnez **IPv6 Firewalling (Activer le pare-feu IPv6)**. Le pare-feu ignore les configurations basées sur IPv6 si vous n'activez pas le pare-feu IPv6. Même si vous activez le trafic IPv6 sur une interface, vous devez aussi activer l'option **IPv6 Firewalling (pare-feu IPv6)** pour que le pare-feu IPv6 fonctionne.
Prise en charge ERSPAN	Activez le pare-feu pour mettre fin aux tunnels GRE (Generic Routing Encapsulation) et décapsuler les données ERSPAN (Encapsulated Remote Switched Port Analyzer). Ceci est utile pour les services de sécurité tels que iot security. Les commutateurs réseau reflètent le trafic réseau et utilisent ERSPAN pour l'envoyer au pare-feu via des tunnels GRE. Après avoir décapsulé les données, le pare-feu les inspecte de la même manière qu'il inspecte le trafic reçu sur un port TAP. Il crée ensuite des journaux d'application améliorés (ECL) et du trafic, des menaces, wildfire, URL, données, GTP (lorsque GTP est activé), SCTP (lorsque SCTP est activé), tunnel, authentification et journaux de déchiffrement. Le pare-feu transmet ces journaux au service de journalisation où IoT Security accède aux données et les analyse.
Activer la trame Jumbo Global MTU	Sélectionnez cette option pour activer la prise en charge de trames Jumbo sur les interfaces Ethernet. Les trames Jumbo disposent d'une unité de transmission maximale (MTU) de 9,192 octets et sont disponibles sur certains modèles uniquement. • Si vous ne validez pas**Enable Jumbo Frame (Activer la trame Jumbo)**, la **Global MTU (MTU globale)** est de 1,500 octets par défaut (plage de 576 à 1 500). • Si vous validez **Enable Jumbo Frame (Activer la trame Jumbo)** Jumbo, la **Global MTU (MTU globale)** est de 9 192 octets par défaut (plage de 9 192 à 9 216 octets). *Les trames Jumbo peuvent utiliser jusqu'à cinq fois plus de mémoire que les paquets normaux et peuvent réduire le nombre de mémoires tampons des paquets disponibles de 20 %. Ceci réduit la taille de la file d'attente dédiée aux tâches hors service et d'identification des applications, ainsi qu'aux autres tâches similaires de traitement des paquets. A partir de PAN-OS 8.1, si vous activez la configuration MTU globale de trames jumbo et redémarrez votre pare-feu, les mémoires tampons des paquets sont redistribuées pour traiter les trames jumbo plus efficacement.*

Paramètres de session	Description
	Si vous activez les trames Jumbo et qu'une MTU spécifique n'est pas configurée sur certaines interfaces, ces dernières héritent automatiquement de la taille de trame Jumbo. Par conséquent, avant d'activer les trames Jumbo, si vous avez une interface sur laquelle vous ne voulez pas autoriser des trames Jumbo, vous devez définir la MTU de cette interface sur 1,500 octets ou une autre valeur. Pour configurer le MTU pour l'interface (**Network (Réseau)** > **Interfaces** > **Ethernet**), reportez-vous à la section Interface de couche 3 de la série PA-7000.
Session de diffusion DHCP	Si votre pare-feu agit en tant que serveur DHCP, sélectionnez cette option pour activer les journaux de session pour les paquets de diffusion DHCP. L'option de Session de diffusion DHCP active la génération de Journaux d'application améliorée (Journaux EAL) pour DHCP afin que IoT Security et les autres services les utilisent. Si vous n'activez pas cette option, le pare-feu transfère les paquets sans créer de journaux pour les paquets de diffusion DHCP.
l'inspection des en-têtes L3 et L4	Active l'inspection des en-têtes Layer3 et Layer4. Sélectionnez cette option pour écrire des signatures de menaces personnalisées basées sur les champs d'en-tête L3 et L4 via le profil Protection de zone afin de vous défendre contre les vulnérabilités qui ne sont généralement pas traitées par les mises à jour de signatures standard, telles que celles présentes dans certains appareils IoT. *Vous devez redémarrer le pare-feu pour que la modification de configuration prenne effet.*
MTU IPv6 min. pour le réseau NAT64	Saisissez la MTU globale du trafic traduit en IPv6. La valeur par défaut de 1 280 octets est basée sur la MTU minimum standard du trafic IPv6 (plage de 1 280 à 9 216).
Taux de sursouscription NAT	Sélectionnez le taux de sursouscription NAT DIPP, qui est le nombre de fois que le pare-feu peut utiliser la même adresse IP traduite et une paire de ports identiques simultanément. La réduction du taux de sursouscription diminue le nombre de traductions de périphérique source, mais étend les fonctionnalités des règles NAT. • **Platform Default (Valeur par défaut de la plate-forme)** – La configuration explicite du taux de sursouscription est désactivée et le taux de sursouscription par défaut du modèle s'applique. Voir les taux par défaut des modèles de pare-feu à l'adresse https://www.paloaltonetworks.com/products/product-selection.html. • **1x** – 1 fois. Cela signifie aucune sursouscription ; le pare-feu ne peut pas utiliser la même adresse IP traduite et la même paire de ports plus d'une fois simultanément. • **2x** – 2 fois.

Paramètres de session	Description
	• **4x** – 4 fois. • **8x** – 8 fois.
Taux de paquets ICMP inaccessibles (par sec)	Définissez le nombre maximum de réponses ICMP inaccessibles que le pare-feu peut envoyer par seconde. Cette limite est partagée par les paquets IPv4 et IPv6. La valeur par défaut est de 200 messages par seconde (plage de 1 à 65 535).
Vieillissement accéléré	Permet d'accélérer le vieillissement des sessions inactives. Sélectionnez cette option pour activer le vieillissement accéléré et préciser le seuil (en %) et le facteur d'échelle. Lorsque la table de la session atteint **Accelerated Aging Threshold (Seuil du vieillissement accéléré)** (% saturé), PAN-OS applique **Accelerated Aging Scaling Factor (Facteur d'échelle du vieillissement accéléré)** est appliqué aux calculs de vieillissement de toutes les sessions. Le facteur d'échelle par défaut est de 2, ce qui signifie que le vieillissement accéléré se produit à un taux deux fois plus élevé que la durée d'inactivité configurée. La durée d'inactivité configurée divisée par 2 a pour conséquence un délai plus court (réduit de moitié). Pour calculer le vieillissement accéléré d'une session, PAN-OS divise la durée d'inactivité configurée (pour ce type de session) par le facteur d'échelle afin de déterminer un délai plus court. Par exemple, si le facteur d'échelle est de 10, une session qui expirerait normalement au bout de 3 600 secondes expirerait 10 fois plus vite (en 1/10e du temps), c'est-à-dire au bout de 360 ;secondes. *Activez un seuil de vieillissement accéléré et définissez un facteur d'échelle acceptable pour libérer plus rapidement l'espace de la table des sessions lorsque celle-ci commence à se remplir.*
Protection de la mémoire tampon des paquets	A partir de PAN-OS 10.0, la protection tampon des paquets est activée par défaut de façon globale et pour chaque zone. Il est recommandé de conserver l'activation de la protection de la mémoire tampon des paquets globalement et à chaque zone pour protéger les mémoires tampons des pare-feux des attaques DoS et des sessions et sources agressives. Cette option protège les mémoires tampons de réception du pare-feu contre les attaques ou le trafic abusif qui provoque la sauvegarde des ressources du système et la suppression du trafic légitime. La protection de la mémoire tampon des paquets identifie les sessions incriminées, utilise Random Early Detection (RED, Détection anticipée aléatoire) en tant que première ligne de défense et abandonne la session ou bloque l'adresse IP offensante si l'abus se poursuit. Si le pare-feu détecte de nombreuses petites sessions ou la création rapide de sessions (ou les deux) à partir d'une adresse IP spécifique, il bloque cette adresse IP.

Paramètres de session	Description
	Prenez les mesures de base de l'utilisation des mémoires tampons des paquets du pare-feu pour comprendre la capacité du pare-feu et veiller à ce qu'il soit bien configuré de sorte que seule une attaque puisse entraîner une forte hausse de l'utilisation de la mémoire tampon. • **Alert (%) (Alerte (%))** : lorsque l'utilisation de la mémoire tampon des paquets dépasse ce seuil pendant plus de 10 secondes, le pare-feu crée un journal d'événements toutes les minutes. Le pare-feu génère des événements de journal lorsque la protection de la mémoire tampon des paquets est activée globalement (la plage est comprise entre 0 et 99 % ; par défaut : 50 %). Si la valeur est de 0 %, le pare-feu ne crée pas de journaux d'événements. Commencez par la valeur de seuil par défaut et ajustez-la, au besoin. • **Activate (%) (Activer [%])** – Lorsque ce seuil est atteint, le pare-feu commence à limiter les sessions les plus abusives (la plage est comprise entre 0 et 99 % ; par défaut : 80 %). Si la valeur est de 0 %, le pare-feu n'applique pas la RED. Commencez par la valeur de seuil par défaut et ajustez-la, au besoin.
Protection de la mémoire tampon des paquets (suite)	• (Pare-feu matériels exploitant PAN-OS 10.0 ou un version ultérieure) En tant qu'alternative à la protection tampon de paquets qui se base sur les pourcentages d'utilisation (décrits ci-dessus), vous pouvez déclencher la protection tampon de paquets sur la base du CPU traitant la latence en activant **Buffering Latency Based (Basé sur la latence de tampon)** et en configurant les paramètres suivants : • **Latency Alert (millisecondes) (Alerte de latence)** : lorsque la latence dépasse ce seuil, le pare-feu commence à générer un événement de journal d'alerte toutes les minutes ; la plage est de 1 à 20 000 ; la valeur par défaut est 50. • **Latency Activate (millisecondes) (Activation de latence)** : lorsque la latence dépasse ce seuil, le pare-feu active l'Abandon anticipé aléatoire (RED) sur les paquets entrants et commence à générer un journal d'activation toutes les 10 secondes (la plage est de 1 à 20 000 ; la valeur par défaut est de 200). • **Latency Max Tolerate (millisecondes) (Tolérance max de latence)** lorsque la latence dépasse ce seuil, le pare-feu utilise RED avec une probabilité d'abandon proche de 100 % (la plage est de 1 à 20 000 ms ; la valeur par défaut est de 500 ms). Si la latence actuelle est une valeur comprise entre le seuil Latency Activate (Activation de latence) et le seuil Latency Max Tolerate (Tolérance max de latence), le pare-feu calcule la probabilité d'abandon RED comme suit : (latence actuelle - seuil **Latency Activate (Activation de latence)**) / seuil **(Latency Max Tolerate (Tolérance max de latence)** - seuil **Latency Activate (Activation de latence)**). Par exemple, si la latence actuelle est 300, Latency Activate (Activation de latence) est 200, et Latency Max Tolerate

Paramètres de session	Description
	(Tolérance max de latence) est 500, alors (300-200)/(500-200) = 1/3, ce qui signifie que le pare-feu utilise une probabilité d'abandon RED d'environ 33 %.
Protection de la mémoire tampon des paquets (suite)	• **Block Hold Time (sec) (Délai de maintien du blocage (sec))** – La période, en secondes, pendant laquelle cette session est autorisée à se poursuivre avant que la session ne soit abandonnée ou l'adresse IP source est bloquée (la plage est comprise entre 0 et 65 535 ; par défaut : 60). Ce minuteur surveille les sessions limitées par RED pour voir si elles continuent de s'obstiner à utiliser la mémoire tampon ou la latence au-dessus du seuil configuré. Si le comportement abusif se poursuit après le délai de maintien du blocage, la session est abandonnée. Si la valeur est 0, le pare-feu n'abandonne pas les sessions en fonction de la protection de la mémoire tampon des paquets. Commencez par la valeur par défaut, surveillez l'utilisation de la mémoire tampon des paquets ou la latence et ajustez la valeur de la durée, au besoin. • **Block Duration (sec) (Durée de blocage [secondes])** – La période, en secondes, pendant laquelle une session abandonnée reste abandonnée ou pendant laquelle une adresse IP bloquée reste bloquée (la plage est comprise entre 1 et 15 999 999 ; par défaut : 3 600). Utiliser la valeur par défaut, à moins que le blocage d'une adresse IP pendant une heure serait trop sévère pour vos conditions d'affaires, dans ce cas, vous pouvez réduire la durée. Surveillez l'utilisation de la mémoire tampon des paquets ou la latence et ajustez la durée, au besoin. *La traduction de l'adresse réseau (NAT) peut accroître l'utilisation de la mémoire tampon des paquets. Si une telle traduction affecte l'utilisation de la mémoire tampon, réduisez le délai de maintien du blocage pour bloquer les sessions individuelles plus rapidement et réduirez la durée du blocage pour que les autres sessions provenant de l'adresse IP sous-jacente ne soient pas indûment pénalisées.*
Mise en tampon de configuration de route multidiffusion	Sélectionnez cette option (désactivée par défaut) pour activer la mise en tampon de configuration de route multidiffusion, qui permet au pare-feu de préserver le premier paquet dans une session multidiffusion lorsque l'entrée de la route multidiffusion ou la base d'informations de transfert (FIB) n'existe pas encore pour le groupe multidiffusion correspondant. Par défaut, le pare-feu ne procède pas à la mise en tampon du premier paquet multidiffusion dans une nouvelle session ; il utilise plutôt le premier paquet pour paramétrer la route multidiffusion. Ce comportement est normal pour le trafic multicast. Si vos serveurs de contenu sont directement connectés au pare-feu et que votre application personnalisée ne peut pas prendre en charge le premier paquet dans la session en cours de suppression, vous n'avez qu'à activer la mise en tampon de configuration de route multidiffusion.

Paramètres de session	Description
Taille de tampon de configuration de route multidiffusion	Si vous activez la Mise en tampon de configuration de route multidiffusion, vous pouvez régler la taille du tampon, qui spécifie la taille du tampon par flux (plage de 1 à 2 000 ; par défaut 1 000.) Le pare-feu peut mettre en tampon un maximum de 5 000 paquets.

Délais d'expiration de session

Certains délais d'expiration de session définissent la durée pendant laquelle PAN-OS maintient une session sur le pare-feu après son inactivité. Par défaut, lorsque le délai du protocole expire, PAN-OS ferme la session. Le délai d'expiration des sessions en état de rejet définit la durée maximale pendant laquelle une session demeure ouverte après que PAN-OS l'a refusée en fonction des règles de politique de Sécurité.

Vous pouvez définir plus particulièrement un délai d'expiration pour les sessions TCP, UDP, ICMP et SCTP sur le pare-feu. Le délai d'expiration **Default (Par défaut)** s'applique à tout autre type de session. Tous ces délais d'expiration sont globaux, ce qui signifie qu'ils s'appliquent à toutes les sessions de ce type sur le pare-feu.

Outre les paramètres généraux, vous pouvez définir des délais d'expiration pour une application particulière dans l'onglet **Objects (Objets)** > **Applications**. Les délais d'expiration disponibles pour cette application s'affichent dans la fenêtre'A0;Options. Le pare-feu applique les délais d'expiration d'application à une application qui se trouve dans un état établi. Une fois configurés, les délais d'expiration d'une application remplacent les délais d'expiration de session TCP, UDP ou SCTP généraux.

Les options de cette section vous permettent de configurer les paramètres d'expiration de session généraux (spécifiquement pour les sessions TCP, UDP, ICMP, SCTP ainsi que pour tous les autres types de sessions).

Les valeurs par défaut sont des valeurs optimales et il est recommandé d'utiliser les valeurs par défaut. Toutefois, vous pouvez les modifier selon vos besoins en matière de réseau. La définition d'une valeur trop faible peut engendrer une certaine sensibilité aux retards mineurs sur le réseau et une impossibilité d'établir une connexion avec le pare-feu, tandis qu'une valeur trop élevée peut entraîner un retard dans la détection des échecs.

Paramètres de délais d'expiration de session	Description
Default (Par défaut)	Durée maximale, en secondes, pendant laquelle une session non TCP/UDP, non SCTP ou non ICMP peut être ouverte sans aucune réponse (plage de 1 à 15 999 999 ; par défaut 30).
Supprimer les valeurs par défaut	Durée maximale (en secondes) pendant laquelle une session non TCP/UDP/ SCTP reste ouverte après que PAN-OS l'a refusée en fonction des règles de politiques de Sécurité configurées sur le pare-feu (plage entre 1 et 15 999 999, par défaut 60).
Supprimer TCP	Durée maximale(en secondes) pendant laquelle une session TCP reste ouverte après que PAN-OS l'a refusée en fonction des règles de politiques

Paramètres de délais d'expiration de session	Description
	de Sécurité configurées sur le pare-feu (plage entre 1 et 15 999 999, par défaut 90).
Supprimer UDP	Durée maximale (en secondes) pendant laquelle une session UDP reste ouverte après que PAN-OS l'a refusée en fonction des règles de politiques de Sécurité configurées sur le pare-feu (plage entre 1 et 15 999 999, par défaut 60).
ICMP	Durée maximale pendant laquelle une session ICMP peut être ouverte sans aucune réponse ICMP (plage de 1 à 15 999 999 ; par défaut 6).
Balayage	Durée maximal, en secondes, pendant laquelle une session peut rester inactive avant que le pare-feu arrête la session et récupère les ressources de la mémoire tampon que la session utilisait. Le temps d'inactivité est le temps qui a passé depuis que la session a été actualisée pour la dernière fois par un paquet ou un événement. La plage est comprise entre 5 et 30 ; la valeur par défaut est 10.
TCP	Durée maximale pendant laquelle une session TCP reste ouverte sans aucune réponse TCP, une fois qu'une session TCP se trouve dans un état Établi (après que la liaison a été établie et/ou que les données ont été transmises) ; (plage de 1 à 15 999 999 ; par défaut 3 600).
Établissement de liaison TCP	Durée maximale, en secondes, entre la réception du paquet SYN-ACK et le paquet ACK suivant pour complètement établir la session (plages de 1 à 60 ; par défaut 10).
Initialisation TCP	Durée maximale, en secondes, entre la réception du paquet SYN et le paquet SYN-ACK avant de démarrer le minuteur d'établissement de liaison TCP (plages de 1 à 60 ; par défaut 5).
Délai d'attente des sessions TCP à moitié fermées	Durée maximale, en secondes, entre la réception du premier paquet FIN et celle du second paquet FIN ou RST (plage de 1 à 604 800 ; par défaut 120).
Délai d'attente des sessions TCP en état time_wait	Durée maximale, en secondes, après la réception du second paquet FIN ou RST (plages de 1 à 600 ; par défaut 15).
RST non vérifié	Durée maximale, en secondes, après la réception d'un paquet RST qui ne peut pas être vérifié (le paquet RST se trouve dans la fenêtre TCP, mais dispose d'un numéro de séquence inattendu ou provient d'un chemin asymétrique) ; (plages de 1 à 600 ; par défaut 30).
UDP	Durée maximale, en secondes, pendant laquelle une session UDP reste ouverte sans aucune réponse UDP (plage de 1 à 1 599 999 ; par défaut 30).

Paramètres de délais d’expiration de session	Description
Authentication Portal (Portail d’authentification)	Le délai d’expiration de session d’authentification, en secondes, du formulaire Web du Portail d’authentification (par défaut 30, plage de 1 à 1 599 999). Pour accéder au contenu demandé, l'utilisateur doit saisir les informations d'identification d'authentification dans ce formulaire et être authentifié avec succès. Le délai d’expiration de session d’authentification, en secondes, du formulaire Web du Portail d’authentification (par défaut 30, plage de 1 à 1 599 999). Pour accéder au contenu demandé, l'utilisateur doit saisir les informations d'identification d'authentification dans ce formulaire et être authentifié avec succès.
SCTP INIT	Durée de temps maximale, en secondes, après la réception d’un bloc SCTP INIT au cours de laquelle le pare-feu doit recevoir le bloc INIT ACK avant que le pare-feu n’arrête l’initiation de l’association SCTP (plage comprise entre 1 et 60 ; par défaut 5).
SCTP COOKIE	Durée de temps maximale, en secondes, après la réception d’un bloc SCTP INIT ACK avec paramètre d’état COOKIE, au cours de laquelle le pare-feu doit recevoir le bloc COOKIE ECHO avant que le pare-feu n’arrête l’initiation de l’association SCTP (plage comprise entre 1 et 600 ; par défaut 60).
Supprimer SCTP	Durée maximale, en secondes, pendant laquelle une association SCTP reste ouverte après que PAN-OS a refusé la session en fonction des règles de politique de Sécurité configurées sur le pare-feu (plage entre 1 et 604 800 ; par défaut 30).
SCTP	Durée de temps maximale, en secondes, qui peut s’écouler sans qu’aucun trafic SCTP pour association ne se présente avant que toutes les sessions de l’association n’expirent (plage comprise entre 1 et 604 800 ; par défaut 3 600).
Arrêt SCTP	Durée de temps maximale, en secondes, que le pare-feu attend qu’un bloc SHUTDOWN SCTP reçoive un bloc SHUTDOWN ACK avant que le pare-feu n’ignore le bloc SHUTDOWN (plage comprise entre 1 et 600 ; par défaut 30).

Paramètres TCP

Le tableau suivant décrit les paramètres TCP.

Paramètres TCP	Description
Transférer les segments excédant le nombre permis par la file d'attente TCP hors service	Sélectionnez cette option si vous souhaitez que le pare-feu transfère les segments qui dépassent la limite de 64 par session permise par la file d'attente TCP hors service. Si vous désactivez cette option, le pare-feu supprime les segments qui dépassent la limite de la file d'attente hors service. Pour afficher un décompte du nombre de segments que le pare-feu a supprimé en raison de l'activation cette option, exécutez la commande CLI suivante : `afficher le compteur tcp_exceed_flow_seg_limit mondial` *Cette option est désactivée par défaut et devrait le rester pour garantir un déploiement plus sécurisé. La désactivation de cette option peut entraîner une augmentation de la latence sur le flux spécifique ayant reçu plus de 64 segments hors service. Il ne devrait pas y avoir de perte de connectivité étant donné que la pile TCP doit gérer la retransmission des segments manquants.*
Autoriser le défi ACK / Autoriser l'ACK arbitraire en réponse à SYN	Activez cette option pour autoriser une réponse à un ACK de défi (également appelé ACK arbitraire) dans les cas où le serveur répond au SYN client avec un ACK au lieu d'un SYN/ACK. Par exemple, les ACK de défi peuvent être envoyés à partir du serveur à des fins d'atténuation des attaques, et l'activation de ce paramètre sur le pare-feu permet la communication entre le client et le serveur afin que le processus ACK de défi puisse être terminé même lorsque la négociation est hors d'état ou hors séquence.
Supprimer les segments dont l'option d'horodatage est invalide	L'horodatage TCP enregistre le moment où le segment a été envoyé et autorise le pare-feu à vérifier que l'horodatage est valide pour cette session, ce qui empêche le numéro de séquence TCP d'être englobé. L'horodatage TCP est également utilisé pour calculer le temps d'aller-retour. Si cette option est activée, le pare-feu supprime les paquets dont l'horodatage est invalide. Pour afficher un décompte du nombre de segments que le pare-feu a supprimé en raison de l'activation cette option, exécutez la commande CLI suivante : `afficher le compteur tcp_invalid_ts_option mondial`

Paramètres TCP	Description
	Cette option est activée par défaut et devrait le rester pour garantir un déploiement plus sécurisé. L'activation de cette option ne doit pas entraîner une dégradation des performances. Toutefois, si une pile de réseau génère incorrectement des segments dont la valeur de l'option d'horodatage TCP est invalide, le fait d'activer cette option peut entraîner des problèmes de connectivité.
Chemin asymétrique	Réglez globalement si des paquets contenant des ACK désynchronisés ou des numéros de séquence hors de la fenêtre doivent être supprimés ou ignorés. • **Drop (supprimer)** - Supprimez des paquets contenant un chemin asymétrique. • **Bypass (ignorer)** - Ignorez l'analyse de paquets contenant un chemin asymétrique. *Pour contrôler le paramètre des profiles de protection de zone individuels, modifiez le paramètre **Asymmetric Path (chemin asymétrique)** dans* Abandon de TCP.
Indicateur de données urgentes	Utilisez cette option pour configurer si le pare-feu permet ou non l'utilisation du pointeur urgent (indicateur bit URG) dans l'en-tête TCP. Le pointeur urgent figurant dans l'en-tête TCP permet de promouvoir un paquet pour un traitement immédiat ; le pare-feu le supprime de la file d'attente de traitement et l'envoie vers la pile TCP/IP de l'hôte. Ce processus est appelé 'AB; traitement hors bande 'BB;. Étant donné que l'implémentation du pointeur urgent varie selon l'hôte, sélectionnez cette option pour **Effacer** (le paramètre par défaut et recommandé) afin d'éviter toute ambiguïté, en interdisant le traitement hors bande pour que le bit hors bande de la charge utile soit intégré à la charge utile et que le paquet ne soit pas traité en urgence. En outre, le paramètre **Effacer** garantit que le pare-feu identifie le flux exact dans la pile du protocole en tant qu'hôte à qui le paquet est destiné. Pour afficher un décompte du nombre de segments dans lesquels le pare-feu a effacé l'indicateur URG lorsque cette option est définie sur **Effacer**, exécutez la commande CLI suivante : `afficher le compteur tcp_clear_urg global`

Paramètres TCP	Description
	*Par défaut, cet indicateur est défini sur **Effacer** et devrait le rester pour garantir un déploiement plus sécurisé. Cela ne devrait pas entraîner une dégradation des performances ; dans les rares cas où les applications, telles que telnet, utilisent la fonction données urgentes, le protocole TCP peut être affecté. Si vous définissez cet indicateur sur **Do Not Modify Ne pas modifier**, le pare-feu autorise les paquets portant l'indicateur bit URG dans l'en-tête TCP et permet le traitement hors-bande (not recommnded (non recommandé)).*
Supprimer les segments sans indicateur	Les segments TCP illégaux qui ne disposent d'aucun indicateur peuvent être utilisés pour échapper à l'inspection du contenu. Si cette option est activée (par défaut), le pare-feu supprime les paquets qui ne disposent d'aucun indicateur dans l'en-tête TCP. Pour afficher un décompte du nombre de segments que le pare-feu a supprimés en raison de la définition de cette option, exécutez la commande CLI suivante : `afficher le compteur tcp_flag_zero global` *Cette option est activée par défaut et devrait le rester pour garantir un déploiement plus sécurisé. L'activation de cette option ne doit pas entraîner une dégradation des performances. Toutefois, si une pile de réseau génère incorrectement des segments sans indicateur TCP, le fait d'activer cette option peut entraîner des problèmes de connectivité.*
Supprimer l'option MPTCP	Activé globalement par défaut pour convertir les connexions MPTCP (TCP à chemins multiples) en connexions TCP standards. *Pour autoriser MCTCP, modifier le paramètre **Multipath TCP (MPTCP) Options (Options TCP à chemins multiples)** dans Abandon de TCP.*
Texte en clair SIP TCP	Sélectionnez une des options suivantes pour régler le comportement proxy en texte en clair pour les sessions SIP TCP lorsqu'un en-tête segmenté SIP est détecté. • **Always Off (toujours éteint)** : Désactive le proxy de texte en clair. Désactivez le proxy lorsque la taille du message SIP est en général plus petit que le MSS et lorsque les messages SIP entrent dans un seul segment, ou si vous avez besoin d'assurer que les ressources proxy TCP sont réservées pour le proxy de transfert SSL ou HTTP/2.

Paramètres TCP	Description
	• **Always enabled (toujours activé)** : Par défaut. Utilise le proxy TCP pour tous les SIP par les sessions TCP pour aider à corriger le réassemblage et l'ordre des segments TCP pour un bon fonctionnement ALG. • **Automatically enable proxy when needed (Activer le proxy automatiquement lorsque cela est nécessaire)**: lorsque cette option est activée, le proxy de texte en clair est automatiquement activé pour les sessions lorsque ALG détecte une fragmentation de message SIP. Aide à optimiser le proxy lorsqu'il est aussi utilisé pour le proxy de transfert SSL ou HTTP/2.
Scan de retransmission TCP (PAN-OS 10.0.2 or later (PAN-OS 10.0.2 ou version ultérieure))	Si cette option est activée, le checksum du paquet original est scanné lorsqu'un paquet retransmis est repéré. S'il y a une différence de checksum entre le paquet original et le paquet retransmis, le paquet retransmis est supposé être malveillant et st supprimé.

Paramètres de décryptage : Vérification de la révocation du certificat

Sélectionnez **Session**, puis dans les Paramètres de déchiffrement, sélectionnez **Vérification de la révocation du certificat** pour définir les paramètres décrits dans le tableau suivant.

Caractéristiques de la session: paramètres de vérification de la révocation du certificat	Description
Activer : CRL	Sélectionnez cette option pour utiliser la méthode de liste de révocation du certificat (CRL) afin de vérifier l'état de révocation des certificats. Si vous activez également le protocole OCSP (Online Certificate Status Protocol), le pare-feu essaie d'abord OCSP ; si le serveur OCSP est indisponible, le pare-feu essaie alors la méthode CRL. Pour plus d'informations sur les certificats de déchiffrement, voir Clés et certificats de déchiffrement.
Délai de réception: CRL	Si vous avez activé la méthode CRL pour vérifier l'état de révocation des certificats, indiquez l'intervalle en secondes (1 à 60 ; 5 par défaut) après lequel le pare-feu n'attend plus la réponse du service CRL.
Activer : OCSP	Sélectionnez cette option pour utiliser OCSP afin de vérifier l'état de révocation des certificats.
Délai de réception: OCSP	Si vous avez activé la méthode OCSP pour vérifier l'état de révocation des certificats, indiquez l'intervalle en secondes (1 à 60 ; 5 par défaut) après lequel le pare-feu n'attend plus la réponse du répondeur OCSP.

Caractéristiques de la session: paramètres de vérification de la révocation du certificat	Description
Bloquer une session dont l'état du certificat est inconnu	Sélectionnez cette option pour bloquer les sessions SSL/TLS lorsque le service OCSP ou CRL renvoie un état de révocation de certificat inconnu. Sinon, le pare-feu poursuit la session.
Bloquer une session dont le délai d'attente de vérification de l'état du certificat a expiré	Sélectionnez cette option pour bloquer les sessions SSL/TLS une fois que le pare-feu a enregistré un délai d'expiration de la demande OCSP ou CRL. Sinon, le pare-feu poursuit la session.
Délai d'expiration du statut du certificat	Indiquez l'intervalle en secondes (1 à 60 ; 5 par défaut) après lequel le pare-feu n'attend plus la réponse d'aucun service d'état de certificat et applique la logique de blocage de la session que vous avez éventuellement définie. Le **Délai d'expiration du statut du certificat** correspond au **Délai de réception** des méthodes OCSP/CRL de la manière suivante : • Si vous activez les deux méthodes, OCSP et CRL : le pare-feu enregistre un délai d'expiration de la demande après l'expiration de la plus courte des deux durées : la valeur **Certificate Status Timeout (Délai d'expiration du statut du certificat)** ou l'agrégation des deux valeurs **Receive Timeout (Délai de réception)**. • Si vous activez uniquement la méthode OCSP : le pare-feu enregistre un délai d'expiration de la demande après l'expiration de la plus courte des deux durées : la valeur **Certificate Status Timeout (Délai d'expiration du statut du certificat)** ou la valeur **Receive Timeout (Délai de réception)** par la méthode OCSP. • Si vous activez uniquement la méthode CRL : le pare-feu enregistre un délai d'expiration de la demande après l'expiration de la plus courte des deux durées : la valeur **Délai d'expiration du statut du certificat** ou la valeur **Délai de réception** par la méthode CRL.

Paramètres de décryptage : Paramètres de certificat du serveur proxy de transfert

Dans les paramètres de décryptage (onglet **Session**), sélectionnez **Paramètres du proxy de transfert SSL** pour configurer la **Taille de la clé RSA** ou **Taille de la clé ECDSA** et l'algorithme de hachage des certificats que le pare-feu présente aux clients lors de l'établissement de sessions pour le déchiffrement du proxy de transfert SSL/TLS. Le tableau suivant décrit ces paramètres.

Caractéristiques de la session: Paramètres de certificat du serveur proxy de transfert	
Taille de la clé RSA	Sélectionnez l'une des options suivantes :

Caractéristiques de la session: Paramètres de certificat du serveur proxy de transfert	
	• **Définie par l'hôte de destination** (par défaut) : sélectionnez cette option si vous souhaitez que le pare-feu génère des certificats en fonction de la clé utilisée par le serveur de destination : • Si le serveur utilise une clé RSA de 1 024 bits, le pare-feu génère un certificat avec cette taille de clé et un algorithme de hachage SHA1. • Si le serveur de destination utilise une taille de clé supérieure à 1 024 bits (par exemple, 2 048 ou 4 096 bits), le pare-feu générera un certificat qui utilisera une clé de 2 048 bits et un algorithme de hachage SHA-256. • **1024-bit RSA** : sélectionnez cette option si vous souhaitez que le pare-feu génère des certificats qui utilisent une clé RSA de 1 024 bits et l'algorithme de hachage SHA-256, quelle que soit la taille de clé utilisée par le serveur de destination. Depuis le 31 décembre 2013, les Certificate Authorities (autorités de certification - CA) publiques et les navigateurs les plus courants ont limité la prise en charge des certificats X.509 qui utilisent des clés de moins de 2 048 bits. À l'avenir, selon les paramètres de sécurité définis, un navigateur peut avertir l'utilisateur ou bloquer entièrement la session SSL/TLS lorsque de telles clés lui sont présentées. • **2048-bit RSA** : sélectionnez cette option si vous souhaitez que le pare-feu génère des certificats qui utilisent une clé RSA de 2 048 bits et l'algorithme de hachage SHA-256, quelle que soit la taille de clé utilisée par le serveur de destination. Les CA publiques et les navigateurs les plus courants prennent en charge les clés de 2 048 bits qui offrent une meilleure sécurité que les clés de 1 024 bits.
Taille de la clé ECDSA	Sélectionnez l'une des options suivantes : • **Définie par l'hôte de destination** (par défaut) : sélectionnez cette option si vous souhaitez que le pare-feu génère des certificats en fonction de la clé utilisée par le serveur de destination : • Si le serveur utilise une clé ECDSA de 256 bits ou de 384 bits, le pare-feu génère un certificat avec cette taille de clé. • Si le serveur de destination utilise une taille de clé supérieure à 384 bits, le pare-feu générera un certificat qui utilisera une clé de 521 bits. • **256-bit ECDSA** : sélectionnez cette option si vous souhaitez que le pare-feu génère des certificats qui utilisent une clé ECDSA de 256 bits, quelle que soit la taille de clé utilisée par le serveur de destination. • **384-bit ECDSA** : sélectionnez cette option si vous souhaitez que le pare-feu génère des certificats qui utilisent une clé ECDSA de 384 bits, quelle que soit la taille de clé utilisée par le serveur de destination.

Paramètres de décryptage : Paramètres de décryptage SSL

Sélectionnez **SSL Decryption Settings (Paramètres de décryptage SSL)** pour enable inspection of SSL/TLS handshakes (activer l'inspection des négociations SSL/TLS) lorsque les utilisateurs naviguent vers des sites Web via une connexion HTTPS décryptée. Le moteur de détection de contenu et de menaces (CTD) sur le pare-feu évaluera le contenu de la poignée de main par rapport aux règles de la politique de sécurité, ce qui permet au pare-feu d'appliquer les règles le plus tôt possible dans la session. Vous devez disposer d'un abonnement au filtrage d'URL, configurer le SSL Forward Proxy (proxy de transfert SSL) ou SSL Inbound Inspection (inspection SSL entrante) et bloquer des catégories d'URL spécifiques dans vos règles de stratégie de sécurité pour utiliser cette fonctionnalité.

Les pages de réponse du filtrage d'URL ne s'affichent pas pour les sites bloqués lors de l'inspection d'établissement de liaison SSL/TLS. Après avoir détecté le trafic des catégories bloquées, le pare-feu réinitialise la connexion HTTPS, mettant fin à la poignée de main et empêchant la notification de l'utilisateur par page de réponse. Au lieu de cela, le navigateur affiche un message d'erreur de connexion standard.

Paramètres de décryptage SSL	Description
Envoyer les messages d'établissement de connexion à CTD pour inspection	Sélectionnez cette option pour permettre à CTD d'inspecter les liaisons SSL/TLS pendant les sessions Web déchiffrées.

Paramètres de session VPN

Sélectionnez **Session**, puis dans Paramètres de session VPN, configurez les paramètres généraux liés au pare-feu établissant une session VPN. Le tableau suivant décrit ces paramètres.

Paramètres de session VPN	Description
Seuil d'activation du cookie	Indiquez un nombre maximum de SA IKE demi-ouvertes IKEv2 autorisés par pare-feu, au-dessus duquel une validation du cookie est effectuée. Lorsque le nombre de SA IKE demi-ouvertes est supérieur au Seuil d'activation du cookie, le répondeur demande un cookie, et l'initiateur doit répondre par un IKE_SA_INIT contenant un cookie. Si la validation du cookie réussit, une autre session SA peut être ouverte. Une valeur de 0 signifie que la validation du cookie est toujours activée. Le Seuil d'activation du cookie est un paramètre de pare-feu global et il doit être inférieur au paramètre Nombre max de SA demi-ouvertes, qui est également global (plage comprise entre 0 et 65 535 ; par défaut 500).
Nombre max de SA demi-ouvertes	Indiquez le nombre maximum de SA IKE demi-ouvertes IKEv2 que les initiateurs peuvent envoyer au pare-feu sans obtenir de réponse. Une fois le nombre maximum atteint, le pare-feu ne répondra pas aux nouveaux paquets IKE_SA_INIT (plage comprise entre 1 et 65 535 ; par défaut 65 535).

Paramètres de session VPN	Description
Certificats mis en mémoire cache max	Indiquez le nombre maximum de certificats d'autorité de certification (AC) homologues récupérés via HTTP que le pare-feu peut mettre en mémoire cache. Cette valeur est utilisée uniquement par le Hachage IKEv2 et la fonction d’URL (plage comprise entre 1 et 4 000 ; par défaut 500).

Appareil > Configuration > ACE

Activez ou désactivez App-ID Cloud Engine (ACE). ACE est désactivé par défaut. Pour activer ACE, cochez la case afin qu'ACE ne soit pas désactivé.

Vous devez disposer d'une licence SaaS Security Inline valide sur le pare-feu pour utiliser ACE. Si vous n'avez pas de licence SaaS Security Inline sur un pare-feu, ce pare-feu ne peut pas installer les identifiants d'application ACE ou les utiliser dans la politique de sécurité. Panorama ne nécessite pas de licence pour gérer les pare-feux qui utilisent ACE.

Périphérique > Configuration > DLP

- **Périphérique** > **setup** > **DLP**

Configurez les paramètres réseau pour les fichiers numérisés vers le service cloud Enterprise Data Loss Prevention (DLP).

Champ	Description
Latence maximale (s)	Spécifiez la latence maximale en secondes (entre **1** et **240**) pour un téléchargement de fichier avant qu'une action ne soit prise par le pare-feu. La valeur par défaut est **60**.
Action sur la latence maximale	Spécifiez l'action que le pare-feu prend lorsqu'une latence de téléchargement de fichier atteint la **latence maximale** configurée. • **Allow (Autoriser)** (par défaut) : le pare-feu permet à un téléchargement de fichier de continuer vers le service cloud DLP lorsque la latence maximale est atteinte. • **Block (Bloquer)** : le pare-feu bloque un téléchargement de fichier vers le service cloud DLP qui atteint la latence maximale configurée.
Taille maximale du fichier (Mo)	Appliquez une taille de fichier maximale (entre **1** et **20**) pour le téléchargement vers le service cloud DLP. La valeur par défaut est **20**.
Action sur la taille maximale du fichier	Spécifiez l'action que le pare-feu prend lorsqu'un téléchargement de fichier atteint la **Max File Sized (taille maximale de fichier)** configurée. • **Allow (Autoriser)** (par défaut) : le pare-feu permet à un téléchargement de fichier de continuer vers le service cloud DLP si le fichier a la taille de fichier maximale configurée. • **Block (Bloquer)** : le pare-feu bloque un téléchargement de fichier vers le service cloud DLP si le fichier a la taille de fichier maximale configurée.
Fichiers journaux non analysés	Cochez (activez) pour générer une alerte dans le journal de filtrage des données lorsqu'un fichier n'a pas pu être téléchargé sur le service cloud DLP.
Action sur n'importe quelle erreur	Spécifiez l'action que le pare-feu prend lorsqu'une erreur est rencontrée lors d'un téléchargement de fichier vers le service cloud DLP.

Champ	Description
	• **Allow (Autoriser)** (par défaut) : le pare-feu permet à un téléchargement de fichier de continuer vers le service cloud DLP si une erreur est rencontrée lors du téléchargement. • **Block (Bloquer)** : le pare-feu bloque un téléchargement de fichier vers le service cloud DLP si une erreur est rencontrée lors du téléchargement.

Périphérique > Haute disponibilité

- Périphérique > Haute disponibilité

Pour la redondance, déployez vos pare-feu Palo Alto Networks de nouvelle génération selon une configuration haute disponibilité de paires HA ou d'un cluster HA. Lorsque deux pare-feux HA fonctionnent en tant que paire HA, il y a deux déploiements HA.

- Actif / passif – Pour ce déploiement, l'homologue actif synchronise en permanence sa configuration et ses informations de session avec l'homologue passif sur deux interfaces dédiées. Dans l'éventualité où survient une interruption matérielle ou logicielle sur le pare-feu actif, le pare-feu passif devient automatiquement actif sans qu'il y ait perte de service. Les déploiements HD actifs/passifs sont pris en charge par tous les modes de l'interface : câble virtuel, couche 2 ou couche 3.
- Actif / actif – Pour ce déploiement, les deux homologues HD sont actifs et traitent le trafic. Ces déploiements sont les plus adaptés pour les scénarios impliquant un routage asymétrique ou dans les cas où vous souhaitez autoriser des protocoles de routage dynamique (OSPF, BGP) pour maintenir le statut actif entre les deux pairs. La HD Active/active est uniquement prise en charge dans les modes d'interface à câble virtuel et de couche 3. En plus des liens HD1 et HD2, des déploiements actifs/actifs exigent une liaison HD3 dédié. La liaison HD3 est utilisée en tant que liaison de transfert des paquets pour la configuration de session et la gestion du trafic asymétrique.

> *Dans une paire HD, les deux homologues doivent être du même modèle, exécuter la même version PAN-OS et la même version du Contenu, et disposer du même ensemble de licences.*
>
> *De plus, pour les pare-feu VM-Series, les deux homologues doivent se trouver sur le même hyperviseur, et le même nombre de cœurs de processeur doit être alloué sur chaque homologue.*

Sur les modèles de pare-feu compatibles, vous pouvez créer un cluster de pare-feux HA pour la survie de la session et entre les centres de données. Si un lien tombe en panne, les sessions basculent sur un autre pare-feu du cluster. Cette synchronisation est utile dans les cas où les homologues HA sont répartis entre plusieurs centres de données ou entre un centre de données actif et un centre de données en veille. Un autre cas d'utilisation est la mise à l'échelle horizontale, dans laquelle vous ajoutez des membres du cluster HA à un seul centre de données pour augmenter la sécurité et assurer la survie des sessions. Les homologues HA peuvent appartenir à un cluster HA et ils comptent alors comme deux pare-feux dans le cluster. Le nombre de pare-feux compatibles dans un cluster HA dépend du modèle de pare-feu.

- Considérations importantes pour la configuration HD
- HA Paramètres généraux
- Communications HA
- Surveillance des chemins et des liens HA
- Actif HA/Config active
- Config. du cluster

Considérations importantes pour la configuration HD

Les points suivants sont importants lors de la configuration d'une paire HA.

- Le sous-réseau utilisé pour l'adresse'A0;IP locale et d'homologue ne doit pas être réutilisé sur le routeur virtuel.
- Les versions OS et du Contenu doivent être identiques sur les deux pare-feu. Une disparité peut empêcher les pare-feu de l'homologue de se synchroniser.
- Les voyants sont verts sur les ports HD du pare-feu actif et orange sur le pare-feu passif.
- Pour comparer les configurations des pare-feu local et homologue à l'aide l'outil **Config Audit (Audit de configuration)** de l'onglet **Device (Périphérique)**, sélectionnez la configuration locale souhaitée dans la zone de sélection de gauche et la configuration de l'homologue dans la zone de sélection de droite.
- Synchronisez les pare-feu via l'interface Web en cliquant sur **Push Configuration (Diffuser la configuration)** dans le widget HD du **Dashboard (Tableau de bord)**. La configuration du pare-feu duquel vous diffusez la configuration remplace celle présente sur le pare-feu homologue. Pour synchroniser les pare-feu à partir de la CLI du pare-feu actif, utilisez la commande request high-availability sync-to-remote running-config.

Dans une configuration HD active/passive comportant des pare-feu qui utilisent des ports 10 gigabits SFP+, lorsqu'un basculement a lieu et que le pare-feu actif passe à l'état passif, le port 10 gigabits Ethernet est désactivé puis réactivé afin d'être actualisé, mais il ne permet pas la transmission jusqu'à ce que le pare-feu soit de nouveau actif. Si vous disposez d'un logiciel de surveillance sur le périphérique voisin, il indique le bagotement du port, car ce dernier devient inactif, puis de nouveau actif. Ce qui n'est pas le cas avec les autres ports, notamment le port 1 gigabit Ethernet, qui est désactivé, mais qui permet encore la transmission ; par conséquent, le bagotement n'est pas détecté par le périphérique voisin.

HA Paramètres généraux

- Périphérique > Haute disponibilité > Généralités

Pour configurer les paires haute disponibilité (HA) ou les membres du cluster HA, commencez par sélectionner **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **General (Généralités)** et configurez les paramètres généraux.

Paramètres HA	Description
Onglet Général	
Paramètres de la paire HA — Configuration	**Enable HA Pair (Activer la paire HA)** pour activer la fonctionnalité de paire HA et accéder aux paramètres suivants : • **Group ID (ID du groupe)** : saisissez un numéro pour identifier la paire HD (1 à 63). Ce champ est requis (et doit être unique) si plusieurs paires HD résident sur le même domaine de diffusion. • **Description** – (Facultatif) Saisissez une description pour la paire HD. • **Mode** : définissez le type de déploiement HD : **Active Passive (Actif passif)** ou **Active Active (Actif actif)**.

Paramètres HA	Description
	• **Device ID (ID de périphérique)** : dans la configuration active/active, définissez l'ID de périphérique pour déterminer quel homologue sera actif principal (définissez l'**Device ID (ID de périphérique)** à **0**) et lequel sera actif secondaire (définissez l'**Device ID (ID de périphérique)** à **1**). • **Enable Config Sync (Activer la synchronisation de la configuration)** : sélectionnez cette option pour activer la synchronisation des paramètres de configuration entre les homologues. *Activez la synchronisation de la configuration pour que les deux périphériques disposent toujours de la même configuration et qu'ils traitent le trafic de la même façon.* • **Peer HA1 IP Address (Adresse IP de l'homologue HD1)** : saisissez l'adresse IP de l'interface HD1 du pare-feu de l'homologue. • **Adresse IP de l'homologue HD1 de secours** – Saisissez l'adresse IP de la liaison de contrôle de secours de l'homologue. *Configurez une adresse IP de l'homologue HD1 de secours pour permettre à la liaison de secours de préserver la synchronisation et la mise à jour des pare-feux en cas d'échec de la liaison principale.*
Paramètres Actifs/ Passifs	• **Passive Link State (État passif de la liaison)** : sélectionnez l'une des options suivantes pour spécifier si les liaisons de données sur le pare-feu passif devraient demeurer comme elles sont. Cette option n'est pas disponible sur le pare-feu VM-Series dans AWS. • **Shutdown (Arrêter)** : force l'arrêt de la liaison de l'interface. Il s'agit de l'option par défaut qui empêche la création de boucles dans le réseau. • **Auto** : les liaisons qui possèdent une connectivité physique demeurent les mêmes physiquement, mais dans un état désactivé ; elles ne participent pas à l'apprentissage ARP ou au transfert des paquets. Cette option est utile pour le traitement des temps de convergence lors du basculement puisque le pare-feu gagne du temps pour effectuer la récupération des liaisons. Afin d'éviter des boucles de réseau, ne sélectionnez pas cette option si des interfaces de couche 2 sont configurées sur le pare-feu. *Si aucune interface de couche 2 n'est configurée pour le pare-feu, réglez le **Passive Link State (État passif de la liaison)** sur **auto**.* • **Monitor Fail Hold Down Time (min) (Temps d'attente actif après l'échec de la surveillance (min))** : nombre de minutes pendant lesquelles un pare-feu sera dans un état non fonctionnez avant de devenir passif (plage de 1 à 60). Ce minuteur est utilisé en cas de pulsations ou de

Paramètres HA	Description
	messages hello manqués en raison d'un échec de surveillance des liaisons ou des chemins.
Paramètres de sélection	Définissez ou activez les paramètres suivants'A0;: • **Device Priority (Priorité du périphérique)** : saisissez une valeur de priorité pour identifier le pare-feu actif. Le pare-feu ayant la valeur la plus faible (priorité la plus élevée) devient le pare-feu actif (plage de 0 et 255) lorsque la fonction de préemption est activée sur les deux pare-feu de la paire. • **Preemptive (Préemptif)** : active le pare-feu prioritaire pour qu'il reprenne l'opération active (active/passive) ou active principale (active/active) après la récupération d'un échec. Vous devez activer l'option de préemption sur les deux pare-feus pour que le pare-feu prioritaire puisse reprendre l'opération active ou active principale après la récupération d'un échec. Si ce paramètre est désactivé, le pare-feu de priorité inférieure reste actif ou actif principal même si le pare-feu prioritaire est en cours de récupération suite à un échec.  *La décision d'activer l'option **Preemptive (préemption)** dépend de vos exigences d'affaires. Si vous exigez que le périphérique principal soit le périphérique actif, activez l'option **Preemptive (préemption)** de sorte qu'après la récupération d'un échec, le périphérique principal remplace le périphérique secondaire. Si vous exigez le moins d'événements de basculement possible, désactivez les options **Preemptive (Préemption)** pour qu'après un basculement, la paire HA ne bascule de nouveau pour faire du pare-feu prioritaire le pare-feu principal.* • **Heartbeat Backup (Sauvegarde de pulsation)** : utilise les ports de gestion des pare-feu HD afin d'indiquer un chemin de sauvegarde des messages de pulsations et Hello. L'adresse'A0;IP du port de gestion est partagée avec l'homologue HD via la liaison de contrôle HA1. Aucune configuration supplémentaire n'est requise.  *Activez la **Heartbeat Backup (Sauvegarde des pulsations)** si vous utilisez un port sur bande pour les liaisons HD1 et HD1 de secours. N'activez pas la **Heartbeat Backup (Sauvegarde des pulsations)** si vous utilisez un port de gestion sur bande pour les liaisons HD1 et HD1 de secours.*
	• **HA Timer Settings (Paramètres du minuteur HD)** : sélectionnez l'un des profils prédéfinis : • **Recommended (Recommandé)** : utilisez les paramètres types du minuteur de basculement. À moins que vous soyez certain d'avoir besoin de paramètres différents, il est recommandé d'utiliser les paramètres **Recommended (Recommandés)**.

Paramètres HA	Description
	• **Aggressive (Agressif)** : Utilisation pour des paramètres de minuteur de basculement plus rapide.  *Pour afficher la valeur prédéfinie d'un minuteur inclus dans un profil, sélectionnez **Advanced (Avancé)** et **Load Recommended (Charger le profil recommandé)** ou **Load Aggressive (Charger le profil agressif)**. Les valeurs prédéfinies de votre modèle matériel s'affichent alors à l'écran.* • **Advanced (Avancé)** : vous permet de personnaliser les valeurs de manière à ce qu'elles répondent à vos besoins en matière de réseau pour chacun des minuteurs suivants'A0;: • **Promotion Hold Time (Délai de maintien de promotion)** : nombre de millisecondes pendant lesquelles l'homologue passif (en mode active/passive) ou de l'homologue actif secondaire (en mode active/active) avant de prendre l'état de l'homologue actif ou actif principal après la perte de la communication avec l'homologue HD. Ce délai de maintien démarre après la déclaration de l'échec de l'homologue uniquement. • **Hello Interval (ms) (Intervalle Hello)** : nombre de millisecondes entre l'envoi des paquets hello et la vérification que le programme HD sur l'autre pare-feu est opérationnel (plage de 8 000 à 60 000 ; par défaut 8 000). • **Heartbeat Interval (ms) (Intervalle de pulsation)** : précisez la fréquence de l'échange de messages de pulsations entre les homologues HD sous la forme d'une commande ping ICMP (plage de 1 000 à 60 000 ms ; aucune valeur par défaut).
	• **Flap Max (battement max.)**Un battement est comptabilisé lorsque le pare-feu n'est plus à l'état actif pendant 15'A0;minutes après son dernier état actif. Préciser le nombre maximum de battements autorisés avant que le pare-feu ne soit considéré comme suspendu et que le pare-feu passif ne prenne le relais (plage de 0 à 16 ; par défaut 3). La valeur 0 signifie qu'il n'y a pas de valeur maximum (nombre infini de battements avant que le pare-feu ne devienne actif). • **Preemption Hold Time (Délai de maintien de préemption)** : nombre de minutes que prend un homologue passif ou actif secondaire avant de prendre l'état de l'homologue actif ou actif principal (plage de 1 à 60 ; par défaut 1). • **Monitor Fail Hold Up Time (ms) (Temps d'attente actif après l'échec de la surveillance (ms))** : intervalle de temps en millisecondes pendant lequel le pare-feu reste actif après un échec de surveillance des chemins ou des liaisons. Ce paramètre est recommandé pour empêcher un basculement HD dû à l'instabilité occasionnelle de périphériques à proximité (plage de 0 à 60 000 ; valeur par défaut 0).

Paramètres HA	Description
	• **Additional Master Hold Up Time (ms) (Temps d'attente actif principal supplémentaire (min))** – temps supplémentaire en millisecondes qui s'applique aux mêmes événements que le Temps d'attente actif après l'échec de la surveillance (plage de 0 à 60 000, valeur par défaut 500). Cette durée supplémentaire s'applique uniquement à l'homologue actif en mode active/passive et à l'homologue actif principal en mode active/active. Ce délai est recommandé pour empêcher un basculement lorsque les deux homologues rencontrent le même échec de surveillance des liens ou chemins simultanément.
Paramètres du profil SSH HA	Un type de profil de service SSH qui s'applique aux sessions SSH pour les connexions de gestion des appareils haute disponibilité (HA) sur votre réseau. Pour appliquer un profil HA existant, sélectionnez un profil, cliquez sur **OK**, et **Commit (validez)** votre modification. *Vous devez effectuer un redémarrage de service SSH depuis le CLI pour activer le profil.* Pour plus d'informations, consultez Périphérique > Gestion des certificats > Profil de service SSL.
Paramètres de création de clusters	**Enable Cluster Participation (Activez la participation à un cluster)** pour accéder aux paramètres de création de clusters. Les pare-feux qui sont compatibles avec la création de clusters HA permettent aux clusters des pare-feux membres (individuels ou paires HA dans lesquelles chaque pare-feu dans une paire compte pour le total). Le nombre de membres par cluster qu'un modèle de pare-feu peut supporter est le suivant : • PA-3200 Series : 6 membres • PA-5200 Series : 16 membres • PA-5450 : 8 membres • PA-7080 Series : 4 membres • PA-7050 Series : 6 membres Configurez le cluster : • **Cluster ID (ID de cluster)**, un ID numérique unique pour un cluster HA dans lequel tous les membres peuvent partager l'état de la session (la plage est de 1 à 99 ; il n'y a pas de valeur par défaut). • **Cluster Description (Description du cluster)**—Description brève et utile du cluster. • **Cluster Synchronization Timeout (min) (Délai d'expiration de synchronisation du cluster)** : nombre maximum de minutes que le pare-feu local attend avant de passer à l'état Actif lorsqu'un autre membre du cluster (par exemple, dans un état inconnu) empêche la synchronisation complète du cluster (la plage est de 0 à 30 ; la valeur par défaut est 0).

Paramètres HA	Description
	• **Monitor Fail Hold Down Time (min) (Temps de maintien en cas de panne d'un moniteur)** : nombre de minutes après lequel un lien descendant est testé à nouveau pour voir s'il est à nouveau fonctionnel (la plage est de 1 à 60 ; la valeur par défaut est 1).
Commandes opérationnelles	
Suspendre le périphérique local (ou Rendre fonctionnel le périphérique local)	Pour faire passer l'homologue HA local à l'état suspendu et désactiver temporairement la fonction HA sur celui-ci, utilisez la commande opérationnelle CLI suivante : • **`request high-availability state suspend (demande de suspension d'état de haute disponibilité)`** Pour faire repasser l'homologue HA local suspendu en état de fonctionnement, utilisez la commande opérationnelle CLI : • **`request high-availability state functional (demande de fonctionnement d'état de haute disponibilité)`** Pour tester le basculement, vous pouvez activer le pare-feu actif (ou actif principal).

Communications HA

- Périphérique > Haute disponibilité > Communications HA

Pour configurer des liens HA pour des paires HA ou des clusters HA, sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **HA Communications (Communications HA)**.

Liaisons HA	Description
Liaison de contrôle HA1 / Liaison de contrôle (sauvegarde HA1)	Les pare-feu d'une paire HA utilisent des liaisons HA pour synchroniser des données et gérer des informations d'état. Certains modèles de pare-feu disposent d'une liaison de contrôle dédiée et d'une liaison de contrôle de secours dédiée ; par exemple, les pare-feu PA-5200 Series ont HA1-A et HA1-B. Dans ce cas, vous devriez activer l'option de sauvegarde des pulsations dans Elections Settings (Paramètres de sélection). Si vous utilisez un port HA1 dédié pour la liaison Liaison de contrôle HA et un port de données comme Liaison de contrôle (HA de secours), il est recommandé d'activer l'option Sauvegarde de pulsation. Pour les pare-feu ne disposant pas d'un port HA dédié, le pare-feu PA-220 par exemple, vous devez configurer le port de gestion pour la connexion Liaison de contrôle HA et une interface de port de données doit être définie sur le type HA pour la connexion Liaison de contrôle HA1 de secours. Le port de gestion étant alors utilisé, vous n'avez pas besoin d'activer l'option Sauvegarde de pulsation,

Liaisons HA	Description
	car les sauvegardes des pulsations sont déjà exécutées via la connexion de l'interface de gestion. Sur le pare-feu VM-Series dans AWS, le port de gestion sert de liaison HA1. *Lorsque vous utilisez un port de données pour la liaison de contrôle HA, gardez en tête que les messages de contrôle doivent être transférés entre le panneau de données et le panneau de gestion. Ainsi, en cas d'échec dans le panneau de données, les homologues ne peuvent communiquer les informations relatives à la liaison de contrôle HA et un basculement se produit. Il convient d'utiliser les ports HA dédiés ou, sur les pare-feu ne disposant pas d'un port HA dédié, d'utiliser le port de gestion.*
Liaison de contrôle HA1 / Liaison de contrôle (sauvegarde HA1)	Indiquez les paramètres suivants pour les liaisons de contrôle HA principale et de secours : • **Port** : sélectionnez le port HA des interfaces HA1 principale et de secours. Le paramètre de secours est facultatif. • **IPv4/IPv6 Address (Adresse IPv4/6)** : saisissez l'adresse IPv4 ou IPv6 des interfaces HA1 principale et de secours. Le paramètre de secours est facultatif. *Les pare-feu PA-3200 Series ne prennent pas en charge l'adresse IPv6 pour les interfaces HA1 de secours ; utilisez une adresse IPv4.* • **Netmask (Masque réseau)** – Saisissez le masque réseau de l'adresse IP (255.255.255.0 par exemple) des interfaces HA1 principale et de secours. Le paramètre de secours est facultatif. • **Gateway (Passerelle)** : saisissez l'adresse IP de la passerelle par défaut des interfaces HA1 principale et de secours. Le paramètre de secours est facultatif. • **Link Speed (Vitesse de liaison)** (modèles dotés de ports HA dédiés uniquement) : sélectionnez la vitesse de la liaison de contrôle entre les pare-feu pour le port HA1 dédié. • **Link Duplex (Mode duplex de la liaison)** (modèles dotés de ports HA dédiés uniquement) : sélectionnez une option de duplex pour la liaison de contrôle entre les pare-feu pour le port HA1 dédié. • **Encryption Enabled (Cryptage activé)** : activez le chiffrement après l'exportation de la clé HA de l'homologue HA et son importation sur ce pare-feu. La clé HA de ce pare-feu doit également être exportée depuis ce pare-feu et importée sur l'homologue HA. Configurez ce paramètre pour l'interface

Liaisons HA	Description
	HA1 principale. Importez / exportez des clés sur la page Certificats (voir Périphérique > Gestion des certificats > Profil du certificat). *Activez le chiffrement lorsque les pare-feu ne sont pas directement connectés (les connexions HA1 passent par les périphériques réseau qui peuvent inspecter, traiter ou capturer le trafic).* • **Monitor Hold Time (ms) (Temps d'attente pour la surveillance (ms))** – Saisissez la durée d'attente, en millisecondes, du pare-feu avant de déclarer un échec d'homologue dû à l'échec d'une liaison de contrôle (1 000 à 60 000 ms, par défaut, 3 000 ms). Cette option surveille l'état de la liaison physique des ports HA1.
Liaison de données (HA2)	Indiquez les paramètres suivants pour les liaisons de données principale et de secours'A0;: • **Port** : sélectionnez le port HA. Configurez ce paramètre pour les interfaces HA2 principale et de secours. Le paramètre de secours est facultatif.

Liaisons HA	Description
lorsqu'une liaison de secours HA2 est configurée, un basculement vers la liaison de secours se produit en cas d'échec d'une liaison physique. Lorsque l'option HA2 persistante est activée, le basculement se produit également en cas d'échec des messages de persistance HA dû au seuil défini.	• **IP Address (Adresse IP)** : précisez l'adresse IPv4 ou IPv6 des interfaces HA2 principale et de secours. Le paramètre de secours est facultatif. • **Netmask (Masque réseau)** : précisez le masque réseau des interfaces HA2 principale et de secours. Le paramètre de secours est facultatif. • **Gateway (Passerelle)** : précisez la passerelle par défaut des interfaces HA2 principale et de secours. Le paramètre de secours est facultatif. Si les adresses IP HA2 des pare-feu se trouvent dans le même sous-réseau, le champ Passerelle ne doit pas être renseigné. • **Enable Session Synchronization (Activer la synchronisation de la session)** : activez la synchronisation des informations relatives à la session avec le pare-feu passif, puis choisissez une option de transport. *Activez la synchronisation de la session pour que le périphérique secondaire dispose de la session dans son panneau de données, qui autorise le pare-feu à mettre en correspondance les paquets à la session synchronisée et à transférer rapidement les paquets. Si vous n'activez pas la synchronisation de la session, le pare-feu doit créer la session de nouveau, ce qui introduit la latence et pourrait entraîner l'abandon des connexions.*

Liaisons HA	Description
	• **Transport** : choisissez l'une des options de transport suivantes : • **Ethernet** : utilisez cette option lorsque les pare-feu sont connectés dos-à-dos ou via un commutateur (Ethertype 0x7261). • **IP** : utilisez cette option lorsque le transport de couche 3 est nécessaire (protocole IP n°99). • **UDP** : utilisez cette option pour que la somme de contrôle soit calculée sur l'ensemble du paquet et non sur l'en-tête comme avec l'option IP (port UDP n°29281). L'avantage d'utiliser le mode UDP est la présence de la somme de contrôle UDP pour vérifier l'intégrité d'un message de synchronisation de la session. • (Models with dedicated HA ports only (Modèles dotés de ports HA dédiés uniquement)) **Link Speed (liaison de vitesse)** : sélectionnez la vitesse de la liaison de contrôle entre les homologues pour le port HA2 dédié. • (Models with dedicated HA ports only (Modèles avec ports HA dédiés uniquement)) **Link Duplex (Mode duplex de la liaison)** : sélectionnez une option de duplex pour la liaison de contrôle entre les homologues pour le port HA2 dédié. • **HA2 Keep-alive (HA2 persistante)** : il est recommandé de sélectionner cette option pour surveiller la qualité de la liaison de données HA2 entre les homologues HA. Cette option est désactivée par défaut et vous pouvez l'activer sur un ou les deux homologues. Si cette option est activée, les homologues utiliseront des messages persistants pour surveiller la connexion HA2 afin de détecter une défaillance en fonction du **Threshold (Seuil)** que vous avez défini (par défaut 10 000 ms). Si vous activez la HA2 persistante, l'Action de récupération HA2 persistante sera entreprise. Sélectionnez une **Action** : • **Log Only (Journalisation seulement)** : consigne les défaillances de l'interface HA2 dans le journal système en tant qu'événements critiques. Sélectionnez cette option pour les déploiements actifs/passifs parce que l'homologue actif est le seul pare-feu effectuant le transfert du trafic. L'homologue passif est dans un état de sauvegarde et ne transfère pas le trafic ; ainsi, un chemin de données divisé n'est pas nécessaire. Si vous n'avez pas configuré de liaisons de secours HA2, la synchronisation de l'état sera éteinte. Un journal d'informations est généré en cas de récupération du chemin HA2. • **Split Datapath (Chemin de données divisé)** : sélectionnez cette option dans les déploiements HA actifs/actifs pour indiquer à chaque homologue de prendre possession de leurs tables d'état et de session locaux lorsqu'il détecte une défaillance de l'interface HA2. Aucune synchronisation de l'état et de la session ne peut se produire sans connectivité HA2 ; cette action permet une gestion séparée des tables de session pour assurer le transfert réussi du trafic par chaque homologue HA. Pour éviter cette situation, configurez une liaison de secours HA2.

Liaisons HA	Description
	• **Threshold (ms) (Seuil (ms))** – La durée pendant laquelle les messages de persistance ont échoué avant le déclenchement de l'une des actions ci-dessus (plage de 5 000 à 60 000, par défaut 10 000).
Liens de cluster	Configurer les paramètres des liens HA4 qui sont des liens de cluster HA dédiés qui synchronisent l'état de la session entre tous les membres du cluster qui ont la même ID de cluster. Le lien HA4 entre les membres du cluster détecte des échecs de connectivité entre les membres du cluster. • **Port** : Sélectionnez une interface HA qui sera le lin HA4 (par exemple, ethernet1/1). • **IPv4/IPv6 Address (Adresse IPv4:IPv6)** : Saisissez l'adresse IP de l'interface HA4 locale. • **Netmask (Masque de réseau)** : saisissez le masque de réseau. • **HA4 Keep-alive Threshold (ms) Seuil HA4 Keep-alive (ms))** : Durée pendant laquelle le pare-feu doit recevoir des keepalives d'un membre du cluster afin de savoir que le membre du cluster fonctionne (la plage va de 5 000 à 60 000 ; par défaut 10 000). Configurez les paramètres de sauvegarde HA4 : • **Port** : sélectionnez une interface HA qui sera le lien de sauvegarde HA4. • **IPv4/IPv6 Address (Adresse IPv4/IPv6)** : saisissez l'adresse du lien de sauvegarde HA4 local. • **Netmask (Masque de réseau)** : saisissez le masque de réseau.

Surveillance des chemins et des liens HA

- Périphérique > Haute disponibilité > Surveillance des liens et des chemins

Pour définir les conditions de basculement HA, configurez le lien HA let la surveillance des chemins ; sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **Link and Path Monitoring (Surveillance des liens et des chemins)**.

La surveillance des liaisons et des chemins n'est pas disponible pour le pare-feu VM-Series dans AWS.

Paramètres de surveillance des chemins et des liens HA	Description
Surveillance des liaisons	Indiquez les options suivantes'A0;: • **Enabled (Activé)** : activez la surveillance des liaisons. Elle permet de déclencher un basculement en cas d'échec d'une liaison physique ou d'un groupe de liaisons physiques.

Paramètres de surveillance des chemins et des liens HA	Description
	• **Failure Condition (Condition d'échec)** : sélectionnez cette option en cas de basculement lorsqu'un ou tous les groupes de liaisons surveillés ne répondent pas. *Activez et configurez la surveillance des chemins ou la surveillance des liaisons pour déclencher un basculement en cas d'échec d'un chemin ou d'une liaison. Configurez au moins un **Path Group (Groupe de chemins)** pour la surveillance des chemins et configurez au moins un **Link Group (Groupe de liaisons)** pour la surveillance des liaisons.*
Groupes de liaisons	Définissez un ou plusieurs groupes de liaisons afin de surveiller des liaisons Ethernet spécifiques. Pour ajouter un groupe de liaisons, précisez les informations suivantes, puis cliquez sur **Add (Ajouter)** : • **Name (Nom)** : donnez un nom au groupe de liaisons. • **Enabled (Activé)** : activez le groupe de liaisons. • **Failure Condition (Condition d'échec)** – Sélectionnez en cas d'échec lorsqu'une ou toutes les liaisons sélectionnées sont défaillantes. • **Interfaces** : sélectionnez une ou plusieurs interfaces Ethernet à surveiller.
Surveillance des chemins	Indiquez les options suivantes'A0;: • **Enabled (Activé)** : Active la surveillance des chemins sur la base de la surveillance des chemins Virtual Wire combinée ou indépendante, surveillance des chemins VLAN et surveillance des chemins Routeur virtuel*. La surveillance des chemins permet au pare-feu de surveiller les adresses'A0;IP de destination définies en envoyant des messages ping ICMP afin de vérifier qu'elles répondent. Utilisez la surveillance des chemins pour les configurations à câble virtuel, couche 2 ou couche 3 dans lesquelles la surveillance des autres périphériques du réseau est requise pour le basculement, mais où la surveillance des liaisons seule ne suffit pas. • **Failure Condition (Condition d'échec)**: • **Any (indifférent)**—(par défaut) le pare-feu déclenche un basculement HA lorsque la surveillance des chemins d'un virtual wire ou d'un VLAN ou d'un routeur virtuel* échoue. • **Any (indifférent)**—(par défaut) le pare-feu déclenche un basculement HA lorsque la surveillance des chemins d'un virtual wire ou d'un VLAN ou d'un routeur virtuel* échoue (quel que soit celui des trois qui est activé). **Si vous avez activé Routage avancé, le routeur logique remplace le routeur virtuel et vous pouvez activer la Surveillance des chemins du routeur logique.*

Paramètres de surveillance des chemins et des liens HA	Description
	*Activez et configurez la surveillance des chemins ou la surveillance des liaisons pour déclencher un basculement en cas d'échec d'un chemin ou d'une liaison. Configurez au moins un **Path Group (Groupe de chemins)** pour la surveillance des chemins et configurez au moins un **Link Group (Groupe de liaisons)** pour la surveillance des liaisons.*
Groupe de chemins	Définissez un ou plusieurs groupes de chemins afin de surveiller des adresses de destination spécifiques pour le type d'interface. **Add Virtual Wire Path (Ajouter le chemin Virtual Wire)**, et **Add VLAN Path (Ajouter le chemin VLAN)**, et **Add Virtual Router Path (Ajouter le chemin du routeur virtuel)**. (Si vous avez activé le Routage avancé, vous pouvez **Add Logical Router Path (Ajouter le chemin du routeur logique)**). Pour chaque type de surveillance des chemins que vous ajouté, indiquez ce qui suit : • **Name (Nom)**—Sélectionnez virtual wire, VLAN, ou routeur virtuel* pour surveiller (les choix dans le menu déroulant se basent sur le type de surveillance de chemins que vous ajoutez). • **Source IP (IP source)** : pour les interfaces câble virtuel et VLAN, saisissez l'adresse IP source utilisée dans les pings envoyés au routeur du saut suivant (adresse IP de destination). Le routeur local doit être en mesure de transmettre l'adresse au pare-feu. (L'adresse IP source de groupes de chemins associés aux routeurs virtuels est automatiquement configurée en tant qu'adresse IP de l'interface indiquée dans la table de routage comme interface d'entrée de l'adresse IP de destination définie.) • **Enabled (Activé)**: Active la surveillance de virtual wire, VLAN, ou routeur virtuel*. • **Failure Condition (Condition d'échec)**: • **Any (indifférent)** (par défaut) : le pare-feu détermine que virtual wire, VLAN, ou le routeur virtuel* a échoué quand un échec de ping se produit dans n'importe quel groupe d'IP de destination. • **All (Tous)** : le pare-feu détermine que le virtual wire, VLAN ou routeur virtuel* a échoué lorsqu'un échec de ping se produit dans tous les groupes d'IP. *Le basculement HA réel est déterminé par la Condition d'échec que vous réglez pour la Surveillance des chemins, qui tient compte de la surveillance des chemins virtual wire, VLAN et routeur virtuel* (quel que soit celui que vous avez activé).*

Paramètres de surveillance des chemins et des liens HA	Description
	• **Intervalle des requêtes ping** – Indiquez l'intervalle entre les requêtes ping envoyées à l'adresse de destination (plage de 200 à 60 000 ms ; par défaut 200 ms). • **Ping Count (Nombre de requêtes ping)** – Indiquez le nombre d'échecs de requêtes ping avant de déclarer un échec (plage de 3 à 10 ; par défaut 10).  **Si vous avez activé Routage avancé, le routeur logique remplace le routeur virtuel et vous pouvez activer la Surveillance des chemins du routeur logique.*
IP de destination pour le groupe de chemins	• **Destination IP (IP de destination)—Add (Ajoutez)** un ou plusieurs groupes d'adresses IP de destination à surveiller pour le chemin. • **Destination IP Group (Groupe d'IP de destination)** : saisissez un nom pour le groupe. • **Add (Ajoutez)** une ou plusieurs adresses **IP de destination** à surveiller pour le groupe. • **Enabled (Activé)** : sélectionnez pour activer le groupe d'IP de destination. • **Failure Condition (Condition d'échec)**: Sélectionnez **Any (indifférent)** (pour indiquer sur si un échec de ping se produit pour n'importe quelle adresse IP du groupe, le groupe de destination est considéré comme avoir échoué) ou **All (Toutes)** (pour indiquer sur si un échec de ping se produit pour toutes les adresses IP du groupe, le groupe de destination est considéré comme avoir échoué).

Actif HA/Config active

- Périphérique > Haute disponibilité > Config Active/Active

Pour configurer les paramètres pour une paire HA Active/Active, sélectionnez **Device (Périphérique)** > **High Availability (Haute disponibilité)** > **Active/Active Config (Config Active/Active)**.

Paramètres de Configuration Active/Active	Description
Transfert des paquets	Cliquez sur **Enable (Activer)** pour activer les homologues afin qu'ils transfèrent les paquets vers la liaison HA3 pour la configuration de session et pour l'inspection de la couche 7 (inspection de l'App-ID, du Content-ID et des menaces) des sessions asymétriquement acheminées.

Paramètres de Configuration Active/Active	Description
Interface HA3	Sélectionnez l'interface de données que vous prévoyez utiliser pour transférer des paquets entre les homologues HA actifs/actifs. L'interface que vous utilisez doit être une interface dédiée de couche 2 dont le type d'interface est défini à **HA**. *Si la liaison HA3 échoue, l'homologue actif secondaire passera à l'état non fonctionnel. Pour éviter cette situation, configurez une interface de groupe d'agrégation de liaison (LAG) avec deux ou plusieurs interfaces physiques en tant que liaison HA3. Le pare-feu ne prend pas en charge une liaison de secours HA3. Une interface globale comprenant de multiples interfaces fournira une capacité supplémentaire et une redondance des liaisons pour prendre en charge le transfert des paquets entre les homologues HA.* *Lorsque vous utilisez l'interface HA3, vous devez activer les trames Jumbo sur tous les périphériques réseau intermédiaires.*
Sync VR	Forcez la synchronisation de tous les routeurs virtuels configurés sur les homologues HA. Utilisez cette option lorsque le routeur virtuel n'est pas configuré pour fonctionner avec des protocoles de routage dynamique. Les deux homologues doivent être connectés au même routeur de saut suivant via un réseau commuté et utiliser uniquement un routage statique.
Synchronisation QoS	Synchronisez la sélection du profil de qualité de service (QoS) sur toutes les interfaces physiques. Utilisez cette option lorsque les homologues disposent de vitesses de liaison similaires et que les mêmes profils QoS sont requis sur toutes les interfaces physiques. Ce paramètre s'applique à la synchronisation des paramètres de QoS de l'onglet **Network (Réseau)**. La politique de QoS est synchronisée, quel que soit ce paramètre.
Temps d'attente provisoire (s)	En cas d'échec d'un pare-feu en configuration HA active/active échoue, celui-ci passe à l'état provisoire. La transition de l'état provisoire à l'état actif secondaire déclenche le Temps d'attente provisoire, au cours duquel le pare-feu tente de créer des contiguïtés de routage et de remplir sa table de routage avant de traiter les paquets. Sans ce minuteur, le pare-feu de récupération passe immédiatement à l'état actif/secondaire et rejette silencieusement les paquets, car il ne dispose pas des itinéraires nécessaires (60 secondes par défaut).
Sélection du propriétaire de la session	Le propriétaire de la session est responsable de toutes les inspections de couche 7 (App-ID et Content-ID) de la session et de générer tous les journaux de trafic de la session. Sélectionnez l'une des options suivantes pour spécifier la façon de déterminer le propriétaire de la session pour un paquet :

Paramètres de Configuration Active/Active	Description
	• **First packet (Premier paquet)** : sélectionnez cette option pour désigner le pare-feu qui reçoit le premier paquet dans une session en tant que propriétaire de la session. Il s'agit de la configuration recommandée pour minimiser le trafic sur HA3 et répartir la charge du panneau de données entre les homologues. • **Primary Device (Périphérique principal)** : sélectionnez cette option si vous souhaitez que le pare-feu actif principal accueille toutes les sessions. Dans ce cas, si le pare-feu actif secondaire reçoit le premier paquet, il transfère tous les paquets nécessitant une inspection de couche 7 du pare-feu actif principal sur la liaison HA3.
Adresse virtuelle	Cliquez sur **Add (Ajouter)**, sélectionnez l'onglet **IPv4** ou **IPv6**, puis cliquez à nouveau sur **Add (Ajouter)** pour saisir des options afin de spécifier le type d'adresse virtuelle HA à utiliser : Partage de charge ARP ou flottante Vous pouvez également mélanger le type de types d'adresse virtuelle dans l'homologue. Par exemple, vous pourriez utiliser le partage de charge ARP sur l'interface LAN et une adresse IP flottante sur l'interface WAN. • **Floating (Adresse IP flottante)** : saisissez une adresse IP qui se déplacera entre les homologues HA en cas d'échec d'une liaison ou d'un système. Configurez deux adresses IP flottantes sur l'interface de sorte que chaque pare-feu dispose d'une adresse propre, puis définir la priorité. En cas d'échec de l'un des pare-feu, l'adresse IP flottante est transmise à l'homologue HA. • **Device 0 Priority (Priorité périphérique 0)** : définissez la priorité du pare-feu à ID de périphérique 1 afin de déterminer quel pare-feu dispose de l'adresse IP flottante. Le pare-feu avec la valeur la plus faible dispose de la priorité la plus élevée. • **Device 1 Priority (Priorité périphérique 1)** : définissez la priorité du pare-feu à ID de périphérique 1 afin de déterminer quel pare-feu dispose de l'adresse IP flottante. Le pare-feu avec la valeur la plus faible dispose de la priorité la plus élevée. • **Failover address if link state is down (Adresse de basculement si l'état de liaison est inactif)** : utilisez l'adresse de basculement lorsque l'état de liaison est inactif sur l'interface. • **Floating IP bound to the Active-Primary HA device (Adresse IP flottante liée au périphérique HA actif principal)** : sélectionnez cette option pour lier l'adresse IP flottante à l'homologue actif principal. Dans le cas où un homologue ne fonctionne pas, le trafic est envoyé en continu à l'homologue actif principal, même après le rétablissement du pare-feu défaillant et devient l'homologue actif secondaire.
Adresse virtuelle (suite)	• **ARP Load Sharing (Partage de charge ARP)** : saisissez une adresse IP qui sera partagée par la paire HD et qui fournira des services de passerelle aux hôtes. Cette option est uniquement nécessaire si le pare-feu est situé sur le

Paramètres de Configuration Active/Active	Description
	même domaine de diffusion que les hôtes. Sélectionnez le **Device Selection Algorithm (Algorithme de sélection du périphérique)** : • **IP Modulo (Modulo IP)** : sélectionnez le pare-feu qui répondra aux requêtes ARP en fonction de la parité de l'adresse IP des demandeurs ARP. • **IP Hash (Hachage IP)** : sélectionnez le pare-feu qui répondra aux requêtes ARP en fonction d'un hachage de l'adresse IP des demandeurs ARP.

Config. du cluster

- Périphérique > Haute disponibilité > Config. du cluster

Ajoutez des membres à un cluster en sélectionnant **Périphérique** > **Haute disponibilité** > **Config. du cluster**.

Config. du cluster	Description
Ajouter	Cliquez sur **Ajouter**pour ajouter un membre du cluster. Vous devez ajouter le pare-feu local et si vous utilisez des paires HA, vous devez ajouter les deux homologues HA de la paire en tant que membres du cluster. • (Pare-feux compatibles) **Numéro de série** : Saisissez le numéro de série unique du membre du cluster. • (Panorama) **Périphérique** : Sélectionnez un périphérique dans la liste déroulante et saisissez un **Nom de périphérique**. • **Adresse IP HA4** : Saisissez l'adresse IP du lien HA4 pour le membre du cluster. • **Adresse IP HA4 de secours** : Saisissez l'adresse IP du lien HA4 de secours pour le membre du cluster. • **Synchronisation des sessions** : Sélectionnez la synchronisation des sessions avec ce membre du cluster. • **Description** : Saisissez une description utile.
Supprimer	Sélectionnez un ou plusieurs membres du cluster et **supprimez** ceux-ci du cluster.
Activer	(Pare-feux compatibles) Vous pouvez déterminer si oui ou non un membre du cluster synchronise les sessions avec les autres membres. Par défaut, tous les membres sont autorisés à synchroniser les sessions. Si vous désactivez la synchronisation pour un ou plusieurs membres, sélectionnez **Activer** pour réactiver la synchronisation pour un ou plusieurs membres.

Config. du cluster	Description
Désactiver	(Pare-feux compatibles) Sélectionnez un ou plusieurs membres et **Désactiver** la synchronisation avec les autres membres.
Actualiser	(Panorama) Sélectionnez**Actualiser** pour actualiser la liste des périphériques HA dans le cluster HA.

Périphérique > Carte de transfert des journaux

- Périphérique > Carte de transfert des journaux

La Log Forwarding Card (Carte de transfert des journaux ; LFC) est une carte de journal haute performance qui transfère tous les journaux des panneaux de données (trafic et menace, par exemple) depuis le pare-feu vers un ou plusieurs systèmes de journalisation externes, comme Panorama, Firewall Data Lake ou un serveur syslog. Comme les journaux des panneaux de données ne sont plus disponibles sur le pare-feu local, l'onglet ACC est supprimé de l'interface Web de gestion et **Monitor (Surveiller)** > **Logs (Journaux)**ne contient que les journaux de gestion (Configuration, Système et Alarmes).

Vous devez configurer les ports de la LFC. Si vous configurez LFC 1/1 à l'aide d'un câble de dérivation, vous avez accès à jusqu'à huit ports de dérivation 10G. Cela configure automatiquement les ports 1 à 4 dans la première interface et configure automatiquement les ports 5 à 8 dans la seconde interface. Vous pouvez utiliser une ou les deux interfaces pour fournir une connectivité jusqu'à 40G ou 80G respectivement. Le périphérique lié doit être configuré pour utiliser le LAG pour tous les ports connectés au LFC.

Si vous configurez LFC 1/9, vous avez accès à jusqu'à deux ports 40G. Cela configure automatiquement le port 9 dans la première interface et configure automatiquement le port 10 dans la seconde interface. Vous pouvez utiliser une ou les deux interfaces pour fournir une connectivité jusqu'à 40G ou 80G respectivement. Le périphérique lié doit être configuré pour utiliser le LAG pour tous les ports connectés au LFC.

Le LFC ne prend actuellement pas en charge LACP.

Configurez les ports sous **Device card (Carte de périphérique)** > **Log Forwarding (transfert des journaux**. Le pare-feu utilise ces ports pour transférer les journaux des panneaux de données à un système externe, comme Panorama ou un serveur syslog.

Reportez-vous au Guide de référence matérielle du pare-feu PA-7000 Series pour obtenir des informations sur les exigences et les composants de la LFC.

Pour une interface LFC, configurez les paramètres décrits dans le tableau suivant.

Paramètres d'une interface LFC	Description
(Nom	Saisissez un nom d'interface. Pour un LFC, vous devez sélectionner **lfc1/1** ou **lfc1/9** dans le menu déroulant.
Commentaire	Saisissez une description de l'interface (facultatif).
IPv4	Si votre réseau utilise IPv4, définissez les options suivantes : • **IP address (Adresse IP)** - Adresse IPv4 du port. • **Netmask (Masque réseau)** - Masque réseau de l'adresse IPv4 du port. • **Default Gateway (Passerelle par défaut)** - Adresse IPv4 de la passerelle par défaut du port.

Paramètres d’une interface LFC	Description
IPv6	Si votre réseau utilise IPv6, définissez les options suivantes : • **IP address (Adresse IP)** - Adresse IPv6 du port. • **Default Gateway (Passerelle par défaut)** - Adresse IPv6 de la passerelle par défaut du port.
Vitesse de liaison	Sélectionnez la vitesse de l'interface en Mbits/s (**10000** ou **40000**) ou sélectionnez **auto** (par défaut) pour que le pare-feu détermine automatiquement la vitesse en fonction de la connexion. La vitesse d'interface disponible dépend du Nom utilisé (lfc1/1 ou lfc1/9). **Auto** est la seule option possible pour les interfaces dont la vitesse ne peut être configurée.
état des liaisons	Indiquez si l'état de l'interface est activé (**up (actif)**), désactivé **down (inactif)**) ou automatiquement déterminé en fonction de la connexion (**auto**). La valeur par défaut est **auto**.
Priorité du port LACP	LACP n'est actuellement pas pris en charge sur le LFC.

Les sous-interfaces sont disponibles si vous avez activé la fonctionnalité de systèmes virtuels multiples. Pour configure an LFC subinterface (configurer une sous-interface LFC), ajoutez une sous-interface et utilisez les paramètres décrits dans le tableau suivant.

Le transfert de journaux vers un serveur externe n'est pas encore pris en charge sur les sous-interfaces LFC. Pour transférer les journaux vers un serveur externe, vous devez utiliser l'interface LFC principale.

Paramètres d’une sous-interface LFC	Description
Nom de l'interface	**Nom de l'interface** (en lecture seule) affiche le nom de l'interface de carte de journal sélectionnée. Dans le champ adjacent, saisissez un suffixe numérique (1-9 999) pour identifier la sous-interface.
Commentaire	Saisissez une description de l'interface (facultatif).
Étiquette	Saisissez le **Tag (Étiquette)** VLAN (0-4 094) de la sous-interface. *Donnez à l’étiquette le même numéro que la sous-interface pour simplifier son utilisation.*
système virtuel - vsys	Sélectionnez le système virtuel auquel la sous-interface Carte de transfert des journaux ; LFC est affectée. Sinon, vous pouvez cliquer sur **Systèmes virtuels** pour ajouter un nouveau système virtuel. Une fois qu'une sous-interface LFC est

Paramètres d’une sous-interface LFC	Description
	affectée à un système virtuel, cette interface est utilisée comme interface source pour tous les services qui transfèrent les journaux (Syslog, messagerie, SNMP) depuis la carte de journal.
IPv4	Si votre réseau utilise IPv4, définissez les options suivantes : • **IP address (Adresse IP)** - Adresse IPv4 du port. • **Netmask (Masque réseau)** - Masque réseau de l'adresse IPv4 du port. • **Default Gateway (Passerelle par défaut)** - Adresse IPv4 de la passerelle par défaut du port.
IPv6	Si votre réseau utilise IPv6, définissez les options suivantes : • **IP address (Adresse IP)** - Adresse IPv6 du port. • **Default Gateway (Passerelle par défaut)** - Adresse IPv6 de la passerelle par défaut du port.

Périphérique > Audit de configuration

Sélectionnez **Périphérique** > **Audit de configuration** pour afficher les différences entre les fichiers de configuration. La page affiche les configurations côte à côte dans des volets distincts et met en évidence les différences ligne par ligne en utilisant des codes de couleurs pour indiquer les ajouts (vert), les modifications (jaune) ou les suppressions (rouge) :

Paramètres d’audit de configuration	Description
Menus déroulants de noms de configuration (sans référence)	Sélectionnez deux configurations à comparer dans les menus déroulants de noms de configuration (sans référence) (les valeurs par défaut sont **Configuration active** et **Configuration candidate**). *Vous pouvez filtrer un menu déroulant en saisissant une chaîne de texte dérivée de la valeur **Description** de l’opération de validation associée à la configuration souhaitée (reportez-vous à la section Validation des modifications).*
Menu déroulant Contexte	Utilisez le menu déroulant **Contexte** pour spécifier le nombre de lignes à afficher avant et après que les différences aient été mises en évidence dans chaque fichier. Le fait de spécifier plus de lignes peut vous aider à corréler les résultats de l'audit des paramètres dans l'interface Web. Si vous définissez le **Contexte** à **Tous**, les résultats incluent l'ensemble des fichiers de configuration.
accéder	Cliquez sur **Lancer** pour débuter l'audit.
Précédent (‹‹) et Suivant (››)	Ces flèches de navigation sont activées lorsque des versions de configuration consécutives sont sélectionnées dans les menus déroulants de noms de configuration. Cliquez sur ‹‹ pour comparer la paire précédente de configurations dans les menus déroulants ou cliquez sur ›› pour comparer la prochaine paire de configurations.

Périphérique > Profils de mot de passe

- Périphérique > Profils de mot de passe
- Panorama > Profils de mot de passe

Sélectionnez **Périphérique** > **Profils de mot de passe** ou **Panorama** > **Profils de mot de passe** pour définir les exigences relatives au mot de passe de base pour les comptes locaux individuels. Les profils de mot de passe remplacent tous les paramètres Complexité minimale du mot de passe que vous avez définis pour tous les comptes locaux (**Périphérique** > **Configuration** > **Gestion**).

Pour appliquer un profil de mot de passe à un compte, sélectionnez **Périphérique** > **Administrateurs** (pare-feu) ou à **Panorama** > **Administrateurs** (Panorama), sélectionnez un compte et ensuite choisissez le **Profil de mot de passe**.

Vous ne pouvez pas attribuer des profils de mot de passe à des comptes administratifs qui utilisent l'authentification de la base de données locale (voir Périphérique > Base de données d'utilisateurs locale > Utilisateurs).

Pour créer un profil de mot de passe, cliquez sur **Ajouter** et spécifiez les informations répertoriées dans le tableau suivant.

Paramètres du profil de mot de passe	Description
Nom	Saisissez un nom pour identifier le profil de mot de passe (31 caractères maximum). Celui-ci est sensible aux majuscules et minuscules et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Période de modification du mot de passe requise (jours)	Requiert que les administrateurs modifient régulièrement leurs mots de passe en fonction du nombre de jours défini (plage de 0 à 365 jours). Exemple'A0;: si la valeur est définie sur 90, les administrateurs sont invités à modifier leurs mots de passe tous les 90 jours. Vous pouvez également définir un message d'avertissement d'expiration de 0 à 30 jours et indiquer un délai supplémentaire.
Avertissement avant la date d'expiration (jours)	Si une période de modification du mot de passe requise est définie, ce paramètre peut être utilisé pour demander à l'utilisateur de modifier son mot de passe à chaque connexion à mesure que la date de modification du mot de passe requise approche (plage de 0 à 30).
Nombre d'ouvertures de session Administrateur après expiration	Autorisez l'administrateur à se connecter pour un certain nombre de fois une fois son compte arrivé à expiration. Par exemple, si la valeur est définie sur 3 et que le compte a expiré, il peut se connecter 3 autres fois avant que le compte ne soit verrouillé (plage de 0 à 3).

Paramètres du profil de mot de passe	Description
Période de grâce après expiration (jours)	Autorise l’administrateur à se connecter le nombre de jours indiqué une fois son compte arrivé à expiration (plage de 0 à 30).

Exigences relatives au nom d’utilisateur et au mot de passe

Le tableau suivant répertorie les caractères valides pouvant être utilisés dans les noms d'utilisateurs et les mots de passe des comptes PAN-OS et Panorama.

Account Type (Type de compte)	Restrictions de nom d’utilisateur et de mot de passe
Jeu de caractères du mot de passe	Aucune restriction ne s'applique aux jeux de caractères des mots de passe.
Admin à distance, SSL-VPN ou Portail d’authentification	Les caractères suivants ne sont pas autorisés dans le nom d'utilisateur'A0;: • Apostrophe inversée (`) • Crochets angulaires (< and >) • Perluète (&) • Astérisque (*) • A commercial (@) • Point d'interrogation (?) • Barre verticale (|) • Guillemet simple (‘) • Point-virgule (;) • Guillemet double (") • Dollar ($) • Parenthèses ('(' et ')') • Deux-points (':')
Comptes administrateur locaux	Les caractères suivants sont autorisés dans les noms d'utilisateurs locaux: • Minuscules (a-z) • Majuscules (A-Z) • Chiffres (0-9) • Trait de soulignement (_) • Point (.)

Account Type (Type de compte)	Restrictions de nom d’utilisateur et de mot de passe
	• Trait d'union (-) *les noms d'utilisateurs ne peuvent pas commencer par un tiret (-).* Les noms d'utilisateur administrateur ne peuvent pas être composés uniquement de chiffres. Ils doivent comporter au moins un caractère alphabétique ou un caractère de symbole juridique. Par exemple, **1234_567**, **1234a789_** et **c7897432** sont des noms d'utilisateur valides. **12345678** n'est pas un nom d'utilisateur valide.
Mots de passe de l'administrateur	Les mots et expressions couramment utilisés ne sont pas autorisés comme mots de passe, quelle que soit la combinaison de lettres majuscules et minuscules. *Des exemples de mots et d’expressions couramment utilisés incluent Admin, password, PASSWORD, letmein, pa55word, QwErTy et q1w2e3r4.*

Périphérique > Administrateurs

Les comptes administrateur contrôlent l'accès aux pare-feu et à Panorama. Un administrateur de pare-feu peut disposer d'un accès complet ou en lecture seule à un pare-feu ou à un système virtuel d'un pare-feu. Les pare-feu ont un compte **admin** prédéfini qui dispose d'un accès complet.

Pour définir les administrateurs Panorama, voir Panorama > Périphériques gérés > Récapitulatif.

Les options d'authentification suivantes sont prises en charge:

- Authentification par mot de passe : l'administrateur saisit un nom d'utilisateur et un mot de passe pour se connecter. Aucun certificat n'est requis pour cette authentification. Vous pouvez l'utiliser conjointement avec d'autres profils d'authentification, ou pour l'authentification de base de données locale.
- Authentification du certificat du client (Web) : aucun nom d'utilisateur ni mot de passe n'est requis pour cette authentification ; le certificat suffit pour authentifier l'accès au pare-feu.
- Authentification des clés publiques (SSH) : l'administrateur génère une paire de clés publique/privée sur la machine qui doit accéder au pare-feu, puis charge la clé publique sur le pare-feu pour permettre un accès sécurisé sans devoir saisir un nom d'utilisateur ni un mot de passe.

Pour ajouter un administrateur, cliquez sur **Ajouter** et renseignez les informations suivantes :

Paramètres du compte administrateur	Description
Nom	Donnez un nom de connexion à l'administrateur (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. N'utilisez que des lettres, des chiffres, des tirets, des points et des caractères de soulignement. les noms d'utilisateurs ne peuvent pas commencer par un tiret (-).
Profil d'authentification	Sélectionnez un profil d'authentification pour l'authentification de l'administrateur Vous pouvez utiliser ce paramètre pour l’authentification RADIUS, TACACS+, LDAP, Kerberos, SAML ou de base de données locale. Pour plus de détails, voir Périphérique > Profil d’authentification.
Utiliser uniquement l’authentification du certificat client (Web)	Sélectionnez cette option pour utiliser l'authentification du certificat du client pour l'accès au Web. Si vous sélectionnez cette option, un nom d'utilisateur et un mot de passe ne sont pas requis ; le certificat suffit pour authentifier l'accès au pare-feu.
Nouveau mot de passe Confirmer le nouveau mot de passe	Saisissez et confirmez un mot de passe sensible à la casse pour l’administrateur (64 caractères maximum). Vous pouvez également sélectionner **Configuration** > **Gestion** pour imposer un nombre minimal de caractères requis pour le mot de passe.

Paramètres du compte administrateur	Description
	Pour garantir la sécurité de l'interface de gestion des pare-feu, nous recommandons que vous changiez les mots de passe administrateur régulièrement en utilisant des lettres en minuscules, en majuscules et des chiffres. Vous pouvez également configurer les paramètres de Complexité minimale des mots de passe *pour tous les administrateurs du pare-feu.*
Utiliser l'authentification à clef publique (SSH)	Sélectionnez cette option pour utiliser l'authentification de clé publique SSH. Cliquez sur **Importer la clé** et recherchez le fichier de clé publique à sélectionner. La clé chargée s'affiche dans la zone de texte en lecture seule. Les formats de fichier de clé pris en charge sont IETF SECSH et OpenSSH. Les algorithmes de clé pris en charge sont DSA (1 024 bits) et RSA (768 à 4 096 bits). *Si l'authentification des clés publiques échoue, le pare-feu demande à l'administrateur son nom d'utilisateur et mot de passe.*
Type d'administrateur	Affectez un rôle à cet administrateur. Le rôle détermine les éléments que l'administrateur peut consulter et modifier. Si vous sélectionnez **Basé sur les rôles**, sélectionnez un profil de rôle personnalisé dans la liste déroulante. Pour plus de détails, voir Périphérique > Rôles admin. Si vous sélectionnez **Dynamique**, vous pouvez choisir l'un des rôles prédéfinis suivants : • **Super utilisateur** – Dispose d'un accès complet au pare-feu et peut définir de nouveaux comptes administrateur et de nouveaux systèmes virtuels. Vous devez posséder des privilèges de super utilisateur pour créer un utilisateur administratif avec privilèges de super utilisateur. • **Super utilisateur** (lecture seule) – Dispose d'un accès en lecture seule au pare-feu. • **Administrateur du périphérique** – Dispose d'un accès complet à tous les paramètres du pare-feu, sauf pour la définition de nouveaux comptes ou de nouveaux systèmes virtuels. • **Administrateur du périphérique** (lecture seule) – Dispose d'un accès en lecture seule à l'ensemble des paramètres du pare-feu, sauf aux profils de mot de passe (aucun accès) et

Paramètres du compte administrateur	Description
	aux comptes administrateur (seul le compte connecté est visible). • **Administrateur du système virtuel** - A accès à des systèmes virtuels spécifiques du pare-feu pour créer et gérer des aspects particulier des systèmes virtuels (si la fonction de systèmes virtuels multiples est activée). Un administrateur du système virtuel n'a pas accès aux interfaces de réseau, aux routeurs virtuels, aux tunnels IPSec, aux VLAN, aux câbles virtuels, aux tunnels GRE, à DHCP, au proxy DNS, à QoS, à LLDP ou aux profils réseaux. • **Administrateur du système virtuel** (lecture seule) - A accès en lecture seule à des systèmes virtuels spécifiques du pare-feu pour visualiser des aspects particuliers des systèmes virtuels (si la fonction de systèmes virtuels multiples est activée). Un administrateur du système virtuel ayant un accès en lecture seule n'a pas accès aux interfaces de réseau, aux routeurs virtuels, aux tunnels IPSec, aux VLAN, aux câbles virtuels, aux tunnels GRE, à DHCP, au proxy DNS, à QoS, à LLDP ou aux profils réseaux.
système virtuel - vsys (Rôle administrateur du système virtuel uniquement)	Cliquez sur **Ajouter** pour sélectionner les systèmes virtuels que peut gérer l'administrateur.
Profil de mot de passe	Sélectionnez le profil de mot de passe, le cas échéant. Pour créer un nouveau profil de mot de passe, voir Périphérique > Profils de mot de passe. *Créez un profil de mot de passe pour les administrateurs pour veiller à ce que les mots de passe des administrateurs expirent après une période de temps configurée. La modification fréquente des mots de passe des administrateurs permet aux pirates d'utiliser les identifiants enregistrés ou volés.*

Périphérique > Rôles admin

Sélectionnez **Périphérique** > **Rôles administrateur** pour définir les profils de Rôles administrateur, qui sont des rôles personnalisés déterminant les privilèges d'accès et les responsabilités des utilisateurs administratifs. Vous affectez des profils de Rôle administrateur ou des rôles dynamiques lorsque vous créez des comptes administratifs (Périphérique > Administrateurs).

Pour définir des profils de Rôle administrateur pour les administrateurs Panorama, voir Panorama > Admin Roles (Panorama > Rôles administrateurs).

Le pare-feu possède trois rôles prédéfinis que vous pouvez utiliser pour établir des critères communs. Vous utilisez tout d'abord le rôle super utilisateur pour la configuration initiale du pare-feu et pour créer les comptes administrateur de l'administrateur de sécurité, de l'administrateur d'audit et de l'administrateur cryptographique. Après avoir créé ces comptes et appliqué les Rôles admin aux critères communs appropriés, vous devez ensuite vous connecter en utilisant ces comptes. Le compte super utilisateur par défaut en mode FIPS-CC (FIPS [Federal Information Processing Standard] / CC [Common Criteria]) est **admin** et le mot de passe par défaut est **paloalto**. En mode d'utilisation standard, le compte par défaut est **admin** et le mot de passe **admin**. Les rôles administrateur prédéfinis sont créés sans fonction de chevauchement, à l'exception près qu'ils disposent tous d'un accès en lecture seule à la piste de vérification (sauf l'administrateur d'audit qui dispose d'un accès en lecture/suppression complet). Ces rôles administrateur ne peuvent pas être modifiés et sont définis comme suit'A0;:

- auditadmin : l'administrateur d'audit est responsable de la révision régulière des données d'audit du pare-feu.
- cryptoadmin : l'administrateur cryptographique est responsable de la configuration et de la maintenance des éléments cryptographiques liés à l'établissement de connexions sécurisées avec le pare-feu.
- Securityadmin – L'Administrateur de la sécurité est responsable de toutes les autres tâches administratives (la création de la politique de Sécurité par exemple) non exécutées par les deux autres rôles administrateur.

Pour ajouter un profil de Rôle administrateur, cliquez sur **Ajouter** et spécifiez les paramètres décrits dans le tableau suivant.

Créez des règles personnalisées pour restreindre l'accès des administrateurs à ce que chaque type d'administrateur a besoin. Pour chaque type d'administrateur, activez, désactivez ou configurez l'accès en lecture seule pour l'accès ***Web UI (UI Web)****,* ***XML/ REST API (API REST/XML)****,* ***Ligne de commande****, et accès* ***REST API****.*

Paramètres du rôle administrateur	
Nom	Saisissez un nom pour identifier ce rôle administrateur (31 caractères maximum). Celui-ci est sensible aux majuscules et minuscules et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Description	(Facultatif) Saisissez une description pour le rôle (255 caractères maximum).

Paramètres du rôle administrateur	
Rôle	Sélectionnez la portée des responsabilités administratives : • **Périphérique** – Le rôle s'applique à l'ensemble du pare-feu, peu importe s'il possède plus d'un système virtuel (vsys). • **Système virtuel** - Le rôle s'applique à des systèmes virtuels spécifiques du pare-feu et à des aspects spécifiques des systèmes virtuels (si la fonction de systèmes virtuels multiples est activée). Un profil du rôle admin basé sur un **système virtuel** n'a pas accès à l'onglet **Web UI** des interfaces de réseau, des VLAN, des câbles virtuels, des tunnels IPSec, des tunnels GRE, du DHCP, du proxy DNS, du QoS ou des profils réseaux. Vous sélectionnez les systèmes virtuels lorsque vous créez des comptes administratifs (Périphérique > Administrateurs).
Interface Utilisateur Web	Cliquez sur les icônes pour que les fonctions spécifiques à l'interface Web définissent les privilèges d'accès autorisé : • **Activer** – Accès en lecture/écriture à la fonction sélectionnée. • **Lecture seule** – Accès en lecture seule à la fonction sélectionnée. • **Désactiver** – Aucun accès à la fonction sélectionnée.
API XML	Cliquez sur les icônes pour que les fonctions spécifiques de l'API XML définissent les privilèges d'accès autorisé (**Activer**, ou **Désactiver)**).
Ligne de commande	Sélectionnez le type de rôle d'accès à la CLI. La valeur par défaut est **Aucun**, ce qui signifie que l'accès à la CLI n'est pas autorisé. Les autres options varient selon la portée du Rôle : • **Périphérique** • **super utilisateur** – Dispose d'un accès complet au pare-feu et peut définir de nouveaux comptes administrateur et de nouveaux systèmes virtuels. Vous devez posséder des privilèges de super utilisateur pour créer un utilisateur administratif avec privilèges de super utilisateur. • **super lecteur** – Dispose de l'accès en lecture seule au pare-feu. • **administrateur de périphérique** – Dispose d'un accès complet à tous les paramètres du pare-feu, sauf pour la définition de nouveaux comptes ou de nouveaux systèmes virtuels. • **lecteur de périphérique** – Dispose d'un accès en lecture seule à l'ensemble des paramètres du pare-feu, sauf aux profils de mot de passe (aucun accès) et aux comptes administrateur (seul le compte connecté est visible).

Paramètres du rôle administrateur	
	• **système virtuel - vsys** • **vsysadmin** : a accès aux systèmes virtuels spécifiques du pare-feu pour créer et gérer des aspects particuliers des systèmes virtuels. Le paramètre **vsysadmin** ne contrôle pas les fonctions du pare-feu et du réseau (comme le routage statique ou dynamique, les adresses IP des interfaces, les tunnels IPSec, les VLAN, les câbles virtuels, les routeurs virtuels, les tunnels GRE, le DHCP, le proxy DNS, la QoS, le LLDP ou les profils de réseaux). • **vsysreader** : a un accès en lecture seule aux systèmes virtuels spécifiques du pare-feu et aux aspects particuliers d'un système virtuel. Le paramètre **vsysreader** ne n'a pas accès aux fonctions du pare-feu et du réseau (comme le routage statique ou dynamique, les adresses IP des interfaces, les tunnels IPSec, les VLAN, les câbles virtuels, les routeurs virtuels, les tunnels GRE, le DHCP, le proxy DNS, la QoS, le LLDP ou les profils de réseaux).
REST API	Cliquez sur les icônes pour que les fonctions spécifiques de REST API définissent les privilèges d'accès autorisé (**Activer**, **Lecture seule** ou **Désactiver**).

Périphérique > Domaine d'accès

- Périphérique > Domaine d'accès

Configurez les domaines d’accès pour restreindre l’accès administrateur aux systèmes virtuels spécifiques sur le pare-feu. Le pare-feu prend uniquement en charge les domaines d’accès si vous utilisez un serveur RADIUS, TACACS+ ou SAML (IDP) pour gérer l’authentification et l’autorisation de l’administrateur. Pour activer les domaines d’accès, vous devez définir :

- Un profil de serveur pour le serveur d’authentification externe – Voir Périphérique > Profils de serveur > RADIUS, Périphérique > Profils de serveur > TACACS+ et Périphérique > Profils de serveur > Fournisseur d’identité SAML.
- Les attributs spécifiques aux fournisseurs (VSA) RADIUS, les VSA TACACS+, ou les attributs SAML.

Lorsqu’un administrateur tente de se connecter au pare-feu, ce dernier interroge le serveur externe pour connaître le domaine d’accès de l’administrateur. Le serveur externe renvoie le domaine associé et le pare-feu restreint alors l’administrateur aux systèmes virtuels que vous avez spécifiés dans le domaine d’accès. Si le pare-feu n’utilise pas un serveur externe pour authentifier et autoriser les administrateurs, les paramètres **Périphérique** > **Domaine d’accès** sont ignorés.

Sur Panorama, vous pouvez gérer les domaines d’accès localement ou en utilisant les VSA RADIUS, les VSA TACACS+ ou les attributs SAML (voir Panorama > Domaines d’accès*).*

Paramètres du domaine d’accès	Description
Name (Nom)	Donnez un nom au domaine d’accès (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. N'utilisez que des lettres, chiffres, traits d'union, traits de soulignement et points.
Systèmes virtuels	Sélectionnez des systèmes virtuels dans la colonne Disponible et cliquez sur **Ajouter** pour les ajouter. Les domaines d'accès ne sont pris en charge que sur les pare-feu prenant en charge des systèmes virtuels.

Périphérique > Profil d'authentification

Utilisez cette page pour configurer les paramètres d’authentification des administrateurs et des utilisateurs finaux. Les pare-feu et Panorama prennent en charge les services d’authentification locaux, RADIUS, TACACS+, LDAP, Kerberos, SAML 2.0 et multifacteur (MFA).

*Créez au moins un profil pour fournir l’authentification externe, qui permet de conserver toutes les demandes d’authentification en un seul endroit, ce qui facilite la gestion, et utilise un processus d’authentification standard qui comprend des services comme le suivi. Il est recommandé de créer et de prioritiser (**Périphérique** > **Séquence d'authentification**) plusieurs profils d’authentification à l’aide de méthodes diverses pour faire face aux échecs d’authentification et de créer au moins un compte de connexion auquel revenir si toutes les méthodes externes échouent.*

Vous pouvez également utiliser cette page pour enregistrer un pare-feu ou un service Panorama (tel qu’un accès administratif à l’interface Web) avec un fournisseur d’identité SAML (IDP). L’enregistrement du service permet au pare-feu ou à Panorama d’utiliser l’IDP pour authentifier les utilisateurs qui demandent le service. Vous enregistrez un service en saisissant ses métadonnées SAML sur l’IDP. Le pare-feu et Panorama facilitent l’enregistrement en générant automatiquement un fichier de métadonnées SAML en fonction du profil d’authentification que vous avez attribué au service. Vous pouvez d’ailleurs exporter ce fichier de métadonnées vers l’IDP.

- Profil d'authentification
- Exportation des métadonnées SAML à partir d’un Profil d’authentification

Profil d'authentification

- Périphérique > Profil d'authentification

Sélectionnez **Périphérique** > **Profil d’authentification** ou **Panorama** > **Profil d’authentification** pour gérer les profils d’authentification. Pour créer un nouveau profil, vous devez en **Ajouter** un et remplir les champs suivants.

*Après la configuration d’un profil d’authentification, utilisez les commandes en mode CLI **`test authentication`** d’authentification test pour déterminer si le pare-feu ou le serveur de gestion Panorama peut communiquer avec le serveur d’authentification dorsal et si la demande d’authentification est fructueuse. Vous pouvez effectuer des tests d’authentification sur la configuration candidate pour déterminer si la configuration est correcte avant de la valider.*

Paramètres de profil d’authentification	Description
Nom	Saisissez un nom pour identifier le profil. Celui-ci est sensible aux majuscules et minuscules, peut comporter 31 caractères maximum, et peut inclure uniquement des lettres, chiffres, espaces, traits d'union, traits de soulignement et des points. Le nom doit être unique au **Emplacement** actuel (pare-feu ou

Paramètres de profil d'authentification	Description
	système virtuel) par rapport aux autres profils d'authentification et séquences d'authentification. *Dans un pare-feu en mode plusieurs systèmes virtuels, si le **Emplacement** du profil d'authentification est un système virtuel, ne saisissez pas le même nom qu'une séquence d'authentification dans l'emplacement Partagé. De même, si le profil **Emplacement** est Partagé, ne saisissez pas le même nom qu'une séquence dans un système virtuel. Même si vous pouvez valider un profil et une séquence d'authentification avec les mêmes noms dans ces cas de figure, des erreurs de référence sont possibles.*
Emplacement	Sélectionnez la portée dans laquelle le profil est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Partagé** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner l' **Emplacement)** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le profil, vous ne pouvez plus changer son **Emplacement**.
Onglet Authentification Le pare-feu appelle le service d'authentification que vous configurez dans cet onglet avant de faire appel aux services d'authentification multifacteur (MFA) que vous ajoutez dans l'Onglet Facteurs. *Si le pare-feu s'intègre avec un fournisseur MFA par l'intermédiaire de RADIUS au lieu de l'API fournisseur, vous devez configurer un profil de serveur RADIUS pour ce fournisseur et non un profil de serveur MFA.*	
Type	Sélectionnez le type de service qui fournit la première (et éventuellement la seule) demande d'authentification que les utilisateurs voient. En fonction de votre sélection, la boîte de dialogue affiche d'autres paramètres que vous définissez pour le service. Les options à votre disposition sont les suivantes : • **Aucun** – N'utilisez aucune authentification. • **Cloud Authentication Service (Service d'authentification cloud)** : utilisez le service d'authentification basé sur le cloud fournit par Cloud Identity Engine. • **Base de données locale** – Utilisez la base de données d'authentification sur le pare-feu. Cette option n'est pas disponible sur Panorama. • **RADIUS** – Utilisez un serveur Remote Authentication Dial-in User Service (RADIUS). • **TACACS+** – Utilisez un serveur Terminal Access Controller Access-Control System Plus (TACACS+).

Paramètres de profil d'authentification	Description
	• **LDAP** – Utilisez un serveur Lightweight Directory Access Protocol (LDAP). • **Kerberos** – Utilisez un serveur Kerberos. • **SAML** – Utilisez un fournisseur d'identité Security Assertion Markup Language 2.0 (SAML 2.0) (IDP). *Les administrateurs peuvent utiliser SAML pour s'authentifier sur le pare-feu ou l'interface Web Panorama, mais pas sur le CLI.*
Profil de serveur (RADIUS, TACACS+, LDAP ou Kerberos uniquement)	Sélectionnez le profil de serveur d'authentification dans la liste déroulante. Reportez-vous à la section Périphérique > Profils de serveur > RADIUS, Périphérique > Profils de serveur > TACACS+, Périphérique > Profils de serveur > LDAP ou Périphérique > Profils de serveur > Kerberos.
Profil du serveur IDP (SAML uniquement)	Sélectionnez le profil de serveur du fournisseur d'identité SAML dans la liste déroulante. Reportez-vous à la section Périphérique > Profils de serveur > Fournisseur d'identité SAML.
Récupérer le groupe d'utilisateurs auprès de RADIUS (RADIUS uniquement)	Sélectionnez cette option pour collecter des informations sur les groupes d'utilisateurs à partir des Attributs spécifiques aux fournisseurs (VSA) définis sur le serveur RADIUS. Le pare-feu utilise les informations pour faire correspondre les utilisateurs s'authentifiant aux entrées de la Liste d'autorisations, pas pour appliquer les politiques ou générer des rapports.
Récupérer le groupe d'utilisateurs auprès de TACACS+ (TACACS+ uniquement)	Sélectionnez cette option pour collecter des informations sur les groupes d'utilisateurs à partir des Attributs spécifiques aux fournisseurs (VSA) définis sur le serveur TACACS+. Le pare-feu utilise les informations pour faire correspondre les utilisateurs s'authentifiant aux entrées de la Liste d'autorisations, pas pour appliquer les politiques ou générer des rapports.
Attributs connexion (LDAP uniquement)	Saisissez un attribut d'annuaire LDAP qui identifie de manière unique l'utilisateur et qui sert d'identifiant de connexion pour cet utilisateur.
Avertissement pour l'expiration du mot de passe (LDAP uniquement)	Si le profil d'authentification s'applique aux utilisateurs GlobalProtect, saisissez le nombre de jours avant expiration du mot de passe pour démarrer l'affichage de messages de notification aux utilisateurs afin de les avertir que leurs mots de passe expirent dans x jours. Par défaut, les messages de notification s'affichent sept jours avant l'expiration du mot de passe (plage de 1 à 255). Les utilisateurs ne pourront pas accéder au VPN si leur mot de passe expire.

Paramètres de profil d'authentification	Description
	Envisagez l'option de configurer les agents GlobalProtect de manière à utiliser la méthode de pré-ouverture de session Cela permettra aux utilisateurs de se connecter au domaine pour changer leur mot de passe même après expiration du mot de passe. Si les utilisateurs autorisent l'expiration de leur mot de passe, l'administrateur peut affecter un mot de passe LDAP temporaire afin de permettre aux utilisateurs de se connecter au VPN. Dans ce flux de travail, nous recommandons de définir la **modifiication d'authentification** dans la configuration du portail sur **Authentification par cookie pour actualiser la configuration** (sinon, le mot de passe temporaire sera utilisé pour l'authentification sur le portail, mais la connexion à la passerelle échouera, empêchant l'accès au VPN).
Certificat de signature des demandes (SAML uniquement)	Sélectionnez le certificat que le pare-feu utilisera pour signer les messages SAML qu'il envoie au fournisseur d'identité (IDP). Ce champ est requis si vous activez l'option **Sign SAML Message to IdP (Signer le message SAML vers IDP)** dans le **IdP Server Profile (Profil de serveur IDP)** (voir Périphérique > Profils de serveur > Fournisseur d'identité SAML). Sinon, sélectionner un certificat pour signer des messages SAML est facultatif. Lors de la génération ou de l'importation d'un certificat et de sa clé privée associée, les attributs d'utilisation des clés spécifiés dans le certificat contrôlent la manière dont vous pouvez utiliser la clé : • Si le certificat énumère explicitement les attributs d'utilisation des clés, l'un des attributs doit être la Signature numérique, qui n'est pas disponible dans les certificats que vous générez sur le pare-feu. Dans ce cas, vous devez Importer le certificat et la clé à partir de l'autorité de certification (CA) de votre entreprise ou d'une autorité de certification tierce. • Si le certificat ne spécifie pas les attributs d'utilisation des clés, vous pouvez utiliser la clé à toutes fins utiles, y compris la signature de messages. Dans ce cas, vous pouvez utiliser n'importe quelle méthode pour obtenir le certificat et la clé pour signer des messages SAML. *Palo Alto Networks recommande d'utiliser un certificat de signature pour assurer l'intégrité des messages SAML envoyés à IDP.*
Activer la déconnexion unique	Sélectionnez cette option pour permettre aux utilisateurs de vous déconnecter de tous les services authentifiés en vous déconnectant de n'importe quel service unique. La fermeture de session unique (SLO) s'applique uniquement aux

Paramètres de profil d'authentification	Description
(SAML uniquement)	services auxquels les utilisateurs ont accès via l'authentification SAML. Les services peuvent être externes ou internes à votre organisation (par exemple, l'interface Web du pare-feu). Cette option ne s'applique que si vous avez saisi une **URL de fermeture de session unique du fournisseur d'identité** dans le Profil du serveur IDP. Vous ne pouvez pas activer la SLO pour les utilisateurs du Portail d'authentification. *Après la fermeture de session des utilisateurs, le pare-feu supprime automatiquement leurs* mappages d'adresse IP / nom d'utilisateur .
Profil du certificat (SAML uniquement)	Sélectionnez le Profil de certificat que le pare-feu utilise pour valider : • Le**Certificat du fournisseur d'identité** spécifié dans le Profil de serveur IDP. L'IDP utilise ce certificat pour s'authentifier sur le pare-feu. Le pare-feu valide le certificat lorsque vous effectuez l'action visant à **Valider** la configuration du profil d'authentification. • Les messages SAML que l'IDP envoie au pare-feu pour l'authentification d'ouverture de session unique (SSO) et l'authentification de fermeture de session unique (SLO). L'IDP utilise l'**Identity Provider Certificate (Certificat du fournisseur d'identité)** spécifié dans le Profil de serveur IDP pour signer les messages. Voir Périphérique > Gestion des certificats > Profil de certificat.
Domaine d'utilisateur ET Modificateur du nom d'utilisateur (All authentication types except SAML and Cloud Authentication Service (Tous les types d'authentification sauf SAML et Cloud Authentication Service)	Le pare-feu utilise le **User Domain (Domaine utilisateur)** pour faire correspondre les utilisateurs s'authentifiant aux entrées de la Liste d'autorisations et pour le mappage de groupe User-ID . Vous pouvez indiquer un **Modificateur du nom d'utilisateur** pour modifier le format du domaine et le nom d'utilisateur qu'un utilisateur saisit lors de la connexion. Le pare-feu utilise la chaîne modifiée pour l'authentification. Choisissez l'une des options suivantes : • Pour envoyer uniquement l'entrée non modifiée de l'utilisateur, laissez le **Domaine utilisateur** par défaut et définissez le **Modificateur du nom d'utilisateur** à la variable **%USERINPUT%** (par défaut). • Pour ajouter un domaine à la saisie utilisateur, saisissez un **Domaine utilisateur** et définissez le **Modificateur du nom d'utilisateur** sur **%USERDOMAIN%\%USERINPUT%**.

Paramètres de profil d'authentification	Description
	• Pour ajouter un domaine à l'entrée utilisateur, entrez un **domaine** utilisateur et définissez le **modificateur de nom d'utilisateur sur %USERINPUT %@%USERDOMAIN%**. *Si le **modificateur** de nom d'utilisateur inclut la variable %USERDOMAIN%, la **valeur Domaine** utilisateur remplace toute chaîne de domaine entrée par l'utilisateur. Si vous précisez la valeur %USERDOMAIN% et que vous ne renseignez pas **Domaine utilisateur**, le pare-feu supprime toute chaîne de domaine saisie par l'utilisateur. Le pare-feu résout les noms de domaine en nom NetBIOS approprié pour le mappage de groupe User-ID. Ceci s'applique aux domaines parent et enfant. Les modificateurs de **Domaine utilisateur** sont prioritaires sur les noms NetBIOS dérivés automatiquement.* • Pour permettre au pare-feu d'utiliser le type de profil de serveur pour déterminer comment et à quel moment dans la séquence d'authentification modifier le format de la saisie utilisateur, saisissez manuellement **`None (Aucune)`** en tant que **Modificateur du nom d'utilisateur**. Pour obtenir plus d'informations sur cette option, reportez-vous à la section Configurer un profil et une séquence d'authentification dans le Guide de l'administrateur PAN-OS.
Partition Kerberos (All authentication types except SAML and Cloud Authentication Service (Tous les types d'authentification sauf SAML et Cloud Authentication Service)	Si votre réseau prend en charge l'ouverture de session unique (SSO) Kerberos, saisissez la **Partition Kerberos** (127 caractères maximum). Il s'agit de la partie du nom d'hôte dans le nom de connexion utilisateur. Par exemple, le nom de compte utilisateur utilisateur@EXEMPLE.LOCAL comporte la partition EXEMPLE.LOCAL.
Keytab Kerberos (All authentication types except SAML and Cloud Authentication Service (Tous les types d'authentification sauf SAML et Cloud	Si votre réseau prend en charge l'ouverture de session unique Kerberos (SSO) cliquez sur **Importer**, puis sur **Parcourir** pour localiser le fichier de keytab, puis cliquez sur **OK**. Un keytab contient les informations de compte Kerberos (nom principal et mot de passe haché) du pare-feu, qui sont nécessaires pour l'authentification SSO. Chaque profil d'authentification peut comporter un keytab. Pendant l'authentification, le pare-feu tente tout d'abord d'utiliser le keytab pour établir une SSO. S'il réussit et que l'utilisateur tentant l'accès figure dans la Liste d'autorisations, l'authentification réussit immédiatement. Sinon, le processus d'authentification revient à l'authentification manuelle

Paramètres de profil d'authentification	Description
Authentication Service)	(nom d'utilisateur / mot de passe) du **Type** spécifié, qui ne doit pas nécessairement être Kerberos. *Si le pare-feu est en mode FIPS/CC, l'algorithme doit être aes128-cts-hmac-sha1-96 ou aes256-cts-hmac-sha1-96. Sinon, vous pouvez également utiliser des3-cbc-sha1 ou arcfour-hmac. Cependant, si l'algorithme contenu dans le keytab ne correspond pas à l'algorithme contenu dans le ticket de service généré par le Service d'émission de tickets pour que les clients puissent activer la SSO, le processus de SSO échoue. Le rôle de votre administrateur Kerberos est de déterminer les algorithmes utilisés par les tickets de service.*
Attribut du nom d'utilisateur (SAML uniquement)	Saisissez l'attribut SAML qui identifie le nom d'utilisateur d'un utilisateur s'authentifiant dans les messages envoyés par l'IDP (la valeur par défaut est **nom d'utilisateur**). Si le **IdP Server Profile (Profil de serveur IDP)** contient des métadonnées qui spécifient un attribut de nom d'utilisateur, le pare-feu renseigne automatiquement ce champ avec cet attribut. Le pare-feu correspond aux noms d'utilisateur récupérés à partir des messages SAML avec les utilisateurs et les groupes d'utilisateurs dans **Liste d'autorisations** du profil d'authentification. Puisque vous ne pouvez pas configurer le pare-feu pour modifier la chaîne domaine / nom d'utilisateur qu'un utilisateur saisit pendant les connexions SAML, le nom d'utilisateur de connexion doit correspondre exactement à une entrée de **Liste d'autorisations**. C'est le seul attribut SAML qui est obligatoire. *Les messages SAML peuvent afficher le nom d'utilisateur dans le champ objet. Le pare-feu vérifie automatiquement le champ objet si l'attribut du nom d'utilisateur n'affiche pas le nom d'utilisateur.*
Attribut du groupe d'utilisateurs (SAML uniquement)	Saisissez l'attribut SAML qui identifie le groupe d'utilisateurs d'un utilisateur s'authentifiant dans les messages envoyés par l'IDP (la valeur par défaut est **groupe d'utilisateurs**). Si le **Profil de serveur IDP** contient des métadonnées qui spécifient un attribut de groupe d'utilisateurs, le champ utilise automatiquement cet attribut. Le pare-feu utilise les informations de groupe pour faire correspondre les utilisateurs s'authentifiant aux entrées de **Liste d'autorisations** et non aux politiques ou aux rapports.
Attribut du rôle admin (SAML uniquement)	Saisissez l'attribut SAML qui identifie le rôle administrateur d'un utilisateur s'authentifiant dans les messages envoyés par l'IDP (la valeur par défaut est **rôle administrateur**). Cet attribut s'applique uniquement aux administrateurs de pare-feu et non aux utilisateurs finaux. Si le **Profil de serveur IDP** contient des métadonnées qui spécifient un attribut de rôle administrateur, le pare-feu renseigne automatiquement ce champ avec cet attribut. Le pare-feu correspond à ses rôles (dynamiques) prédéfinis ou à des profils des profils de

Paramètres de profil d'authentification	Description
	Rôle administrateur avec les rôles extraits des messages SAML pour renforcer le contrôle d'accès basé sur les rôles. Si un message SAML a plusieurs valeurs de rôle administrateur pour un administrateur avec un seul rôle, la mise en correspondance s'applique uniquement à la première valeur (la plus à gauche) dans l'attribut du rôle administrateur. Pour un administrateur avec plus d'un rôle, la mise en correspondance peut s'appliquer à plusieurs valeurs dans l'attribut.
Attribut du domaine d'accès (SAML uniquement)	Saisissez l'attribut SAML qui identifie le domaine d'accès d'un utilisateur s'authentifiant dans les messages envoyés par l'IDP (la valeur par défaut est **domaine d'accès**). Cet attribut s'applique uniquement aux administrateurs de pare-feu et non aux utilisateurs finaux. Si le **Profil de serveur IDP** contient des métadonnées qui spécifient un attribut de domaine d'accès, le pare-feu renseigne automatiquement ce champ avec cet attribut. Le pare-feu fait correspondre ses domaines d'accès configurés localement avec ceux récupérés à partir des messages SAML pour appliquer le contrôle d'accès. Si un message SAML a plusieurs valeurs du domaine d'accès pour un administrateur avec un seul domaine d'accès, la mise en correspondance s'applique uniquement à la première valeur (la plus à gauche) dans l'attribut du domaine d'accès. Pour un administrateur avec plus d'un domaine d'accès, la mise en correspondance peut s'appliquer à plusieurs valeurs dans l'attribut.
Région (Cloud Authentication Service only (Service d'authentification de cloud uniquement))	Sélectionnez le point de terminaison régional pour votre instance Cloud Identity Engine. *La région que vous sélectionnez doit correspondre à la région que vous sélectionnez lorsque vous activate (activez) votre instance Cloud Identity Engine.*
Instance (Cloud Authentication Service only (Service d'authentification de cloud uniquement))	Si vous avez plusieurs instances, sélectionnez l'instance Cloud Identity Engine que vous souhaitez utiliser.
Profil (Cloud Authentication Service only (Service d'authentification de cloud uniquement))	Si vous avez plusieurs identity provider profile (profils de fournisseur d'identité) Cloud Identity Engine (profil IdP), sélectionnez le profil IdP Cloud Identity Engine que vous souhaitez utiliser.
Déréglage d'horloge maximum (secondes)	Saisissez l'intervalle de temps maximal acceptable en secondes entre le moment où l'IDP envoie le message et le moment où le système de pare-feu

Paramètres de profil d'authentification	Description
(Cloud Authentication Service only (Service d'authentification de cloud uniquement))	valide le message qu'il reçoit de la part de l'IDP (la plage est de 1 à 900, la valeur par défaut est de 60). Si l'intervalle de temps dépasse cette valeur, la validation (et donc l'authentification) échoue.
forcer l'authentification multifacteur dans le cloud (Cloud Authentication Service only (Service d'authentification de cloud uniquement))	Activez **force multi-factor authentication in cloud forcer l'authentification multifacteur dans le cloud)** si votre IdP est configuré pour obliger les utilisateurs à se connecter à l'aide de l'authentification multifacteur.
Onglet Facteurs	
Activer les facteurs d'authentification supplémentaires	Sélectionnez cette option si vous souhaitez que le pare-feu appelle des facteurs d'authentification supplémentaires (demandes) après la réponse fructueuse des utilisateurs au premier facteur (spécifié dans le champ **Type** dans l'onglet **Authentification**). *Des facteurs d'authentification supplémentaires sont pris en charge pour l'authentification des utilisateurs finaux via la Politique d'authentification uniquement. Des facteurs supplémentaires ne sont pas pris en charge pour l'authentification des utilisateurs distants aux portails et passerelles GlobalProtect ou pour l'authentification des administrateurs à l'interface Web de Panorama ou PAN-OS. Bien que vous puissiez configurer des facteurs supplémentaires, ceux-ci ne seront pas appliqués dans le cadre de ces cas pratiques. Vous pouvez toutefois procéder à l'intégration aux fournisseurs MFA au moyen de RADIUS ou de SAML pour tous les cas pratiques d'authentification.* Après avoir configuré un profil d'authentification utilisant une authentification multifacteur (MFA), vous devez l'affecter à un objet d'application d'authentification (Objets > Authentification) et affecter l'objet aux règles de la politique d'Authentification (Politiques > Authentification) qui contrôlent l'accès à vos ressources réseau.
Facteurs	Ajoutez un profil de serveur MFA (Périphérique > Profils de serveur > Authentification multifacteur) pour chaque facteur d'authentification que le pare-feu appelle après que les utilisateurs répondent avec succès au premier facteur (spécifié dans le champ **Type** dans l'onglet **Authentification**). Le

Paramètres de profil d'authentification	Description
	pare-feu appelle chaque facteur dans l'ordre du haut vers le bas dans lequel vous répertoriez les services MFA qui fournissent les facteurs. Pour changer l'ordre, sélectionnez un profil de serveur et **Déplacer en haut** ou **Déplacer en bas**. Vous pouvez indiquer jusqu'à trois facteurs supplémentaires. Chaque service MFA fournit un facteur. Certains services MFA permettent aux utilisateurs de choisir un facteur à partir d'une liste composée de plusieurs facteurs. Le pare-feu s'intègre avec ces services MFA au moyen des API des fournisseurs. Des intégrations des API des fournisseurs MFA sont ajoutées périodiquement via les mises à jour de contenu Applications ou Applications et menaces.
Onglet Avancé	
Liste d'autorisations	Cliquez sur **Add (Ajouter)** et sélectionnez **tous** ou sélectionnez les utilisateurs et groupes spécifiques autorisés à s'authentifier avec ce profil. Lorsqu'un utilisateur s'authentifie, le pare-feu fait correspondre le nom d'utilisateur ou le groupe associé aux entrées de cette liste. Si vous n'ajoutez pas d'entrées, aucun utilisateur ne peut s'authentifier. *Pour restreindre l'authentification uniquement aux utilisateurs qui ont besoin d'un accès pour des raisons professionnelles légitimes et pour réduire la surface d'attaque, précisez des utilisateurs ou des groupes d'utilisateurs et évitez d'utiliser l'option **tous**.* *Si vous avez saisi une valeur **Domaine utilisateur**, vous ne devez pas nécessairement préciser de domaines dans **Allow List (Liste d'autorisation)**. Par exemple, si le **Domaine utilisateur** est **businessinc** et que vous souhaitez ajouter l'utilisateur **admin1** à **Liste d'autorisations**, la saisie de **`admin1`** a le même effet que la saisie de **`businessinc\admin1`**. Vous pouvez préciser des groupes existant déjà dans votre service d'annuaires ou préciser des groupes personnalisés sur la base de filtres LDAP.*
Tentatives échouées (Tous les types d'authentification à l'exception de SAML)	Saisissez le nombre d'échecs de tentatives de connexion successives (0 à 10) autorisés par le pare-feu avant de verrouiller le compte utilisateur. Une valeur de 0 indique un nombre illimité de tentatives de connexion. La valeur par défaut est de 0 pour les pare-feu en mode opérationnel normal et de 10 pour les pare-feu en mode FIPS-CC. *Définissez le nombre de **Tentatives échouées** sur 5 ou moins pour permettre un nombre raisonnable de nouvelles tentatives en cas de fautes de frappe, tout en empêchant les systèmes malveillants de tenter des méthodes d'attaque par force pour se connecter au pare-feu.*

Paramètres de profil d’authentification	Description
	*Si vous définissez les **Tentatives échouées** sur une valeur autre que 0 mais que vous conservez la valeur **Durée de verrouillage** de 0, les **Tentatives échouées** sont ignorées et l'utilisateur n'est jamais verrouillé.*
Durée de verrouillage (Tous les types d’authentification à l’exception de SAML)	Saisissez le nombre de minutes (plage comprise entre 0 et 60 ; par défaut 0) pendant lesquelles le pare-feu verrouille un compte utilisateur après que l’utilisateur a atteint le nombre de **Tentatives échouées**. Une valeur de 0 signifie que le verrouillage s’applique jusqu’à ce qu’un administrateur déverrouille manuellement le compte utilisateur. *Définissez la **Durée de verrouillage** sur au moins 30 minutes pour empêcher les tentatives de connexion continues d’un acteur malveillant.* *Si vous définissez **Durée de verrouillage** sur une valeur autre que 0 mais que vous conservez la valeur **Tentatives échouées** de 0, **Durée de verrouillage** est ignorée et l'utilisateur n'est jamais verrouillé.*

Exportation des métadonnées SAML à partir d’un Profil d’authentification

- Périphérique > Profil d'authentification

Le pare-feu et Panorama peuvent utiliser un fournisseur d’identité SAML (IDP) pour authentifier les utilisateurs qui demandent des services. Pour les administrateurs, le service est accessible depuis l’interface Web. Pour les utilisateurs finaux, le service peut être Portail d’authentification ou GlobalProtect, ce qui permet d’accéder aux ressources de votre réseau. Pour activer l’authentification SAML pour un service, vous devez enregistrer ce service en saisissant des informations spécifiques le concernant sur l’IDP, sous la forme de métadonnées SAML. Le pare-feu et Panorama simplifient l’enregistrement en générant automatiquement un fichier de métadonnées SAML en fonction du profil d’authentification que vous avez attribué au service, et vous pouvez exporter ce fichier de métadonnées vers l’IDP. L’exportation des métadonnées est une alternative plus simple à la saisie des valeurs pour chaque champ de métadonnées dans l’IDP.

Certaines des métadonnées du fichier exporté proviennent du profil de serveur SAML IDP affecté au profil d’authentification (Périphérique > Profils de serveur> Fournisseur d’identité SAML). Toutefois, le fichier exporté spécifie toujours POST comme méthode de liaison HTTP, quelle que soit la méthode spécifiée dans le profil de serveur SAML IDP. IDP utilisera la méthode POST pour transmettre des messages SAML au pare-feu ou à Panorama.

Pour exporter des métadonnées SAML à partir d'un profil d'authentification, cliquez sur les **Metadata (Métadonnées)** SAML dans la colonne Authentification et complétez les champs suivants. Pour importer le fichier de métadonnées dans un IDP, reportez-vous à votre documentation IDP.

Paramètres d'exportation de métadonnées SAML	Description
Commandes	Sélectionnez le service pour lequel vous voulez exporter les métadonnées SAML. • **management (gestion)** (par défaut) – Fournit un accès administrateur à l'interface Web. • **authentication-portal (portail d'authentification)** – Fournit à l'utilisateur final un accès aux ressources du réseau via le Portail d'authentification. • **global-protect (protection globale)** – Fournit à l'utilisateur final un accès aux ressources du réseau via GlobalProtect. Votre sélection détermine les autres champs affichés par la boîte de dialogue.
[Gestion | Portail d'authentification | GlobalProtect] Profil d'authentification	Saisissez le nom du profil d'authentification à partir duquel vous exportez des métadonnées. La valeur par défaut représente le profil à partir duquel vous avez ouvert la boîte de dialogue en cliquant sur le lien **Metadata (Métadonnées)**.
Choix de gestion (Gestion uniquement)	Sélectionnez une option pour spécifier une interface activée pour le trafic de gestion (comme l'interface MGT) : • **Interface** – Sélectionnez l'interface à partir de la liste des interfaces du pare-feu. • **IP Hostname (Nom d'hôte IP)** – Saisissez l'adresse IP ou le nom d'hôte de l'interface. Si vous saisissez un nom d'hôte, le serveur DNS doit avoir un enregistrement d'adresse (A) qui correspond à l'adresse IP.
[Portail d'authentification | GlobalProtect] Système virtuel (Portail d'authentification ou GlobalProtect uniquement)	Sélectionne le système virtuel pour lequel les paramètres du Portail d'authentification ou du portail GlobalProtect sont définis.
Nom d'hôte IP (Portail d'authentification	Saisissez l'adresse IP ou le nom d'hôte du service. • **Authentication Portal (Portail d'authentification)** – Saisissez l'adresse IP ou le nom d'hôte pour **Redirect Host (Rediriger l'hôte)** (**Device (Périphérique)** > **User Identification (Identification**

Paramètres d’exportation de métadonnées SAML	Description
ou GlobalProtect uniquement)	**utilisateur)** > **Authentication Portal Settings (Paramètres du Portail d’authentification)**). • **GlobalProtect** – Saisissez le **Hostname (nom d’hôte)** ou l’**IP Address (adresse IP)** du portail GlobalProtect. Si vous saisissez un nom d’hôte, le serveur DNS doit avoir un enregistrement d’adresse (A) qui correspond à l’adresse IP.

Périphérique > Séquence d'authentification

- Périphérique > Séquence d'authentification
- Panorama > Séquence d'authentification

Dans certains environnements, les comptes utilisateur se trouvent dans plusieurs répertoires (par exemple LDAP et RADIUS). Une séquence d'authentification est un ensemble de profils d'authentification que le pare-feu tente d'utiliser pour authentifier des utilisateurs lorsqu'ils se connectent. Le pare-feu essaie les profils de manière séquentielle en partant du haut de la liste vers le bas, en appliquant les valeurs d'authentification, de SSO Kerberos, de liste d'autorisation et de verrouillage de compte pour chacun d'entre eux jusqu'à ce qu'un profil authentifie avec succès l'utilisateur. Le pare-feu ne refuse l'accès que si l'authentification de tous les profils de la séquence échoue. Pour plus d'informations sur les profils d'authentification, voir Périphérique > Profil d'authentification.

Configurez une séquence d'authentification détenant plusieurs profils d'authentification qui utilisent des méthodes d'authentification différentes. Configurez au moins deux méthodes d'authentification externes et une méthode d'authentification locale (interne), pour que les problèmes de connectivité n'empêchent pas l'authentification. Faites du profil d'authentification locale le dernier profil de la séquence, pour qu'il ne soit utilisé que si toutes les méthodes d'authentification externes échouent. (L'authentification externe fournit des services d'authentification dédiés, fiables et centralisés, y compris des fonctions de journalisation et de dépannage.)

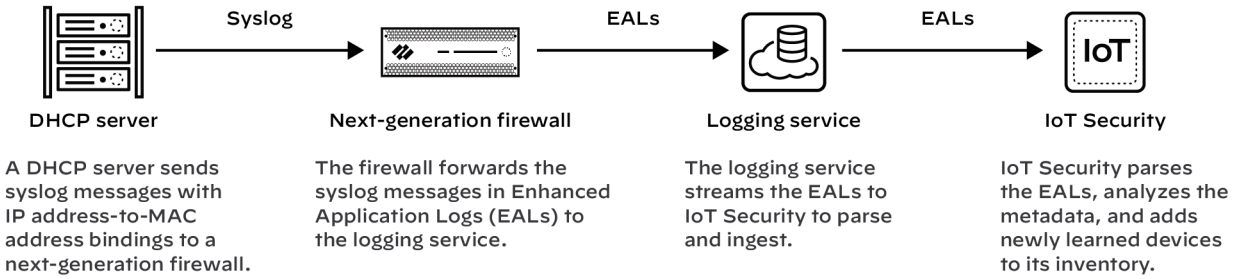
Paramètres de séquence d'authentification	Description
Nom	Saisissez un nom pour identifier la séquence. Celui-ci est sensible à la casse, peut comporter 31 caractères maximum, et peut inclure uniquement des lettres, chiffres, espaces, traits d'union, traits de soulignement et des points. Le nom doit être unique au **Emplacement** actuel (pare-feu ou système virtuel) par rapport aux autres séquences d'authentification et profils d'authentification. *Si un pare-feu comporte plusieurs systèmes virtuels (mode multi-vsys), si l' **Emplacement)** de la séquence d'authentification est un système virtuel (vsys), ne saisissez pas le même nom de profil d'authentification dans l'emplacement Partagé. De même, si la séquence **Emplacement** est **Partagée**, ne saisissez pas le même nom qu'un profil dans un système virtuel. Même si vous pouvez valider une séquence et un profil d'authentification avec les mêmes noms dans ces cas de figure, des erreurs de référence sont possibles.*
Emplacement	Sélectionnez la portée dans laquelle la séquence est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys),

Paramètres de séquence d'authentification	Description
	sélectionnez un système virtuel ou **Partagé** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner l' **Emplacement** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré la séquence, vous ne pouvez plus changer son **Emplacement**.
Utiliser le domaine pour déterminer le profil d'authentification	Les options suivantes s'appliquent uniquement aux profils d'authentification LDAP et sont activées par défaut. • **Exit the sequence on failed authentication (Quitter la séquence en cas d'échec de l'authentification)**— Si le nom de domaine saisi par l'utilisateur lors de la connexion correspond à un nom de domaine dans n'importe quel profil d'authentification de la séquence d'authentification (avec ou sans normalisation), le pare-feu interrompt la séquence d'authentification s'il ne parvient pas à authentifier le utilisateur au lieu de terminer le reste de la séquence d'authentification dans l'ordre de haut en bas. *Cette option s'applique uniquement si le pare-feu correspond au nom de domaine avec un profil d'authentification dans la séquence.* • **Utiliser le domaine de l'ID utilisateur pour déterminer le profil d'authentification**: normalise le nom de domaine que l'utilisateur entre lors de la connexion avant d'utiliser le nom de domaine pour vérifier les profils d'authentification dans l'ordre. Si vous ne sélectionnez pas cette option, le pare-feu ne normalise pas le nom de domaine que l'utilisateur saisit lors de la connexion avant d'appliquer la séquence du profil d'authentification. Si vous désactivez cette option, le pare-feu ne normalise pas le nom de domaine et essaie de faire correspondre le nom de domaine avec les profils d'authentification dans l'ordre de haut en bas même si l'authentification échoue.
Profiles d'authentification	Cliquez sur **Ajouter** et choisissez dans la liste déroulante pour chaque profil d'authentification que vous souhaitez ajouter à la séquence. Pour changer l'ordre de la liste, sélectionnez un profil, puis cliquez sur **Déplacer en haut** ou sur **Déplacer en bas**. Pour supprimer un profil, sélectionnez-le, puis cliquez sur **Supprimer**. *Vous ne pouvez pas ajouter un profil d'authentification qui spécifie un profil de serveur d'authentification multifacteur (MFA) ou un profil de serveur de fournisseur d'identité de langage de balisage d'assertion de sécurité (SAML).*

Périphérique > IoT > Serveur DHCP

IoT Security s’appuie sur des liaisons d’adresse IP à adresse MAC pour attribuer les comportements réseau observés aux appareils IoT et les suivre de manière unique. IoT Security utilise généralement le trafic DHCP collecté par les pare-feu de nouvelle génération pour apprendre les liaisons d’adresse IP à adresse MAC et suivre les modifications d’adresse IP. Toutefois, lorsqu’il n’est pas possible de positionner un pare-feu dans le chemin de données DHCP, vous pouvez utiliser cette méthode pour ingérer les journaux du serveur DHCP et étendre la visibilité du trafic DHCP.

Dans les zones du réseau où il est difficile d’acheminer le trafic DHCP vers ou via un pare-feu, configurez les serveurs DHCP pour qu’ils envoient leurs journaux de serveur sous forme de messages syslog au pare-feu. Le pare-feu transfère ensuite les messages en tant que journaux d’application améliorés (EAL) avec un sous-type de dhcp-syslog via le service de journalisation à IoT Security. IoT Security les analyse pour apprendre les liaisons d’adresse IP à adresse MAC, puis ajoute les appareils nouvellement appris à son inventaire.



Prérequis

- Un serveur DHCP avec des fonctionnalités syslog configuré pour envoyer des messages à un serveur syslog exécuté sur un pare-feu de nouvelle génération
- Un pare-feu de nouvelle génération exécutant PAN-OS 11.0 ou version ultérieure avec un abonnement IoT Security actif

Configurer le pare-feu nouvelle génération

Configurez votre pare-feu de nouvelle génération pour recevoir les messages syslog d’un ou plusieurs serveurs DHCP. Le pare-feu transfère automatiquement les messages syslog qu’il reçoit sous forme d’EAL au service de journalisation, qui les transmet à IoT Security pour analyse et analyse.

1. Ajoutez un serveur DHCP au pare-feu de nouvelle génération.

   Connectez-vous à votre pare-feu de nouvelle génération, sélectionnez **Device (Appareil)** > **IoT** > **+Add (+ Ajouter)**, configurez les éléments suivants, puis cliquez sur **OK** :

Champ	Description
Nom	Entrez un nom pour le serveur DHCP. Il peut contenir jusqu’à 32 caractères, espaces compris.
Description	Entrez une remarque sur le serveur DHCP pour référence ultérieure. Il peut contenir jusqu’à 256 caractères, espaces compris.

Champ	Description
Activé	Sélectionnez cette option pour permettre au pare-feu d'écouter les connexions du serveur DHCP et de les traiter lorsqu'elles se présentent.
Adresse IP	Entrez l'adresse IP à partir de laquelle le serveur DHCP se connectera au pare-feu. L'adresse peut être au format IPv4 ou IPv6. Un nom de domaine complet n'est pas autorisé.
Protocole	Sélectionnez **TCP**, **UDP**, ou **SSL**. Lorsque vous faites votre choix, tenez compte de ce qui est important pour la connexion entre le serveur DHCP et le pare-feu. TCP assure la fiabilité de la transmission, mais pas la sécurité. UDP offre une faible surcharge de traitement et des vitesses plus rapides, mais manque de fiabilité et de sécurité. SSL offre fiabilité et sécurité, mais entraîne plus de frais généraux. *Le pare-feu écoute les connexions serveur DHCP à l'aide de TCP et UDP sur le port 10514 et les connexions utilisant SSL sur le port 16514.*

2. Répétez l'étape précédente pour ajouter d'autres serveurs DHCP.

   Ajoutez d'autres serveurs DHCP pour étendre la visibilité du trafic DHCP sur l'ensemble de votre réseau selon vos besoins. Tous les pare-feu de nouvelle génération prennent en charge un maximum de 100 serveurs DHCP par pare-feu.

Configurer les serveurs DHCP pour Syslog

Configurez vos serveurs DHCP pour envoyer des messages syslog de leurs journaux de serveur à l'interface de gestion du pare-feu de nouvelle génération. Assurez-vous de configurer les serveurs DHCP pour utiliser le même protocole configuré pour eux sur le pare-feu : TCP, UDP ou SSL. Consultez la documentation de vos serveurs DHCP pour obtenir des instructions de configuration.

Vérifiez l'état de la connexion au serveur DHCP

Pour afficher tous les serveurs DHCP configurés, sélectionnez **Device (Appareil)** > **IoT**.

Un cercle vert à côté du nom d'un serveur DHCP signifie qu'il a été configuré dans Panorama et qu'il est en lecture seule lorsqu'il est affiché dans l'interface Web du pare-feu local de nouvelle génération.

Lorsqu'un serveur DHCP utilisant TCP ou SSL est actuellement connecté au pare-feu, « Connecté » apparaît dans la colonne État. « Connecté » apparaît également dans cette colonne si un serveur DHCP utilisant UDP a été connecté au cours des deux dernières heures. À tout autre moment, la colonne État est vide, ce qui indique que le serveur n'est pas actuellement connecté au pare-feu.

Les commandes CLI suivantes sont également utiles pour vérifier les paramètres du serveur DHCP, l'état de leurs connexions et les données qu'ils fournissent à IoT Security :

`Afficher l'état du serveur DHCP IoT { ALL | SERVER <server-name> }`	La saisie de **`all (tout)`** affiche un tableau avec tous les serveurs DHCP configurés sur le pare-feu, les numéros de port sur lesquels ils se connectent et leur état de connexion actuel.

	La saisie de **server (serveur) <server-name>** affiche des informations détaillées sur un serveur DHCP spécifique et son activité récente.
show IoT eal dhcp-syslog-eal	Cette commande affiche des informations relatives aux DAL contenant des messages syslog du serveur DHCP.

Périphérique > Redistribution des données

Ces paramètres définissent les méthodes que le pare-feu ou Panorama utilise pour redistribuer les données.

Que voulez-vous faire ?	Reportez-vous à la section :
Ajouter ou supprimer des agents de redistribution	Périphérique > Redistribution des données > Agents
Afficher les informations sur les clients de redistribution des données.	Périphérique > Redistribution des données > Clients
Configurer le nom de collecteur de l'agent de redistribution des données et la clé pré-partagée.	Périphérique > Redistribution des données > Paramètres du collecteur
Définissez les sous-réseaux que l'agent de redistribution des données inclut ou exclut lors de la redistribution des données.	Périphérique > Redistribution des données > Inclure/ Exclure des réseaux

Périphérique > Redistribution des données > Agents

Ajouter un agent de Redistribution des données à l'aide d'un numéro de série ou d'un hôte et des informations du port.

Paramètres de l'agent de redistribution des données	Description
Nom	Saisissez un nom pour l'agent de redistribution des données (jusqu'à 31 caractères). Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Activé	Sélectionnez cette option pour activer l'agent de redistribution des données.
Ajouter un agent à l'aide de	Sélectionnez la façon dont vous voulez ajouter l'agent de redistribution des données : • **Numéro de série**— Sélectionnez cette option puis sélectionnez le numéro de série.

Paramètres de l’agent de redistribution des données	Description
	• **Hôte et port**—Sélectionnez cette option et saisissez les informations d’hôte et de port suivantes : • **Hôte**— Saisissez le nom de l’hôte. • **LDAP Proxy**— Sélectionnez cette option pour utiliser l’hôte en tant que proxy LDAP. • **Port**— Saisissez le numéro du port sur lequel l’agent écoute les requêtes. • **Nom du collecteur** : Saisissez le **Nom du collecteur** et la **Clé pré-partagée** qui identifient le pare-feu ou le système virtuel en tant qu’agent User-ID.
Type de données	Sélectionnez le type de données que vous voulez redistribuer (IP utilisant des mappages, Etiquettes d’IP, Etiquettes d’utilisateur, HIP ou Liste de quarantaine).

Après avoir configuré un agent de redistribution des données, vous pouvez afficher les informations suivantes pour l’agent de redistribution :

Informations sur	l’agent de redistribution de données Description
Numéro de	série Numéro d’identification de l’agent.
Host	Les information de l’hôte.
Nom du collecteur Nom	de l’agent collecteur.
HIP	Le profil d’information d’hôte de l’agent.
Mappages d’utilisateurs IP	Les Informations de mappage adresse IP-nom d’utilisateur.
Etiquettes IP	Les informations de mappage étiquette/adresse IP.
Liste de quarantaine	Affiche une liste des périphériques qui sont en quarantaine.
Groupe d’utilisateurs dynamique	Les informations de mappage nom d’utilisateur à balise.
Connecté	Indique si l’agent est connecté au service de redistribution.

Périphérique > Redistribution des données > Clients

Sélectionnez **Périphérique** > **Redistribution des données** > **Clients** pour afficher les informations suivantes pour chaque client de redistribution :

Informations sur l’agent de redistribution	Description
Informations sur l’hôte	Informations sur l’hôte pour le client.
Port	Le port que le client de redistribution utilise.
ID Vsys	L’identification pour le système virtuel auquel le client de redistribution est connecté.
Version	La version PAN-OS du client.
État	Affiche le statut du client de redistribution.
PDF/CSV	Les rôles administrateur qui sont au moins dotés de l’accès en lecture seule peuvent exporter le tableau de des informations de redistribution des données au format **PDF/CSV**.
Actualiser les connectés	Met à jour les informations de tous les clients de redistribution connectés.

Périphérique > Redistribution des données > Paramètres du collecteur

Pour configurer une connexion vers un agent de redistribution d’ID utilisateur, saisissez un nom pour le collecteur et la clé pré-partagée.

Paramètres de l’agent de redistribution des données	Description
Nom du collecteur	Saisissez un **Nom de collecteur** (jusqu’à 255 caractères alphanumériques) pour identifier l’agent de redistribution.
Clé pré-partagée du collecteur / Confirmer la clé pré-partagée du collecteur	Saisissez et confirmez la **Clé pré-partagée** (jusqu’à 255 caractères alphanumériques) du collecteur.

Périphérique > Redistribution des données > Inclure/Exclure des réseaux

Utilisez la liste d’inclusion/exclusion de réseaux pour définir les sous-réseaux que l’agent de distribution inclut ou exclut lorsqu’il redistribue les mappages.

Tâche	Description
Ajouter	Pour restreindre la découverte à un sous-réseau donné, **Add (Ajoutez)** un profil de sous-réseau et remplissez les champs suivants : • **Name (Nom)** : saisissez un nom pour identifier le sous-réseau. • **Enabled (Activé)** : sélectionnez cette option pour activer l'inclusion ou l'exclusion du sous-réseau lors de la surveillance du serveur. • **Détection (Discovery)** : précisez si l'agent User-ID va **Inclure** ou **Exclude (Exclure)** le sous-réseau. • **Adresse réseau** : saisissez la plage d'adresses IP du sous-réseau. L'agent applique une règle implicite à la liste qui va tout exclure. Par exemple, si vous ajoutez le sous-réseau 10.0.0.0/8 avec l'option **Inclure,** l'agent exclut tous les autres sous-réseaux, même si vous ne les ajoutez pas à la liste. Ajoutez des entrées avec l'option **Exclure** uniquement si vous souhaitez que l'agent exclue un sous-ensemble de sous-réseaux que vous avez implicitement inclus. Par exemple, si vous ajoutez 10.0.0.0/8 avec l'option **Inclure** et que vous ajoutez 10.2.50.0/22 avec l'option **Exclure**, l'agent User-ID procédera à une découverte sur tous les sous-réseaux de 10.0.0.0/8, sauf 10.2.50.0/22, et exclura tous les sous-réseaux n'appartenant pas à 10.0.0.0/8. Si vous ajoutez des profils **Exclure** sans ajouter de profils **Include (Inclure)**, l'agent exclura tous les sous-réseaux et pas uniquement ceux que vous avez ajoutés.
Supprimer	Pour supprimer un sous-réseau de la liste, sélectionnez-le et cliquez sur **Delete (Supprimer)**. **Conseil**: Pour supprimer un sous-réseau de la liste Inclure/Exclure des réseaux sans effacer sa configuration, modifiez le profil du sous-réseau et désélectionnez l'option **Enabled (Activé)**.
Séquence réseau d'inclusion/ exclusion personnalisée	Par défaut, l'agent évalue les sous-réseaux dans leur ordre d'ajout, les premiers en tête de liste et les derniers en bas de liste. Pour modifier l'ordre d'évaluation, cliquez sur **Séquence réseau d'inclusion/exclusion personnalisée**. Vous pouvez ensuite **Add (Ajouter)**, **Delete (Supprimer)**, **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)** les sous-réseaux pour créer un ordre d'évaluation personnalisé.

Périphérique > Quarantaine du périphérique

La page **Périphérique** > **Quarantaine des périphériques** affiche les périphériques qui sont sur la liste de quarantaine.

Un périphérique qui apparaît dans cette liste de quarantaine suite aux actions suivantes :

- L'administrateur du système a ajouté le périphérique à cette liste manuellement.

  Afin de manuellement **Add (Ajouter)** un périphérique, saisissez le **Host ID** et, en option, le **Serial Number (Numéro de série)** du périphérique que vous devez mettre en quarantaine.
- L'administrateur du système a sélectionné la colonne d'identifiant de l'hôte depuis les journaux de Trafic, GlobalProtect, des menaces ou les Journaux unifiés a sélectionné un périphérique dans cette colonne puis a sélectionné **Block Device**.
- L'appareil a été ajouté automatiquement à la liste de quarantaine :
  - Utilisation d'un profil de transfert de journal avec une règle de stratégie de sécurité dont la liste de correspondances avait une action intégrée définie sur **Quarantaine**.

    *L'ID d'hôte s'affiche automatiquement dans les journaux GlobalProtect. Pour que l'identifiant de l'hôte s'affiche dans les journaux de Trafic, des menaces ou Unifiés, le pare-feu doit avoir au moins une règle de politique de sécurité dans le **Périphérique source** réglée sur **Quarantaine**. Sans ce réglage dans la politique de sécurité, les journaux de Trafic, menaces ou Unifiés n'auront pas l'identifiant de l'hôte, et le profil de transfert des journaux n'entrera pas en vigueur.*
  - Utilisation des paramètres du journal des correspondances HIP avec action intégrée définie sur **Quarantaine**.

    Le pare-feu nécessite une licence d'abonnement GlobalProtect pour ajouter manuellement ou automatiquement des appareils GlobalProtect à la liste de quarantaine et bloquer la connexion pour les appareils*mis en quarantaine.*
- L'appareil a été ajouté à la liste de quarantaine à l'aide d'un API.
- Le pare-feu a reçu la liste de quarantaine dans le cadre d'une saisie redistribuée (la liste de quarantaine a été redistribuée depuis un autre appareil ou pare-feu Panorama).

Le tableau de Quarantaine des périphériques comprend les champs suivants.

Champ	Description
ID d'hôte	Identifiant (ID) d'hôte de l'hôte qui est bloqué.
Motif	Le motif est que le périphérique est en quarantaine. Un motif **Admin Add (ajout par un admin)** signifie qu'un administrateur a manuellement ajouté le périphérique au tableau.
Horodatage	L'heure à laquelle l'administrateur ou la règle de politique de sécurité a ajouté le périphérique à la liste de quarantaine.

Champ	Description
Périphérique/appli source	L’adresse IP de Panorama, du pare-feu ou de l’application tierce qui a ajoutée le périphérique à la liste de quarantaine.
Numéro de série	(En option) Le numéro de série du périphérique en quarantaine (s’il est disponible).
Nom d'utilisateur	(En option) Le nom d'utilisateur du client utilisateur de GlobalProtect qui était connecté au périphérique lorsque celui-ci a été mis en quarantaine.

Vous pouvez exporter la liste des périphériques mis en quarantaine vers un fichier pdf ou csv.

Périphérique > Sources d'informations de machine virtuelle

Cet onglet suit de façon proactive les modifications sur les machines virtuelles installées sur l'une de ces sources : serveur VMware ESXi, serveur VMware vCenter, Amazon Web Services, Virtual Private Cloud (AWS-VPC) ou Google Compute Engine (GCE).

Lors de la surveillance des serveurs ESXi qui font partie de la solution VM-Series édition NSX, utilisez des Groupes d'adresses dynamiques plutôt que d'utiliser des Sources d'informations de machine virtuelle pour en apprendre davantage sur les changements dans l'environnement virtuel. Pour la solution VM-Series édition NSX, le Gestionnaire NSX fournit à Panorama des informations sur le groupe de sécurité NSX auquel appartient une adresse IP. Les informations du Gestionnaire NSX fournit le contexte global permettant la définition des critères de correspondance dans un Groupe d'adresses dynamiques, car il utilise l'ID du profil de service en tant qu'attribut distinctif et vous permet de mettre en œuvre correctement la politique lorsque vous avez des adresses IP qui se chevauchent entre les différents groupes de sécurité NSX.

Vous pouvez enregistrer jusqu'à 32 étiquettes pour une adresse IP.

Vous pouvez surveiller les sources d'informations de deux manières différentes'A0;:

- Le pare-feu peut surveiller votre serveur VMware ESXi, le serveur VMware vCenter, les instances GCE ou les VPC, et récupérer les modifications apportées aux invités configurés sur les sources surveillées. Vous pouvez configurer jusqu'à 10 sources (cumulatif de toutes les sources sur tous les systèmes virtuels configurés) sur un firewall.

  Les conditions suivantes s’appliquent lorsque vos pare-feu sont configurés dans une configuration High Availability (Haute disponibilité ; HA).

  - **Configuration HA active/passive** : seul le pare-feu actif surveille les sources d'informations de machine virtuelle.
  - **Configuration HA active/active** : seul le pare-feu possédant la valeur de priorité `primaire` surveille les sources d'informations de machine virtuelle.

  Pour savoir comment les sources d'informations de machine virtuelle et les groupes d'adresses dynamiques fonctionnent de manière synchrone et vous permettent de surveiller les modifications dans l'environnement virtuel, reportez-vous au Guide de déploiement VM-Series.
- Pour le mappage des adresses IP aux noms d’utilisateurs, vous pouvez configurer les sources d'informations de machine virtuelle sur l'agent User-ID Windows ou sur le pare-feu pour surveiller les serveurs VMware ESXi et vCenter, et récupérer les modifications des invités configurés sur le serveur. L’agent User-ID Windows prend en charge un maximum de 100 sources. La prise en charge de AWS et de Google Compute Engine n’est pas disponible pour l'agent User-ID.

  VMware'A0;Tools doit être installé et exécuté sur chaque machine virtuelle se trouvant sur un serveur'A0;ESXi ou vCenter surveillé. VMware Tools permet de les adresses IP et d'autres valeurs affectées à chaque machine virtuelle.

Pour collecter les valeurs affectées aux machines virtuelles surveillées, le pare-feu surveille les attributs énumérés dans les tableaux suivants.

Attributs surveillés sur une source VMware

- UUID
- Name (Nom)
- Système d’exploitation invité
- Annotation
- État de la machine virtuelle : l'état d'alimentation peut être `poweredOff` (Mis hors tension), `poweredOn` (Mis sous tension), `standBy` (En veille) ou `unknown` (Inconnu).
- Version
- Réseau : Nom du commutateur virtuel, Nom du groupe de ports et ID de VLAN
- Nom du conteneur : Nom vCenter, Nom de l'objet de centre de données, Nom du pool de ressources, Nom du cluster, Hôte et Adresse IP de l'hôte.

Attributs surveillés sur AWS-VPC

- Architecture
- Système d’exploitation invité
- ID d’image
- ID de l’instance
- État de l’instance
- Type d’instance
- Nom de la clé
- Emplacement : Location, Nom du groupe et Zone de disponibilité
- Nom DNS privé
- Nom DNS public
- ID de sous-réseau
- Étiquette (clé, valeur) ; jusqu’à 18 étiquettes prises en charge par instance
- ID VPC

Attributs surveillés pour Google Compute Engine (CGE)

- Nom d'hôte de la machine virtuelle
- Type de machine
- Numéro du projet
- Source (Type de système d’exploitation)
- Status (État)
- Sous-réseau

Attributs surveillés pour Google Compute Engine (CGE)
• Réseau VPC • Employé

Add (Ajouter) : cliquez sur **Add (Ajouter)** pour ajouter une nouvelle source pour la surveillance des machines virtuelles, puis renseignez les informations en fonction de la source que vous surveillez :

- Pour les serveurs VMware ESXi ou vCenter, reportez-vous aux Paramètres pour activer les sources d'informations de machine virtuelle pour les serveurs VMware ESXi et vCenter.
- Pour AWS-VPC, reportez-vous aux Paramètres pour activer les sources d'informations de machine virtuelle pour AWS VPC.
- Pour Google Compute Engine (GCE), reportez-vous à la section Paramètres pour activer les sources d'informations de machine virtuelle pour Google Compute Engine.

Refresh Connected (Actualiser les éléments connectés) : actualise l'état de la connexion qui s'affiche à l'écran ; cette option n'actualise pas la connexion entre le pare-feu et les sources surveillées.

Delete (Supprimer) : supprime la source d'informations de machine virtuelle que vous sélectionnez.

PDF/CSV : exporte le tableau de configuration des sources d'informations de machine virtuelle au format PDF ou dans un fichier Comma-Separated Values (valeur séparée par une virgule ; CSV). Reportez-vous à la section Exportation du tableau de configuration.

Paramètres pour activer les sources d'informations de machine virtuelle pour les Serveurs VMware ESXi et vCenter

Le tableau suivant décrit les paramètres que vous pouvez configurer pour activer les sources d'informations de machine virtuelle pour les serveurs VMware ESXi et vCenter.

Pour récupérer les étiquettes des machines virtuelles, le pare-feu exige un compte avec accès en lecture seule sur les serveurs VMware ESXi et vCenter.

Paramètres pour activer les sources d'informations de machine virtuelle pour VMware ESXi ou les serveurs vCenter	
Name (Nom)	Saisissez un nom permettant d'identifier la source surveillée (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Type	Indiquez si l'hôte/la source surveillé(e) est un **ESXi server (Serveur ESXi)** ou un **vCenter server (Serveur vCenter)**.
Description	(Facultatif) Ajoutez une étiquette permettant d'identifier l'emplacement ou la fonction de la source.
Port	Indiquez le port d'écoute de l'hôte/la source (port par défaut : 443).

Paramètres pour activer les sources d’informations de machine virtuelle pour VMware ESXi ou les serveurs vCenter	
Activé	Par défaut, la communication entre le pare-feu et la source configurée est activée. L'état de la connexion entre la source surveillée et le pare-feu s'affiche dans l'interface comme suit'A0;: •  Connecté •  Déconnecté •  En attente ; l’état de la connexion s’affiche également en jaune lorsque la source surveillée est désactivée. Désélectionnez l'option **Enabled (Activé)** pour désactiver la communication entre l'hôte et le pare-feu.
délai d'expiration	Saisissez l'intervalle en heures après lequel la connexion à la source surveillée est fermée, si l'hôte ne répond pas (plage de 2 à 10 ; par défaut 2). (Facultatif) Pour modifier la valeur par défaut, vous devez **Activer le délai d’expiration lorsque la source est déconnectée** et indiquer une valeur. Lorsque la limite définie est atteinte, si l’hôte n’est pas accessible ou ne répond pas, le pare-feu ferme la connexion à la source.
Source	Saisissez le nom de domaine complet (FQDN) ou l'adresse'A0;IP de l'hôte/ la source surveillé(e).
Username (Nom d’utilisateur)	Indiquez le nom d'utilisateur requis pour l'authentification auprès de la source.
Mot de passe	Saisissez et confirmez le mot de passe.
Intervalle de mise à jour	Indiquez l'intervalle (en secondes) auquel le pare-feu récupère les informations de la source (plage de 5 à 600 ; par défaut 5).

Paramètres pour activer les sources d’informations de machine virtuelle pour AWS VPC

Le tableau suivant décrit le paramètre que vous configurez pour activer les sources d’informations de machine virtuelle pour un AWS VPC.

Paramètres pour activer les sources d’informations de machine virtuelle pour AWS VPC	
Name (Nom)	Saisissez un nom permettant d'identifier la source surveillée (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement.
Type	Sélectionnez **AWS VPC**.
Description	(Facultatif) Ajoutez une étiquette permettant d’identifier l’emplacement ou la fonction de la source.
Activé	Par défaut, la communication entre le pare-feu et la source configurée est activée. L'état de la connexion entre la source surveillée et le pare-feu s'affiche dans l'interface comme suit'A0;: •  Connecté •  Déconnecté •  En attente ; l’état de la connexion s’affiche également en jaune lorsque la source surveillée est désactivée. Désélectionnez l'option **Enabled (Activé)** pour désactiver la communication entre l'hôte et le pare-feu.
Source	Ajoutez l'URI dans lequel Virtual Private Cloud (VPC) réside. Par exemple, ec2.us-west-1.amazonaws.com La syntaxe est ec2.<*your_AWS_region*>.amazonaws.com ; pour AWS China, la syntaxe est : ec2.<AWS_region>.amazonaws.com.cn
ID de clé d’accès	Saisissez la chaîne de texte alphanumérique qui identifie de manière unique l’utilisateur qui possède ou est autorisé à accéder au compte AWS. Ces informations font partie des informations d'identification de sécurité'A0;AWS. Le pare-feu nécessite les informations d'identification (l'ID de clé d'accès et la clé d'accès secrète) pour pouvoir signer numériquement les appels de l'API aux services AWS.
Clé d'accès secrète	Saisissez et confirmez le mot de passe.
Intervalle de mise à jour	Indiquez l’intervalle, en secondes, auquel le pare-feu récupère les informations de la source (plage de 60 à 1 200 ; par défaut 60).

Paramètres pour activer les sources d’informations de machine virtuelle pour AWS VPC	
délai d'expiration	Intervalle en heures après lequel la connexion à la source surveillée est fermée, si l'hôte ne répond pas (par défaut 2) (Facultatif) **Activer le délai d’expiration lorsque la source est déconnectée**. Lorsque la limite définie est atteinte, si la source n’est pas accessible ou ne répond pas, le pare-feu ferme la connexion à la source.
ID VPC	Saisissez l'ID du AWS-VPC à surveiller, par exemple, vpc-1a2b3c4d. Seules les instances'A0;EC2 déployées dans ce VPC sont surveillées. Si votre compte est configuré pour utiliser un VPC par défaut, l'ID du VPC par défaut est répertoriée sous Attributs du compte'A0;AWS.

Paramètres pour activer les sources d’informations de machine virtuelle pour Google Compute Engine

Périphérique > **Source d'informations de machine virtuelle** > **Ajouter**

Le tableau suivant décrit les paramètres que vous devez configurer pour activer les sources d’informations de machine virtuelle pour les instances de Google Compute Engine sur Google Cloud Platform. Activez la surveillance des instances de Google Compute Engine (GCE) pour permettre au pare-feu (physique ou virtuel sur site, ou fonctionnant dans Google Cloud) de récupérer une balise, une étiquette ou toute autre métadonnée sur les instances s’exécutant dans une zone particulière de Google Cloud du projet. Pour obtenir de plus amples renseignements sur l’utilisation du pare-feu VM-Series dans Google Cloud Platform, consultez le Guide de déploiement VM-Series.

Paramètres pour activer les sources d’informations de machine virtuelle pour Google Compute Engine	
Name (Nom)	Saisissez un nom permettant d'identifier la source surveillée (31 caractères maximum). Le nom est sensible à la casse, doit être unique et peut inclure uniquement des lettres, chiffres, espaces, traits d’union et traits de soulignement.
Type	Sélectionnez **Google Compute Engine**.
Description	(Facultatif) Ajoutez une étiquette permettant d’identifier l’emplacement ou la fonction de la source.
Activé	La communication entre le pare-feu et la source configurée est activée par défaut. L'état de la connexion entre la source surveillée et le pare-feu s'affiche dans l'interface comme suit : 

Paramètres pour activer les sources d’informations de machine virtuelle pour Google Compute Engine	
	• -Lié  • -Débranché  • —En attente ou la source surveillée est désactivée. Décochez l'option **Activé** pour désactiver la communication entre la source configurée et le pare-feu. Lorsque vous désactivez la communication, toutes les adresses IP et balises enregistrées sont supprimées du groupe d'adresses dynamiques associé. C’est-à-dire que les règles de politique ne s’appliqueront pas aux instances GCE de ce projet Google Cloud.
Type d'authentification de service	Sélectionnez le pare-feu VM-Series qui fonctionne sur GCE ou sur un compte de service. • **VM-Series running on GCE (Pare-feu VM-Series fonctionnant sur GCE)** : sélectionnez cette option sur le pare-feu matériel ou VM-Series sur lequel vous activez la Surveillance VM n’est pas déployé dans Google Cloud Platform. • **Service Account (Compte de service)** : sélectionnez cette option si vous surveillez les instances de Google Cloud Engine sur un pare-feu qui n’est pas déployé dans Google Cloud Platform. Cette option vous permet d’utiliser un compte Google spéciale qui appartient à la machine virtuelle ou à l’application plutôt que d’utiliser un compte d’utilisateur final. Le compte de service doit disposer des politiques IAM (privilège **Compute Engine** > **Compute Viewer**) qui autorisent l’accès à l’API Google API et qui l’autorisent à interroger les machines virtuelles dans le projet Google Cloud Project afin d’obtenir les métadonnées des machines virtuelles.
Informations d’identification pour le compte de service	(Uniquement pour le compte de service) Téléchargez le fichier JSON qui contient les informations d’identification pour le compte de service. Ce fichier permet au pare-feu de s’authentifier auprès de l’instance et autorise l'accès aux métadonnées. Vous pouvez créer un compte sur la console Google Cloud (**IAM & admin (IAM & administrateur)** > **Service Accounts (Comptes de service)**). Reportez-vous à la documentation de Google pour obtenir des informations sur la création d’un compte, sur l’ajout d’une clé et sur le téléchargement du fichier JSON que vous devez charger sur le pare-feu.

Paramètres pour activer les sources d’informations de machine virtuelle pour Google Compute Engine	
Numéro du projet	Entrez la chaîne de texte alphanumérique qui identifie de manière unique le projet Google Cloud que vous souhaitez surveiller.
Nom de la zone	Saisissez les informations sur la zone sous forme d’une chaîne contenant un maximum de 63 caractères de longueur. Par exemple : **`us-west1-a`**.
Intervalle de mise à jour	Indiquez l’intervalle (en secondes) auquel le pare-feu récupère les informations de la source (plage de 60 à 1 200 ; par défaut 60).
délai d'expiration	Intervalle (en heures) après lequel la connexion à la source surveillée est fermée si l'hôte ne répond pas (par défaut 2) (Facultatif) **Activer le délai d’expiration lorsque la source est déconnectée**. Lorsque la limite définie est atteinte, si la source n’est pas accessible ou ne répond pas, le pare-feu ferme la connexion à la source. Lorsque la source est déconnectée, toutes les étiquettes et adresses IP qui ont été enregistrées depuis ce projet sont supprimées du groupe d’adresses dynamiques.

Périphérique > Résolution des problèmes

- **Périphérique** > **Dépannage**
- **Panorama** > **Périphériques gérés** > **Dépannage**

Avant de valider des changements de configuration apportés à un groupe de périphériques ou à un modèle, testez la fonctionnalité à partir de l'interface Web pour vérifier que les changements n'ont pas introduit de problèmes de connectivité dans la configuration active et que vos politiques autorisent ou refusent correctement le trafic.

- **Tests de correspondance de la politique**
  - Correspondance de la politique de sécurité
  - Correspondance de la politique QoS
  - Correspondance de la politique d'authentification
  - Correspondance politique SSL/déchiffrement
  - Correspondance de la politique NAT
  - Correspondance à la politique PBF (transfert basé sur une politique)
  - Correspondance de la politique DoS
- **Tests de connectivité**
  - Routage
  - Test WildFire
  - Archivage sécurisé des menaces
  - Ping
  - Trace Route
  - Connectivité du collecteur de journaux
  - Liste dynamique externe
  - Serveur de mises à jour
  - État du service de journalisation du cloud de test GP
  - État du service du cloud de test GP

Correspondance de la politique de sécurité

Champ	Description
Configuration du test	
Sélectionner le test	Sélectionnez le test de correspondance à la politique à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs

Champ	Description
	et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.
De	Saisissez la zone d'où le trafic tire son origine.
A	Sélectionnez la zone de destination du trafic.
Source	Saisissez l'adresse IP d'où le trafic tire son origine.
Destination	Saisissez l'adresse IP de destination du trafic.
Port de destination	Saisissez le port de destination spécifique pour lequel le trafic est prévu.
Source User (Utilisateur source)	Saisissez l'utilisateur de qui provient le trafic.
Protocole	Saisissez le protocole IP utilisé pour l'acheminement. La valeur peut aller de 0 à 255.
Affichez toutes les règles de correspondance potentielles jusqu'à la première règle d'autorisation.	Activez cette option pour afficher toutes les correspondances de règles potentielles jusqu'au résultat de la première règle mise en correspondance. Désélectionnez (décochez) cette option pour obtenir uniquement la première règle mise en correspondance dans les résultats des tests.
Application	Sélectionnez le trafic d'application que vous souhaitez tester.
Catégorie	Sélectionnez la catégorie de trafic que vous souhaitez tester.
(Pare-feu uniquement) Vérifiez le masque HIP.	Cochez cette option pour vérifier l'état de sécurité du périphérique final qui accède à votre réseau.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic.

Champ	Description
	• État : indique l’état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n’a pu être effectué, l’un des résultats suivants s’affiche : • `N/A` : le test ne s’applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée. • `Shared policy disabled on device` : Les paramètres de Panorama sur le périphérique ne permettent pas la transmission de la politique à partir de Panorama.

Correspondance de la politique QoS

Champ	Description
Configuration du test	
Sélectionner le test	Sélectionnez le test de correspondance à la politique à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d’accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.
De	Saisissez la zone d'où le trafic tire son origine.
A	Sélectionnez la zone de destination du trafic.
Source	Saisissez l’adresse IP d'où le trafic tire son origine.
Destination	Saisissez l'adresse IP de destination du trafic.
Port de destination	Saisissez le port de destination spécifique pour lequel le trafic est prévu.
Source User (Utilisateur source)	Sélectionnez l’utilisateur de qui provient le trafic.

Champ	Description
Protocole	Saisissez le protocole IP utilisé pour l'acheminement. La valeur peut aller de 0 à 255.
Application	Sélectionnez le trafic d’application que vous souhaitez tester.
Catégorie	Sélectionnez la catégorie de trafic que vous souhaitez tester.
Type de point de code	Sélectionnez le type de codage par point de code que vous voulez tester.
Valeur de point de code	Spécifiez la valeur du codage par point de code : • **DSCP** : de 0 à 63 • **ToS** : de 0 à 7
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l’état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n’a pu être effectué, l’un des résultats suivants s’affiche : • `N/A` : le test ne s’applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée. • `Shared policy disabled on device` : Les paramètres de Panorama sur le périphérique ne permettent pas la transmission de la politique à partir de Panorama.

Correspondance de la politique d’authentification

Champ	Description
Configuration du test	
Sélectionner le test	Sélectionnez le test de correspondance à la politique à exécuter.

Champ	Description
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.
De	Saisissez la zone d'où le trafic tire son origine.
A	Sélectionnez la zone de destination du trafic.
Source	Saisissez l'adresse IP d'où le trafic tire son origine.
Destination	Saisissez l'adresse IP de destination du trafic.
Catégorie	Sélectionnez la catégorie de trafic que vous souhaitez tester.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche : • `N/A` : le test ne s'applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée. • `Shared policy disabled on device` : Les paramètres de Panorama sur le périphérique ne permettent pas la transmission de la politique à partir de Panorama.

Correspondance politique SSL/déchiffrement

Champ	Description
Configuration du test	
Sélectionner le test	Sélectionnez le test de correspondance à la politique à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.
De	Saisissez la zone d'où le trafic tire son origine.
A	Sélectionnez la zone de destination du trafic.
Source	Saisissez l'adresse IP d'où le trafic tire son origine.
Destination	Saisissez l'adresse IP de destination du trafic.
Application	Sélectionnez le trafic d'application que vous souhaitez tester.
Catégorie	Sélectionnez la catégorie de trafic que vous souhaitez tester.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`.

Champ	Description
	• Résultat : affiche le résultat du test. Si le test n’a pu être effectué, l’un des résultats suivants s’affiche : • `N/A` : le test ne s’applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée.

Correspondance de la politique NAT

Champ	Description
Configuration du test	
Sélectionner le test	Sélectionnez le test de correspondance à la politique à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d’accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.
De	Saisissez la zone d'où le trafic tire son origine.
A	Sélectionnez la zone de destination du trafic.
Source	Saisissez l’adresse IP d'où le trafic tire son origine.
Destination	Saisissez l'adresse IP de destination du trafic.
Port source	Saisissez le port spécifique d'où le trafic tire son origine.
Port de destination	Saisissez le port de destination spécifique pour lequel le trafic est prévu.
Protocole	Saisissez le protocole IP utilisé pour l'acheminement. La valeur peut aller de 0 à 255.
Vers l'interface	Saisissez l’interface de destination du périphérique vers laquelle le trafic doit se rendre.

Champ	Description
ID du périphérique HA	Saisissez l'ID du périphérique HA : • **0** : homologue HA principal • **1** : homologue HA secondaire
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche : • `N/A` : le test ne s'applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée. • `Shared policy disabled on device` : Les paramètres de Panorama sur le périphérique ne permettent pas la transmission de la politique à partir de Panorama.

Correspondance à la politique PBF (transfert basé sur une politique)

Champ	Description
Configuration du test	
Sélectionner le test	Sélectionnez le test de correspondance à la politique à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.

Champ	Description
De	Saisissez la zone d'où le trafic tire son origine.
Interface d’origine	Saisissez l’interface du périphérique de laquelle le trafic tire son origine.
Source	Saisissez l’adresse IP d'où le trafic tire son origine.
Destination	Saisissez l'adresse IP de destination du trafic.
Port de destination	Saisissez le port de destination spécifique pour lequel le trafic est prévu.
Source User (Utilisateur source)	Saisissez l’utilisateur de qui provient le trafic.
Protocole	Saisissez le protocole IP utilisé pour l'acheminement. La valeur peut aller de 0 à 255.
Application	Sélectionnez le trafic d’application que vous souhaitez tester.
ID du périphérique HA	ID du périphérique HA : • **0** : homologue HA principal • **1** : homologue HA secondaire
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l’état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n’a pu être effectué, l’un des résultats suivants s’affiche : • `N/A` : le test ne s’applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée. • `Shared policy disabled on device` : Les paramètres de Panorama sur le périphérique ne permettent pas la transmission de la politique à partir de Panorama.

Correspondance de la politique DoS

Champ	Description
Configuration du test	
Sélectionner le test	Sélectionnez le test de correspondance à la politique à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.
De	Saisissez la zone d'où le trafic tire son origine.
A	Sélectionnez la zone de destination du trafic.
Interface d'origine	Saisissez l'interface du périphérique de laquelle le trafic tire son origine.
Vers l'interface	Saisissez l'interface de destination du périphérique vers laquelle le trafic doit se rendre.
Source	Saisissez l'adresse IP d'où le trafic tire son origine.
Destination	Saisissez l'adresse IP de destination du trafic.
Port de destination	Saisissez le port de destination spécifique pour lequel le trafic est prévu.
Source User (Utilisateur source)	Saisissez l'utilisateur de qui provient le trafic.
Protocole	Saisissez le protocole IP utilisé pour l'acheminement. La valeur peut aller de 0 à 255.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé :

Champ	Description
	• Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche : • `N/A` : le test ne s'applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée.

Routage

Champ	Description
Sélectionner le test	Sélectionnez le test de connectivité à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.
Recherche FiB, Recherche Mfib	Sélectionnez l'une des recherches suivantes : • **FiB** : Effectuez la recherche d'itinéraires au sein de la table de routage active. • **Mfib** : Effectuez la recherche d'itinéraires multicast au sein de la table de routage active.
IP de destination	Saisissez l'adresse IP vers laquelle le trafic doit se rendre.
Virtual Router (routeur virtuel - VR)	Routeur virtuel spécifique au sein duquel le test de routage est effectué. Sélectionnez le routeur virtuel dans le menu déroulant.
ECMP	
IP source	Saisissez l'adresse IP spécifique de laquelle provient le trafic.

Champ	Description
Port source	Saisissez le port spécifique duquel provient le trafic.
IP de destination	Saisissez l'adresse IP spécifique vers laquelle le trafic doit se rendre.
Port de destination	Saisissez le port de destination spécifique pour lequel le trafic est prévu.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche : • `N/A` : le test ne s'applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée.

Test WildFire

Champ	Description
Sélectionner le test	Sélectionnez le test de connectivité à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.
contrôle	Sélectionnez le canal WildFire : **`Public`** ou **`Private`**.

Champ	Description
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche : • `N/A` : le test ne s'applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée.

Archivage sécurisé des menaces

Champ	Description
Sélectionner le test	Sélectionnez le test de connectivité à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic.

Champ	Description
	• État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche : • `N/A` : le test ne s'applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée.

Ping

Le test de résolution de problèmes ping n'est pris en charge que sur les pare-feu exécutant les versions 9.0 ou ultérieures de PAN-OS.

Champ	Description
Sélectionner le test	Sélectionnez le test de connectivité à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.
Contourne la table de routage, utilise l'interface spécifiée	Activez cette option pour contourner la table de routage et utiliser une interface spécifiée. Désélectionnez (décochez) cette option pour tester la table de routage configurée.
Nombre	Saisissez le nombre de requêtes à envoyer. Le nombre par défaut est 5.
Ne pas fragmenter les paquets de demande d'écho (IPv4)	Activez cette option pour éviter de fragmenter les paquets de requêtes écho du test. Désactivation
Force to IPv6 destination	Activez cette option effectuer le test de force vers la destination IPv6.
Intervalle	Précisez un délai, en secondes, entre les requêtes (plage comprise entre 1 et 2 000 000 000).
Source	Saisissez l'adresse source de la requête écho.

Champ	Description
Ne tentez pas d’imprimer les adresses symboliquement.	Activez cette option pour afficher les adresses IP dans les résultats des tests et pour ne pas résoudre l’adresse IP/nom d’hôte. Désactivez (décochez) cette option pour résoudre les adresses IP/noms d’hôte.
Pattern	Spécifiez le modèle de remplissage hexadécimal.
Taille	Saisissez la taille, en octets, des paquets de requêtes (la plage est comprise entre 0 et 65 468).
Tos	Saisissez la valeur adresse IP type de service (plage comprise entre 1 et 255).
TTL	Saisissez la valeur de durée de vie IP en sauts - valeur de la limite de sauts IPv6 (plage comprise entre 1 et 255).
Afficher les résultats détaillés	Activez cette option pour afficher les résultats détaillés du test.
Hôte	Saisissez le nom d'hôte ou l'adresse IP de l’hôte distant.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l’état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n’a pu être effectué, l’un des résultats suivants s’affiche : • `N/A` : le test ne s’applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée.

Trace Route

Champ	Description
Sélectionner le test	Sélectionnez le test de connectivité à exécuter.

Champ	Description
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.
Utilisez IPv4	Activez cette option pour utiliser l'adresse IPv4 des périphériques sélectionnés.
Utilisez IPv6	Activez cette option pour utiliser l'adresse IPv6 des périphériques sélectionnés.
Premier TTL	Saisissez la durée de vie utilisée dans le premier paquet à analyser sortant (plage comprise entre 1 et 255).
Max TTL	Saisissez les sauts de durée de vie maximaux (plage comprise entre 1 et 255).
Port	Saisissez le numéro de port de base utilisé dans le sondage.
Tos	Saisissez la valeur adresse IP type de service (plage comprise entre 1 et 255).
Attente	Indiquez le nombre de secondes pendant lesquelles attendre une réponse (plage comprise entre 1 et 99 999).
Suspendu	Saisissez le temps, en millisecondes, pendant lesquelles faire un arrêt entre les sondages (la valeur est comprise entre 1 et 2 000 000 000).
Définir le bit « Ne pas fragment »	Activez cette option pour ne pas fragmenter le paquet ICMP en plusieurs paquets si le chemin ne peut prendre en charge l'unité de transmission maximale (MTU).
Activer le débogage au niveau du socket	Activez cette option pour vous permettre de déboguer au niveau du socket.
Passerelle	Indiquez un maximum de huit passerelles de routage de source souple.

Champ	Description
Ne tentez pas d’imprimer les adresses symboliquement.	Activez cette option pour afficher les adresses IP dans les résultats des tests et pour ne pas résoudre l’adresse IP/nom d’hôte. Désactivez (décochez) cette option pour résoudre les adresses IP/noms d’hôte.
Contourner les tables de routage et envoyer directement à un hôte	Activez cette option pour contourner les tables de routage et effectuez le test directement auprès de l’hôte.
Source	Saisissez une adresse source dans les paquets à analyser sortants.
Hôte	Saisissez le nom d'hôte ou l'adresse IP de l’hôte distant.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l’état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n’a pu être effectué, l’un des résultats suivants s’affiche : • `N/A` : le test ne s’applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée.

Connectivité du collecteur de journaux

Champ	Description
Sélectionner le test	Sélectionnez le test de connectivité à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d’accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.

Champ	Description
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels qui ont été sélectionnés à des fins de test.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche : • `N/A` : le test ne s'applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée.

Liste dynamique externe

Champ	Description
Sélectionner le test	Sélectionnez le test de connectivité à exécuter.
(Panorama uniquement) Sélectionnez le périphérique	**Select device/VSYS (Sélectionnez le périphérique/le système virtuel)** pour spécifier les périphériques et les systèmes virtuels pour lesquels tester la fonctionnalité de la politique. Les administrateurs et les utilisateurs des groupes de périphériques et des modèles se voient présenter les périphériques et les systèmes virtuels selon leur domaine d'accès. De plus, vous pouvez sélectionner le serveur de gestion Panorama en tant que périphérique.
(Panorama uniquement) Sélectionnez les périphériques	Dresse la liste des périphériques et des systèmes virtuels sélectionnés à des fins de test.
Test URL	Spécifiez l'URL à utiliser pour tester la connexion.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté.

Champ	Description
	(Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche : • `N/A` : le test ne s'applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée.

Serveur de mises à jour

Champ	Description
Sélectionner le test	Sélectionnez le test de connectivité à exécuter.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. (Panorama uniquement) Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche : • `N/A` : le test ne s'applique pas au périphérique. • `Device not connected` : la connexion au périphérique a été abandonnée.

État du service de journalisation du cloud de test GP

Testez l'état de connectivité au service de journalisation du cloud. Ce test n'est disponible que sur un serveur de gestion Panorama exécutant la version 1.3 ou ultérieure du plug-in des services de cloud.

Champ	Description
Sélectionner le test	Sélectionnez le test de connectivité à exécuter.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche :

État du service du cloud de test GP

Testez l'état de connectivité à GlobalProtect en tant que Service. Ce test n'est disponible que sur un serveur de gestion Panorama exécutant la version 1.3 ou ultérieure du plug-in des services de cloud.

Champ	Description
Sélectionner le test	Sélectionnez le test de connectivité à exécuter.
Résultats	Sélectionnez cette option pour afficher les détails des résultats du test exécuté. Lorsque vous exécutez le test pour plusieurs périphériques gérés, les résultats affichent les informations suivantes pour chaque périphérique testé : • Groupe de périphériques : nom du groupe de périphériques auquel le pare-feu qui traite le trafic appartient. • Pare-feu : nom du pare-feu qui traite le trafic. • État : indique l'état du test : `Success` ou `Failure`. • Résultat : affiche le résultat du test. Si le test n'a pu être effectué, l'un des résultats suivants s'affiche :

Périphérique > Systèmes virtuels

Un système virtuel (vsys) est une instance de pare-feu indépendante (virtuelle) que vous pouvez gérer séparément dans un pare-feu physique. Chaque système virtuel peut être un pare-feu indépendant ayant sa politique de Sécurité, ses interfaces et administrateurs propres. Un système virtuel vous permet de segmenter l'administration de toutes les politiques, de la génération de rapports et des fonctions de visibilité proposées par le pare-feu.

Par exemple, si vous souhaitez personnaliser les fonctions de sécurité du trafic associé à votre service financier, vous pouvez définir un système virtuel Finance et définir des politiques de sécurité spécifiques à ce service. Pour optimiser l'administration des politiques, vous pouvez séparer la gestion des comptes administrateur pour les fonctions réseau et de pare-feu générales, tout en créant des comptes administrateur de système virtuel qui permettent d'accéder à chaque système virtuel. Cela permet à l'administrateur de système virtuel du service Finance de gérer la politique de sécurité de ce service uniquement.

Les fonctions de réseautage (tels que le routage statique et dynamique, les adresses IP des interfaces et les tunnels IPSec) appartiennent à un pare-feu complet et à ses systèmes virtuels. Une configuration de système virtuel (**Device [appareil]** > **Virtual Systems [système virtuels]**) ne contrôle pas les fonctions du pare-feu et du réseau (comme le routage statique ou dynamique, les adresses IP des interfaces, les tunnels IPSec, les VLAN, les câbles virtuels, les routeurs virtuels, les tunnels GRE, le DHCP, le proxy DNS, la QoS, le LLDP et les profils de réseaux). Pour chaque système virtuel, vous pouvez spécifier un ensemble d'interfaces de pare-feu physiques et logiques (notamment des VLAN et des câbles virtuels) et des zones de sécurité. Si vous avez besoin d'une segmentation de routage pour chaque système virtuel, vous devez créer et affecter des routeurs virtuels supplémentaires et affecter des interfaces, des VLAN et des câbles virtuels, le cas échéant.

Si vous utilisez un modèle Panorama pour définir vos systèmes virtuels, vous pouvez définir un système virtuel par défaut. Le système virtuel par défaut et la fonction de systèmes virtuels multiples déterminent si un pare-feu accepte des configurations spécifiques au système virtuel lors de la validation d'un modèle :

- Les pare-feux qui ont la fonction de systèmes virtuels multiples activée acceptent des configurations spécifiques au système virtuel pour tous les systèmes virtuels définis dans le modèle.
- Les pare-feux qui n'ont pas la fonction de systèmes virtuels multiples activée acceptent des configurations spécifiques uniquement au système virtuel par défaut. Si vous ne configurez pas de système virtuel par défaut, ces pare-feu n'accepteront pas de configurations propres au système virtuel.

> *Les pare-feu PA-400, PA-3200, PA-5200, ainsi que les pare-feu PA-5400 Series et PA-7000 Series prennent en charge plusieurs systèmes virtuels. Cependant, les pare-feu PA-400 Series et PA-3200 Series exigent une licence pour l'activation de plusieurs systèmes virtuels. Les pare-feu PA-220 et PA-800 Series ne prennent pas en charge plusieurs systèmes virtuels.*

Avant d'activer plusieurs systèmes virtuels, notez les points suivants :

- Un administrateur de système virtuel crée et gère tous les éléments nécessaires à la politique de sécurité par système virtuel attribué.
- Les zones sont des objets au sein d'un système virtuel. Avant de définir une politique ou un objet de politique, sélectionnez le **Virtual System (Système virtuel)** approprié dans la liste déroulante de l'onglet **Policies (Politiques)** ou **Objects (Objets)**.

- Vous pouvez définir des destinations de journalisation à distance (SNMP, Syslog et messages), des applications, des services et des profils applicables à tous les systèmes virtuels (partagés) ou à un seul système virtuel.
- Si vous disposez de plusieurs systèmes virtuels, vous pouvez sélectionner un système virtuel en tant que pôle User-ID afin de partager les informations de mappage adresse IP/nom d'utilisateur entre les systèmes virtuels.
- Vous pouvez configurer des itinéraires de service globaux (pour tous les systèmes virtuels d'un pare-feu) ou spécifiques aux systèmes virtuels (Périphérique > Configuration > Services).
- Vous pouvez renommer un système virtuel uniquement sur le pare-feu local. La modification du nom d'un système virtuel n'est pas prise en charge sur Panorama. Si vous renommez un système virtuel sur Panorama, il en résulte un tout nouveau système virtuel, ou le nom du système virtuel est associé au mauvais système virtuel sur le pare-feu.

Avant de définir un système virtuel, vous devez d'abord activer la fonctionnalité de systèmes virtuels multiples sur le pare-feu. Sélectionnez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)**, modifiez les **General Settings (Paramètres généraux)**, sélectionnez **Multi Virtual System Capability (Fonction de systèmes virtuels multiples)**, puis cliquez sur **OK**. Ceci ajoute une page **Device (Périphérique)** > **Virtual Systems (Systèmes virtuels)**. Sélectionnez la page, **Add (Ajoutez)** un système virtuel et indiquez les informations suivantes.

Paramètres d'un système virtuel	Description
ID	Saisissez l'identifiant (entier) du système virtuel. Pour plus d'informations sur le nombre de systèmes virtuels pris en charge, reportez-vous à la fiche technique de votre modèle de pare-feu. *si vous utilisez un modèle Panorama pour configurer le système virtuel, ce champ ne s'affiche pas.*
Name (Nom)	Saisissez un nom pour identifier le système virtuel (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement. *si vous utilisez un modèle Panorama pour appliquer des configurations de système virtuel, le nom du système virtuel dans le modèle doit correspondre au nom du système virtuel sur le pare-feu.*
Autoriser le transfert du contenu déchiffré	Sélectionnez cette option pour autoriser le système virtuel à transférer du contenu déchiffré à un service externe lors de la mise en miroir du port ou de l'envoi de fichiers WildFire pour analyse. Reportez-vous également à la section Mise en miroir du port de déchiffrement.
Onglet Général	Sélectionnez un objet de **DNS Proxy (Proxy DNS)** si vous souhaitez appliquer des règles de proxy DNS à ce système virtuel. (Réseau > Proxy DNS). Pour inclure des objets d'un type donné, sélectionnez ce type (interface, VLAN, câble virtuel, routeur virtuel ou système virtuel visible), **Add (Ajoutez)** un objet,

Paramètres d'un système virtuel	Description
	puis sélectionnez l'objet dans la liste déroulante. Vous pouvez ajouter un ou plusieurs objets d'un quelconque type. Pour supprimer un objet, sélectionnez-le et **Delete (Supprimez)**-le.
Onglet Ressource	Indiquez les limites de ressources suivantes autorisées pour ce système virtuel : Chaque champ affiche la plage de valeurs valide; qui varie selon le modèle de pare-feu. Le paramètres par défaut est fixé sur 0, ce qui signifie que la limite du système virtuel est la limite du modèle de pare-feu. Cependant, la limite d'un paramètre spécifique n'est pas reproduite pour chaque système virtuel. Par exemple, si un pare-feu dispose de quatre systèmes virtuels, chaque système virtuel ne peut disposer du nombre total de règles de décryptage autorisées par pare-feu. Une fois que le nombre total de règles de décryptage pour tous les systèmes virtuels atteint la limite du pare-feu, vous ne pouvez en ajouter plus. • **Sessions Limit (Limite de sessions)** : nombre maximum de sessions. *Si vous utilisez la commande `show session meter` de la CLI, le pare-feu affiche le nombre maximal de sessions autorisé par plan de données, le nombre de sessions actuelles qui sont utilisées par le système virtuel et le nombre limité de sessions par système virtuel. Sur les pare-feu PA-5200 Series ou PA-7000 Series, le nombre de sessions actuelles qui sont utilisées peut être supérieur au nombre maximal de sessions configuré, puisque chaque système virtuel comporte plusieurs plans de données. La limite des sessions que vous avez configurée sur un pare-feu PA-5200 Series ou PA-7000 Series s'applique à chaque plan de données ; le nombre maximal par système virtuel est donc supérieur.* • **Security Rules (Règles de sécurité)** : nombre maximum de règles de sécurité. • **NAT Rules (Règles NAT)** : nombre maximum de règles NAT. • **Decryption Rules (Règles de décryptage)** : nombre maximum de règles de déchiffrement. • **QoS Rules (Règles QoS)** : nombre maximum de règles QoS. • **Application Override Rules (Règles de contrôle prioritaire sur l'application)** : nombre maximum de règles de contrôle prioritaire sur l'application. • **Policy Based Forwarding Rules (Règles de transfert basé sur une politique)** : nombre maximum de règles de transfert basé sur une politique (PBF). • **Authentication Rules (Règles d'authentification)** : nombre maximal de règles d'authentification. • **DoS Protection Rules (Règles de protection DoS)** : nombre maximum de règles de déni de service (DoS).

Paramètres d’un système virtuel	Description
	• **Site to Site VPN Tunnels (Tunnels VPN de site à site)** : nombre maximum de tunnels VPN de site à site. • **Concurrent GlobalProtect Tunnels (Tunnels GlobalProtect simultanés)** : nombre maximum d'utilisateurs GlobalProtect à distance simultanés. • **Inter-Vsys User-ID Data Sharing (Partage de données d’ID utilisateur Inter-Vsys)**— La configuration d’un concentrateur de données d’ID utilisateur nécessite des privilèges de superutilisateur ou d’administrateur. • **Make this vsys a User-ID data hub (Faites de ce vsys un concentrateur de données USER-ID)** : autorisez tous les autres systèmes virtuels du pare-feu à accéder aux mappages partagés. Après avoir activé cette option, sélectionnez le **Mapping Type (type de mappage)** que vous souhaitez partager : Mappages adresse IP-nom d’utilisateur (**IP User Mapping (Mappage d’utilisateurs IP))**, mappages de groupes (**User Group Mapping (Mappage de groupe d’utilisateurs**), ou les deux. • **Changer**le hub: si vous souhaitez modifier quel vsys est le hub de données User-ID, sélectionnez un nouveau vsys pour réaffecter ce vsys en tant que hub de données User-ID. Pour arrêter d’utiliser le vsys comme concentrateur de données User-ID, sélectionnez **Aucun**.

Périphérique > Passerelles partagées

Les passerelles partagées permettent à plusieurs systèmes virtuels de partager une seule interface pour la communication externe (généralement connectée à un réseau en amont commun, tel qu'un Fournisseur de services Internet). Tous les systèmes virtuels communiquent avec le monde extérieur via l'interface physique à l'aide d'une adresse IP unique. Un routeur virtuel est utilisé pour acheminer le trafic de tous les systèmes virtuels via la passerelle partagée.

Les passerelles partagées utilisent des interfaces de Niveau 3 et au moins une interface de Niveau3 doit être configurée en tant que passerelle partagée. Les communications provenant d'un système virtuel et quittant le pare-feu via une passerelle partagée nécessitent des politiques similaires aux communications entre deux systèmes virtuels. Vous pouvez configurer une zone « vsys externe » pour définir les règles de sécurité du système virtuel.

Paramètres de passerelle partagée	Description
ID	Identifiant de la passerelle (non utilisé par le pare-feu).
Nom	Saisissez un nom pour la passerelle partagée (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement. Seul le nom est requis.
Proxy DNS	(Facultatif) Si un proxy DSN est configuré, sélectionnez le(s) serveur(s) DNS à utiliser pour les requêtes de nom de domaine.
Interfaces	Sélectionnez les interfaces que la passerelle partagée utilisera.

Périphérique > Gestion des certificats

- Périphérique > Gestion des certificats > Certificats
- Périphérique > Gestion des certificats > Profil de certificat
- Périphérique > Gestion des certificats > Répondeur OCSP
- Périphérique > Gestion des certificats > Profil de service SSL/TLS
- Périphérique > Gestion des certificats > SCEP
- Périphérique > Gestion des certificats > Exclusion du déchiffrement SSL
- Périphérique > Gestion des certificats > Profil de service SSL

Périphérique > Gestion des certificats > Certificats

Sélectionnez **Périphérique** > **Gestion des certificats** > **Certificats** > **Certificats de périphérique** pour gérer (générer, importer, renouveler, supprimer et révoquer) les certificats, qui sont utilisés pour sécuriser la communication à travers un réseau. Vous pouvez également exporter et importer la clé haute disponibilité (HD) utilisée pour sécuriser la connexion entre les homologues HD sur le réseau. Sélectionnez **Périphérique** > **Gestion des certificats** > **Certificats** > **Autorités de certification de confiance par défaut** pour afficher, activer et désactiver les autorités de certification (AC) approuvées par le pare-feu.

Pour plus d'informations sur la façon de mettre en œuvre des certificats sur le pare-feu et Panorama, reportez-vous à la section Gestion des certificats.

- Gestion des certificats du pare-feu et de Panorama
- Gestion des autorités de certification de confiance par défaut
- Périphérique > Gestion des certificats > Profil de certificat
- Périphérique > Gestion des certificats > Répondeur OCSP
- Périphérique > Gestion des certificats > Profil de service SSL/TLS
- Périphérique > Gestion des certificats > SCEP
- Périphérique > Clé principale et diagnostics

Gestion des certificats du pare-feu et de Panorama

- Périphérique > Gestion des certificats > Certificats > Certificats de périphérique
- Panorama > Gestion des certificats > Certificats

Sélectionnez **Device (Périphérique)** > **Certificate Management (Gestion des Certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats du périphérique)** ou **Panorama** > **Certificate Management (Gestion des Certificats)** > **Certificats** > **Device Certificates (Certificats du périphérique)** pour afficher les certificats que le pare-feu ou Panorama utilise pour certaines tâches telles que la sécurisation de l'accès à l'interface Web, le déchiffrement SSL ou le LSVPN.

Voici quelques utilisations possibles des certificats. Définissez l'utilisation du certificat après que vous l'avez généré (voir Gestion des autorités de certification de confiance par défaut).

- **Forward Trust (Approbation de transfert)** – Le pare-feu utilise ce certificat pour signer une copie du certificat du serveur que le pare-feu présente aux clients lors du Décryptage du proxy de transfert SSL lorsque l'autorité de certification (AC) qui a signé le certificat du serveur se trouve dans la liste des AC de confiance du pare-feu.
- **Forward Untrust (Non-approbation de transfert)** – Le pare-feu utilise ce certificat pour signer une copie du certificat du serveur que le pare-feu présente aux clients lors du Déchiffrement du proxy de transfert SSL lorsque l'autorité de certification (CA) qui a signé le certificat du serveur ne se trouve pas dans la liste des AC de confiance du pare-feu.
- **Trusted Root CA (CA racine approuvée)** – Le pare-feu utilise ce certificat en tant qu'AC de confiance pour le Déchiffrement du proxy de transfert SSL, GlobalProtect, le Contrôle prioritaire de l'URL par l'administrateur et le Portail d'authentification. Le pare-feu dispose d'une liste

importante de CA de confiance. Le certificat CA racine de confiance s'applique aux autres CA de confiance pour votre organisation, mais qui ne figurent pas dans la liste prédéfinie du CA de confiance.

- **SSL Exclude (Certificat d'exclusion SSL)** – Le pare-feu utilise ce certificat si vous définissez la configuration des exceptions au Déchiffrement afin d'exclure certains serveurs du Déchiffrement SSL/TLS.
- **Certificate for Secure Syslog (Certificat pour Secure Syslog)** – Le pare-feu utilise ce certificat pour sécuriser la transmission de journaux sous forme de messages Syslog vers un serveur Syslog.

Pour générer un certificat, cliquez sur Générer et renseignez les champs suivants :

Une fois qu'un certificat a été généré, la page affichera Autres actions prises en charge pour gérer les certificats.

Paramètres de génération d'un certificat	Description
Type de certificat	Sélectionnez l'entité qui génère le certificat. **Local** – Le pare-feu ou Panorama génère le certificat. **SCEP** – Un serveur SCEP (Simple Certificate Enrollment Protocol, Protocole d'inscription de certificats simple) génère le certificat et l'envoie au pare-feu ou à Panorama.
Nom du certificat	Required (Requis) Saisissez un nom (maximum de 63 caractères sur le pare-feu ou de 31 caractères sur Panorama) pour identifier le certificat. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Profil SCEP	(Certificats SCEP uniquement) Sélectionnez un **SCEP Profile (Profil SCEP)** pour définir comment le pare-feu ou Panorama communique avec un serveur SCEP et pour définir les paramètres du certificat SCEP. Pour plus de détails, voir Périphérique > Gestion des certificats > SCEP. Vous pouvez configurer un pare-feu servant de portail GlobalProtect pour solliciter des certificats SCEP sur demande et déployer automatiquement les certificats aux terminaux. Les autres champs de la boîte de dialogue Générer un certificat ne s'appliquent pas aux certificats SCEP. Après avoir spécifié le **Certificate Name (Nom du certificat)** et le **SCEP Profile (Profil SCEP)**, cliquez sur **Generate (Générer)**.
Common Name (nom commun - CN)	(Requis) Saisissez l'adresse IP ou le FQDN qui apparaîtra sur le certificat.

Paramètres de génération d’un certificat	Description
Partagé	Sur un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez **Shared (Partagé)** si vous souhaitez que le certificat s'applique à chaque système virtuel.
Signés par	Pour signer le certificat, vous pouvez utiliser un certificat d’autorité de certification (AC) que vous avez importé dans le pare-feu. Le certificat peut également être auto-signé, auquel cas le pare-feu constitue l’autorité de certification. Si vous utilisez Panorama, vous pouvez également générer un certificat auto-signé pour Panorama. Si vous avez importé des certificats d’autorité de certification ou que vous en avez émis sur le pare-feu (auto-signé), la liste déroulante inclut les autorités de certification disponibles pour signer le certificat que vous créez. Pour générer une demande de signature de certificat (CSR), sélectionnez **External Authority (CSR) (Autorité externe (demande de signature de certificat))**. Vous pouvez exporter la CSR et l’envoyer à l’AC pour signature après que le pare-feu a généré le certificat et la paire de clés.
Autorité de certification	Sélectionnez cette option si vous souhaitez que le pare-feu génère le certificat. Désignez ce certificat comme une CA afin de pouvoir l'utiliser pour signer d'autres certificats sur le pare-feu.
Blocage d’exportation de clé privée	Lorsque vous générez un certificat, sélectionnez cette option pour empêcher tous les administrateurs, y compris les super utilisateurs, d’exporter la clé privée.
Répondeur OCSP	Sélectionnez un profil de répondeur OCSP dans le menu déroulant (voir Périphérique > Gestion des certificats > Répondeur OCSP). Le nom d'hôte correspondant apparaît dans le certificat.
Algorithme	Sélectionnez un algorithme de génération de clé pour le certificat : **RSA** ou **Elliptic Curve DSA** (ECDSA). ECDSA utilise des clés de plus petite taille que l’algorithme RSA, et offre donc une meilleure performance de traitement des connexions SSL/TLS. ECDSA offre également une sécurité supérieure ou égale à celle de RSA. ECDSA est recommandé pour les navigateurs et systèmes d’exploitation clients qui le prennent en charge, mais vous devrez peut-être sélectionner RSA pour la compatibilité avec les navigateurs et systèmes d’exploitation existants.

Paramètres de génération d'un certificat	Description
	Les pare-feu exécutant PAN-OS 6.1 ou versions antérieures supprimeront tous les certificats ECDSA que vous appliquez à partir de Panorama et aucun certificat RSA signé par une autorité de certification de certificat ECDSA ne sera valide sur ces pare-feu. Vous ne pouvez pas utiliser un Module de sécurité matériel (HSM) pour stocker les clés ECDSA privées utilisées pour le décryptage du Proxy de transfert SSL ou l'Inspection SSL entrante.
Nombre de bits	Sélectionnez la longueur de la clé du certificat. Si le pare-feu est en mode FIPS-CC et que l'**Algorithm (Algorithme)** de génération de clé est **RSA**, les clés RSA générées doivent comporter **2 048** ou **3 027** bits. Si l'**Algorithm (Algorithme)** est **Elliptic Curve DSA**, les deux options de longueur de clé (**256** et **384**) s'appliquent.
Résumer	Sélectionnez l'algorithme **Digest (Résumer)** du certificat. Les options disponibles dépendent de l'**Algorithm (Algorithme)** de génération de clé : • **RSA** : **MD5**, **SHA1**, **SHA256**, **SHA384** ou **SHA512** • **Elliptic Curve DSA** : **SHA256** ou **SHA384** Si le pare-feu est en mode FIPS-CC et que l'**Algorithm (Algorithme)** de génération de clé est **RSA**, vous devez sélectionner **SHA256**, **SHA384** ou **SHA512** comme algorithme **Digest (Résumer)**. Si l'**Algorithm (Algorithme)** est **Elliptic Curve DSA**, les deux algorithmes **Digest (Résumer)** (**SHA256** et **SHA384**) s'appliquent. *Les certificats clients utilisés lors de la demande de services de pare-feu basés sur TLSv1.2 (comme l'accès administrateur à l'interface Web) ne peuvent avoir **SHA512 (sha512)** comme algorithme Résumer. Les certificats clients doivent utiliser un algorithme Résumer inférieur (tel que **SHA384**) ou vous devez limiter la **Max Version (Version max)** à **TLSv1.1** lorsque vous configurez les profils de service SSL/TLS pour les services de pare-feu (voir Périphérique > Gestion des certificats > Profil de service SSL/TLS).*
Expiration (jours)	Indiquez le nombre de jours de validité du certificat (la valeur par défaut est 365).

Paramètres de génération d’un certificat	Description
	*Si vous indiquez une **Validity Period (Période de validité)** dans une configuration satellite GlobalProtect, cette valeur appliquera un contrôle prioritaire sur la valeur saisie dans ce champ.*
Attributs du certificat	Cliquez sur **Add (Ajouter)** pour ajouter des **Certificate Attributes (Attributs de certificat)** supplémentaires permettant d'identifier l'entité pour laquelle vous émettez le certificat. Vous pouvez ajouter les attributs suivants'A0;: **Country (Pays)**, **State (État)**, **Locality (Région)**, **Organization (Organisation)**, **Department (Service)** et **Email (Adresse e-mail)**. De plus, vous pouvez définir l'un des champs Autre nom de l'objet suivants'A0;: **Host Name (Nom d'hôte)** (SubjectAltName:DNS), **IP (Adresse IP)** (SubjectAltName:IP) et **Alt Email (Autre adresse e-mail)** (SubjectAltName:email). *Pour ajouter un pays comme attribut de certificat, sélectionnez**Country (Pays)** dans la colonne **Type**, puis cliquez sur **Value (Valeur)** pour voir les indicatifs de pays ISO 6366.*

Si vous avez configuré un module de sécurité matériel (HSM), les clés privées sont stockées sur le stockage de module de sécurité matériel externe, et non sur le pare-feu.

Autres actions prises en charge pour gérer les certificats

Après avoir généré le certificat, ses détails s’affichent sur la page et les actions suivantes sont disponibles :

Autres actions prises en charge pour gérer les certificats	Description
Supprimer	Sélectionnez le certificat et **Supprimez**-le. *Si le pare-feu possède une politique de déchiffrement, vous ne pouvez pas supprimer un certificat pour lequel l’utilisation est réglée comme **Certificat d’approbation de transfert** or **Certificat de non-approbation de transfert**. Pour modifier l’utilisation du certificat, voir* Gestion des autorités de certification de confiance par défaut.
Révoquer	Sélectionnez le certificat que vous souhaitez révoquer et cliquez sur **Revoke (Révoquer)**. Le certificat passe immédiatement à l'état révoqué. Aucune validation n'est requise.

Autres actions prises en charge pour gérer les certificats	Description
Renouveler	Lorsqu'un certificat expire ou est sur le point d'expirer, sélectionnez le certificat correspondant et cliquez sur **Renew (Renouveler)**. Définissez la période de validité (en jours) du certificat et cliquez sur **OK**. Si le pare-feu est la CA ayant généré le certificat, le pare-feu le remplacera par un nouveau certificat doté d'un numéro de série différent mais des mêmes attributs que l'ancien. Si une autorité de certification externe (AC) a signé le certificat et que le pare-feu utilise la méthode OCSP (Online Certificate Status Protocol) pour vérifier le statut de révocation du certificat, le pare-feu utilise les informations du répondeur OCSP pour mettre à jour le statut du certificat.
Importer	Cliquez pour **Importer** un certificat et configurez-le comme suit : • Saisissez un nom de certificat pour identifier le certificat. • Recherchez le fichier de certificat. Si vous importez un certificat **PKCS12** et une clé privée, un seul fichier contient ces deux éléments. Si vous importez un certificat **PEM**, le fichier ne contient que le certificat. • Sélectionnez le **File Format (Format de fichier)** du certificat. • Sélectionnez **Private key resides on Hardware Security Module (La clé privée se trouve sur le module de sécurité matériel)** si un module de sécurité matériel stocke la clé privée de ce certificat. Pour plus de détails sur les modules de sécurité matériels, voir Périphérique > Configuration > Module de sécurité matériel (HSM). • **Import Private Key (Importer une clé privée)** comme requise (format PEM uniquement). Si vous avez sélectionné **PKCS12** comme **Format de fichier** du certificat, le **Fichier du certificat** sélectionné comprend la clé. Si vous avez sélectionné le format **PEM**, recherchez le fichier de clé privée chiffré (généralement *.key). Pour les deux formats, saisissez la **Phrase secrète** et **Confirmez la phrase secrète**. Lorsque vous importez un certificat et sélectionnez **Import Private Key (Importer la clé privée)**, sélectionnez**Block Private Key Export (Bloquer l'exportation de clé privée)** pour empêcher les administrateurs, y compris les super utilisateurs, d'exporter la clé privée. *Lorsque vous importez un certificat sur un pare-feu de Palo Alto Networks ou un serveur Panorama qui est en mode FIPS-CC, vous devez importer le certificat en tant que Certificat codé en base-64 (PEM) et vous devez crypter la clé privée avec AES. En outre, vous devez utiliser SHA1 comme méthode de dérivation de clé basée sur la phrase secrète.*

Autres actions prises en charge pour gérer les certificats	Description
	Pour importer un certificat PKCS12, convertissez le certificat au format PEM (en utilisant un outil tel que OpenSSL) ; assurez-vous que la phrase secrète que vous utilisez pendant la conversion comporte au moins de six caractères.
Export (Exporter)	Sélectionnez le certificat que vous souhaitez exporter, cliquez sur **Exporter**, puis sélectionnez un **Format de fichier** : • Clé privée et certificat chiffrés (PKCS12) - Le fichier exporté contiendra à la fois le certificat et la clé privée. • Certificat codé en base-64 (PEM) - Si vous souhaitez exporter également la clé privée, sélectionnez Exporter la clé privée, saisissez une Phrase secrète puis Confirmez la phrase secrète. • Certificat codé binaire (DER) - Vous pouvez exporter uniquement le certificat, et non la clé : ignorez les champs Exporter la clé privée et Phrase secrète.
Importer la clé HA Exporter la clé HA	Les clés HA doivent être échangées entre les homologues de pare-feu; la clé du pare-feu'A0;1 doit être exportée, puis importée sur le pare-feu et vice-versa. Pour importer des clés pour la haute disponibilité (HA), cliquez sur **Import HA Key (Importer la clé HA)** et cliquez sur **Browse (Parcourir)** pour rechercher le fichier de clé à importer. Pour exporter des clés pour HA, cliquez sur **Export HA Key (Exporter la clé HA)** et indiquez l'emplacement où enregistrer le fichier.
Définissez l'utilisation du certificat.	Dans la colonne Nom, cliquez sur le certificat, puis sélectionnez les options appropriées selon l'utilisation prévue du certificat.
PDF/CSV	Les rôles administrateur qui sont au moins dotés de l’accès en lecture seule peuvent exporter le tableau de configuration des certificats gérés au format **PDF/CSV**. Vous pouvez appliquer des filtres pour créer des sorties du tableau de configuration plus précises, par exemple, pour effectuer des audits. Seules les colonnes qui sont visibles dans l’interface Web seront exportées. Reportez-vous à la section Exportation du tableau de configuration.

Gestion des autorités de certification de confiance par défaut

- Périphérique > Gestion des certificats > Certificats > Autorités de certification de confiance par défaut

Cette page vous permet d'afficher, de désactiver ou d'exporter les autorités de certification (AC) pré-incluses approuvées par le pare-feu. La liste prédéfinie des AC comprend les fournisseurs de certificats de confiance et les plus courants qui sont responsables de la génération des certificats dont le pare-feu a

besoin pour sécuriser les connexions à l’Internet. Pour chaque AC racine de confiance, le nom, l'objet, l'émetteur, la date d'expiration et l'état de validité s'affichent.

Par défaut, le pare-feu n’approuve pas les AC intermédiaires, puisque ceux-ci ne font pas partie de la chaîne de confiance entre le pare-feu et le CA racine de confiance. Vous devez ajouter manuellement les AC intermédiaires que vous voulez que le pare-feu approuve de même que les autres AC d’entreprises de confiance dont votre organisation a besoin (**Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **Certificates (Certificats)** > **Device Certificates (Certificats de périphérique)**).

Paramètres des autorités de certification de confiance	Description
Activer	Si vous avez désactivé une autorité de certification, vous pouvez la **Enable (Réactiver)**.
Désactivation	Sélectionnez l’autorité de certification et **Disable (Désactivez)**-la. Vous pouvez utiliser cette option si vous souhaitez seulement faire confiance à certains AC ou si vous souhaitez tous les désactiver et faire confiance uniquement à votre AC locale.
Export (Exporter)	Sélectionnez le certificat AC et cliquez sur **Export (Exporter)** pour l'exporter. Cette action vous permet de l’importer dans un autre système ou de consulter le certificat hors ligne.

Périphérique > Gestion des certificats > Profil de certificat

- **Périphérique** > **Gestion des certificats** > **Profil du certificat**
- **Panorama** > **Gestion des certificats** > **Profil du certificat**

Les profils de certificat indiquent les certificats de l'autorité de certification (AC) qui doivent être utilisés pour vérifier les certificats clients, comment vérifier l'état de révocation des certificats et de quelle façon cet état permet de restreindre l'accès. Vous sélectionnez les profils quand vous configurez l'authentification du certificat pour Portail d'authentification, GlobalProtect, VPN de site à site IPsec, Dynamic DNS (DNS dynamique ; DDNS) et accès de l'interface Web aux pare-feu et à Panorama. Vous pouvez configurer un profil de certificat distinct pour chacun de ces services.

Paramètres d'un profil de certificat	Description
Nom	(Nécessaire) Saisissez un nom pour identifier le profil (maximum de 63 caractères sur le pare-feu ou de 31 caractères sur Panorama). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Emplacement	Sélectionnez la portée dans laquelle le profil est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Partagé** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner l' **Emplacement)** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le profil, vous ne pouvez plus changer son **Emplacement**.
Champ du nom d'utilisateur	Si GlobalProtect utilise les certificats uniquement pour l'authentification auprès du portail et de la passerelle, le logiciel PAN-OS utilise le champ de certificat sélectionné dans la liste déroulante **Champ Nom d'utilisateur** comme nom d'utilisateur et le fait correspondre à l'adresse IP pour le service User-ID : • **Sujet** : le nom commun. • **Autre objet** : le Nom principal ou le nom de messagerie. • **Aucun** : Généralement utilisée pour l'authentification avant ouverture de session ou de périphériques GlobalProtect.
Domaine	Saisissez le domaine NetBIOS de manière à ce que le logiciel PAN-OS puisse mapper les utilisateurs via la fonctionnalité User-ID.
Certificats de l'autorité de certification	(Nécessaire) **Ajoutez** un **CA Certificat** à affecter au profil. Éventuellement, si le pare-feu utilise la méthode OCSP (Online Certificate Status Protocol) pour vérifier le statut de révocation du certificat, vous pouvez configurer les champs suivants pour appliquer

Paramètres d’un profil de certificat	Description
	un contrôle prioritaire sur le comportement par défaut. Pour la plupart des déploiements, ces champs ne s'appliquent pas. • Par défaut, le pare-feu utilise les informations du (accès aux informations de l'autorité ; AIA) du certificat pour extraire les informations sur le répondeur OCSP. Pour appliquer un contrôle prioritaire sur les informations d’AIA, saisissez une **Default OCSP URL (URL OCSP par défaut)** (commençant par **`http://`** ou par **`https://`**). • Par défaut, le pare-feu utilise le certificat sélectionné dans le champ **CA Certificate (Certificat AC)** pour valider les réponses OCSP. Pour utiliser un certificat différent pour la validation, sélectionnez-le dans le champ **CA Certificat pour la vérification OCSP)**. De plus, saisissez un **Nom de modèle** pour identifier le modèle qui a été utilisé pour signer le certificat.
Utiliser CRL	Sélectionnez cette option pour utiliser une liste de révocation de certificat (CRL) afin de vérifier l'état de révocation des certificats.
Utiliser OCSP	Sélectionnez cette option pour utiliser OCSP afin de vérifier l'état de révocation des certificats. *si vous sélectionnez OCSP et CRL, le pare-feu essaie d'abord le protocole OCSP et ne fait appel à la méthode'A0;CRL en secours que si le répondeur OCSP est indisponible.*
Délai d'expiration de la réception CRL	Indiquez l’intervalle (de 1 à 60 secondes) après lequel le pare-feu n’attend plus la réponse du service CRL.
Délai d'attente en réception OCSP	Indiquez l’intervalle (de 1 à 60 secondes) après lequel le pare-feu n’attend plus la réponse du répondeur OCSP.
Délai d'expiration du statut du certificat	Indiquez l’intervalle (de 1 à 60 secondes) après lequel le pare-feu n’attend plus la réponse d’aucun service d’état du certificat et applique la logique de blocage de la session que vous avez définie.
Bloquer une session si le statut du certificat est inconnu	Sélectionnez cette option si vous souhaitez que le pare-feu bloque les sessions lorsque le service OCSP ou CRL renvoie un état de révocation de certificat *inconnu*. Sinon, le pare-feu poursuit les sessions.

Paramètres d’un profil de certificat	Description
Bloquer une session si le statut du certificat ne peut pas être récupéré avant le délai d'expiration	Sélectionnez cette option si vous souhaitez que le pare-feu bloque les sessions une fois qu'il a enregistré un délai d'expiration de la demande OCSP ou CRL. Sinon, le pare-feu poursuit les sessions.
Bloquer les sessions si le certificat n'a pas été généré pour le périphérique s'authentifiant	(GlobalProtect uniquement) Sélectionnez cette option si vous souhaitez que le pare-feu bloque les sessions lorsque l'attribut numéro de série qui figure dans le champ sujet du certificat client ne correspond pas à l'ID de l'hôte que l'application GlobalProtect signale pour le point de terminaison. Sinon, le pare-feu autorise la session. Cette option ne s’applique qu’à l’authentification du certificat GlobalProtect.

Périphérique > Gestion des certificats > Répondeur OCSP

Sélectionnez **Périphérique** > **Gestion des certificats** > **Répondeur OCSP** pour définir un répondeur (serveur) OCSP (Online Certificate Status Protocol) pour vérifier l'état de révocation des certificats.

Outre l'ajout d'un répondeur OCSP, pour activer OCSP, vous devez effectuer les tâches suivantes :

- Activez la communication entre le pare-feu et le serveur OCSP : sélectionnez **Périphérique** > **Configuration** > **Gestion**, puis sélectionnez **HTTP OCSP** Paramètres de l'interface de gestion, et cliquez sur **OK**.
- Si le pare-feu déchiffre le trafic SSL/TLS sortant, vous pouvez le configurer pour vérifier l'état de révocation des certificats du serveur de destination : sélectionnez **Périphérique** > **Configuration** > **Sessions**, puis cliquez sur **Paramètres de révocation du certificat de décryptage**, sélectionnez **Activer** dans les paramètres OCSP, ensuite saisissez le **Délai de réception** (l'intervalle après lequel le pare-feu n'attend plus de réponse OCSP), puis cliquez sur **OK**.
- Pour configurer le pare-feu lui-même comme un répondeur OCSP, vous pouvez éventuellement ajouter un profil de gestion d'interface à l'interface utilisée pour les services OCSP. D'abord, sélectionnez **Réseau** > **Profils de réseau** > **Gestion de l'interface**, cliquez sur **Ajouter**, sélectionnez **HTTP OCSP**, puis cliquez sur **OK**. Ensuite, sélectionnez **Réseau** > **Interfaces**, cliquez sur le nom de l'interface que le pare-feu utilisera pour les services OCSP, sélectionnez **Avancé** > **Autres informations**, choisissez le profil de Gestion d'interface configuré, enfin cliquez sur **OK** et sur **Valider**.

Activez un répondeur OCSP de sorte que vous soyez avisé de la révocation éventuelle d'un certificat afin de pouvoir prendre les mesures appropriées pour établir une connexion sécurisée au portail et aux passerelles.

Paramètres du répondeur OCSP	Description
Nom	Saisissez un nom pour identifier le répondeur (31 caractères maximum). Ce nom est sensible aux majuscules et minuscules Il doit être unique et utiliser uniquement des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement.
Emplacement	Sélectionnez la portée dans laquelle le répondeur est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Partagé** (tous les systèmes virtuels). Dans les autres contextes, vous ne pouvez pas sélectionner le **Emplacement** ; sa valeur est prédéfinie sur Partagé. Après avoir enregistré le répondeur, vous ne pouvez plus changer son **Emplacement**.
Nom de l'hôte	Saisissez le nom d'hôte (recommandé) ou l'adresse IP du répondeur OCSP. À partir de cette valeur, PAN-OS déduit automatiquement une URL et l'ajoute au certificat en cours de vérification. Si vous configurez le pare-feu comme un répondeur OCSP, le nom d'hôte doit se résoudre en une adresse IP dans l'interface que le pare-feu utilise pour les services OCSP.

Périphérique > Gestion des certificats > Profil de service SSL/TLS

- Périphérique > Gestion des certificats > Profil de service SSL/TLS
- Panorama > Gestion des certificats > Profil de service SSL/TLS

Les profils de service SSL/TLS définissent un certificat du serveur et une version de protocole ou une plage e versions pour les services de pare-feu ou Panorama utilisant SSL/TLS (comme l'accès administrateur à l'interface Web). En définissant les versions de protocole, les profils vous permettent de limiter les suites de chiffrements disponibles pour sécuriser les communications avec les systèmes client demandant les services.

En ce qui concerne les systèmes clients qui requièrent un pare-feu ou les services Panorama, la liste d'approbation de certificats (CTL) doit inclure le certificat de l'autorité de certification (CA) qui a délivré le certificat spécifié dans le profil de service SSL/TLS. Dans le cas contraire, les utilisateurs constateront une erreur de certificat lorsqu'ils solliciteront les services. La plupart des certificats d'une tierce CA sont présents par défaut sur les navigateurs des clients. Si une entreprise ou une CA de certificat généré par un pare-feu est l'émetteur, vous devez déployer ce certificat CA à la liste CTL dans les navigateurs des clients.

Pour ajouter un profil, cliquez sur **Ajouter** et renseignez les champs dans le tableau suivant.

Paramètres de profil de service SSL/TLS	Description
Nom	Saisissez un nom pour identifier le profil (31 caractères maximum). Ce nom est sensible aux majuscules et minuscules. Il doit être unique et utiliser uniquement des lettres, des nombres, des espaces, des traits d'union et des traits de soulignement.
Partagé	Si le pare-feu comporte plusieurs systèmes virtuels (vsys), sélectionner cette option rend le profil disponible sur tous les systèmes virtuels. Cette option est sélectionnée par défaut et le profil s'applique uniquement au système virtuel sélectionné dans l'onglet **Périphérique**, dans la liste déroulante **Emplacement**.
certificat	Sélectionner, importer ou générer un certificat de serveur à associer au profil (voir Gérer les certificats du pare-feu et de Panorama). *n'utilisez pas de certificats d'autorité de certification (AC) pour les services ; utilisez des certificats signés uniquement.*

Paramètres de profil de service SSL/TLS	Description
Version min Version max	Sélectionnez la première (**Version min**) et la dernière (**Version max**) version de TLS que les services peuvent utiliser : **TLSv1.0**, **TLSv1.1**, **TLSv1.2**, **TLSv1.3**, ou **Max** (la dernière version disponible). ***TLSv1.1 (TLSv1.1)*** *est la version de TLS la plus ancienne qui est prise en charge sur les pare-feu en mode FIPS-CC sur lesquels PAN-OS 8.0 ou une version ultérieure de PAN-OS est installé ; ne sélectionnez pas* ***TLSv1.0 (TLSv1.0)****.* *Les certificats clients qui sont utilisés lors de la demande de services de pare-feu reposant sur* ***TLSv1.2*** *ne peuvent pas avoir SHA512 en tant qu'algorithme de chiffrement. Les certificats clients doivent utiliser un algorithme de chiffrement inférieur (tel que SHA384) ou vous devez limiter la* ***Version max*** *à* ***TLSv1.1*** *pour les services.* *Utilisez la version la plus forte possible du protocole de sorte à fournir la sécurité la plus forte au réseau. Si vous le pouvez, définissez la* ***Min Version (Version min)*** *sur* ***TLSv1.2*** *ert la* ***Max Version (Version max)*** *sur* ***Max****.*

Périphérique > Gestion des certificats > SCEP

Le protocole de recrutement de certificat simple (SCEP) fournit un mécanisme pour générer un certificat unique aux terminaux, aux passerelles et aux périphériques satellites. Sélectionnez **Périphérique** > **Gestion des certificats** > **SCEP** pour créer une configuration SCEP.

Pour plus d'informations sur la création d'un profil SCEP, reportez-vous à la section Déploiement de certificats au moyen de SCEP

.

Pour démarrer une nouvelle configuration SCEP, cliquez sur **Ajouter** et renseignez les champs suivants.

Paramètres SCEP	Description
Nom	Indiquez un Nom descriptif pour identifier cette configuration SCEP, comme SCEP_*Exemple*. Ce nom distingue un profil SCEP des autres instances que vous pourriez trouver parmi les profils de configuration.
Emplacement	Si le système dispose de plusieurs systèmes virtuels, sélectionnez l'Emplacement du profil. L'emplacement précise où la configuration SCEP est disponible.
Mot de passe à usage unique (demande d'authentification)	
Demande d'authentification SCEP	(Facultatif) Pour rendre la génération de certificats basée sur SCEP plus sécurisée, vous pouvez configurer un mécanisme de réponse au défi SCEP (un mot de passe à usage unique [OTP]) entre l'infrastructure à clé publique (PKI) et le portail pour chaque demande de certificat. *Après avoir configuré ce mécanisme, son fonctionnement est invisible et aucune autre intervention de votre part n'est nécessaire.* Le mécanisme de contestation que vous sélectionnez détermine la source de l'OTP. Si vous sélectionnez **Fixé**, copiez le mot de passe d'authentification à partir du serveur SCEP pour le PKI et saisissez la chaîne dans la boîte de dialogue **Mot de passe** qui s'affiche sur le portail lorsqu'il est configuré comme **Fixé**. Chaque fois que le portail demande un certificat, il utilise ce mot de passe pour s'authentifier avec le PKI. Si vous sélectionnez **Dynamique**, vous saisissez le nom d'utilisateur et le mot de passe de votre choix (ceux-ci peuvent être les informations d'identification de l'administrateur PKI) et **URL du serveur** SCEP où le client portail saisit ces informations d'identification. Ce nom d'utilisateur et ce mot de passe demeurent les mêmes lorsque le serveur SCEP génère de manière transparente un mot de passe OTP pour le portail lors de chaque demande de certificat. (Lors de chaque demande de certificat, vous pouvez afficher ce changement d'OTP après un rafraîchissement de l'écran dans le champ « Le mot de passe d'authentification est ».) L'ICP transmet au portail

Paramètres SCEP	Description
	de manière transparente chaque nouveau mot de passe. Le portail utilise ensuite le mot de passe pour sa demande de certificat. *Pour vous conformer à la norme américaine du traitement de l'information (FIPS), sélectionnez **Dynamique**, indiquez ensuite une **URL du serveur** qui utilise le protocole HTTPS, puis activez **SCEP Server SSL Authentication (Authentification SSL du serveur SCEP)**. (L'opération FIPS-CC est indiquée sur la page de connexion du pare-feu et dans la barre d'état du pare-feu.)*
Configuration	
URL du serveur	Saisissez l'URL à laquelle le portail demande et qui reçoit des certificats clients de la part du serveur SCEP. Exemple : `http:// <hostname or IP>/certsrv/mscep/.`
Nom CA-IDENT	Saisissez une chaîne pour identifier le serveur SCEP. Longueur maximale de 255 caractères.
Objet	Configurez le sujet pour inclure des informations d'identification sur le périphérique et, éventuellement, sur l'utilisateur et pour inclure ces informations dans la demande de signature de certificat (CSR) sur le serveur SCEP. Lorsqu'il est utilisé pour demander des certificats clients pour les terminaux, le terminal envoie des informations d'identification relatives au périphérique qui incluent sa valeur d'ID d'hôte. La valeur d'ID d'hôte varie selon le type de périphérique, soit GUID (Windows), adresse MAC de l'interface (Mac), Android ID (appareils Android), UDID (périphériques iOS), ou un nom unique qui GlobalProtect assigne (Chrome). Lorsqu'il est utilisé pour demander des certificats pour les périphériques satellites, la valeur d'ID de l'hôte est le numéro de série du périphérique. Pour indiquer des informations supplémentaires dans la CSR, saisissez le nom du Sujet. Le sujet doit être un nom différent au format *<attribute>=<value>* et doit inclure la clé du nom commun (CN). Par exemple : `O=acme,CN=acmescep` Il existe deux façons d'indiquer le CN : • (Recommandé) **CN par jeton d'authentification –** Saisissez l'un des jetons supportés **`$USERNAME`**, **`$EMAILADDRESS`**, ou **`$HOSTID`**. Utilisez la variable nom d'utilisateur ou adresse de messagerie pour vous assurer que le portail demande des certificats pour un utilisateur

Paramètres SCEP	Description

	spécifique. Pour demander des certificats pour le périphérique uniquement, indiquez la variable ID d'hôte. Lorsque le portail GlobalProtect insère les paramètres SCEP dans l'agent, la portion NC du nom du sujet est remplacée par la valeur réelle (nom d'utilisateur, ID d'hôte ou adresse e-mail) du propriétaire du certificat. Par exemple :
	
	`O=acme,CN=$HOSTID`
	
	• **CN statique** : Le CN que vous indiquez sera utilisé comme sujet pour tous les certificats générés par le serveur SCEP. Par exemple :
	
	`O=acme,CN=acmescep`

Autre type de nom de l'objet	Après avoir sélectionné un type autre qu'**Aucun**, une boîte de dialogue s'affiche pour que vous y saisissiez la valeur appropriée : • **RFC 822 Name (Nom RFC 822)** : saisissez le nom de la messagerie dans l'objet du certificat ou l'extension alternative du nom de l'objet. • **DNS Name (Nom DNS)** : saisissez le nom DNS utilisé pour évaluer les certificats. • **Uniform Resource Identifier (URI) (Identifiant URI)** – Saisissez le nom de la ressource URI à partir de laquelle le client obtient le certificat.
Paramètres cryptographiques	• **Nombre de bits** – Sélectionnez le **Nombre de bits** de la clé pour le certificat. Si le pare-feu est en mode FIPS-CC, les clés générées doivent être d'au moins 2 048 bits. (L'opération FIPS-CC est indiquée sur la page de connexion du pare-feu et dans la barre d'état du pare-feu.) • **Résumer** - Sélectionnez l'algorithme **Résumer** du certificat : **SHA1**, **SHA256**, **SHA384** ou **SHA512**. Si le pare-feu est en mode FIPS-CC, vous devez sélectionner **SHA256**, **SHA384** ou **SHA512** comme algorithme **Résumer**.
Utiliser en tant que signature numérique	Sélectionnez cette option pour configurer le terminal afin d'utiliser la clé privée dans le certificat dans le but de valider une signature numérique.
Utiliser pour le chiffrement de la clé	Sélectionnez cette option pour configurer le terminal client afin d'utiliser la clé privée dans le certificat dans le but de crypter les données échangées par le biais de la connexion HTTPS établie avec les certificats générés par le serveur SCEP.
Empreinte du certificat de l'autorité de certification	(Facultatif) Pour garantir que le portail se connecte au bon serveur SCEP, saisissez la **Empreinte du certificat de l'autorité de certification)**. Vous pouvez obtenir cette empreinte auprès de l'interface du serveur SCEP dans le champ **Empreinte numérique**.

Paramètres SCEP	Description
	Connectez-vous à l’interface utilisateur administrative du serveur SCEP (par exemple, à l’adresse http://<hostname or IP>/CertSrv/mscep_admin/). Copiez l’empreinte numérique et saisissez-la dans **Empreinte du certificat de l’autorité de certification**.
Authentification SSL du serveur SCEP	Pour activer le protocole SSL, sélectionnez la racine **Certificat CA** pour le serveur SCEP. Vous pouvez activer l'authentification SSL mutuelle entre le serveur SCEP et le portail GlobalProtect en sélectionnant **Certificat client**.

Périphérique > Gestion des certificats > Exclusion du déchiffrement SSL

Visualiser et gérer les exclusions de déchiffrement SSL. Il existe deux types d'exclusions de déchiffrement, les exclusions prédéfinies et les exclusions personnalisées :

- Les exclusions de décodage prédéfinies permettent aux applications et aux services qui peuvent être interrompus de rester chiffré lorsque le pare-feu les déchiffre. Palo Alto Networks définit les exclusions de déchiffrement prédéfinies et fournit des mises à jour et des ajouts à la liste des exclusions prédéfinies à intervalles réguliers dans le cadre de la mise à jour des contenus des applications et des menaces. Les exclusions prédéfinies sont activées par défaut, mais vous pouvez choisir de désactiver l'exclusion si nécessaire.
- Vous pouvez créer des exclusions de déchiffrement personnalisées pour exclure le trafic du serveur du déchiffrement. Tout le trafic provenant ou destiné au serveur ciblé reste chiffré.

Vous pouvez également exclure le trafic du déchiffrement en fonction de l'application, de la source, de la destination, de la catégorie d'URL et du service.

Utilisez les paramètres de cette page pour Modifier ou ajouter une exclusion de déchiffrement et pour Gérer les exclusions de déchiffrement.

Paramètres des exclusions de déchiffrement SSL	Description
Modifier ou **Ajouter** une exclusion de déchiffrement	
Nom d'hôte	Saisissez un **Nom d'hôte** pour définir une exclusion de déchiffrement personnalisée. Le pare-feu compare le nom d'hôte à la SNI demandée par le client ou le CN présenté dans le certificat du serveur. Le pare-feu exclut du déchiffrement les sessions où le serveur présente un CN qui contient le domaine défini. Vous pouvez utiliser des astérisques (*) en tant que caractères génériques pour créer des exclusions de déchiffrement pour plusieurs noms d'hôte associés à un domaine. Les astérisques se comportent de la même façon que les carets (^) se comportent avec les exceptions de catégories URL : chaque astérisque indique un sous-domaine variable (étiquette) dans le nom d'hôte. Ceci vous permet de créer des exclusions aussi bien très spécifiques que très générales. Par exemple : • mail.*.com correspond à mail.company.com, mais ne correspond pas à mail.company.sso.com. • *.company.com correspond à tools.company.com, mais ne correspond pas à eng.tools.company.com. • *.*.company.com correspond à eng.tools.company.com, mais ne correspond pas à eng.company.com.

Paramètres des exclusions de déchiffrement SSL	Description
	• *.*.*.company.com correspond à corp.exec.mail.company.com, mais ne correspond pas à corp.mail.company.com. • mail.google.* correspond à mail.google.com, mais ne correspond pas à mail.google.uk.com. • mail.google.*.* correspond à mail.google.co.uk, mais ne correspond pas à mail.google.com. Par exemple, pour utiliser des caractères génériques pour exclure video-stats.video.google.com du décryptage, mais sans exclure video.google.com du décryptage, excluez *.*.google.com *Peu importe le nombre d'astérisques qui précèdent le nom d'hôte (sans une étiquette de caractère non générique qui précède le nom d'hôte), le nom d'hôte correspond à l'entrée. Par exemple, *.google.com, *.*.google.com et *.*.*.google.com correspondent tous à google.com. Cependant, *.dev.*.google.com ne correspond par à google.com, car une étiquette (dev) n'est pas un caractère générique.* Les noms d'hôtes doivent être uniques pour chaque saisie. Si une saisie prédéfinie fournie au pare-feu correspond à une saisie personnalisée existante, la saisie personnalisée est prioritaire. Vous ne pouvez pas modifier le Nom d'hôte pour une exclusion de déchiffrement prédéfinie.
Partagé	Sélectionnez **Partager** pour partager une exclusion de déchiffrement sur tous les systèmes virtuels dans un pare-feu à plusieurs systèmes virtuels. Alors que les exclusions de déchiffrement prédéfinies sont partagées par défaut, vous pouvez activer et désactiver les saisies prédéfinies et personnalisées pour un système virtuel spécifique.
Description	(Optionnel) Décrivez l'application que vous excluez du déchiffrement, y compris la raison pour laquelle l'application s'interrompt lors du déchiffrement.
Exclure	Exclure l'application du déchiffrement. Désactivez cette option pour commencer à déchiffrer une application précédemment exclue du déchiffrement.
Gestion des exclusions de déchiffrement	
Activer	Cliquez sur **Activer** une ou plusieurs saisies pour les exclure du déchiffrement.

Paramètres des exclusions de déchiffrement SSL	Description
Désactivation	Cliquez sur **Désactiver** une ou plusieurs exclusions de déchiffrement prédéfinies. Étant donné que les exclusions de déchiffrement identifient les applications qui s'interrompent lors du déchiffrement, la désactivation de l'une de ces saisies entraînera la non-prise en charge de l'application. Le pare-feu tentera de déchiffrer l'application et l'application s'interrompra. Vous pouvez utiliser cette option si vous souhaitez vous assurer que certaines applications chiffrées ne pénètrent pas sur votre réseau.
Afficher les données obsolètes	Cliquez sur **Afficher les données obsolètes** pour afficher les entrées prédéfinies que Palo Alto Networks ne définit plus comme des exclusions de déchiffrement. **En savoir plus sur les saisies obsolètes :** Les mises à jour des exclusions de décodage prédéfinies (y compris la suppression d'une saisie prédéfinie) sont envoyées au pare-feu dans le cadre des mises à jour du contenu des Applications et des Menaces. Les saisies prédéfinies et disposant de l'option **Exclure du déchiffrement** activée sont automatiquement supprimées de la liste des exclusions de déchiffrement SSL lorsque le pare-feu reçoit une mise à jour de contenu qui ne comporte plus cette saisie. Toutefois, les saisies prédéfinies avec l'option **Exclure du déchiffrement** désactivée restent dans la liste de déchiffrement SSL même si le pare-feu reçoit une mise à jour de contenu qui ne comporte plus cette saisie. Lorsque vous cliquez sur **Afficher les données obsolètes**, vous verrez que ces saisies prédéfinies désactivées ne sont pas appliquées à l'heure actuelle. Vous pouvez supprimer manuellement ces saisies si nécessaire.
Afficher le cache d'exclusion locale	**Afficher le cache d'exclusion locale** affiche les sites que le pare-feu a automatiquement exclus du décryptage du fait de circonstances techniques empêchant le décryptage comme des certificat, une authentification client coincés ou des cryptogrammes non compatibles. Le cache de décryptage SSL est différent de la liste d'exclusion de décryptage (**Périphérique** > **Gestion du certificat** > **Exclusion de décryptage SSL**), qui contient les sites qui empêche le décryptage que Palo Alto Networks a identifiés et auxquels vous pouvez ajouter les exclusions de décryptage permanentes que vous souhaitez faire. Le pare-feu remplit le Cache de décryptage SSL avec les exceptions de décryptage trouvées en local, sur la base des paramètres du profil de description associé à la règle de politique de décryptage qui contrôle le trafic. Les sites exclus demeurent 12 heures dans le cache et finissent par expirer. Chaque saisie d'exclusion comprend des informations sur l'application, le serveur, la raison pour laquelle le pare-feu a automatiquement exclu le site du décryptage, le profil de décryptage appliqué au trafic et le Vsys.

Périphérique > Gestion des certificats > Profil de service SSL

Les profils de service SSH vous permettent de limiter les algorithmes de cryptogramme, échange de clé t code d'authentification du message qui cryptent et protègent l'intégrité de vos données. Spécifiquement, ces profils renforcent la protection des données pendant les sessions SSH entre l'interface de votre ligne de commande (CLI) et les connexions de gestion et les appareils haute disponibilité (HA) de votre réseau. Vous pouvez aussi générer une nouvelle clé d'hôte SSH et indiquer les seuils (volume de données, intervalle de temps et compte de paquets) qui lance une nouvelle clé SSH.

Pour configurer un profil de service SSH, **Ajoutez** un profil de serveur, HA ou de gestion, remplissez les champs dans le tableau comme il convient, puis cliquez sur **OK** et **validez** vos modifications.

La procédure d'application d'un profil diffère selon le type de profil.

- Pour appliquer un profil HA, sélectionnez Périphérique > Haute disponibilité > Généralités. Paramètres du profil HA SSH, sélectionnez un profil existant. Cliquez sur **OK (OK)** et sur **Commit (Valider)** pour enregistrer vos modifications.
- Pour appliquer un profil Management - Server, sélectionnez Périphérique > Configuration > Gestion. Sous SSH Management Profiles Settings (Paramètres des profils de gestion SSH), sélectionnez un profil existant. Cliquez sur **OK** et sur **Valider** pour enregistrer vos modifications.

Après avoir appliqué un profil, vous devez effectuer un redémarrage de service SSH depuis le CLI pour activer le profil.

Paramètres de profil de service SSL.	Description
Nom	Donnez un nom au profil HIP (jusqu'à 31 caractères maximum). Le nom est sensible aux majuscules et minuscules, doit être unique et peut inclure uniquement des lettres, chiffres, espaces, traits d'union et traits de soulignement.
Cryptogrammes	Sélectionnez les algorithmes de cryptogramme que votre serveur acceptera pour le cryptage des sessions SSH.
KEX	Sélectionnez les algorithmes d'échange de clé que votre serveur acceptera pendant une session SSH.
MAC	Sélectionnez les algorithmes de code d'authentification de message que votre serveur acceptera pendant une session SSH.
Hostkey	Sélectionnez un type de clé d'hôte et la longueur de la clé pour générer une nouvelle paire de clés de l'algorithme de la clé d'hôte et de la longueur de clé.

Paramètres de profil de service SSL.	Description
	Après avoir sélectionné un type de clé d'hôte, vous pouvez saisir une longueur de clé. Le type de clé et la longueur par défaut est RSA 2048.
Données	Réglez le volume maximum de données (en mégaoctets) transmis avant une nouvelle clé SSH (plage de 10 à 4000; par défaut la valeur du cryptogramme que vous avez sélectionné).
Intervalle	Réglez l'intervalle de temps maximum (en secondes) avant une nouvelle clé SSH (plage de 10 à 3 600 ; par défaut une nouvelle clé basée sur l'absence d'intervalle).
Paquets	Réglez le nombre maximum de paquets (2^n) avant une nouvelle clé SSH. Si vous ne configurez pas ce paramètre, la session aura une nouvelle clé après 2 *28* *paquets. Afin de garantir une nouvelle clé plus fréquente, indiquez une valeur dans une fourchette de 12 à 27.*

Périphérique > Pages de réponse

Les pages de réponse personnalisées correspondent aux pages Web qui s'affichent lorsqu'un utilisateur tente d'accéder à une URL. Vous pouvez définir un message HTML personnalisé qui est téléchargé et affiché à la place de la page Web ou du fichier demandé.

Chaque système virtuel peut disposer de pages de réponse personnalisées propres. Le tableau suivant décrit les types de page de réponse personnalisée prenant en charge des messages personnalisés.

Types de page de réponse personnalisée	Description
Page de blocage de l'antivirus	Accès bloqué en raison d'une infection par un virus.
Page de blocage des applications	Accès bloqué, car l'application est bloquée par une règle de politique de Sécurité.
Page confort du Portail d'authentification	Le pare-feu affiche cette page afin que les utilisateurs puissent saisir leurs informations d'identification de connexion pour accéder aux services qui sont soumis aux règles de politique d'authentification (voir Politiques > Authentification). Saisissez un message qui indique aux utilisateurs comment relever ce défi d'authentification. Le pare-feu authentifie les utilisateurs en fonction du **Profil d'authentification** indiqué dans l'objet d'application de l'authentification attribué à une règle d'authentification (voir Objets > Authentification). *Vous pouvez afficher des instructions d'authentification uniques pour chaque règle d'authentification en saisissant un **Message** dans l'objet d'application de l'authentification associé. Le message défini dans l'objet remplace le message défini sur la Page Confort du portail d'authentification.*
Page de blocage du filtrage des données	Le contenu a été mis en correspondance avec un profil de filtrage des données et bloqué, parce que de l'information sensible a été détectée.
Page de poursuite du blocage des fichiers	Page destinée aux utilisateurs pour confirmer que le téléchargement doit se poursuivre. Cette option est disponible uniquement si la fonction de poursuite est activée dans le profil de sécurité. Sélectionnez Objets > Profils de sécurité > Blocage des fichiers.
Page de blocage des fichiers	Accès bloqué car l'accès au fichier est bloqué.

Types de page de réponse personnalisée	Description
Page d'aide de l'application GlobalProtect	Page d'aide personnalisée destinée aux utilisateurs de GlobalProtect (accessible à partir du menu des paramètres de panneau d'état GlobalProtect).
Page de connexion du portail GlobalProtect	Page de connexion destinée aux utilisateurs tentant de s'authentifier à la page Web du portail GlobalProtect.
Page d'accueil du portail GlobalProtect	Page d'accueil destinée aux utilisateurs qui réussissent à s'authentifier à la page Web du portail GlobalProtect.
Page de bienvenue de l'application GlobalProtect	Page de bienvenue destinée aux utilisateurs qui réussissent à se connecter à GlobalProtect.
Page de connexion MFA	Le pare-feu affiche cette page afin que les utilisateurs puissent relever les défis d'authentification multi-facteur (MFA) lorsqu'ils accèdent à des services qui sont soumis aux règles de politique d'authentification (voir Politiques > Authentification). Saisissez un message qui indique aux utilisateurs comment relever ce défi MFA.
Page d'erreur interne de l'authentification SAML	Page destinée à informer les utilisateurs que l'authentification SAML a échouée. La page contient un lien permettant à l'utilisateur de tenter une nouvelle authentification.
Page de notification des erreurs de certificat SSL	Notification indiquant qu'un certificat SSL a été révoqué.
Page d'exclusion de décryptage SSL	Page d'avertissement de l'utilisateur indiquant que le pare-feu décryptera les sessions SSL pour procéder à leur inspection.
Page de blocage du filtrage et des correspondances de catégories des URL	Accès bloqué par un profil de filtrage des URL ou parce que la catégorie d'URL est bloquée par une règle de politique de Sécurité.
Page de maintien et de contrôle prioritaire du filtrage des URL	Page incluant la politique de blocage initiale permettant aux utilisateurs d'ignorer le blocage. Par exemple, un utilisateur qui pense que la page a été bloquée de manière inappropriée peut cliquer sur **Continuer** pour accéder à la page. Avec la page de contrôle prioritaire, un mot de passe est requis pour que l'utilisateur puisse avoir le contrôle prioritaire sur la politique bloquant cette URL. Reportez-vous à la section Contrôle prioritaire de l'URL par l'administrateur pour obtenir des instructions sur la définition du mot de passe de contrôle prioritaire.

Types de page de réponse personnalisée	Description
Page de blocage de la mise en œuvre de la recherche sécurisée du filtrage des URL	Accès bloqué par une règle de politique de Sécurité dotée d'un profil de filtrage des URL pour lequel l'option **Mise en œuvre de la recherche sécurisée** est activée. Cette page est présentée à l'utilisateur si une recherche est effectuée à l'aide de Google, Bing, Yahoo, Yandex ou YouTube et que le paramètre de recherche sécurisée de son compte de moteur de recherche ou de navigateur n'est pas défini sur strict. La page de blocage invite l'utilisateur à définir les paramètres de recherche sécurisée sur Strict.
Page de blocage anti-hameçonnage	S'affiche aux utilisateurs lorsqu'ils tentent de saisir des informations d'identification d'entreprise valides (noms d'utilisateur ou mots de passe) sur une page Web sur laquelle l'envoi des informations d'identification est bloqué. L'utilisateur peut accéder au site, mais il ne peut toujours pas saisir des informations d'identification d'entreprise valides pour tous les formulaires Web associés. Sélectionnez Objets > Profils de sécurité > Filtrage des URL pour activer la détection des informations d'identification et contrôler l'envoi des informations d'identification sur les pages Web en fonction de la catégorie d'URL.
Page de poursuite anti-hameçonnage	Cette page met en garde les utilisateurs contre la transmission des informations d'identification de l'entreprise (noms d'utilisateur et mots de passe) vers un site Web. La mise en garde des utilisateurs contre la transmission des informations d'identification peut les décourager de réutiliser les informations d'identification de l'entreprise et les informer sur les éventuelles tentatives d'hameçonnage. Les utilisateurs visualisent cette page lorsqu'ils tentent de saisir des informations d'identification sur un site pour lequel les autorisations d'**Envoi des informations d'identification de l'utilisateur** sont définies sur **continuer** (voir Objets > Profils de sécurité > Filtrage des URL). Ils doivent sélectionner **Continuer** pour saisir les informations d'identification sur le site.

Vous pouvez exécuter l'une des fonctions suivantes pour les **Pages de réponse**.

- Pour importer une page de réponse HTML personnalisée, cliquez sur le lien du type de page que vous souhaitez modifier, puis cliquez sur Importer/Exporter. Recherchez la page. Un message indiquant si l'importation a abouti s'affiche. Pour que l'importation aboutisse, le fichier doit être au format HTML.
- Pour exporter une page de réponse HTML personnalisée, cliquez sur **Export (Exporter)** pour le type de page. Indiquez si le fichier doit être ouvert ou enregistré sur le disque, puis sélectionnez **Toujours utiliser la même option**, le cas échéant.
- Pour activer ou désactiver la page **Blocage des applications** ou les pages **Exclusion de décryptage SSL**, cliquez sur **Activer** pour le type de page. Sélectionnez ou désélectionnez **Activer**, le cas échéant.

- Pour utiliser la page de réponse par défaut au lieu de la page personnalisée précédemment chargée, supprimez la page de blocage personnalisée et validez. La page de blocage par défaut devient la nouvelle page active.

Périphérique > Paramètres des journaux

Sélectionnez **Périphérique** > **Paramètres des journaux** pour configurer des alarmes, effacer des journaux ou activer le transfert des journaux à Panorama, au service de journalisation et aux services externes.

- Sélection des destinations du transfert des journaux
- Définition des paramètres d’alarme
- Effacer les journaux

Sélection des destinations du transfert des journaux

Périphérique > **Paramètres des journaux**

La page Log Settings (Paramètres des journaux) vous permet de configurer le transfert des journaux vers :

- **Panorama, récepteurs de pièges SNMP, serveurs e-mail, serveurs Syslog et serveurs HTTP** : vous pouvez également ajouter ou supprimer des étiquettes à partir d’une adresse IP source ou de destination dans une entrée de journal ; tous les types de journaux, sauf les journaux Système et les journaux de Configuration prennent en charge l’étiquetage.
- **Service de journalisation** : si vous disposez d'un abonnement à un Service de journalisation et que vous avez activé le Service de journalisation (Périphérique > Configuration > Gestion), le pare-feu enverra alors les journaux au Service de journalisation lorsque vous configurez le transfert des journaux vers Panorama/le Service de journalisation. Panorama interrogera le Service de journalisation pour accéder aux journaux, pour afficher les journaux et pour générer des rapports.
- **Centre de sécurité Azure** : l’intégration au Centre de sécurité Azure est disponible pour les pare-feu VM-Series dans Azure.
  - Si vous avez lancé le pare-feu depuis le Centre de sécurité Azure, une règle de politique de sécurité contenant les profils de transfert des journaux est automatiquement activée pour vous.
  - Si vous avez lancé le pare-feu VM-Series à partir de la Place de marché Azure ou au moyen de modèles Azure personnalisés, vous devez sélectionnez manuellement **Azure-Security-Center-Integration (Intégration au Centre de sécurité Azure)** pour transférer les journaux système, les journaux User-ID et les journaux de correspondance HIP au Centre de sécurité Azure et utiliser le profil de transfert des journaux pour les autres types de journaux (voir Objets > Transfert des journaux).

    Le niveau gratuit du Centre de sécurité est automatiquement activé avec votre abonnement à Azure.

Vous pouvez transférer les types de journaux suivants : journaux Système, de Configuration, User-ID, de Correspondance HIP et journaux de Corrélation. Pour indiquer les destinations pour chaque type de journal, vous devez **Ajouter** un ou plusieurs profils de liste de correspondance (jusqu’à 64) et renseigner les champs décrits dans le tableau suivant.

Pour transférer les journaux de Trafic, de Menaces, d’envois WildFire, de Filtrage des URL, de Filtrage des données, d’Inspection des tunnels, de journaux GTP et de journaux d’Authentification, vous devez configurer un profil de Transfert des journaux (voir Objets > Transfert des journaux).

Paramètres du profil de la liste de correspondance	Description
Name (Nom)	Saisissez un nom (jusqu'à 31 caractères) pour identifier le profil de la liste de correspondance. Un nom valide doit commencer par un caractère alphanumérique et peut contenir des zéros, des caractères alphanumériques, des traits de soulignement, des traits d'union, des points ou des espaces.
Filtre	Par défaut, le pare-feu transfère **All Logs (Tous les journaux)** du type pour lequel vous ajoutez le profil de liste de correspondance. Pour transférer un sous-ensemble de journaux, ouvrez le menu déroulant et sélectionnez un filtre existant ou sélectionnez **Filter Builder (Générateur de filtre)** pour ajouter un nouveau filtre. Pour chaque requête dans un nouveau filtre, il vous faut renseigner les champs suivants et **Add (Ajouter)** la requête : • **Connector (Connecteur)** – Sélectionnez le connecteur logique (ET/OU) pour la requête. Sélectionnez **Negate (Ignorer)** si vous ne voulez pas appliquer le connecteur logique. Par exemple, pour éviter de transférer les journaux à partir d'une zone non approuvée, sélectionnez **Negate (Ignorer)**, sélectionnez **Zone** en tant qu'attribut, sélectionnez **equal (égal)** en tant qu'Opérateur et saisissez le nom de la Zone non approuvée dans la colonne Valeur. • **Attribute (Attribut)** – Sélectionnez un attribut de journal. Les attributs disponibles varient selon le type de journal. • **Operator (Opérateur)** - Sélectionnez des critères pour déterminer si un attribut s'applique (comme =). Les critères disponibles varient selon le type de journal. • **Value (Valeur)** : indiquez la valeur de l'attribut à faire correspondre. Pour afficher ou exporter les journaux auxquels correspond le filtre, sélectionnez **View Filtered Logs (Afficher les journaux filtrés)**. Cet onglet propose les mêmes options que les pages de l'onglet **Monitoring (Surveillance)** (telles que **Monitoring (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)**). *Définissez le filtre pour le transfert des journaux pour tous les niveaux de gravité d'événement (le filtre par défaut est fixé sur **All Logs [Tous les journaux]**). Pour créer des méthodes de transfert des journaux distinctes pour différents niveaux de gravité, spécifiez un ou plusieurs niveaux de gravité dans le **Filter (Filtre)**, configurez une **Forward Method (Méthode de transfert)**, puis répétez le processus pour les autres niveaux de gravité.*

Paramètres du profil de la liste de correspondance	Description
Description	Saisissez une description (jusqu'à 1 023 caractères) pour expliquer le but de ce profil de liste de correspondance.
Panorama/Service de journalisation	Sélectionnez **Panorama/Logging Service (Panorama/Service de journalisation)** si vous souhaitez transmettre des journaux au Service de journalisation, aux collecteurs de journaux ou au serveur de gestion Panorama. Si vous activez cette option, vous devez configurer le transfert des journaux vers Panorama . *Vous ne pouvez pas transférer les Journaux de corrélation du pare-feu à Panorama. Panorama génère des Journaux de corrélation en fonction des journaux provenant du pare-feu.*
SNMP	Cliquez pour **Ajouter** un ou plusieurs profils de serveur pour transférer des journaux en tant que pièges SNMP (voir Périphérique > Profils de serveur > Piège SNMP).
Messagerie	Cliquez pour **Ajouter** un ou plusieurs profils de serveur de messagerie pour transférer des journaux en tant que notifications par e-mail (voir Périphérique > Profils de serveur > E-mail).
Syslog	Cliquez pour **Ajouter** un ou plusieurs profils de serveur Syslog pour transférer des journaux en tant que messages Syslog (voir Périphérique > Profils de serveur > Syslog).
HTTP	Cliquez pour **Ajouter** un ou plusieurs profils de serveur HTTP pour transférer des journaux en tant que requêtes HTTP (voir Périphérique > Profils de serveur > HTTP).
Actions intégrées	Vous pouvez sélectionner deux types d'actions intégrées lorsqu vous **Add (Ajouter)** une action à faire : l'Étiquetage et l'Intégration. • **Étiquetage** : vous pouvez ajouter une action pour tous les types de journaux qui incluent une adresse IP source ou de destination dans

Paramètres du profil de la liste de correspondance	Description
	l’entrée de journal en configurant les paramètres suivants en fonction de vos besoins. *Vous pouvez identifier uniquement l’adresse IP source dans les journaux de Corrélation et les journaux de Correspondance HIP. Vous ne pouvez configurer aucune action pour les journaux Système et les journaux de Configuration parce que le type de journal n’inclut pas une adresse IP dans l’entrée de journal.* • Cliquez pour **Add (Ajouter)** une action et saisissez un nom pour la décrire. • Sélectionnez l’adresse IP que vous souhaitez étiqueter automatiquement (**Source Address (Adresse source)** ou **Destination Address (Adresse de destination)**). • Sélectionnez l’action – **Add Tag (Ajouter une étiquette)** ou **Remove Tag (Supprimer une étiquette)**. • Choisissez si vous souhaitez enregistrer l’adresse IP et étiqueter le mappage sur l’agent **Local User-ID (User-ID local)** sur ce pare-feu ou Panorama, ou sur un agent **Remote User-ID (User-ID à distance)**. • Pour enregistrer l’adresse IP et étiqueter le mappage sur un agent **User-ID à distance**, sélectionnez le profil de serveur HTTP (Périphérique > Profils de serveur > HTTP) qui permettra le transfert. • Configurez le **Timeout (Délai)**, en minutes, de l’indicateur d'adresse IP à définir, la période de temps pendant laquelle le mappage adresse IP/étiquette est maintenu. Si vous définissez le délai sur 0, le mappage de l’indicateur d'adresse IP n’expire jamais (la plage est définie entre 0 et 43 200 [30 jours] ; la valeur par défaut est 0). *Vous pouvez uniquement configurer un délai avec l’action **Add Tag (Ajouter une étiquette)**.* • Saisissez ou sélectionnez les **Tags (Étiquettes)** que vous souhaitez appliquer ou supprimer de la source cible ou de l’adresse IP de destination. • **Intégration** : disponible uniquement pour les pare-feu VM-Series dans Azure. **Add (Ajoutez)** un nom et utilisez cette action pour transférer les journaux sélectionnés au Centre de sécurité Azure. Si cette option ne s’affiche pas, il se peut que votre abonnement à Azure ne vous autorise pas à utiliser le Centre de sécurité Azure.

Paramètres du profil de la liste de correspondance	Description
	Pour ajouter un périphérique à la liste de quarantaine sur la base du filtre du profil de transfert des journaux, sélectionnez **Quarantine (Quarantaine)**.

Définition des paramètres d’alarme

- Périphérique > Paramètres des journaux

Utilisez les Paramètres d’alarme pour configurer Alarmes pour la CLI et l’interface Web. Vous pouvez configurer les notifications pour les événements suivants :

- Une règle de sécurité (ou un groupe de règles) correspondait à un seuil spécifié et était comprise dans un intervalle de temps spécifié.
- Le seuil d'échecs de chiffrement/déchiffrement est atteint.
- La base de données de journaux pour chaque type de journal est quasiment pleine ; le quota par défaut est défini pour envoyer une notification lorsque 90 % de l'espace disque disponible est utilisé. La configuration d'alarmes vous permet d'entreprendre une action lorsque le disque est plein, et les journaux sont supprimés.

Lorsque vous activez des alarmes, vous pouvez afficher la liste actuelle en cliquant sur **Alarmes** (Alarms) en bas de l’interface Web.

Pour ajouter une alarme, modifiez les Paramètres d’alarme qui sont décrits dans le tableau suivant.

Paramètres du journal des alarmes	Description
Activer les alarmes	Les alarmes ne sont visibles que si vous cliquez sur **Activer les alarmes**. *Si vous désactivez les alarmes, le pare-feu ne vous informe pas des événements critiques qui nécessitent une action. Par exemple, une alarme vous indique quand la clé principale est sur le point d’expirer. Si la clé expire avant que vous ne la modifiiez, le pare-feu redémarre en mode Maintenance et requiert une réinitialisation d’usine.*
Activer les notifications d'alarme CLI	Activez les notifications d'alarme CLI lorsque des alarmes se produisent.
Activer les notifications d'alarme Web	Ouvrez une fenêtre pour afficher les alarmes de sessions utilisateur, notamment lorsqu'elles se produisent et lorsqu'elles sont reçues.
Activer les alarmes sonores	Une tonalité d'alarme sonore retentira toutes les 15 secondes sur l'ordinateur de l'administrateur lorsque l'administrateur est connecté à l'interface Web et que des alarmes ne sont pas acquittées. La tonalité

Paramètres du journal des alarmes	Description
	d'alarme retentira jusqu'à ce que l'administrateur acquitte toutes les alarmes. Pour afficher et acquitter les alarmes, cliquez sur **Alarmes**. Cette fonction est disponible uniquement lorsque le pare-feu est en mode FIPS-CC.
Seuil d'échec du chiffrement/ déchiffrement	Indiquez le nombre d'échecs de chiffrement/déchiffrement après lequel une alarme est déclenchée.
<*Type de journal* > Base de données du journal	Générez une alarme lorsqu'une base de données de journaux atteint le pourcentage de taille maximale indiqué.
Seuil des violations de sécurité / Intervalle temporel des violations de sécurité	Une alarme est générée si une adresse IP ou un port spécifique correspond à une règle de refus le nombre de fois défini dans le paramètre **Seuil des violations de sécurité** sur la période (en secondes) indiquée dans le paramètre **Intervalle temporel des violations de sécurité**.
Seuil des violations / Intervalle temporel des violations / Etiquettes de stratégies de sécurité	Une alarme est générée si l'ensemble de règles atteint le nombre de limites de violations de règle spécifié dans le champ **Seuil des violations de sécurité** sur la période indiquée dans le champ **Période des violations**champ. Les violations sont comptabilisées lorsqu'une session correspond à une politique de refus. Utilisez des **Étiquettes de politique de sécurité** pour préciser les tags pour lesquelles les seuils de violations généreront des alarmes. Ces étiquettes peuvent être définies lors de la définition des politiques de sécurité.
Audit sélectif	Les options d'audit sélectif sont disponibles uniquement lorsque le pare-feu est en mode FIPS-CC. Définissez les paramètres suivants : • **Journalisation spécifique FIPS-CC** : active la journalisation verbeux requise pour la conformité aux Critères communs (CC). • **Journalisation des paquets supprimés** : consigne les paquets supprimés par le pare-feu. • **Interdiction de la journalisation des réussites d'ouverture de session** : cesse de consigner les connexions administrateur réussies au pare-feu. • **Interdiction de la journalisation des échecs d'ouverture de session** : cesse de consigner les connexions administrateur échouées au pare-feu. • **Journalisation des sessions TLS** : consigne les ouvertures de sessions TLS.

Paramètres du journal des alarmes	Description
	• **CA (OCSP/CRL) Journalisation des ouvertures de session AC (OCSP/CRL))** : consigne les ouvertures de session entre le pare-feu et une autorité de certification lorsque le pare-feu envoie une requête de vérification de l'état de révocation de certificat en utilisant le protocole OCSP (Online Certificate Status Protocol) ou une demande de serveur CRL (liste de révocation du certificat). (Cette option est désactivée par défaut.) • **Journalisation d'ouvertures de session IKE** : consigne les ouvertures de session IKE IPSec lorsque la passerelle VPN du pare-feu s'authentifie auprès d'un homologue. L'homologue peut être un pare-feu Palo Alto Networks ou un autre périphérique de sécurité utilisé pour initier et mettre fin à des connexions VPN. Le nom de l'interface qui est spécifié dans le journal est l'interface qui est liée à la passerelle IKE. Le nom de la passerelle IKE est également affiché, le cas échéant. La désactivation de cette option arrête la journalisation de tous les événements de journalisation IKE. (Cette option est activée par défaut.) • **Administrateurs supprimés** : cesse la journalisation des modifications apportées à la configuration du pare-feu par les administrateurs répertoriés.

Effacer les journaux

- Périphérique > Paramètres des journaux

Vous pouvez effacer les journaux sur le pare-feu lorsque vous cliquez sur Gérer les journaux à la page Paramètres des journaux. Cliquez sur le type de journal que vous souhaitez effacer et cliquez sur **Oui** pour confirmer la demande.

Pour supprimer automatiquement les journaux et les rapports, vous pouvez configurer les périodes d'expiration. Pour plus d'informations, reportez-vous à la section Paramètres de journalisation et de génération de rapports.

Périphérique > Profils de serveur

Les rubriques suivantes décrivent les paramètres du profil de serveur que vous pouvez configurer sur le pare-feu :

- Périphérique > Profils de serveur > Piège'A0;SNMP
- Périphérique > Profils de serveur > Syslog
- Périphérique > Profils de serveur > Messagerie
- Périphérique > Profils de serveur > HTTP
- Périphérique > Profils de serveur > NetFlow
- Périphérique > Profils de serveur > RADIUS
- Périphérique > Profils de serveur > TACACS+
- Périphérique > Profils de serveur > LDAP
- Périphérique > Profils de serveur > Kerberos
- Périphérique > Profils de serveur > Fournisseur d’identité SAML
- Périphérique > Profils de serveur > DNS
- Périphérique > Profils de serveur > Authentification multi-facteur

Périphérique > Profils de serveur > Piège'A0;SNMP

SNMP (Simple Network Management Protocol) est un protocole standard permettant la surveillance des périphériques sur votre réseau. Pour vous informer d'événements système ou de menaces sur votre réseau, les périphériques surveillés envoient des pièges SNMP aux gestionnaires SNMP (serveurs de pièges). Sélectionnez **Périphérique** > **Profils de serveur** > **Piège SNMP** ou **Panorama** > **Profils de serveur** > **Piège SNMP** pour configurer le profil de serveur autorisant le pare-feu ou Panorama à envoyer des pièges aux gestionnaires SNMP. Pour activer les messages SNMP GET (requêtes de statistiques d'un gestionnaire SNMP), reportez-vous à la section Activation de la surveillance SNMP.

Après avoir créé le profil de serveur, vous devez préciser les types de journaux pour lesquels le pare-feu enverra des pièges SNMP (voir Périphérique > Paramètres des journaux). Pour obtenir la liste des MIB que vous devez charger dans le gestionnaire SNMP afin qu'il puisse interpréter les pièges, reportez-vous à MIB pris en charge.

ne supprimez pas un profil de serveur utilisé par un quelconque paramètre de journal système ou profil de journalisation.

Paramètres du profil de serveur de pièges SNMP	Description
Nom	Saisissez un nom pour le profil SNMP (31 caractères maximum). Celui-ci est sensible aux majuscules et minuscules et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Emplacement	Sélectionnez la portée dans laquelle le profil est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Partagé** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner l' **Emplacement)** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le profil, vous ne pouvez plus changer son **Emplacement**.
Version	Sélectionnez la version de SNMP : **V2c** (par défaut) ou **V3**. Votre sélection détermine les autres champs affichés dans la boîte de dialogue. Pour ces deux versions, vous pouvez ajouter jusqu'à quatre gestionnaires SNMP. *Utilisez SNMPv3, qui fournit l'authentification et d'autres fonctions pour garantir la sécurité des connexions réseau.*
Pour SNMP V2c	
Nom	Donnez un nom au gestionnaire SNMP. Ce nom peut comporter jusqu'à 31 caractères, à savoir des caractères alphanumériques, des points, des traits de soulignement ou des traits d'union.

Paramètres du profil de serveur de pièges SNMP	Description
Gestionnaire SNMP	Indiquez le nom de domaine complet ou l'adresse IP du gestionnaire SNMP.
Communauté	Saisissez la chaîne de communauté qui identifie une *communauté* SNMP composée de gestionnaires SNMP et de périphériques surveillés, et qui sert également de mot de passe pour authentifier les membres de la communauté entre eux lors du transfert de pièges. La chaîne peut comporter 127 caractères maximum, accepte tous les caractères et est sensible à la casse. *N'utilisez pas la chaîne de communauté publique définie par défaut (ne définissez pas la chaîne de communauté sur **public [publique]** ou **privée**). Utilisez des chaînes de communauté uniques, qui évitent les conflits si vous utilisez plusieurs services SNMP. Les messages SNMP contenant des chaînes de communautés en clair, tenez compte des exigences de sécurité de votre réseau lors de la définition de l'appartenance à la communauté (accès administrateur).*
Pour SNMP V3	
Nom	Donnez un nom au gestionnaire SNMP. Ce nom peut comporter jusqu'à 31 caractères, à savoir des caractères alphanumériques, des points, des traits de soulignement ou des traits d'union.
Gestionnaire SNMP	Indiquez le nom de domaine complet ou l'adresse IP du gestionnaire SNMP.
Utilisateur	Saisissez un nom d'utilisateur pour identifier le compte utilisateur SNMP (31 caractères maximum). Le nom d'utilisateur que vous configurez sur le pare-feu doit correspondre au nom d'utilisateur configuré sur le gestionnaire SNMP.
Id du Moteur	Précisez l'ID du moteur du pare-feu. Lorsqu'un gestionnaire SNMP et le pare-feu s'authentifient entre eux, les messages de pièges utilisent cette valeur pour identifier le pare-feu de manière unique. Si vous ne renseignez pas ce champ, les messages utilisent le numéro de série du pare-feu pour l'**ID du moteur**. Si vous saisissez une valeur, elle doit être au format hexadécimal, préfixée par 0x et comporter entre 10 et 128 caractères supplémentaires pour représenter n'importe quel nombre de 5 à 64 octets (2 caractères par octet). Pour les pare-feu d'une configuration haute disponibilité (HD), ne renseignez pas le champ pour que le gestionnaire SNMP puisse identifier l'homologue HD qui a envoyé les pièges ; sinon, la valeur est synchronisée et les deux homologues utiliseront le même **ID du moteur**.

Paramètres du profil de serveur de pièges SNMP	Description
Mot de passe d'authentification	Indiquez le mot de passe d'authentification de l'utilisateur SNMP. Le pare-feu utilise le mot de passe pour s’authentifier sur le gestionnaire SNMP. Le mot de passe doit comporter entre 8 et 256 caractères et tous les caractères sont autorisés.
Mot de passe privé	Indiquez le mot de passe privé de l'utilisateur SNMP. Le mot de passe doit comporter entre 8 et 256 caractères et tous les caractères sont autorisés.
Protocole d'authentification	Sélectionnez l'algorithme de hachage sécurisé (SHA) pour le mot de passe du gestionnaire SNMP. Vous pouvez sélectionner **SHA-1**, **SHA-224**, **SHA-256**, **SHA-384**, ou **SHA-512**.
Protocole de confidentialité	Sélectionnez Advanced Encryption Standard (AES) pour les interruptions SNMP et les réponses aux demandes de statistiques. Vous pouvez sélectionner **AES-128**, **AES-192**, ou **AES-256**.

Périphérique > Profils de serveur > Syslog

Sélectionnez **Périphérique** > **Profils de serveurs** > **Syslog** ou **Panorama** > **Profils de serveurs** > **Syslog** pour configurer un profil de serveur pour transmettre les journaux de pare-feu, les journaux Panorama et les journaux de Collecteur de journaux en tant que messages Syslog vers un serveur Syslog. Pour définir un profil de serveur Syslog, cliquez sur **Ajouter** et remplissez les champs Nouveau serveur Syslog.

- *Pour sélectionner le profil du serveur Syslog pour les journaux Système, de Configuration, de User-ID, de Correspondance HIP et de Corrélation, voir* Périphérique > Paramètres des journaux.
- *Pour sélectionner le profil de serveur Syslog pour les journaux de trafic, de menaces, WildFire, de filtrage des URL, de filtrage de données, d'inspection des tunnels, d'authentification et de GTP, voir* Objets > Transfert des journaux.
- *Vous ne pouvez pas supprimer un profil de serveur utilisé par le pare-feu dans des paramètres du journal système ou de configuration, ou des profils de journalisation.*

Paramètres du serveur Syslog	Description
Nom	Saisissez un nom pour le profil Syslog (31 caractères maximum). Celui-ci est sensible aux majuscules et minuscules et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Emplacement	Sélectionnez la portée dans laquelle le profil est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Partagé** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner l' **Emplacement)** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le profil, vous ne pouvez plus changer son **Emplacement**.
Onglet Serveurs	
Nom	Cliquez sur **Ajouter** et saisissez un nom pour le serveur Syslog (31 caractères maximum). Celui-ci est sensible aux majuscules et minuscules et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Serveur	Saisissez l'adresse IP ou le nom de domaine complet du serveur syslog.
Transport	Indiquez si les messages Syslog doivent être transportés sur UDP, TCP ou SSL.

Paramètres du serveur Syslog	Description
	*Utilisez **SSL** pour chiffrer et sécuriser les données envoyées à un serveur syslog. Les données sont envoyées via UDP ou TCP en texte en clair et sont lisibles dans le transit.*
Port	Saisissez le numéro de port du serveur Syslog (le port standard pour UDP est 514 ; le port standard pour SSL est 6514 ; pour TCP, vous devez indiquer un numéro de port).
Format	Indiquez le forma Syslog à utiliser : BSD (par défaut) ou IETF.
Facilité	Sélectionnez l'une des valeurs Syslog standard. Sélectionnez la valeur correspondant à la manière selon laquelle votre serveur Syslog utilise le champ de la fonctionnalité pour gérer les messages. Pour plus d'informations sur le champ de la fonctionnalité, reportez-vous à RFC 3164 (format BSD) ou RFC 5424 (format IETF).
Onglet Format de journal personnalisé	
Type de journal	Cliquez sur le type de journal pour ouvrir une boîte de dialogue dans laquelle vous pouvez indiquer un format de journal personnalisé. Dans la boîte de dialogue, cliquez sur un champ pour l'ajouter à la zone du format de journal. D'autres chaînes de texte peuvent être modifiées directement dans la zone du format de journal. Cliquez sur **OK** pour enregistrer les paramètres. Consultez une description de chaque champ pouvant être utilisé pour les journaux personnalisés Pour plus d'informations sur les champs pouvant être utilisés pour les journaux personnalisés, voir Périphérique > Profils de serveur > E-mail.
Échappement	Indiquez des séquences d'échappement. **Caractères d'échappement** est une liste de tous les caractères d'échappement sans espaces.

Périphérique > Profils de serveur > Messagerie

Sélectionnez **Périphérique** > **Profils de serveurs** > **Messagerie** ou **Panorama** > **Profils de serveurs** > **Messagerie** pour configurer un profil de serveur pour transmettre des journaux en tant que notifications par courrier électronique. Pour définir un profil de serveur de messagerie, cliquez sur **Ajouter** un profil et indiquez les paramètres de notification par courrier électronique.

- *Pour sélectionner le profil du serveur de messagerie pour les journaux Système, de Configuration, de User-ID, de Correspondance HIP et de Corrélation, voir* Périphérique > Paramètres des journaux.
- *Pour sélectionner le profil de serveur de messagerie pour les journaux de trafic, de menaces, WildFire, de filtrage des URL, de filtrage de données, d'inspection des tunnels, d'authentification et de GTP, voir* Objets > Transfert des journaux.
- *Vous pouvez également planifier les rapports de messagerie* Surveillance > Rapports au format PDF > Planificateur de messagerie.
- *Vous ne pouvez pas supprimer un profil de serveur utilisé par le pare-feu dans des paramètres du journal système ou de configuration, ou des profils de journalisation.*

Paramètres de notification par courrier électronique	Description
Nom	Saisissez un nom pour le profil de serveur (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Emplacement (systèmes virtuels uniquement)	Sélectionnez la portée dans laquelle le profil est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Partagé** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner l'**Emplacement)** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le profil, vous ne pouvez plus changer son **Emplacement**.
Onglet Serveurs	
Nom	Saisissez un nom pour identifier le serveur (31 caractères maximum). Ce champ est un simple intitulé et ne doit pas comporter le nom d'hôte d'un serveur de messagerie existant.

Paramètres de notification par courrier électronique	Description
Nom d’affichage de la messagerie	Saisissez le nom indiqué dans le champ **From (De)** du courrier électronique.
De	Saisissez l’adresse électronique de l’expéditeur, par exemple alerte_securite@societe.com.
A	Saisissez l'adresse électronique du destinataire.
Destinataires supplémentaires	Facultativement, saisissez l'adresse électronique d'un autre destinataire. Vous ne pouvez ajouter qu'un seul destinataire supplémentaire. Pour ajouter plusieurs destinataires, saisissez l'adresse e-mail d'une liste de distribution.
Passerelle de messagerie	Saisissez l’adresse IP ou le nom d'hôte du serveur qui envoie l’e-mail.
Protocole	Sélectionnez le protocole que vous souhaitez utiliser pour envoyer l’email (**SMTP non authentifié** ou **SMTP over TLS (SMTP via TLS)**).
Port	Saisissez le numéro de port que vous voulez utiliser pour envoyer l’e-mail s’il est différent de celui par défaut (25 pour SMTP ou 587 pour TLS).
Version TLS (SMTP sur TLS uniquement)	Sélectionnez la version TLS que vous souhaitez utiliser (**1.2** ou **1.1**). *Nous conseillons fortement d’utiliser la dernières version TLS.*
Méthode d'authentification (SMTP sur TLS uniquement)	Sélectionnez la méthode d'authentification que vous voulez utiliser : • **Auto** (par défaut) : autorisez le client et le serveur de messagerie à déterminer la méthode d'authentification. • **Connexion** : Utilisez l’encodage Base64 pour le nom d’utilisateur et le mot de passe et transmettez-les séparément. • **Simple**: Utilisez l’encodage Base64 pour le nom d’utilisateur et le mot de passe et transmettez-les ensemble.
Profil de certificat (SMTP sur TLS uniquement)	Sélectionnez le profil de certificat pour que le pare-feu l’utilise afin d’authentifier le serveur de messagerie.
Nom d'utilisateur (SMTP sur TLS uniquement)	Saisissez le nom d’utilisateur du compte qui envoie l’e-mail.

Paramètres de notification par courrier électronique	Description
Mot de passe (SMTP sur TLS uniquement)	Saisissez le mot de passe du compte qui envoie l’e-mail.
Confirmer le mot de passe (SMTP sur TLS uniquement)	Saisissez le mot de passe du compte qui envoie l’e-mail.
Tester la connexion (SMTP sur TLS uniquement)	Confirmez la connexion entre le serveur de messagerie et le pare-feu.
Onglet Format de journal personnalisé	
Type de journal	Cliquez sur le type de journal pour ouvrir une boîte de dialogue dans laquelle vous pouvez indiquer un format de journal personnalisé. Dans la boîte de dialogue, cliquez sur un champ pour l'ajouter à la zone du format de journal. Cliquez sur **OK** pour enregistrer vos modifications.
Échappement	Indiquez les **caractères d’échappement** (tous les caractères ne sont pas interprétés littéralement) sans espace et indiquez le**caractères d’échappement** de la séquence d’espacement.

Périphérique > Profils de serveur > HTTP

Sélectionnez **Périphérique** > **Profils de serveurs** > **HTTP** ou **Panorama** > **Profils de serveurs** > **HTTP** pour configurer un profil de serveur pour transmettre des journaux. Vous pouvez configurer le pare-feu pour transférer des journaux vers une destination HTTP(S) ou pour l'intégrer à un service HTTP qui expose une API et vous pouvez modifier l'URL, l'en-tête HTTP, les paramètres et la charge utile dans la requête HTTP pour répondre à vos besoins. Vous pouvez également utiliser le profil de serveur HTTP pour accéder aux pare-feu exécutant l'agent User-ID intégré à PAN-OS et enregistrer une ou plusieurs étiquettes sur une adresse IP source ou de destination sur les journaux générés par un pare-feu.

Pour utiliser le profil de serveur HTTP pour transférer les journaux :

- *Voir Périphérique > Paramètres du journal pour les journaux du système, de configuration, d'User-ID, de correspondance HIP et de corrélation.*
- *Voir Objets > Transfert de journaux pour les journaux de trafic, de menaces, WildFire, de filtrage des URL, de filtrage des données, d'inspection des tunnels, d'authentification et de GTP.*

*Vous ne pouvez pas supprimer un profil de serveur HTTP s'il est utilisé pour transférer des journaux. Pour supprimer un profil de serveur sur le pare-feu ou Panorama, vous devez supprimer toutes les références au profil à partir du profil **Périphérique** > **Paramètres du journal** ou **Objets** > **Transfert des journaux**.*

Pour définir un profil de serveur HTTP, cliquez sur **Ajouter** un nouveau profil et configurez les paramètres dans le tableau suivant.

Paramètres du serveur HTTP	Description
Nom	Saisissez un nom pour le profil de serveur (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Un nom valide doit commencer par un caractère alphanumérique et peut contenir des zéros, des caractères alphanumériques, des traits de soulignement, des traits d'union, des points ou des espaces.
Emplacement	Sélectionnez la portée dans laquelle le profil de serveur est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Partagé** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner l' **Emplacement** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le profil, vous ne pouvez plus changer l' **Emplacement**.

Paramètres du serveur HTTP	Description
Enregistrement des balises	L'enregistrement des étiquettes vous permet d'ajouter ou de supprimer une étiquette sur une adresse IP source ou de destination dans une entrée de journal et d'enregistrer l'adresse IP et le mappage des étiquettes sur l'agent User-ID sur un pare-feu utilisant une adresse HTTP(S). Vous pouvez ensuite définir des groupes d'adresses dynamiques qui utilisent ces étiquettes comme critères de filtrage pour déterminer leurs membres et appliquer les règles de politique à une adresse IP en fonction des étiquettes. Cliquez pour **Ajouter** les détails de connexion pour activer l'accès HTTP(S) à l'agent User-ID sur un pare-feu. Pour enregistrer des étiquettes sur l'agent User-ID de Panorama, vous n'avez pas besoin d'un profil de serveur. En outre, vous ne pouvez pas utiliser le profil de serveur HTTP pour enregistrer des étiquettes dans un agent User-ID exécuté sur un serveur Windows.
Onglet Serveurs	
Nom	Cliquez pour **Ajouter** un serveur HTTP(s) et saisissez un nom (jusqu'à 31 caractères) ou un agent User-ID distant. Un nom valide doit être unique et doit commencer par un caractère alphanumérique. Le nom peut contenir des zéros, des caractères alphanumériques, des tirets bas, des traits d'union, des points ou des espaces. Un profil de serveur peut inclure jusqu'à quatre serveurs.
Adresse	Saisissez l'adresse IP du ou des serveurs HTTP. En ce qui concerne l'enregistrement des étiquettes, indiquez l'adresse IP sur le pare-feu configuré en tant qu'agent User-ID.
Protocole	Sélectionnez le protocole : HTTP ou HTTPS.
Port	Saisissez le numéro de port sur lequel il est possible d'accéder au serveur ou au pare-feu. Le port 80 est le port par défaut utilisé pour HTTP, tandis que pour HTTPS il s'agit du port 443. Pour l'enregistrement des étiquettes, le pare-feu utilise HTTP ou HTTPS pour se connecter au serveur Web sur les pare-feu qui sont configurés en tant qu'agents User-ID.
Version TLS	Sélectionnez la TLS Version (Version TLS) prise en charge par le protocole SSL sur le serveur : La valeur par défaut est de **1.2**.
Profil du certificat	Sélectionnez le profil de certificat à utiliser pour la connexion TLS avec le serveur.

Paramètres du serveur HTTP	Description
	Le pare-feu utilisera le profil de certificat spécifié pour valider le certificat du serveur lors de l'établissement d'une connexion sécurisée au serveur.
Méthode HTTP	Sélectionnez la méthode HTTP que le serveur prend en charge. Les options sont GET, PUT, POST (par défaut) et DELETE. Pour l'agent User-ID, utilisez la méthode GET.
Nom d'utilisateur	Saisissez le nom d'utilisateur qui a des autorisations d'accès pour réaliser la méthode HTTP que vous avez sélectionnée. Si vous enregistrez des étiquettes de l'agent User-ID sur un pare-feu, le nom d'utilisateur doit être celui d'un administrateur ayant un rôle de super utilisateur.
Mot de passe	Saisissez le mot de passe pour vous authentifier sur le serveur ou sur le pare-feu.
Tester la connexion au serveur	Sélectionnez un serveur et cliquez sur **Tester la connexion au serveur** pour tester la connectivité réseau au serveur. Ce test ne teste pas la connectivité d'un serveur qui exécute l'agent User-ID.
Onglet Format de la charge utile	
Type de journal	Le type de journal disponible pour le transfert HTTP s'affiche. Cliquez sur le type de journal pour ouvrir une boîte de dialogue dans laquelle vous pouvez indiquer un format de journal personnalisé.
Format	S'affiche si le type de journal utilise le format par défaut, un format prédéfini ou un format de charge utile personnalisé que vous avez défini.
Formats prédéfinis	Sélectionnez le format qui sera utilisé pour le transfert de journaux pour votre service ou votre fournisseur. Les formats prédéfinis sont affichés à l'aide de mises à jour de contenu et peuvent être modifiés chaque fois que vous installez une nouvelle mise à jour de contenu sur le pare-feu ou sur Panorama.
Nom	Saisissez un nom pour le format de journal personnalisé.
Format de l'URI	Indiquez la ressource à laquelle vous souhaitez envoyer des journaux en utilisant HTTP(S). Si vous créez un format personnalisé, l'**URI** est le terminal de ressource pour le service HTTP. Le pare-feu ajoute l'URI à l'adresse IP que vous avez définie précédemment pour construire l'URL de la requête HTTP. Assurez-vous que le format de l'URI et de la charge utile correspond à la

Paramètres du serveur HTTP	Description
	syntaxe requise par votre fournisseur tiers. Vous pouvez utiliser n'importe quel attribut pris en charge sur le type de journal sélectionné dans l'en-tête HTTP, les paramètres, les paires de valeurs et la charge utile requise.
En-têtes HTTP	Ajoutez un en-tête et sa valeur correspondante.
par le fournisseur	Indiquez les paramètres optionnels et les valeurs.
Charge utile	Sélectionnez les attributs de journal que vous souhaitez inclure en tant que charge utile dans le message HTTP pour le serveur Web externe.
Envoyer le journal de test	Cliquez sur ce bouton pour valider le fait que le serveur Web externe reçoit la demande et la charge utile au bon format.

Périphérique > Profils de serveur > NetFlow

Les pare-feu de Palo Alto Networks peuvent exporter des statistiques sur le trafic IP sur leurs interfaces sous forme de champs NetFlow vers un collecteur NetFlow. Le collecteur NetFlow est un serveur que vous utilisez pour analyser le trafic réseau pour la sécurité, l'administration, la comptabilité et le dépannage. Tous les pare-feu de Palo Alto Networks prennent en charge la version 9 de NetFlow. Les pare-feu ne prennent en charge que le protocole NetFlow unidirectionnel, et non bidirectionnel. Les pare-feu effectuent le traitement de NetFlow sur tous les paquets IP des interfaces et ne prennent pas en charge le NetFlow échantillonné. Vous pouvez exporter des enregistrements NetFlow pour les interfaces Niveau3, Niveau 2, câble virtuel, tap, VLAN, loopback et tunnel. Pour les interfaces Ethernet agrégées, vous pouvez exporter des enregistrements pour le groupe agrégé, mais pas pour les interfaces individuelles dans le groupe. Les pare-feu prennent en charge les modèles NetFlow standards et d'entreprise (propres à PAN-OS), qui sont utilisés par les collecteurs NetFlow pour déchiffrer les champs NetFlow. Les pare-feu choisissent un modèle en fonction du type de données exportées : trafic IPv4 ou IPv6, avec ou sans NAT, et avec des champs standard ou entreprise.

Pour configurer les exportations NetFlow, vous devez **Ajouter** un profil de serveur NetFlow pour indiquer les serveurs NetFlow qui recevront les données exportées et pour spécifier les paramètres d'exportation. Après avoir affecté le profil à une interface (voir Réseau > Interfaces), le pare-feu exporte les données NetFlow pour l'ensemble du trafic passant par cette interface vers les serveurs spécifiés.

Paramètres de Netflow	Description
Nom	Saisissez un nom pour le profil Netflow (31 caractères maximum). Celui-ci est sensible aux majuscules et minuscules et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Taux de rafraîchissement du modèle	Le pare-feu actualise régulièrement les modèles NetFlow pour réévaluer le modèle à utiliser (en cas de changement du type de données exportées) et pour appliquer les modifications nécessaires aux champs du modèle sélectionné. Indiquez la fréquence à laquelle le pare-feu actualise les modèles NetFlow en **Minutes** (la plage est comprise entre 1 et 3 600, la valeur par défaut est de 30) et en **Paquets** (pour les enregistrements exportés, la plage est comprise entre 1 et 600, la valeur par défaut est 20), selon les exigences de votre collecteur NetFlow. Le pare-feu actualise le modèle après que le seuil soit dépassé. Le taux de rafraîchissement requis dépend du collecteur NetFlow. Si vous ajoutez plusieurs collecteurs'A0;NetFlow au profil de serveur, utilisez la valeur du collecteur dont le taux de rafraîchissement est le plus élevé.
Délai d'activation	Indiquez la fréquence (en minutes) à laquelle le pare-feu exporte les enregistrements de données pour chaque session (plage de 1 à 60 ; par défaut 5). Définissez cette fréquence en fonction de la fréquence à laquelle vous souhaitez que le collecteur NetFlow mette à jour les statistiques du trafic.

Paramètres de Netflow	Description
Types de champs PAN-OS	Exportez des champs spécifiques à PAN-OS pour l'App-ID et le service User-ID dans des enregistrements Netflow.
Serveurs	
Nom	Indiquez un nom pour identifier le serveur (31 caractères maximum). Celui-ci est sensible aux majuscules et minuscules et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement.
Serveur	Saisissez le nom d'hôte ou l'adresse IP du serveur. Vous pouvez ajouter deux serveurs maximum par profil.
Port	Indiquez le numéro de port d’accès au serveur (par défaut 2 055).

Périphérique > Profils de serveur > RADIUS

Sélectionnez **Périphérique** > **Profils de serveurs** > **RADIUS** ou **Panorama** > **Profils de serveurs** > **RADIUS** pour configurer les paramètres des serveurs Service d'authentification d'usager distant ; RADIUS) auxquels les profils d'authentification font référence (voir Périphérique > Profil d'authentification). Vous pouvez utiliser RADIUS pour authentifier les utilisateurs finaux qui accèdent à vos ressources réseau (via GlobalProtect ou le portail d'authentification), pour authentifier les administrateurs définis localement sur le pare-feu ou sur Panorama et pour authentifier et autoriser les administrateurs définis en externe sur le serveur RADIUS.

Paramètres du serveur RADIUS	Description
Nom du profil	Saisissez un nom pour identifier le profil de serveur (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Emplacement	Sélectionnez la portée dans laquelle le profil est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Partagé** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner l'**Emplacement)** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le profil, vous ne pouvez plus changer son **Emplacement**.
Pour les administrateurs uniquement	Sélectionnez cette option pour préciser que seuls les comptes administrateur peuvent utiliser le profil pour l'authentification. Pour les pare-feu comportant plusieurs systèmes virtuels, cette option n'apparaît que si le **Emplacement** est **Partagé**.
délai d'expiration	Saisissez un intervalle, en secondes, après lequel une requête d'authentification arrive à expiration (plage de 1 à 30 ; par défaut 3). *Si vous utilisez le profil du serveur RADIUS pour intégrer le pare-feu avec un service MFA, indiquez un intervalle qui donne aux utilisateurs suffisamment de temps pour répondre à la demande d'authentification. Par exemple, si le service MFA demande un Mot de passe à usage unique ; OTP), les utilisateurs ont besoin de temps pour visualiser l'OTP sur leur périphérique final, puis pour saisir l'OTP sur la page de connexion MFA.*
Protocole d'authentification	Sélectionnez le **Protocole d'authentification** que le pare-feu utilise pour sécuriser une connexion au serveur RADIUS : • **PEAP-MSCHAPv2** : (Par défaut) Protected EAP et protocole MSCHAPv2 (Microsoft Challenge-Handshake Authentication

Paramètres du serveur RADIUS	Description
	Protocol) offre une sécurité accrue par rapport au protocole PAP ou CHAP en transmettant le nom d'utilisateur et le mot de passe dans un tunnel chiffré • **PEAP with GTC (PEAP-GTC)** : sélectionnez Protected EAP (PEAP) avec la Generic Token Card (carte à jeton générique ; GTC) pour utiliser des jetons à usage unique dans un tunnel chiffré. • **EAP-TTLS with PAP (EAP-TTLS avec PAP)** : sélectionnez EAP avec TTLS (Tunneled Transport Layer Security) et le protocole PAP pour transporter des identifiants en texte claire pour l'autorisation PAP dans un tunnel chiffré. • **Chap** : sélectionnez le protocole CHAP (Challenge-Handshake Authentication Protocol) si le serveur RADIUS ne prend pas en charge le protocole EAP ou PAP ou s'il n'est pas configuré pour celui-ci. • **PAP** : sélectionnez le protocole PAP (Password Authentication Protocol) si le serveur RADIUS ne prend pas en charge le protocole EAP ou CHAP ou s'il n'est pas configuré pour celui-ci.
Autorisez les utilisateurs à modifier les mots de passe après leur expiration.	(PEAP-MSCHAPv2 et GlobalProtect 4.1 ou version ultérieure) : sélectionnez cette option pour autoriser les utilisateurs de GlobalProtect à modifier leurs mots de passe expirés.
Rendre l'identité externe anonyme	(PEAP-MSCHAPv2, PEAP avec GTC ou EAP-TTLS avec PAP) Cette option est activée par défaut pour assurer l'anonymat de l'identité de l'utilisateur dans le tunnel externe que le pare-feu crée après s'être authentifié auprès du serveur. *Certaines configurations du serveur Radius pourraient ne pas prendre en charge les ID externes anonymes, vous pourriez donc devoir décocher cette option. Lorsqu'elle est décochée, les noms d'utilisateur sont transmis en texte clair.*
Profil du certificat	(PEAP-MSCHAPv2, PEAP avec GTC ou EAP-TTLS avec PAP) Sélectionnez ou configurez un Profil de certificat à associer à un profil de serveur RADIUS. Le pare-feu utilise le Profil du certificat pour s'authentifier auprès du serveur RADIUS.
Relances	Précisez le nombre de nouvelles tentatives après l'expiration du délai d'attente (plage de 1 à 5 ; valeur par défaut de 3).
Serveurs	Configurez les informations de chaque serveur dans l'ordre indiqué. • **Nom** - Saisissez un nom pour identifier le serveur.

Paramètres du serveur RADIUS	Description
	• **Serveur RADIUS** - Saisissez l'adresse IP ou le nom de domaine complet du serveur. • **Secret/Confirmer le secret** - Saisissez et confirmez une clé pour vérifier et chiffer la connexion entre le pare-feu et le serveur RADIUS. • **Port** - Saisissez le port du serveur (la plage est comprise entre 1 et 65 535 ; par défaut 1812) pour les requêtes d’authentification.

Périphérique > Profils de serveur > TACACS+

Sélectionnez **Périphérique** > **Profils de serveurs** > **TACACS+** ou **Panorama** > **Profils de serveurs** > **TACACS+** pour configurer les paramètres qui définissent la façon dont le pare-feu ou Panorama se connecte aux serveurs Terminal Access Controller Access-Control System Plus (TACACS+) (Voir Périphérique > Profil d'authentification). Vous pouvez utiliser TACACS+ pour authentifier les utilisateurs finaux qui accèdent à vos ressources réseau (via GlobalProtect ou le portail d'authentification), pour authentifier les administrateurs définis localement sur le pare-feu ou sur Panorama et pour authentifier et autoriser les administrateurs définis en externe sur le serveur TACACS+.

Paramètres du serveur TACACS+	Description
Nom du profil	Saisissez un nom pour identifier le profil de serveur (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Emplacement	Sélectionnez la portée dans laquelle le profil est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Partagé** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner l' **Emplacement)** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le profil, vous ne pouvez plus changer son **Emplacement**.
Pour les administrateurs uniquement	Sélectionnez cette option pour préciser que seuls les comptes administrateur peuvent utiliser le profil pour l'authentification. Pour les pare-feu à plusieurs systèmes virtuels, cette option n'apparaît que si l'**Emplacement** est **Partagé**.
délai d'expiration	Saisissez un intervalle, en secondes, après lequel une requête d'authentification arrive à expiration (plage de 1 à 30 ; par défaut 3).
Protocole d'authentification	Sélectionnez le **Protocole d'authentification** que le pare-feu utilise pour sécuriser une connexion au serveur TACACS+ : • **CHAP** – Le protocole CHAP (Challenge-Handshake Authentication Protocol) est le protocole qui est utilisé par défaut et qui est privilégié, car il est plus sécurisé que le protocole PAP. • **PAP** – Sélectionnez le protocole PAP (Password Authentication Protocol) si le serveur TACACS+ ne prend pas en charge le protocole CHAP ou s'il n'est pas configuré pour celui-ci. • **Auto** – Le pare-feu tente d'abord de s'authentifier à l'aide du protocole CHAP. Si le serveur TACACS+ ne répond pas, le pare-feu fait appel au protocole PAP.
Utiliser une simple connexion pour toutes les authentifications	Sélectionnez cette option pour utiliser la même session TCP pour toutes les authentifications. Cette option améliore la performance en empêchant le

Paramètres du serveur TACACS+	Description
	traitement requis d'ouvrir et de fermer une session TCP distincte pour chaque événement d'authentification.
Serveurs	Cliquez sur **Ajouter** et indiquez les paramètres suivants pour chaque serveur TACACS+ : • **Nom** - Saisissez un nom pour identifier le serveur. • **Serveur TACACS+** - Saisissez l'adresse IP ou le nom de domaine complet du serveur TACACS+. • **Secret/Confirmer le secret** - Saisissez et confirmez une clé pour vérifier et crypter la connexion entre le pare-feu et le serveur TACACS+. • **Port** - Saisissez le port du serveur (par défaut 49) pour les requêtes d'authentification.

Périphérique > Profils de serveur > LDAP

- **Périphérique** > **Profils de serveur** > **LDAP**
- **Panorama** > **Profils de serveur** > **LDAP**

Ajoutez ou sélectionnez un profil de serveur LDAP pour configurer les paramètres pour les serveurs Lightweight Directory Access Protocol (protocole allégé d'accès annuaire ; LDAP) auxquels les profils d'authentification font référence (voir Périphérique > Profil d'authentification). Vous pouvez utiliser LDAP pour authentifier les utilisateurs finaux qui accèdent à vos ressources réseau (via GlobalProtect ou le portail d'authentification) et les administrateurs définis localement sur le pare-feu ou sur Panorama.

Paramètres du serveur LDAP	Description
Nom du profil	Saisissez un nom pour identifier le profil (31 caractères maximum). Celui-ci est sensible aux majuscules et minuscules et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Emplacement	Sélectionnez la portée dans laquelle le profil est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Partagé** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner l' **Emplacement)** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le profil, vous ne pouvez plus changer son **Emplacement**.
Pour les administrateurs uniquement	Sélectionnez cette option pour préciser que seuls les comptes administrateur peuvent utiliser le profil pour l'authentification. Pour les pare-feu comportant plusieurs systèmes virtuels, cette option n'apparaît que si l'**Emplacement** est **Partagé**.
Liste du serveur	Pour chaque serveur LDAP, **Ajoutez** un **Nom** d'hôte, l'adresse IP ou le nom de domaine complet (**Serveur LDAP**), ainsi que le **Port** (par défaut 389). *Configurez au moins deux serveurs LDAP pour fournir la redondance.*
Type	Choisissez le type de serveur dans le menu déroulant.
Base DN	Indiquez le contexte racine dans le serveur d'annuaires afin d'affiner la recherche d'informations d'utilisateur ou de groupe.
Bind DN	Indiquez le nom de connexion (nom distinctif) du serveur d'annuaires. *Le compte Bind DN doit avoir l'autorisation nécessaire pour consulter le répertoire LDAP.*

Paramètres du serveur LDAP	Description
Mot de passe/ Confirmer le mot de passe	Indiquez le mot de passe du compte Bind. L'agent enregistre le mot de passe chiffré dans le fichier de configuration.
Lier le délai d'attente	Indiquez l'heure limite (en secondes) imposée lors de la connexion au serveur d'annuaire (la plage est comprise entre 1 et 30 ; par défaut 30).
Délai d'attente de la recherche	Indiquez l'heure limite (en secondes) imposée lors de recherches d'annuaires (la plage est comprise entre 1 et 30 ; par défaut 30).
Intervalle de relance	Indiquez l'intervalle (en secondes) après lequel le système tente de se connecter au serveur LDAP après une tentative infructueuse précédente (plage de 1 à 3 600 secondes ; par défaut 60).
Exiger une connexion sécurisée SSL/TLS	Sélectionnez cette option si vous souhaitez que le pare-feu utilise SSL ou TLS pour les communications avec le serveur d'annuaires. Le protocole dépend du port du serveur : • 389 (par défaut) – TLS (le pare-feu utilise plus précisément la fonction Démarrer l'opération TLS, qui met à niveau la connexion en texte brut initiale en TLS.) • 636 : SSL. • Tout autre port : le pare-feu tente tout d'abord d'utiliser TLS. Si le serveur d'annuaires ne prend pas en charge TLS, le pare-feu fera appel à SSL. *Cette option est recommandée, car elle accroît la sécurité et qu'elle est sélectionnée par défaut.*
Vérifier le certificat du serveur pour les sessions SSL	Sélectionnez cette option (décochée par défaut) si vous souhaitez que le pare-feu vérifie le certificat présenté par le serveur d'annuaires pour les connexions SSL/TLS. Le pare-feu vérifie deux aspects du certificat : • Le certificat est approuvé et valide. Pour que le pare-feu approuve le certificat, son autorité de certification (AC) racine et tous les certificats intermédiaires doivent se trouver dans le magasin de certificats sous **Périphérique** > **Gestion de certificats** > **Certificats** > **Certificats de périphérique**. • Le nom du certificat doit correspondre au **Nom** d'hôte du serveur LDAP. Le pare-feu vérifie tout d'abord la correspondance de l'attribut de certificat Autre nom de l'objet, puis l'attribut DN de l'objet. Si le certificat utilise le nom de domaine complet du serveur d'annuaires, vous devez utiliser le nom de domaine complet dans le champ **LDAP Server (Serveur LDAP)** pour que la correspondance du nom réussisse.

Paramètres du serveur LDAP	Description
	Si la vérification échoue, la connexion échouera également. Pour activer cette vérification, vous devez également sélectionner **Exiger une connexion sécurisée SSL/TLS**. *Activez la vérification par le pare-feu du certificat du serveur pour les sessions SSL pour accroître la sécurité.*

Périphérique > Profils de serveur > Kerberos

Sélectionnez **Périphérique** > **Profils de serveur** > **Kerberos** ou **Panorama** > **Profils de serveur** > **Kerberos** pour configurer un profil de serveur permettant aux utilisateurs de s'authentifier de manière native auprès d'un contrôleur de domaine Active Directory ou d'un serveur d'authentification compatible avec Kerberos V5. Après avoir configuré un profil de serveur Kerberos, vous pouvez l'affecter à un profil d'authentification (voir Périphérique > Profil d'authentification). Vous pouvez utiliser Kerberos pour authentifier les utilisateurs finaux qui accèdent à vos ressources réseau (via GlobalProtect ou le portail actif) et les administrateurs définis localement sur le pare-feu ou sur Panorama.

pour utiliser l'authentification Kerberos, votre serveur Kerberos dorsal doit être accessible via une adresse IPv4. Les adresses IPv6 ne sont pas prises en charge.

Paramètres du serveur Kerberos	Description
Nom du profil	Saisissez un nom pour identifier le serveur (31 caractères maximum). Celui-ci est sensible aux majuscules et minuscules et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Emplacement	Sélectionnez la portée dans laquelle le profil est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Partagé** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner l' **Emplacement)** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le profil, vous ne pouvez plus changer son **Emplacement**.
Pour les administrateurs uniquement	Sélectionnez cette option pour préciser que seuls les comptes administrateur peuvent utiliser le profil pour l'authentification. Pour les pare-feu comportant plusieurs systèmes virtuels, cette option n'apparaît que si l'**Emplacement** est **Partagé**.
Serveurs	Pour chaque serveur Kerberos, cliquez sur **Ajouter** et précisez les paramètres suivants : • **Nom** - Donnez un nom au serveur. • **Serveur Kerberos** - Saisissez l'adresse IPv4 ou le nom de domaine complet du serveur. • **Port** - Saisissez un port facultatif (la plage est comprise entre 1 et 65 535 ; par défaut 88) pour les communications avec le serveur.

Périphérique > Profils de serveur > Fournisseur d’identité SAML

Utilisez cette page pour enregistrer un fournisseur d’identité (IDP) SAML 2.0 (Security Assertion Markup Language) avec le pare-feu ou Panorama. L’enregistrement est une étape nécessaire pour que le pare-feu ou Panorama fonctionnent en tant que fournisseur de services SAML, qui contrôle l’accès à vos ressources réseau. Lorsque les administrateurs et les utilisateurs finaux demandent des ressources, le fournisseur de services redirige les utilisateurs vers l’IDP pour l’authentification. Les utilisateurs finaux peuvent être des utilisateurs de GlobalProtect ou du portail d’authentification. Les administrateurs peuvent être gérés localement sur le pare-feu et sur Panorama ou gérés en externe dans le magasin d’identité de l’IDP. Vous pouvez configurer une ouverture de session unique (SSO) en SAML afin que chaque utilisateur puisse accéder automatiquement à plusieurs ressources après avoir ouvert une session. Vous pouvez également configurer une ouverture de session unique (SSO) en SAML afin que chaque utilisateur puisse se connecter simultanément à tous les services SSO en se déconnectant de tout service unique.

Les séquences d’authentification ne prennent pas en charge les profils d’authentification qui spécifient les profils de serveur d’IDP en SAML.

Dans la plupart des cas, vous ne pouvez pas utiliser une SSO pour accéder à plusieurs applications sur le même appareil mobile.

Vous ne pouvez pas activer la SLO pour les utilisateurs du Portail d’authentification.

La manière la plus simple de créer un profil de serveur d’IDP en SAML est d’**Importer** un fichier de métadonnées contenant les informations d’enregistrement de l’IDP. Après avoir enregistré un profil de serveur avec des valeurs importées, vous pouvez éditer le profil pour modifier les valeurs. Si l’IDP ne fournit pas de fichier de métadonnées, vous pouvez **Ajouter** le profil de serveur et saisir manuellement les renseignements. Après avoir créé un profil de serveur, affectez-le à un profil d’authentification (voir Périphérique > Profil d’authentification) pour un pare-feu ou des services Panorama spécifiques.

Paramètres du serveur du fournisseur d’identité SAML	Description
Nom du profil	Saisissez un nom pour identifier le serveur (31 caractères maximum). Celui-ci est sensible aux majuscules et minuscules et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement.
Emplacement	Sélectionnez la portée dans laquelle le profil est disponible. Dans le contexte d’un pare-feu comportant plusieurs systèmes virtuels, sélectionnez un système virtuel ou sélectionnez **Partagé** (tous les systèmes virtuels). Dans n’importe quel autre contexte, vous ne pouvez pas sélectionner l’ **Emplacement** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le profil, vous ne pouvez plus changer son **Emplacement**.

Paramètres du serveur du fournisseur d'identité SAML	Description
Pour les administrateurs uniquement	Sélectionnez cette option pour préciser que seuls les comptes administrateur peuvent utiliser le profil pour l'authentification. Pour les pare-feu comportant plusieurs systèmes virtuels, cette option n'apparaît que si le **Emplacement** est **Partagé**.
ID de fournisseur d'identité	Saisissez un identifiant pour l'IDP. Votre IDP vous donne cette information.
Certificat du fournisseur d'identité	Sélectionnez le certificat que l'IDP utilise pour signer les messages SAML qu'il envoie au pare-feu. Vous devez sélectionner un certificat de l'IDP pour assurer l'intégrité des messages que l'IDP envoie au pare-feu. Pour valider le certificat de l'IDP auprès d'une autorité de certification (CA), vous devez indiquer un **Profil de certificat** pour tout profil d'authentification qui fait référence au profil de serveur de l'IDP (voir Périphérique > Profil d'authentification). Lors de la génération ou de l'importation d'un certificat et de sa clé privée associée, n'oubliez pas que les attributs d'utilisation des clés spécifiés dans le certificat contrôlent ce que vous pouvez utiliser avec la clé. Si le certificat énumère explicitement les attributs d'utilisation des clés, l'un des attributs doit être la Signature numérique, qui n'est pas disponible dans les certificats que vous générez sur le pare-feu. Dans ce cas, vous devez Importer le certificat et la clé à partir de l'autorité de certification (CA) de votre entreprise ou d'une autorité de certification tierce. Si le certificat ne spécifie pas les attributs d'utilisation des clés, vous pouvez utiliser la clé à toutes fins utiles, y compris la signature de messages. Dans ce cas, vous pouvez utiliser n'importe quelle méthode pour obtenir le certificat et la clé pour signer des messages SAML. Les certificats IDP prennent en charge les algorithmes suivants : • **Algorithmes à clé publique** : RSA (1 024 bits ou plus) et ECDSA (toutes les tailles). Un pare-feu en mode FIPS/CC prend en charge RSA (2 048 bits ou plus) et ECDSA (toutes les tailles). • **Algorithmes de signature** – SHA1, SHA256, SHA384 et SHA512. Un pare-feu en mode FIPS/CC prend en charge SHA256, SHA384 et SHA512.
URL d'authentification unique du fournisseur d'identité	Saisissez l'URL que l'IDP promeut pour son service d'authentification unique (SSO). Si vous créez le profil de serveur en important un fichier de métadonnées et que le fichier indique plusieurs URL SSO, le pare-feu utilise la première URL qui indique une méthode de liaison POST ou une méthode de redirection.

Paramètres du serveur du fournisseur d'identité SAML	Description
	Palo Alto Networks recommande fortement d'utiliser une URL qui est fondée sur HTTPS, même si SAML prend également en charge le HTTP.
URL de déconnexion unique du fournisseur d'identité	Saisissez l'URL que l'IDP promeut pour son service de déconnexion unique (SLO). Si vous créez le profil de serveur en important un fichier de métadonnées et que le fichier indique plusieurs URL SLO, le pare-feu utilise la première URL qui indique une méthode de liaison POST ou une méthode de redirection. *Palo Alto Networks recommande fortement d'utiliser une URL qui est fondée sur HTTPS, même si SAML prend également en charge le HTTP.*
Liaison HTTP SAML d'authentification unique	Sélectionnez la liaison HTTP associée à l'**URL d'authentification unique du fournisseur d'identité**. Le pare-feu utilise la liaison pour envoyer des messages SAML à l'IDP. Les options à votre disposition sont les suivantes : • **POST** – Le pare-feu envoie des messages utilisant des formulaires HTML codés en base64. • **Redirection** – Le pare-feu envoie des messages d'authentification encodés en base64 et codés en URL dans les paramètres d'URL. *Si vous importez un fichier de métadonnées de l'IDP qui possède plusieurs URL d'authentification unique, le pare-feu utilise la liaison de la première URL qui utilise la méthode POST ou la méthode de redirection. Le pare-feu ignore les URL qui utilisent d'autres liaisons.*
Liaison HTTP SAML de déconnexion unique	Sélectionnez la liaison HTTP associée à l'**URL de déconnexion unique du fournisseur d'identité**. Le pare-feu utilise la liaison pour envoyer des messages SAML à l'IDP. Les options à votre disposition sont les suivantes : • **POST** – Le pare-feu envoie des messages utilisant des formulaires HTML codés en base64. • **Redirection** – Le pare-feu envoie des messages d'authentification encodés en base64 et codés en URL dans les paramètres d'URL.

Paramètres du serveur du fournisseur d'identité SAML	Description
	Si vous importez un fichier de métadonnées de l'IDP qui possède plusieurs URL de déconnexion unique, le pare-feu utilise la liaison de la première URL qui utilise la méthode POST ou la méthode de redirection. Le pare-feu ignore les URL qui utilisent d'autres liaisons.
Métadonnées du fournisseur d'identité	Ce champ s'affiche uniquement si vous cliquez pour **Importer** un fichier de métadonnées de l'IDP que vous avez téléchargé sur le pare-feu depuis l'IDP. Le fichier indique les valeurs et le certificat de signature pour un nouveau profil de serveur de l'IDP en SAML. Vous devez **Naviguer** sur le fichier, indiquer le Nom de profil et le Déréglage d'horloge maximum, puis cliquer sur **OK** pour créer le profil. Vous pouvez également si vous le souhaitez éditer le profil pour modifier les valeurs importées.
Confirmer le certificat du fournisseur d'identité	Sélectionnez cette option pour valider la chaîne de confiance et éventuellement l'état de révocation du certificat de signature de l'IDP. Pour activez cette option, une autorité de certificat (CA) doit émettre votre certificat de signature de l'IDP. Vous devez créer un profil de certificat qui a l'autorité de certificat (CA) qui a émis le certificat de signature de l'IDP. Dans le profil d'authentification, sélectionnez le profil du serveur SAML et le profil de certificat pour valider le certificat de l'IDP (voir Périphérique > Profil d'authentification). Si le certificat de signature de l'IDP est un certificat auto-signé, il n'y pas de chaîne de confiance, par conséquent, vous ne pouvez pas activer cette option. Le pare-feu valide toujours la signature des réponses et des assertions SAML auprès du certificat de fournisseur d'identité que vous activiez ou non l'option **Confirmer le certificat du fournisseur d'identité**. Si votre IdP fournit un certificat auto-signé, assurez-vous d'utiliser PAN-OS 11.0 ou une version ultérieure pour éviter l'exposition au CVE-2020-2021.
Signer le message SAML vers IdP	Sélectionnez cette option pour indiquer que le pare-feu signe les messages qu'il envoie à l'IDP. Le pare-feu utilise le **Certificat de signature des demandes** que vous indiquez dans un profil d'authentification (voir Périphérique > Profil d'authentification). *L'utilisation d'un certificat de signature garantit l'intégrité des messages envoyés à l'IDP.*
Déréglage d'horloge maximum	Saisissez l'intervalle de temps maximal acceptable en secondes entre le moment où l'IDP envoie le message et le moment où le système de pare-feu valide le message qu'il reçoit de la part de l'IDP (la plage est de 1 à 900, la valeur par défaut est de 60). Si l'intervalle de temps dépasse cette valeur, la validation (et donc l'authentification) échoue.

Périphérique > Profils de serveur > DNS

Pour simplifier la configuration d'un système virtuel, un profil de serveur DNS vous permet de préciser le système virtuel configuré, une source d'héritage ou les adresses DNS principale et secondaire des serveurs DNS, ainsi que l'interface source et l'adresse source (itinéraire de service) qui seront utilisées dans les paquets envoyés au serveur DNS. L'interface source et l'adresse source sont utilisées comme interface de destination et adresse de destination dans la réponse du serveur DNS.

Un profil de serveur DNS s'applique à un système virtuel uniquement, et non à l'emplacement Partagé global.

Paramètres de profil de serveur DNS	Description
Nom	Nom du profil de serveur DNS.
Emplacement	Sélectionnez le système virtuel auquel le profil s'applique.
Source de l'héritage	Sélectionnez **Aucun** si les adresses du serveur DNS ne sont pas héritées. Sinon, précisez le serveur DNS duquel le profil doit hériter des paramètres.
Vérifier l'état de la source de l'héritage	Cliquez pour afficher des informations sur la source de l'héritage.
DNS principal	Indiquez l'adresse IP du serveur DNS principal.
DNS secondaire	Indiquez l'adresse IP du serveur DNS secondaire.
Itinéraire de service IPv4	Sélectionnez cette option si vous souhaitez préciser que les paquets destinés au serveur DNS proviennent d'une adresse IPv4.
Interface source	Indiquez l'interface source utilisée par les paquets destinés au serveur DNS.
Adresse source	Indiquez l'adresse source IPv4 de laquelle les paquets destinés au serveur DNS proviennent.
Itinéraire de service IPv6	Sélectionnez cette option si vous souhaitez préciser que les paquets destinés au serveur DNS proviennent d'une adresse IPv6.
Interface source	Indiquez l'interface source utilisée par les paquets destinés au serveur DNS.
Adresse source	Indiquez l’adresse source IPv6 de laquelle les paquets destinés au serveur DNS proviennent.

Périphérique > Profils de serveur > Authentification multi-facteur

Utilisez cette page pour configurer un profil de serveur d'authentification multi-facteur (MFA) qui définit comment le pare-feu se connecte à un serveur MFA. MFA peut protéger vos ressources les plus importantes en veillant à ce que les pirates ne puissent pas accéder à votre réseau et ne puissent pas le contourner en compromettant un seul facteur d'identification (par exemple, en volant les informations d'identification de connexion). Après avoir configuré le profil du serveur, affectez-le aux profils d'authentification pour les services nécessitant une authentification (voir Périphérique > Profil d'authentification).

Pour les cas d'utilisation d'authentification suivants, le pare-feu s'intègre aux fournisseurs d'authentification multifacteur (MFA) utilisant RADIUS et SAML :

- Authentification utilisateur distante via des portails et des passerelles GlobalProtect™.
- Authentification des administrateurs dans l'interface Web de PAN-OS et de Panorama™.
- Authentification via la stratégie d'authentification.

De plus, le pare-feu peut également s'intégrer aux fournisseurs MFA en utilisant l'API pour appliquer la MFA via la politique d'authentification applicable aux utilisateurs finaux uniquement (ne s'applique pas à l'authentification GlobalProtect ni à l'authentification des administrateurs).

La procédure complète utilisée pour configurer le MFA requiert des tâches supplémentaires autres que la création d'un profil de serveur.

Les séquences d'authentification ne prennent pas en charge les profils d'authentification qui spécifient les profils de serveur MFA.

Si le pare-feu s'intègre avec votre fournisseur MFA via RADIUS, configurez un profil de serveur RADIUS (voir Périphérique > Profils de serveur > RADIUS). Le pare-feu prend en charge tous les fournisseurs MFA via RADIUS.

Paramètres du serveur MFA	Description
Nom du profil	Saisissez un nom pour identifier le serveur (31 caractères maximum). Celui-ci est sensible aux majuscules et minuscules et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Emplacement	Sur un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou l'emplacement **Partagé**. Après avoir enregistré le profil, vous ne pouvez plus changer son **Emplacement**.
Profil du certificat	Sélectionnez le **Profil du certificat** qui indique le certificat de l'autorité de certification (CA) que le pare-feu utilisera pour valider le certificat du

Paramètres du serveur MFA	Description
	serveur MFA lors de la configuration d'une connexion sécurisée au serveur. Pour plus d'informations, voir Périphérique > Gestion des certificats > Profil de certificat.
Fournisseur MFA / Valeur	Sélectionnez un **fournisseur MFA** et saisissez une **Valeur** pour chaque attribut de fournisseur. Les attributs varient selon le fournisseur. Reportez-vous à la documentation de votre fournisseur pour connaître les valeurs correctes. • **Duo v2** : • **Hôte API** – Le nom d'hôte du serveur Duo v2. • **Clé d'intégration** et **clé secrète –** Le pare-feu utilise ces clés pour s'authentifier sur le serveur Duo v2 et pour signer les demandes d'authentification qu'il envoie au serveur. Pour sécuriser ces clés, la clé principale sur le pare-feu les chiffres automatiquement afin que leurs valeurs en clair ne soient pas exposées dans le stockage du pare-feu. Contactez votre administrateur Duo v2 pour obtenir les clés. • **Délai avant expiration** – Saisissez le temps en secondes après lequel le pare-feu expire lorsqu'il tente de communiquer avec l'**hôte API** (la plage est comprise entre 5 et 600, la valeur par défaut est de 30). Cet intervalle doit être plus long que le délai d'expiration entre l'hôte API et le périphérique final de l'utilisateur. • **URI de base** – Si votre organisation héberge un serveur proxy d'authentification local pour le serveur Duo v2, saisissez l'URI du serveur proxy (par défaut / auth / v2). • **Okta Adaptive** : • **Hôte API –** Le nom d'hôte du serveur Okta. • **URI de base** – Si votre organisation héberge un serveur proxy d'authentification local pour le serveur Okta, saisissez l'URI du serveur proxy (par défaut / API / v1). • **Jeton** – Le pare-feu utilise ce jeton pour s'authentifier sur le serveur Okta et pour signer les demandes d'authentification qu'il envoie au serveur. Pour sécuriser ce jeton, la clé principale sur le pare-feu le chiffre automatiquement afin que ses valeurs en clair ne soient pas exposées dans le stockage du pare-feu. Contactez votre administrateur Okta pour obtenir le jeton. • **Organisation** – Le sous-domaine de votre organisation pour l'**Hôte API**. • **Délai avant expiration** – Saisissez le temps en secondes après lequel le pare-feu expire lorsqu'il tente de communiquer avec l'**hôte API** (la plage est comprise entre 5 et 600, la valeur par défaut est de 30). Cet intervalle doit être plus long que le délai d'expiration entre l'hôte API et le périphérique final de l'utilisateur.

Paramètres du serveur MFA	Description
	• **PingID** : • **URI de base** – Si votre organisation héberge un serveur proxy d'authentification local pour le serveur PingID, saisissez l'URI du serveur proxy (par défaut / PingID / 4). • **Nom d'hôte** – Saisissez le nom d'hôte du serveur PingID (par défaut idpxnyl3m.pingidentity.com). • **Utilisation de la clé en base64** et du **jeton –** Le pare-feu utilise la clé et le jeton pour s'authentifier sur le serveur PingID et pour signer les demandes d'authentification qu'il envoie au serveur. Pour sécuriser la clé et le jeton, la clé principale sur le pare-feu les chiffres automatiquement afin que leurs valeurs en clair ne soient pas exposées dans le stockage du pare-feu. Contactez votre administrateur PingID pour obtenir les valeurs. • **ID de l'organisation client PingID** – L'identifiant PingID pour votre organisation. • **Délai avant expiration** – Saisissez le temps en secondes après lequel le pare-feu expire lorsqu'il tente de communiquer avec le serveur PingID spécifié dans le champ **Nom de l'hôte** (la plage est comprise entre 5 et 600, la valeur par défaut est de 30). Cet intervalle doit être plus long que le délai d'expiration entre le serveur PingID et le périphérique final de l'utilisateur.

Périphérique > Base de données d'utilisateurs locale > Utilisateurs

Vous pouvez configurer une base de données locale sur le pare-feu pour stocker les informations d'authentification pour les administrateurs du pare-feu, les utilisateurs finaux du Portail d'authentification et les utilisateurs finaux qui s'authentifient sur un Portail GlobalProtect et une passerelle GlobalProtect. L'authentification de la base de données locale ne nécessite aucun service d'authentification externe, vous pouvez effectuer toute la gestion du compte sur le pare-feu. Après avoir créé la base de données locale et (éventuellement) assigné les utilisateurs aux groupes (voir Périphérique > Base de données locale des utilisateurs > Groupes d'utilisateurs), vous pouvez cliquer sur Périphérique > Profil d'authentification en fonction de la base de données locale.

Vous ne pouvez pas configurer la section Périphérique > Profils de mots de passe pour les comptes administratifs qui utilisent l'authentification de la base de données locale.

Pour **Ajouter** un utilisateur local à la base de données, configurez les paramètres décrits dans le tableau suivant.

Paramètres d'utilisateur local	Description
Nom	Saisissez un nom pour identifier l'utilisateur (31 caractères maximum). Celui-ci n'est pas sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Emplacement	Sélectionnez la portée dans laquelle le compte utilisateur est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Partagé** (tous les systèmes virtuels). Dans n'importe quel autre contexte, vous ne pouvez pas sélectionner l'**Emplacement** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le compte utilisateur, vous ne pouvez plus changer son **Emplacement**.
Mode	Utilisez ce champ pour préciser l'option d'authentification : • **Mot de passe** - Saisissez et confirmez un mot de passe pour l'utilisateur. • **Hachage du mot de passe** – Saisissez une chaîne de mot de passe haché. Cela peut être utile si, par exemple, vous souhaitez réutiliser les informations d'identification pour un compte Unix existant, mais que vous ne connaissez pas le mot de passe en clair, seulement le mot de passe haché. Le pare-feu accepte n'importe quelle chaîne de 63 caractères indépendamment de l'algorithme utilisé pour générer la valeur de hachage. La commande CLI opérationnelle **`request password-hash password`** utilise l'algorithme SHA256 en modes normal et CC/FIPS.

Paramètres d’utilisateur local	Description
	Tous les paramètres de Complexité minimale du mot de passe *que vous avez définis pour le pare-feu (**Périphérique** > **Configuration** > **Gestion**) ne s’appliquent pas aux comptes qui utilisent un **Mot de passe haché**.*
Activer	Sélectionnez cette option pour activer le compte utilisateur.

Périphérique > Base de données d'utilisateurs locale > Groupes d'utilisateurs

Sélectionnez **Périphérique** > **Base de données d’utilisateurs locale** > **Groupes d’utilisateurs** pour ajouter des informations de groupes d’utilisateurs à la base de données locale.

Paramètres de groupe d’utilisateurs locaux	Description
Name (Nom)	Saisissez un nom pour identifier le groupe (31 caractères maximum). Celui-ci n’est pas sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement.
Emplacement	Sélectionnez la portée dans laquelle le groupe d'utilisateurs est disponible. Dans le contexte d'un pare-feu comportant plusieurs systèmes virtuels (vsys), sélectionnez un système virtuel ou **Partagé** (tous les systèmes virtuels). Dans n’importe quel autre contexte, vous ne pouvez pas sélectionner le **Emplacement** ; sa valeur est prédéfinie sur Partagé (pare-feu) ou sur Panorama. Après avoir enregistré le groupe d'utilisateurs, vous ne pouvez plus changer son **Emplacement**.
Tous les utilisateurs locaux	Cliquez sur **Ajouter** pour sélectionner les utilisateurs que vous souhaitez ajouter au groupe.

Périphérique > Exportation programmée des journaux

Vous pouvez planifier des exportations des journaux et les enregistrer sur un serveur FTP (File Transfer Protocol) au format CSV ou utilisez la fonction SCP (Secure Copy) pour transférer des données en toute sécurité entre le pare-feu et un hôte distant. Les profils des journaux contiennent les informations relatives à la planification et au serveur FTP. Par exemple, un profil peut déterminer que les journaux du jour précédent sont collectés chaque jour à 15 heures et stockés sur un serveur FTP spécifique.

Cliquez sur **Ajouter** et renseignez les informations suivantes :

Paramètres d'exportation programmée des journaux	Description
Nom	Saisissez un nom pour identifier le profil (31 caractères maximum). Celui-ci est sensible aux majuscules et minuscules et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement. Une fois le profil créé, vous ne pouvez pas en modifier le nom.
Description	Saisissez une description (facultatif) (jusqu'à 255 caractères).
Activer	Sélectionnez cette option pour activer la planification des exportations des journaux.
Type de journal	Sélectionnez le type de journal (**trafic**, **menace**, **gtp**, **sctp**, **tunnel**, **id utilisateur**, **autorisation**, **url**, **données**, **correspondance HIP** ou **wildfire**). La valeur par défaut est trafic.
Heure (quotidienne) de début de l'exportation programmée	Saisissez l'heure (hh:mm) à laquelle le démarrage de l'exportation doit débuter en utilisant le format d'horloge 24 heures (00:00 - 23:59).
Protocole	Sélectionnez le protocole à utiliser pour l'exportation des journaux entre le pare-feu et un hôte distant : • **FTP** – Ce protocole n'est pas sécurisé. • **SCP** – Ce protocole est sécurisé. Après avoir renseigné les champs restants, vous devez cliquer sur **Tester la connexion au serveur SCP** pour tester la connectivité entre le pare-feu et le serveur SCP et vous devez vérifier et accepter la clé d'hôte du serveur SCP.
Nom d'hôte	Saisissez l'adresse'A0;IP ou le nom d'hôte du serveur FTP utilisé pour l'exportation.
Port	Saisissez le numéro de port utilisé par le serveur FTP. La valeur par défaut est 21.

Paramètres d’exportation programmée des journaux	Description
Chemin d'accès	Précisez le chemin d'accès sur le serveur FTP qui sera utilisé pour stocker les informations exportées.
Activer le mode passif FTP	Sélectionnez cette option pour utiliser le mode passif pour l'exportation. Cette option est cochée par défaut.
Nom d’utilisateur	Saisissez le nom d'utilisateur d'accès au serveur FTP. La valeur par défaut est anonyme.
Mot de passe/ Confirmer le mot de passe	Saisissez le mot de passe d'accès au serveur FTP. Le mot de passe n’est pas nécessaire si l’utilisateur est anonyme.
Tester la connexion au serveur SCP (Protocole SCP uniquement)	Si vous définissez le **Protocol (protocole)** sur **SCP**, vous devez cliquer sur ce bouton pour tester la connectivité entre le pare-feu et le serveur SCP. Une fenêtre contextuelle s’affiche vous demandant d’entrer **Password (mot de passe)** en texte clair du serveur SCP, puis **Confirm Password (confirmer le mot de passe)**. *Si vous utilisez un modèle Panorama pour configurer la planification de l’exportation de journal, vous devez réaliser cette étape après avoir validé la configuration du modèle sur les pare-feu. Une fois le modèle validé, connectez-vous à chaque pare-feu, ouvrez la planification de l’exportation des journaux et cliquez sur **Testez la connexion au serveur SCP)**.*

Périphérique > Logiciel

Sélectionnez **Périphérique** > **Logiciel** pour afficher les versions logicielles disponibles, télécharger ou charger une version, installer une version (une licence de support est requise), supprimer une image logicielle du pare-feu ou consulter les notes de version.

Avant d'effectuer une mise à niveau vers une version antérieure ou ultérieure de votre logiciel :

- Passez en revue les Notes de version en vigueur pour consulter les descriptions des nouvelles caractéristiques et des modifications apportées aux comportements par défaut dans une version et pour connaître le chemin de migration pour la mise à niveau du logiciel.
- Examinez les éléments à considérer pour la mise à niveau vers une version antérieure ou ultérieure ainsi que les instructions de mises à niveau dans le PAN-OS® 11.0 New Features Guide (Guide des nouvelles caractéristiques de Pan-OS® version 11.0).
- Assurez-vous que les paramètres de date et d'heure du pare-feu sont à jour. Le logiciel PAN-OS est signé numériquement et le pare-feu vérifie la signature avant l'installation d'une nouvelle version. Si les paramètres de date et d'heure du pare-feu ne sont pas à jour et que le pare-feu interprète que la signature du logiciel est par la suite incorrecte, il affichera le message suivant :

```
Échec du déchiffrement : GnuPG edit non-zero, avec le code 171072
 Impossible de charger dans le gestionnaire de logiciels PAN.
```

Le tableau suivant vous aide à utiliser la page **Logicielle**.

Champs optionnels du logiciel	Description
Version	Répertorie les versions logicielles actuellement disponibles sur le serveur de mises à jour Palo Alto Networks. Pour vérifier si une nouvelle version du logiciel est disponible auprès de Palo Alto Networks, cliquez sur **Vérifier maintenant**. Le pare-feu utilise l'itinéraire de service pour se connecter au serveur de mises à jour, y rechercher de nouvelles versions et, si des mises à jour sont disponibles, les afficher en tête de liste.
Taille	Indique la taille de l'image logicielle.
Date de version	Indique la date et l'heure de disponibilité de la version auprès de Palo Alto Networks.
Disponible	Indique que la version correspondante de l'image logicielle est chargée ou téléchargée sur le pare-feu.
Actuellement installé	Indique si la version correspondante de l'image logicielle est activée et en cours d'exécution sur le pare-feu.
Action	Indique l'action que vous pouvez entreprendre pour l'image logicielle correspondante comme suit :

Champs optionnels du logiciel	Description
	• **Valider :**la version logicielle correspondante est disponible sur le serveur de mise à jour palo alto networks ; cliquez pour télécharger **une version logicielle disponible et ses dépendances logicielles ou de contenu à** partir du serveur de mise à jour ou d'un serveur SCP. • **Installer** : la version correspondante du logiciel a été téléchargée ou chargée sur le pare-feu ; cliquez sur **Installer** pour installer le logiciel. Un redémarrage est requis pour terminer le processus de mise à niveau. • **Réinstaller** : la version correspondante du logiciel a été précédemment installée ; cliquez sur **Réinstaller** pour réinstaller la même version.
Notes de version	Cette option fournit un lien vers les notes de version relatives à la mise à jour logicielle correspondante. Ce lien est disponible uniquement pour les mises à jour que vous avez téléchargées depuis le serveur de mises à jour Palo Alto Networks : il ne s'applique pas aux mises à jour chargées.
	Il supprime l'image logicielle précédemment téléchargée ou chargée à partir du pare-feu. Vous ne souhaiterez peut-être supprimer que l'image de base de versions antérieures pour lesquelles une mise à niveau ne sera pas nécessaire. Par exemple, si vous exécutez la version 10.1, vous pouvez supprimer l'image de base de 10.0 si vous pensez avoir besoin d'une version antérieure.
Vérifier maintenant	Permet de vérifier si une nouvelle mise à jour logicielle est disponible auprès de Palo Alto Networks. *Vous avez des difficultés à vérifier les mises à jour logicielles ? Reportez-vous à* cet article *pour obtenir des solutions à certains des problèmes de connectivité courants.*
Télécharger	Permet d'importer une image de mise à jour logicielle d'un ordinateur auquel le pare-feu a accès. Vous effectuez généralement cette action si le pare-feu n'a pas accès à Internet, ce qui est nécessaire pour télécharger des mises à jour du serveur de mises à jour Palo Alto Networks. Pour effectuer des chargements, utilisez un ordinateur connecté à Internet pour vous rendre sur le site Web de Palo Alto Networks, téléchargez l'image logicielle à partir du Site de support (Mises à jour logicielles), téléchargez la mise à jour sur votre ordinateur, puis sélectionnez **Périphérique** > **Logiciel** sur le pare-feu et cliquez sur **Télécharger** l'image logicielle. Dans une configuration haute disponibilité (HD), vous pouvez sélectionner l'option **Synchroniser sur homologue** pour appliquer l'image logicielle importée à l'homologue HD. Après le chargement, la page **Logiciel** affiche les mêmes informations (version et taille par exemple), ainsi que les options **Installer** / **Réinstaller** pour les logiciels chargés et téléchargés. L'option **Release Notes** n'est pas active pour les logiciels chargés.

Périphérique > Mises à jour dynamiques

- Périphérique > Mises à jour dynamiques
- Panorama > Mises à jour dynamiques

Palo Alto Networks publie régulièrement des mises à jour qui incluent les applications nouvelles et modifiées, la protection contre les menaces les fichiers de dictionnaire de l'appareil pour IoT Security, ainsi que des fichiers de données GlobalProtect via des mises à jour dynamiques. Le pare-feu peut extraire ces mises à jour et les utiliser pour appliquer la politique, sans exiger de modifications de configuration. Les mises à jour d'application et certaines mises à jour antivirus sont disponibles sans abonnement ; d'autres sont liées à vos abonnements.

Vous pouvez consulter les dernières mises à jour, lire les notes de version de chaque mise à jour, puis sélectionner la mise à jour que vous souhaitez télécharger et installer. Vous pouvez également rétablir la version précédemment installée d'une mise à jour.

L'établissement d'un calendrier de mises à jour dynamiques vous permet de définir la fréquence à laquelle le pare-feu vérifie la présence de nouvelles mises à jour et, le cas échéant, les télécharge ou les installe. Dans le cas particulier des mises à jour de contenu des applications et des menaces, vous pourriez souhaiter définir un calendrier qui échelonne les mises à jour d'applications nouvelles et modifiées après les mises à jour des menaces ; vous disposeriez ainsi de plus de temps pour évaluer l'incidence des applications nouvelles et modifiées sur votre politique de sécurité, tout en vous assurant que les protections contre les menaces les plus récentes sont installées sur votre pare-feu.

Options des mises à jour dynamiques	Description
Version	Répertorie les versions actuellement disponibles sur le serveur de mises à jour Palo Alto Networks. Pour vérifier si une nouvelle version du logiciel est disponible auprès de Palo Alto Networks, cliquez sur **Vérifier maintenant**. Le pare-feu utilise l'itinéraire de service pour se connecter au serveur de mises à jour, y rechercher de nouvelles versions du contenu et, si des mises à jour sont disponibles, les afficher en tête de liste.
Dernière vérification	Affiche la date et l'heure auxquelles le pare-feu s'est connecté pour la dernière fois au serveur de mises à jour et a vérifié si une mise à jour était disponible.
Programmer	Vous permet de planifier la fréquence de récupération des mises à jour. Vous pouvez définir la fréquence et le moment où les mises à jour dynamiques du contenu se produisent, soit la **Récurrence** et l'intervalle de temps, ainsi que l'option permettant de **Télécharger uniquement** ou de **Télécharger et installer** les mises à jour planifiées. Dans le cas des mises à jour Antivirus, et Applications et menaces, vous avez l'option de définir un seuil de temps minimum de disponibilité d'une mise à jour de contenu qu'un pare-feu doit attendre avant de l'installer. Il arrive, très rarement, qu'une erreur se glisse dans une mise à jour de contenu. Ce seuil fait en sorte que le pare-feu ne télécharge que

Options des mises à jour dynamiques	Description
	des versions de contenu qui sont disponibles et fonctionnent dans les environnements des clients depuis la période de temps indiquée. Pour ce qui est des mises à jour de contenu Applications et Menaces, vous pouvez également définir un seuil qui s'applique spécialement aux mises à jour de contenu des applications nouvelles et modifiées. Un seuil prolongé pour les mises à jour de contenu des applications vous donne plus de temps pour évaluer et ajuster votre politique de sécurité en fonction des changements qui accompagnent les applications nouvelles ou modifiées. Pour les mises à jour WildFire, vous avez l'option de récupérer les signatures en temps réel, ce qui vous permet d'accéder aux signatures dès qu'elles sont générées. Les signatures qui sont téléchargées au cours d'une vérification d'échantillon sont enregistrées dans la mémoire cache du pare-feu et sont disponibles pour des recherches rapides (locales). De plus, afin de maximiser la couverture, le pare-feu téléchargera aussi automatiquement un package de signatures supplémentaire de façon régulière lorsque les signatures en temps réel sont activées. Ces signatures complémentaires sont ajoutées à la mémoire cache du pare-feu et restent disponibles jusqu'à ce qu'elles soient dépassées, actualisées ou remplacées par de nouvelles signatures. *Pour obtenir de l'aide sur l'obtention optimale des mises à jour de contenu Applications et Menaces afin d'assurer la disponibilité continue des applications et la protection contre les dernières menaces, consultez les* Pratiques exemplaires relatives aux mises à jour des applications et des menaces.
Nom du fichier	Affiche le nom du fichier inclut les informations de version du contenu.
Caractéristiques	Répertorie le type de signatures que la version du contenu peut contenir. Pour les versions du contenu Applications et menaces, ce champ peut afficher une option pour consulter les **Applications et menaces**. Sélectionnez cette option pour afficher les nouvelles signatures d'applications disponibles depuis la dernière version du contenu installée sur le pare-feu. Vous pouvez également utiliser la boîte de dialogue **New Applications (Nouvelles applications)** pour **Activer / désactiver** de nouvelles applications. Vous pouvez choisir de désactiver une nouvelle application incluse dans une version du contenu si vous souhaitez empêcher l'impact sur la politique d'une application identifiée de manière unique (une application pouvant être traitée différemment avant et après l'installation du contenu si une application déjà connue est identifiée et classée différemment).

Options des mises à jour dynamiques	Description
	Pour Device Dictionary, ce champ est **IoT**, abréviation de *IoT Security*, le service Cloud Security, qui utilise le dictionnaire d'appareil comme composant essentiel dans l'application précise des règles de stratégie de sécurité basées sur Device-ID.
Type	Indique si le téléchargement inclut une mise à jour complète ou incrémentielle de la base de données.
Taille	Affiche la taille du module de mise à jour du contenu.
Sha256	Somme de contrôle utilisée pour vérifier l'intégrité du fichier.
Date de version	Date et heure de disponibilité de la version du contenu auprès de Palo Alto Networks.
Téléchargé	Une coche dans cette colonne indique que la version du contenu correspondante a été téléchargée sur le pare-feu.
Actuellement installé	Une coche dans cette colonne indique que la version du contenu correspondante est en cours d'exécution sur le pare-feu.
Action	Indique l'action que vous pouvez entreprendre pour l'image logicielle correspondante comme suit : • **Télécharger** - La version du contenu correspondante est disponible sur le serveur de mises à jour Palo Alto Networks ; cliquez sur **Télécharger** pour télécharger les versions du contenu. Si le pare-feu ne dispose pas d'un accès à Internet, utilisez un ordinateur branché à l'Internet pour consulter le Portail de support aux clients, puis sélectionner **Mises à jour dynamiques**. Trouvez la version du contenu que vous souhaitez télécharger et cliquez sur **Télécharger** pour enregistrer le module de mise à jour sur votre ordinateur local. Ensuite cliquez sur **Charger** pour charger manuellement l'image logicielle au pare-feu. De plus, le téléchargement d'une version du contenu Applications et menaces active l'option **Réviser les politiques** qui sont affectées par les nouvelles signatures d'applications incluses dans cette version. • **Réviser les politiques** (contenu Applications et menaces uniquement) – Révisez l'impact des politiques pour les nouvelles applications incluses dans une version du contenu. Utilisez cette option pour évaluer le traitement d'une application avant et après l'installation d'une version du contenu. Vous pouvez également utiliser la boîte de dialogue Examen de la politique pour ajouter ou supprimer une application en attente (une application téléchargée avec une version du contenu, mais non installée sur le pare-feu) à ou à partir d'une règle de politique de Sécurité existante. Les changements de

Options des mises à jour dynamiques	Description
	politiques des applications en attente ne s'appliquent que lorsque la version du contenu correspondante est installée. • **Examiner les applications** (contenu Applications et Menaces uniquement) – Affichez les signatures d'applications, nouvelles et modifiées, disponibles depuis la dernière version du contenu installée sur le pare-feu. Si une mise à jour de contenu introduit des changements qui pourraient avoir une incidence sur la mise en œuvre des applications critiques, ces applications sont alors marquées et un examen de la politique est recommandé. Cliquez sur Réviser les politiques pour voir l'incidence des mises à jour de contenu sur votre politique de sécurité existante. Vous pouvez également désactiver une application jusqu'à ce que vous ayez le temps d'examiner son incidence sur la politique. • **Installer** - La version du contenu correspondante a été téléchargée sur le pare-feu ; cliquez sur **Installer** pour installer la mise à jour. Lorsque vous installez une nouvelle version du contenu Applications et menaces, vous êtes invité à choisir l'option **Désactiver les nouvelles applications dans la mise à jour du contenu**. Cette option vous protège contre les dernières menaces, vous permettant ainsi d'activer des applications après la préparation de mises à jour de politique en raison de l'impact de nouvelles signatures d'applications (pour activer des applications précédemment désactivées, sélectionnez **Applications et menaces** sur la page Mises à jour dynamiques ou sélectionnez **Objets** > **Application**). • **Rétablir** : la version du contenu correspondante a été précédemment téléchargée. Pour réinstaller la même version, cliquez sur **Rétablir**.
Documentation	Cette option fournit un lien vers les notes de version relatives à la version correspondante.
	Supprimez la version du contenu précédemment téléchargée à partir du pare-feu.
Télécharger	Si le pare-feu n'a pas accès au Serveur de mises à jour Palo Alto Networks, vous pouvez télécharger manuellement les mises à jour dynamiques dans la section Mises à jour dynamiques du Site de support de Palo Alto Networks. Après avoir téléchargé une mise à jour sur votre ordinateur, cliquez sur **Charger** pour charger la mise à jour du pare-feu. Sélectionnez ensuite **Installer depuis le fichier**, puis sélectionnez le fichier que vous avez téléchargé.
Installer depuis le fichier	Après avoir chargé manuellement un fichier de mise à jour sur le pare-feu, utilisez cette option pour installer le fichier. Dans le menu déroulant **Type de module**, sélectionnez le type de mise à jour que vous installez (**Application et menaces**, **Antivirus** ou **WildFire**) et cliquez sur **OK**,

Options des mises à jour dynamiques	Description
	sélectionnez ensuite le fichier que vous souhaitez installer, puis cliquez sur **OK** pour lancer l'installation.

Périphérique > Licences

Sélectionnez **Périphérique** > **Licences** pour activer des licences sur tous les modèles de pare-feu. Lorsque vous souscrivez à un abonnement auprès de Palo Alto Networks, vous recevez un code d'autorisation pour activer une ou plusieurs clés de licence.

Sur le pare-feu VM-Series, cette page vous permet également de désactiver une machine virtuelle (MV).

Les actions suivantes sont disponibles dans la page Licences :

- Récupérer les clés de licence auprès du serveur de licences : Sélectionnez cette option pour activer des abonnements souscrits qui requièrent un code d'autorisation et qui ont été activés sur le portail de support.
- Activer la fonction à l'aide du code d'autorisation : Sélectionnez cette option pour activer des abonnements souscrits qui requièrent un code d'autorisation et qui n'ont pas été activés sur le portail de support. Saisissez ensuite votre code d'autorisation, puis cliquez sur **OK**.
- Charger manuellement la clé de licence : si le pare-feu ne parvient pas à se connecter au serveur de licences et que vous souhaitez charger manuellement des clés de licence, téléchargez le fichier de la clé de licence à l'adresse https://support.paloaltonetworks.com et enregistrez-le localement. Cliquez sur Charger manuellement la clé de licence, sur Parcourir, sélectionnez le fichier, puis cliquez sur OK.

  *Pour activer une licence pour le filtrage des URL, vous devez l'installer, télécharger la base de données, puis cliquer sur **Activer**. Si vous utilisez PAN-DB pour le filtrage des URL, vous devrez **Télécharger** la base de données d'amorçage initiale, puis cliquer sur **Activer**.*

  *Vous pouvez également exécuter la commande de la CLI **`request url-filtering paloaltonetworks region <nom de la région>`**.*
- **Désactiver MV** : Cette option est disponible sur le pare-feu VM-Series avec le modèle Bring Your Own License (apportez votre propre licence) qui prend en charge les licences permanentes et basées sur une durée ; le modèle de licence à la demande ne prend pas en charge cette fonctionnalité. Cliquez sur **Désactiver MV** lorsque vous n'avez plus besoin d'une instance du pare-feu VM-Series. Cela vous permet de libérer toutes les licences actives (licences d'abonnement, licences de Capacité MV et droits de support) qui utilisent cette option. Les licences sont recréditées sur votre compte et vous pouvez les appliquer à une nouvelle instance d'un pare-feu VM-Series lorsque vous en avez besoin. Lorsque la licence est désactivée, la fonctionnalité du pare-feu VM-Series est désactivée et l'état du pare-feu est « sans licence ». Cependant, la configuration demeure intacte.
  - Cliquez sur **Continuer manuellement** si le pare-feu VM-Series ne dispose pas d'un accès direct à Internet. Le pare-feu génère un fichier de jeton. Cliquez sur **Exporter le jeton de licence** pour enregistrer le fichier de jeton sur votre ordinateur local, puis redémarrez le pare-feu. Connectez-vous au portail d'Assistance Palo Alto Networks, sélectionnez **Actifs** > **Périphériques** ainsi que **Désactiver la VM)** pour utiliser ce fichier de jeton et terminer le processus de désactivation.
  - Cliquez sur **Continuer** pour désactiver les licences sur le pare-feu VM-Series. Cliquez sur **Redémarrer maintenant** pour terminer le processus de désactivation de licence.
  - Cliquez sur **Annuler** si vous souhaitez annuler et fermer la fenêtre Désactiver MV.

- **Mettre à niveau la capacité de la machine virtuelle** : cette option vous permet d'améliorer les capacités de votre pare-feu VM-Series actuellement autorisé. Lors de l'amélioration des capacités, le pare-feu VM-Series conserve toute la configuration et les abonnements qu'il avait avant la mise à jour.
  - Si votre pare-feu est connecté au serveur de licence – Sélectionnez **Code d'autorisation**, saisissez votre code dans le champ Code d'autorisation et cliquez sur **Continuer** pour lancer la mise à jour des capacités.
  - Si votre pare-feu n'est pas connecté au serveur de licence – Sélectionnez **Clé de licence**, cliquez sur **Compléter manuellement** pour générer un fichier de jeton et enregistrer le fichier de jeton sur votre ordinateur local. Connectez-vous ensuite au Portail de support de Palo Alto Networks, sélectionnez **Actifs** > **Périphériques** et cliquez sur **Désactiver licence(s)** pour utiliser le fichier de jeton. Téléchargez la clé de licence pour votre pare-feu VM-Series sur votre ordinateur local, ajoutez la clé de licence au pare-feu et cliquez sur **Continuer** pour terminer la mise à niveau des capacités.
  - Si votre pare-feu est connecté au serveur de licence, mais que vous n'avez pas de code d'autorisation – Sélectionnez l'option **Récupérer auprès du serveur de licences**, mettez à jour la licence de capacité du pare-feu sur le serveur de licences avant d'essayer de mettre à jour la capacité, puis, après avoir vérifié que la licence a bien été mise à jour sur le serveur de licences, cliquez sur **Continuer** pour lancer la mise à jour de la capacité.

Périphérique > Support

- Périphérique > Support
- Panorama > Support

Sélectionnez **Périphérique** > **Assistance** ou **Panorama** > **Support (Assistance)** pour accéder aux options relatives au support. Vous pouvez consulter les informations de contact de Palo Alto Networks, la date d'expiration du support, ainsi que les alertes produit et de sécurité de Palo Alto Networks en fonction du numéro de série de votre pare-feu.

Exécutez l'une des fonctions suivantes sur cette page:

- **Assistance** – Fournit des informations sur l'état de l'assistance de l'appareil et fournit un lien pour activer l'assistance à l'aide d'un code d'autorisation.
- **Alertes de production / alertes d'application et de menace** – Ces alertes sont récupérées à partir des serveurs de mises à jour Palo Alto Networks lorsqu'un utilisateur actualise / accède à cette page. Pour consulter les informations des alertes de production, ou celles des alertes d'application et de menace, cliquez sur le nom de l'alerte. Les alertes de production sont publiées en cas de rappel à grande échelle ou de problème urgent relatif à une version donnée. Les alertes d'application et de menace sont publiées si des menaces significatives sont détectées.
- **Liens** – Fournit des liens communs d'assistance pour vous aider à gérer votre appareil et pour accéder aux coordonnées de l'assistance.
- **Fichier de support technique** – Cliquez sur **Générer le fichier de support technique** pour générer un fichier système qui permet à l'équipe d'assistance de vous aider à résoudre les problèmes que vous êtes susceptibles de rencontrer avec le pare-feu. Une fois le fichier généré, cliquez sur **Download Tech Support File (Télécharger le fichier de support technique)**, puis envoyez le fichier au service de support Palo Alto Networks.

  Si votre navigateur est configuré pour ouvrir automatiquement les fichiers après le téléchargement, vous devriez désactiver cette option afin que le navigateur télécharge le fichier de support plutôt que d'essayer de l'ouvrir et de l'extraire.
- **Stats Dump File (Fichier de collecte des statistiques)** (pare-feu uniquement) – Cliquez sur **Generate Stats Dump File (Générer le fichier de collecte des statistiques)** pour générer un ensemble de rapports XML qui récapitulent le trafic réseau au cours des 7 derniers jours. Une fois que le rapport est généré, vous pouvez **Download Stats Dump File (Télécharger le fichier de vidage des statistiques)**. L'ingénieur système de Palo Alto Networks ou d'un partenaire homologué utilise ce rapport pour générer un résumé dans l'application Security Lifecycle Review (SLR). Le résumé de SLR met en évidence ce qui a été trouvé sur le réseau, ainsi que les risques opérationnels ou de sécurité associés pouvant être présents ; celui-ci est généralement utilisé dans le cadre du processus d'évaluation. Pour plus d'informations sur le résumé de l'application SLR, contactez votre ingénieur système de Palo Alto Networks ou d'un partenaire homologué.

  Pour les pare-feux gérés par un serveur d'administration Panorama™, vous pouvez générer un fichier de vidage de statistiques pour un seul pare-feu géré à la fois ou générer un seul fichier de vidage de statistiques pour tous les pare-feux gérés par Panorama.
- **Fichiers noyau (core)** – Si votre pare-feu connaît une défaillance du système fonctionnel, il générera un fichier noyau qui contient des détails sur le processus et la raison de son échec. Cliquez sur le lien **Download Core Files (Télécharger les fichiers noyau)** pour afficher une liste des fichiers noyaux

disponibles, puis cliquez sur le nom d’un fichier noyau pour le télécharger. Après avoir téléchargé le fichier, chargez-le dans un dossier d’assistance de Palo Alto Networks pour obtenir de l’aide sur ce problème.

Le contenu des fichiers noyaux peut uniquement être interprété par un ingénieur d’assistance de Palo Alto Networks.

- **Fichiers Pcap de débogage et de gestion** : si votre pare-feu rencontre un échec de capture de paquets, il génère un fichier de capture de paquets (pcap) contenant des détails sur le débogage et la gestion des raisons de son échec. Cliquez sur **Télécharger les fichiers** Pcap de débogage et de gestion pour afficher la liste des fichiers pcap disponibles, puis cliquez sur un nom de fichier pcap pour le télécharger. Après avoir téléchargé le fichier, chargez-le dans un dossier d’assistance de Palo Alto Networks pour obtenir de l’aide sur ce problème.

Périphérique > Clé principale et diagnostics

- **Périphérique** > **Clé principale et diagnostics**
- **Panorama** > **Clé principale et diagnostics**

Modifiez la clé principale qui chiffre tous les mots de passe et les clés privées sur le pare-feu ou Panorama (telle que la clé RSA pour l'authentification des administrateurs qui accèdent à la CLI). Le chiffrement des mots de passe et des clés améliore la sécurité en garantissant que leurs valeurs en clair n'apparaîtront pas sur le pare-feu ou sur Panorama.

La seule façon de restaurer la clé principale par défaut est de rétablir les réglages d'usine.

Palo Alto Networks vous recommande de configurer une nouvelle clé principale plutôt que d'utiliser la clé par défaut, de stocker la clé dans un endroit sûr et de la modifier régulièrement. Pour plus de sécurité, vous pouvez utiliser un module matériel de sécurité pour crypter la clé principale (voir Périphérique > Configuration > HSM). La configuration d'une clé principale unique sur chaque pare-feu ou sur chaque serveur de gestion Panorama garantit qu'un pirate qui découvre la clé principale d'un périphérique ne peut pas accéder aux mots de passe et aux clés privées d'un autre de vos appareils. Toutefois, vous devez utiliser la même clé principale pour plusieurs appareils dans les cas suivants :

- **Configurations de la Haute disponibilité (HD)** – Si vous déployez des pare-feu ou Panorama dans une configuration HD, utilisez la même clé principale pour les pare-feu ou les serveurs de gestion Panorama dans la paire. Dans le cas contraire, la synchronisation HD ne fonctionne pas.
- **Panorama managing WildFire appliances and Log Collectors (Panorama gérant les appareils WildFire et les collecteurs de journaux)** : vous devez configurer la même clé principale sur Panorama, les appareils WildFire et les collecteurs gérés. Dans le cas contraire, les opérations de transfert de Panorama échoueront.

Pour configurer une clé principale, modifiez les paramètres de la Clé principale et utilisez le tableau suivant pour déterminer quelles sont les valeurs appropriées :

Paramètres de clé principale et de diagnostics	Description
Clé principale	Activez la configuration d'une clé principale unique. Désactivez (décochez) l'utilisation de la clé principale par défaut.
Clé principale active	Indiquez la clé actuellement utilisée pour crypter toutes les clés privées et tous les mots de passe sur le pare-feu.
Nouvelle clé principale Confirmer la clé principale	Pour modifier la clé principale, saisissez une chaîne de 16 caractères et confirmez la nouvelle clé.

Paramètres de clé principale et de diagnostics	Description
Durée de vie	Indiquez le nombre de **Jours** et **Heures** au bout desquels la clé principale arrive à expiration. La valeur doit être comprise entre 1 et 438 000 jours (50 ans). Vous devez configurer une nouvelle clé principale avant que la clé actuelle n'expire. Si la clé principale expire, le pare-feu ou Panorama redémarre automatiquement en mode Maintenance. Vous devez alors procéder à une réinitialisation *Réglez la **Durée de vie** sur deux ans ou moins, en fonction du nombre de cryptages effectués par le périphérique. Plus un périphérique effectue de cryptages, plus la **Durée de vie** que vous devez définir est courte. L'essentiel est de ne pas être à court de cryptages uniques avant de changer la clé principale. Chaque clé principale peut fournir jusqu'à 2^^32 cryptages uniques et répétitions de cryptage, ce qui est un risque de sécurité.* *Définissez **Délai de rappel** pour la clé principale et lorsque la notification de rappel a lieu, modifiez la clé principale.*
Heure de rappel	Saisissez le nombre de **Jours** et **Heures** avant que la clé principale n'expire lorsque le pare-feu génère une alarme d'expiration. Le pare-feu ouvre automatiquement la boîte de dialogue Alarmes système pour afficher l'alarme.

Paramètres de clé principale et de diagnostics	Description
	*Réglez le rappel de manière à ce qu'il vous laisse suffisamment de temps pour configurer une nouvelle clé principale avant son expiration dans une fenêtre de maintenance programmée. Lorsque le **Time for Reminder (Délai de rappel)** expire et que le pare-feu ou Panorama envoie un journal de notification, changez la clé principale, n'attendez pas l'expiration de la **Lifetime (Durée de vie)**. Pour les périphériques groupés, suivez chaque dispositif (par exemple, les pare-feu que Panorama gère et les paires HA de pare-feu) et lorsque la valeur de rappel expire pour un dispositif quelconque du groupe, changez la clé principale.* *Pour s'assurer que l'alarme d'expiration s'affiche, sélectionnez **Périphérique** > **Paramètres du journal**, modifiez les paramètres d'alarme et cliquez sur **Activer les alarmes**.*
Stocké sur le module de sécurité matériel	Activez cette option uniquement si la clé principale est cryptée sur un Module de sécurité matériel (HSM). Vous ne pouvez pas utiliser de module de sécurité matériel sur une interface dynamique telle qu'un client DHCP ou PPPoE. La configuration du module de sécurité matériel (HSM) n'est pas synchronisée entre les pare-feu homologues en mode HD. Par conséquent, chaque homologue dans une paire HD peut se connecter à une source différente du module de sécurité matériel. Si vous utilisez Panorama et souhaitez synchroniser la configuration sur les deux homologues, utilisez des modèles Panorama pour configurer la source du module de sécurité matériel sur les pare-feu gérés. Le pare-feu PA-220 ne prend pas en charge HSM.
Renouvellement automatique de la clé principale	Permet le renouvellement automatique de la clé principale du nombre de jours et d'heure spécifiés. Désactivez (décochez) cette option pour autoriser l'expiration de la clé principale à la fin de sa durée de vie configurée. Procédez au **Renouvellement automatique de la clé principale** en indiquant le nombre de **Jours** et **Heures** desquels prolonger le chiffrement de la clé principale (plage de 1 heure à 730 jours).

Paramètres de clé principale et de diagnostics	Description
	*Si vous activez la fonction **Renouvellement automatique de la clé principale**, réglez-la de manière à ce que la durée totale (durée de vie plus durée de renouvellement automatique) n'entraîne pas l'épuisement des cryptages uniques du périphérique. Par exemple, si vous pensez que le périphérique consommera le nombre de cryptages uniques de la clé principale dans deux ans et demi, vous pouvez fixer la **Lifetime (Durée de vie)** à deux ans, fixer le **Time for Reminder (Délai de rappel)** à 60 jours et fixer le **Auto Renew Master Key (Renouvellement automatique de la clé principale)** à 60-90 jours pour disposer du temps supplémentaire nécessaire pour configurer une nouvelle clé principale avant l'expiration de la **Lifetime (Durée de vie)**. Toutefois, la meilleure pratique consiste toujours à changer la clé principale avant l'expiration de la durée de vie pour s'assurer qu'aucun périphérique ne répète les cryptages.*
Critères communs	En mode Critères Communs, d'autres options sont disponibles et vous permettent d'exécuter un auto-test d'algorithme cryptographique et un auto-test d'intégrité logicielle. Un calendrier est également inclus pour définir les heures auxquelles les deux auto-tests seront exécutés.

Déployer la clé principale

Déployez une clé principale ou mettez à jour une clé principale existante d’un pare-feu géré, d’un collecteur de journaux ou d’un appareil WF-500 directement à partir de Panorama.

Champ	Description
Déployer la clé principale	
Filtre	Filtrez les appareils gérés qui doivent s’afficher selon la plateforme, les groupes de périphériques, les modèles, les étiquettes, l’état HA ou la version du logiciel.
Nom du périphérique	Nom du pare-feu géré.
Version du logiciel	La version du logiciel qui s’exécute sur le périphérique géré.
État	L’état de la connexion du périphérique géré peut être `Connecté`, `Déconnecté` ou `inconnu`.

Champ	Description
État du déploiement de la clé principale	
Nom du périphérique	Nom du pare-feu géré.
État	État du déploiement de la clé principale.
Résultat	Résultats du déploiement de la clé principale. Les résultats peuvent être `Oui` ou `Echec`.
Progression	Progression (%) du déploiement de la clé principale.
Détails	Détails du déploiement de la clé principale. Si le déploiement échoue, les raisons de l'échec s'affichent ici.
Résumé	
Progression	Affiche une barre de progression qui présente la progression du déploiement de la clé principale. Les informations suivantes s'affichent : • **Résultats atteints** : Nombre de périphériques sur lesquels la clé principale a été déployée avec succès. • **Résultats en attente** : Nombre de périphériques sur lesquels le déploiement de la clé principale est en attente. • **Résultats échoués** : Nombre de périphériques sur lesquels le déploiement de la clé principale a échoué.

Appareil > Recommandation de politique > IoT

Affichez des informations sur les recommandations de règles de stratégie de IoT Security. IoT Security utilise les métadonnées que le pare-feu collecte à partir du trafic sur votre réseau pour déterminer le comportement à autoriser pour les appareils, puis génère des recommandations pour les règles de stratégie de sécurité à appliquer.

Bouton/Champs	Description
Détails de l'importation de la politique	Affichez les informations détaillées sur la recommandation de règle, comme le **Lieu** du groupe de périphériques, le **nom de la règle**, le **utilisateur** qui a importé la politique, si la recommandation de règle de politique **est à jour**, quand la recommandation de règle de politique a été importée et quand la recommandation de règle de politique a été mise à jour pour la dernière fois.
Importé dans	Pour les pare-feu de nouvelle génération, cela montre le système virtuel dans lequel une recommandation de règle de stratégie a été importée. Pour Panorama, cela montre les groupes d'appareils dans lesquels une recommandation de règle de stratégie a été importée.
Nom de la règle de stratégie	Nom d'une règle de stratégie, qui est par défaut une concaténation du nom du jeu de stratégies IoT Security et du nom de l'application.
Groupe d'appareils suggéré	Groupe d'appareils qu'IoT Security a suggéré pour une règle de stratégie après avoir pris connaissance des zones et des groupes d'appareils dans les journaux qu'il a reçus des pare-feu de nouvelle génération.
Profil du périphérique source	Profil d'appareil à partir duquel la recommandation de règle de stratégie autorise le trafic.
Source Zones (Zones source)	Zones sources à partir desquelles la recommandation de règle de stratégie autorise le trafic. Les zones sources peuvent être ajoutées manuellement dans IoT Security.
Utilisateur source	Importez les zones source pour la recommandation de règle de politique. Celui-ci est inutilisé et toujours vide.

Bouton/Champs	Description
Périphérique source	Le périphérique source pour la recommandation de règle de politique. Celui-ci est inutilisé et toujours vide.
Adresse source	Importez l'adresse source pour la recommandation de règle de politique. Celui-ci est inutilisé et toujours vide.
Profil du périphérique de destination	Profils d'appareil de destination auxquels la recommandation de règle de stratégie autorise le trafic.
IP du périphérique de destination	Adresse IP des appareils vers lesquels la recommandation de règle de stratégie autorise le trafic.
Nom de domaine complet de destination	Noms de domaine complets (FQDN) auxquels la recommandation de règle de stratégie autorise le trafic.
Destination Zones (Zones de destination)	Zones de destination vers lesquelles la recommandation de règle de stratégie autorise le trafic. Les zones de destination peuvent être ajoutées manuellement dans IoT Security.
Profils de sécurité de destination	Profils de sécurité autorisés par la recommandation de règle de stratégie.
Destination Services	Les services (par exemple, `ssl`) que la recommandation de règle de politique autorise.
Catégorie d'URL de destination	Les catégories de URL Filtering vers lesquelles la recommandation de règle de politique autorise le trafic.
Applications de la destination	Les applications que la recommandation de règle de politique autorise.
Balises de destination	Balises qui identifient la règle de stratégie pour la recommandation de règle de stratégie. *Ne modifiez pas les balises de la règle de stratégie ; si vous modifiez les balises, le pare-feu ne peut pas reconstruire les mappages de stratégie.*

Bouton/Champs	Description
Description	Description de Sécurité IoT pour l'ensemble de stratégies auquel appartient une règle.
Périphérique interne	Identifie si le périphérique vient d'une zone qui est interne à votre réseau (`Oui`) ou d'une zone faisant face à un internet externe (`Non`).
Action	Identifie l'action pour cette recommandation de règle de politique qui est toujours `allow (autoriser)`).
Nouvelles mises à jour disponibles	`Yes (Oui)` indique qu'une mise à jour d'une recommandation de règle de stratégie est disponible pour une règle correspondante dans la base de règles. (Panorama) L'importation de règles de stratégie à partir de Panorama remplace les recommandations de règles actuelles et leurs règles correspondantes, précédemment importées, dans la base de règles. Après cela, le champ Nouvelle mise à jour disponible n'indique plus qu'une mise à jour est en attente et passe de`Yes (oui)` à `No (Non)`. Si vous avez plusieurs groupes d'appareils, la valeur reste `Yes (Oui)` jusqu'à ce que vous importiez des règles de stratégie dans chacun d'eux. (PAN-OS UI (interface utilisateur PAN-OS)) Notez les détails de toutes les recommandations de règles de politique avec `Yes (Oui)` dans la colonne Nouvelles mises à jour disponibles, puis modifiez et enregistrez la règle de stratégie importée correspondante sur la page **Policies (Politiques)** pour qu'elle corresponde à la recommandation de règle de stratégie mise à jour. Ensuite **Sync Policy Rules (synchronisez les règles de politique)** pour actualiser le mappage entre les règles modifiées et les recommandations de règles. La valeur de la colonne Nouvelles mises à jour disponibles passe ensuite de `Yes (Oui)` à `No (Non)`.
Afficher uniquement ce pare-feu	IoT Security transmet automatiquement les règles de tous les ensembles de stratégies activés à Panorama et à tous les pare-feu de nouvelle génération. Par conséquent, un pare-feu peut avoir des règles qui ne s'appliquent pas à lui. Pour afficher uniquement les règles qui s'appliquent au pare-feu local, **affichez uniquement ce pare-feu**.

Bouton/Champs	Description
Importer la ou les règles de stratégie	Une fois que Sécurité IoT a envoyé les recommandations de règles de stratégie à Panorama ou aux pare-feu et qu'elles se trouvent dans la base de données des recommandations de stratégie, vous pouvez sélectionner une ou plusieurs (jusqu'à dix) que vous souhaitez importer dans la base de règles de stratégie, puis cliquer sur **Import Policy Rule (Importer une règle de politique)**. Dans la boîte de dialogue Importer une règle de stratégie qui s'affiche, choisissez le nom d'une règle de stratégie dans la base de règles après laquelle importer les règles de stratégie sélectionnées ou laissez-la vide pour importer les règles sélectionnées en haut. Si une recommandation de règle de stratégie est importée dans la base de règles, puis modifiée ultérieurement dans IoT Security, vous pouvez utiliser Panorama pour la réimporter. Étant donné que l'interface utilisateur PAN-OS ne vous permet pas de réimporter des règles, vous pouvez utiliser Panorama ou modifier la règle dans la base de règles PAN-OS pour qu'elle corresponde à la recommandation modifiée, puis **Sync Policy Rules (synchroniser les règles de politique)**.
Supprimer le mappage de politique	Si vous n'avez plus besoin d'une ou de plusieurs recommandations de règles de stratégie, vous pouvez sélectionner jusqu'à dix recommandations à la fois, puis **Remove Policy Mapping (supprimer le mappage de politique)** correspondante. *Vous pouvez ensuite supprimer manuellement les règles correspondantes de la base de règles.*
Synchronisation des règles de politique	Si les mappages ne sont plus synchronisés (par exemple, si vous restaurez une configuration précédente), vous pouvez **Sync Policy Rules (synchroniser les règles de politique)** pour restaurer le mappage entre les règles de politique dans la base de règles et les recommandations de règles de politique.

Périphérique > Politique > Recommandation SaaS

Affichez des informations sur les recommandations de règles de politique de Prisma SaaS et importez les stratégies dans le pare-feu.

Champ	Description
Utilisateur source	Administrateur qui a envoyé la recommandation de règle de politique au pare-feu.
Périphérique source	Le périphérique source pour la recommandation de règle de politique.
Emplacement	Le groupe de périphériques sur Panorama où la recommandation de règle de politique est disponible.
Profils de sécurité	Le profil de sécurité que la recommandation de règle de politique autorise.
Applications	Applications ou groupes d'applications que la recommandation de règles de politique autorise. Cliquez sur les noms des groupes d'applications pour afficher les applications individuelles de ce groupe.
Étiquettes	Les étiquettes qui identifient la règle de politique pour la recommandation de règle de politique. *Ne modifiez pas les étiquettes de la règle de politique ; si vous modifiez les étiquettes, le pare-feu ne peut pas reconstruire le mappage de la politique.*
Description	Description que l'administrateur SaaS Prisma donne à la recommandation de règle de politique.
Recommandation active	Détermine si cette recommandation de règle de politique est • `active (actif)`— Actuellement utilisé dans la stratégie de politique SaaS de Prisma. • `removed (supprimée)`— Supprimé de la politique par l'administrateur SaaS Prisma. L'administrateur du pare-feu ne peut plus importer la règle de stratégie et doit **Remove Policy Mapping (supprimer le mappage de**

Champ	Description
	politique) du pare-feu, puis supprimer la règle de politique de sécurité de la base de règles du pare-feu. Ne laissez pas les règles supprimées dans la base de règles du pare-feu.
Action	Identifie l'action pour cette recommandation de règle de politique, `allow (autoriser)` ou `deny (refuser)`.
Nouvelle mise à jour disponible	Identifie qu'il existe une nouvelle mise à jour pour la recommandation de règle de politique. Vérifiez la colonne **Applications** pour les modifications apportées à l'application. Si vous êtes d'accord avec les modifications, sélectionnez la règle et **Import Policy Rule (Importer la règle de politique)** pour mettre à jour la politiqueque vous devez importer à partir de Prisma SaaS. Lorsque vous importez la mise à jour de recommandation de règle de politique, le pare-feu met à jour dynamiquement la règle de politique de sécurité et ses objets associés.
Importer la règle de politique	Importe les recommandations de règles de politique sélectionnées à partir de Prisma SaaS.
Supprimer le mappage de politique	Si vous n'avez plus besoin de la recommandation de règle de politique pour un périphérique, vous pouvez **supprimer le mappage de la politique** pour celui-ci. *Vous devez également supprimer la règle de stratégie correspondant à la recommandation de règle de stratégie.*
Synchronisation des règles de politique	Si l'administrateur SaaS supprime une recommandation de politique et que vous **Remove Policy Mappings (supprimez les mappages)** de politique pour elle et supprimez la règle de politique de sécurité, la règle supprimée peut rester dans la liste des recommandations de règles si les informations ne sont pas synchronisées. **Sync Policy Rules (Synchronisez les règles de politique)** pour les synchroniser.

Identification utilisateur

L’identification d’utilisateurs (User-ID™) est une fonctionnalité des pare-feu de nouvelle génération Palo Alto Networks® qui s’intègre harmonieusement avec une gamme d’offres de services d’annuaires d’entreprise et de terminaux afin d’associer des activités et des politiques de sécurité à des noms d’utilisateur et à des, et non seulement à des adresses IP. La configuration de la fonction User-ID permet au Centre de commande de l’application (ACC), à App-Scope, aux rapports et aux journaux d’inclure les noms d’utilisateur en plus des adresses IP d’utilisateur.

- Périphérique > Identification utilisateur > Mappage d'utilisateur
- Périphérique > Identification utilisateur > Sécurité de la connexion
- Périphérique > Identification utilisateur > Agents de Terminal Server
- Périphérique > Identification utilisateur > Paramètres de mappage de groupe
- Identification de l’appareil > de l’utilisateur > adresse source approuvée
- Périphérique > Identification utilisateur > Paramètres du portail d’authentification
- Device > User Identification > Cloud Identity Engine (Périphérique > Identification de l’utilisateur > Moteur d’identification du cloud

Vous souhaitez en savoir plus ?

Voir User-ID

Périphérique > Identification utilisateur > Mappage d'utilisateur

Configurez l’agent User-ID intégré à PAN-OS exécuté sur le pare-feu pour Associer les adresses IP vers des noms d’utilisateur.

Que voulez-vous faire ?	Reportez-vous à la section :
Configurer l’agent User-ID intégré à PAN-OS.	Configuration de l'agent User-ID Palo Alto Networks
Gérer l’accès aux serveurs que l’agent User-ID surveille pour extraire les informations d’association d’utilisateur.	Surveillance des serveurs
Gérer les sous-réseaux que le pare-feu inclut ou exclut lors de l’association des adresses IP aux noms d’utilisateurs.	Inclure ou exclure des sous-réseaux pour l’association d’utilisateur
Vous souhaitez en savoir plus ?	Configuration du Mappage d’utilisateur à l’aide de l’Agent User-ID intégré à PAN-OS

Configuration de l'agent User-ID Palo Alto Networks

Ces paramètres définissent les méthodes que l’agent User-ID utilise pour effectuer le mappage d’utilisateur.

Que voulez-vous faire ?	Reportez-vous à la section :
Permettre à l’agent User-ID d’utiliser Windows Management Instrumentation (WMI, Infrastructure de gestion Windows) pour sonder les systèmes clients ou Windows Remote Management (WinRM) sur HTTP ou HTTPS pour surveiller les serveurs afin d’extraire les informations d’association d’utilisateur.	Compte de surveillance du serveur

Que voulez-vous faire ?	Reportez-vous à la section :
Surveiller les journaux des serveurs pour y déceler les informations de mappage d'utilisateur à l'aide de l'agent User-ID.	Surveillance du serveur
Autoriser l'agent User-ID à sonder les systèmes client pour extraire les informations de mappage d'utilisateur.	Sondage du client
Veiller à ce que le pare-feu dispose des informations de mappage d'utilisateur les plus récentes lorsque les utilisateurs naviguent sur Internet et obtiennent de nouvelles adresses IP.	Cache
Configurer l'agent User-ID pour qu'il puisse analyser syntaxiquement les messages Syslog pour extraire les informations de mappage d'utilisateur.	Filtres Syslog
Configurer l'agent User-ID pour qu'il omette des noms d'utilisateur donnés du processus de mappage.	Liste des utilisateurs ignorés

Compte de surveillance du serveur

- **Périphérique** > **Identification utilisateur** > **Mappage d'utilisateur** > **Configuration de l'agent User-ID Palo Alto Networks** > **Compte de surveillance du serveur**

Pour configurer l'agent User-ID intégré à PAN-OS pour qu'il puisse utiliser l'Instrumentation de gestion Windows (WMI) pour sonder les systèmes clients ou Windows Remote Management (WinRM) sur HTTP ou HTTPS pour surveiller les serveurs afin d'extraire les informations de mappage d'utilisateur, remplissez les champs suivants.

Vous pouvez également Configuration de l'accès aux serveurs surveillés en configurant un serveur Kerberos pour l'authentification de la surveillance du serveur au moyen de Windows Remote Management (WinRM) sur HTTP ou HTTPS.

Étant donné que le sondage WMI se fie à des données renvoyées depuis un terminal, Palo Alto Network ne vous recommande pas d'utiliser cette méthode pour obtenir des informations de mappage User-ID dans un réseau haute sécurité. Si vous configurez l'agent User-ID pour obtenir des informations de mappage en analysant les journaux d'événements de sécurité Active Directory (AD) ou les messages syslog, ou en utilisant l'API XML, Palo Alto Networks vous recommande de désactiver le sondage WMI.

Si vous utilisez le sondage WMI, ne l'activez pas sur des interfaces externes et non fiables. En effet, cela provoque l'envoi des sondes WMI contenant des informations sensibles par l'agent en dehors de votre réseau, par exemple le nom d'utilisateur, le nom de domaine et le hachage du mot de passe du compte de service de l'agent User-ID. Un pirate pourrait potentiellement exploiter ces informations pour pénétrer et accéder à votre réseau.

Paramètres d'authentification de Active Directory	Description
Nom d'utilisateur	Saisissez les informations d'identification de domaine (**User Name (Nom d'utilisateur)** et **Password (Mot de passe)**) du compte utilisé par le pare-feu pour accéder aux ressources Windows. Le compte doit être autorisé à effectuer des requêtes WMI sur les ordinateurs client et à surveiller les serveurs Microsoft Exchange et les contrôleurs de domaine. Utilisez la syntaxe domaine\nom d'utilisateur pour définir **User Name (Nom d'utilisateur)**. Si vous Configuration de l'accès aux serveurs surveillés en utilisant Kerberos pour authentifier le serveur, entrez le User Principal Name (nom principal de l'utilisateur ; UPN) Kerberos.
Nom DNS du domaine	Saisissez le nom DNS du serveur faisant l'objet de la surveillance. Si vous Configuration de l'accès aux serveurs surveillés en utilisant Kerberos pour authentifier le serveur, entrez le domaine de la partition Kerberos. Vous devez configurer ce paramètre si vous utilisez **WinRM-HTTP** en tant que protocole de transport lorsque vousConfiguration de l'accès aux serveurs surveillés.
Mot de passe/Confirmer le mot de passe	Saisissez et confirmez le mot de passe du compte utilisé par le pare-feu pour accéder aux ressources Windows.
Profil du serveur Kerberos	Sélectionnez le profil du serveur Kerberos qui contrôle l'accès à la partition pour extraire les journaux de sécurité et les informations de sessions du serveur faisant l'objet de la surveillance au moyen de WinRM sur HTTP ou HTTPS.

La procédure complète pour configurer l'agent User-ID intégré à PAN-OS pour qu'il puisse surveiller les serveurs et sonder les clients exige l'accomplissement de tâches supplémentaires en plus de la définition des paramètres d'authentification Active Directory.

Surveillance du serveur

- **Périphérique** > **Identification utilisateur** > **Mappage d'utilisateur** > **Configuration de l'agent User-ID Palo Alto Networks** > **Moniteur de serveur**

Pour permettre à l'agent User-ID d'associer les adresses IP aux noms d'utilisateur en recherchant des événements de connexion dans les journaux d'événements de sécurité des serveurs, configurez les paramètres décrits dans le tableau suivant.

Si la charge de la requête est élevée pour les journaux des serveurs Windows, les sessions du serveur Windows, ou les serveurs eDirectory, le retard observé entre les requêtes pourrait considérablement dépasser la fréquence ou l'intervalle spécifié.

La procédure complète pour configurer l'agent User-ID intégré à PAN-OS pour qu'il puisse surveiller les serveurs exige l'accomplissement de tâches supplémentaires en plus de la configuration des paramètres de surveillance du serveur.

Paramètres de surveillance du serveur	Description
Activer le journal de sécurité	Sélectionnez cette option pour activer la surveillance des journaux de sécurité sur les serveurs Windows.
Fréquence de surveillance du journal du serveur (en secondes)	Indiquez la fréquence, en secondes, à laquelle le pare-feu interroge les journaux de sécurité du serveur Windows pour extraire les informations de mappage d'utilisateur (intervalle compris entre 1 et 3 600 ; valeur par défaut : 2). Il s'agit de l'intervalle entre le moment où le pare-feu termine le traitement de la dernière requête et où le pare-feu envoi la requête suivante. *Si la surveillance des journaux ne se produit pas assez souvent, le dernier mappage adresse IP/utilisateur pourrait ne pas être disponible. Une surveillance trop fréquente des journaux par le pare-feu pourrait avoir une incidence sur le contrôleur de domaine, sur la mémoire, sur le processeur et sur l'application de la politique User-ID. Commencez par une valeur se situant entre 2 et 30 secondes, puis revoyez la valeur en fonction de l'incidence sur le rendement ou de la fréquence des mises à jour des mappages d'utilisateur.*
Activer la session	Sélectionnez cette option pour activer la surveillance des sessions d'utilisateur sur les serveurs surveillés. Chaque fois qu'un utilisateur se connecte à un serveur, une session est créée ; le pare-feu peut utiliser ces informations pour identifier l'adresse IP de l'utilisateur.

Paramètres de surveillance du serveur	Description
	*Vous ne devez pas **Activer la session**. Ce paramètre nécessite que l'agent User-ID possède un compte Active Directory avec des privilèges d'Opérateur de serveur afin de pouvoir lire toutes les sessions utilisateur. Au lieu de cela, vous devez utiliser une intégration Syslog ou API XML pour surveiller les sources qui recueillent les événements de connexion et de déconnexion pour tous les types de périphériques et de systèmes d'exploitation (plutôt qu'uniquement les systèmes d'exploitation Windows), tels que les contrôleurs sans fil et les NAC.*
Fréquence de lecture de la session serveur (en secondes)	Indiquez la fréquence, en secondes, à laquelle le pare-feu interroge les sessions d'utilisateurs Windows pour extraire les informations de mappage d'utilisateur (intervalle compris entre 1 et 3 600 ; valeur par défaut : 10). Il s'agit de l'intervalle entre le moment où le pare-feu termine le traitement de la dernière requête et commence celui de la suivante.
Intervalle de requête de Novell eDirectory (en secondes)	Indiquez la fréquence, en secondes, à laquelle le pare-feu interroge les serveurs eDirectory Novell pour extraire les informations de mappage d'utilisateur (intervalle compris entre 1 et 3 600 ; valeur par : 30). Il s'agit de l'intervalle entre le moment où le pare-feu termine le traitement de la dernière requête et commence celui de la suivante.
Profil de service Syslog	Sélectionnez un profil de service SSL/TLS indiquant le certificat et les versions SSL/TLS autorisées pour les communications entre le pare-feu et des expéditeurs Syslog surveillés par l'agent User-ID. Pour plus de détails, voir Périphérique > Gestion des certificats > Profil de service SSL / TLS et Filtres Syslog. Si vous sélectionnez **none (aucun)**, le pare-feu utilisera son certificat prédéfini et autosigné.

Sondage du client

- **Périphérique** > **Identification utilisateur** > **Mappage d'utilisateur** > **Configuration de l'agent User-ID Palo Alto Networks** > **Sondage du client**

N'activez pas le sondage client sur des réseaux de haute sécurité ou sur des interfaces externes non fiables, car il peut poser des risques de sécurité s'il n'est pas correctement configuré. Si vous activez la sonde client sur une zone externe non approuvée, cela pourrait permettre à un attaquant d'envoyer une sonde en dehors de votre réseau, ce qui pourrait entraîner la divulgation du nom du compte de service de l'agent User-ID, du nom de domaine et du hachage du mot de passe crypté.

Au lieu de cela, Palo Alto Network vous recommande fortement de collecter des informations de mappage utilisateur à partir de sources isolées et fiables, telles que des contrôleurs de domaine ou des intégrations avec Syslog ou XML API (API XML), pour capturer en toute sécurité les informations de mappage utilisateur à partir de tout type d'appareil ou système d'exploitation.

Vous pouvez configurer l'agent d'ID utilisateur intégré PAN-OS pour effectuer une client probing analyse client WMI (Windows Management Instrumentation) pour chaque système client identifié par le processus de mappage utilisateur. L'agent User-ID sondera régulièrement chaque adresse IP reconnue pour vérifier que le même utilisateur est toujours connecté. Lorsque le pare-feu rencontre une adresse IP pour laquelle il ne dispose pas de mappage d'utilisateur, il envoie l'adresse à l'agent pour sondage immédiat. Pour configurer les paramètres du sondage du client, remplissez les champs suivants. La complete procedure (procédure complète) pour configurer l'agent User-ID intégré à PAN-OS pour qu'il puisse sonder les clients exige l'accomplissement de tâches supplémentaires en plus de la configuration des paramètres du sondage du client.

Paramètres de Sondage du client	Description
Activer le sondage	Sélectionnez cette option pour activer l'interrogation WMI.
Intervalle de sondage (min)	Saisissez l'intervalle de sondage en minutes (plage de 1 à 1 440, par défaut 20). Il s'agit de l'intervalle entre le moment où le pare-feu termine le traitement de la dernière demande et commence celui de la prochaine demande. Dans les déploiements massifs, il est important de définir un intervalle approprié permettant le sondage de chaque client qui a été identifié par le processus de mappage d'utilisateur. Par exemple, si vous disposez de 6000 utilisateurs et d'un intervalle de 10 minutes, 10 requêtes WMI par seconde sont nécessaires pour chaque client. *Si la charge de la requête de sondage est élevée, le retard observé entre les requêtes pourrait considérablement dépasser l'intervalle que vous aurez indiqué.*

Cache

- **Périphérique** > **Identification utilisateur** > **Mappage d'utilisateur** > **Configuration de l'agent User-ID Palo Alto Networks** > **Cache**

Pour veiller à ce que le pare-feu dispose des informations d'association d'utilisateur les plus récentes lorsque les utilisateurs naviguent sur Internet et obtiennent de nouvelles adresses IP, configurez les délais de suppression des associations d'utilisateurs de la mémoire cache du pare-feu. Ce délai d'expiration s'applique aux associations d'utilisateurs découverts grâce à toute méthode, à l'exception du Portail d'authentification. Pour les associations découvertes au moyen du Portail d'authentification, définissez le délai d'expiration dans les Paramètres du portail d'authentification (Périphérique > Identification de l'utilisateur > Paramètres du portail d'authentification, champs **Timer (Minuteur)** et **Idle Timer (Minuterie d'inactivité)**).

Pour mettre en correspondance les noms d'utilisateurs recueillis des sources User-ID même si aucune domaine n'est inclus, configurez le pare-feu pour permettre la mise en correspondance des noms d'utilisateurs sans domaines. Vous ne devriez utiliser cette option que si les noms d'utilisateur de votre organisation ne sont pas dupliqués entre les domaines.

Paramètres du cache	Description
Activer le délai d'identification utilisateur	Sélectionnez cette option pour activer une valeur de délai de saisie du mappage d'utilisateur. Quand la valeur de délai de saisie est atteinte, le pare-feu la supprime et extrait un nouveau mappage. Cela permet de s'assurer que le pare-feu dispose des informations les plus récentes lorsque les utilisateurs naviguent sur Internet et obtiennent de nouvelles adresses IP. *Activez le délai pour s'assurer que le pare-feu dispose des plus récentes informations de mappage utilisateur/adresse IP.*
Délai d'identification utilisateur (en minutes)	Définissez la valeur du délai d'expiration en minutes des entrées d'association d'utilisateur (plage de 1 à 3 600 ; valeur par défaut : 45). *Définissez la valeur du délai à la demi-vie du bail DHCP ou à la durée de vie du ticket Kerberos.* *Si vous configurez des pare-feu pour redistribuer les informations d'association, chaque pare-feu efface les entrées d'association qu'il reçoit en fonction du délai d'expiration que vous avez défini sur ce pare-feu et non sur les délais d'expiration définis dans les pare-feu de transfert.*
Autoriser la mise en correspondance des noms d'utilisateurs sans domaines	Sélectionnez cette option pour autoriser le pare-feu à mettre les utilisateurs en correspondance si le domaine n'est pas fourni par la source User-ID. Pour prévenir la mauvaise identification des utilisateurs, ne sélectionnez cette option que si vos noms d'utilisateur ne sont pas dupliqués entre les domaines.

Paramètres du cache	Description
	Avant d'activer cette option, vérifiez que le pare-feu a récupéré les mappages de groupe auprès du serveur LDAP.

Filtres Syslog

- **Périphérique** > **Identification utilisateur** > **Mappage d'utilisateur** > **Configuration de l'agent User-ID Palo Alto Networks** > **Filtres Syslog**

L'agent User-ID utilise les profils d'analyse syntaxique Syslog pour filtrer les messages Syslog envoyés par les expéditeurs Syslog que l'agent surveille pour extraire les informations de mappage nom d'utilisateur/adresse IP (voir Configuration de l'accès aux serveurs surveillés). Chaque profil peut analyser les messages Syslog pour l'un des types d'événements suivants, mais pas les deux :

- Événements d'authentification (connexion) - Utilisés pour ajouter des mappages d'utilisateur au pare-feu.
- Événements de déconnexion - Utilisés pour supprimer les mappages d'utilisateurs qui ne sont plus d'actualité. La suppression de mappages obsolètes est utile dans les environnements où les affectations d'adresses IP changent souvent.

Palo Alto Networks fournit au pare-feu des profils d'analyse syntaxique Syslog prédéfinis par l'intermédiaire de Mise à jour de contenu des applications. Pour mettre à jour dynamiquement la liste des profils à mesure que les fournisseurs développent de nouveaux filtres, planifiez ces mises à jour de contenu dynamiques (voir Périphérique> Mises à jour dynamiques). Les profils prédéfinis sont globaux pour le pare-feu, tandis que les profils personnalisés que vous configurez s'appliquent uniquement au système virtuel (**Location (Emplacement)**) sélectionné sous **Device (Périphérique)** > **User Identification (Identification de l'utilisateur)** > **User Mapping (Mapping utilisateur)**.

Les messages Syslog doivent respecter les critères suivants pour qu'un agent User-ID les analyse :

- Chaque message doit être une chaîne de texte sur une seule ligne. Une nouvelle ligne (\n) ou un retour à la ligne et une nouvelle ligne (\r\n) sont les délimiteurs de sauts de ligne.
- La taille maximum pour les messages individuels est de 8 000 octets.
- Les messages envoyés via UDP doivent être contenus dans un seul paquet ; les messages envoyés via SSL peuvent couvrir plusieurs paquets. Un seul paquet peut contenir plusieurs messages.

Pour configurer un profil personnalisé, cliquez sur **Add (Ajouter)** et renseignez les paramètres décrits dans le tableau suivant. Les descriptions de champs dans ce tableau utilisent un exemple d'événement de connexion depuis un message Syslog avec le format suivant :

```
[Mar Jul 5 13:15:04 2005 CDT] Succès de l'authentification de
 l'administrateur Utilisateur:domaine\johndoe_4 Source:192.168.0.212
```

La procédure complète de configuration de l'agent User-ID pour analyser un expéditeur Syslog pour les informations de mappage d'utilisateur nécessite des tâches supplémentaires en plus de la création d'un profil d'analyse syntaxique Syslog.

Champ	Description
Profil d'analyse syntaxique Syslog	Donnez un nom au profil HIP (63 caractères alpha-numériques maximum).
Description	Saisissez une description du profil (255 caractères alpha-numériques maximum).
Type	Définissez le type d'analyse syntaxique du filtrage des informations de mappage d'utilisateur : • **Regex Identifier (Identifiant d'expression régulière)** – Utilisez **Event Regex (Expression régulière d'événements)**, **Username Regex (Expression régulière de nom d'utilisateur)**, et **Address Regex (Expression régulière d'adresse)** pour préciser les expressions régulières (regex) qui décrivent les modèles de recherche utilisés pour identifier et extraire les informations de mappage d'utilisateur des messages Syslog. Le pare-feu utilisera la Regex pour faire correspondre les événements d'authentification ou de déconnexion dans les messages Syslog, ainsi que les noms d'utilisateur et les adresses IP dans les messages correspondants. • **Field Identifier (Identificateur de champ)** – Utilisez les champs **Event String (Chaîne d'événements)**, **Username Prefix (Préfixe du nom d'utilisateur)**, **Username Delimiter (Séparateur de nom d'utilisateur)**, **Address Prefix (Préfixe d'adresse)**, **Address Delimiter (Séparateur d'adresse)** et **Adresses Per Log (Adresses par journal)** pour définir les chaînes à mettre en correspondance avec l'événement d'authentification ou de déconnexion et pour identifier les informations de mappage d'utilisateur dans les messages Syslog. Les champs restants dans la boîte de dialogue varient en fonction de votre sélection. Configurez les champs comme décrit dans les lignes suivantes.
Expression régulière d'événements	Renseignez l'expression régulière qui permet d'identifier les événements d'authentification ou de déconnexion réussis. Pour le message d'exemple utilisé avec ce tableau, l'expression régulière **`(authentication\ success) {1}`** extrait la première **`{1}`**instance de la chaîne `authentication success`. La barre oblique inversée avant l'espace est un caractère d'échappement Regex standard qui indique au moteur Regex de ne pas traiter l'espace comme caractère spécial.
Expression régulière de nom d'utilisateur	Renseignez l'expression régulière pour identifier le champ de nom d'utilisateur dans les messages d'authentification ou de déconnexion réussis. Pour le message d'exemple utilisé avec ce tableau, la Regex **`User:([a-zA-Z0-9\\\._]+)`** correspond à

Champ	Description
	la chaîne `User:johndoe_4` et extrait acme\johndoe1 comme nom d'utilisateur.
Expression régulière d'adresse	Renseignez l'expression régulière qui permet d'identifier la partie de l'adresse IP dans les messages d'authentification réussis ou de déconnexion. Dans le message d'exemple utilisé avec ce tableau, l'expression régulière **`Source:([0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3})`** correspond à l'adresse IPv4 `Source:192.168.0.212` et ajoute 192.168.0.212 en tant qu'adresse IP dans le mappage nom d'utilisateur.
Chaîne d'événements	Saisissez une chaîne correspondante pour identifier les messages de déconnexion ou de réussite de l'authentification. Pour le message d'exemple utilisé avec ce tableau, vous devez saisir la chaîne **`authentication success`**.
Préfixe du nom d'utilisateur	Saisissez la chaîne correspondante pour identifier le début du champ Nom d'utilisateur dans les messages d'authentification ou de déconnexion Syslog. Le champ ne prend pas en charge les expressions régulières telles que **`\s`** (pour un espace) ou **`\t`** (pour un onglet). Dans le message d'exemple utilisé avec ce tableau, `Utilisateur :` identifie le début du champ de nom d'utilisateur.
Séparateur de nom d'utilisateur	Saisissez le délimiteur pour marquer la fin du champ Nom d'utilisateur dans un message d'authentification ou de déconnexion. Utilisez \s pour indiquer un espace autonome (comme dans le message d'exemple) et \t pour indiquer un onglet.
Préfixe d'adresse	Saisissez la chaîne correspondante pour identifier le début du champ Adresse IP dans les messages Syslog. Le champ ne prend pas en charge les expressions régulières telles que **`\s`** (pour un espace) ou **`\t`** (pour un onglet). Dans le message d'exemple utilisé avec ce tableau, `Source :` identifie le début du champ de l'adresse.
Séparateur d'adresse	Saisissez la chaîne correspondante qui marque la fin du champ Adresse IP dans les messages de réussite d'authentification ou de déconnexion. Par exemple, saisissez **`\n`** pour indiquer que le délimiteur est un saut de ligne.
Adresses par journal	Saisissez le nombre maximum d'adresses IP que le pare-feu doit analyser (valeur par défaut : 1; plage comprise entre 1 et 3).

Liste des utilisateurs ignorés

- **Périphérique** > **Identification utilisateur** > **Mappage d'utilisateur** > **Configuration de l'agent User-ID Palo Alto Networks** > **Liste des utilisateurs ignorés**

La liste des utilisateurs ignorés définit les comptes utilisateur pour lesquels le mappage nom d'utilisateur / adresse IP n'est pas requis (par exemple, les comptes de kiosques). Pour configurer la liste, cliquez sur **Add (Ajouter)** et saisissez un nom d'utilisateur. Vous pouvez utiliser un astérisque comme caractère générique permettant la correspondance de plusieurs noms d'utilisateur. Il ne peut toutefois être placé qu'à la toute fin de l'entrée. Par exemple, **corpdomain\it-admin*** correspond à tous les administrateurs dans le domaine **corpdomain** domaine dont les noms d'utilisateur commencent par la chaîne **it#admin**. Vous pouvez ajouter un maximum de 5 000 entrées à exclure du mappage d'utilisateur.

Définissez la liste des utilisateurs ignorés sur le pare-feu faisant office d'agent User-ID, et non pas sur le client. Si vous définissez la liste des utilisateurs ignorés sur le pare-feu client, les utilisateurs qui figurent dans la liste font toujours l'objet d'un mappage lors de la redistribution.

Surveillance des serveurs

- Périphérique > Identification utilisateur > Mappage d'utilisateur

Utilisez la section Surveillance des serveurs pour définir les serveurs Microsoft Exchange, les contrôleurs de domaine Active Directory (AD), les serveurs Novell eDirectory ou les expéditeurs Syslog que l'agent User-ID doit surveiller pour déceler des événements de connexion.

- Configuration de l'accès aux serveurs surveillés
- Gestion de l'accès aux serveurs surveillés
- Inclure ou exclure des sous-réseaux pour l'association d'utilisateur

Configuration de l'accès aux serveurs surveillés

Utilisez la section Surveillance du serveur pour **Ajouter** des profils de serveur qui indiquent les serveurs que le pare-feu surveillera.

Configurez au moins deux serveurs surveillés par User-ID. Ainsi, en cas d'échec d'un serveur, le pare-feu peut tout de même découvrir les mappages adresse IP/nom d'utilisateur.

La procédure complète pour configurer l'agent User-ID intégré à PAN-OS pour qu'il surveille les serveurs exige l'accomplissement des tâches supplémentaires outre la création de profils de serveurs.

Paramètres de surveillance du serveur	Description
Nom	Saisissez un nom de serveur.
Description	Saisissez une description du serveur.
Activé	Sélectionnez cette option pour activer la surveillance des journaux sur ce serveur.
Type	Sélectionnez le type de serveur. Votre sélection détermine les autres champs que ce dialogue affichera.

Paramètres de surveillance du serveur	Description
	• **Microsoft Active Directory** • **Microsoft Exchange** • **Novell eDirectory** • **Expéditeur Syslog**
Protocole de transport (Microsoft Active Directory et Microsoft Exchange uniquement)	Sélectionnez le protocole de transport : • **WMI** : (par défaut) Utilisez Windows Management Instrumentation (WMI) pour sonder chaque adresse IP découverte et vérifier que le même utilisateur demeure connecté. • **Win-RM-HTTP** : Utilisez Windows Remote Management (WinRM) sur HTTP pour surveiller les journaux de sécurité et les informations de session sur le serveur. Le pare-feu chiffre la charge utile avec la clé de session Kerberos. • **Win-RM-HTTPS** : Utilisez Windows Remote Management (WinRM) sur HTTPS pour surveiller les journaux de sécurité et les informations de session sur le serveur. Pour exiger la validation des certificats du serveur avec le serveur Windows lorsque vous utilisez l'authentification Kerberos, veillez à configurer NTP dans les Paramètres des services globaux et à sélectionner l'autorité de certificat racine en tant que profil de certificat (Périphérique > Identification utilisateur > Sécurité de la connexion).
Adresse réseau	Saisissez l'adresse IP du serveur ou le nom de domaine complet du serveur surveillé. Si vous utilisez Kerberos à des fins d'authentification du serveur, vous devez entrer un FQDN. Cette option n'est pas prise en charge si le **Type** est **Novell eDirectory**.
Profil de serveur (Novell eDirectory uniquement)	Sélectionnez un profil de serveur LDAP pour la connexion au serveur eDirectory (Périphérique > Profils de serveurs > LDAP).
Connection Type (Expéditeur Syslog uniquement)	Sélectionnez si l'agent User-ID doit écouter les messages Syslog sur le port **UDP** (514) ou le port **SSL** (6 514). Si vous sélectionnez **SSL**, le **Syslog Service Profile (Profil du service Syslog)** que vous sélectionnez lors de l'activation de la Surveillance du serveur détermine les versions SSL/TLS qui sont autorisées et le certificat que le pare-feu utilise pour sécuriser une connexion avec l'expéditeur Syslog.

Paramètres de surveillance du serveur	Description
	*En tant que meilleure pratique en termes de sécurité, sélectionnez **SSL** lorsque vous utilisez l'agent User-ID intégré à PAN-OS pour mapper les adresses IP à des noms d'utilisateur. Si vous sélectionnez **UDP**, assurez-vous que l'expéditeur Syslog et le client se trouvent tous les deux sur un réseau sécurisé dédié pour empêcher les hôtes non approuvés d'envoyer du trafic UDP au pare-feu.*
Filtre (Expéditeur Syslog uniquement)	Si le **Type** de serveur est **Expéditeur Syslog**, vous devez **Ajouter** un ou plusieurs profils profil d'analyse syntaxique Syslog à utiliser pour l'extraction des noms d'utilisateur et des adresses IP des messages syslog reçus de ce serveur. Vous pouvez ajouter un profil personnalisé (reportez-vous à la section Filtres Syslog) ou un profil prédéfini. Pour chaque profil, définissez le **Type d'événement** : • **Connexion** – L'agent User-ID analyse les messages Syslog pour les événements de connexion pour créer des associations d'utilisateurs. • **Déconnexion** – L'agent User-ID analyse les messages Syslog pour les événements de déconnexion pour supprimer les associations d'utilisateurs qui ne sont plus d'actualité. Dans les réseaux où l'affectation des adresses IP est dynamique, la suppression automatique améliore la précision des associations des utilisateurs en veillant à ce que l'agent associe chaque adresse IP uniquement à l'utilisateur actuellement concerné. *Si vous ajoutez un profil d'analyse syntaxique Syslog prédéfini, vérifiez son nom pour déterminer s'il est destiné à correspondre aux événements de connexion ou de déconnexion.*
Nom de domaine par défaut (Expéditeur Syslog uniquement)	(Facultatif) Si le **Type** de serveur est **Expéditeur Syslog**, entrez un nom de domaine pour remplacer le nom de domaine actuel qui se trouve dans le nom d'utilisateur de votre message syslog ou ajouter le domaine au nom d'utilisateur si votre message syslog ne contient pas de domaine.

Gestion de l'accès aux serveurs surveillés

Effectuez les tâches suivantes à la section Surveillance des serveurs afin de gérer l'accès aux serveurs que l'agent User-ID surveille pour extraire des informations de mappage d'utilisateur.

Tâche	Description
Afficher les informations sur les serveurs	Pour chaque serveur surveillé, la page Mappage d'utilisateur affiche l'État de la connexion établie entre l'agent User-ID et le serveur. Après avoir cliqué sur **Add (Ajouter)** pour ajouter un serveur, le pare-feu essaie de s'y connecter. Si la tentative de connexion est réussie, la section Surveillance des serveurs indique Connecté dans la

Tâche	Description
	colonne État. Si le pare-feu ne parvient pas à se connecter, la colonne État présente une condition d'erreur, telle que `Connexion refusée` ou `Expiration du délai de connexion`. Pour des détails sur les autres champs de la section Surveillance des serveurs, reportez-vous à Configuration de l'accès aux Serveurs surveillés.
Ajouter	Pour effectuer la Configuration de l'accès aux Serveurs surveillés, vous devez **Add (Ajouter)** chaque serveur que l'agent User-ID surveillera pour extraire les informations de mappage d'utilisateur.
Supprimer	Pour supprimer un serveur du processus de mappage d'utilisateur (détection), sélectionnez le serveur et cliquez sur **Delete (Supprimer)**. **Conseil**: Pour supprimer un serveur de la détection sans supprimer sa configuration, modifiez l'entrée du serveur et décochez l'option **Enabled (Activé)**.
Découvrez	Vous pouvez automatiquement **Discover (Détecter)** des contrôleurs de domaine Microsoft Active Directory au moyen de DNS. Le pare-feu détecte les contrôleurs de domaine en fonction du nom de domaine saisi dans la page **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)**, section **General Settings (Paramètres généraux)**, champ **Domain (Domaine)**. Une fois qu'il a détecté un contrôleur de domaine, le pare-feu crée une entrée pour ce dernier dans la liste Surveillance des serveurs ; vous pouvez ensuite activer le serveur pour qu'il effectue la surveillance. *la fonction de **Discover (Détection)** fonctionne uniquement pour les contrôleurs de domaine, pas pour les serveurs Exchange ou eDirectory.*

Inclure ou exclure des sous-réseaux pour l'association d'utilisateur

- Périphérique > Identification utilisateur > Mappage d'utilisateur

Utilisez la liste Inclure/Exclure des réseaux pour définir les sous-réseaux que l'agent User-ID inclura ou exclura lorsqu'il effectue le mappage nom d'utilisateur/adresse IP (détection). Par défaut, si vous n'ajoutez pas de sous-réseaux à la liste, l'agent User-ID effectue une détection des sources d'identification utilisateur dans tous les sous-réseaux, sauf lorsqu'il utilise le sondage WMI des systèmes clients qui possèdent des adresses IPv4 publiques. (Les adresses IPv4 publiques sont celles qui sont à l'extérieur de la portée de RFC 1918 et RFC 3927).

Pour activer le sondage WMI des adresses IPv4 publiques, vous devez ajouter leurs sous-réseaux à la liste et définir leur option **Discovery (Détection)** sur **Include (Inclure)**. Si vous configurez le pare-feu pour qu'il puisse redistribuer les informations de mappage d'utilisateurs aux autres pare-feu, les limites de découverte indiquées dans la liste vont s'appliquer aux informations redistribuées.

Utilisez les listes d'inclusion et d'exclusion pour définir les sous-réseaux dans lesquels le pare-feu effectuer le mappage d'utilisateurs.

Vous pouvez exécuter les tâches suivantes sur la liste Inclure/Exclure des réseaux :

Tâche	Description
Ajouter	Pour restreindre la découverte à un sous-réseau donné, **Add (Ajoutez)** un profil de sous-réseau et remplissez les champs suivants : • **Name (Nom)** : saisissez un nom pour identifier le sous-réseau. • **Enabled (Activé)** : sélectionnez cette option pour activer l'inclusion ou l'exclusion du sous-réseau lors de la surveillance du serveur. • **Détection (Discovery)** : précisez si l'agent User-ID va **Inclure** ou **Exclude (Exclure)** le sous-réseau. • **Network Address (Adresse réseau)** : saisissez la plage d'adresses IP du sous-réseau. L'agent User-ID applique une règle implicite à la liste qui va tout exclure. Par exemple, si vous ajoutez le sous-réseau 10.0.0.0/8 avec l'option **Inclure,** l'agent User-ID exclut tous les autres sous-réseaux, même si vous ne les ajoutez pas à la liste. Ajoutez des entrées avec l'option **Exclude (Exclure)** uniquement si vous souhaitez que l'agent User-ID exclue un sous-ensemble de sous-réseaux que vous avez implicitement inclus. Par exemple, si vous ajoutez 10.0.0.0/8 avec l'option **Include (Inclure)** et que vous ajoutez 10.2.50.0/22 avec l'option **Exclude (Exclure)**, l'agent User-ID procédera à une découverte sur tous les sous-réseaux de 10.0.0.0/8, sauf 10.2.50.0/22, et exclura tous les sous-réseaux n'appartenant pas à 10.0.0.0/8. Si vous ajoutez des profils **Exclude (Exclure)** sans ajouter de profils **Include (Inclure)**, l'agent User-ID exclura tous les sous-réseaux et pas uniquement ceux que vous avez ajoutés.
Supprimer	Pour supprimer un sous-réseau de la liste, sélectionnez-le et cliquez sur **Delete (Supprimer)**. **Conseil**: Pour supprimer un sous-réseau de la liste Inclure/Exclure des réseaux sans effacer sa configuration, modifiez le profil du sous-réseau et désélectionnez l'option **Enabled (Activé)**.
Séquence Inclure/ Exclure les réseaux personnalisée	Par défaut, l'agent User-ID évalue les sous-réseaux dans leur ordre d'ajout, les premiers en tête de liste et les derniers en bas de liste. Pour modifier l'ordre d'évaluation, cliquez sur **Custom Include/Exclude Network Sequence (Séquence réseau d'inclusion/exclusion personnalisée)**. Vous pouvez ensuite **Add (Ajouter)**, **Delete (Supprimer)**, **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)** les sous-réseaux pour créer un ordre d'évaluation personnalisé.

Périphérique > Identification utilisateur > Sécurité de la connexion

Modifiez ( ) les paramètres de Sécurité de la connexion User-ID pour sélectionner le profil du certificat utilisé par le pare-feu afin de valider le certificat présenté par les agents User-ID Windows. Le pare-feu utilise le profil du certificat sélectionné pour vérifier l'identité de l'agent User-ID en validant le certificat du serveur présenté par l'agent.

Tâche	Description
Profil de certificat User-ID	Dans le menu déroulant, sélectionnez le profil du certificat à utiliser lors de l'authentification des agents User-ID Windows ou sélectionnez Nouveau profil du certificat pour créer un nouveau profil du certificat. Sélectionnez **Aucun** pour supprimer le profil du certificat et utiliser plutôt l'authentification par défaut. Pour exiger la validation des certificats du serveur avec le serveur Windows lorsque vous Configuration de l'accès aux serveurs surveillés à l'aide de Kerberos pour l'authentification du serveur, veillez à configurer NTP dans les Paramètres des services globaux et sélectionnez l'autorité de certificat racine en tant que profil de certificat.
Supprimer tout (Configuration du modèle uniquement)	Supprime le profil du certificat associé à la configuration de la Sécurité de la connexion User-ID pour le modèle sélectionné.

Périphérique > Identification utilisateur > Agents de Terminal Server

Sur un système qui prend en charge plusieurs utilisateurs qui partagent une même adresse IP, l'agent Terminal Server (TS) identifie chaque utilisateur en lui affectant une plage de ports spécifiques. L'agent TS indique à chaque pare-feu connecté la plage de ports qui a été affectée afin que les pare-feu puissent appliquer la politique en fonction des utilisateurs et des groupes d'utilisateurs.

Tous les modèles de pare-feu peuvent collecter des informations de mappage de noms d'utilisateur vers des ports à partir de plus de 5 000 systèmes multi-utilisateurs. Le nombre d'agents TS à partir duquel un pare-feu peut collecter les informations de mappage varie selon le modèle de pare-feu.

Vous devez installer et configurer les agents TS avant d'en configurer l'accès. La procédure complète visant à configurer le mappage d'utilisateur pour les utilisateurs de serveurs de terminaux nécessite des tâches supplémentaires en plus de la configuration des connexions aux agents TS.

Vous pouvez exécuter les tâches suivantes pour gérer l'accès aux agents TS :

Tâche	Description
Affichage de l'information / Actualisation de la connexion	À la page **Terminal Server Agents (Agents de Terminal Server)**, la colonne Connecté affiche l'état des connexions du pare-feu vers les agents TS. Une icône verte indique une connexion réussie, une icône jaune indique une connexion désactivée et une icône rouge indique un échec de connexion. Si vous pensez que l'état de la connexion a changé depuis votre première ouverture de la page, cliquez sur **Refresh Connected (Actualisation de la connexion)** pour mettre à jour l'affichage.
Ajouter	Pour configurer l'accès à un agent TS, cliquez sur **Ajouter** et configurez les champs suivants : • **Nom** – Saisissez un nom permettant d'identifier l'agent TS (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement. • **Host (Hôte)** - Saisissez l'adresse IP statique ou le nom d'hôte du serveur de terminaux sur lequel l'agent TS est installé. • **Port** – Saisissez le numéro de port (valeur par défaut : 5 009) que le service Agent TS utilise pour communiquer avec le pare-feu. • **Alternative Hosts (Hôtes de remplacement)** – Si le serveur de terminal sur lequel l'agent TS est installé dispose de plusieurs adresses IP qui peuvent apparaître comme adresse IP source du trafic sortant, cliquez sur **Ajouter** et saisissez jusqu'à huit adresses IP statiques ou noms d'hôte supplémentaires. • **Enabled (Activé)** - Sélectionnez cette option pour activer le pare-feu afin de communiquer avec cet agent TS.

Tâche	Description
Supprimer	Pour supprimer la configuration qui permet l'accès à un agent TS, sélectionnez l'agent et cliquez sur **Delete (Supprimer)**. *Pour désactiver l'accès à un agent TS sans supprimer sa configuration, modifiez-le et désélectionnez l'option **Activé**.*
PDF/CSV	Les rôles administrateur qui sont au moins dotés de l'accès en lecture seule peuvent exporter le tableau de configuration du périphérique au format **PDF/CSV**. Vous pouvez appliquer des filtres pour créer des sorties du tableau de configuration plus précises, par exemple, pour effectuer des audits. Seules les colonnes qui sont visibles dans l'interface Web seront exportées. Reportez-vous à la section Exportation du tableau de configuration.

Périphérique > Identification utilisateur > Paramètres de mappage de groupe

- **Périphérique** > **Identification utilisateur** > **Paramètres du mappage de groupe**

Pour baser des politiques de sécurité et des rapports sur des utilisateurs ou un groupe d'utilisateurs, le pare-feu doit récupérer la liste des groupes et la liste des membres correspondante spécifiée et gérée sur vos serveurs d'annuaire. Le pare-feu prend en charge divers serveurs d'annuaires LDAP, notamment Microsoft Active Directory (AD), Novell eDirectory et Sun ONE Directory Server.

Le nombre de groupes distincts d'utilisateurs que chaque pare-feu ou Panorama peut référencer parmi toutes les politiques varie selon le modèle. Cependant, peu importe le modèle, vous devez configurer un profil de serveur LDAP (Périphérique > Profils de serveur > LDAP) avant de pouvoir créer une configuration de mappage de groupe.

La procédure complète pour associer des noms d'utilisateur à des groupes exige l'accomplissement de tâches supplémentaires en plus de la création de configurations d'association de groupe.

Add (Ajoutez) et configurez les champs suivants, au besoin, pour créer une configuration d'association de groupe. Pour supprimer une configuration d'associations de groupe, sélectionnez-la, puis cliquez sur **Delete (Supprimer)**. Si vous souhaitez désactiver une configuration d'association de groupe sans l'effacer, modifiez la configuration et désélectionnez l'option **Enabled (Activée)**.

Si vous créez plusieurs configurations de mappage de groupe qui utilisent le même nom unique (DN) ou le même serveur LDAP de base, les configurations de mappage de groupe ne peuvent pas contenir des groupes qui se chevauchent (par exemple, la Liste d'inclusion d'une configuration de mappage de groupe n peut pas contenir un groupe qui est aussi dans une configuration de mappage de groupe différente).

Paramètres d'association de groupe - Profil de serveur	Configuré dans	Description
Nom	**Périphérique** > **Identification utilisateur** > **Paramètres du mappage de groupe**	Donnez un nom pour identifier la configuration d'association de groupe (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Profil de serveur	**Périphérique** > **Identification utilisateur** > **Paramètres du mappage de groupe** > **Profil de serveur**	Sélectionnez le profil de serveur'A0;LDAP à utiliser pour le mappage de groupe sur ce pare-feu.

Paramètres d’association de groupe - Profil de serveur	Configuré dans	Description
Intervalle de mise à jour		Indiquez l’intervalle en secondes après lequel le pare-feu établit une connexion au serveur d’annulaire LDAP pour obtenir toutes les mises à jour des groupes que les politiques de pare-feu utilisent (plage comprise entre 60 et 86 400).
Domaine d'utilisateur		Par défaut, le champ **User Domain (Domaine d'utilisateur)** est vide : le pare-feu détecte automatiquement les noms de domaine des serveurs Active Directory. Si vous saisissez une valeur, elle remplacera tout nom de domaine que le pare-feu récupère de la source LDAP. Votre entrée doit correspondre au nom NetBIOS. *Ce champ n'affecte que les noms d'utilisateur et de groupe récupérés dans la source LDAP. Pour remplacer le domaine associé à un nom d’utilisateur pour l’authentification de l’utilisateur, configurez le **User Domain (Domaine d'utilisateur)** et le **Username Modifier (Modificateur du nom d’utilisateur)** pour le profil d’authentification que vous attribuez à cet utilisateur (voir Périphérique > Profil d’authentification).*
Objets du groupe		• **Search Filter (Filtre de recherche)** : saisissez une requête LDAP qui précise les groupes à récupérer et à suivre. • **Object Class (Classe d'objets)** : saisissez une définition de groupe. Le paramètre par défaut est objectClass=group, ce qui indique que le système récupère tous les objets de l'annuaire correspondant au **Search Filter (Filtre de recherche)** de groupe, dont objectClass=group.

Paramètres d’association de groupe - Profil de serveur	Configuré dans	Description
Objets utilisateur		• **Filtre de recherche** : saisissez une requête LDAP qui précise les utilisateurs à récupérer et à suivre. • **Object Class (Classe d'objet)** : saisissez une définition d'un objet utilisateur. Par exemple, dans Active Directory, cet attribut est *user*.
Activé		Sélectionnez cette option pour activer le profil de serveur pour le mappage de groupe.
Récupérez la liste des périphériques gérés		Pour les déploiements GlobalProtect, sélectionnez cette option pour permettre au pare-feu d’extraire les numéros de série à partir d’un serveur d’annuaires (comme Active Directory). GlobalProtect peut ainsi identifier l’état des points de terminaison qui se connectent et appliquer les politiques de sécurité basées sur HIP en fonction de la présence du numéro de série des points de terminaison.
Attributs utilisateur	**Device (Périphérique) > User Identification (Identification utilisateur) > Group Mapping Settings (Paramètres de mappage de groupe) > User and**	Précisez les attributs d’annuaire pour identifier les utilisateurs : • **Nom d’utilisateur**principal : spécifiez l’attribut que la source d’ID utilisateur fournit pour le nom d’utilisateur (par

Paramètres d’association de groupe - Profil de serveur	Configuré dans	Description
	Group Attributes (Attributs utilisateur et groupe)	exemple, **`userPrincipalName`** ou **`sAMAccountName`**) *Le nom d’utilisateur principal est la façon dont le pare-feu identifie l’utilisateur dans les journaux, les rapports et les configurations de stratégie, même si le pare-feu reçoit d’autres formats des sources d’ID utilisateur. Si vous ne spécifiez pas de format, le pare-feu utilise le format `sAMAccountName` par défaut pour Active Directory et le format `uid` pour Novell eDirectory et Sun ONE Directory Server.* • **E-Mail (Courriel)** : spécifiez l’attribut que la source User-ID fournit à l’adresse électronique. La valeur par défaut est **`mail`**. • **Autre nom d’utilisateur 1 à 3 :**spécifiez jusqu’à trois attributs supplémentaires qui correspondent aux formats que vos sources d’ID utilisateur peuvent envoyer. *Si vous configurez un serveur Active Directory, l’autre nom d’utilisateur 1 est `userPrincipalName` par défaut.*
Attributs de groupes		Précisez les attributs que les sources User-ID utilisent pour identifier les groupes : • **Group Name (Nom du groupe)** : précisez l'attribut que la source User-ID utilise pour l’attribut nom de groupe. Par défaut, l’attribut d’Active Directory est `name` et celui de Novell eDirectory et de Sun ONE Directory Server est `cn`. • **Group Member (Membre du groupe)** : spécifiez l’attribut que la source User-ID

Paramètres d’association de groupe - Profil de serveur	Configuré dans	Description
		utilise pour le membre du groupe. La valeur par défaut est `member`. • **E-Mail (Courriel)** : spécifiez l’attribut que la source User-ID utilise pour l’adresse électronique. La valeur par défaut est `mail`.
Groupes disponibles Groupes inclus	**Périphérique** > **Identification utilisateur** > **Paramètres du mappage de groupe** > **Liste d’inclusion de groupe**	Utilisez ces champs pour restreindre le nombre de groupes que le pare-feu affiche lorsque vous créez une règle de sécurité. Parcourez l'arborescence LDAP pour trouver les groupes que vous souhaitez utiliser dans les règles. Pour inclure un groupe, sélectionnez-le et ajoutez-le () dans la liste des Groupes disponibles. Pour supprimer un groupe de la liste, sélectionnez-le et supprimez-le () de la liste des Groupes inclus.  *N’incluez que les groupes que vous devez inclure pour que le pare-feu ne puisse récupérer les associations de groupe d’utilisateurs que pour les groupes nécessaires et non pas de l'arbre au complet de l’annuaire LDAP.*
Nom Filtre LDAP	**Périphérique** > **Identification utilisateur** > **Paramètres du mappage de groupe** > **Groupe personnalisé**	Créez des groupes personnalisés basés sur des filtres LDAP de manière à pouvoir baser les politiques du pare-feu sur les attributs utilisateur qui ne correspondent pas aux groupes d’utilisateurs existants dans le répertoire LDAP. Le service User-ID mappe tous les utilisateurs du répertoire LDAP correspondant au filtre du groupe personnalisé. Si vous créez un groupe personnalisé dont le Nom distingué (ND) est le même que le nom de domaine d'un groupe Active Directory existant, le pare-feu va utiliser le groupe personnalisé dans toutes les références à ce nom (par exemple, dans les politiques et les journaux). Pour créer un groupe personnalisé,

Paramètres d’association de groupe - Profil de serveur	Configuré dans	Description
		cliquez sur **Add (Ajouter)** et configurez les champs suivants : • **Name (Nom)** : saisissez un nom de groupe personnalisé qui est unique dans la configuration d’association de groupe du pare-feu ou du système virtuel actuel. • **LDAP Filter (Filtre LDAP)** : saisissez un filtre de 2 048 caractères maximum. *Utilisez uniquement les attributs indexés dans le filtre pour faciliter les recherches LDAP et minimiser l’impact sur les performances sur le serveur d’annuaire LDAP ; le pare-feu ne valide pas les filtres LDAP.* Le maximum combiné pour les listes **Included Groups (Groupes inclus)** et **Custom Group (Groupe personnalisé)** correspond à 640 saisies. Pour supprimer un groupe personnalisé, sélectionnez-le, puis cliquez sur **Delete (Supprimer)**. Pour copier un groupe personnalisé, sélectionnez-le, cliquez sur **Clone (Cloner)**, puis modifiez les champs de manière appropriée. *Après avoir ajouté ou cloné un groupe personnalisé, vous devez **Commit (Valider)** vos modifications avant que votre nouveau groupe personnalisé soit disponible dans les politiques et les objets.*

Périphérique > Identification utilisateur> Adresse source fiable

Explicit Proxy (Proxy explicite) permet au trafic provenant uniquement d'adresses IP spécifiques de s'authentifier en utilisant le protocole X-Authenticated-User (XAU). Créez un address object (objet adresse) puis **edit (Modifiez)** la configuration Adresse source approuvée et ajoutez l'objet adresse pour spécifier les adresses IP où XAU est autorisé pour l'authentification pour le proxy explicite. Pour plus d'informations, reportez-vous à Secure Mobile Users with an Explicit Proxy (Utilisateurs mobiles sécurisés avec un proxy explicite).

Champs d’adresse source fiable	Description
Activé	Sélectionnez cette option pour activer la configuration de l'adresse source approuvée.
Adresse source fiable	**Add (Ajouter)** une adresse source approuvée Les X-Authenticated-User (XAU) contenus dans les requêtes entrantes de ces adresses sources sont approuvés pour le proxy explicite. Vous pouvez également **Search (rechercher)** la liste des adresses sources approuvées ou **Delete (Supprimer)** une adresse source si nécessaire.

Périphérique > Identification utilisateur > Paramètres du portail d’authentification

Modifiez (⚙) les paramètres du Authentication Portal (Portail d’authentification) pour configurer le pare-feu afin qu’il puisse authentifier les utilisateurs dont le trafic correspond à une règle de politique d’authentification.

Si le Portail d’authentification utilise un profil de service SSL/TLS (Périphérique > Gestion des certificats > Profil de service SSL/TLS), un profil d’authentification (Périphérique > Profil d’authentification), ou un profil de certificat (Périphérique > Gestion des certificats > Profil du certificat), configurez le profil avant de commencer. La procédure complète pour configurer le Portail d’authentification requiert des tâches supplémentaires en plus de la configuration de ces profils.

*Vous devez **Enable Authentication Portal (Activer le portail d’authentification)** pour appliquer la politique d’authentification (voir Policies > Authentication (Politiques > Authentification)).*

Champs	Description
Activer le Portail d’authentification)	Sélectionnez cette option pour activer le Portail d’authentification.
Minuteur d'inactivité (minutes)	Saisissez la valeur TTL (Time-To-Live) de l’utilisateur en minutes pour une session du Portail d’authentification (plage comprise entre 1 et 1 440 ; par défaut 15). Ce minuteur est remis à zéro à chaque activité de l'utilisateur du portail d’authentification. Si la durée d’inactivité d’un utilisateur dépasse la valeur du **Idle Timer (Minuteur d’inactivité)**, PAN-OS supprime le mappage d’utilisateur du Portail d’authentification et l’utilisateur doit se connecter à nouveau.
Temps (minutes)	Il s’agit de la valeur TTL maximale en minutes, c’est-à-dire le délai maximum pendant lequel une session du Portail d’authentification peut demeurer mappée (plage comprise entre 1 et 1 440 ; par défaut 60). Une fois cette durée écoulée, PAN-OS supprime le mappage, et les utilisateurs doivent se réauthentifier même si la session est active. Ce minuteur permet d’éviter les mappages obsolètes et remplace la valeur **Idle Timer (Minuteur d’inactivité)**. *Il est recommandé de toujours définir le **Timer (Minuteur)** d’expiration sur une valeur supérieure à celle du **Idle Timer (Minuteur d’inactivité)**.*
Profil de service SSL/TLS	Pour indiquer un certificat du serveur de pare-feu et les protocoles autorisés pour sécuriser les requêtes de redirection, sélectionnez un profil de service SSL/TLS (voir Périphérique > Gestion des certificats > Profil de service SSL/TLS). Si vous

Champs	Description
	sélectionnez **None (Aucun)**, le pare-feu utilise son certificat local par défaut pour les connexions SSL/TLS. *Dans le profil de service SSL/TLS, définissez la **Min Version (Version min)** sur **TLSv1.2** et définissez la **Max Version (Version max)** sur **Max** pour fournir la sécurité la plus forte contre les vulnérabilités du protocole SSL/TLS. L'établissement de la **Max Version (Version max)** sur **Max** garantit que le pare-feu utilise toujours la dernière version au fur et à mesure que les protocoles plus forts deviennent disponibles.* Pour rediriger de manière transparente les utilisateurs sans afficher d'erreurs de certificat, assignez un profil associé à un certificat correspondant à l'adresse IP de l'interface vers laquelle les requêtes Web sont redirigées.
Profil d'authentification	Vous pouvez sélectionner un profil d'authentification (Périphérique > Profil d'authentification) pour authentifier les utilisateurs lorsque leur trafic correspond à une règle de politique d'authentification (Politiques > Authentification). Cependant, le profil d'authentification que vous sélectionnez dans les Paramètres du portail d'authentification s'applique uniquement aux règles qui font référence à l'un des objets d'application d'authentification par défaut (Objects > Authentication (Objets > Authentification)). Ceci est généralement le cas juste après une mise à niveau vers PAN-OS 8.0, car toutes les règles d'authentification font initialement référence aux objets par défaut. Pour les règles qui font référence aux objets d'application d'authentification personnalisés, sélectionnez le profil d'authentification lorsque vous créez l'objet.
Port réseau GlobalProtect pour les invites d'authentification entrante (UDP)	Indiquez le port utilisé par GlobalProtect™ pour recevoir les invites d'authentification entrantes des passerelles multi-facteur (MFA). (La plage est comprise entre 1 et 65 536 ; par défaut 4 501). Pour prendre en charge l'authentification multi-facteur, un point de terminaison GlobalProtect doit recevoir et reconnaître les invites UDP qui proviennent de la passerelle MFA. Lorsqu'un point de terminaison GlobalProtect reçoit un message UDP sur le port réseau spécifié et que le message UDP provient d'un pare-feu ou d'une passerelle de confiance, GlobalProtect affiche le message d'authentification (voir Personnaliser l'application GlobalProtect
Mode	Sélectionnez la manière dont le pare-feu capture les requêtes Web pour l'authentification : • **Transparent**: le pare-feu intercepte les requêtes Web conformément à la règle d'authentification et emprunte l'identité de l'URL de destination d'origine, en émettant un message HTTP 401 pour inviter l'utilisateur à s'authentifier. Toutefois, étant donné que le pare-feu ne dispose pas du certificat de l'URL de destination, le navigateur affiche une erreur de certificat aux utilisateurs qui tentent d'accéder à un site sécurisé. N'utilisez donc ce mode qu'en cas de nécessité, dans des déploiements de couche 2 ou virtuels par exemple.

Champs	Description
	• **Redirect (Rediriger)** – Le pare-feu intercepte les requêtes Web selon la règle d'authentification et les redirige vers l'Hôte de redirection indiqué. Le pare-feu utilise une redirection HTTP 302 pour inciter l'utilisateur à s'authentifier. Il est recommandé d'utiliser la fonction de **Redirect (redirection)**, car elle fournit une meilleure expérience aux utilisateurs finaux (elle n'affiche aucune erreur de certificat et autorise les cookies de session qui permettent une navigation transparente, car la **Redirect (redirection)** n'effectue aucune réaffection à l'expiration des délais). Cependant, il nécessite que vous activiez les pages de réponse sur le profil de gestion d'interface attribué à l'interface de couche 3 d'entrée (pour plus de détails, voir Réseau > Profils réseau > Gestion d'interface et interface de couche 3 de la gamme PA-7000). Un autre avantage du mode de redirection est qu'il autorise les cookies de session, qui permettent à l'utilisateur de continuer à naviguer vers des sites authentifiés sans nécessiter de re-mappage à chaque fois que les délais expirent. Ceci est particulièrement utile pour les utilisateurs passant d'une adresse IP à une autre (du LAN d'entreprise au réseau sans fil par exemple), car ils ne doivent pas nécessairement s'authentifier à nouveau lorsque leur adresse IP change tant que la session est ouverte. Le mode ***Redirect (Rediriger)*** *est requis si le Portail d'authentification utilise l'authentification SSO Kerberos, car le navigateur fournit des informations d'identification uniquement aux sites approuvés. Le mode* ***Redirect (Rediriger)*** *est également requis si le Portail d'authentification utilise l'authentification multi-facteur (MFA).*
Cookie de session (Mode Rediriger uniquement)	• **Enable (Activer)** : sélectionnez cette option pour activer les cookies de session. • **Timeout (Délai)** : si vous **Enable (Activez)** les cookies de session, ce minuteur précise le nombre de minutes pendant lesquelles le cookie est valide (intervalle compris entre 60 et 10 080 ; valeur par défaut : 1 440). *Définissez une valeur de délai assez courte, pour éviter qu'elle n'entraîne d'entrées de mappage utilisateur obsolètes dans les cookies, mais assez longue pour favoriser une bonne expérience utilisateur en évitant d'inviter les utilisateurs à se connecter plusieurs fois au cours d'une session. Commencez par une valeur inférieure ou égale à 480 minutes (8 heures) et ajustez la valeur au besoin.* • **Roaming (Itinérance)** – Sélectionnez cette option pour mettre en mémoire le cookie si l'adresse IP subit une modification lorsque la session est active (par exemple, quand le point de terminaison passe d'un réseau filaire à un réseau sans fil). L'utilisateur doit uniquement se réauthentifier si le cookie expire ou si l'utilisateur ferme le navigateur.
Rediriger l'hôte	Indiquez le nom d'hôte intranet qui résout en adresse IP l'interface de couche 3 vers laquelle le pare-feu redirige les requêtes Web.

Champs	Description
(Mode Rediriger uniquement)	*Si les utilisateurs s'authentifient via l'ouverture de session unique (SSO) Kerberos, le **Redirect Host (Hôte de redirection)** doit être identique au nom d'hôte indiqué dans le* Keytab Kerberos.
Profil du certificat	Vous pouvez sélectionner un profil de certificat (Périphérique > Gestion des certificats > Profil du certificat) pour authentifier les utilisateurs lorsque leur trafic correspond à une règle de politique d'authentification (Politiques > Authentification). Pour ce type d'authentification, le Portail d'authentification invite le navigateur du point de terminaison à présenter un certificat client. Par conséquent, vous devez déployer des certificats clients à chaque système utilisateur. En outre, vous devez installer sur le pare-feu le certificat d'autorité de certification (CA) qui a émis les certificats clients et qui a attribué le certificat AC au profil du certificat. Il s'agit de la seule méthode d'authentification permettant une authentification **Transparent (Transparente)** des points de terminaison macOS et Linux.

Device > User Identification > Cloud Identity Engine (Périphérique > Identification de l’utilisateur > Moteur d’identification du cloud

Add (Ajoutez) un profil Cloud Identity Engine à votre pare-feu pour utiliser Cloud Identity Engine comme source d'informations d'identification utilisateur. Lorsque vous créez un profil Cloud Identity Engine, vous pouvez appliquer des politiques de sécurité basées sur les utilisateurs ou les groupes en fonction des informations sur les utilisateurs et les groupes à partir des annuaires sur site ou dans le cloud que vous configurez dans l'application Cloud Identity Engine. Vous pouvez également **Delete (supprimer)** un profil ou exporter un fichier **PDF/CSV** des profils Cloud Identity Engine actuels.

Avant de pouvoir configurer un profil Cloud Identity Engine sur le pare-feu, vous devez install (installer) un certificat d'appareil et activate (activer) une instance Cloud Identity Engine sur le hub.

Pour rechercher les profils, entrez un mot-clé comme filtre (🔍) et **Apply Filter (Appliquer le filtre)** (→).

Paramètres de Cloud Identity Engine	Description
Nom	Saisissez un **Name (nom)** (jusqu'à 31 caractères) pour le profil Cloud Identity Engine. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement.
Instance (Exemple)	Saisissez les informations suivantes pour configurer le profil Cloud Identity Engine : • **Region (Région)** : sélectionnez le point de terminaison régional pour votre instance Cloud Identity Engine. *La région que vous sélectionnez doit correspondre à la région que vous sélectionnez lorsque vous activate (activez) votre instance Cloud Identity Engine.* • **Cloud Identity Engine Instance (Instance Cloud Identity Engine)** : si vous disposez de plusieurs instances, sélectionnez l'instance Cloud Identity Engine que vous souhaitez utiliser. • **Domain (Domaine)**—Sélectionnez le domaine qui contient les répertoires que vous souhaitez utiliser. • **Update Interval (min) (Intervalle de mise à jour (min))** : saisissez le nombre de minutes pendant lesquelles le pare-feu doit attendre entre les mises à jour La valeur par défaut est de 60 minutes et la plage est de 5 à 1440.

Paramètres de Cloud Identity Engine	Description
	Lorsque vous avez terminé de configurer le profil Cloud Identity Engine, confirmez que le profil est **Enabled (activé)**.
Attributs utilisateur	Sélectionnez un **Directory Attribute (attribut de répertoire)** pour chaque **Name (nom)** d'attribut utilisateur. Vous devez sélectionner un **Primary Username (nom d'utilisateur principal)** ; tous les autres champs sont facultatifs.
Attributs de groupes	Sélectionnez un **Directorate Attribute (attribut de répertoire)** pour chaque **Name (nom)** d'attribut de groupe. Vous devez sélectionner un **Group Name (nom de groupe)** ; le champ restant est facultatif.
Attributs de périphériques	(GlobalProtect only (GlobalProtect uniquement)) Si vous utilisez GlobalProtect et que vous avez activé la vérification du numéro de série, sélectionnez le **Endpoint Serial Number (numéro de série du point de terminaison)** pour permettre à Cloud Identity Engine de collecter les numéros de série des points de terminaison gérés. Ces informations sont utilisées par le portail GlobalProtect pour vérifier si le numéro de série existe dans le répertoire pour vérifier que le point de terminaison est géré par GlobalProtect.

GlobalProtect

GlobalProtect™ propose une infrastructure complète pour la gestion de votre personnel mobile pour permettre un accès sécurisé à tous vos utilisateurs, indépendamment des périphériques qu'ils utilisent ou de l'endroit où ils se trouvent. Les pages de l'interface Web du pare-feu suivantes vous permettent de configurer et de gérer les composants de GlobalProtect :

- Réseau > GlobalProtect > Portails
- Réseau > GlobalProtect > Passerelles
- Réseau > GlobalProtect > Gestionnaire de périphériques mobiles
- Réseau > GlobalProtect > Applications sans client
- Réseau > GlobalProtect > Groupes d'applications sans client
- Objets > GlobalProtect > Objets HIP
- Objets > GlobalProtect > Profils HIP
- Périphérique > Client GlobalProtect

Vous souhaitez en savoir plus ?

Reportez-vous au Guide de l'administrateur GlobalProtect pour en savoir plus sur GlobalProtect, y compris à propos des détails sur la configuration de l'infrastructure GlobalProtect, la façon d'utiliser les informations de l'hôte pour appliquer la politique ainsi que les instructions étape par étape pour des configurations standard de déploiements GlobalProtect.

Réseau > GlobalProtect > Portails

Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** pour configurer et gérer un portail GlobalProtect™. Le portail fournit les fonctions de gestion de l'infrastructure GlobalProtect. Chaque terminal qui participe au réseau GlobalProtect reçoit ses informations de configuration du portail, notamment des informations sur les passerelles disponibles ainsi que les certificats clients requis pour que l'application se connecte à une passerelle. De plus, le portail contrôle le comportement et la distribution du logiciel de l'application GlobalProtect à la fois sur les terminaux Windows et Mac OS. Pour les points de terminaison Linux, vous devez obtenir le logiciel du site de soutien ; pour les périphériques mobiles, l'application GlobalProtect est distribuée via App Store Apple pour les périphériques iOS, via Google Play pour les périphériques Android et via Microsoft Store pour Windows Phone et d'autres périphériques UWP Windows. Pour les Chromebooks, l'application GlobalProtect est distribuée par la console de gestion Chromebook ou via Google Play).

Pour ajouter une configuration de portail, cliquez sur **Add (Ajouter)** ; la boîte de dialogue Portail GlobalProtect s'affiche alors.

Que voulez-vous faire ?	Reportez-vous à la section :
Quels paramètres généraux devrais-je configurer pour le portail GlobalProtect ?	Onglet Général Portails GlobalProtect
Comment puis-je associer un profil d'authentification à une configuration de portail ou de passerelle ?	Onglet d'Authentification des portails GlobalProtect
Comment puis-je définir les données que l'application GlobalProtect collecte auprès des points de terminaison ?	Onglet Collecte de données du portail GlobalProtect
Quelles options d'authentification client puis-je configurer ?	Onglet Authentification de l'agent des portails GlobalProtect
Comment puis-je assigner une configuration à un groupe spécifique d'appareils, en me basant sur le système d'exploitation, l'utilisateur et/ou le groupe d'utilisateurs ?	Onglet des Critères de sélection de la configuration de l'agent des portails GlobalProtect
Comment puis-je configurer les paramètres et la priorité des passerelles internes ?	Onglet Agent interne des portails GlobalProtect
Comment puis-je configurer les paramètres et la priorité des passerelles externes ?	Onglet Agent externe des portails GlobalProtect

Que voulez-vous faire ?	Reportez-vous à la section :
Comment puis-je créer des configurations client pour différents types d'utilisateurs ?	Onglet GlobalProtect Portals Agent (Agent des portails GlobalProtect)
Quels paramètres puis-je personnaliser concernant le look et le comportement de l'application GlobalProtect?	Onglet Application de l’agent des portails GlobalProtect
Comment puis-je configurer les options de collecte de données ?	Onglet Collecte de données de l’agent des portails GlobalProtect
Comment puis-je configurer le portail GlobalProtect pour permettre l’accès aux applications Web sans installer l’application GlobalProtect ?	Onglet des VPN sans client des portails GlobalProtect
Comment puis-je étendre ma connectivité VPN à un pare-feu qui agit comme un satellite ?	Onglet du satellite du portail GlobalProtect
Vous souhaitez en savoir plus ?	Pour obtenir des instructions détaillées sur la configuration du portail, reportez-vous à la section Configuration d’un portail GlobalProtect du *Guide de l’administrateur de GlobalProtect*.

Onglet Général Portails GlobalProtect

- **Réseau** > **GlobalProtect** > **Portails** > ***<portal-config>*** > **Général**

Sélectionnez l’onglet **General (Général)** pour définir les paramètres réseau que l’application GlobalProtect utilise pour se connecter au portail GlobalProtect. En option, vous pouvez désactiver la page de connexion ou spécifier un portail de connexion et des pages d'aide personnalisé pour GlobalProtect. Pour plus d’informations sur la création et l’importation des pages personnalisées, reportez-vous à la section Personnaliser les pages Ouverture de session sur le portail, Accueil et Aide dans le Guide de l’administrateur de GlobalProtect.

Paramètres du portail GlobalProtect	Description
Name (Nom)	Saisissez un nom pour le portail (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement.
Location (Emplacement)	Pour un pare-feu en mode Plusieurs systèmes virtuels, **Location (Emplacement)** correspond au système virtuel (vsys) sur lequel le portail GlobalProtect est disponible. Pour un pare-feu qui n'est pas en mode

Paramètres du portail GlobalProtect	Description
	Plusieurs systèmes virtuels, la sélection **Location (Emplacement)** n'est pas disponible. Après avoir enregistré le portail, vous ne pouvez plus changer **Location (Emplacement)**.
paramètres du réseau	
Interface	Sélectionnez le nom de l'interface de pare-feu qui sera le point d'entrée pour les communications avec les points de terminaison distants et les pare-feu. *N’affectez pas un profil de gestion de l’interface qui autorise Telnet, SSH, HTTP ou HTTPS à une interface sur laquelle vous avez configuré un portail ou une passerelle GlobalProtect, car ce faisant vous exposeriez l’interface de gestion à l’Internet. Reportez-vous à la section* Bonnes pratiques de l'accès administratif *pour obtenir de plus amples précisions sur la manière de protéger l’accès à votre réseau de gestion.*
Adresse IP	Spécifiez l’adresse IP sur laquelle exécuter le service Web du portail GlobalProtect. Sélectionnez le **Type d’adresse IP**, puis saisissez l’**Adresse IP**. • L’adresse IP peut être de type **IPv4** (pour le trafic IPv4 uniquement), **IPv6** (pour le trafic IPv6 uniquement) ou **IPv4 et IPv6**. Utilisez **IPv4 and IPv6 (IPv4 et IPv6)** si votre réseau prend en charge les configurations en double pile, où IPv4 et IPv6 fonctionnent en même temps. • L’adresse IP doit être compatible avec le type d’adresse IP. Par exemple, 172.16.1.0 pour IPv4 ou 21DA:D3:0:2F3b pour IPv6. • Si vous choisissez **IPv4 et IPv6**, saisissez le type d’adresse IP appropriée pour chacun.
Paramètres des journaux	
Journaliser une communication SSL réussie	(En option) Crée des journaux détaillés des communication de décryptage SSL réussies. Cette option est désactivée par défaut.

Paramètres du portail GlobalProtect	Description
	*Les journaux consomment de l'espace de stockage. Avant de journaliser les communications SSL réussies, assurez-vous d'avoir les ressources nécessaires pour stocker les journaux. Modifiez **Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **Logging and Reporting Settings (Paramètres de journalisation et de création de rapports)** pour vérifier l'attribution de mémoire de journaux actuelle et réattribuer de la mémoire de journaux entre les types de journaux.*
Journaliser une communication SSL avortée	Crée des journaux détaillés des communications de décryptage SSL avortées afin que vous puissiez trouver la cause des problèmes de décryptage. Cette option est activée par défaut. *Les journaux consomment de l'espace de stockage. Pour attribuer plus (ou moins) d'espace de stockage de journaux aux journaux de décryptage, modifiez l'attribution de mémoire de journaux (**Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **Logging and Reporting Settings (Journalisation et création de rapports)**).*
Transfert des journaux	Indiquez la méthode et l'emplacement de transfert des journaux (de décryptage) de communication GlobalProtect SSL.
Apparence	
Page de connexion au portail	(Facultatif) Choisissez une page de connexion personnalisée pour l'accès utilisateur au portail. Vous pouvez sélectionner la page **factory-default (remise à zéro «sortie d'usine»)** ou **Import (Importer)** une page personnalisée. La valeur par défaut est **None (Aucun)**. Pour empêcher l'accès à cette page depuis un navigateur Web, vous devez **Désactiver** cette page.
Page d'accueil du portail	(Facultatif) Choisissez une page d'accueil personnalisée pour le portail. Vous pouvez sélectionner la page **factory-default (remise à zéro «sortie d'usine»)** ou **Import (Importer)** une page personnalisée. La valeur par défaut est **None (Aucun)**.
Page d'aide de l'application	(Facultatif) Choisissez une page d'aide personnalisée facultative pour aider l'utilisateur à utiliser GlobalProtect. Vous pouvez sélectionner la page **factory-default (remise à zéro «sortie d'usine»)** ou **Import (Importer)** une page personnalisée. La page d'aide programmée par défaut est fournie avec le logiciel de l'application GlobalProtect. Si vous sélectionnez une page d'aide personnalisée, le portail GlobalProtect fournit la page d'aide

Paramètres du portail GlobalProtect	Description
	avec la configuration du portail GlobalProtect. Lorsque vous laissez la valeur par défaut (**None (Aucune)**), l'application GlobalProtect supprime la page et supprime l'option du menu.

Onglet de Configuration de l'Authentification des portails GlobalProtect

- **Réseau** > **GlobalProtect** > **Portails** > ***<portal-config>*** > **Authentification**

Sélectionnez l'onglet **Authentication (Authentification)** pour configurer les divers paramètres du portail GlobalProtect™ :

- Un profil de service SSL/TLS que le portail et les serveurs utilisent pour l'authentification. Le profil de service est indépendant des autres paramètres d'Authentification.
- Les schémas d'authentification uniques qui sont basés principalement sur le système d'exploitation de l'utilisateur terminal et secondairement sur un profil d'authentification facultatif.
- (Facultatif) Un **Certificate Profile (Profil du certificat)** qui permet à GlobalProtect d'utiliser un profil de certificat spécifique pour authentifier l'utilisateur. Le certificat du client doit correspondre au profil du certificat (si les certificats clients font partie du plan de sécurité).

Paramètres d'authentification du portail GlobalProtect	Description
Authentification du serveur	
Profil de service SSL/TLS	Sélectionnez un profil de service SSL/TLS existant. Le profil indique un certificat et les protocoles autorisés pour protéger le trafic sur l'interface de gestion. Le champ Common Name (nom commun ; CN) et, le cas échéant, le champ Subject Alternative Name (autre nom de l'objet ; SAN) du certificat associé au profil doivent correspondre à l'adresse IP ou au FQDN de l'**Interface** sélectionnée dans l'onglet **General (Général)**. *Dans les configurations VPN GlobalProtect, utilisez un profil associé à un certificat d'une autorité de certification tierce de confiance ou un certificat généré par votre autorité de certification d'entreprise interne.*
Authentification du client	
Name (Nom)	Entrez un nom pour identifier la configuration de l'authentification client. (La configuration de l'authentification du client est indépendante du profil de service SSL/TLS). Vous pouvez créer plusieurs configurations d'authentification client et les différencier par système d'exploitation. Par exemple, vous pouvez ajouter un

Paramètres d’authentification du portail GlobalProtect	Description
	profil d'authentification unique pour les points de terminaison Windows et un autre profil d'authentification pour les points de terminaison macOS. *Bien que vous puissiez ajouter plusieurs configurations d'authentification client pour le même système d'exploitation, le pare-feu sélectionne toujours le profil d'authentification en haut de la liste pour authentifier tous les utilisateurs utilisant ce système d'exploitation spécifique.* Vous pouvez également créer des configurations que GlobalProtect déploie sur les applications en mode **Pre-logon (Préouverture de session)** (c'est-à-dire avant que l'utilisateur ne se connecte au système) ou qu’il applique à n'importe quel utilisateur. (Préouverture de session établit un tunnel VPN à une passerelle GlobalProtect avant que l'utilisateur se connecte à GlobalProtect.)
Système d’exploitation	Pour déployer un profil d’authentification client spécifique sur le système d’exploitation d’un point de terminaison, vous devez **Add (Ajouter)** le système d’exploitation (**Tous**, **Android**, **Chrome**, **iOS**, **Linux**, **Mac**, **Windows** ou **WindowsUWP**). Le système d'exploitation est le différentiateur principal entre les configurations. (Voir le Profil d'Authentification pour une différenciation plus poussée.) Les options additionnelles du **Browser (Navigateur)** et du **Satellite** vous permettent de spécifier le profil d'authentification à utiliser pour des scénarios spécifiques. Sélectionnez **Browser (Navigateur)** pour spécifier le profil d'authentification à utiliser pour authentifier un utilisateur accédant au portail à partir d'un navigateur Web avec l'intention de télécharger l'application GlobalProtect (Windows et Mac). Sélectionnez **Satellite** pour spécifier le profil d'authentification à utiliser pour authentifier le satellite (LSVPN).
Profil d'authentification	En plus de distinguer une configuration d'authentification de client par le système d'exploitation, vous pouvez différencier davantage en spécifiant un profil d'authentification. (Vous pouvez créer un **New Authentication Profile (Nouveau profil d'authentification)** ou en sélectionnez un existant.) Pour configurer plusieurs options d'authentification pour un système d'exploitation, vous pouvez créer plusieurs profils d'authentification de client. *Si vous configurez un LSVPN dans **Gateways (Passerelles)**, vous ne pouvez pas enregistrer cette configuration sauf si vous sélectionnez un profil d'authentification ici. Aussi, si vous envisagez d'utiliser des numéros de série pour authentifier les satellites, le portail doit avoir un profil d'authentification disponible quand il ne peut pas localiser ou valider un numéro de série de pare-feu.*

Paramètres d’authentification du portail GlobalProtect	Description
	Voir également Périphérique > Profil d’authentification.
Étiquette de nom d’utilisateur	Indiquez une étiquette de nom d’utilisateur personnalisée pour la connexion au portail GlobalProtect. Par exemple, **Nom d’utilisateur (uniquement)** ou **Adresse électronique (nomd’utilisateur@domaine)**.
Étiquette de mot de passe	Indiquez une étiquette de mot de passe personnalisée pour la connexion au portail GlobalProtect. Par exemple, **Mot de passe (Turc)** ou **Code secret** (pour l’authentification basée sur jeton à deux facteurs).
Message d'authentification	Pour aider les utilisateurs finaux à connaître le type d'informations dont ils ont besoin pour se connecter, entrez un message ou gardez le message par défaut. La longueur est de 256 caractères maximum.
Permettre l’authentification avec les informations d'identification de l'utilisateur OU le certificat du client	Si vous sélectionnez **No (Non)**, les utilisateurs doivent s’authentifier auprès de la passerelle en utilisant les informations d'identification de l'utilisateur et les certificats de client. Si vous sélectionnez **Yes (Oui)**, les utilisateurs peuvent s’authentifier auprès de la passerelle en utilisant les informations d'identification de l'utilisateur ou les certificats de client.
Profil du certificat	
Profil du certificat	(Facultatif) Sélectionnez le **Certificate Profile (Certificat du profil)** que le portail utilise pour correspondre aux certificats clients qui viennent des extrémités utilisateur. Avec un Profil du certificat, le portail n'authentifie l'utilisateur que si le certificat du client correspond à ce profil. Si vous établissez l’option **Allow Authentication with User Credentials OR Client Certificate (Permettre l’authentification avec les informations d'identification de l'utilisateur OU le certificat du client)** sur **No (Non)**, vous devez sélectionner un **Certificate Profile (Profil de certificat)**. Si vous établissez l’option **Allow Authentication with User Credentials OR Client Certificate (Permettre l’authentification avec les informations d'identification de l'utilisateur OU le certificat du client)** sur **Yes (Oui)**, le **Certificate Profile (Profil de certificat)** est facultatif. Le profil de certificat est indépendant du système d'exploitation. En outre, ce profil est actif même si vous activez Contournement d’authentification, qui remplace le Profil d’authentification pour permettre l’authentification en utilisant des témoins chiffrés.

Onglet Collecte de données du portail GlobalProtect

Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Portals (Portails)** > **<portal-config>**Portal Data Collection (Collecte de données du portail) pour définir les données que l’application GlobalProtect

collecte des points de terminaison et pour envoyer les données des critères de sélection de configuration après la connexion des utilisateurs au portail.

Paramètres de collecte de données du portail GlobalProtect	Description
Profil du certificat	Sélectionnez le profil de certificat que le portail GlobalProtect utilise pour apparier le certificat de machine envoyé par l'application GlobalProtect.
Vérifications personnalisées	Définissez les informations personnalisées sur l'hôte que l'application doit collecter : • **Windows** : **Add (Ajouter)** pour ajouter une vérification d'une clé de registre et/ou d'une valeur de clé particulière. • **Mac** : **Add (Ajouter)** pour ajouter une vérification d'une clé plist ou d'une valeur de clé particulière.

Onglet GlobalProtect Portals Agent (Agent des portails GlobalProtect)

- **Réseau** > **GlobalProtect** > **Portails** > **<*portal-config*>** > **Agent**

Sélectionnez l'onglet **Agent** pour définir les paramètres de configuration de l'agent. Le portail GlobalProtect déploie la configuration de l'appareil une fois que la connexion est établie en premier.

Vous pouvez également spécifier que le portail déploie automatiquement les certificats de l'autorité de certification (CA) et les certificats intermédiaires. Si les terminaux ne font pas confiance aux certificats de serveur que les passerelles GlobalProtect et GlobalProtect Mobile Manager Security utilisent, les terminaux ont besoin de ces certificats pour établir des connexions HTTPS aux passerelles ou Mobile Security Manager. Le portail pousse les certificats que vous spécifiez ici au client avec la configuration du client.

Pour ajouter un certificat AC de racine de confiance, **Add (Ajouter)** un certificat existant ou **Import (Importer)** un nouveau. Pour installer (transparent) les certificats CA de la racine de confiance qui sont nécessaires pour le décryptage du proxy de transfert SSL dans le magasin de certificats du client, sélectionnez **Install in Local Root Certificate Store (Installer dans le magasin de certificats de la racine locale)**.

Spécifiez le certificat CA racine de confiance que l'application GlobalProtect utilise pour vérifier l'identité du portail et des passerelles GlobalProtect. Si le portail ou la passerelle présente un certificat qui n'a pas été signé ou émis par la même autorité de certification qui a émis la CA racine de confiance, l'applcation GlobalProtect ne peut établir de connexion avec le portail ou la passerelle.

Si vous disposez de différents types d'utilisateurs qui requièrent différentes configurations, vous pouvez créer des configurations d'agent séparées pour les appuyer. Le portail utilise ensuite le nom d'utilisateur ou de groupe et/ou le système d'exploitation du client pour déterminer la configuration de l'agent à déployer. Comme avec les évaluations des règles de sécurité, le portail recherche une

correspondance en commençant par le sommet de la liste. Lorsque le portail trouve une correspondance, il fournit la configuration correspondante à l'application. Par conséquent, si vous disposez de plusieurs configurations d'agents, il est important de les ordonner de manière à ce que les configurations plus spécifiques (c'est-à-dire les configurations pour certains utilisateurs ou systèmes) soient au-dessus des configurations plus génériques. Utilisez les boutons **Move Up (Monter)** et **Move Down (Descendre)** pour réordonner les configurations. Au besoin, **Add (Ajouter)** une nouvelle configuration de l'agent. Pour plus d'informations sur la configuration du portail et la création de configurations d'agent, reportez-vous à Portails GlobalProtect dans le Guide de l'administrateur de GlobalProtect. Lorsque vous souhaitez **Add (Ajouter)** une nouvelle configuration d'agent ou modifier une configuration existante, la fenêtre **Configurations** s'ouvre et affiche cinq onglets, qui sont décrits dans les tableaux suivants :

- Onglet Authentification de l'agent des portails GlobalProtect
- Onglet des Critères de sélection de la configuration de l'agent des portails GlobalProtect
- Onglet Agent interne des portails GlobalProtect
- Onglet Agent externe des portails GlobalProtect
- Onglet Application de l'agent des portails GlobalProtect
- Onglet Collecte de données HIP de l'agent des portails GlobalProtect

Onglet Authentification de l'agent des portails GlobalProtect

- **Réseau** > **GlobalProtect** > **Portails** > ***<portal-config>*** > **Agent** > ***<agent-config>*** > **Authentification**

Sélectionnez l'onglet **Authentication (Authentification)** pour configurer les paramètres d'authentification qui s'appliquent à la configuration de l'agent.

Paramètres de configuration du portail client GlobalProtect	Description
Onglet Authentification	
Name (Nom)	Entrez un nom descriptif pour cette configuration pour l'authentification du client.
Certificat du client	(Facultatif) Sélectionnez la source qui distribue le certificat client à un point de terminaison, qui présente ensuite le certificat aux passerelles. Un certificat client est nécessaire si vous configurez l'authentification SSL mutuelle. *Si vous incluez un certificat client dans la configuration du portail pour appareils mobiles, vous ne pouvez utiliser l'authentification par certificat client que dans la configuration de la passerelle car la phrase secrète du certificat client est enregistrée dans la configuration du portail. De plus, le certificat client ne peut être utilisé qu'une fois le certificat récupéré à partir de la configuration du portail.*

Paramètres de configuration du portail client GlobalProtect	Description
	Si SCEP est configuré pour la pré-connexion dans la configuration du client portail, le portail génère un certificat de la machine qui est stocké dans le magasin de certificats du système pour l'authentification et les connexions de la passerelle. Pour utiliser un certificat **Local** du pare-feu plutôt qu'un certificat généré par le PKI via **SCEP,** sélectionnez un certificat qui est déjà téléchargé sur le pare-feu. Si vous utilisez une autorité de certification interne pour distribuer les certificats aux points de terminaison, sélectionnez **None (Aucun)** (par défaut). Lorsque vous sélectionnez **None (Aucun)**, le portail ne pousse pas un certificat au point de terminaison.
Enregistrer les informations d'identification de l'utilisateur	Sélectionnez **Yes (Oui)** pour enregistrer le nom d'utilisateur et le mot de passe sur l'application ou sélectionnez **No (Non)** pour forcer les utilisateurs à fournir le mot de passe soit de manière transparente via le point de terminaison ou en le saisissant manuellement à chaque fois qu'ils se connectent. Sélectionnez **Save Username Only (Enregistrer nom d'utilisateur seulement)** pour enregistrer seulement le nom d'utilisateur à chaque fois qu'un utilisateur se connecte. Sélectionnez **Only with User Fingerprint (Uniquement à partir de l'empreinte digitale de l'utilisateur)** pour permettre l'ouverture de session avec ses données biométriques. Lorsque l'option d'ouverture de session avec empreintes digitales est activée sur un terminal, GlobalProtect utilise les informations d'identification enregistrées de l'utilisateur lorsque le balayage de l'empreinte digitale correspond à une empreinte digitale de confiance sur le terminal. *N'enregistrez pas les informations d'identification de l'utilisateur, car il pourrait alors être plus facile pour les utilisateurs non autorisés d'obtenir accès à des ressources sensibles et à des informations confidentielles. Les utilisateurs doivent manuellement saisir leurs informations d'identification chaque fois qu'ils se connectent à GlobalProtect.*
Contournement d'Authentification	
Générer le témoin pour le contournement de l'authentification	Sélectionnez cette option pour configurer le portail pour qu'il génère des témoins spécifiques terminaux chiffrés. Le portail

Paramètres de configuration du portail client GlobalProtect	Description
	envoie ce témoin au terminal après que l'utilisateur se soit authentifié une première fois avec le portail.
Accepter le témoin pour le contournement de l'authentification	Sélectionnez cette option pour configurer le portail pour authentifier les points de terminaison par le biais d'un témoin crypté valide. Lorsque le terminal présente un témoin valide, le portail vérifie que le témoin a été chiffré par le portail, déchiffre le témoin, puis authentifie l'utilisateur.
Durée de vie du témoin	Spécifiez les heures, les jours ou les semaines pour lesquelles le témoin est valide. La durée de vie typique est de 24 heures. Les plages sont 1 à 72 heures, 1 à 52 semaines ou 1 à 365 jours. Après l'expiration du témoin, l'utilisateur doit entrer les informations de connexion et le portail encrypte ensuite un nouveau témoin à envoyer à l'utilisateur terminal.
Certificat pour chiffrer/déchiffrer le témoin	Sélectionnez le certificat à utiliser pour chiffrer et déchiffrer le témoin. *Veiller à ce que le portail et les passerelles utilisent le même certificat pour chiffrer et déchiffrer les témoins. (Configurer le certificat dans le cadre d'une configuration d'une passerelle client. Voir Réseau > GlobalProtect > Passerelles).*
Composants nécessitant des mots de passe dynamiques (Authentification à deux facteurs)	
Pour configurer GlobalProtect afin qu'il supporte les mots de passe dynamiques, tels que les mots de passe à usage unique (OTP), spécifier les types de portail ou de passerelles qui requièrent que les utilisateurs saisissent des mots de passe dynamiques. Lorsque l'authentification à deux facteurs n'est pas activée, GlobalProtect utilise l'authentification régulière en utilisant les informations de connexion (tels que AD) et un certificat. Lorsque vous activez un portail ou un type de passerelle pour l'authentification à deux facteurs, ce portail ou cette passerelle invite l'utilisateur, après l'authentification initiale du portail, à présenter des informations d'identification et un second OTP (ou un autre mot de passe dynamique). Toutefois, si vous activez également le contournement d'authentification, un témoin crypté est utilisé pour authentifier l'utilisateur (après que l'utilisateur se soit d'abord authentifié pour une nouvelle session) et, par conséquent, est prioritaire sur l'obligation de ré-entrer les informations d'identification (aussi longtemps que le témoin est valide). Par conséquent, l'utilisateur est connecté de manière transparente à chaque fois que nécessaire tant que le témoin est valide. Vous spécifiez la durée de vie du témoin.	
Portail	Sélectionnez cette option pour utiliser les mots de passe dynamiques pour se connecter au portail.

Paramètres de configuration du portail client GlobalProtect	Description
Passerelles internes - tout	Sélectionnez cette option pour utiliser les mots de passe dynamiques pour se connecter à des passerelles internes.
Passerelles externes – manuelles uniquement	Sélectionnez cette option pour utiliser les mots de passe dynamiques pour se connecter à des passerelles externes qui sont configurées en tant que passerelles **Manual (Manuel)**.
Passerelles externes – détection automatique	Sélectionnez cette option pour utiliser les mots de passe dynamiques pour se connecter à toute passerelle externe restante que l'application peut automatiquement découvrir (passerelles qui ne sont pas configurées en tant que **Manual (Manuelle)**).

Onglet des Critères de sélection de la configuration de l’agent des portails GlobalProtect

- **Réseau** > **GlobalProtect** > **Portails** > **<*portal-config*>** > **Agent** > **<*agent-config*>** > **Critères de sélection de configuration**

Sélectionnez l’onglet **Config Selection Criteria (Critères de sélection de la configuration)** pour configurer les critères de correspondance utilisés pour identifier le type de point de terminaison dans les déploiements ayant des points de terminaison gérés et non gérés. Le portail peut transmettre des configurations spécifiées au point de terminaison selon le type de point de terminaison.

Paramètres des critères de sélection de la configuration du portail GlobalProtect	Description
Onglet Utilisateur/Groupe d'utilisateurs	
Système d’exploitation	**Add (Ajoutez)** un ou plusieurs systèmes d’exploitation (OS) de point de terminaison pour spécifier les points de terminaison qui reçoivent cette configuration. Le portail apprend automatiquement le système d'exploitation du point de terminaison et intègre les détails de ce système d'exploitation dans la configuration du client. Vous pouvez sélectionner **Any (Tous)** les systèmes d’exploitation ou un système d’exploitation spécifique (**Android**, **Chrome**, **iOS**, **IoT [IdO]**, **Linux**, **Mac**, **Windows** ou **WindowsUWP**).
Utilisateur/Groupe d'utilisateurs	**Add (Ajouter)** les groupes d'utilisateurs ou les utilisateurs spécifiques auxquels cette configuration s’applique.

Paramètres des critères de sélection de la configuration du portail GlobalProtect	Description
	*Vous devez configurer le mappage de groupe (**Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Group Mapping Settings (Paramètres de mappage des groupes)**) avant de pouvoir sélectionner les groupes d'utilisateurs.* Pour déployer cette configuration à tous les utilisateurs, sélectionnez **any (indifférent)** dans le menu déroulant **User/User Group (Utilisateur/Groupe d'utilisateurs)**. Pour déployer cette configuration uniquement aux utilisateurs disposant d'applications GlobalProtect en mode préouverture de session, sélectionnez **pre-logon (préouverture de session)** dans le menu déroulant **User/User Group (Utilisateur/Groupe d'utilisateurs)**.
Vérifications des périphériques	
Le compte machine existe avec le numéro de série du périphérique,	Configurez les critères de correspondance en fonction de l'existence du numéro de série du point de terminaison dans Active Directory.
Profil du certificat	Sélectionnez le profil de certificat que le portail GlobalProtect utilise pour apparier le certificat de machine envoyé par l'application GlobalProtect.
Vérifications personnalisées	
Vérifications personnalisées	Sélectionnez cette option pour définir les informations personnalisées sur l'hôte à faire correspondre.
Clé de registre	Pour rechercher une clé de registre spécifique sur les points de terminaison Windows, **Add (Ajoutez)** la **Registry Key (Clé de registre)** pour effectuer la mise en correspondance. Pour faire correspondre uniquement les points de terminaison qui ne disposent pas de la clé de registre spécifiée ou de la valeur de la clé, activez l'option **Key does not exist or match the specified value data (La clé n'existe pas ou ne correspond pas aux données de la**

Paramètres des critères de sélection de la configuration du portail GlobalProtect	Description
	valeur définies). Pour la mise en correspondance avec des valeurs spécifiques, **Add (Ajoutez)** la **Registry Value (Valeur de registre)** et les **Value Data (Données de la valeur)**. Pour faire correspondre les points de terminaison qui n'ont pas la valeur de Registre spécifiée, sélectionnez **Negate (Annuler)**. Lorsque vous sélectionnez l'option **Negate (Annuler)** vous devez laisser le champ **Value data (Données de la valeur)** vide. Vous pouvez sélectionner l'option **Negate (Annuler)** pour une valeur de Registre dans Vérifications personnalisées dans le portail GlobalProtect qui n'a pas la valeur de Registre spécifiée (correspondant à l'absence de valeur de Registre). *Si vous configurez une valeur de Registre avec l'option **Negate (Annuler)** et laissez le champ **Value Data (Données de la valeur)** vide, **Negate (Annuler)** fonctionne sur la valeur de Registre.L'option **Negate (Annuler)** et la correspondance des **Value Data (données de valeur)** s'excluent mutuellement et vous ne pouvez pas configurer l'option **Value Data (Données de la valeur)** et l'option **Negate (Annuler)** ensemble.*
Plist	Pour rechercher une entrée spécifique dans la Property List (plist) sur les points de terminaison macOS, **Add (Ajoutez)** le nom du **Plist**. Pour la mise en correspondance uniquement avec les points de terminaison qui ne disposent pas du plist spécifié, activez l'option **Plist does not exist (Le plist n'existe pas)**. Pour la mise en correspondance avec des paires de valeurs de clé spécifiques dans la plist, **Add (Ajoutez)** la **Key (Clé)** et la **Value (Valeur)** correspondante. Pour la mise en correspondance avec les points de terminaison qui ne disposent clairement pas de la clé ou de la valeur spécifiée, cochez la case **Negate (Ignorer)**

Onglet Agent interne des portails GlobalProtect

- **Réseau** > **GlobalProtect** > **Portails** > ***<portal-config>*** > **Agent** > ***<agent-config>*** > **Interne**

Sélectionnez l’onglet **Internal (Interne)** pour configurer les paramètres de la passerelle interne pour une configuration d’agent.

Paramètres internes du portail GlobalProtect	Description
Détection d'hôte interne	
Détection d'hôte interne	Sélectionnez cette option pour permettre à l'application GlobalProtect de déterminer si elle est à l'intérieur du réseau d'entreprise. Cela s'applique aux points de terminaison lorsqu'un tunnel n'est pas requis dans le réseau d'entreprise ou lorsque les points de terminaison sont configurés pour communiquer avec des passerelles internes. Le choix de la fonction de détection d'hôte interne est une bonne pratique pour ces points de terminaison. La configuration des passerelles internes est cependant facultative. Lorsque l'utilisateur tente de se connecter, l'application effectue une recherche DNS inversée d'un hôte interne en utilisant le **Hostname (Nom d'hôte)** spécifié à l'**IP Address (Adresse IP)** spécifiée. L'hôte sert de point de référence qui n'a pas besoin d'être accessible, mais la recherche DNS inversée ne devrait réussir que lorsque le point de terminaison se trouve à l'intérieur du réseau de l'entreprise. Si l'application trouve l'hôte, le point de terminaison se trouve à l'intérieur du réseau et l'application se connecte à une passerelle interne, si elle est configurée, ou l'application GlobalProtect affiche l'état de la connexion comme interne. Si l'application ne parvient pas à trouver l'hôte interne, le point de terminaison se trouve en dehors du réseau et l'application établit un tunnel vers l'une des passerelles externes. • L’adresse IP peut être de type **IPv4** (trafic IPv4 uniquement), **IPv6** (trafic IPv6 uniquement) ou les deux. Utilisez **IPv4** et **IPv6** si votre réseau prend en charge les configurations en double pile, où IPv4 et IPv6 fonctionnent en même temps. • L’adresse IP doit être compatible avec le type d’adresse IP. Par exemple, 172.16.1.0 pour IPv4 ou 21DA:D3:0:2F3b pour IPv6. • Si vous choisissez **IPv4** et **IPv6,** saisissez le type d’adresse IP appropriée pour chacun.
Nom d'hôte	Saisissez le **Hostname (Nom d'hôte)** permettant de résoudre l'adresse IP ci-dessus sur le réseau interne.
Passerelles internes	
Spécifiez les passerelles internes auxquelles une application peut	**Add (Ajouter)** les passerelles internes qui comprennent les informations suivantes pour chacune :

Paramètres internes du portail GlobalProtect	Description
demander l’accès et également fournir des rapports de HIP (si HIP est activé à l’onglet Collecte de données de l’agent des portails GlobalProtect).	• **Name (Nom)** – Étiquette de 31 caractères maximum permettant d'identifier la passerelle. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement. • **Address (Adresse)** – L'adresse IP ou le nom de domaine complet (FQDN) de l'interface pare-feu pour la passerelle. Cette valeur doit correspondre au nom commun (CN) et SAN (si spécifié) dans le certificat de serveur de passerelle. Par exemple, si vous avez utilisé un FQDN pour générer le certificat, vous devez entrer le nom de domaine complet (FQDN) ici. • **Source Address (Adresse source)** – Une adresse source ou un pool d’adresses pour les points de terminaison. Lorsque les utilisateurs se connectent, GlobalProtect reconnaît l’adresse source du périphérique. Seules les applications GlobalProtect dont les adresses IP sont incluses dans le pool d’adresses source peuvent s’authentifier auprès de cette passerelle et envoyer des rapports HIP. • **DHCP Option 43 Code (Code 43 option DHCP)** (Windows et Mac uniquement) – Les codes de sous-options DHCP pour la sélection de la passerelle. Spécifiez un ou plusieurs codes de sous-options (en décimal). L’application GlobalProtect lit l’adresse de la passerelle à partir des valeurs définies par les codes de sous-options.

Onglet Agent externe des portails GlobalProtect

- **Réseau** > **GlobalProtect** > **Portails** > *<**portal-config**>* > **Agent** > *<**agent-config**>* > **Plate-forme**

Sélectionnez l’onglet **External (Externe)** pour configurer les paramètres de la passerelle externe pour une configuration d’agent.

Paramètres externes du portail GlobalProtect	Description
Heure limite (sec)	Indiquez le nombre de secondes qu'une application attend que toutes les passerelles disponibles répondent avant de sélectionner la meilleure passerelle. Pour les demandes de connexion ultérieures, l'application tente de se connecter uniquement aux passerelles qui ont répondu avant la coupure. Une valeur de 0 signifie que l’application utilise le **TCP Connection Timeout (Délai d’expiration de connexion TCP)** dans la **AppConfigurations (Configuration des applications)** de l’onglet **App (Application)** (la plage est comprise entre 0 et 10 ; 5 par défaut).
Passerelles externes	
Spécifiez la liste des pare-feu pour lesquels	**Add (Ajouter)** des passerelles externes qui comprennent les informations suivantes pour chacune :

Paramètres externes du portail GlobalProtect	Description
les applications peuvent essayer de se connecter lors de l'établissement d'un tunnel alors qu'elles ne sont pas sur le réseau d'entreprise.	• **Name (Nom)** – Étiquette de 31 caractères maximum permettant d'identifier la passerelle. Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement. • **Address (Adresse)** – L’adresse IP ou le nom de domaine complet (FQDN) où la passerelle est configurée. Cette valeur doit correspondre au nom commun (CN) et SAN (si spécifié) dans le certificat de serveur de passerelle. Par exemple, si vous avez utilisé un FQDN pour générer le certificat, vous devez également saisir le nom de domaine complet (FQDN) ici. • **Source Region (Région source)** – Région source pour les points de terminaison. Lorsque les utilisateurs se connectent, GlobalProtect reconnaît la région du point de terminaison et permet aux utilisateurs de se connecter uniquement aux passerelles configurées pour cette région. En ce qui concerne les choix de passerelle, la région source est considérée en premier, suivie par la passerelle. • **Priority (Priorité)** – Sélectionnez une valeur (**Highest (La plus élevée)**, **High (Élevée)**, **Medium (Moyenne)**, **Low (Faible)**, **Lowest (La plus faible)** ou **Manual only (Manuel uniquement)**) pour permettre à l'application de déterminer la passerelle à utiliser. **Manual only (Manuel uniquement)** empêche l’application GlobalProtect de tenter de se connecter à cette passerelle lorsque la **Détection automatique** est activée sur le point de terminaison. L’application commencera par contacter toutes les passerelles marquées d’une priorité **Highest (Absolue)**, **High (Élevée)** ou **Medium (Moyenne)** et établira un tunnel avec la passerelle qui répond le plus rapidement. Si les passerelles ayant la priorité la plus élevée sont inaccessibles, l’application contacte ensuite les autres passerelles qui possèdent des valeurs de priorité inférieures (elle exclut les passerelles **Manual only (Manuel uniquement)**). • **Manual (Manuel)** – Sélectionnez cette option pour permettre aux utilisateurs de sélectionner manuellement (ou basculer vers) une passerelle. L'application GlobalProtect peut se connecter à n'importe quelle passerelle externe pour laquelle l'option **Manual (Manuel)** est configurée. Lorsque l'application se connecte à une autre passerelle, le tunnel existant est déconnecté et un nouveau tunnel est établi. Les passerelles manuelles peuvent également proposer des méthodes d'authentification différentes de celles de la passerelle principale. Si un point de terminaison est redémarré ou si une nouvelle découverte est exécutée, l'application GlobalProtect se connecte à la passerelle principale. Cette fonction est utile si un groupe d'utilisateurs doit se connecter temporairement à une passerelle spécifique afin d'accéder à un segment sécurisé de votre réseau.
VPN tiers	

Paramètres externes du portail GlobalProtect	Description
VPN tiers	Pour indiquer à l'application GlobalProtect d'ignorer les clients VPN tierce partie sélectionnés, afin que GlobalProtect ne soit pas en conflit avec eux, **Add (Ajouter)** le nom du client VPN : Sélectionnez le nom de la liste, ou entrez le nom dans le champ prévu. GlobalProtect ignore les paramètres d'itinéraire pour les clients VPN spécifiés si vous configurez cette fonctionnalité.

Onglet Application de l’agent des portails GlobalProtect

- **Réseau** > **GlobalProtect** > **Portails** > ***<portal-config>*** > **Agent** > ***<agent-config>*** > **Appli**

Sélectionnez l’onglet **App (Appliquer)** pour définir comment les utilisateurs finaux interagissent avec les applications GlobalProtect installées sur leurs systèmes. Vous pouvez définir différents paramètres d'application pour les différentes configurations d'agent GlobalProtect que vous avez créées. Consultez le GlobalProtect Administrator’s Guide (Guide de l’administrateur GlobalProtect) pour en savoir plus sur les dernières mises à jour des paramètres de GlobalProtect App Customization (Personnalisation de l’application GlobalProtect).

Paramètres de configuration de l’application GlobalProtect	Description
Page d’accueil	Sélectionnez une page d'accueil à afficher aux utilisateurs finaux lors d'une connexion à GlobalProtect. Vous pouvez sélectionner la page **factory-default (par défaut)** ou **Import (Importer)** une page personnalisée. La valeur par défaut est **None (Aucun)**.
Configurations d'application	
Méthode de connexion	• **On-demand (Manual user initiated connection) (Sur demande (Connexion initiée manuellement par l'utilisateur))** – Les utilisateurs doivent lancer l'application GlobalProtect, puis initier une connexion au portail et entrer leurs informations d'identification GlobalProtect. Cette option est principalement utilisée pour les connexions d'accès à distance. • **Connexion-Utilisateur (Toujours Activée)** : L'application GlobalProtect établit automatiquement une connexion au portail après que l'utilisateur se connecte à un terminal. Le portail répond en fournissant à l’application la configuration de l'agent appropriée. Par la suite, l’application met en place un tunnel vers l’une des passerelles spécifiées dans la configuration de l’agent qu’il a reçue du portail.

Paramètres de configuration de l’application GlobalProtect	Description
	• **Pre-logon (Pré-ouverture de session)** – La pré-ouverture de session garantit que les utilisateurs distants de Windows et Mac sont toujours connectés au réseau d’entreprise et active les scripts d’ouverture de session utilisateur et l’application de règles de domaine lorsque l’utilisateur se connecte au terminal. Étant donné que le terminal peut se connecter au réseau d’entreprise comme s’il était interne, les utilisateurs peuvent se connecter avec de nouveaux mots de passe lorsque leurs mots de passe expirent ou recevoir une aide pour la récupération de mot de passe s’ils oublient leur mot de passe. Avec la préouverture de session, l’application GlobalProtect établit un tunnel VPN vers une passerelle GlobalProtect avant que l’utilisateur se connecte au terminal ; le terminal demande l’authentification en soumettant un certificat de machine pré-installé à la passerelle. Ensuite, sur les terminaux Windows, la passerelle réaffecte le tunnel VPN depuis l’utilisateur de la pré-ouverture de session vers le nom d’utilisateur connecté au terminal. Sur les terminaux Mac, l’application procède à sa déconnexion et crée un nouveau tunnel VPN pour l’utilisateur. Il existe deux méthodes de pré-ouverture de session, dont chacune permet la même fonctionnalité de pré-ouverture de session qui se déroule avant que les utilisateurs ne se connectent au terminal. Cependant, après la connexion des utilisateurs au terminal, c’est la méthode de pré-ouverture de session qui détermine le moment où la connexion de l’application GlobalProtect est établie : • **Pre-logon (Always On) (Pré-ouverture de session (Toujours activée))** – L’application GlobalProtect tente automatiquement de se connecter et de se reconnecter aux passerelles GlobalProtect. Les périphériques mobiles ne prennent pas en charge les fonctionnalités de pré-ouverture de session et utilisent par conséquent la méthode de connexion **User-logon (Always On) (Connexion utilisateur (Toujours activée))** par défaut, si cette méthode de connexion est spécifiée. • **Pre-logon then On-demand (Pré-ouverture de session puis À la demande)** – Les utilisateurs doivent lancer l’application GlobalProtect, puis établir la connexion manuellement. Les périphériques mobiles ne prennent pas en charge les fonctionnalités de pré-ouverture de session et utilisent par conséquent la méthode de connexion **À la demande (Connexion**

Paramètres de configuration de l’application GlobalProtect	Description
	initiée manuellement par l’utilisateur) par défaut, si cette méthode de connexion est spécifiée.
Intervalle de rafraîchissement de configuration de l'application GlobalProtect (en heures)	Indiquez le nombre d’heures que le portail GlobalProtect attend avant la prochaine actualisation de la configuration d’une application (plage comprise entre 1 et 168 ; 24 par défaut).
Autoriser l'utilisateur à désactiver GlobalProtect App	Indique si les utilisateurs sont autorisés à désactiver l'application GlobalProtect et, si oui, lequel, le cas échéant, ils doivent désactiver avant de pouvoir désactiver l'application : • **Allow (Autoriser)** – Permettre à tout utilisateur de désactiver l'application GlobalProtect au besoin. • **Disallow (Ne pas autoriser)** – Ne pas permettre aux utilisateurs finaux de désactiver l'application GlobalProtect. • **Allow with Comment (Permettre avec commentaire)** – Permettre aux utilisateurs de désactiver l'application GlobalProtect sur leur terminal, mais exiger qu'ils indiquent la raison de la désactivation de l'application. L’application GlobalProtect invite l’utilisateur à : • Spécifiez la raison de la déconnexion de l’application. • Choisissez la raison dans la liste affichée, telle que la vitesse Internet lente ou la latence. *Les raisons de la déconnexion ne s'affichent que si vous configurez **Display the following reasons to disconnect GlobalProtect (Always-on mode) (Afficher les raisons suivantes pour déconnecter GlobalProtect (mode toujours activé))**. Si vous n'avez pas configuré l'application GlobalProtect pour afficher les raisons de la déconnexion, les utilisateurs finaux sont invités à fournir une raison pour se déconnecter de l'application.* • **Allow with Passcode (Permettre avec code secret)** – Permettre aux utilisateurs d'entrer un code secret pour désactiver l'application GlobalProtect. Cette option nécessite que l'utilisateur entre et confirme une valeur de Code Secret qui, comme un mot de passe, ne s'affiche pas lorsque saisie. En règle générale, les administrateurs fournissent un mot de passe aux utilisateurs avant que des événements non planifiés ou imprévus empêchent les

Paramètres de configuration de l’application GlobalProtect	Description
	utilisateurs de se connecter au réseau en utilisant le VPN GlobalProtect. Vous pouvez fournir le mot de passe par e-mail ou l’afficher sur le site Web de votre organisation. • **Allow with Ticket (Permettre avec ticket)** – Cette option active un mécanisme basé sur le temps de réponse dans lequel, après qu'un utilisateur tente de désactiver GlobalProtect, le terminal affiche un numéro de requête hexadécimal de 8 caractères. L'utilisateur doit contacter l'administrateur ou l'équipe de soutien du pare-feu (de préférence par téléphone par mesure de sécurité) afin de lui fournir ce numéro. À partir du pare-feu (**Network (Réseau)** > **GlobalProtect** > **Portals (Portails)**), l’administrateur ou la personne responsable du soutien peut alors cliquer sur **Generate Ticket (Générer le ticket)**, puis entrer le numéro de **Request (requête)** de ticket pour obtenir le numéro de **Ticket** (également un numéro hexadécimal de 8 caractères). L'administrateur ou la personne responsable du soutien fournit ce numéro de ticket à l'utilisateur qui l’entre alors dans le champ de réponse pour désactiver l'application.
Autoriser l’utilisateur à désinstaller l’application GlobalProtect (Windows uniquement)	Indique si les utilisateurs sont autorisés à désinstaller l'application GlobalProtect et, si oui, que doivent-ils faire, le cas échéant, avant de pouvoir désinstaller l'application : • **Allow (Autoriser)** – Permettre à tout utilisateur de désinstaller l'application GlobalProtect au besoin. • **Disallow (Ne pas autoriser)** – Ne pas permettre aux utilisateurs finaux de désinstaller l'application GlobalProtect. • **Allow with Password (Autoriser avec un mot de passe)** - Imposer un mot de passe pour désinstaller l’application GlobalProtect. Cette option nécessite que l’utilisateur saisit et confirme un mot de passe avant de pouvoir procéder à la désinstallation. Vous pouvez fournir le mot de passe par e-mail ou l’afficher sur le site Web de votre organisation. Cette option nécessite la version de contenu 8196-5685 ou toute version ultérieure.
Permettre à l'utilisateur de mettre à niveau l'app GlobalProtect	Indique si les utilisateurs finaux peuvent mettre à niveau le logiciel de l’application GlobalProtect et, s'ils le peuvent, s'ils peuvent choisir le moment de la mise à niveau : • **Disallow (Désactiver)** – Empêche les utilisateurs de mettre à niveau le logiciel de l’application.

Paramètres de configuration de l’application GlobalProtect	Description
	• **Allow Manually (Autoriser manuellement)** – Autoriser les utilisateurs à vérifier manuellement les mises à niveau et à les lancer en sélectionnant **Check Version (Vérifier Version)** dans l'application GlobalProtect. • **Allow with Prompt (Autoriser avec invite)** (par défaut) – Invite les utilisateurs lorsqu’une nouvelle version est activée sur le pare-feu et permet aux utilisateurs de mettre à niveau leur logiciel lorsqu’ils le souhaitent. • **Allow Transparently (Permettre avec transparence)** – Met automatiquement à niveau le logiciel de l'application lorsqu'une nouvelle version est disponible sur le portail. • **Internal (Interne)** – Mettre automatiquement à niveau le logiciel de l’application chaque fois qu’une nouvelle version est disponible sur le portail. Cependant, vous devez attendre que le terminal soit connecté en interne au réseau de l’entreprise. Cela empêche les retards causés par les mises à niveau sur les connexions à bande passante étroite.
Allow User to Sign Out from GlobalProtect App (Autoriser l’utilisateur à se déconnecter de l’application GlobalProtect) (Windows, macOS, iOS, Android et Chrome uniquement)	Indique si les utilisateurs sont autorisés à se déconnecter manuellement de l’application GlobalProtect : • **Yes (Oui)** – Permettre à tout utilisateur de se déconnecter de l'application GlobalProtect au besoin. • **No (Non)** – Ne pas permettre aux utilisateurs finaux de se déconnecter de l'application GlobalProtect. Cette option nécessite la version de contenu 8196-5685 ou toute version ultérieure.
Utiliser l’ouverture de session unique (Windows)	Sélectionnez **No (Non)** pour désactiver l'authentification unique (SSO). Avec l'ouverture de session unique, l'application GlobalProtect utilise automatiquement les informations d'identification pour s'authentifier et ensuite se connecter au portail et à la passerelle GlobalProtect. GlobalProtect peut également englober des informations d'identification indépendantes afin de garantir l'authentification et la connexion des utilisateurs Windows, même si un fournisseur d'informations d'identification indépendantes est utilisé pour englober les informations d'identification de connexion Windows.
Utiliser l'authentification unique pour la carte à puce (Windows uniquement) (Windows 10 or later (Windows 10 ou version ultérieure))	Utilisez ce paramètre pour permettre aux utilisateurs finaux qui s’authentifient via l’authentification unique (SSO) à l’aide d’une carte à puce de se connecter sans avoir à entrer à nouveau leur numéro d’identification personnel (PIN) de carte à puce dans l’application GlobalProtect pour une

Paramètres de configuration de l’application GlobalProtect	Description
Nécessite Content Release version 8451-6911 ou ultérieure et application GlobalProtect version 6.0.0 ou ultérieure.	expérience d’authentification unique transparente. Notez que GlobalProtect ne peut mettre en cache le code confidentiel que si le fournisseur de la carte à puce l’autorise. Vous devez définir le paramètre prédéployé sur les points de terminaison de l'utilisateur final avant de pouvoir activer l'authentification unique pour le code PIN de la carte à puce. Ensuite, pour activer ce paramètre, sélectionnez **Yes (Oui)**.
Utiliser l’ouverture de session unique (macOS)	Sélectionnez **No (Non)** pour désactiver l'authentification unique (SSO). Avec l'ouverture de session unique, l'application GlobalProtect utilise automatiquement les informations d'identification de macOS pour s'authentifier et ensuite se connecter au portail et à la passerelle GlobalProtect. Cette option nécessite la version de contenu 8196-5685 ou toute version ultérieure.
Effacer les identifiants d’ouverture de session unique à la fermeture de session (Windows uniquement)	Sélectionnez **No (Non)** pour conserver les inforations d’aitjentification uniques lorsque l'utilisateur se déconnecte. Sélectionnez **Yes (Oui)** (par défaut) pour les supprimer et forcer l'utilisateur à entrer ses informations d'identification lors de la prochaine connexion.
Utiliser l’authentification par défaut en cas d’échec d’authentification Kerberos	Sélectionnez **No (Non)** pour utiliser uniquement l'authentification Kerberos. Sélectionnez **Yes (Oui)** (par défaut) pour recommencer l'authentification en utilisant la méthode d'authentification par défaut après un échec de l'authentification avec Kerberos. Cette fonction est prise en charge uniquement sur les points de terminaison Windows et Mac.
Utiliser le navigateur par défaut pour l’authentification SAML (Requires GlobalProtect app 5.2 or later with Content Release version 8284-6139 or later (Nécessite l’application GlobalProtect 5.2 ou ultérieure avec Content Release version 8284-6139 ou ultérieure))	Si vous avez configuré le portail GlobalProtect pour authentifier les utilisateurs finaux via l’authentification SAML (Security Assertion Markup Language), sélectionnez **Yes (Oui)** pour permettre aux utilisateurs de tirer parti de la même connexion pour GlobalProtect avec leurs informations d’identification utilisateur enregistrées sur le default system browser (navigateur système par défaut) tel que Chrome, Firefox ou Safari pour se connecter aux applications compatibles SAML. Notez que vous devez activer ce paramètre si vous utilisez SAML avec le service d’authentification cloud. Si vous activez ce paramètre, vous devez égalementchange the pre-deployment settings (modifier les paramètres de prédéploiement) pour permettre au navigateur par défaut sur les points de terminaison Windows, macOS, Linux,

Paramètres de configuration de l’application GlobalProtect	Description
	Android et iOS d’utiliser le navigateur système par défaut pour l’authentification SAML. *Pour empêcher chaque connexion d’ouvrir un nouvel onglet dans le navigateur par défaut, configurez* an authentication override (un remplacement d’authentification).
Rétablissement automatique du délai de connexion VPN	Entrez un délai d’attente, en minutes, de 0 à 180, pour préciser l'action que l’application GlobalProtect prend lorsqu’un tunnel est déconnecté en raison de l'instabilité du réseau ou que l’état du terminal est modifié lors de l’entrée ; la valeur par défaut est 30. • 0 : désactive cette fonction ; GlobalProtect ne tente pas de rétablir le tunnel après sa déconnexion. • 1 à 180 : active cette fonction ; GlobalProtect tente de rétablir la connexion du tunnel si le tunnel est indisponible pendant une période de temps qui est inférieure à la valeur du délai que vous indiquez ici. Par exemple, si la valeur du délai est fixée à 30 minutes, GlobalProtect ne tente pas de rétablir le tunnel si celui-ci est déconnecté depuis 45 minutes. Toutefois, si le tunnel est déconnecté pendant 15 minutes, GlobalProtect tente de se reconnecter car le nombre de minutes n’a pas dépassé la valeur de délai. *Avec le VPN toujours activé, si un utilisateur passe d’un réseau externe à un réseau interne avant l’expiration de la valeur de délai, GlobalProtect n’effectue pas de découverte de réseau. Par conséquent, GlobalProtect rétablit le tunnel vers la dernière passerelle externe connue. Pour déclencher la détection d’hôte interne, l’utilisateur doit sélectionner Rediscover Network (Redécouvrir le réseau) dans la console GlobalProtect.*
Temps d’attente entre les tentatives de rétablissement de la connexion VPN (min)	Saisissez la période de temps, en secondes, pendant laquelle l’application GlobalProtect attend entre des tentatives de rétablissement de la connexion avec la dernière passerelle à laquelle elle s’est connectée lorsque vous activez l’option **Automatic Restoration of VPN Connection Timeout (Rétablissement automatique du délai de connexion VPN)**. Indiquez un temps d’attente plus long ou plus court selon les

Paramètres de configuration de l’application GlobalProtect	Description
	conditions de votre réseau. La plage est comprise entre 1 et 60. La valeur par défaut est 5.
Application de la stratégie de trafic des points de terminaison (Windows 10 or later and macOS 11 and later only (Windows 10 ou version ultérieure et macOS 11 et versions ultérieures uniquement)) Nécessite Content Release version 8450-6909 ou ultérieure et l’application GlobalProtect 6.0.0 ou ultérieure	Configurez l’application de la stratégie de trafic du point de terminaison pour empêcher le trafic sur la carte physique lorsque le point de terminaison est connecté à GlobalProtect. Cela protège contre les tentatives de contrecarrer la sécurité, telles que les connexions entrantes malveillantes, les applications qui contournent le tunnel en se liant à la carte physique et les utilisateurs finaux qui falsifient la table de routage pour contourner le tunnel GlobalProtect. Sélectionnez l’une des options suivantes pour configurer l’application de la stratégie de trafic des points de terminaison : • **No (Non)**: désactive l’application de la stratégie de trafic des terminaux. Il s'agit du paramètre par défaut. • **TCP/UDP Traffic Based on Tunnel IP Address Type (Trafic TCP/UDP basé sur le type d'adresse IP du tunnel)** : active l'application de la stratégie de trafic des points de terminaison pour le trafic TCP/UDP. Cette fonctionnalité est activée pour le trafic en fonction du type d'adresse IP du tunnel. Si le tunnel est IPv4, cette fonctionnalité s'applique uniquement au trafic IPv4. Si le tunnel est IPv6, cette fonctionnalité s'applique uniquement au trafic IPv6. • **All TCP/UDP Traffic (Tout le trafic TCP/UDP)** : active l'application de la politique de trafic des points de terminaison pour tout le trafic TCP/UDP, quel que soit le type d'adresse IP du tunnel. Si le type d'adresse IP du tunnel est IPv4, l'application de la stratégie de trafic du point de terminaison s'applique à tout le trafic TCP/UDP (IPv4 ou IPv6). Si le type d'adresse IP du tunnel est IPv6, l'application de la stratégie de trafic du point de terminaison s'applique à tout le trafic TCP/UDP (IPv4 ou IPv6). • **All Traffic (Tout le trafic)** : active l'application de la politique de trafic des points de terminaison pour tous les protocoles TCP, UDP, ICMP et tous les autres protocoles, quel que soit le type d'adresse IP du tunnel.
Appliquer la Connexion GlobalProtect pour l’Accès au réseau.	Sélectionnez **Yes (Oui)** pour contraindre la totalité du trafic réseau à traverser un tunnel GlobalProtect. Sélectionnez **No (Non)** (par défaut) si GlobalProtect n’est pas requis pour l’accès au réseau et si les utilisateurs peuvent toujours accéder à Internet même si GlobalProtect est désactivé ou déconnecté.

Paramètres de configuration de l’application GlobalProtect	Description
	Pour fournir des instructions aux utilisateurs avant le blocage du trafic, configurez un **Traffic Blocking Notification Message (message de notification de blocage du trafic)** et spécifiez éventuellement le message (**Traffic Blocking Notification Delay (retard de notification de blocage du trafic)**). Pour permettre le trafic requis pour établir une connexion avec un portail captif, spécifiez un **Captive Portal Exception Timeout (délai d'attente d'exception du portail captif)**. L'utilisateur doit s'authentifier auprès du portail avant que le délai d'expiration expire. Pour fournir des instructions supplémentaires, configurez un **Captive Portal Detection Message (Message de détection du portail captif)**. Vous pouvez également spécifier le moment où le message doit s’afficher (**Captive Portal Notification Delay [Retard de notification du portail captif]**). *Dans la plupart des cas, utilisez la sélection par défaut **No (Non)**. En sélectionnant **Yes (Oui)** vous bloquez tout le trafic réseau depuis et vers le point de terminaison jusqu’à ce que l’application se connecte à une passerelle interne à l’intérieur de l'entreprise ou à une passerelle externe à l’extérieur du réseau de l’entreprise.*
Autoriser le trafic vers les hôtes/ réseaux spécifiés lorsque l’application de la connexion GlobalProtect pour l’accès réseau est activée et que la connexion GlobalProtect n’est pas établie	Si vous le souhaitez, spécifiez un maximum de dix adresses IP ou segments de réseau pour lesquels vous souhaitez autoriser l’accès lorsque vous appliquez GlobalProtect pour l’accès au réseau, mais que la connexion n’est pas établie. Séparez plusieurs valeurs par des virgules et n’ajoutez pas d’espace entre les entrées. Les exclusions peuvent améliorer l’expérience utilisateur en permettant aux utilisateurs d’accéder aux ressources locales lorsque GlobalProtect est déconnecté. Par exemple, lorsque GlobalProtect n’est pas connecté, GlobalProtect peut exclure les adresses locales de liaison pour autoriser l’accès à un segment de réseau local ou à un domaine de diffusion.
Autoriser le trafic vers les FDQN spécifiés lorsque l’application de la connexion GlobalProtect pour l’accès réseau est activée et que la connexion GlobalProtect n’est pas établie	Spécifiez les noms de domaine complets (FQDN) auxquels vous autorisez l’accès lorsque vous appliquez des connexions GlobalProtect pour l’accès réseau. Vous pouvez configurer un maximum de 40 noms de domaine entièrement qualifiés pour lesquels vous souhaitez autoriser l’accès lorsque vous appliquez les connexions GlobalProtect pour l’accès au réseau et que GlobalProtect ne peut établir de connexion. En

Paramètres de configuration de l'application GlobalProtect	Description
(Windows et macOS 10.15.4 ou version ultérieure) Nécessite la version 8284-6139 ou ultérieure de Content Release et l'application GlobalProtect 5.2 ou ultérieure.	configurant des exclusions FQDN, vous pouvez améliorer l'expérience utilisateur en permettant aux utilisateurs finaux d'accéder aux ressources spécifiques lorsque GlobalProtect est déconnecté. Par exemple, le terminal peut communiquer avec un fournisseur d'identité hébergé sur le cloud (IdP) pour des besoins d'authentification ou avec un serveur de gestion de périphérique à distance même lorsque l'option Appliquer GlobalProtect pour l'accès au réseau est activée. *En raison d'un changement récent dans macOS, l'application de connexions GlobalProtect avec des exclusions de nom de domaine complet pour plusieurs extensions réseau chargées à la fois ne fonctionne pas dans certaines situations, par exemple dans les environnements où DnsClient.Net, GlobalProtect avec le paramètre Autoriser le trafic vers le nom de domaine complet spécifié lorsque l'option* ***Allow traffic to specified FQDN when Enforce GlobalProtect Connection for Network Access is enabled and GlobalProtect Connection is not established (Appliquer la connexion GlobalProtect pour l'accès réseau est activée et que la connexion GlobalProtect n'est pas établie)*** *et Cortex XDR sont en cours d'exécution.*
Expiration de l'exception du portail captif (sec)	Afin d'imposer GlobalProtect pour l'accès au réseau, mais fournir un délai supplémentaire pour permettre aux utilisateurs de se connecter à un portail captif, spécifiez le délai d'attente en secondes (entre 0 et 3 600). Par exemple, une valeur de 60 signifie que l'utilisateur doit se connecter au portail captif dans un délai d'une minute après que GlobalProtect l'ait détecté. Une valeur de 0 signifie que GlobalProtect ne permet pas aux utilisateurs de se connecter à un portail captif et bloque immédiatement l'accès.
Lancer automatiquement la page Web dans le navigateur par défaut lors de la détection du portail captif	Pour automatiquement lancer votre navigateur Web par défaut lors de la détection du portail captif afin de permettre aux utilisateurs de se connecter facilement au portail captif, saisissez le Fully Qualified Domain Name ou l'adresse IP du site Web que vous souhaitez utiliser pour la tentative de connexion initiale qui initie le trafic Web lors du lancement du navigateur Web par défaut (longueur maximale de 256 caractères). Le portail captif intercepte alors cette

Paramètres de configuration de l'application GlobalProtect	Description
	tentative de connexion et redirige le navigateur Web par défaut à la page de connexion au portail captif. Si le champ est vide (par défaut), GlobalProtect ne lance pas automatiquement le navigateur Web par défaut lors de la détection du portail captif.
Retard de notification de blocage du trafic (sec)	Spécifiez une valeur, en secondes, pour déterminer quand afficher le message de notification. GlobalProtect démarre le compte à rebours pour afficher la notification une fois que le réseau est accessible (la plage est de 5 à 120, la valeur par défaut est 15).
Afficher le message de notification de blocage du trafic	Spécifiez si un message doit apparaître lorsque GlobalProtect est requis pour l'accès au réseau. Sélectionnez **No (Non)** pour désactiver le message. Sélectionnez **Yes (Oui)** pour activer le message (GlobalProtect affiche le message lorsqu'il est déconnecté mais qu'il détecte que le réseau est accessible).
Message de notification de blocage du trafic	Personnalisez un message de notification à afficher aux utilisateurs lorsque GlobalProtect est requis pour accéder au réseau. GlobalProtect affiche le message lorsqu'il est déconnecté mais qu'il détecte que le réseau est accessible. Le message peut indiquer le motif du blocage du trafic et fournir des instructions sur la manière de se connecter. Par exemple : `Pour accéder au réseau, vous devez d'abord vous connecter à GlobalProtect.` Le message doit contenir un maximum de 512 caractères.
Autoriser l'utilisateur à désactiver les notifications de blocage du trafic	Sélectionnez **No (Non)** pour toujours afficher les notifications de blocage du trafic. Par défaut, la valeur est définie sur **Yes (Oui)**, ce qui signifie que les utilisateurs sont autorisés à désactiver les notifications.
Afficher le message de détection du portail captif	Spécifie si un message s'affiche lorsque GlobalProtect détecte un portail captif. Sélectionnez **Yes (Oui)** pour afficher le message. Sélectionnez **No (Non)** (par défaut) pour supprimer le message (GlobalProtect n'affiche pas de message lorsqu'il détecte un portail captif).

Paramètres de configuration de l’application GlobalProtect	Description
	Si vous activez un Message de détection de portail captif, le message apparaît 85 secondes avant l’Expiration de l’exception du portail captif. Donc, si l’Expiration de l’exception du portail de capture est de 90 secondes ou moins, le message apparaît 5 secondes après la détection d’un portail captif.
Message de détection du portail captif	Personnalisez un message de notification à afficher aux utilisateurs lorsque GlobalProtect détecte le réseau qui fournit des instructions supplémentaires pour se connecter à un portail captif. Par exemple : `GlobalProtect a temporairement autorisé l’accès au réseau pour vous permettre de vous connecter à Internet. Suivez les instructions de votre fournisseur d’accès Internet. Si vous laissez la connexion expirer, ouvrez GlobalProtect et cliquez sur Connexion pour réessayer.` Le message doit contenir un maximum de 512 caractères.
Délai de notification du portail captif (sec)	Si vous activez le message de détection du portail captif, vous pouvez spécifier le délai en secondes après lequel, à la suite de la détection du portail captif, GlobalProtect affichera le message de détection (la plage est comprise de 1 à 120 ; par défaut 5).
Recherche dans le magasin de certificats du client	Sélectionnez le type de certificat ou de certificats qu'une application cherche dans son magasin de certificats personnel. L'application GlobalProtect utilise le certificat pour s'authentifier sur le portail ou sur une passerelle, puis pour établir un tunnel VPN vers la passerelle GlobalProtect. • **User (Utilisateur)** – Authentification en utilisant le certificat local au compte de l’utilisateur. • **Machine** – Authentification en utilisant un certificat qui est local au terminal. Ce certificat s'applique à tous les comptes d'utilisateurs autorisés à utiliser le terminal. • **User and machine (Utilisateur et machine)** (par défaut) – Authentification utilisant le certificat d'utilisateur et le certificat de la machine.
Période de renouvellement de certificat SCEP (jours)	Ce mécanisme est pour le renouvellement d'un certificat SCEP généré avant que le certificat n'expire effectivement.

Paramètres de configuration de l’application GlobalProtect	Description
	Vous spécifiez le nombre maximal de jours avant l’expiration du certificat pendant lequel le portail peut requérir un nouveau certificat du serveur SCEP dans votre système PKI (la plage est de 0 à 30, 7 par défaut). Une valeur de 0 signifie que le portail ne renouvelle pas automatiquement le certificat du client quand il actualise une configuration de client. Pour qu'une application obtienne le nouveau certificat, l'utilisateur doit se connecter au cours de la période de renouvellement (le portail ne demande pas le nouveau certificat pour un utilisateur au cours de cette période de renouvellement à moins que l'utilisateur se connecte). Par exemple, supposons qu'un certificat client a une durée de vie de 90 jours et que cette période de renouvellement du certificat est de 7 jours. Si un utilisateur se connecte au cours des 7 derniers jours de la durée de vie certificat, le portail génère le certificat et le télécharge avec une configuration client rafraîchie. Voir Intervalle de rafraîchissement de configuration de l’application GlobalProtect (heures).
Sélection du Certificat Client selon un OID inclus dans une clé étendue (Windows and macOS only (Windows et macOS uniquement))	Utilisez cette option pour fournir un identificateur d’objet (OID) que GlobalProtect doit utiliser pour déterminer le certificat client à sélectionner afin de simplifier et d’améliorer le processus de sélection des certificats lorsque plusieurs certificats sont installés sur vos points de terminaison macOS ou Windows. Par défaut, GlobalProtect filtre automatiquement les certificats pour ceux qui spécifient un objectif d’authentification client (OID 1.3.6.1.5.5.7.3.2), il n’est donc pas nécessaire de spécifier l’OID associé à l’authentification client. Toutefois, si vous souhaitez utiliser un OID différent pour distinguer le certificat que GlobalProtect doit sélectionner, vous pouvez spécifier une utilisation de certificat différente lorsque vous créez le certificat, puis définir le **Extended Key Usage OID for Client Certificate (certificat client pour l’OID d’utilisation étendue de clé)** sur l’OID correspondant. Certains des OID les plus couramment utilisés sont: • 1.3.6.1.5.5.7.3.1 : Authentification du serveur • 1.3.6.1.5.5.7.3.3 : Signature de codes • 1.3.6.1.5.5.7.3.4 : Protection des e-mails • 1.3.6.1.5.5.7.3.5 : Système terminal IPSec • 1.3.6.1.5.5.7.3.6 : Tunnel IPsec • 1.3.6.1.5.5.7.3.7 : Utilisateur IPSec

Paramètres de configuration de l’application GlobalProtect	Description
	• 1.3.6.1.5.5.7.3.8 : Horodatage • 1.3.6.1.5.5.7.3.9 : Signature du PSOC
Maintenir la connexion lors du retrait de Carte à puce (Windows uniquement)	Sélectionnez **Yes (Oui)** pour conserver la connexion lorsqu’un utilisateur retire une carte à puce contenant un certificat de client. Sélectionnez **No (Non)** (par défaut) pour mettre fin à la connexion lorsqu’un utilisateur retire une carte à puce.
Activer la visualisation avancée	Sélectionnez **No (Non)** pour restreindre l'interface utilisateur de l’application à la vue minimale, de base (par défaut).
Permettre à l'utilisateur de désactiver la page de bienvenue	Sélectionnez **No (Non)** pour forcer l'affichage de la page de bienvenue chaque fois qu'un utilisateur établit une connexion. Cette restriction empêche l'utilisateur d'ignorer des informations importantes comme les conditions que votre organisation peut exiger pour garantir la conformité.
Demander à l’utilisateur d’accepter les conditions d’utilisation avant la création du tunnel	Sélectionnez **Yes (Oui)** pour demander à l’utilisateur final d’accepter les conditions d’utilisation afin de se conformer aux politiques de l’entreprise et pour afficher une page permettant de consulter les conditions d’utilisation de votre entreprise avant de se connecter à GlobalProtect. Avant de définir cette option sur **Yes (Oui)**, vous devez configurer la GlobalProtect Welcome page (page d’accueil GlobalProtect) via **Network (réseau)** > **GlobalProtect** > **Portals (Portails)** > ***<portal_config*** > **General (généralités)).**
Activer l’option de Redécouverte du réseau	Sélectionnez **No (Non)** pour empêcher les utilisateurs de lancer manuellement une redécouverte du réseau.
Activer l’option de Renvoi du profil d’hôte	Sélectionnez **No (Non)** pour empêcher les utilisateurs de déclencher manuellement le renvoi des dernières données HIP.
Permettre à l’Utilisateur de modifier l’Adresse du portail	Sélectionnez **No (Non)** pour désactiver le champ **Portal (Portail)** de l'onglet **Home (Accueil)** dans l'application GlobalProtect. Toutefois, comme l'utilisateur peut ensuite définir un portail auquel se connecter, vous devez fournir l'adresse du portail par défaut dans le Registre Windows ou Macplist : • **Windows registry**—`HKEY_LOCAL_MACHINE \SOFTWARE\PaloAlto Networks \GlobalProtect\PanSetup` with key `Portal`

Paramètres de configuration de l’application GlobalProtect	Description
	• **Mac plist** – `/Library/Preferences/com.paloaltonetworks.GlobalProtect.pansetup.plist` avec la clé `Portal` Pour plus d’informations sur le prédéploiement de l’adresse du portail, voir Paramètres de l’application à personnaliser dans le Guide de l’Administrateur GlobalProtect.
Permettre à l'utilisateur de continuer avec un certificat de serveur de portail invalide	Sélectionnez **No (Non)** pour empêcher l'application d'établir une connexion au portail si le certificat du portail n'est pas valide.
Afficher l'icône GlobalProtect	Sélectionnez **No (Non)** pour masquer l'icône GlobalProtect sur le point de terminaison. Si l'icône est masquée, les utilisateurs ne peuvent pas effectuer certaines tâches, telles que l'affichage des informations de dépannage, changer les mots de passe, redécouvrir le réseau, ou d'effectuer une connexion à la demande. Cependant, les messages de notification HIP, les invitations de connexion et les dialogues de certificats s'affichent lorsque l'interaction de l'utilisateur est nécessaire.
Délai d'expiration pour renommer le tunnel de bascule d'utilisateur (sec) (Windows uniquement)	Indiquez le nombre de secondes durant lesquelles un utilisateur distant doit être authentifié par une passerelle GlobalProtect après la connexion à un terminal en utilisant le protocole Remote Desktop Protocol (RDP) de Microsoft (la plage est de 0 à 600, 0 par défaut). Exiger que l'utilisateur distant s'authentifie dans un laps de temps limité maintient la sécurité. Après l'authentification du nouvel utilisateur et la commutation du tunnel à l'utilisateur, la passerelle renomme le tunnel. Une valeur de 0 signifie que le tunnel actuel de l’utilisateur n’est pas renommé, mais, au contraire, est immédiatement interrompu. Dans ce cas, l'utilisateur distant obtient un nouveau tunnel et n'a aucune limite de temps pour l'authentification à une passerelle (autre que le délai d'attente TCP configuré).
Délai d’expiration pour renommer le tunnel de pré-ouverture de session (sec) (Windows uniquement)	Ce paramètre contrôle la manière dont GlobalProtect gère le tunnel de pré-ouverture de session qui relie un terminal à la passerelle. Une valeur de -1 signifie que le tunnel de pré-ouverture de session n’expire pas après la connexion d’un utilisateur au terminal ; GlobalProtect renomme le tunnel pour le réaffecter

Paramètres de configuration de l’application GlobalProtect	Description
	à l’utilisateur. Cependant, le tunnel persiste même si le renommage échoue ou si l’utilisateur ne se connecte pas à la passerelle GlobalProtect. Une valeur de 0 signifie que lorsque l’utilisateur se connecte au terminal, GlobalProtect ferme immédiatement le tunnel de pré-ouverture de session au lieu de le renommer. Dans ce cas, GlobalProtect lance un nouveau tunnel pour l’utilisateur plutôt que de permettre à ce dernier de se connecter sur le tunnel de pré-ouverture de session. Généralement, ce paramètre est très utile lorsque vous définissez la **Connect Method (Méthode de connexion)** sur **Pre-logon then On-demand (Pré-ouverture de session puis À la demande)**, ce qui force l’utilisateur à lancer manuellement la connexion après la connexion initiale. Une valeur de 1 à 7200 indique le nombre de secondes pendant lesquelles le tunnel de pré-ouverture de session peut rester actif après qu’un utilisateur se connecte au terminal. Pendant ce temps, GlobalProtect applique des règles au tunnel de pré-ouverture de session. Si l’utilisateur s’authentifie avec la passerelle GlobalProtect avant l’expiration du délai, GlobalProtect réaffecte le tunnel à l’utilisateur. Si l’utilisateur ne s’authentifie pas avec la passerelle GlobalProtect avant l’expiration du délai, GlobalProtect met fin au tunnel de pré-ouverture de session.
Délai de conservation du tunnel après la déconnexion de l’utilisateur (secondes)	Pour que GlobalProtect puisse conserver le tunnel VPN existant après la déconnexion des utilisateurs de leur terminal, spécifiez un **Preserve Tunnel on User Logoff Timeout (Délai de conservation du tunnel après la déconnexion de l’utilisateur)** (plage comprise entre 0 et 600 secondes ; valeur par défaut : 0 seconde). Si vous acceptez la valeur par défaut (`0`), GlobalProtect ne conserve pas le tunnel lorsque l’utilisateur se déconnecte.
Message personnalisé d’expiration de mot de passe (Authentification LDAP uniquement)	Créer un message personnalisé à afficher aux utilisateurs lorsque leur mot de passe est sur le point d'expirer. La longueur du message est de 200 caractères maximum.
Utiliser automatiquement SSL lorsque IPSec est peu fiable (heures)	Précisez la période de temps (en heures) pendant laquelle vous voulez que l'application GlobalProtect **Automatically Use SSL When IPSec Is Unreliable (Utilise automatiquement SSL lorsque IPSec est peu fiable)** (la plage est comprise entre 0 et 168 heures). Si vous configurez cette option, l’application GlobalProtect ne tente pas d’établir de tunnel IPSec au cours de la période de temps spécifiée. Ce minuteur

Paramètres de configuration de l’application GlobalProtect	Description
	est lancé chaque fois qu’un tunnel IPSec devient indisponible en raison d’un délai d'expiration keepalive du tunnel. Si vous acceptez la valeur par défaut de **0**, l’application ne recommence pas à établir un tunnel SSL si elle peut établir un tunnel IPSec. Elle revient à l’établissment d’un tunnel SSL uniquement lorsque le tunnel IPSec ne peut être établi.
Afficher la notification de secours IPSec vers SSL Nécessite la version de publication de contenu 8387-6595 ou ultérieure et la version 6.0 ou ultérieure de l’application GlobalProtect.	Sélectionnez **No (Non)** si vous ne souhaitez pas que les utilisateurs voient un message de notification indiquant que leur connexion est passée d’IPSec à SSL. Par défaut, les utilisateurs seront avertis.
Se connecter au moyen de SSL uniquement Nécessite la version 6.0 ou ultérieure de l’application GlobalProtect.	Sélectionnez **Yes (Oui)** si vous souhaitez que les utilisateurs puissent choisir d’utiliser SSL au lieu d’IPSec.
MTU de connexion GlobalProtect (octets)	Saisissez la valeur de l’unité de transmission maximale (MTU) de connexion entre 1000 et 1420 octets qui est utilisée par l’application GlobalProtect pour se connecter à la passerelle. La valeur par défaut est 1400 octets. Vous pouvez optimiser l’expérience de connexion pour les utilisateurs finaux qui se connectent sur des réseaux qui nécessitent des valeurs de MTU inférieures à la norme de 1500 octets. En réduisant la taille de MTU, vous pouvez éliminer les problèmes de performance et connectivité qui se produisent du fait de la fragmentation lorsque les connexions de tunnel VPN passent par plusieurs Internet Service Providers (fournisseur d'accès à Internet - ISP) et des chemins d’accès de réseau avec une MTU inférieure à 1500 octets.
Nombre maximum de tentatives de connexion à la passerelle interne	Saisissez le nombre maximum de fois où l’agent GlobalProtect devrait réessayer la connexion à une passerelle interne après que la première tentative échoue (la plage est de 0 à 100 ; 0 par défaut, ce qui signifie que l’application GlobalProtect ne relance pas la connexion). En augmentant la valeur, vous permettez à l'application de se connecter automatiquement à une passerelle interne qui est temporairement indisponible ou inaccessible lors de la première tentative de connexion, mais redevient disponible avant que le nombre spécifié de tentatives soit épuisé. L'augmentation de la valeur assure également que la

Paramètres de configuration de l’application GlobalProtect	Description
	passerelle interne reçoit les informations de l'utilisateur et de l'hôte les plus à jour.
Activer la détection avancée des hôtes internes	Pour ajouter une couche de sécurité supplémentaire lors de la détection interne de l’hôte par l’application GlobalProtect. Avec la détection avancée de l’hôte interne, l’application valide le certificat de serveur des passerelles internes en plus d’effectuer une recherche DNS inversée de l’hôte interne pour déterminer si l’application se trouve à l’intérieur du réseau d’entreprise. Sélectionnez **Yes (Oui)** pour permettre à l’application GlobalProtect de valider le certificat de serveur des passerelles internes en plus d’effectuer une recherche DNS inversée de l’hôte interne lors de la détection de l’hôte interne. Sélectionnez **No (Non)** (par défaut) pour que l’application GlobalProtect effectue une détection d’hôte interne sans valider le certificat de serveur des passerelles internes.
Délai d'expiration de connexion au portail (sec.)	Le nombre de secondes (entre 1 et 600) avant qu’une requête de connexion au portail n’expire en raison de l’absence de réponse du portail. Lorsque votre pare-feu utilise des versions de contenu Applications et menaces antérieures à 777-4484, la valeur par défaut est 30. À partir de la version de contenu 777-4484, la valeur par défaut est 5.
Délai d'expiration de connexion TCP (sec.)	Le nombre de secondes (entre 1 et 600) avant qu'une demande de connexion TCP n’expire en raison de la non-réponse de l'une ou l'autre extrémité de la connexion. Lorsque votre pare-feu utilise des versions de contenu Applications et menaces antérieures à 777-4484, la valeur par défaut est 60. À partir de la version de contenu 777-4484, la valeur par défaut est 5.
Délai d'expiration de réception TCP (sec)	Le nombre de secondes avant qu’une connexion TCP n’expire en raison de la réponse partielle d’une demande de connexion TCP (la plage est de 1 à 600, 30 par défaut).
Option de segmentation du tunnel	Spécifiez s’il faut activer le domaine à tunnel fractionné et/ou la fonctionnalité DNS fractionné pour le trafic en fonction de l’exclusion ou de l’inclusion des domaines configurés sur la passerelle GlobalProtect sous **Network > GlobalProtect > Gateway > Agent > Client Setting > (Client Config) > Split Tunnel > Domain and Application (Réseau > GlobalProtect > Passerelle > Agent > Paramètres client > (Config client) > Tunnel de séparation > Domaine et application**.

Paramètres de configuration de l'application GlobalProtect	Description
	Trafic réseau uniquement : sélectionnez cette option pour activer uniquement le domaine à tunnel fractionné pour le trafic conformément à l'inclusion ou à l'exclusion des domaines configurés sur la passerelle GlobalProtect sous **Network > GlobalProtect > Gateway > Agent > Client Setting > (Client Config) > Split Tunnel > Domain and Application**. **Trafic réseau et DNS** : sélectionnez cette option pour activer à la fois le domaine à tunnel fractionné et le DNSfractionné pour le trafic conformément à l'inclusion ou à l'exclusion des domaines configurés sur la passerelle **GlobalProtect sous Network > GlobalProtect > Gateway > Agent > Client Setting > (Configuration client) > Split Tunnel > Domain and Application**. Cette option nécessite la version de contenu 8284-6139 ou toute version ultérieure.
Résoudre tous les FQDN à l'aide des serveurs DNS assignés par le tunnel (Windows uniquement)	(GlobalProtect 4.0.3 et versions ultérieures) Configurez les préférences de résolution DNS lorsque le tunnel GlobalProtect est connecté aux points de terminaison Windows : • Sélectionnez **Yes (Oui)** (par défaut) pour que l'application GlobalProtect puisse autoriser les points de terminaison Windows à résoudre toutes les requêtes DNS auprès des serveurs DNS que vous configurez sur la passerelle au lieu d'autoriser le point de terminaison à envoyer certaines requêtes DNS aux serveurs DNS établis sur l'adaptateur physique. • Sélectionnez **No (Non)** pour permettre aux points de terminaison Windows d'envoyer les requêtes DNS au serveur DNS établi sur l'adaptateur physique si la requête initiale envoyée au serveur DNS configuré sur la passerelle n'est pas résolue. Cette option conserve le comportement natif de Windows pour interroger tous les serveurs DNS sur tous les adaptateurs de manière récursive, ce qui peut toutefois se traduire par de longues périodes d'attente pour résoudre certaines requêtes DNS. Pour configurer les paramètres DNS de l'application GlobalProtect 4.0.2 et ses versions antérieures, utilisez l'option **Update DNS Settings at Connect (Mettre à jour les paramètres de DNS à la connexion)**.
Mettre à jour les paramètres de DNS à la connexion	(GlobalProtect 4.0.2 et versions antérieures) Configurez les préférences relatives au serveur DNS pour le tunnel GlobalProtect :

Paramètres de configuration de l’application GlobalProtect	Description
(Windows uniquement) (plus utilisé)	• Sélectionnez **No (Non)** (par défaut) pour permettre aux points de terminaison Windows d’envoyer les requêtes DNS au serveur DNS établi sur l'adaptateur physique si la requête initiale envoyée au serveur DNS configuré sur la passerelle n’est pas résolue. Cette option conserve le comportement natif de Windows pour interroger tous les serveurs DNS sur tous les adaptateurs de manière récursive, ce qui peut toutefois se traduire par de longues périodes d’attente pour résoudre certaines requêtes DNS. • Sélectionnez **Yes (Oui)** pour permettre aux points de terminaison Windows de résoudre toutes les requêtes DNS auprès des serveurs DNS que vous configurez sur la passerelle au lieu des serveurs DNS établis sur l'adaptateur physique sur le point de terminaison. Lorsque vous activez cette option, GlobalProtect applique strictement les paramètres DNS de la passerelle et remplace les paramètres statiques de tous adaptateurs physiques. *Lorsque ce paramètre est activé, (définir sur **Yes (Oui)**) il se peut que GlobalProtect n’arrive pas à restaurer les paramètres DNS précédemment enregistrés et, par conséquent, que le point de terminaison ne puisse pas résoudre les requêtes DNS. Cette fonctionnalité n’est plus utilisée et est remplacée par une implémentation améliorée permettant d’éviter que ce scénario ne se produise. Si vous utilisée auparavant cette fonctionnalité, nous vous recommandons de passer à l’application GlobalProtect 4.0.3 ou à une version ultérieure.* Pour configurer les paramètres DNS de l’application GlobalProtect 4.0.3 ou d’une version ultérieure, utilisez l’option **Resolve All FQDNs Using DNS Servers Assigned by the Tunnel (Résoudre tous les FQDN à l'aide des serveurs DNS assignés par le tunnel)**.
URL du fichier PAC (Proxy Auto-Configuration)	Sélectionnez **Yes (Oui)** pour envoyer l’URL de vos fichiers PAC (proxy auto-configuration) de l’application GlobalProtect vers vos points de terminaison. Spécifiez l’URL du fichier PAC (Proxy Auto-Configuration) que vous souhaitez pousser vers le point de terminaison pour configurer les paramètres de proxy. La longueur maximale de l’URL est de 256 caractères. Les méthodes d’URL de fichier

Paramètres de configuration de l’application GlobalProtect	Description
	PAC (Proxy Auto-Configuration) suivantes sont prises en charge : • Norme PAC (Proxy Auto-Config) (par exemple, http://pac.<hostname or IP>/proxy.pac). • Norme WPAD (Web Proxy Auto-Discovery Protocol) (par exemple, http://wpad.<hostname or IP>/wpad.dat).
Détecter le proxy pour chaque connexion (Windows uniquement)	Sélectionnez **No (Non)** pour détecter automatiquement le proxy pour la connexion de portail et utiliser ce proxy pour les connexions ultérieures. Sélectionnez **Yes (Oui)** (par défaut) pour détecter automatiquement le proxy à chaque connexion.
Définissez le proxy du tunnel (Windows et Mac uniquement)	Spécifiez si GlobalProtect doit utiliser ou contourner les proxys. Sélectionnez **No (Non)** pour exiger le contournement des proxys par GlobalProtect. Sélectionnez **Yes (Oui)** pour exiger l’utilisation des proxys par GlobalProtect. Selon l’utilisation des proxys GlobalProtect, des systèmes d’exploitation des points de terminaison et du type de tunnel, le trafic réseau fonctionnera différemment.
Envoyer immédiatement un rapport HIP si l’état du centre de sécurité de Windows (WSC) change (Windows uniquement)	Sélectionnez **No (Non)** pour empêcher l'application GlobalProtect d'envoyer des données de HIP lorsque le statut du Centre de sécurité Windows (WSC) change. Sélectionnez **Yes (Oui)** (par défaut) pour envoyer immédiatement les données HIP lorsque le statut du WSC change.
Activer les invites d’authentification entrantes des passerelles MFA	Pour prendre en charge la Multi-Factor Authentication (authentification multi-facteur ; MFA), un point de terminaison GlobalProtect doit recevoir et reconnaître les invites UDP qui proviennent de la passerelle. Sélectionnez **Yes (Oui)** pour permettre à un point de terminaison GlobalProtect de recevoir et d’accepter l’invite. Sélectionnez **No (Non)** (par défaut) pour que GlobalProtect bloque les invites UDP en provenance de la passerelle.
Port réseau pour les invites d’authentification entrante (UDP)	Spécifie le numéro de port qu’un point de terminaison GlobalProtect utilise pour recevoir les invites d’authentification entrantes en provenance des passerelles MFA. Le port par défaut est 4501. Pour changer de port, indiquez un chiffre entre 1 et 65 535.
Passerelles MFA de confiance	Spécifie la liste des pare-feu ou des passerelles d’authentification auxquels un point de terminaison GlobalProtect fait confiance pour l’authentification multi-facteur. Lorsqu’un point de terminaison GlobalProtect reçoit un message UDP sur le port réseau spécifié, GlobalProtect

Paramètres de configuration de l’application GlobalProtect	Description
	affiche un message d’authentification uniquement si l’invite UDP provient d’une passerelle de confiance.
Message d'authentification entrant	Personnalisez un message de notification à afficher lorsque les utilisateurs tentent d’accéder à une ressource qui nécessite une authentification supplémentaire. Lorsque les utilisateurs tentent d’accéder à une ressource qui nécessite une authentification supplémentaire, GlobalProtect reçoit un paquet UDP contenant l’invite d’authentification entrante et affiche ce message. Le paquet UDP contient également l’URL menant à la page du Portail d’authentification que vous avez précisée lors de la Configuration de l’authentification multi-facteur. GlobalProtect ajoute automatiquement l’URL au message. Par exemple : `Vous avez tenté d’accéder à une ressource protégée qui nécessite une authentification supplémentaire. Procédez à l’authentification sur` Le message doit contenir un maximum de 255 caractères.
IPv6 préféré	Spécifie le protocole privilégié pour les communications des points de terminaison de GlobalProtect. Sélectionnez **No (Non)** pour remplacer le protocole privilégié par IPv4. Sélectionnez Oui (par défaut) pour que IPv6 devienne la connexion privilégiée d’un environnement en double pile.
Message de changement de mot de passe	Personnalise un message visant la définition des exigences ou des politiques en matière de mots de passe lorsque les utilisateurs modifient leur mot de passe Active Directory (répertoire actif ; AD). Par exemple : `Les mots de passe doivent contenir au moins un chiffre et une lettre majuscule.` Le message doit contenir un maximum de 255 caractères pour les langages Unicodes sur 2 octets, comme le chinois simplifié. Pour le japonais, le message doit contenir un maximum de 128 caractères.
Critères de sélection de la passerelle de journaux	Sélectionnez **Yes (oui)** pour activer l’application GlobalProtect et envoyer les journaux de critères de sélection de passerelle au pare-feu. La valeur par défaut est **No (Non)**.

Paramètres de configuration de l’application GlobalProtect	Description
	L’application n’envoie pas les journaux améliorés pour les critères de sélection de passerelle au pare-feu.
Activer la collecte de journaux d’applications Autonomous DEM et GlobalProtect pour le dépannage Nécessite la version 8350-14191 ou ultérieure de Content Release ou version ultérieure ; Nécessite l’application GlobalProtect 5.2.5 ou version ultérieure.	Sélectionnez **Yes (Oui)** pour permettre à l’application GlobalProtect d’afficher l’option **Report an issue (Signaler un problème)** afin de permettre aux utilisateurs finaux d’envoyer les journaux de dépannage et de diagnostic directement à Cortex Data Lake. Vous devez configurer le certificat Cortex Data Lake qui est poussé depuis le portail en tant que certificat client pour afficher l'option **Report an issue (Signaler un problème)**. Ce certificat est utilisé pour que le client s'authentifie auprès de Cortex Data Lake lors de l'envoi des journaux. Lorsque ce paramètre est défini sur **No (Non)** (par défaut), l'application GlobalProtect n'affiche pas l'option **Report an issue (Signaler un problème)** et les utilisateurs finaux ne peuvent pas envoyer les journaux de dépannage et de diagnostic à Cortex Data Lake.
Afficher la notification des mises à jour DEM autonomes	Sélectionnez **Yes (Oui)** si vous souhaitez que les utilisateurs voient les notifications chaque fois que l’agent ADEM est mis à jour.
Exécuter les tests de diagnostic pour ces serveurs Web de destination Nécessite la version 8350-14191 ou ultérieure de Content Release ou version ultérieure ; Nécessite l’application GlobalProtect 5.2.5 ou version ultérieure.	Entrez jusqu’à dix URL de destination HTTPS pour lancer des tests de performances pour l’exploration. Ces tests de diagnostic ne sont exécutés que si vous avez choisi **Enable Autonomous DEM and GlobalProtect App Log Collection for Troubleshooting (activer Autonomous DEM et GlobalProtect App Log Collection pour le dépannage)**. Les URL de destination que vous entrez peuvent être des adresses IP ou des noms de domaine complets (par exemple, https://10.10.10.10/resource.html, https://webserver/file.pdf ou https://google.com).
Agent de point de terminaison DEM autonome pour Prisma Access (Windows et Mac uniquement) Fonctionne sur Windows 10 et macOS uniquement; Version de version de contenu 8393-6628 ou ultérieure ; Nécessite l’application GlobalProtect 5.2.6 ou version ultérieure.	Spécifiez si vous souhaitez installer l’agent de point de terminaison Autonomous DEM (ADEM) pendant l’installation de l’application GlobalProtect et autorisez les utilisateurs finaux à activer ou désactiver les tests d’expérience utilisateur à partir de l’application. • **Select Install and user can enable/disable agent from GlobalProtect (Sélectionnez Installer et l'utilisateur peut activer/désactiver l'agent de GlobalProtect)** pour installer l'agent de point de terminaison ADEM lors de l'installation de l'application GlobalProtect et autoriser les utilisateurs finaux à activer ou désactiver les tests d'expérience utilisateur à partir de l'application GlobalProtect.

Paramètres de configuration de l’application GlobalProtect	Description
	• Sélectionnez **Install and user cannot enable/disable agent from GlobalProtect (Installer et l'utilisateur ne peut pas activer/désactiver l'agent de GlobalProtect)** pour installer l'agent de point de terminaison ADEM lors de l'installation de l'application GlobalProtect, et ne pas autoriser les utilisateurs finaux à activer ou désactiver les tests d'expérience utilisateur à partir de l'application GlobalProtect. • **Select Do Not Install (Ne pas installer)** (par défaut) pour ne pas installer l'agent de point de terminaison ADEM lors de l'installation de l'application GlobalProtect.
Périphérique ajouté au message de quarantaine	Par défaut, GlobalProtect affiche le message suivant lorsque l’appareil d’un utilisateur final est mis en quarantaine : `L’accès au réseau à partir de cet appareil a été restreint conformément à la stratégie de sécurité de votre organisation. Veuillez contacter votre administrateur informatique.` Vous pouvez remplacer ce message par défaut par votre propre message personnalisé de 512 caractères maximum.
Périphérique supprimé du message de quarantaine	Par défaut, GlobalProtect affiche le message suivant lorsque l’appareil d’un utilisateur final est mis en quarantaine : `L’accès au réseau à partir de cet appareil a été rétabli conformément à la stratégie de sécurité de votre organisation.` Vous pouvez remplacer ce message par défaut par votre propre message personnalisé de 512 caractères maximum.
Affichez le panneau d’état lors du démarrage (Windows uniquement)	Sélectionnez **Yes (Oui)** pour afficher automatiquement le panneau d'état GlobalProtect lorsque les utilisateurs établissent une connexion pour la première fois. Sélectionnez **No (Non)** pour supprimer le panneau d'état GlobalProtect lorsque les utilisateurs établissent une connexion pour la première fois.
Autoriser l’interface utilisateur GlobalProtect à persister pour les entrées utilisateur	Sélectionnez **Yes (Oui)** pour permettre à l’application GlobalProtect de continuer à afficher le panneau d’état à l’écran lorsque les utilisateurs finaux saisissent leurs informations d’identification.

Paramètres de configuration de l’application GlobalProtect	Description
(Windows 10 or later and macOS (Windows 10 ou version ultérieure et macOS)) Nécessite la version de version de contenu 8450-6909 ou ultérieure et l’application GlobalProtect 6.0.0 ou ultérieure.	
Désactiver l'application GlobalProtect	
Code secret/Confirmer le code secret	Entrez et puis confirmez le code secret si les paramètres pour **Allow User to Disable GlobalProtect App (Permettre à l'Utilisateur de désactiver l'application GlobalProtect)** est **Allow with Passcode (Permettre avec code secret)**. Traitez ce code secret comme un mot de passe : enregistrez et stockez-le dans un endroit sûr. Vous pouvez distribuer le code secret aux nouveaux utilisateurs de GlobalProtect par e-mail ou l'afficher dans une zone de support de votre site Web de l'entreprise. Si les circonstances empêchent le terminal d'établir une connexion VPN et que cette fonction est activée, un utilisateur peut entrer ce code secret dans l'interface de l'application pour désactiver l'application GlobalProtect et obtenir l'accès à Internet sans utiliser le VPN.
Nombre maximal de fois que l’utilisateur peut se déconnecter	Indiquez le nombre maximum de fois qu'un utilisateur peut déconnecter GlobalProtect avant de devoir se connecter à un pare-feu. La valeur par défaut de 0 signifie que les utilisateurs n'ont pas de limite au nombre de fois où ils peuvent déconnecter l'application.
Délai d’expiration avant déconnexion (min)	Spécifiez le nombre maximal de minutes que l'application GlobalProtect peuvent être désactivés. Une fois que le temps spécifié passe, l'application tente de se connecter au pare-feu. La valeur par défaut de 0 indique que la période de déconnexion est illimitée. *Définir une valeur de délai de déconnexion pour restreindre la période de temps pendant laquelle les utilisateurs peuvent déconnecter l’application. Ainsi, GlobalProtect peut reprendre et établir le VPN lorsque le délai est dépassé afin de protéger l’utilisateur et de sécuriser son accès aux ressources.*

Paramètres de configuration de l’application GlobalProtect	Description
Paramètres Mobile Security Manager	
Mobile Security Manager	Si vous utilisez le gestionnaire de sécurité mobile de GlobalProtect pour la gestion des périphériques mobiles (MDM), saisissez l'adresse IP ou le nom de domaine complet (FQDN) de l'interface d'inscription/d'enregistrement du périphérique sur l'appareil GP-100.
Port d'inscription	Le numéro de port que le terminal mobile doit utiliser pour l'inscription lors de la connexion au gestionnaire de sécurité mobile de GlobalProtect. Le Gestionnaire de sécurité mobile écoute sur le port 443 par défaut. *Gardez ce numéro de port afin qu’un certificat ne soit pas demandé aux utilisateurs finaux mobiles au cours du processus d’inscription (les autres valeurs possibles sont 443, 7443 et 8443).*

Onglet Collecte de données HIP de l’agent des portails GlobalProtect

- **Réseau** > **GlobalProtect** > **Portails** > **<*portal-config*>** > **Agent** > **<*agent-config*>** > **Collecte de données HIP**

Sélectionnez l’onglet **HIP Data Collection (Collecte de données HIP)** pour définir les données que l’application collecte à partir du point de terminaison du rapport HIP :

Paramètres de Configuration de collecte des données HIP GlobalProtect	Description
Collecter les données HIP	Désactivez cette option pour empêcher l'application de collecter et d'envoyer des données HIP. *Activez la collecte des données HIP pour l’application de la politique fondée sur HIP sur GlobalProtect, pour que le pare-feu puisse associer les données HIP des points de terminaison aux objets HIP et/ou aux profils HIP que vous définissez, puis appliquez la politique appropriée.*
Temps d’attente max (sec)	Indiquez le nombre de secondes que l'application doit rechercher des données HIP avant de soumettre les données disponibles (plage comprise entre 10 et 60 ; 20 par défaut).

Paramètres de Configuration de collecte des données HIP GlobalProtect	Description
Profil du certificat	Sélectionnez le profil de certificat que le portail GlobalProtect utilise pour apparier le certificat de machine envoyé par l'application GlobalProtect.
Exclure les catégories	Sélectionnez **Exclude Categories (Exclure catégories)** pour définir les catégories d'informations sur l'hôte pour lesquelles vous ne souhaitez pas que l'application collecte des données HIP. Sélectionnez une **Category (Catégorie)** (comme la prévention de la perte de données) à exclure de la collecte HIP. Après avoir sélectionné une catégorie, vous pouvez **Add (Ajouter)** un Fournisseur particulier, puis vous pouvez **Add (Ajouter)** des produits spécifiques en provenance du fournisseur pour affiner l'exclusion au besoin. Cliquez sur **OK** pour sauvegarder les paramètres dans chaque dialogue.
Vérifications personnalisées	Sélectionnez **Custom Checks (Vérifications personnalisées)** pour définir les informations personnalisées sur l'hôte que l'application doit collecter. Par exemple, si vous disposez d'applications non incluses dans les listes de fournisseurs et/ou de produits, qui sont requises pour la création d'objets HIP, vous pouvez créer une vérification personnalisée qui vous permet de déterminer si l'application est installée (doit avoir une clé de registre Windows ou Plist Mac correspondante) ou est présentement en cours d'exécution (a un processus en cours d'exécution correspondant) : • **Windows** : **Add (Ajouter)** pour ajouter une vérification d'une clé de registre et/ou d'une valeur de clé particulière. • **Mac** : **Add (Ajouter)** pour ajouter une vérification d'une clé plist ou d'une valeur de clé particulière. • **Process List (Liste des processus)** : **Add (Ajouter)** les processus que vous souhaitez vérifier sur les terminaux de l'utilisateur pour voir s'ils sont en cours d'exécution. Par exemple, pour déterminer si une application est en cours d'exécution, ajoutez le nom du fichier exécutable à la liste des processus. Vous pouvez ajouter une liste de processus dans l'onglet **Windows** ou **Mac**.

Onglet des VPN sans client des portails GlobalProtect

- **Réseau** > **GlobalProtect** > **Portails** > ***<portal-config>*** > **VPN sans client**

Vous pouvez désormais configurer le portail GlobalProtect pour fournir un accès distant sécurisé aux applications Web d'entreprise communes qui utilisent les technologies HTML, HTML5 et JavaScript. Les utilisateurs ont l'avantage d'un accès sécurisé à partir de navigateurs Web sur lesquels SSL est activé sans installer le logiciel GlobalProtect. Cela est utile lorsque vous devez activer l'accès à ces applications pour des partenaires ou des entrepreneurs et pour activer de manière sécurisée les actifs non gérés, y compris les appareils personnels. Cette fonctionnalité nécessite que vous installiez un abonnement GlobalProtect sur le pare-feu qui héberge le VPN sans client depuis le portail GlobalProtect. Sélectionnez l'onglet **Clientless**

VPN (VPN sans client) pour configurer les paramètres du VPN sans client de GlobalProtect sur le portail, comme décrit dans le tableau suivant :

Paramètres de configuration sans client du portail GlobalProtect	Description
Onglet Général	
VPN sans client	Sélectionnez **Clientless VPN (VPN sans client)** pour spécifier des informations générales sur la session VPN sans client :
Nom d'hôte	L'adresse IP ou FQDN pour le portail GlobalProtect qui héberge la page de destination des applications Web. Le VPN sans client GlobalProtect réécrit les URL de l'application avec ce nom d'hôte. *Si vous utilisez la Traduction des adresses réseau (NAT) pour fournir un accès au portail GlobalProtect, l'adresse IP ou FQDN que vous saisissez doit correspondre à (ou se résoudre en) l'adresse IP NAT du portail GlobalProtect (l'adresse IP publique).*
Zone de sécurité	La zone pour la configuration VPN sans client. Les règles de sécurité définies dans cette zone contrôlent les applications auxquelles les utilisateurs peuvent accéder.
Proxy DNS	Le serveur DNS qui résout les noms des applications. Sélectionnez un serveur **DNS Proxy (Proxy DNS)** ou configurez un **New DNS Proxy (Nouveau proxy DNS)** (Réseau > Proxy DNS).
Durée de vie de la connexion	Le nombre de **Minutes** (entre 60 et 1 440) ou d'**Hours (Heures)** (entre 1 et 24, la valeur par défaut est 3) durant lequel une session VPN SSL sans client est valide. Après la durée spécifiée, les utilisateurs doivent se réauthentifier et démarrer une nouvelle session VPN sans client.
Délai d'inactivité	Le nombre de **Minutes** (entre 5 et 1 440, la valeur par défaut est 30) ou d'**Hours (Heures)** (entre 1 et 24) durant lequel une session VPN SSL sans client peut rester inactive. S'il n'y a pas d'activité de la part d'un utilisateur pendant la durée spécifiée, il doit se réauthentifier et démarrer une nouvelle session VPN sans client.
Nombre max. d'utilisateurs	Le nombre maximum d'utilisateurs qui peuvent être connectés sur le portail en même temps (la valeur par défaut est 10, la plage est de 1 à aucun maximum). Lorsque le nombre maximum d'utilisateurs est atteint, les utilisateurs VPN sans client supplémentaires ne peuvent pas se connecter au portail.

Paramètres de configuration sans client du portail GlobalProtect	Description
Onglet Applications	
Mappage des applications aux utilisateurs	Vous pouvez **Ajouter** un ou plusieurs **Association des applications aux utilisateurs** pour correspondre aux utilisateurs avec des applications publiées. Cette association définit quels utilisateurs ou groupes d'utilisateurs peuvent utiliser un VPN sans client pour accéder aux applications. Vous devez définir les applications et les groupes d'applications avant de les associer aux utilisateurs (Réseau > GlobalProtect > Applications sans client et Réseau > GlobalProtect > Groupes d'applications sans client). • **Name (Nom)** : donnez un nom au mappage (31 caractères maximum). Le nom est sensible à la casse, doit être unique et peut inclure uniquement des lettres, chiffres, espaces, traits d'union et traits de soulignement. • **Display application URL address bar Allow user to launch unpublished applications (Afficher la barre d'adresse URL d'application)** – Sélectionnez cette option pour afficher une barre d'adresse URL à partir de laquelle les utilisateurs peuvent lancer des applications qui ne sont pas publiées sur la page de renvoi des applications. Lorsque cette option est activée, les utilisateurs peuvent cliquer sur le lien **Application URL (URL de l'application)** qui figure sur la page et indiquer une URL.
Utilisateur/Groupe d'utilisateurs	Vous pouvez **Add (Ajoutez)** des utilisateurs individuels ou des groupes d'utilisateurs auxquels appliquer la configuration d'application actuelle. Ces utilisateurs ont la permission de lancer les applications configurées à l'aide d'un VPN sans client GlobalProtect. *Vous devez configurer l'association de groupe (**Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Group Mapping Settings (Paramètres d'association des groupes)**) avant de pouvoir sélectionner les groupes.* En plus des utilisateurs et des groupes, vous pouvez spécifier quand ces paramètres sont applicables aux utilisateurs ou groupes : • **any (tous)** : la configuration de l'application s'applique à tous les utilisateurs (pas besoin d'**Add (Ajouter)** des utilisateurs ou des groupes d'utilisateurs). • **select (sélectionner)** : la configuration d'application s'applique uniquement aux utilisateurs et groupes d'utilisateurs que vous souhaitez **Add (Ajouter)** à cette liste.

Paramètres de configuration sans client du portail GlobalProtect	Description
Applications	Vous pouvez **Ajouter** des applications individuelles ou des groupes d'applications à l'association. Les **Source Users (Utilisateurs source)** que vous avez inclus à la configuration peuvent utiliser le VPN sans client GlobalProtect pour lancer les applications que vous ajoutez.
Onglet Paramètres Chiffrement	
Versions du protocole	Sélectionnez les versions TLS/SSL minimales et maximales requises. Plus la version TLS est élevée, plus la connexion est sécurisée. Les choix comprennent **SSLv3**, **TLSv1.0**, **TLSv1.1** ou **TLSv1.2**.
Algorithmes d'échange de clés	Sélectionnez les types d'algorithmes pris en charge pour l'échange de clés. Les choix comprennent **RSA**, Diffie-Hellman (**DHE**) ou Diffie-Hellman basé sur les courbes elliptiques éphémères (**ECDHE)**.
Algorithmes de chiffrement	Sélectionnez les algorithmes de cryptage pris en charge. **AES128** ou supérieur est recommandé.
Algorithmes d'authentification	Sélectionnez les algorithmes d'authentification pris en charge. Les choix sont les suivants : **MD5**, **SHA1**, **SHA256** ou **SHA384**. **SHA256** ou supérieur est recommandé.
Vérification des certificats du serveur	Choisissez les mesures à prendre pour les problèmes suivants, qui peuvent survenir lorsqu'une application présente un certificat de serveur : • **Block sessions with expired certificate (Bloquer les sessions avec un certificat expiré)** : si le certificat du serveur a expiré, bloquez l'accès à l'application. • **Block sessions with untrusted issuers (Bloquer les sessions avec des émetteurs non approuvés)** : si le certificat du serveur est émis à partir d'une autorité de certification non approuvée, bloquez l'accès à l'application. • **Block sessions with unknown certificate status (Bloquer les sessions dont l'état du certificat est inconnu)** : si le service OCSP ou CRL renvoie un état de révocation de certificat `unknown (inconnu)`, bloquez l'accès à l'application. • **Block sessions on certificate status check timeout (Bloquer les sessions dont le délai d'attente de vérification de l'état du certificat a expiré)** : si l'état du certificat vérifie les délais avant de recevoir une réponse de tout service d'état du certificat, bloquez l'accès à l'application.
Onglet Proxy	

Paramètres de configuration sans client du portail GlobalProtect	Description
Nom	Une étiquette qui se compose d'un maximum de 31 caractères afin de permettre l'identification du serveur proxy que le portail GlobalProtect utilise pour accéder aux applications publiées. Le nom est sensible à la casse, doit être unique et peut inclure uniquement des lettres, chiffres, espaces, traits d'union et traits de soulignement.
Domaines	Ajoutez les domaines servis par le serveur proxy.
Utiliser le proxy	Sélectionnez cette option pour autoriser le portail GlobalProtect à utiliser le serveur proxy pour accéder aux applications publiées.
Serveur Port	Spécifiez le nom d'hôte (ou l'adresse IP) et le numéro de port du serveur proxy.
Utilisateur Mot de passe	Spécifiez le nom d'utilisateur et le mot de passe nécessaires pour se connecter au serveur proxy. Saisissez à nouveau le mot de passe pour le vérifier.
Onglet Paramètres avancés	
Réécrire la liste des domaines d'exclusion	(Facultatif) Vous pouvez **Ajouter** des noms de domaine, des noms d'hôte ou des adresses IP pour **Rewrite Exclude Domain List (Réécrire la liste des domaines d'exclusion)**. Le VPN sans client agit comme un proxy inversé et modifie les pages renvoyées par les applications publiées. Lorsqu'un utilisateur distant accède à l'URL, les demandes passent par le portail GlobalProtect. Dans certains cas, l'application peut comporter des pages auxquelles il n'est pas nécessaire d'accéder via le portail. Spécifiez les domaines qui doivent être exclus des règles de réécriture et qui ne peuvent pas être réécrits. Les chemins ne sont pas pris en charge dans les noms d'hôte et de domaine. Le caractère générique (*) pour les noms d'hôte et de domaine ne peut apparaître qu'au début du nom (par exemple, * .etrade.com).

Onglet du satellite du portail GlobalProtect

- **Réseau** > **GlobalProtect** > **Portails** > ***<portal-config>*** > **Satellite**

Un satellite est un pare-feu Palo Alto Networks®, généralement dans une succursale, qui agit en tant qu'application GlobalProtect pour permettre au satellite d'établir une connectivité VPN avec une passerelle GlobalProtect. Comme une application GlobalProtect, le satellite reçoit sa configuration initiale du portail, qui inclut les certificats et les informations de routage de configuration VPN lui permettant de se connecter à toutes les passerelles configurées pour établir une connectivité VPN.

Avant de définir les paramètres de configuration satellite GlobalProtect sur le pare-feu de la succursale, vous devez configurer une interface dotée de la connectivité WAN, puis paramétrer une zone de sécurité et une politique, afin d'autoriser le réseau LAN de la succursale à communiquer avec Internet. Vous pouvez ensuite sélectionner l'onglet **Satellite** pour configurer les paramètres de configuration satellite GlobalProtect sur le portail, comme décrit dans le tableau suivant :

Paramètres de configuration satellite du portail GlobalProtect	Description
Général	• **Name (Nom)** : un nom pour cette configuration satellite sur le portail GlobalProtect. • **Configuration Refresh Interval (hours) (Intervalle d'actualisation de la configuration (heures))** : la fréquence à laquelle le satellite doit rechercher des mises à jour de la configuration sur le portail (par défaut 24, plage de 1 à 48).
Périphériques	**Add (Ajouter)** un satellite en utilisant le **Serial Number (Numéro de série)** du pare-feu. Le portail peut accepter un numéro de série ou des identifiants de connexion pour identifier qui demande une connexion. Pour authenticate the satellite to the portal for the first time (authentifier le satellite auprès du portail pour la première fois), l'administrateur du satellite doit fournir un nom d'utilisateur et un mot de passe. Une fois que le satellite s'est authentifié avec succès, le **Satellite Hostname (nom d'hôte du satellite)** est automatiquement ajouté au portail.
Utilisateur/Groupe d'utilisateurs d'inscription	Le portail peut utiliser les paramètres **Enrollment User/User Group (Inscription utilisateur/groupe d'utilisateurs)** avec ou sans les numéros de série pour faire correspondre un satellite à cette configuration. **Add (Ajouter)** l'utilisateur ou le groupe que vous souhaitez contrôler avec cette configuration. *Avant de pouvoir limiter la configuration à des groupes spécifiques, vous devez activer Mappage du groupe dans le pare-feu (**Device (Périphérique)** > **User Identification (Identification utilisateur)** > **Group Mapping Settings (Paramètres de mappage de groupe)**).*
Passerelles	Cliquez sur **Add (Ajouter)** pour saisir l'adresse IP ou le nom d'hôte de la ou des passerelles par lesquelles les satellites dans cette configuration peuvent établir des tunnels IPSec. Dans le champ **Gateways (Passerelles)**, saisissez le nom de domaine complet, FQDN, ou l'adresse IP de l'interface sur laquelle la passerelle est configurée. Les adresses IP peuvent être spécifiées en tant que **IPv6**, **IPv4**, ou les deux. Sélectionnez **IPv6 Preferred (IPv6 Privilégié)** pour spécifier la préférence des connexions IPv6 dans un environnement en double pile.

Paramètres de configuration satellite du portail GlobalProtect	Description
	(Facultatif) Si vous ajoutez deux passerelles ou plus à la configuration, la **Routing Priority (Priorité de routage)** aide le satellite à choisir la passerelle préférée (plage de 1 à 25). Les nombres inférieurs ont une priorité plus élevée (pour les passerelles qui sont disponibles). Le satellite multiplie la priorité de routage par 10 pour déterminer la mesure de routage. *Les itinéraires publiés par la passerelle sont installés sur le satellite en tant qu'itinéraires statiques. La mesure de l'itinéraire statique correspond à 10 fois la priorité de routage. Si vous disposez de plusieurs passerelles, veillez à définir également la priorité d'itinéraire pour s'assurer que les itinéraires publiés par les passerelles de secours incluent des mesures supérieures aux mêmes itinéraires publiés par les passerelles principales. Par exemple, si vous définissez la priorité de routage de la passerelle principale et de la passerelle de secours sur 1 et 10, respectivement, le satellite utilisera la mesure 10 pour la passerelle principale et 100 pour la passerelle de secours.* Le satellite partage également son réseau et les informations de routage avec les passerelles si vous **Publish all static and connected routes to Gateway (Publiez toutes les routes statiques et connectées à la passerelle)** (**Network (Réseau)** > **IPSec tunnels (Tunnels IPSec)** > **<tunnel** > **Advanced (Avancé)** - disponible uniquement lorsque vous sélectionnez **GlobalProtect Satellite on the <tunnel (Satellite GlobalProtect sur le <tunnel** > **General (Général)**).
CA racine approuvée	Cliquez sur **Add (Ajouter)**, puis sélectionnez le certificat AC utilisé pour générer les certificats serveur de passerelle. Les certificats de l'autorité de certification racine de confiance sont transmis aux points de terminaison en même temps que la configuration de l’agent du portail. *Spécifiez une autorité de certification racine de confiance pour vérifier les certificats du serveur de la passerelle et pour établir des connexions de tunnel VPN aux passerelles GlobalProtect. Il est recommandé que toutes vos passerelles utilisent le même émetteur.* *Vous pouvez cliquer sur **Import (Importer)** ou **Generate (Générer)** un certificat AC racine pour la délivrance de certificats de vos serveurs de passerelle si un n'existe pas déjà sur le portail.*

Paramètres de configuration satellite du portail GlobalProtect	Description
Certificat du client	
Local	• **Issuing Certificate (Publication du certificat)** – Sélectionnez le CA racine qui émet le certificat utilisé par le portail pour émettre des certificats à un satellite après la réussite de son authentification. Si le certificat nécessaire n'existe pas déjà sur le pare-feu, vous pouvez **Import (Importer)** ou**Generate (Générer).** *Si un certificat ne réside pas déjà sur le pare-feu, vous pouvez **Import (Importer)** ou **Generate (Générer)** un certificat d'émission.* • **OCSP Responder (Répondeur OCSP)** – Sélectionnez le Répondeur OCSP utilisé par le satellite pour vérifier le statut de révocation des certificats présentés par le portail et les passerelles. Sélectionnez **None (Aucun)** pour spécifier qu'OCSP n'est pas utilisé pour la vérification de la révocation d'un certificat. *Activez un répondeur OCSP de satellite de sorte que vous soyez avisé de la révocation éventuelle d'un certificat afin de pouvoir prendre les mesures appropriées pour établir une connexion sécurisée au portail et aux passerelles. Pour activer un répondeur OCSP de satellite, vous devez également activer **CRL** et **OCSP** dans les paramètres Certificate Revocation Checking (Vérification de la révocation du certificat) (**Device [Périphérique]** > **Setup [Configuration]** > **Session** > **Decryption Settings [Paramètres de déchiffrement]**).* • **Validity Period (Période de validité)** (jours) – Spécifiez la durée de vie du certificat du satellite GlobalProtect (la plage est de 7 à 365 ; 7 par défaut). • **Certificate Renewal Period (Période de renouvellement du certificat)** (jours) – Indiquez le nombre de jours avant l'expiration pendant lesquels les certificats peuvent être renouvelés automatiquement (plage est de 3 à 30 ; 3 par défaut).
SCEP	• **SCEP** – Sélectionnez un profil SCEP pour générer des certificats clients. Si le profil n'est pas dans le menu déroulant, vous pouvez créer un **Nouveau** profil. • **Certificate Renewal Period (Période de renouvellement du certificat)** (jours) – Indiquez le nombre de jours avant

Paramètres de configuration satellite du portail GlobalProtect	Description
	l’expiration pendant lesquels les certificats peuvent être renouvelés automatiquement (plage est de 3 à 30 ; 3 par défaut).

Réseau > GlobalProtect > Passerelles

Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Gateways (Passerelles)** pour configurer une passerelle GlobalProtect. Une passerelle peut fournir des connexions VPN pour les applications GlobalProtect ou pour les satellites GlobalProtect.

À partir de la boîte de dialogue Passerelle GlobalProtect, **Ajouter** une nouvelle configuration de passerelle ou sélectionnez une configuration de passerelle existante pour la modifier.

Que voulez-vous faire ?	Reportez-vous à la section :
Quels paramètres généraux puis-je configurer pour la passerelle GlobalProtect ?	Onglet Général des passerelles GlobalProtect
Comment puis-je configurer l'authentification de la passerelle client ?	Onglet d’authentification de la passerelle GlobalProtect
Comment puis-je configurer les tunnels et les paramètres réseau qui permettent à une application d'établir un tunnel VPN avec la passerelle ?	Onglet Agent de passerelles GlobalProtect
Comment puis-je configurer les paramètres du tunnel et de réseau pour permettre aux satellites d'établir des connexions VPN avec une passerelle agissant comme un satellite?	Onglet GlobalProtect Gateway Satellite(Satellite de la passerelle GlobalProtect)
Vous souhaitez en savoir plus ?	Pour obtenir des instructions détaillées sur la configuration du portail, reportez-vous à la section Configuration d’un portail GlobalProtect du Guide de l’administrateur de GlobalProtect.

Onglet Général des passerelles GlobalProtect

- **Réseau** > **GlobalProtect** > **Passerelles** > ***<gateway-config>*** > **Général**

Sélectionnez l’onglet **General (Général)** pour définir l’interface de passerelle à laquelle les applications peuvent se connecter et indiquer comment la passerelle authentifie les points de terminaison.

Paramètres généraux d’une passerelle GlobalProtect	Description
Name (Nom)	Donnez un nom à la passerelle (**31** caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement.
Location (Emplacement)	Pour un pare-feu en mode Plusieurs systèmes virtuels, **Location (Emplacement)** correspond au système virtuel (vsys) sur lequel la passerelle GlobalProtect est disponible. Pour un pare-feu non en mode Plusieurs systèmes virtuels, le champ **Location (Emplacement)** n'apparaît pas dans la boîte de dialogue Passerelle GlobalProtect. *Après avoir enregistré la configuration de la passerelle, vous ne pouvez plus changer son **Location (Emplacement)**.*
Paramètres de la zone réseau	
Interface	Sélectionnez le nom de l'interface pare-feu qui servira de l'interface d'entrée pour les terminaux distants. (Ces interfaces doivent déjà exister.) *N’affectez pas un profil de gestion de l’interface qui autorise Telnet, SSH, HTTP ou HTTPS à une interface sur laquelle vous avez configuré un portail ou une passerelle GlobalProtect, car ce faisant vous exposeriez l’interface de gestion à l’Internet. Reportez-vous à la section* Bonnes pratiques de l'accès administratif *pour obtenir de plus amples précisions sur la manière de protéger l’accès à votre réseau de gestion.*
Adresse IP	(Facultatif) Spécifiez l'adresse IP d'accès à la passerelle. Sélectionnez le **Type d’adresse IP**, puis saisissez l’**Adresse IP**. • L’adresse IP peut être de type **IPv4** (trafic IPv4 uniquement), **IPv6** (trafic IPv6 uniquement) ou **IPv4 et IPv6**. Utilisez **IPv4 et IPv6** si votre réseau prend en charge les configurations en double pile, où IPv4 et IPv6 fonctionnent en même temps. L’adresse IP doit être compatible avec le type d’adresse IP. Par exemple, 172.16.1.0 pour IPv4 ou 21DA:D3:0:2F3b pour IPv6. Si vous choisissez **IPv4 et IPv6**, saisissez le type d’adresse appropriée pour chacun.
Paramètres des journaux	
Journaliser une communication SSL réussie	(En option) Crée des journaux détaillés des communication de décryptage SSL réussies. Cette option est désactivée par défaut.

Paramètres généraux d'une passerelle GlobalProtect	Description
	Les journaux consomment de l'espace de stockage. Avant de journaliser les communications SSL réussies, assurez-vous d'avoir les ressources nécessaires pour stocker les journaux. Modifiez ***Device (Périphérique)*** > ***Setup (Configuration)*** > ***Management (Gestion)*** > ***Logging and Reporting Settings (Paramètres de journalisation et de création de rapports)*** *pour vérifier l'attribution de mémoire de journaux actuelle et réattribuer de la mémoire de journaux entre les types de journaux.*
Journaliser une communication SSL avortée	Crée des journaux détaillés des communications de décryptage SSL avortées afin que vous puissiez trouver la cause des problèmes de décryptage. Cette option est activée par défaut. *Les journaux consomment de l'espace de stockage. Pour attribuer plus (ou moins) d'espace de stockage de journaux aux journaux de décryptage, modifiez l'attribution de mémoire de journaux (****Device (Périphérique)*** > ***Setup (Configuration)*** > ***Management (Gestion)*** > ***Logging and Reporting Settings (Journalisation et création de rapports)****).*
Transfert des journaux	Indiquez la méthode et l'emplacement de transfert des journaux (de décryptage) de communication GlobalProtect SSL.

Onglet d'authentification de la passerelle GlobalProtect

- **Réseau** > **GlobalProtect** > **Passerelles** > ***<gateway-config>*** > **Authentification**

Sélectionnez l'onglet **Authentication (Authentification)** pour identifier le profil de service SSL/TLS et pour configurer les détails de l'authentification du client. Vous pouvez ajouter plusieurs configurations d'authentification du client.

Paramètres d'authentification de la passerelle GlobalProtect	
Profil de service SSL/TLS	Sélectionnez un profil de service SSL/TLS pour sécuriser cette passerelle GlobalProtect. Pour obtenir des renseignements sur les contenus d'un profil de service, reportez-vous à la section Périphérique > Gestion des certificats > Profil de service SSL/TLS.
Zone d'Authentification du Client	

Paramètres d’authentification de la passerelle GlobalProtect	
Name (Nom)	Saisissez un Nom unique pour identifier cette configuration.
Système d’exploitation	Par défaut, la configuration s'applique à tous les points de terminaison. Vous pouvez filtrer la liste des points de terminaison par système d’exploitation (**Android**, **Chrome, iOS, IoT [IdO], Linux**, **Mac**, **Windows** ou**WindowsUWP**), par périphériques **Satellite,** ou par clients VPN IPSec tiers (**X-Auth**). Le système d'exploitation est le différentiateur principal entre plusieurs configurations. Si vous avez besoin de plusieurs configurations pour un système d'exploitation, vous pouvez en outre distinguer les configurations par votre choix de profil d'authentification. *Ordonnez les configurations des plus spécifiques au sommet de la liste aux plus générales en bas.*
Profil d'authentification	Choisissez un profil ou une séquence d'authentification de la liste déroulante pour l'accès à la passerelle. Reportez-vous à la section Périphérique > Profil d’authentification. *Aux fins d'authentification du client, assurez-vous que le profil d'authentification utilise RADIUS ou SAML avec l’authentification à deux facteurs. Si vous n’utilisez pas RADIUS ou SAML, vous n'avez pas à configurer un profil de certificat en plus d’un profil d’authentification.*
Étiquette de nom d’utilisateur	Indiquez une étiquette de nom d’utilisateur personnalisée pour la connexion à la passerelle GlobalProtect. Par exemple, **Nom d’utilisateur (uniquement)** ou **Adresse électronique (nomd’utilisateur@domaine)**.
Étiquette de mot de passe	Indiquez une étiquette de mot de passe personnalisée pour la connexion à la passerelle GlobalProtect. Par exemple, **Mot de passe (Turc)** ou **Code secret** (pour l’authentification basée sur jeton à deux facteurs).
Message d'authentification	Pour aider les utilisateurs finaux à connaître les informations d'identification qu'ils doivent utiliser pour se connecter à cette passerelle, vous pouvez saisir un message ou garder le message par défaut. Le message peut avoir un maximum de 256 caractères.

Paramètres d’authentification de la passerelle GlobalProtect	
Permettre l’authentification avec les informations d'identification de l'utilisateur OU le certificat du client	Si vous sélectionnez **No (Non)**, les utilisateurs doivent s’authentifier auprès de la passerelle en utilisant les informations d'identification de l'utilisateur et les certificats de client. Si vous sélectionnez **Yes (Oui)**, les utilisateurs peuvent s’authentifier auprès de la passerelle en utilisant les informations d'identification de l'utilisateur ou les certificats de client.
Profil du certificat	
Profil du certificat	(Facultatif) Sélectionnez le **Profil du certificat** que le portail utilise pour correspondre aux certificats clients qui proviennent des points d’extrémité utilisateur. Avec un Profil de certificat, la passerelle n'authentifie l'utilisateur que si le certificat du client correspond à ce profil. Si vous établissez l’option **Allow Authentication with User Credentials OR Client Certificate (Permettre l’authentification avec les informations d'identification de l'utilisateur OU le certificat du client)** sur **No (Non)**, vous devez sélectionner un **Certificate Profile (Profil de certificat)**. Si vous établissez l’option **Allow Authentication with User Credentials OR Client Certificate (Permettre l’authentification avec les informations d'identification de l'utilisateur OU le certificat du client)** sur **Yes (Oui)**, le **Certificate Profile (Profil de certificat)** est facultatif. Le profil de certificat est indépendant du système d'exploitation.
Bloquer une connexion pour les périphériques en quarantaine	Indiquez si vous voulez bloquer la connexion à la passerelle pour les périphériques clients GlobalProtect qui sont dans la liste de quarantaine (**Device (Périphérique)** > **Device Quarantine (périphériques en quarantaine)**).

Onglet Agent de passerelles GlobalProtect

- **Réseau** > **GlobalProtect** > **Portails** > **<*portal-config*>** > **Agent**

Sélectionnez l’onglet **Agent** pour configurer les paramètres du tunnel qui permettent à l’application d’établir un tunnel VPN avec la passerelle. En outre, cet onglet vous permet de spécifier les délais d’attente pour les VPN, les services de réseau de DNS et WINS, et les messages de notification de HIP pour les utilisateurs finaux sur la correspondance ou non à un profil de HIP attaché à une règle de politique de Sécurité.

Configurer les paramètres de l'Agent sur les onglets suivants :

- Onglet Paramètres du tunnel
- Onglet Paramètres du client

- Onglet Pools d’adresses IP du client
- Onglet Services du réseau
- Onglet Paramètres de connexion
- Onglet Trafic vidéo
- Onglet Notification HIP

Onglet Paramètres du tunnel

- **Réseau** > **GlobalProtect** > **Passerelles** > **<*gateway-config*>** > **Agent** > **<*agent-config*>** > **Paramètres du tunnel**

Sélectionnez l’onglet **Tunnel Settings (Paramètres du tunnel)** pour activer la tunnellisation et configurer les paramètres du tunnel.

Les paramètres de tunnel doivent être définis si vous configurez une passerelle externe. Si vous configurez une passerelle interne, les paramètres de tunnel sont facultatifs.

Paramètres de configuration du mode tunnel du client GlobalProtect	Description
Mode tunnel	Sélectionnez le **Tunnel Mode (Mode tunnel)** pour activer le mode tunnel, puis spécifiez les paramètres suivants : • **Tunnel Interface (Interface de tunnel)** - Choisissez une interface de tunnel pour l'accès à la passerelle. • **Max User (Nombre max. d'utilisateurs)** - Précisez le nombre maximum d'utilisateurs pouvant accéder à la passerelle simultanément, pour l'authentification ainsi que les mises à jour HIP et de l'application GlobalProtect. Si le nombre maximum d'utilisateurs est atteint, les utilisateurs suivants se voient refuser l'accès et un message d'erreur indiquant que le nombre maximum d'utilisateurs est atteint s'affiche (la plage varie d’une plateforme à l’autre et s’affiche lorsque le champ est vide). • **Enable IPSec (Activer IPSec)** - Sélectionnez cette option pour activer le mode IPSec pour le trafic des points de terminaison, IPSec devenant ainsi la méthode principale et SSL-VPN la méthode de secours. Les autres options ne sont pas disponibles jusqu'à ce qu’IPSec soit activé. • **GlobalProtect IPSec Crypto (Crypto IPSec GlobalProtect)** - Sélectionnez un profil crypto IPSec GlobalProtect qui définit les algorithmes d'authentification et de cryptage pour les tunnels VPN. Le profil **default (par défaut)** utilise le cryptage AES-128-CBC et l'authentification SHA1. Pour plus d’informations, reportez-vous à Réseau > Profils réseau > Crypto IPSec GlobalProtect. • **Enable X-Auth Support (Activer la prise en charge X-Auth)** - Sélectionnez cette option pour activer la prise en charge Extended Authentication (X-Auth) dans la passerelle GlobalProtect lorsque

Paramètres de configuration du mode tunnel du client GlobalProtect	Description
	le mode IPSec est activé. La prise en charge X-Auth permet aux clients VPN IPSec tiers prenant en charge X-Auth (le client VPN IPSec sur les périphériques Apple iOS et Android et le client VPNC sous Linux, par exemple) d'établir un tunnel VPN avec la passerelle GlobalProtect. L'option X-Auth permet au client VPN d'accéder à distance à une passerelle GlobalProtect. Comme l'accès X-Auth fournit des fonctionnalités GlobalProtect limitées, songez à utiliser l'application GlobalProtect pour pouvoir accéder facilement à l'ensemble des fonctions de sécurité offertes par GlobalProtect sur les périphériques iOS et Android. En sélectionnant **X-Auth Support (Prise en charge X-Auth)** pour activer les options **Group Name (Nom du groupe)** et **Group Password (Mot de passe du groupe)** : • Si le nom et le mot de passe de groupe sont précisés, la première phase d'authentification requiert que les deux parties utilisent ces informations d'identification pour s'authentifier. La seconde phase requiert un nom d'utilisateur et un mot de passe valides, qui sont définis dans le profil d'authentification configuré dans la section Authentification. • Si aucun nom et mot de passe de groupe n'est défini, la première phase d'authentification est basée sur un certificat valide présenté par le client VPN tiers. Ce certificat est ensuite validé dans le profil du certificat configuré dans la section Authentification. • Par défaut, l'utilisateur ne doit pas se réauthentifier lorsque la clé utilisée pour établir le tunnel IPSec expire. Pour exiger que l'utilisateur se réauthentifie, décochez l'option **Skip Auth on IKE Rekey (Ignorer l'authentification lors du renouvellement de la clé)**.

Onglet Paramètres du client

- **Réseau** > **GlobalProtect** > **Passerelles** > ***<gateway-config>*** > **Agent** > ***<agent-config>*** > **Paramètres du client**

Sélectionnez l'onglet **Paramètres du client** pour configurer les paramètres de la carte réseau virtuelle sur le point de terminaison lorsque l'application GlobalProtect établit un tunnel avec la passerelle.

Certaines options Paramètres du client sont uniquement disponibles si vous avez activé le mode tunnel et défini une interface de tunnel dans l'onglet Paramètres du tunnel.

Paramètres de la passerelle client GlobalProtect et configuration réseau	Description
Critères de sélection de la configuration	
Nom	Saisissez un nom pour identifier la configuration des paramètres du client (jusqu'à 31 caractères). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Utilisateur source	**Ajouter** les groupes d'utilisateurs ou les utilisateurs spécifiques auxquels cette configuration s'applique. *Vous devez configurer le mappage de groupe (**Périphérique** > **Identification Utilisateur** > **Paramètres de mappage des groupes**) avant de pouvoir sélectionner les utilisateurs et les groupes.* Pour déployer cette configuration à tous les utilisateurs, sélectionnez **tout** dans le menu déroulant **Utilisateur source**. Pour déployer cette configuration uniquement aux utilisateurs disposant d'applications GlobalProtect en mode préouverture de session, sélectionnez **préouverture de session** dans le menu déroulant **Utilisateur source**. *La configuration des paramètres du client est déployée aux utilisateurs uniquement si l'utilisateur correspond aux critères définis pour **Utilisateur source**, **Système d'exploitation** et **Adresse source**.*
Système d'exploitation	Pour déployer cette configuration selon le système d'exploitation du point de terminaison, vous devez **Ajouter** un système d'exploitation (**Android**, **Chrome**, **iOS**, **IdO**, **Linux**, **Mac**, **Windows** ou **WindowsUWP**). Vous pouvez également définir cette valeur sur **toute**, de sorte que la configuration de déploiement est basée uniquement sur le groupe d'utilisateurs ou l'utilisateur et non pas sur le système d'exploitation du point de terminaison. *La configuration des paramètres du client est déployée aux utilisateurs uniquement si l'utilisateur correspond aux critères définis pour **Utilisateur source**, **Système d'exploitation** et **Adresse source**.*

Paramètres de la passerelle client GlobalProtect et configuration réseau	Description
Adresse source	Pour déployer cette configuration selon l'emplacement de l'utilisateur, **Ajoutez** une **Region** source ou une **Adresse IP** locale (IPv4 et IPv6). Pour déployer cette configuration à tous les emplacements d'utilisateurs, ne précisez aucune **Région** ou **Adresse IP**. Vous devez également laisser ces champs vides si vos utilisateurs utilisent la version 4.0 ou une version antérieure de l'application GlobalProtect, car cette fonction n'est pas prise en charge sur les versions antérieures de l'application GlobalProtect. *La correspondance de la **Adresse source** réussit si l'emplacement d'un utilisateur se connectant correspond à la **Région** ou à la **IP Address (Adresse IP)** que vous configurez.* *La configuration des paramètres du client est déployée aux utilisateurs uniquement si l'utilisateur correspond aux critères définis pour **Utilisateur source**, **Système d'exploitation** et **Adresse source**.*
Onglet de Contournement d'authentification	
Contournement d'Authentification	Activer la passerelle pour utiliser des témoins sécurisés, spécifiques au périphérique et chiffrés pour authentifier l'utilisateur une fois que l'utilisateur s'identifie pour la première fois en utilisant le régime d'authentification spécifié par le profil d'authentification ou le certificat. • **Generate cookie for authentication override (Générer témoin pour contournement de l'authentification)** : Pendant la durée de vie du témoin, l'agent présente ce témoin chaque fois que l'utilisateur s'authentifie avec la passerelle. • **Durée de vie des cookies** : spécifiez les heures, les jours ou les semaines pour lesquelles le témoin est valide. La durée de vie typique est de 24 heures. Les plages sont 1 à 72 heures, 1 à 52 semaines ou 1 à 365 jours. Après l'expiration du témoin, l'utilisateur doit entrer les informations d'identification et le portail chiffre ensuite un nouveau témoin à envoyer à l'utilisateur terminal. • **Accepter le témoin pour écraser l'authentification** : Sélectionnez cette option pour configurer la passerelle pour accepter l'authentification en utilisant le témoin chiffré. Lorsque l'agent présente le témoin, la passerelle

Paramètres de la passerelle client GlobalProtect et configuration réseau	Description
	valide que le témoin a été chiffré par la passerelle avant l'authentification de l'utilisateur. • **Certificat pour chiffrer/déchiffrer le témoin** : Sélectionnez le certificat à utiliser pour chiffrer et déchiffrer le témoin. *Veiller à ce que le portail et la passerelle utilisent le même certificat pour chiffrer et déchiffrer les témoins.*
Onglet Pools d’adresses IP	
Récupérer l'attribut Adresse IP tramée auprès du serveur d'authentification	Sélectionnez cette option pour permettre à la passerelle GlobalProtect d'attribuer des adresses IP fixes à l'aide d'un serveur d'authentification externe. Lorsque cette option est activée, la passerelle GlobalProtect alloue l'adresse IP pour la connexion à des périphériques en utilisant l'attribut Adresse IP adresse tramée du serveur d'authentification.
Pool d'adresses IP du serveur d'authentification	**Ajouter** un sous-ensemble ou une plage d'adresses IP à attribuer aux utilisateurs distants. Lorsque le tunnel est établi, la passerelle GlobalProtect affecte l'adresse IP dans cette plage aux périphériques se connectant à l'aide de l'attribut Adresse IP tramée du serveur d'authentification. Vous pouvez ajouter des adresses IPv4 (comme 192.168.74.0/24 et 192.168.75.1-192.168.75.100) ou des adresses IPv6 (comme 2001:aa::1-2001:aa::10). Vous pouvez activer et configurer l'**Authentification du serveur du pool d'adresses IP** uniquement si vous activez **Récupérer l'attribut d'adresse IP du serveur d'authentification)**. *le pool d'adresses IP du serveur d'authentification doit être suffisamment important pour prendre en charge toutes les connexions simultanées. L'attribution d'adresse IP est fixe et est conservée une fois l'utilisateur déconnecté. Configure plusieurs plages à partir de différents sous-réseaux permet au système de fournir aux clients une adresse IP non conflictuelle avec les autres interfaces du client.* Les serveurs et les routeurs des réseaux doivent acheminer le trafic de ce pool d'adresses IP vers le pare-feu. Par exemple,

Paramètres de la passerelle client GlobalProtect et configuration réseau	Description
	pour le réseau 192.168.0.0/16, un utilisateur distant peut recevoir l'adresse 192.168.0.10.
Pool d'adresses IP	**Ajouter** une plage d'adresses IP à attribuer aux utilisateurs distants. Une fois le tunnel établi, une interface est créée sur le terminal de l'utilisateur distant avec une adresse de cette plage. Vous pouvez ajouter des adresses IPv4 (comme 192.168.74.0/24 et 192.168.75.1-192.168.75.100) ou des adresses IPv6 (comme 2001:aa::1-2001:aa::10). *pour éviter les conflits, le pool d'adresses IP doit être suffisamment important pour prendre en charge toutes les connexions simultanées. La passerelle gère un index de clients et d'adresses IP de sorte que le client reçoive automatiquement la même adresse IP lors de sa connexion suivante. La configuration de plusieurs plages à partir de différents sous-réseaux permet au système de fournir aux clients une adresse IP non conflictuelle avec les autres interfaces du client.* Les serveurs et les routeurs des réseaux doivent acheminer le trafic de ce pool d'adresses IP vers le pare-feu. Par exemple, pour le réseau 192.168.0.0/16, un utilisateur distant peut se voir attribuer l'adresse 192.168.0.10.
Onglet segmentation du tunnel	
Onglet Itinéraires d'accès	
Aucun accès direct au réseau local	Sélectionnez cette option pour désactiver la segmentation des tunnels, notamment l'accès direct aux réseaux locaux sur les terminaux Windows et MacOS. Cette fonction empêche les utilisateurs d'envoyer du trafic à des proxys ou des ressources locales, une imprimante à domicile par exemple. Lorsque le tunnel est établi, l'ensemble du trafic est acheminé via le tunnel et la mise en œuvre des politiques par le pare-feu s'applique à celui-ci.
Inclure	Veuillez **Ajouter** les itinéraires à inclure dans le tunnel VPN. Ce sont les itinéraires que la passerelle applique au point de terminaison des utilisateurs distants pour préciser les points de terminaison d'utilisateur qui peuvent être envoyés au moyen de la connexion VPN.

Paramètres de la passerelle client GlobalProtect et configuration réseau	Description
	Vous pouvez inclure des sous-réseaux IPv6 ou IPv4. Sur PAN-OS 8.0.2 et les versions ultérieures, un maximum de 100 itinéraires d'accès peuvent être utilisés pour inclure le trafic dans une configuration de passerelle de tunnel séparé. En combinaison avec la version 4.1.x de l'application GlobalProtect ou une version ultérieure, jusqu'à 1 000 itinéraires d'accès peuvent être utilisés. *Pour inclure tous les sous-réseaux de destination ou les objets d'adresses, **Incluez** 0.0.0.0/0 et ::/0 comme itinéraires d'accès.*
Exclure	Veuillez **Ajouter** des itinéraires à exclure du tunnel VPN. Ces itinéraires sont envoyés aux points de terminaison par le biais de l'adaptateur physique plutôt qu'au moyen de la carte virtuelle (le tunnel). Vous pouvez définir les itinéraires que vous envoyez au moyen du tunnel VPN comme des itinéraires que vous incluez dans le tunnel, les itinéraires que vous excluez du tunnel ou une combinaison des deux. Par exemple, vous pouvez paramétrer une segmentation des tunnels pour permettre aux utilisateurs distants d'accéder à Internet sans recourir au tunnel VPN. Les itinéraires exclus doivent être plus spécifiques que les itinéraires inclus pour éviter d'exclure plus de trafic que ce que vous en avez l'intention. Vous pouvez exclure des sous-réseaux IPv6 ou IPv4. Le pare-feu prend en charge un maximum de 100 itinéraires d'accès exclus dans une configuration de passerelle de tunnel séparé. En combinaison avec la version 4.1 de l'application GlobalProtect ou une version ultérieure, jusqu'à 200 itinéraires d'accès exclus peuvent être utilisés. Vous ne pouvez exclure les itinéraires d'accès des terminaux exécutant Android sur Chromebook. Seuls les itinéraires IPv4 sont pris en charge sur les Chromebook. Si vous n'activez pas le split tunneling, chaque demande est acheminée via le tunnel (pas de split tunneling). Dans ce cas, chaque requête Internet passe par le pare-feu puis vers le réseau. Cette méthode peut permettre d'empêcher un tiers externe d'accéder aux terminaux de l'utilisateur et ainsi accéder au réseau interne (le terminal de l'utilisateur servant alors de pont).
Onglet Domaine et Application	

Paramètres de la passerelle client GlobalProtect et configuration réseau	Description
Inclure le Domaine	**Ajoutez** le logiciel à la demande (SaaS) ou les applications sur le cloud public que vous voulez inclure dans le tunnel VPN sur la base du domaine et du port de destination (facultatif). Ce sont les applications que la passerelle applique au point de terminaison des utilisateurs distants pour préciser les points de terminaison d'utilisateur qui peuvent être envoyés au moyen de la connexion VPN. ICMP n'est pas inclus. Vous pouvez ajouter un maximum de 200 entrées à la liste. Par exemple, ajoutez **`*.office365.com`** pour autoriser tout le trafic Office 365 à passer par le tunnel VPN. *Vous pouvez configurer une liste de ports pour chaque domaine. Si aucun port n'est configuré, tous les ports du domaine spécifié sont assujettis à cette politique.*
Exclure un Domaine	**Ajoutez** le logiciel à la demande (SaaS) ou les applications sur le cloud public que vous voulez exclure du tunnel VPN sur la base du domaine et du port de destination (facultatif). Ces applications sont envoyées aux points de terminaison par le biais de l'adaptateur physique plutôt qu'au moyen de la carte virtuelle (le tunnel). Vous pouvez ajouter un maximum de 200 entrées à la liste. Par exemple, ajoutez le domaine **`*.ringcentral.com`** pour exclure tout le trafic RingCentral du tunnel VPN. *Vous pouvez configurer une liste de ports pour chaque domaine. Si aucun port n'est configuré, tous les ports du domaine spécifié sont assujettis à cette politique.* Si vous n'activez pas le split tunneling, chaque demande est acheminée via le tunnel (pas de split tunneling). Dans ce cas, chaque requête Internet passe par le pare-feu puis vers le réseau. Cette méthode peut empêcher des tiers externes d'accéder aux points de terminaison utilisateur dans le but d'obtenir l'accès au réseau interne.
Inclure le Nom de processus de l'application client	**Ajoutez** le chemin complet de chaque processus applicatif dont vous souhaitez inclure le trafic dans votre tunnel VPN. Ce sont les applications que la passerelle applique aux points de terminaison des utilisateurs distants pour préciser ce que ces points de terminaison d'utilisateur peuvent être envoyés

Paramètres de la passerelle client GlobalProtect et configuration réseau	Description
	au moyen de la connexion VPN. Vous pouvez ajouter un maximum de 200 entrées à la liste. Par exemple, ajoutez **`/Application/Safari.app/Contents/MacOS/Safari`** pour autoriser tout le trafic Safari à passer par le tunnel VPN sur les points de terminaison MacOS.
Exclure le Nom de processus de l'application client	**Ajoutez** le chemin complet de chaque processus applicatif pour lequel vous souhaitez exclure le trafic de votre tunnel VPN. Ces applications sont envoyées aux points de terminaison par le biais de l'adaptateur physique plutôt qu'au moyen de la carte virtuelle (le tunnel). Vous pouvez ajouter un maximum de 200 entrées à la liste. Par exemple, pour exclure le trafic de l'application RingCentral : • Pour les terminaux Windows, ajoutez **`%AppData%\Local\RingCentral\SoftPhoneApp\Softphone.exe`** et **`%AppData%\Local\RingCentral\SoftPhoneApp\SoftphoneMapiBridge.exe`** • Pour les terminaux macOS, ajoutez **`/Applications/RignCentral for Mac.app/Contents/MacOS/Softphone`** Si vous n'activez pas le split tunneling, chaque demande est acheminée via le tunnel (pas de split tunneling). Dans ce cas, chaque requête Internet passe par le pare-feu puis vers le réseau. Cette méthode peut empêcher des tiers externes d'accéder aux points de terminaison utilisateur dans le but d'obtenir l'accès au réseau interne.
Onglet Services du réseau	
Serveur DNS	Précisez l'adresse IP du serveur DNS auquel l'application GlobalProtect disposant de cette configuration de paramètres du client envoie des requêtes DNS. Vous pouvez ajouter plusieurs serveurs DNS en séparant chaque adresse IP avec une virgule.
Suffixe DNS	Spécifiez le suffixe DNS que le point de terminaison doit utiliser localement lorsqu'un nom d'hôte non qualifié que le point de terminaison ne peut pas résoudre est saisi. Vous pouvez saisir plusieurs suffixes DNS (maximum de 100) en séparant chaque suffixe par une virgule.

Onglet Pools d’adresses IP du client

- **Réseau** > **GlobalProtect** > **Passerelles** > ***<gateway-config>*** > **Agent** > ***<agent-config>*** > **Pools d’adresses IP du client**

Sélectionnez l’onglet **Pool d’adresses IP du client** pour configurer le pool d’adresses IP globales qui est utilisé pour affecter les adresses IPv4 ou IPv6 à tous les points de terminaison qui se connectent à la passerelle GlobalProtect™.

Paramètres de configuration du pool d’adresses IP du client de la passerelle GlobalProtect	Description
Pool d'adresses IP	**Ajouter** une plage d'adresses IPv4 ou IPv6 à attribuer aux utilisateurs distants. Après avoir établi le tunnel, la passerelle GlobalProtect attribue les adresses IP de cette plage à toutes les terminaisons qui se connectent via ce tunnel. *Si vous configurez des pools d'adresses IP au niveau de la passerelle (**Réseau** > **GlobalProtect** > **Passerelles** > **<gateway-config>** > **Configuration de la passerelle GlobalProtect** > **Agent** > **Pool d'adresses IP du client**), ne configurez pas de pools d’adresses IP au niveau du client (**Réseau** > **GlobalProtect** > **Passerelles** > **<gateway-config>** > **Configuration de la passerelle GlobalProtect** > **Agent** > **Paramètres du client** > **<client-setting>** > **Configurations** > **Pool d'adresses IP**).*

Onglet Services du réseau

- **Réseau** > **GlobalProtect** > **Passerelles** > ***<gateway-config>*** > **Agent** > ***<agent-config>*** > **Services du réseau**

Sélectionnez l'onglet **Network Services (Services du réseau)** pour configurer les paramètres DNS qui sont affectés à la carte réseau virtuelle sur le point de terminaison lorsque l'application GlobalProtect établit un tunnel avec la passerelle.

*Les options Services réseau sont disponibles uniquement si vous avez activé le mode tunnel et défini une interface de tunnel dans l’*onglet Paramètres de tunnel.

Paramètres de configuration des services réseau du client GlobalProtect	Description
Source de l'héritage	Sélectionnez une source pour la propagation du serveur DNS et d'autres paramètres entre le client DHCP ou l'interface client PPPoE sélectionné et la configuration des applications GlobalProtect. Grâce à ce paramètre, l'ensemble des configurations du réseau client, les serveurs DNS et WINS par exemple, est hérité de la configuration de l'interface sélectionnée dans Source de l'héritage.
Vérifier l'état de la source de l'héritage	Cliquez sur Source de l'héritage pour consulter les paramètres du serveur actuellement attribués aux interfaces client.
DNS principal DNS secondaire	Saisissez les adresses IP des serveurs principal et secondaire qui fournissent le service DNS aux clients.
WINS principal WINS secondaire	Saisissez les adresses IP des serveurs principal et secondaire qui fournissent le service Windows Internet Name Service (Service d'attribution de nom Internet Windows ; WINS) aux points de terminaison.
Hériter des suffixes DNS	Sélectionnez cette option pour hériter des suffixes DNS de la source de l'héritage.
Suffixe DNS	**Add (Ajouter)** un suffixe que le point de terminaison doit utiliser localement lorsqu'un nom d'hôte non qualifié, qu'il ne peut pas résoudre, est saisi. Vous pouvez saisir plusieurs suffixes (maximum de 100) en les séparant chaque suffixe par une virgule.

Onglet Paramètres de connexion

- **Réseau** > **GlobalProtect** > **Passerelles** > **<*gateway-config*>** > **Agent** > **<*agent-config*>** > **Paramètres de connexion**

Sélectionnez l'onglet **Connection Settings (Paramètres de connexion)** pour définir les paramètres des délais d'expiration et les restrictions d'utilisation de l'authentification par cookie pour l'application GlobalProtect™.

Paramètres de connexion du mode tunnel du client GlobalProtect	Description
Configuration du délai avant expiration	
Durée de vie de la connexion	Indiquez le nombre de jours, heures ou minutes autorisés pour une session de connexion de passerelle.

Paramètres de connexion du mode tunnel du client GlobalProtect	Description
Avertir avant l'expiration de la durée de vie de la connexion	Définissez le temps en minutes (la valeur par défaut est de 30 minutes) pour programmer l'affichage des notifications d'expiration de la durée de vie de la connexion sur l'application GlobalProtect. La **Notify Before Lifetime Expires (notification avant l'expiration de la durée de vie)** doit être inférieure à la **Login Lifetime (durée de vie de la connexion)**.
Message d’expiration de la durée de vie de la connexion	Vous permet de modifier le message d'expiration de durée de vie de connexion par défaut et de créer un message personnalisé que vous souhaitez afficher aux utilisateurs lorsque leurs sessions de durée de vie de connexion sont sur le point d'expirer. La longueur du message est de 127 caractères maximum.
Déconnexion en cas d'inactivité	Spécifiez la durée (en minutes) après laquelle une session inactive est automatiquement déconnectée (la plage pour le mode tunnel est de 5 à 43200 et pour le mode non tunnel de 120 à 43200 minutes ; la valeur par défaut est de 180 minutes). Les utilisateurs sont déconnectés de GlobalProtect si l'application GlobalProtect n'a pas acheminé le trafic via le tunnel VPN ou si la passerelle ne reçoit pas de vérification HIP du point de terminaison au cours de la période configurée.
Notifier avant la déconnexion d’inactivité (minutes)	Définissez le délai de notification avant la déconnexion en cas d'inactivité en minutes (la valeur par défaut est de 30 minutes) pour programmer l'affichage de la notification de déconnexion en cas d'inactivité sur l'application. La **Notify Before Inactivity Logout (notification avant la déconnexion en cas d'inactivité)**doit être inférieure à la **Inactivity Logout period (période de déconnexion en cas d'inactivité)**.
Message de déconnexion pour inactivité	Vous permet de modifier le message par défaut et de créer un message personnalisé que vous souhaitez afficher aux utilisateurs lorsque leurs sessions inactives sont sur le point d'expirer. La longueur du message est de 127 caractères maximum.
Avertir les Utilisateurs lors de la déconnexion initiée par l’Administrateur	Activez cette option si vous souhaitez que l'application affiche une notification aux utilisateurs après la déconnexion initiée par l'administrateur.
Message de déconnexion de l’administrateur	Vous permet de modifier le message par défaut et de créer un message personnalisé que vous souhaitez afficher aux utilisateurs après la déconnexion initiée par l'administrateur. La longueur du message est de 127 caractères maximum.
Restrictions d’utilisation de l’authentification par cookie	

Paramètres de connexion du mode tunnel du client GlobalProtect	Description
Désactivez le rétablissement automatique de SSL VPN	Activez cette option pour empêcher le rétablissement automatique des tunnels SSL VPN. *Si vous activez cette option, GlobalProtect ne prendra pas en charge le VPN résilient.*
Restreindre l'utilisation de l'authentification par cookie (pour la restauration automatique du tunnel VPN ou le contrôle prioritaire de l'authentification) afin de	Activer cette option pour restreindre l'utilisation des cookies à des fins d'authentification selon l'une des conditions suivantes : • **L'adresse IP source d'origine pour laquelle le cookie d'authentification a été émis** : restreint l'utilisation des cookies à des fins d'authentification à des points de terminaison ayant la même adresse IP source publique que le point de terminaison pour lequel le cookie a été initialement émis. • **La plage réseau de l'adresse IP source d'origine** : restreint l'utilisation des cookies à des fins d'authentification à des points de terminaison ayant les mêmes adresses IP source publiques au sein de la plage d'adresses IP réseau désignée. Saisissez un **Source IPv4 Netmask (Masque réseau IPv4 source)** pour spécifier une plage d'adresses IPv4 ou saisissez un **Source IPv6 Netmask (Masque réseau IPv6 source)** pour spécifier une plage d'adresses IPv6. Si vous définissez l'un de ces masques réseau sur **0**, cette option est désactivée pour le type d'adresse IP spécifié. Par exemple,vous pouvez définir un masque réseau sur **0** si votre portail ou votre passerelle ne prend en charge qu'un seul type d'adresses IP (IPv4 ou IPv6) ou si vous souhaitez activer cette option pour un seul type d'adresses IP (lorsque votre portail ou votre passerelle prend en charge IPv4 et IPv6). Vous ne pouvez définir qu'un seul masque réseau sur **0** dans une configuration de passerelle donnée ; vous ne pouvez définir simultanément les deux masques réseau sur **0**. Si vous acceptez la valeur de **Source IPv4 Netmask (Masque réseau IPv4 source)** par défaut, soit **32**, l'utilisation des cookies d'authentification est limitée à la même adresse IPv4 publique du point de terminaison auquel le cookie a initialement été émis. Si vous acceptez la valeur de **Source IPv6 Netmask (Masque réseau IPv6 source)** par défaut, soit **128**, l'utilisation des cookies d'authentification est limitée à la même adresse IPv6 publique du point de terminaison auquel le cookie a initialement été émis.

Onglet Trafic vidéo

- **Réseau** > **GlobalProtect** > **Passerelles** > **<*gateway-config*>** > **Agent** > **<*agent-config*>** > **Trafic vidéo**

Sélectionnez l’onglet **Video Traffic** (Trafic vidéo) pour exclure le trafic de diffusion vidéo du tunnel VPN.

Paramètres de configuration du trafic vidéo de la passerelle GlobalProtect	Description
Exclure les applications vidéo du tunnel	Sélectionnez cette option pour autoriser l’exclusion du trafic de diffusion vidéo du tunnel VPN.
Applications	**Add (Ajoutez)** les applications de diffusion vidéo que vous souhaitez exclure du tunnel VPN ou **Browse (Recherchez)**-les. La redirection vidéo s’applique à tout type de trafic vidéo provenant des applications suivantes : • YouTube • Dailymotion • Netflix Pour les autres applications de diffusion vidéo, seuls les types de vidéo suivants peuvent être redirigés : • MP4 • WebM • MPEG Le trafic de diffusion vidéo peut uniquement être exclu du tunnel VPN. Si vous n’excluez aucune application de diffusion vidéo, toutes les requêtes sont acheminées à travers le tunnel (pas de segmentation des tunnels). Dans ce cas, chaque requête Internet passe par le pare-feu puis vers le réseau. Cette méthode peut empêcher des tiers externes d’accéder aux points de terminaison utilisateur dans le but d’obtenir l’accès au réseau interne.

Onglet Notification HIP

- **Réseau** > **GlobalProtect** > **Passerelles** > **<*gateway-config*>** > **Agent** > **<*agent-config*>** > **Notification HIP**

Sélectionnez l’onglet **HIP Notification (Notification HIP)** pour définir les messages de notification à afficher aux utilisateurs finaux lorsqu'une règle de sécurité dotée d'un profil HIP est mise en œuvre.

Ces options ne sont disponibles que si vous avez créé des profils HIP et les avez ajoutés à vos politiques de sécurité.

Paramètres de configuration de notification HIP de l'agent GlobalProtect	Description
Notification HIP	**Ajouter** des notifications HIP et configurer les options. Vous pouvez **Activer** les notifications pour **Mettre le message en correspondance**, **Ne pas mettre le message en correspondance**, ou les deux puis décider de **Montrer la notification en tant qu'infobulle de la barre des tâches** ou **Message contextuel**. Indiquez ensuite le message pour correspondre ou ne pas correspondre. Utilisez ces paramètres pour informer l'utilisateur final de l'état de la machine, par exemple, pour fournir un message d'avertissement indiquant que le système hôte ne dispose pas d'une application requise. Pour Mettre le message en correspondance, vous pouvez également activer l'option **Include Mobile App List (Inclure la liste des applications mobiles)** pour indiquer les applications qui ont déclenché la correspondance HIP. *Vous pouvez formater les messages de notification HIP en HTML enrichi qui peut inclure des liens vers des sites Web externes et des ressources. Utilisez l'hyperlien (*  *) dans la barre d'outils des paramètres de texte enrichi pour ajouter des liens.*

Onglet GlobalProtect Gateway Satellite(Satellite de la passerelle GlobalProtect)

- **Réseau** > **GlobalProtect** > **Passerelles** > **<*gateway-config*>** > **Satellite**

Un périphérique satellite est un pare-feu Palo Alto Networks, généralement dans une succursale, qui agit en tant qu'application de GlobalProtect pour lui permettre d'établir une connectivité VPN avec une passerelle GlobalProtect. Sélectionnez l'onglet **Satellite** pour définir les paramètres réseau et de tunnel de la passerelle pour que les satellites puissent établir des connexions VPN. Vous pouvez également configurer les itinéraires annoncés par les satellites.

- Onglet Paramètres du tunnel
- Onglet Paramètres du réseau
- Onglet Filtre itinéraire

Paramètres de configuration satellite GlobalProtect	Description
Onglet Paramètres du tunnel	

Paramètres de configuration satellite GlobalProtect	Description
Configuration des tunnels	Sélectionnez **Tunnel Configuration (Configuration tunnel)** et sélectionnez une **Tunnel Interface (Interface tunnel)** existante, ou sélectionnez **New Tunnel Interface (Nouvelle interface tunnel)** à partir du menu déroulant. Voir **Réseau > Interfaces > Tunnel** pour plus d'informations. • **Replay attack detection (Détection des attaques par relecture)** – Protégez-vous contre les attaques par relecture. *Activez **Replay attack detection (Détection des attaques par relecture)** pour protéger les satellites GlobalProtect des attaques par relecture si vous activez la configuration des tunnels des satellites.* • **Copy TOS (Copier ToS)** – Copiez l'en-tête ToS (Type of Service) de l'en-tête IP entrant vers l'en-tête IP sortant des paquets encapsulés pour préserver les informations ToS d'origine. • **Configuration refresh interval (hours) (Intervalle d'actualisation de la configuration (heures))** – Spécifiez la fréquence à laquelle les satellites devraient rechercher des mises à jour de la configuration sur le portail (par défaut 2, plage de 1 à 48).
Surveillance du tunnel	Cochez la case **Tunnel Monitoring (Surveillance du tunnel)** pour permettre aux satellites de surveiller les connexions de tunnel de passerelle, leur permettant ainsi de basculer vers une passerelle de secours en cas d'échec de connexion. • **Destination Address (Adresse de destination)** – Indiquez une adresse **IPv4** ou **IPv6** que la surveillance du tunnel utilisera pour déterminer si la connexion à la passerelle a été établie (par exemple, une adresse IP sur le réseau protégé par la passerelle). Si vous avez configuré une adresse IP pour l'interface de tunnel, vous pouvez également ne pas renseigner ce champ. La surveillance des tunnels utilisera alors l'interface de tunnel pour déterminer si la connexion est active. • **Tunnel Monitor Profile (Profil de surveillance du tunnel)** – Le **Failover (Basculement)** vers une autre passerelle est le seul type de surveillance du tunnel pris en charge avec le LSVPN. *Activez la **Tunnel Monitoring (Surveillance des tunnels)** et configurez un profil de surveillance des tunnels pour contrôler l'action de basculement si vous activez la configuration des tunnels des satellites.*
Profils crypto	Sélectionnez un **IPSec Crypto Profile (Profil crypto IPSec)** ou en créer un nouveau. Un chiffrement détermine les protocoles et algorithmes

Paramètres de configuration satellite GlobalProtect	Description
	d'identification, d'authentification et de cryptage des tunnels VPN. Les deux extrémités du tunnel d'un LSVPN étant des pare-feu approuvés au sein de votre entreprise, vous utilisez généralement le profil par défaut qui utilise le protocole ESP, DH groupe 2, le cryptage AES 128 CVC et l'authentification SHA-1. Voir Réseau > Profils réseau > Crypto IPSec GlobalProtect pour plus de détails.
Onglet Paramètres du réseau	
Source de l'héritage	Sélectionnez une source pour la propagation du serveur DNS et d'autres paramètres entre le client DHCP ou l'interface client PPPoE sélectionné et la configuration du satellite GlobalProtect. Grâce à ce paramètre, l'ensemble de la configuration, les serveurs DNS par exemple, est héritée de la configuration de l'interface sélectionnée dans Source de l'héritage.
DNS principal DNS secondaire	Saisissez les adresses IP des serveurs principal et secondaire qui fournissent le service DNS aux satellites.
Suffixe DNS	Cliquez sur **Add (Ajouter)** pour saisir un suffixe que le satellite doit utiliser localement lorsqu'un nom d'hôte non qualifié qu'il ne peut pas résoudre est saisi. Vous pouvez saisir plusieurs suffixes en les séparant par des virgules.
Hériter du suffixe DNS	Sélectionnez cette option pour envoyer le suffixe DNS aux satellites à utiliser localement lorsqu'un nom d'hôte non qualifié qu'ils ne peuvent pas résoudre est saisi.
Pool d'adresses IP	**Add (Ajouter)** une plage d'adresses IP à attribuer à l'interface de tunnel sur les satellites lors de l'établissement du tunnel VPN. Vous pouvez spécifier les adresses IPv6 ou IPv4. *le pool d'adresses IP doit être suffisamment important pour prendre en charge toutes les connexions simultanées. L'attribution d'adresse IP est dynamique et ne s'applique plus une fois le satellite déconnecté. La configuration de plusieurs plages à partir de différents sous-réseaux permet au système de fournir aux satellites une adresse IP non conflictuelle avec les autres interfaces des satellites.* Les serveurs et les routeurs des réseaux doivent acheminer le trafic de ce pool d'adresses IP vers le pare-feu. Par exemple, pour le réseau 192.168.0.0/16, un satellite peut se voir attribuer l'adresse 192.168.0.10. Si vous utilisez un routage dynamique, assurez-vous que le pool d'adresses IP que vous désignez pour les satellites ne chevauche pas les adresses IP

Paramètres de configuration satellite GlobalProtect	Description
	que vous avez attribuées manuellement aux interfaces de tunnel sur vos passerelles et satellites.
Accéder à l'itinéraire	Cliquez sur **Add (Ajouter)**, puis saisissez les itinéraires comme suit : • Si vous souhaitez acheminer l'ensemble du trafic provenant des satellites via le tunnel, ne renseignez pas ce champ. • Pour n'acheminer qu'un trafic donné via la passerelle (split tunneling), spécifiez les sous-réseaux de destination qui doivent être tunnellisés. Dans ce cas, le satellite acheminera le trafic non destiné à un itinéraire d'accès spécifié selon sa propre table de routage. Par exemple, vous pouvez choisir de ne tunnelliser que le trafic destiné à votre réseau d'entreprise et d'utiliser le satellite local pour autoriser l'accès à Internet en toute sécurité. • Si vous souhaitez autoriser le routage entre des satellites, saisissez l'itinéraire récapitulatif du réseau protégé par chaque satellite.
Onglet Filtre itinéraire	
Accepter les itinéraires publiés	Activez l'option **Accept published routes (Accepter les itinéraires publiés)** pour accepter les itinéraires conseillés par le satellite dans la table de routage de la passerelle. Si vous ne sélectionnez pas cette option, la passerelle n'acceptera aucun itinéraire publié par les satellites.
Sous-réseaux autorisés	Si vous souhaitez limiter davantage les itinéraires acceptés, **Add (Ajouter)** Sous-réseaux autorisés et définissez les sous-réseaux pour lesquels la passerelle doit accepter les itinéraires ; les sous-réseaux publiés par les satellites qui ne font pas partie de la liste sont alors filtrés. Par exemple, si tous les satellites sont configurés avec le sous-réseau 192.168.x.0/24 côté LAN, vous pouvez configurer un itinéraire autorisé de 192.168.0.0/16 sur la passerelle. Cette configuration fera en sorte que la passerelle n'accepte que les itinéraires du satellite uniquement s'ils se trouvent sur le sous-réseau 192.168.0.0/16.

Réseau > GlobalProtect > Gestionnaire de périphériques mobiles

Si vous utilisez un gestionnaire de sécurité mobile pour gérer les points de terminaison mobiles des utilisateurs finaux et que vous avez activé l'option de mise en œuvre des politiques HIP, vous devez configurer la passerelle pour communiquer avec le gestionnaire de sécurité mobile et récupérer les rapports HIP pour les points de terminaison gérés.

Il est nécessaire d'**Ajouter** des informations MDM pour le Gestionnaire de sécurité mobile pour permettre à la passerelle de communiquer avec le Gestionnaire de sécurité mobile.

Paramètres du gestionnaire de périphériques mobiles de GlobalProtect	**Description**
Name (Nom)	Donnez un nom au gestionnaire de sécurité mobile (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
	Si le pare-feu est en mode Plusieurs systèmes virtuels, les paramètres MDM affichent le système virtuel (vsys) sur lequel le gestionnaire de sécurité mobile est disponible. Pour un pare-feu non en mode Plusieurs systèmes virtuels, cette option n'apparaît pas dans la boîte de dialogue MDM. Après avoir enregistré le gestionnaire de sécurité mobile, vous ne pouvez plus changer son emplacement.
Paramètres de connexion	
Serveur	Saisissez l'adresse IP ou le nom de domaine complet de l'interface sur le gestionnaire de sécurité mobile où la passerelle se connecte pour récupérer les rapports HIP. Assurez-vous de disposer d'un itinéraire de service sur cette interface.
Port de connexion	Le port de connexion est l'endroit où le gestionnaire de sécurité mobile écoute les demandes de rapports de HIP. Par défaut, le port d'écoute du gestionnaire de sécurité mobile de GlobalProtect est 5008. Si vous utilisez un gestionnaire de sécurité mobile tiers, saisissez le numéro de port d'écoute du serveur pour les demandes de rapports HIP.
Certificat du client	Choisissez le certificat client de la passerelle à présenter au gestionnaire de sécurité mobile, lors de l'établissement d'une connexion HTTPS. Ce certificat est requis uniquement si le gestionnaire de sécurité mobile est configuré pour utiliser l'authentification mutuelle.

Paramètres du gestionnaire de périphériques mobiles de GlobalProtect	Description
CA racine approuvée	Cliquez sur **Add (Ajouter)** et sélectionnez le certificat AC de la racine utilisé pour générer le certificat pour l'interface sur laquelle la passerelle se connectera pour récupérer les rapports HIP. (Ce certificat de serveur peut être différent du certificat délivré pour l'interface d'enregistrement du point de terminaison sur le gestionnaire de sécurité mobile). Vous devez importer le certificat AC racine et l'ajouter à cette liste.

Réseau > GlobalProtect > Applications sans client

Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Clientless Apps (Applications sans client)** pour ajouter des applications accessibles au moyen du VPN sans le client GlobalProtect. Vous pouvez ajouter des applications sans client individuelles, puis sélectionner **Network (Réseau)** > **GlobalProtect** > **Clientless App Groups (Groupes d'applications sans client)** pour définir les groupes d'applications.

VPN sans client GlobalProtect fournit un accès à distance sécurisé aux applications Web d'entreprise courantes qui utilisent les technologies HTML, HTML5 et JavaScript. Les utilisateurs ont l'avantage d'un accès sécurisé à partir de navigateurs Web sur lesquels SSL est activé sans installer le logiciel GlobalProtect. Ceci est utile lorsque vous devez activer l'accès partenaire ou fournisseur aux applications et activer de manière sécurisée les actifs non gérés, y compris les périphériques personnels.

Vous avez besoin des mises à jour dynamiques de **GlobalProtect Clientless VPN (VPN sans client GlobalProtect)** pour utiliser cette fonctionnalité. Cette fonctionnalité requiert également l'installation d'un abonnement GlobalProtect sur le pare-feu qui héberge le VPN sans client du portail GlobalProtect.

Paramètres des applications sans client	Description
Name (Nom)	Saisissez un nom qui décrit l'application (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Location (Emplacement)	Pour un pare-feu en mode Plusieurs systèmes virtuels, **Location (Emplacement)** correspond au système virtuel (vsys) sur lequel la passerelle GlobalProtect est disponible. Pour un pare-feu non en mode Plusieurs systèmes virtuels, le champ **Location (Emplacement)** n'apparaît pas dans la boîte de dialogue Passerelle GlobalProtect. Après avoir enregistré la configuration de la passerelle, vous ne pouvez plus changer son **Location (Emplacement)**.
URL d'accueil de l'application	Saisissez l'URL à laquelle se trouve l'application (jusqu'à 4 095 caractères).
Description de l'application	(Optionnel) Saisissez une description pour l'application (255 caractères maximum). Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Icône de l'application	(Facultatif) Téléchargez une icône pour identifier l'application sur la page d'application publiée. Vous pouvez parcourir pour télécharger l'icône.

Réseau > GlobalProtect > Groupes d’applications sans client

Sélectionnez **Network (Réseau)** > **GlobalProtect** > **Clientless App Groups (Groupes d’applications sans client)** pour regrouper des applications accessibles au moyen du VPN sans client GlobalProtect. Vous pouvez ajouter des applications sans client existantes à un groupe ou configurer de nouvelles applications sans client pour le groupe. Les groupes sont utiles pour travailler avec plusieurs applications simultanément. Par exemple, vous pouvez avoir un ensemble standard d’applications SaaS (comme Workday, JIRA ou Bugzilla) que vous souhaitez configurer pour l’accès VPN sans client.

Paramètres des groupes d’applications sans clients	Description
Name (Nom)	Saisissez un nom qui décrit le groupe d’applications (31 caractères maximum). Le nom est sensible à la casse, doit être unique et peut inclure uniquement des lettres, chiffres, espaces, traits d’union et traits de soulignement.
Location (Emplacement)	Pour un pare-feu en mode Plusieurs systèmes virtuels, **Location (Emplacement)** correspond au système virtuel (vsys) sur lequel la passerelle GlobalProtect est disponible. Pour un pare-feu non en mode Plusieurs systèmes virtuels, le champ **Location (Emplacement)** n'apparaît pas dans la boîte de dialogue Passerelle GlobalProtect. Après avoir enregistré la configuration de la passerelle, vous ne pouvez plus changer son **Location (Emplacement)**.
Applications	Vous devez **Ajouter** une **Application** à partir du menu déroulant ou configurer une nouvelle application sans client et l’ajouter au groupe. Pour configurer une nouvelle application sans client, reportez-vous à Réseau > GlobalProtect > Clientless Applications .

Objets > GlobalProtect > Objets HIP

Sélectionnez **Objects (Objets)** > **GlobalProtect** > **HIP Objects (Objets HIP)** pour définir des objets pour un profil d'information sur l'hôte (HIP). Les objets HIP fournissent les critères de correspondance pour filtrer les données brutes rapportées par une application que vous souhaitez utiliser pour appliquer la politique. Par exemple, si les données brutes de l'hôte comprennent des informations sur plusieurs packages antivirus sur une terminaison, vous pourriez être intéressé par une application particulière parce que votre organisation l'exige. Pour ce scénario, vous créez un objet HIP pour correspondre à l'application spécifique que vous souhaitez appliquer.

Pour définir les objets HIP dont vous avez besoin, vous devez déterminer comment vous allez utiliser les informations sur l'hôte collectées pour mettre en œuvre la politique. N'oubliez pas que les objets HIP forment simplement des blocs qui vous permettent de créer les profils HIP utilisés dans les politiques de sécurité que vous pouvez utiliser. Par conséquent, vous voudrez peut-être garder vos objets simples, en fonction d'une chose, comme la présence d'un type particulier de logiciel requis, l'appartenance à un domaine spécifique ou la présence d'un OS de terminaison spécifique. Avez cette approche, vous pouvez créer une politique HIP très granulaire.

Pour créer un objet HIP, cliquez sur **Add (Ajouter)** ; la boîte de dialogue Objet HIP s'affiche alors. Pour obtenir une description de chaque champ, reportez-vous aux tableaux suivants.

- Onglet Général des objets HIP
- Onglet Périphérique mobile des objets HIP
- Onglet Gestion des correctifs des objets HIP
- Onglet Pare-feu des objets HIP
- Onglet Anti-logiciels malveillants des objets HIP
- Onglet Sauvegarde du disque des objets HIP
- Onglet Cryptage du disque des objets HIP
- Onglet Prévention des pertes de données des objets HIP
- Onglet HIP Objects Certificate (Certificat d'objets HIP)
- Onglet Vérifications personnalisées des objets HIP

Pour plus d'informations sur la création de politiques de sécurité HIP, reportez-vous à la section Configuration de la mise en œuvre d'une politique HIP du *Guide de l'administrateur de GlobalProtect*.

Onglet Général des objets HIP

- **Objets** > **GlobalProtect** > **Objets HIP** > ***<hip-object>*** > **Général**

Sélectionnez l'onglet **General (Général)** pour donner un nom au nouvel objet HIP et configurer l'objet pour correspondre aux informations générales sur l'hôte, telles que le domaine, le système d'exploitation ou le type de connectivité réseau de l'hôte.

Paramètres généraux d’un objet HIP	Description
Name (Nom)	Donnez un nom à l’objet HIP (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement.
Partagé	Si vous sélectionnez **Shared (Partagé)**, les objets HIP actuels deviennent disponibles à : Chaque système virtuel (vsys) sur le pare-feu, si vous êtes connecté à un pare-feu en mode Plusieurs systèmes virtuels. Si vous décochez cette sélection, l'objet sera disponible uniquement sur le système virtuel sélectionné **Virtual System (Système virtuel)**, dans la liste déroulante de l'onglet **Objects (Objets)**. Pour un pare-feu non en mode Plusieurs systèmes virtuels, cette option n'est pas disponible dans la boîte de dialogue Objet HIP. Tous les groupes de périphériques sur Panorama™. Si vous décochez cette sélection, l'objet sera disponible uniquement sur le groupe de périphériques sélectionné dans **Device Group (Groupe de périphériques)**, dans la liste déroulante de l'onglet **Objects (Objets)**. Après avoir enregistré l'objet, vous ne pouvez plus changer son paramètre **Shared (Partagé)**. Sélectionnez **Objects (Objets)** > **GlobalProtect** > **HIP Objects (Objets HIP)** pour connaître le **Location (Emplacement)** actuel.
Description	(Facultatif) Saisissez une description.
Infos sur l'hôte	Sélectionnez cette option pour activer les options pour configurer les informations d'hôte.
Géré	Filtrez selon que le point de terminaison est géré ou non géré. Pour la mise en correspondance avec les points de terminaison gérés, sélectionnez **Yes (Oui)**. Pour la mise en correspondance avec les points de terminaison non gérés, sélectionnez **No (Non)**.
Désactiver le contrôle prioritaire (Panorama uniquement)	Contrôle l'accès forcé à l'objet HIP dans des groupes de périphériques descendants du **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**. Sélectionnez cette option pour empêcher les administrateurs de créer des copies locales de l'objet dans les groupes de périphériques descendants en appliquant un contrôle prioritaire sur ses valeurs héritées. Cette option est désactivée par défaut (le contrôle prioritaire est activé).
Domain (Domaine)	Pour la mise en correspondance avec un nom de domaine, choisissez un opérateur dans la liste déroulante et saisissez une chaîne à mettre en correspondance.
Système d’exploitation	Pour la mise en correspondance avec un système d'exploitation hôte, choisissez **Contains (Contient)** dans la première liste déroulante, sélectionnez

Paramètres généraux d'un objet HIP	Description
	un fournisseur dans la seconde, puis une version de système d'exploitation dans la troisième, ou vous pouvez sélectionner **All (Tout)** pour la mise en correspondance avec n'importe quelle version du fournisseur sélectionné.
Version du client	Pour la mise en correspondance avec un numéro de version spécifique, sélectionnez un opérateur dans la liste déroulante, puis saisissez une chaîne à mettre en correspondance ou non dans la zone de texte.
Nom de l'hôte	Pour la mise en correspondance avec nom d'hôte spécifique, sélectionnez un opérateur dans la liste déroulante, puis saisissez une chaîne de à mettre en correspondance ou non, selon l'opérateur sélectionné) dans la zone de texte.
ID d'hôte	L'ID hôte est un ID unique que GlobalProtect affecte afin d'identifier l'hôte. La valeur d'ID hôte varie selon le type de périphérique : • **Windows** – GUID machine stocké dans le registre Windows (HKEY_Local_Machine\Software\Microsoft\Cryptography\MachineGuid) • **macOS** – Adresse MAC de la première interface de réseau physique intégrée • **Android** – ID Android • **iOS** – UDID • **Linux** – Product UUID extrait du tableau du système DMI • **Chrome** – La chaîne alphanumérique unique d'une longueur de 32 caractères affectée par GlobalProtect. Pour la mise en correspondance avec un nom d'hôte spécifique, sélectionnez l'opérateur dans la liste déroulante, puis saisissez une chaîne à mettre en correspondance (ou non, selon l'opérateur sélectionné) dans la zone de texte.
Numéro de série	Pour la mise en correspondance avec la totalité ou une partie du numéro de série d'un périphérique, choisissez un opérateur dans la liste déroulante et saisissez une chaîne à mettre en correspondance.
Réseau	Ce champ vous permet de filtrer une configuration réseau de périphérique mobile spécifique. Ce critère de correspondance s'applique uniquement aux périphériques mobiles. Sélectionnez un opérateur dans la première liste déroulante, puis le type de connexion réseau à filtrer dans la seconde : **Wi-Fi**, **Mobile**, **Ethernet** (disponible uniquement pour les filtres **Is Not (N'est pas)**) ou **Unknown (Inconnu)**. Une fois le type de réseau sélectionné, saisissez toute chaîne supplémentaire à mettre en correspondance, le cas échéant, notamment l'**Carrier (Opérateur)** mobile ou le **SSID** Wi-Fi.

Onglet Périphérique mobile des objets HIP

- **Objets** > **GlobalProtect** > **Objets HIP** > **<*hip-object*>** > **Périphérique mobile**

Sélectionnez l'onglet **Mobile Devise (Périphérique mobile)** pour activer la correspondance HIP en fonction des données collectées à partir des périphériques mobiles exécutant l'application GlobalProtect.

Pour recueillir les attributs des périphériques mobiles et les utiliser dans les politiques de mise en œuvre HIP, GlobalProtect a besoin d'un serveur MDM. À l'heure actuelle, GlobalProtect prend en charge l'intégration HIP via le serveur MDM AirWatch.

Paramètres de périphérique mobile d'un objet HIP	Description
Périphérique mobile	Sélectionnez cette option pour activer le filtrage sur les données d'accueil collectées à partir d'appareils mobiles qui exécutent l'application GlobalProtect et pour activer les onglets Périphérique, Paramètres et Applications.
onglet Périphérique	• **Model (Modèle)** : pour la mise en correspondance avec un modèle de périphérique spécifique, choisissez un opérateur dans la liste déroulante et saisissez une chaîne à mettre en correspondance. • **Tag (Étiquette)** : pour la mise en correspondance avec une valeur d'étiquette définie sur le gestionnaire de sécurité mobile de GlobalProtect, choisissez un opérateur dans la première liste déroulante, puis une étiquette dans la seconde. • **Phone Number (Numéro de téléphone)** : pour la mise en correspondance avec tout ou partie d'un numéro de téléphone de périphérique, choisissez un opérateur dans la liste déroulante et saisissez une chaîne à mettre en correspondance. • **IMEI** : pour la mise en correspondance avec tout ou partie d'un numéro IMEI (International Mobile Equipment Identity) de périphérique, choisissez un opérateur dans la liste déroulante et saisissez une chaîne à mettre en correspondance.
Onglet Paramètres	• **Code secret** : filtre basé sur la définition ou non d'un code secret pour le périphérique. Pour la mise en correspondance avec les périphériques pour lesquels un code secret a été défini, sélectionnez **Yes (Oui)**. Pour la mise en correspondance avec les périphériques pour lesquels aucun code secret n'a été défini, sélectionnez Non. • **Rooted/Jailbroken (Déverrouillé/Débridé)** : filtre basé sur le déverrouillage/débridage ou non du périphérique. Pour la mise en correspondance avec les périphériques déverrouillés ou débridés, sélectionnez **Yes (Oui)**. Pour la mise en correspondance avec les périphériques non déverrouillés/débridés, sélectionnez **No (Non)**. • **Disk Encryption (chiffrement du disque)** : filtre basé sur le chiffrement ou non des données du périphérique. Pour la mise en

Paramètres de périphérique mobile d'un objet HIP	Description
	correspondance avec les périphériques pour lesquels le chiffrement du disque est activé, sélectionnez Oui. Pour la mise en correspondance avec les périphériques pour lesquels le chiffrement du disque est désactivé, sélectionnez Non. • **Time Since Last Check-in (Temps écoulé depuis le dernier enregistrement)** : filtre basé sur le dernier enregistrement du périphérique auprès du gestionnaire de périphériques mobiles. Sélectionnez un opérateur dans la liste déroulante, puis définissez le nombre de jours depuis le dernier enregistrement. Par exemple, vous pouvez définir un objet correspondant aux périphériques qui n'ont pas été enregistrés au cours des 5 derniers jours.
Onglet Applications	• **Apps (Applications)** : (Périphériques Android uniquement) : Sélectionnez cette option pour activer le filtrage en fonction des applications installées sur le périphérique et de la présence ou non d'applications infectées par des logiciels malveillants. • Onglet **Criteria (Critères)** • **Has Malware (Présente des logiciels malveillants)** – Sélectionnez **Yes (Oui)** pour relier les périphériques qui comportent des applications où des logiciels malveillants sont installés. Sélectionnez **No (Non)** pour relier les périphériques qui ne comportent pas d'applications où des logiciels malveillants sont installés. Sélectionnez **None (Aucun)** pour ne pas utiliser **Has Malware (Présente des logiciels malveillants)** en tant que critère de correspondance. • Onglet **Include (Inclure)** • **Package (Paquet)** – Pour relier les appareils qui ont des applications spécifiques installées, vous devez **Add (Ajouter)** une application et saisir le nom de l'application unique au format DNS inversé. Par exemple, com.netflix.mediaclient, puis saisissez ensuite le **Hash (Hachage)** correspondant à l'application, que l'application GlobalProtect calcule et soumet avec le rapport HIP de l'appareil.

Onglet Gestion des correctifs des objets HIP

- **Objets** > **GlobalProtect** > **Objets HIP** > **<*hip-object*>** > **Gestion des correctifs**

Sélectionnez l'onglet **Patch Management (Gestion des correctifs)** pour activer la correspondance HIP en fonction de l'état des correctifs des points de terminaison GlobalProtect.

Paramètres de gestion des correctifs d'un objet HIP	Description
Gestion des correctifs	Sélectionnez cette option pour activer la correspondance sur l'état de la gestion des correctifs de l'hôte et activer les onglets Critères et Fournisseur.
Onglet Critères	Définissez les paramètres suivants : • **Is Installed (Est installé)** : mise en correspondance en fonction de l'installation ou non du logiciel de gestion des correctifs sur l'hôte. • **Is Enabled (Est activé)** : mise en correspondance en fonction de l'activation ou non du logiciel de gestion des correctifs sur l'hôte. Si la sélection **Is Installed (Est installé)** est décochée, ce champ est automatiquement défini sur **none (aucun)** et ne peut pas être modifié. • **Severity (Gravité)** : sélectionnez à partir de la liste des opérateurs logiques pour faire correspondre si l'hôte a des correctifs manquants du niveau de gravité spécifié. Servez-vous des mappages suivants entre les valeurs de gravité GlobalProtect et les cotes de gravité d'OPSWAT pour comprendre la signification de chacune des valeurs : • **0** : Faible • **1** : Modérée • **2** : Importante • **3** : Critique • **Check (Vérification)** : mise en correspondance en fonction de l'absence ou non de correctifs sur l'hôte. • **Patches (Correctifs)** : mise en correspondance en fonction de la présence ou non de correctifs spécifiques sur l'hôte. Cliquez sur **Add (Ajouter)** et saisissez les ID d'article Kerberos pour les correctifs donnés à rechercher. Par exemple, saisissez **`3128031`** pour rechercher la mise à jour de Microsoft Office 2010 (KB3128031), édition 32 bits.
Onglet du fournisseur	Définir des fournisseurs spécifiques de logiciels et de produits de gestion de correctifs pour rechercher sur le terminal pour trouver une correspondance. Cliquez sur **Add (Ajouter)** et choisissez un **Vendor (Fournisseur)** dans la liste déroulante. Vous pouvez également cliquer sur Ajouter pour choisir un **Product (Produit)** spécifique. Cliquez sur **OK** pour enregistrer les paramètres.

Onglet Pare-feu des objets HIP

- **Objets** > **GlobalProtect** > **Objets HIP** > **<*hip-object*>** > **Pare-feu**

Sélectionnez **Firewall (Pare-feu)** pour activer la correspondance HIP en fonction de l'état du logiciel de pare-feu des points de terminaison GlobalProtect.

Paramètres de pare-feu d'un objet HIP

Sélectionnez **Firewall (Pare-feu)** pour activer la correspondance en fonction du logiciel de pare-feu de l'hôte :

- **Is Installed (Est installé)** : mise en correspondance en fonction de l'installation ou non du logiciel de pare-feu sur l'hôte.
- **Is Enabled (Est activé)** : mise en correspondance en fonction de l'activation ou non du logiciel de pare-feu sur l'hôte. Si la sélection **Is Installed (Est installé)** est décochée, ce champ est automatiquement défini sur **none (aucun)** et ne peut pas être modifié.
- **Vendor and Product (Fournisseur et produit)** : définissez des produits et/ou des fournisseurs de logiciels pare-feu spécifiques à rechercher sur l'hôte pour déterminer une correspondance. Cliquez sur **Add (Ajouter)** et choisissez un **Vendor (Fournisseur)** dans la liste déroulante. Vous pouvez également cliquer sur **Add (Ajouter)** pour choisir un **Product (Produit)**. Cliquez sur **OK** pour enregistrer les paramètres.
- **Exclude Vendor (Exclure le fournisseur)** : sélectionnez cette option pour la mise en correspondance avec les hôtes qui ne disposent d'aucun logiciel du fournisseur donné.

Onglet Anti-logiciels malveillants des objets HIP

- **Objets** > **GlobalProtect** > **Objets HIP** > **<*hip-object*>** > **Anti-logiciels malveillants**

Sélectionnez l'onglet **Anti-Malware (Anti-logiciels malveillants)** vous permet d'activer la correspondance HIP en fonction de la couverture antivirus ou antispyware des points de terminaison GlobalProtect.

Paramètres anti-logiciels malveillants d'un objet HIP

Sélectionnez **Anti-Malware (Anti-logiciels malveillants)** pour activer la correspondance en fonction de la couverture antispyware ou antivirus de l'hôte. Définissez les critères de correspondance supplémentaire comme suit :

- **Is Installed (Est installé)** : mise en correspondance en fonction de l'installation ou non du logiciel antispyware ou antivirus sur l'hôte.
- **Real Time Protection (Est activé)** : mise en correspondance en fonction de l'activation ou non de la protection antispyware ou antivirus en temps réel sur l'hôte. Si la sélection **Is Installed (Est installé)** est décochée, ce champ est automatiquement défini sur **None (Aucun)** et ne peut pas être modifié.
- **Virus Definition Version (Version des définitions de virus)** : met en correspondance en fonction de la mise à jour ou non des définitions de virus dans un nombre de jours spécifié ou une version spécifique.
- **Product Version (Version du produit)** : mise en correspondance avec une version spécifique du logiciel antivirus ou anti-spyware. Pour indiquer une version, sélectionnez un opérateur dans la liste déroulante, puis saisissez une chaîne représentant la version du produit.

Paramètres anti-logiciels malveillants d’un objet HIP
• **Last Scan Time (Temps écoulé depuis la dernière analyse)** : mise en correspondance en fonction de la dernière analyse antispyware ou antivirus. Sélectionnez un opérateur dans la liste déroulante, puis spécifiez le nombre de **Days (Jours)** ou **Hours (Heures)** pour la mise en correspondance. • **Vendor and Product (Fournisseur et produit)** : définissez des produits et/ou des fournisseurs de logiciels antispyware ou antivirus spécifiques à rechercher sur l'hôte pour déterminer une correspondance. Cliquez sur **Add (Ajouter)** et choisissez un **Vendor (Fournisseur)** dans la liste déroulante. Vous pouvez également cliquer sur **Add (Ajouter)** pour choisir un **Product (Produit)**. Cliquez sur **OK** pour enregistrer les paramètres. • **Exclude Vendor (Exclure le fournisseur)** : sélectionnez cette option pour la mise en correspondance avec les hôtes qui ne disposent d'aucun logiciel du fournisseur donné.

Onglet Sauvegarde du disque des objets HIP

- **Objets** > **GlobalProtect** > **Objets HIP** > **<*hip-object*>** > **Sauvegarde du disque**

Sélectionnez l'onglet **Disk Backup (Sauvegarde du disque)** pour activer la correspondance HIP en fonction de l'état de sauvegarde du disque des points de terminaison GlobalProtect.

Paramètres de sauvegarde du disque d’un objet HIP
Sélectionnez **Disk Backup (Sauvegarde de disque)** pour activer la correspondance en fonction de l'état de sauvegarde du disque sur l'hôte, puis définissez les critères de correspondance supplémentaires comme suit : • **Is Installed (Est installé)** : mise en correspondance en fonction de l'installation ou non de sauvegarde du disque sur l'hôte. • **Last Backup Time (Temps écoulé depuis la dernière sauvegarde)** : mise en correspondance en fonction de la dernière sauvegarde du disque. Sélectionnez un opérateur dans la liste déroulante, puis spécifiez le nombre de **Days (Jours)** ou **Hours (Heures)** pour la mise en correspondance. • **Vendor and Product (Fournisseur et produit)** : définissez les fournisseurs et les produits de logiciels de sauvegarde de disque spécifiques à rechercher sur l'hôte. Cliquez sur **Add (Ajouter)** et choisissez un **Vendor (Fournisseur)** dans la liste déroulante. Vous pouvez également cliquer sur **Add (Ajouter)** pour choisir un **Product (Produit)**. Cliquez sur **OK** pour enregistrer les paramètres. • **Exclude Vendor (Exclure le fournisseur)** : sélectionnez cette option pour la mise en correspondance avec les hôtes qui ne disposent d'aucun logiciel du fournisseur donné.

Onglet Cryptage du disque des objets HIP

- **Objets** > **GlobalProtect** > **Objets HIP** > **<*hip-object*>** > **Cryptage du disque**

Sélectionnez l'onglet **Disk Encryption (Chiffrement du disque)** pour activer la correspondance HIP en fonction de l'état de chiffrement du disque des points de terminaison GlobalProtect.

Paramètres de chiffrement du disque d'un objet HIP	Description
Chiffrement du disque	Sélectionnez **Disk Encryption (chiffrement du disque)** pour activer la correspondance en fonction de l'état de chiffrement du disque sur l'hôte.
Critères	Définissez les paramètres suivants : • **Is Installed (Est installé)** : mise en correspondance en fonction de l'installation ou non du logiciel de chiffrement du disque sur l'hôte. • **Encrypted Locations (Emplacements cryptés)** : cliquez sur **Add (Ajouter)** pour spécifier le lecteur ou le chemin d'accès où rechercher le chiffrement du disque, lors de la détermination d'une correspondance : • **Encrypted Locations (Emplacements cryptés)** : saisissez des emplacements spécifiques sur lesquels rechercher le chiffrement sur l'hôte. • **State (État)** : spécifiez la correspondance en fonction de l'état de l'emplacement crypté en choisissant un opérateur dans la liste déroulante, puis en sélectionnant un état possible (**full (total)**, **none (aucun)**, **partial (partiel)**, **not-available (non disponible)**). Cliquez sur **OK** pour enregistrer les paramètres.
Constructeur	Définir les fournisseurs et les produits logiciels de chiffrement de disque spécifiques pour correspondre au terminal. Cliquez sur **Add (Ajouter)** et choisissez un **Vendor (Fournisseur)** dans la liste déroulante. Vous pouvez également cliquer sur **Add (Ajouter)** pour choisir un **Product (Produit)**. Cliquez sur **OK** pour sauvegarder les paramètres et revenir à l'onglet **Disk Encryption (chiffrement du disque)**.

Onglet Prévention des pertes de données des objets HIP

- **Objets** > **GlobalProtect** > **Objets HIP** > **<*hip-object*>** > **Prévention des pertes de données**

Sélectionnez l'onglet **Data Loss Prevention (Prévention des pertes de données)** pour configurer la correspondance HIP qui est basée sur si les points de terminaison GlobalProtect exécutent un logiciel de prévention des pertes de données.

Paramètres de prévention des pertes de données d'un objet HIP
Sélectionnez **Prévention des pertes de données** pour activer la correspondance en fonction de l'état de prévention des pertes de données (DLP) sur l'hôte (hôtes Windows uniquement), puis définissez les critères de correspondance supplémentaires comme suit : • **Is Installed (Est installé)** – Mise en correspondance en fonction de l'installation ou non du logiciel DLP sur l'hôte.

Paramètres de prévention des pertes de données d’un objet HIP
• **Is Enabled (Est activé)** – Mise en correspondance en fonction de l’activation ou non du logiciel DLP sur l’hôte. Si la sélection **Is Installed (Est installé)** est décochée, ce champ est automatiquement défini sur **none (aucun)** et ne peut pas être modifié. • **Vendor and Product (Fournisseur et produit)** – Définissez des produits et/ou des fournisseurs de logiciels DLP spécifiques à rechercher sur l'hôte pour déterminer une correspondance. Cliquez sur **Add (Ajouter)** et choisissez un **Vendor (Fournisseur)** dans la liste déroulante. Vous pouvez également cliquer sur **Add (Ajouter)** pour choisir un **Product (Produit)**. Cliquez sur **OK** pour enregistrer les paramètres. • **Exclude Vendor (Exclure le fournisseur)** : sélectionnez cette option pour la mise en correspondance avec les hôtes qui ne disposent d'aucun logiciel du fournisseur donné.

Onglet HIP Objects Certificate (Certificat d’objets HIP)

- **Objets** > **GlobalProtect** > **Objets HIP** > **<*hip-object*>** > **certificate**

Sélectionnez l’onglet **Certificate (Certificat)** pour permettre la correspondance HIP en fonction du profil de certificat et des autres attributs du certificat.

Paramètres du certificat d’objets HIP
Sélectionnez **Validate Certificate (Valider le certificat)** pour permettre la correspondance en fonction des profils de certificat et des attributs du certificat. Puis définissez les critères de correspondance, comme suit : • **Certificate Profile (Profil du certificat)** : Sélectionnez le profil de certificat que la passerelle GlobalProtect utilisera pour valider le certificat de machine envoyé dans le rapport HIP. • **Certificate Field (Champ du certificat)** : Sélectionnez un attribut de certificat utilisé pour la correspondance avec le certificat de machine. • **Value (Valeur)** : Définissez la valeur de l’attribut.

Onglet Vérifications personnalisées des objets HIP

- **Objets** > **GlobalProtect** > **Objets HIP** > **<*hip-object*>** > **Vérifications personnalisées**

Sélectionnez l'onglet **Custom Checks (Vérifications personnalisées)** pour activer la correspondance HIP en fonction des vérifications personnalisées que vous avez définies sur le portail GlobalProtect. Pour plus d'informations sur l'ajout de vérifications personnalisées à la collecte de données HIP, reportez-vous à la section Réseau > GlobalProtect > Portails.

Paramètres des vérifications personnalisées d’un objet HIP	Description
Vérifications personnalisées	Sélectionnez **Custom Checks (Vérifications personnalisées)** pour permettre la correspondance sur les contrôles personnalisés que vous avez définis sur le portail GlobalProtect.
Liste des processus	Pour rechercher un processus spécifique sur le système hôte, cliquez sur **Add (Ajouter)** et saisissez le nom du processus. Par défaut, l'application recherche les processus en cours d'exécution ; si vous souhaitez vérifier si un processus spécifique n'est pas en cours d'exécution, décochez **Running (En cours d'exécution)**. Les processus peuvent être des processus au niveau système d’exploitation ou des processus de l’application utilisateur.
Clé de registre	Pour rechercher une clé de registre spécifique sur les hôtes Windows, cliquez sur **Add (Ajouter)** et saisissez la **Registry Key (Clé de registre)** pour la mise en correspondance. Pour faire correspondre uniquement les hôtes qui ne disposent pas de la clé de registre spécifiée ou de la valeur de la clé, cochez la case **Key does not exist or match the specified value data (La clé n’existe pas ou ne correspond pas aux données de la valeur définies)**. Pour la mise en correspondance avec des valeurs spécifiques, cliquez sur **Add (Ajouter)**, puis saisissez la **Registry Value (Valeur de registre)** et les **Value Data (Données de la valeur)**. Pour la mise en correspondance avec les hôtes qui ne disposent clairement pas de la valeur ou des données de la valeur spécifiées, sélectionnez **Negate (Inverser)**. Cliquez sur **OK** pour enregistrer les paramètres.
Plist	Pour rechercher une entrée spécifique dans la Property List (plist) sur les hôtes Mac, cliquez sur **Add (Ajouter)** et saisissez le nom du **Plist**. Pour la mise en correspondance uniquement avec les hôtes qui ne disposent pas du plist spécifié, sélectionnez **Plist does not exist (Le plist n'existe pas)**. Pour la mise en correspondance avec une valeur de clé spécifique dans la plist, cliquez sur **Add (Ajouter)**, puis saisissez la **Key (Clé)** et la **Value (Valeur)** correspondante pour la mise en correspondance. Pour la mise en correspondance avec les hôtes qui ne disposent clairement pas de la clé ou de la valeur spécifiée, cochez la case **Negate (Ignorer)** Cliquez sur **OK** pour enregistrer les paramètres.

Objets > GlobalProtect > Profils HIP

Sélectionnez **Objects (Objets)** > **GlobalProtect** > **HIP Profiles (Profils HIP)** pour créer les profils HIP (un ensemble d'objets HIP à évaluer conjointement pour la surveillance ou pour l'application de la politique de sécurité) que vous utilisez pour configurer les politiques de sécurité activées par HIP. Lors de la création de profils HIP, vous pouvez combiner des objets HIP précédemment créés (ainsi que d'autres profils HIP) à l'aide d'une logique booléenne, notamment lorsqu'un flux de trafic est évalué en fonction d'un profil HIP auquel il correspond ou non. En cas de correspondance, la règle de politique correspondante est mise en œuvre ; s'il n'y a pas de correspondance, le flux est évalué en fonction de la règle suivante (comme avec tout autre critère de correspondance de politique).

Pour créer un profil HIP, cliquez sur **Add (Ajouter)**. Le tableau suivant fournit des informations sur les champs à renseigner dans la boîte de dialogue Profil HIP. Pour plus d'informations sur le paramétrage de GlobalProtect et le flux de travail pour la création de politiques de sécurité HIP, reportez-vous à la section Configuration de la mise en œuvre d'une politique HIP du *Guide de l'administrateur de GlobalProtect*.

Paramètres de profil HIP	Description
Name (Nom)	Donnez un nom au profil HIP (**31** caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Description	(Facultatif) Saisissez une description.
Partagé	Sélectionnez **Shared (Partagé)** pour rendre le profil de HIP courant disponible à : • Chaque système virtuel (vsys) sur le pare-feu, si vous êtes connecté à un pare-feu en mode Plusieurs systèmes virtuels. Si vous désactivez cette sélection, le profil est disponible uniquement aux systèmes virtuels sélectionnés dans le menu déroulant **Virtual System (Système virtuel)** dans l'onglet **Objects (Objets)**. Pour un pare-feu non en mode Plusieurs systèmes virtuels, cette option n'apparaît pas dans la boîte de dialogue Profil HIP. • Tous les groupes de périphériques sur Panorama. Si vous décochez cette sélection, le profil sera disponible uniquement sur le groupe de périphériques sélectionné dans **Device Group (Groupe de périphériques)**, dans la liste déroulante de l'onglet **Objects (Objets)**. Après avoir enregistré le profil, vous ne pouvez plus changer son paramètre **Shared (Partagé)**. Sélectionnez **Objects (Objets)** > **GlobalProtect** > **HIP Profiles (Profils HIP)** pour afficher le **Location (Emplacement)** actuel.
Désactiver le contrôle prioritaire (Panorama uniquement)	Contrôle l'accès contrôle prioritaire au profil HIP dans des groupes de périphériques descendants du **Device Group (Groupe de périphériques)** sélectionné dans l'onglet **Objects (Objets)**. Sélectionnez cette option pour empêcher les administrateurs de créer des copies locales du profil dans les groupes de périphériques descendants en appliquant un contrôle prioritaire

Paramètres de profil HIP	Description
	sur les valeurs héritées. Cette option est désactivée par défaut (le contrôle prioritaire est activé).
Correspondance	Cliquez sur **Add Match Criteria (Ajouter un critère de correspondance)** pour HIP Objects/Profiles Builder (ouvrir le générateur de profils/d'objets HIP). Sélectionnez le premier profil ou objet HIP que vous souhaitez utiliser comme critère de correspondance, puis ajoutez-le () à la zone de texte **Match (Faire correspondre)** de la boîte de dialogue Générateur de profils/objets HIP. N'oubliez pas que, si vous souhaitez que le profil HIP évalue l'objet comme correspondance uniquement lorsque le critère de l'objet n'est pas vrai pour un flux, vous devez cocher **NOT (NE PAS)** avant d'ajouter l'objet. Continuez d'ajouter des critères de correspondance appropriés pour le profil que vous créez, en vous assurant de sélectionner l'opérateur booléen correspondant (**AND (ET)** ou **OR (OU)**) entre chaque ajout (et en sélectionner l'opérateur **NOT (NE PAS)**, le cas échéant). Pour créer une expression booléenne complexe, vous devez ajouter manuellement les parenthèses aux bons endroits dans la zone de texte **Match (Faire correspondre)** pour que le profil HIP soit évalué à l'aide de la logique booléenne souhaitée. Par exemple, l'expression suivante indique que le profil HIP correspond au trafic d'un hôte qui dispose du cryptage de disque FileVault (pour les systèmes d'exploitation Mac) ou TrueCrypt (pour les systèmes d'exploitation Windows), appartient au domaine requis et sur lequel un client antivirus Symantec est installé : `((« MacOS » et « FileVault ») ou (« Windows » et « TrueCrypt »)) et « Domaine » et « SymantecAV »` Lorsque vous avez terminé d'ajouter les objets et les profils au nouveau profil HIP, cliquez sur **OK**.

Périphérique > Client GlobalProtect

Les rubriques suivantes décrivent la configuration et la gestion de l’application GlobalProtect.

Que voulez-vous faire ?	Reportez-vous à la section :
Afficher plus d’informations sur les sorties de logiciels GlobalProtect.	Gestion de l’agent logiciel GlobalProtect
Installer le logiciel GlobalProtect.	Paramétrage de l’agent de GlobalProtect
Utiliser le logiciel GlobalProtect.	Utilisation de l'agent de GlobalProtect
Vous souhaitez en savoir plus ?	Pour obtenir des instructions détaillées étape par étape sur la configuration du logiciel GlobalProtect, reportez-vous à la section Déployer le logiciel des applications GlobalProtect du Guide de l’administrateur GlobalProtect.

Gestion du logiciel de l’application GlobalProtect

Sélectionnez **Device (Périphérique)** > **GlobalProtect Client (Client GlobalProtect)** (pare-feu uniquement) pour télécharger et activer le logiciel de l’application GlobalProtect sur le pare-feu qui héberge le portail. Par la suite, les terminaux qui se connectent au portail téléchargent le logiciel de l’application. Dans les configurations d'agent que vous spécifiez sur le portail, vous définissez comment et quand le portail pousse le logiciel aux terminaux. Votre configuration détermine si les mises à jour se font automatiquement lorsque l'application se connecte, que les utilisateurs finaux sont invités à mettre à jour ou si la mise à niveau est interdite pour tout ou un ensemble spécifique d'utilisateurs. Pour plus d’informations, reportez-vous à Permettre à l’utilisateur de mettre à niveau l’application GlobalProtect. Pour plus d’informations sur les options de distribution du logiciel de l’application GlobalProtect et pour obtenir des instructions détaillées sur le déploiement du logiciel, reportez-vous à la section Déploiement du logiciel de l’application GlobalProtect du Guide de l’administrateur de GlobalProtect.

Pour le téléchargement et l'installation initiaux de l'application GlobalProtect, l'utilisateur du point de terminaison doit être connecté avec des droits d'administrateur. Des droits d'administrateur ne sont pas nécessaires pour les mises à niveau ultérieures.

Paramètres du client GlobalProtect	Description
Version	Ce numéro de version du logiciel de l'application GlobalProtect est disponible sur le serveur de mises à jour Palo Alto Networks. Pour vérifier si une nouvelle version du logiciel de l'application est disponible auprès de Palo Alto Networks, cliquez sur **Check Now (Vérifier maintenant)**. Le pare-feu utilise son itinéraire de service pour se connecter au serveur de mises à jour pour déterminer si de nouvelles versions et les afficher en tête de liste.

Paramètres du client GlobalProtect	Description
Taille	Taille du module logiciel de l'application.
Date de version	Date et heure de disponibilité de la version auprès de Palo Alto Networks.
Téléchargé	Une coche dans cette colonne indique que la version correspondante du module logiciel de l'application a été téléchargée sur le pare-feu.
Actuellement activé	Une coche dans cette colonne indique que la version correspondante du module logiciel de l'application a été activée sur le pare-feu et peut être téléchargée par les applications qui s'y connectent. Une seule version du logiciel peut être activée à la fois.
Action (Action)	Indique l'action que vous pouvez entreprendre pour le module logiciel de l'application correspondant comme suit : • **Download (Télécharger)** : la version correspondante du logiciel de l'application est disponible sur le serveur de mises à jour Palo Alto Networks. Cliquez sur **Download (Télécharger)** pour lancer le téléchargement. Si le pare-feu ne dispose d'aucun accès à Internet, utilisez un ordinateur connecté à Internet pour vous rendre sur le site du Support aux clients, puis sélectionnez **Updates (Mises à jour)** > **Software Updates (Mises à jour logicielles)**pour chercher et **Download (Télécharger)** de nouvelles versions du logiciel de l'application sur votre ordinateur local. Ensuite, cliquez sur **Upload (Charger)** pour charger manuellement le logiciel de l'application au pare-feu. • **Activate (Activer)** : la version correspondante du logiciel de l'application a été téléchargée sur le pare-feu, mais les applications ne peuvent pas encore la télécharger. Cliquez sur **Activate (Activer)** pour activer le logiciel et permettre la mise à niveau de l'application. Pour activer une mise à jour logicielle chargée manuellement sur le pare-feu, cliquer **Activate From File (Activer depuis le fichier)** et sélectionner la version que vous souhaitez activer dans la liste déroulante (il se peut que vous deviez actualiser l'écran pour qu'elle s'affiche dans **Currently Activated (Actuellement activé)**). • **Reactivate (Réactiver)** : le logiciel de l'application correspondant a été activé et est prêt à être téléchargé par le point de terminaison. Comme une seule version du logiciel de l'application GlobalProtect peut être active à la fois sur le pare-feu, si vos utilisateurs finaux doivent accéder à une autre version que celle actuellement active, vous devez **Activate (Activer)** cette dernière pour qu'elle devienne la version **Currently Active (Actuellement active)**.
Notes de version	Cette option fournit un lien vers les notes de version GlobalProtect relatives à la version de l'application correspondante.

Paramètres du client GlobalProtect	Description
	Supprimez l'image du logiciel de l'application précédemment téléchargé à partir du pare-feu.

Paramétrage de l’application GlobalProtect

L’application GlobalProtect est une application qui est installée sur le point de terminaison (généralement un ordinateur portatif) pour prendre en charge les connexions que GlobalProtect établies avec les portails et les passerelles. L’application est soutenue par le service GlobalProtect (service PanGP).

Veillez à sélectionner l'option d'installation appropriée pour votre système d'exploitation hôte (32 ou 64 bits). Si vous installez sur un hôte 64 bits, utilisez le navigateur 64 bits et la combinaison Java pour l'installation initiale.

Pour installer l'application, ouvrez le fichier du programme d'installation et suivez les instructions affichées à l'écran.

Utilisation de l'application GlobalProtect

Les onglets du panneau **Paramètres GlobalProtect**, qui s’ouvre lorsque vous lancez l’application GlobalProtect et sélectionnez **Settings (Paramètres)** dans le menu **Paramètres** du panneau d’état GlobalProtect, contiennent des informations utiles sur l’état et les paramètres et fournissent des informations pour vous aider à régler les problèmes de connexion.

- Onglet Général : affiche le nom d’utilisateur et le ou les portails associés au compte GlobalProtect. Vous pouvez également ajouter, supprimer ou modifier des portails à partir de cet onglet.
- **Connection tab (Onglet Connexion)** : affiche la ou les passerelles qui sont configurées pour l’application GlobalProtect et fournit des informations à propos de chaque passerelle :
  - Nom de la passerelle
  - État du tunnel
  - Statut d'authentification
  - Type de connexion
  - Adresse IP ou FQDN de la passerelle (disponible uniquement en mode externe)

  *Pour le mode interne, l’onglet **Connection (Connexion)** présente la liste complète des passerelles disponibles. Pour le mode externe, l’onglet **Connection (Connexion)** affiche la passerelle à laquelle vous êtes connecté ainsi que des détails supplémentaires sur la passerelle (comme l’adresse IP de la passerelle et la disponibilité).*
- **Host Profile tab (Onglet Profil d’hôte)** : affiche les données sur les points de terminaison que GlobalProtect utilise pour la surveillance et l’application des politiques de sécurité par l’intermédiaire du Host Information Profile (Profil d'informations sur l'hôte ; HIP). Cliquez sur **Resubmit Host Profile (Envoyer de nouveau le profil de l'hôte)** pour procéder au renvoi manuel des données HIP à la passerelle.

- **Troubleshooting tab (Onglet Dépannage)** : sur les points de terminaison macOS, cet onglet vous permet de **Collect Logs (Collecter les journaux)** et de définir le **Logging Level (Niveau de journalisation)**. Sur les points de terminaison Windows, cet onglet vous permet de **Collect Logs (Collecter les journaux)**, de définir le **Logging Level (Niveau de journalisation)** et de consulter les informations suivantes pour vous aider dans le dépannage :
  - **Network Configurations (Configurations du réseau)** : indique la configuration actuelle du système.
  - **Routing Table (Table de routage)** - Fournit des informations sur la méthode d'acheminement actuelle de la connexion GlobalProtect.
  - **Sockets** - Fournit des informations sur les sockets des connexions actives.
  - **Logs (Journaux)** : permet à l'utilisateur de consulter les journaux de l'application et du service GlobalProtect. Choisissez le type de journal et le niveau de débogage. Cliquez sur **Start (Démarrer)** pour commencer la journalisation et sur **Stop (Arrêter)** pour l'arrêter.
- **Notification tab (Onglet Notification)** : affiche la liste de notifications déclenchées sur l'application GlobalProtect. Pour voir plus de détails d’une notification donnée, double-cliquez sur celle-ci.

Interface Web de Panorama

Panorama™ est le système de gestion centralisée pour l'ensemble des pare-feu de dernière génération Palo Alto Networks®. Panorama vous permet de superviser toutes les applications, les utilisateurs et le contenu présents sur votre réseau depuis un emplacement unique, puis utilise les informations obtenues pour créer des politiques permettant de contrôler et de protéger votre réseau. L'utilisation de Panorama pour la gestion centralisée des politiques et des pare-feu accroît votre efficacité opérationnelle lorsque vous gérez votre réseau distribué de pare-feux. Panorama est disponible sous forme de plate-forme d'appareil matériel dédiée (Série M) et d'équipement virtuel VMWare (exécuté sur un serveur ESXi ou la plate-forme vCloud Air).

Bien que de nombreux paramètres et affichages de l'interface Web Panorama soient identiques à ceux que vous voyez sur l'interface Web du pare-feu, les rubriques suivantes décrivent les options disponibles exclusivement sur l'interface Web Panorama pour gérer Panorama, les pare-feu et les Collecteurs de journaux.

- Utilisation de l'interface Web de Panorama
- Changement de contexte
- Opérations de validation du Panorama
- Définition des politiques sur Panorama
- Partitions de stockage des journaux pour un appareil virtuel Panorama en Mode hérité
- Panorama > Configuration > Interfaces
- Panorama > Haute disponibilité
- Panorama > Clusters WildFire gérés
- Panorama > Administrateurs
- Panorama > Rôles admin
- Panorama > Domaines d'accès
- Panorama > Transmission programmée des configurations
- Panorama > Périphériques gérés > Récapitulatif
- Panorama > Périphériques gérés > État
- Panorama > Modèles
- Panorama > Groupes de périphériques
- Panorama > Collecteurs gérés
- Panorama > Groupes de collecteurs
- Panorama > Plug-ins
- Panorama > SD-WAN
- Panorama > VMware NSX
- Panorama > Profil d'ingestion des journaux
- Panorama > Paramètres des journaux

- Panorama > Profils de serveur > SCP
- Panorama > Export programmée des configurations
- Panorama > Logiciel
- Panorama > Déploiement du périphérique
- Panorama > Clé d’autorisation de l’enregistrement du périphérique

Vous souhaitez en savoir plus ?

Voir le Guide de l’administrateur Panorama pour plus de détails sur la configuration et l’utilisation de Panorama pour la gestion centralisée.

Utilisation de l’interface Web de Panorama

Les interfaces Web de Panorama et les pare-feu ont le même aspect. Cependant, l’interface Web de Panorama offre des options supplémentaires et un onglet spécifique à Panorama pour la gestion de Panorama ainsi que pour son utilisation en vue de gérer les pare-feu et les Collecteurs de journaux.

Les champs communs suivants apparaissent dans l’en-tête ou le pied de page de plusieurs pages d’interface Web Panorama.

Champs commun	Description
Contexte	Vous pouvez utiliser la liste déroulante **Contexte** qui se trouve au-dessus du menu latéral pour passer de l’interface Web de Panorama à une interface Web du pare-feu (voir Commutation de contexte).
	Dans les onglets **Tableau de bord** et **Surveillance**, cliquez sur actualiser () dans l’en-tête de l’onglet pour actualiser manuellement les données dans ces onglets. Vous pouvez également utiliser le menu déroulant sans référence sur le côté droit de l’en-tête de l’onglet pour sélectionner un intervalle d’actualisation automatique en minutes (**1 min (1 minute)**, **2 mins (2 minutes)** ou **5 mins (5 minutes)**) ; pour désactiver l’actualisation automatique, sélectionnez **Manuel**.
Domaine d'accès	Un domaine d’accès définit l’accès à des groupes de périphériques spécifiques, des modèles et des pare-feu individuels (à travers le menu déroulant **Contexte**). Si vous vous connectez en tant qu’administrateur avec plusieurs domaines d’accès affectés à votre compte, les onglets **Tableau de bord**, **ACC**, et **Surveillance** affichent des informations (comme les données des journaux) uniquement pour le **Domaine d’accès** que vous sélectionnez dans le pied de page de l’interface Web. *Si un seul domaine d’accès est affecté à votre compte, l’interface Web n’affiche pas le menu déroulant **Domaine d’accès**.*
Groupe de périphériques	Un groupe de périphériques englobe des pare-feu et des systèmes virtuels que vous gérez en tant que groupes (voir Panorama > Groupes de périphériques). Les onglets **Tableau de bord**, **ACC**, et **Surveillance** affichent des informations (comme les données des journaux) uniquement pour le **Groupe de périphériques** que vous sélectionnez dans l’en-tête de l’onglet. Dans les onglets **Politiques** et **Objets**, vous pouvez configurer les paramètres pour un **Groupe de périphériques** ou pour tous les groupes de périphériques (sélectionnez **Partagé**).
Modèle	Un modèle est un groupe de pare-feu avec des paramètres réseau et de périphérique communs et une pile de modèles est une combinaison

Champs commun	Description
	de modèles (voir Panorama > Modèles). Dans les onglets **Réseau** et **Périphérique**, vous configurez les paramètres pour un **Modèle** spécifique ou une pile de modèles. Comme vous pouvez modifier les paramètres uniquement dans les modèles individuels, les paramètres de ces onglets sont en lecture seule si vous sélectionnez un ensemble (stack) de modèles.
Visualiser par : Périphérique Mode	Par défaut, les onglets **Réseau** et **Périphérique** affichent les paramètres et les valeurs disponibles pour les pare-feu qui sont en mode de fonctionnement normal et qui prennent en charge plusieurs systèmes virtuels et VPN. Cependant, vous pouvez utiliser les options suivantes pour filtrer les onglets afin d'afficher uniquement les paramètres spécifiques au mode à modifier : • Dans la liste déroulante **Mode**, activez ou désactivez les options **Multi-VSYS**, le **Mode opérationnel** et les options du **Mode VPN**. • Définissez toutes les options de Mode afin de tenir compte de la configuration d'un pare-feu en particulier en le sélectionnant dans le menu déroulant **Visualiser par : périphérique**.

L'onglet **Panorama** fournit les pages suivantes pour la gestion de Panorama et des Collecteurs de journaux.

Pages Panorama	Description
setup	Sélectionnez **Panorama (Panorama)** > **Setup (Configuration)** pour les tâches suivantes : • Préciser des paramètres généraux (par exemple, le nom d'hôte de Panorama) et des paramètres pour l'authentification, les journaux, les rapports, AutoFocus™, les bannières, le message du jour et la complexité des mots de passe. Ces paramètres sont similaires à ceux que vous configurez pour les pare-feu : sélectionnez Périphérique > Configuration > Gestion. • Sauvegarder et restaurer les configurations, redémarrer Panorama et arrêter Panorama. Ces opérations sont similaires à celles que vous effectuer pour les pare-feu : sélectionnez Périphérique > Configuration > Opérations. • Définir les connexions de serveur pour les mises à jour DNS, NTP et Palo Alto Networks. Ces paramètres sont similaires à ceux que vous configurez pour les pare-feu : sélectionnez Périphérique > Configuration > Services. • Configurer les paramètres réseau pour les interfaces Panorama. Sélectionnez Panorama > Configuration > Interfaces. • Précisez les paramètres pour l'appareil WildFire™. Ces paramètres sont similaires à ceux que vous configurez pour les pare-feu : sélectionnez Périphérique > Configuration > WildFire. • Gérer les paramètres des modules de sécurité matériels. Ces paramètres sont similaires à ceux que vous configurez pour les pare-feu : sélectionnez Périphérique > Configuration > HSM.

Pages Panorama	Description
Haute disponibilité	Vous permet de configurer la haute disponibilité pour une paire de serveurs de gestion Panorama. Sélectionnez Panorama > Haute Disponibilité.
Audit de configuration	Vous permet d'afficher les différences entre les fichiers de configuration. Sélectionnez Périphérique > Audit de configuration.
Profils de mot de passe	Vous permet de définir des profils de mot de passe pour les administrateurs de Panorama. Sélectionnez Périphérique > Profils de mot de passe.
Administrateurs	Vous permet de configurer les comptes administrateur Panorama. Sélectionnez Panorama > Administrateurs.  *Si un compte administrateur est verrouillé, la page **Administrateurs** affiche un verrou dans la colonne Utilisateur verrouillé. Vous pouvez cliquer sur le verrou pour déverrouiller le compte.*
Rôles administrateur	Vous permet de définir des rôles administrateur qui contrôlent les privilèges et les responsabilités des administrateurs qui ont accès à Panorama. Sélectionnez Panorama > Rôles administrateur.
Domaine d'accès	Vous permet de contrôler l'accès administrateur aux groupes de périphériques, modèles, piles de modèles et à l'interface Web de pare-feu. Sélectionnez Panorama > Domaines d'accès.
Profil d'authentification	Vous permet de préciser un profil pour authentifier l'accès à Panorama. Sélectionnez Périphérique > Profil d'authentification.
Séquence d'authentification	Vous permet de préciser une série de profils d'authentification à utiliser pour autoriser l'accès à Panorama. Sélectionnez Périphérique > Séquence d'authentification.
Identification utilisateur	Vous permet de configurer un profil de certificat personnalisé pour une authentification mutuelle des agents User-ID. Sélectionnez Device > User Identification > Connection Security (Périphérique > Identification utilisateur > Sécurité de la connexion)
Data Redistribution (Redistribution des données)	Vous permet de sélectionner les données à redistribuer vers les autres pare-feux ou les systèmes de gestion de Panorama. Sélectionnez Device > Data Redistribution (Périphérique > Redistribution des données).
Périphériques gérés	Vous permet de gérer les pare-feu, ce qui inclut l'ajout de pare-feu à Panorama en tant que *périphériques gérés*, l'affichage de la connexion des pare-feu et l'état des licences, l'étiquetage des pare-feu, les mises à jour logicielles et de contenu et le chargement des sauvegardes des configurations. Sélectionnez Panorama > Périphériques gérés > Récapitulatif.

Pages Panorama	Description
Modèles	Vous permet de gérer la configuration des options de configuration dans les onglets **Périphérique** et **Réseau**. Les modèles et les piles de modèles vous permettent de réduire les efforts administratifs grâce au déploiement de plusieurs pare-feu disposant de configurations identiques ou similaires. Sélectionnez Panorama > Modèles.
Groupes de périphériques	Vous permet de configurer les groupes de périphériques, qui regroupent les pare-feu en fonction de leurs fonctionnalités, leur segmentation réseau ou de leur emplacement géographique. Les groupes de périphériques peuvent inclure des pare-feu physiques, des pare-feu virtuels et des systèmes virtuels. Généralement, les pare-feu d'un groupe de périphériques nécessitent des configurations de politiques similaires. À l'aide des onglets **Policies (Politiques)** et **Objects (Objets)** sur Panorama, les groupes de périphériques permettent de mettre en œuvre une approche en couche pour gérer les politiques au sein d'un réseau de pare-feu gérés. Vous pouvez imbriquer des groupes de périphériques à une hiérarchie d'arborescence pouvant comporter un maximum de quatre niveaux. Les groupes descendants héritent automatiquement des politiques et objets des anciens groupes et de l'emplacement Partagé. Sélectionnez Panorama > Groupes de périphériques.
Collecteurs gérés	Vous permet de gérer les Collecteurs de journaux. Étant donné que vous utilisez Panorama pour configurer et gérer les collecteurs de journaux, ils sont également appelés *les collecteurs gérés*. Un collecteur géré peut être local au serveur de gestion Panorama (appareil de la série M ou appareil virtuel Panorama en mode Panorama) ou un Collecteur de journaux dédié (appareil de la série M en mode Collecteur de journaux). Sélectionnez Panorama > Collecteurs gérés. Vous pouvez également installer les Mises à jour logicielles pour les collecteurs de journaux dédiés. *Vous pouvez* convertir un serveur de gestion Panorama en un Collecteur de journaux dédié.
Groupes de collecteurs	Vous permet de gérer les Groupes de collecteurs. Un Groupe de collecteurs regroupe les Collecteurs de journaux pour que vous puissiez appliquer des paramètres de configuration identiques et leur assigner des pare-feu. Panorama distribue uniformément les journaux entre tous les disques d'un collecteur de journaux et tous les membres du groupe de collecteurs. Sélectionnez Panorama > Groupes de collecteurs.
Plug-ins	Vous permet de gérer les plug-ins pour une intégration tierce, par exemple VMware NSX. Sélectionnez Panorama > VMware NSX.

Pages Panorama	Description
VMware NSX	Vous permet d'automatiser l'approvisionnement des pare-feu de série VM en activant la communication entre NSX Manager et Panorama. Sélectionnez Panorama > VMware NSX.
Gestion des certificats	Vous permet de configurer et de gérer des certificats, des profils de certificat et des clés. Sélectionnez Gestion des certificats du pare-feu et de Panorama.
Paramètres des journaux	Vous permet de transférer des journaux aux récepteurs de pièges SNMP (Simple Network Management Protocol / protocole de gestion de réseau simple), serveurs Syslog, serveurs e-mail et serveurs HTTP. Sélectionnez Périphérique > Paramètres des journaux.
Profils de serveur	Vous permet de configurer les profils des différents types de serveurs qui fournissent des services à Panorama. Sélectionnez l'une des options suivantes pour configurer un type de serveur spécifique : • Périphérique > Profils de serveur > Messagerie • Périphérique > Profils de serveur > HTTP • Périphérique > Profils de serveur > Piège'A0;SNMP • Périphérique > Profils de serveur > Syslog • Périphérique > Profils de serveur > RADIUS • Périphérique > Profils de serveur > TACACS+ • Périphérique > Profils de serveur > LDAP • Périphérique > Profils de serveur > Kerberos • Périphérique > Profils de serveur > Fournisseur d'identité SAML
Exportation planifiée des configurations	Vous permet d'exporter les configurations de Panorama et du pare-feu vers serveur FTP ou un serveur SCP (Secure Copy / copie sécurisée) de manière quotidienne. Sélectionnez Panorama > Planifier l'exportation de la configuration.
Logiciels	Vous permet de mettre à jour le logiciel Panorama. Sélectionnez Panorama > Logiciel.
Mises à jour dynamiques	Vous permet de consulter les dernières définitions d'applications et informations sur les nouvelles menaces de sécurité telles que des signatures Antivirus (licence de protection contre les menaces requise) puis de mettre à jour Panorama avec les nouvelles définitions. Sélectionnez Périphérique > Mises à jour dynamiques.
Assistance	Vous permet d'accéder aux alertes produit et de sécurité de Palo Alto Networks. Sélectionnez Panorama > Assistance.

Pages Panorama	Description
Déploiement de périphériques	Vous permet de déployer des mises à jour logicielles et de contenu sur les pare-feu et les Collecteurs de journaux. Sélectionnez Panorama > Déploiement du périphérique.
Clé principale et diagnostics	Vous permet de préciser une clé principale afin de chiffrer des clés privées sur Panorama. Par défaut, Panorama stocke les clés privées sous forme cryptée, même si vous n'indiquez pas une nouvelle clé principale. Sélectionnez Périphérique > Clé principale et diagnostics.

Commutateur de contexte

Dans l’en-tête de chaque interface Web de Panorama, vous pouvez utiliser la liste déroulante **Contexte** qui se trouve au-dessus du menu de gauche pour passer de l’interface Web de Panorama à une interface Web du pare-feu. Lorsque vous sélectionnez un pare-feu, l'interface Web est actualisée pour afficher toutes les pages et options du pare-feu sélectionné pour que vous puissiez le gérer localement. La liste déroulante n’affiche que les pare-feu pour lesquels vous disposez d’un accès administrateur (voir Panorama > Domaines d’accès) et qui sont connectés à Panorama.

Vous pouvez utiliser les Filtres pour rechercher des pare-feu par Plateformes (modèle), Groupes de périphériques, Modèles, Étiquettes ou de l’état HD. Vous pouvez également saisir une chaîne de texte dans la barre de filtrage pour effectuer une recherche par Nom de périphérique.

L’arrière-plan des icônes des pare-feu en mode haute disponibilité (HD) est coloré pour indiquer leur état HD.

Opérations de validation de Panorama

Cliquez sur **Commit (Valider)** en haut à droite de l'interface Web et sélectionnez une action pour les modifications en attente pour la configuration Panorama et les modifications apportées par Panorama aux pare-feu, aux collecteurs de journaux et aux appareils et clusters WildFire :

- **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** – Active les changements que vous avez effectués pour la configuration du serveur de gestion Panorama. Cette action valide également les modifications du groupe de périphériques, du modèle, du groupe de collecteurs, du cluster et des appareils WildFire apportées à la configuration Panorama sans appliquer les modifications aux pare-feu, aux collecteurs de journaux ou aux clusters et appareils WildFire. L'application de ces modifications uniquement à la configuration Panorama vous permet d'enregistrer les modifications qui ne sont pas prêtes à être activées sur les pare-feu, les collecteurs de journaux ou les clusters et appareils WildFire.

  Lorsque vous appliquez les configurations aux périphériques gérés, Panorama 8.0 et les versions ultérieures appliquent la configuration actuelle, qui correspond à la configuration qui est activée sur Panorama. Panorama 7.1 et les versions antérieures appliquent la configuration candidate, qui inclut les modifications non validées. Par conséquent, Panorama 8.0 et les versions ultérieures ne vous permettent pas d'appliquer les modifications apportées aux périphériques gérés jusqu'à ce que vous validiez d'abord les modifications apportées à Panorama.
- **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** – Applique la configuration actuelle de Panorama aux groupes de périphériques, aux modèles, aux groupes de collecteurs et aux clusters et appareils WildFire.
- **Commit (Valider)** > **commit and Push (Valider et appliquer)** – Applique toutes les modifications de configuration à la configuration locale de Panorama, puis applique la configuration actuelle de Panorama aux groupes de périphériques, aux modèles, aux groupes de collecteurs et aux clusters et appareils WildFire.

Vous pouvez filtrer les modifications en attente par administrateur ou *emplacement*, puis vous pouvez confirmer, appliquer, valider ou prévisualiser uniquement ces modifications. L'emplacement peut être des groupes de périphériques spécifiques, des modèles, des groupes de collecteurs, des collecteurs de journaux, des appareils et des clusters WildFire, des paramètres partagés ou le serveur de gestion Panorama.

Lorsque vous validez des modifications, elles deviennent partie intégrante de la configuration actuelle. Les modifications que vous n'avez pas validées font partie de la configuration candidate. Panorama met les demandes de validation en file d'attente pour que vous puissiez initier de nouvelles validations alors qu'une validation antérieure est en cours d'exécution. Panorama exécute les validations dans l'ordre dans lequel elles sont initiées, mais donne la priorité aux validations que Panorama initie automatiquement, comme les actualisations du nom de domaine complet. Cependant, si la file d'attente possède déjà le nombre maximum de validations lancées par l'administrateur, vous devez attendre que Panorama termine le traitement d'une validation en attente avant d'en lancer une nouvelle. Vous pouvez utiliser le Gestionnaire de tâches () pour vider la file d'attente des validations ou pour consulter les informations sur les validations. Pour plus d'informations sur les modifications de configuration, les processus de validation, les validations ou la file d'attente des validations, reportez-vous à la section Opérations de validation sur Panorama. Vous pouvez aussi Enregistrer les configurations candidates, Annuler les modifications et importer, exporter ou charger des configurations (Périphérique > Configuration > Opérations).

Les options suivantes sont disponibles pour confirmer, valider ou prévisualiser les modifications de configuration.

Champ/Bouton	Description
Les options suivantes s'appliquent lorsque vous les validez sur Panorama en sélectionnant **Commit (Valider)** > **Commit to Panorama (Valider sur Panorama)** ou **Commit (Valider)** > **Commit and Push (Valider et appliquer)**.	
Valider toutes les modifications	Confirme toutes les modifications pour lesquelles vous avez des privilèges administratifs (par défaut). Vous ne pouvez pas filtrer manuellement l'étendue des modifications de configuration que Panorama valide lorsque vous sélectionnez cette option. Au lieu de cela, le rôle d'administrateur affecté au compte que vous avez utilisé pour vous connecter détermine l'étendue de validation : • **Rôle du super-utilisateur** – Panorama valide les changements de tous les administrateurs. • **Rôle personnalisé** – Les privilèges du profil de rôle administrateur affecté à votre compte déterminent la portée de validation (voir Panorama > Rôles administrateurs). Si le profil inclut le privilège de **Commit For Other Admins (Valider pour les autres administrateurs)**, Panorama valide les modifications configurées par un ou tous les administrateurs. Si votre profil de rôle administrateur n'inclut pas le privilège de **Commit For Other Admins (Valider pour les autres administrateurs)**, Panorama valide uniquement vos modifications et pas celles des autres administrateurs. Si vous avez mis en place des domaines d'accès, Panorama applique automatiquement ces domaines pour filtrer la portée de validation (voir Panorama > Domaines d'accès). Quel que soit votre rôle administrateur, Panorama ne valide que les modifications de configuration dans les domaines d'accès affectés à votre compte.
Valider les modifications effectuées par	Filtre la portée des changements de configuration que Panorama valide. Le rôle administrateur affecté au compte que vous avez utilisé pour vous connecter détermine vos options de filtrage : • **Rôle du super-utilisateur** – Vous pouvez limiter l'étendue de validation aux modifications apportées par des administrateurs spécifiques et aux modifications effectuées dans des emplacements spécifiques. • **Rôle personnalisé** – Les privilèges du profil de rôle administrateur affecté à votre compte déterminent la portée de validation (voir Périphérique > Rôles administrateurs). Si le profil inclut le privilège **Commit For Other Admins (Valider pour les autres administrateurs)**, vous pouvez limiter l'étendue de validation aux modifications configurées par des administrateurs spécifiques et aux modifications effectuées

Champ/Bouton	Description
	dans des emplacements spécifiques. Si votre profil de Rôle administrateur n'inclut pas le privilège **Commit For Other Admins (Valider pour les autres administrateurs)**, vous pouvez limiter l'étendue de validation uniquement aux modifications que vous avez effectuées dans des emplacements spécifiques. Filtre l'étendue de validation comme suit : • **Filtrer par administrateur** – Même si votre rôle vous permet de valider les modifications effectuées par les autres administrateurs, par défaut, l'étendue de validation inclut uniquement vos modifications. Pour ajouter d'autres administrateurs à la portée de la validation, cliquez sur le lien <*usernames*>, sélectionnez les administrateurs et cliquez sur **OK**. • **Filtrer par emplacement** – Sélectionnez les emplacements spécifiques pour les modifications à Inclure dans la validation. Si vous avez mis en place des domaines d'accès, Panorama filtre automatiquement la portée de validation en fonction de ces domaines (voir Panorama > Domaines d'accès). Quel que soit votre rôle administrateur et vos choix de filtrage, l'étendue de validation inclut uniquement les modifications de configuration dans les domaines d'accès affectés à votre compte. *Après avoir chargé une configuration (Périphérique > Configuration > Opérations), vous devez **Valider toutes les modifications**.* Lorsque vous validez des modifications apportées à un groupe de périphériques, vous devez inclure les modifications de tous les administrateurs qui ont ajouté, supprimé ou repositionné des règles pour la même base de règles dans ce groupe de périphériques.
Étendue de la validation	Répertorie les emplacements contenant des modifications à valider. Différents facteurs déterminent si la liste inclut toutes les modifications ou un sous-ensemble de modifications, comme il est décrit dans Valider toutes les modifications et Valider les modifications effectuées par. Les emplacements peuvent être l'un des éléments suivants : • **shared-object (objet partagé)** – Les paramètres qui sont définis dans l'emplacement Partagé. • ***<device-group>***: Le nom du groupe de périphériques dans lequel les règles de politique ou les objets sont définis. • ***<template>***: Le nom du modèle ou du groupe de modèles dans lequel les paramètres sont définis. • ***<log-collector-group>***: Le nom du groupe de collecteur dans lequel les paramètres sont définis.

Champ/Bouton	Description
	• <***log-collector***>: Le nom du collecteur de journaux dans lequel les paramètres sont définis. • <***wildfire-appliances***>: Le numéro de série de l'appareil WildFire dans lequel les paramètres sont définis. • <***wildfire-appliance-clusters***>: nom du cluster WildFire dans lequel les paramètres sont définis.
Type d'emplacement	Cette colonne classe les emplacements des modifications en attente : • **Panorama** – Paramètres spécifiques à la configuration du serveur de gestion Panorama. • **Device Group (Groupe de périphériques)** – Paramètres définis dans un groupe de périphériques spécifique. • **Template (Modèle)** – Paramètres définis dans un modèle ou un groupe de modèles spécifique. • **Log Collector Group (Groupe de collecteurs de journaux)** – Paramètres qui sont spécifiques à une configuration de groupe de collecteur. • **Log Collector (Collecteur de journaux)** – Paramètres spécifiques à une configuration de collecteur de journaux. • **WildFire Appliance Clusters (Clusters d'appareils WildFire)** – Paramètres spécifiques à une configuration de cluster d'appareils WildFire. • **WildFire Appliances (Appareils WildFire)** – Paramètres spécifiques à un appareil WildFire. • **Autres changements** – Paramètres qui ne sont pas spécifiques à l'une des zones de configuration précédentes (telles que les objets partagés).
Type d'objet	Affiche le type d'objet de la modification de configuration. Par exemple, si vous avez configuré un profil réseau (**Réseau** > **Profiles réseau**), les `profiles` s'affichent. Si vous configurez un groupe d'adresses (**Objets** > **Groupes d'adresses**), `address-group` s'affiche.
Administrateurs	Nom de l'administrateur qui a effectué la modification de configuration.
Inclure dans la validation (Validation partielle uniquement)	Vous permet de sélectionner les modifications que vous souhaitez valider. Par défaut, toutes les modifications de l'**Étendue de validation** sont sélectionnées. Cette colonne s'affiche uniquement après que vous avez choisi de **Valider les modifications effectuées par** des administrateurs spécifiques.

Champ/Bouton	Description
	Il peut y avoir des dépendances affectant les modifications que vous incluez dans une validation. Par exemple, si vous ajoutez un objet et qu'un autre administrateur modifie cet objet, vous ne pouvez pas valider la modification pour l'autre administrateur sans valider votre propre modification.
Regrouper par type	Regroupe la liste des modifications de configuration de l'**Étendue de validation** par **Type d'emplacement**.
Prévisualiser les modifications	Vous permet de comparer les configurations que vous avez sélectionnées dans l'**Étendue de validation** de la configuration en cours d'exécution. La fenêtre de prévisualisation utilise un code couleur pour indiquer quelles modifications sont des ajouts (en vert), des modifications (en jaune) ou des suppressions (en rouge). Pour vous aider à faire correspondre les modifications aux sections de l'interface Web, vous pouvez configurer la fenêtre de prévisualisation pour afficher **Lignes de contexte** avant et après chaque modification. Ces lignes proviennent des fichiers du candidat et des configurations en cours d'exécution que vous comparez. *Étant donné que les résultats de prévisualisation s'affichent dans une nouvelle fenêtre de navigateur, votre navigateur doit autoriser les fenêtres contextuelles. Si la fenêtre de prévisualisation ne s'ouvre pas, reportez-vous à la documentation de votre navigateur pour connaître les étapes permettant d'autoriser les fenêtres contextuelles.*
Modifier le récapitulatif	Répertorie les paramètres individuels pour lesquels vous effectuez des modifications. La liste **Récapitulatif des modifications** affiche les informations suivantes pour chaque paramètre : • **Nom de l'objet** – Le nom qui identifie la politique, l'objet, le paramètre réseau ou le paramètre de périphérique. • **Type** – Le type de paramètre (comme Adresse, règle de Sécurité ou Zone). • **Type d'emplacement** – Indique si le paramètre est défini dans **Groupes de périphériques**, **Modèles**, **Groupes de collecteurs**, **Appareils WildFire** ou **Clusters d'appareils WildFire**. • **Emplacement** – Le nom du groupe de périphériques, du modèle, du groupe de collecteurs, du cluster WildFire ou de l'appareil WildFire où le paramètre est défini. La colonne affiche **Partagé** pour les paramètres qui ne sont pas définis dans ces emplacements.

Champ/Bouton	Description
	• **Opérations** – Indique chaque opération (créer, modifier ou supprimer) exécutée sur le paramètre depuis la dernière validation. • **Propriétaire** – L'administrateur qui a effectué la dernière modification du paramètre. • **Sera validé** – Indique si la validation inclura le paramètre. • **Propriétaires précédents** – Les administrateurs qui ont apporté des modifications au paramètre avant la dernière modification. Vous pouvez éventuellement **Regrouper par** Nom de colonne (comme **Type**).
Confirmer la validation	Vérifie que la syntaxe de la configuration de Panorama est correcte et est complète d'un point de vue sémantique. Le résultat inclut les mêmes erreurs et avertissements qu'une validation afficherait, y compris la règle l'occultation et l'application des avertissements de dépendance. Le processus de validation vous permet de trouver et de corriger les erreurs avant la validation (il ne modifie pas la configuration en cours d'exécution). Cette option est utile si vous avez une fenêtre de validation fixe et que vous souhaitez vous assurer que la validation sera une réussite exempte d'erreur.
Les options suivantes s'appliquent lorsque vous appliquez les modifications de configuration sur les périphériques gérés en sélectionnant **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** ou **Commit (Valider)** > **Commit and Push (Valider et appliquer)**.	
Transférer toutes les modifications	Transmet toutes les modifications pour lesquelles vous avez des privilèges administratifs (par défaut). Vous ne pouvez pas filtrer manuellement l'étendue des modifications de configuration que Panorama transmet lorsque vous sélectionnez cette option. Au lieu de cela, le rôle d'administrateur affecté au compte que vous avez utilisé pour vous connecter détermine la portée de la transmission : • **Rôle du super-utilisateur**: Panorama transmet les changements de tous les administrateurs. • **Rôle personnalisé** – Les privilèges du profil de rôle administrateur affecté à votre compte déterminent la portée de transmission (voir Panorama > Rôles administrateurs). Si le profil inclut le privilège de **Commit For Other Admins (Valider pour les autres administrateurs)**, Panorama transmet les modifications configurées par un ou tous les administrateurs. Si votre profil de rôle administrateur n'inclut pas le privilège de **Push For Other Admins (Transmet pour les autres administrateurs)**, Panorama valide uniquement vos modifications et pas celles des autres administrateurs. Si vous avez mis en place des domaines d'accès, Panorama applique automatiquement ces domaines pour filtrer la portée de transmission (voir Panorama > Domaines d'accès). Quel que soit votre rôle

Champ/Bouton	Description
	administrateur, Panorama ne transmet que les modifications de configuration dans les domaines d'accès affectés à votre compte.
Transmettre les modifications effectuées par	Filtre la portée des changements de configuration que Panorama transmet. Le rôle administrateur affecté au compte que vous avez utilisé pour vous connecter détermine vos options de filtrage : • **Rôle de super-utilisateur** – Vous pouvez limiter la portée de la transmission aux modifications apportées par des administrateurs spécifiques et aux modifications dans des emplacements spécifiques. • **Rôle personnalisé** – Les privilèges du profil de rôle administrateur affecté à votre compte déterminent la portée de validation (voir Périphérique > Rôles administrateurs). Si le profil inclut le privilège de **Transmettre pour les autres administrateurs**, vous pouvez limiter la portée de la transmission aux modifications configurées par des administrateurs spécifiques et aux modifications dans des emplacements spécifiques. Si votre profil de Rôle administrateur n'inclut pas le privilège de **Transmettre pour les autres administrateurs**, vous pouvez limiter la portée de la transmission uniquement aux modifications que vous avez effectuées dans des emplacements spécifiques. Filtrez l'étendue push comme suit : • **Filtrer par administrateur** – Même si votre rôle permet de transmettre les modifications d'autres administrateurs, la portée de la transmission inclut uniquement vos modifications par défaut. Pour ajouter d'autres administrateurs à la portée de l'enregistrement, cliquez sur le lien <*usernames*> , sélectionnez les administrateurs et cliquez sur **OK**. • **Filtrer par emplacement** – Sélectionnez les emplacements spécifiques pour les modifications à Inclure dans la transmission. Si vous avez mis en place des domaines d'accès, Panorama filtre automatiquement la portée de la transmission en fonction de ces domaines (voir Panorama > Domaines d'accès). Quels que soient votre rôle administratif et vos choix de filtrage, la portée de la transmission inclut uniquement les modifications de configuration dans les domaines d'accès affectés à votre compte.
Étendue de la transmission	Liste les emplacements qui ont des modifications à appliquer. Les emplacements que la portée inclut par défaut dépendent des options suivantes que vous sélectionnez : • **Commit (Valider)** > **Commit and Push (Valider et appliquer)** – La portée comprend tous les emplacements avec des modifications nécessitant une validation de la part de Panorama.

Champ/Bouton	Description
	• **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** – La portée comprend tous les emplacements associés aux entités (pare-feux, systèmes virtuels, collecteurs de journaux, clusters WildFire, appareils WildFire) qui sont `Out of Sync (Désynchronisées)` avec la configuration actuelle de Panorama (voir Panorama > Périphériques gérés > Récapitulatif et Panorama > Collecteurs gérés pour le statut de synchronisation). Pour les deux sélections, Panorama filtre la **Portée d'application** par : • **Administrateurs** – Panorama applique les mêmes filtres que pour **la Portée de validation** (voir Appliquer tous les changements ou Appliquer les modifications faites par). • **Domaine d'accès** – Si vous avez mis en place des domaines d'accès, Panorama filtre automatiquement la **Portée d'application** en fonction de ces domaines (voir Panorama > Domaines d'accès). Quel que soit votre rôle administrateur et vos choix de filtrage, l'étendue inclut uniquement les modifications de configuration dans les domaines d'accès affectés à votre compte. Vous pouvez Modifier les sélections pour la **Portée d'application** au lieu d'accepter les emplacements par défaut. Vous pouvez planifier une transmission de configuration lorsque vous sélectionnez **Valider** > **la transmission vers les périphériques**.
Type d'emplacement	Cette colonne classe les emplacements des modifications en attente : • **Groupes de périphériques** – Paramètres définis dans un groupe de périphériques spécifique. • **Modèles** – Paramètres définis dans un modèle ou une pile de modèles spécifique. • **Groupe de collecteurs de journaux** – Paramètres spécifiques à une configuration de groupe de collecteur. • **Clusters WildFire** – Paramètres spécifiques à une configuration de cluster WildFire. • **Appareils WildFire** – Paramètres spécifiques à une configuration d'appareil WildFire.
Type d'objet	Affiche le type d'objet de la modification de configuration. Par exemple, si vous avez configuré un profil réseau (**Réseau** > **Profiles réseau**), les `profiles` s'affichent. Si vous configurez un groupe d'adresses (**Objets** > **Groupes d'adresses**), `address-group` s'affiche.

Champ/Bouton	Description
Entités	Pour chaque groupe de périphériques ou modèle, cette colonne répertorie les pare-feu (par nom de périphérique ou numéro de série) ou les systèmes virtuels (par nom) inclus dans l'opération de validation. **Modifier les sélections** pour modifier la liste des pare-feu ou des systèmes virtuels concernés vers lesquels transmettre les modifications de configuration. *Si vous appliquez les modifications apportées à un groupe de collecteurs, l'opération inclut tous les collecteurs de journaux qui sont des membres du groupe, même s'ils ne sont pas répertoriés.*
Administrateurs	Nom de l'administrateur qui a effectué la modification de configuration.
Inclure dans la transmission	Vous permet de sélectionner les modifications que vous souhaitez transmettre. Par défaut, toutes les modifications contenues dans **Transmettre la portée** sont sélectionnées. Cette colonne s'affiche uniquement après que vous avez choisi de **Transmettre** les modifications effectuées par des administrateurs spécifiques.
Modifier les sélections	Cliquez pour sélectionner les entités à inclure dans l'opération de validation : • Modèles et groupes de périphériques • Groupes de collecteurs de journaux • Appareils et clusters WildFire *Panorama ne vous permettra pas d'appliquer les modifications que vous n'avez pas encore validées dans la configuration de Panorama.*
Modèles et groupes de périphériques	Cliquez pour **Modifier les sélections** et sélectionnez les **Groupes de périphériques** ou les **Modèles** pour afficher les options dans les lignes suivantes.
Filtres	Filtrez la liste des modèles, des piles de modèles ou des groupes de périphériques et les pare-feu et systèmes virtuels associés. Vous pouvez filtrer les pare-feux gérés en fonction de leur état de validation, état du périphérique, étiquettes et état de haute disponibilité (HA).
Name (Nom)	Sélectionnez les modèles, les piles de modèles, les groupes de périphériques, les pare-feu ou les systèmes virtuels à inclure dans l'opération de validation.

Champ/Bouton	Description
État de la dernière validation	Indique si les configurations des pare-feu et des systèmes virtuels sont synchronisées avec les configurations des modèles ou des groupes de périphériques dans Panorama.
État HA	Indique l'état de la haute disponibilité (HA) sur les pare-feu énumérées : • **Active (Actif)** - État opérationnel de gestion du trafic normal. • **Passive (Passif)**- État de sauvegarde normal. • **Initiating (En cours d'initialisation)** - Le pare-feu est dans cet état pendant 60 secondes maximum après le démarrage. • **Non-functional (Non fonctionnel)** - État d'erreur. • **Suspended (Suspendu)** - Un administrateur a désactivé le pare-feu. • **Tentative (Provisoire)** - Pour un événement de surveillance des liaisons ou des chemins dans une configuration active/active.
Modifications en attente de validation (Panorama)	Indique si une validation Panorama est requise (`oui`) ou non (`non`) avant d'appliquer les modifications aux pare-feu et aux systèmes virtuels sélectionnés.
Colonne de prévisualisation des modifications	Cliquez pour **prévisualiser les modifications** pour comparer les configurations que vous avez sélectionnées dans la **Portée d'application** pour la configuration actuelle de Panorama. Panorama filtre les résultats pour afficher uniquement les résultats pour les pare-feu et les systèmes virtuels que vous avez sélectionnés dans l'onglet **Groupes de périphériques** ou **Modèles**. La fenêtre de prévisualisation utilise un code couleur pour indiquer quelles modifications sont des ajouts (en vert), des modifications (en jaune) ou des suppressions (en rouge). *Étant donné que les résultats de prévisualisation s'affichent dans une nouvelle fenêtre de navigateur, votre navigateur doit autoriser les fenêtres contextuelles. Si la fenêtre de prévisualisation ne s'ouvre pas, reportez-vous à la documentation de votre navigateur pour connaître les étapes permettant d'autoriser les fenêtres contextuelles.*
Sélectionner tout	Sélectionne toutes les entrées de la liste.
Désélectionner tout	Désélectionne toutes les entrées de la liste.
Développer tout	Affiche les pare-feu et les systèmes virtuels attribués aux modèles, aux piles de modèles ou aux groupes de périphériques.

Champ/Bouton	Description
Réduire tout	Affiche uniquement les modèles, les piles de modèles ou les groupes de périphériques, mais pas les pare-feu ou les systèmes virtuels qui leur sont attribués.
Regrouper les homologues HA	Regroupe les pare-feu homologues dans une configuration haute disponibilité (HA). La liste qui en résulte affiche alors le pare-feu actif (ou le pare-feu actif / principal dans une configuration active / active) en premier, suivi du pare-feu passif (ou pare-feu actif / secondaire dans une configuration active / active) entre parenthèses. Ceci vous permet d'identifier facilement les pare-feu en mode HA. Lors de l'application de politiques partagées, vous pouvez l'appliquer à la paire regroupée plutôt qu'à chaque homologue.  *pour des homologues HA dans une configuration active/passive, envisagez l'ajout des deux pare-feu ou de leurs systèmes virtuels au même groupe de périphériques, au même modèle ou à la même pile de modèles pour que vous puissiez appliquer la configuration aux deux homologues de façon simultanée.*
Appliquer	Cliquez pour valider les configurations que vous appliquez pour les pare-feu et les systèmes virtuels sélectionnés. Le Gestionnaire des tâches s’ouvre automatiquement pour afficher l’état de la validation.
Filtre sélectionné	Si vous souhaitez afficher uniquement certains pare-feu ou systèmes virtuels, sélectionnez-les puis sélectionnez **Filtre sélectionné**.
Fusionner avec la configuration du candidat	(Selectionné par défaut) Fusionne les modifications de configuration transmises par Panorama en prenant en compte les modifications en attente mises en œuvre localement par les administrateurs sur le pare-feu cible. L’opération de validation déclenche PAN-OS® pour valider les modifications fusionnées. Si vous désélectionnez cette option, la validation exclut la configuration candidate sur le pare-feu.  *Désélectionnez cette option si vous autorisez les administrateurs de pare-feu à valider les modifications localement sur le pare-feu et si vous ne voulez pas inclure ces modifications locales lors de la validation de modifications à partir de Panorama.* Il est également recommandé de faire un audit de configuration sur le pare-feu afin de passer en revue les modifications locales avant d’appliquer les modifications à partir de Panorama (Reportez-vous à la section Périphérique > Audit de configuration).

Champ/Bouton	Description
Inclure les modèles de réseaux et de périphériques (Onglet Groupes de périphériques uniquement)	(Sélectionné par défaut) Applique les changements de groupe de périphériques et les modifications du modèle associé aux pare-feu et aux systèmes virtuels sélectionnés en une seule opération. Pour appliquer ces modifications en tant qu'opérations distinctes, désélectionnez cette option.
Forcer les valeurs du modèle	Remplace tous les paramètres locaux par des objets définis dans les modèles ou les piles de modèles. Cela inclut les objets configurés localement ainsi que les objets poussés à partir de Panorama qui ont été remplacés localement. Si un objet est configuré localement sur le pare-feu, mais n'est pas configuré dans un modèle ou une pile de modèles, il reste inchangé sur le pare-feu et n'est pas supprimé. Le paramètre est désactivé par défaut et doit être activé (coché) à chaque poussée de Panorama vers les pare-feu gérés. *Si vous transmettez un configuration avec l'option **Force Template Values (Forcer les valeurs du modèle)** activée, toutes les valeurs forcées du pare-feu sont remplacées par les valeurs du modèle. Avant d'utiliser cette option, vérifiez les valeurs forcées des pare-feu pour garantir que votre validation ne donne pas lieu à des pannes réseau imprévus ou à des problèmes causés par le remplacement de ces valeurs forcées.*
Groupes de collecteurs de journaux	Cliquez pour **Modifier les sélections** et sélectionnez **Groupes de collecteurs de journaux** à inclure dans l'opération de validation. Cet onglet affiche les options suivantes : • **Tout sélectionner** – Sélectionne chaque groupe de collecteurs dans la liste. • **Tout désélectionner** – Désélectionne chaque groupe de collecteurs dans la liste.
Appareils et clusters WildFire	Pour **Modifier les sélections** et sélectionner les **Clusters et appareils WildFire** pour afficher les options suivantes.
Filtres	Filtre la liste des appareils et des clusters WildFire.
Name (Nom)	Sélectionne les appareils et les clusters WildFire sur lesquels Panorama appliquera les modifications.
État de la dernière validation	Indique si les configurations de l'appareil et du cluster WildFire sont synchronisées avec Panorama.
Aucune sélection par défaut	Activez (cochez) pour supprimer les périphériques sélectionnés par défaut afin de sélectionner manuellement les périphériques

Champ/Bouton	Description
	spécifiques vers les périphériques vers les qu'il faut transférer. Les périphériques par défaut vers lesquels Panorama transfère sont basés sur les modifications de configuration du groupe de périphériques et du modèle affectés. *L'activation de ce paramètre est persistante sur les push vers les appareils (**Commit (valider)** > **Push to Devices (transférer vers les périphériques)** et **Commit (valider)** > **Commit and Push (Valider et transférer)**) et est spécifique au compte d'administrateur qui a activé le paramètre. Une fois que vous avez activé ce paramètre pour un transfert, ce paramètre est activé pour tous les transferts suivants jusqu'à ce qu'il soit désactivé.*
Confirmer la transmission du groupe d'appareils	Valide les configurations que vous appliquez pour les groupes de périphériques dans la liste Portée d'application. Le Gestionnaire des tâches s'ouvre automatiquement pour afficher l'état de la validation.
Confirmer la transmission du modèle	Valide les configurations que vous appliquez pour les modèles dans la liste Portée d'application. Le Gestionnaire des tâches s'ouvre automatiquement pour afficher l'état de la validation.
Regrouper par type d'emplacement	À sélectionner pour utiliser le **Type d'emplacement** pour grouper la liste Portée d'application.
Les options suivantes s'appliquent lorsque vous validez la configuration Panorama ou lorsque vous appliquez les modifications apportées aux périphériques.	
Description	Saisissez une description (jusqu'à 512 caractères) pour aider les autres administrateurs à comprendre les modifications que vous avez effectuées. *Le Journal système pour un événement de validation tronquera la description si elle dépasse 512 caractères.*
Valider / Appliquer / Valider et appliquer	Démarre la validation ou, si d'autres validations sont en attente, ajoute la demande de validation à la file d'attente de validation.

Définition des politiques sur Panorama

Sur Panorama™, les groupes de périphériques vous permettent de gérer de façon centralisée les politiques des pare-feu. Vous pouvez créer les politiques sur Panorama en tant que *Règles avant* ou que *Règles après* ; les Règles avant et les Règles après vous permettent de créer une approche progressive de la mise en œuvre des politiques.

Vous pouvez définir les Règles avant et les Règles après dans un contexte partagé, comme politiques partagées pour tous les pare-feu gérés ou dans un contexte de groupe de périphériques pour les rendre spécifiques à un groupe de périphériques. Avant de définir les Règles avant et les Règles après sur Panorama, puis de les transmettre de Panorama vers les pare-feu gérés, vous pouvez les afficher sur les pare-feu gérés, mais vous pouvez modifier les Règles avant et les Règles après uniquement sur Panorama.

- **Règles amont** – Règles ajoutées au début de la liste des règles et évaluées en premier. Vous pouvez utiliser les pré-règles pour faire respecter la Politique d'utilisation acceptable d'une organisation. Par exemple, vous pouvez bloquer l'accès à des catégories d'URL spécifiques ou permettre du trafic DNS pour tous les utilisateurs.
- **Règles avale** – Les règles ajoutées en fin de liste des règles et évaluées après les règles avant et les règles définies localement sur le pare-feu. Les Règles avales comprennent généralement des règles visant à refuser l'accès au trafic sur la base de l'App-ID™, User-ID™ ou d'un Service.
- **Règles par défaut** – Les règles qui indiquent au pare-feu comment traiter le trafic qui ne correspond à aucune Règle avant, Règle après ou règles de pare-feu local. Ces règles font partie de la configuration prédéfinie de Panorama. Pour **Remplacer** et activer l'édition des paramètres sélectionnés dans ces règles, voir Remplacer ou annuler une règle de politique de sécurité.

Cliquez sur l'option **Prévisualiser les règles** pour afficher une liste de toutes les règles avant de les appliquer sur les pare-feu gérés. Dans chaque base de règles, la hiérarchie des règles est marquée visuellement pour chaque groupe de périphériques (et pare-feu géré), afin de faciliter l'analyse d'un grand nombre de règles.

Lorsque vous ajoutez une nouvelle règle, les données opérationnelles statiques de la règle s'affichent. La colonne universellement unique identifier (identifiant unique universel ; UUID) affiche l'UUID à 36 caractères pour la règle. Le pare-feu génère l'UUID par règle. Cependant, si vous transférez des règles de Panorama, ces règles possèdent le même UUID, qui s'affiche également dans la prévisualisation des règles combinées. La colonne **Créé** affiche l'heure et la date auxquelles la règle a été ajoutée à la base de règles. De plus, la colonne **Modifié** affiche l'heure et la date de la dernière modification de la règle. Si une règle de politique a été créée avant la mise à niveau vers PAN-OS 9.0, les premières données de **Première correspondance** sont utilisées pour établir la date de **Création**. Si aucune donnée de **Première correspondance** n'est disponible pour la règle, l'heure et la date de la mise à niveau du serveur de gestion de Panorama ou du pare-feu vers PAN-OS 9.0 sont utilisées pour établir la date de **Création**.

Lorsque vous ajoutez ou modifiez une règle dans Panorama, un onglet **Cible** s'affiche. Vous pouvez utiliser cet onglet pour appliquer la règle à des pare-feu spécifiques ou à des groupes de périphériques descendants du **Groupe de périphériques** (Ou emplacement partagé) où la règle est définie. Dans l'onglet **Cible**, vous pouvez sélectionner **Tout** (par défaut), ce qui signifie que la règle s'applique à tous les pare-feu et à tous les groupes de périphériques descendants. Pour cibler des pare-feu ou des groupes de périphériques spécifiques, décochez **Any (Tout)** et sélectionnez le nom des pare-feu ou des groupes de périphériques souhaités. Pour exclure des pare-feu spécifiques ou des groupes de périphériques, décochez **Tout,** sélectionnez le nom des pare-feu ou des groupes de périphériques souhaités, puis sélectionnez **Cibler tous les périphériques sauf ceux spécifiés**. Si la liste des groupes de périphériques et des pare-feu

est longue, vous pouvez appliquer des Filtres pour rechercher les saisies par attributs (telles que les Plates-formes) ou par chaîne de texte pour les noms correspondants.

Après que vous avez ajouté et appliqué une règle à Panorama, **Utilisation d'une règle** indique si la règle est Utilisée par tous les périphériques du groupe de périphériques, Partiellement utilisée par certains périphériques du groupes de périphériques ou Inutilisée par les périphériques du groupes de périphériques. Panorama détermine l'utilisation d'une règle en fonction des pare-feu gérés dont le Nombre de correspondance à la règle de politique est activé (activé par défaut). Dans le contexte de Panorama, vous pouvez afficher l'utilisation d'une règle pour une règle de politique partagée sur tous les groupes de périphériques. De plus, vous pouvez modifier le contexte afin de choisir un groupe de périphériques individuels et consulter l'utilisation totale d'une règle de politique sur l'ensemble des périphériques qui forment le groupe de périphériques. **Prévisualiser les règles** présentera le **Hit Count (Nombre de correspondances)**, la **Dernière correspondance** et la **Première correspondance** de chaque règle de politique d'un groupe de périphériques. Le nombre total de mise en correspondance du trafic ainsi les horodatages de la première et de la dernière correspondances perdurent après le redémarrage, la mise à niveau et le rédémarrage du panneau de données. Voir Surveiller l'utilisation d'une règle de politique.

Regroupez des règles par étiquette pour appliquer une étiquette qui vous permet de regrouper des règles de politique similaires pour obtenir une meilleure vision des fonctions des règles et faciliter la gestion des règles de politique à l'échelle de la base de règles. Les règles regroupées par étiquettes présentent la liste des groupes d'étiquettes, tout en préservant la liste de priorité des règles. Vous pouvez ajouter les règles à la fin d'un groupe d'étiquettes, déplacer des règles vers un autre groupe d'étiquettes, appliquer des étiquettes supplémentaires aux règles d'un groupe d'étiquettes et filtrer ou effectuer des recherches à l'aide du groupe d'étiquettes.

Pour suivre les changements apportés aux règles de politique, ajoutez un **Commentaire d'audit** pour décrire les changements que vous apportez et les raisons pour lesquelles une règle a été créée ou modifiée. Une fois le commentaire d'audit saisi et le changement de configuration validé, le commentaire d'audit est préservé dans le **Archive des commentaires d'audit**, où vous pouvez consulter tous les commentaires d'audit précédents pour la règle sélectionnée. Vous pouvez chercher le commentaire d'audit dans la recherche globale. L'archive des commentaires d'audit est en lecture seule.

Les utilisateurs administratifs qui ont accès à l'onglet Politiques peuvent exporter les règles de politique qui sont affichées sur l'interface Web au format **PDF/CSV**. Consultez la section Exportation des données du tableau de configuration.

Pour créer des politiques, reportez-vous à la section correspondante à chaque base de règles:

- Politiques > Sécurité
- Politiques > NAT
- Politiques > QoS
- Politiques > Transfert basé sur une politique
- Politiques > Déchiffrement
- Politiques >Broker de paquets de réseau
- Politiques > Inspection des tunnels
- Politiques > Contrôle prioritaire sur l'application
- Politiques > Authentification
- Politiques > Protection DoS
- Politiques > SD-WAN

Partitions de stockage des journaux pour un appareil virtuel Panorama en Mode hérité

- Panorama > Configuration > Opérations

Par défaut, un appareil virtuel Panorama en mode Hérité comporte une partition de disque unique pour toutes les données et 10,89 Go de cet espace est affecté au stockage de journaux. Accroître la taille du disque n'augmente pas la capacité de stockage des journaux ; cependant, vous pouvez modifier la capacité de stockage des journaux grâce aux options suivantes :

- **Système de fichiers réseau (NFS)** – l'option de montage du stockage NFS n'est disponible que pour les appareils virtuels Panorama en mode héritage et fonctionnant sur un serveur VMware ESXi. Pour monter le stockage NFS, sélectionnez **Storage Partition Setup (Paramétrage de la partition de stockage)** dans la section Divers, définissez la **Storage Partition (Partition de stockage)** sur **NFS V3** et configurez les paramètres comme décrit dans le Tableau : Paramètres de stockage NFS.
- **Stockage interne par défaut** – rétablissez la partition de stockage interne par défaut (applicable uniquement à Panorama sur un serveur ESXi ou sur la plateforme vCloud Air où vous avez précédemment configuré un autre disque de journaux virtuel ou monté sur un NFS). Pour revenir à la partition de stockage interne par défaut, sélectionnez **Configuration de la partition de stockage** dans la section Divers et définissez la **Partition de stockage** sur **Interne**.
- **Disque de journal virtuel** – vous pouvez Ajouter un autre disque virtuel (jusqu'à 8 To) pour Panorama fonctionnant sous VMware ESXi (versions 5.5 et ultérieures) ou pour Panorama fonctionnant sous la plateforme VMware vCloud Air. Par conséquent, Panorama cesse d'utiliser le stockage de journaux de 10,89 Go par défaut sur le disque d'origine et copie tous les journaux existants sur le nouveau disque. (Les versions ESXi antérieures prennent uniquement en charge les disques virtuels de 2 To maximum).

*Vous devez redémarrer Panorama après avoir modifié les paramètres de la partition de stockage : sélectionnez **Panorama** > **Setup (Configuration)** > **Operations (Opérations)** et **Reboot Panorama (Redémarrer Panorama)**.*

Le stockage NFS n'est pas disponible pour l'appareil virtuel Panorama en mode Panorama ou pour les appareils M-Series.

Table 1: Tableau : Paramètres de stockage NFS

Paramètres de partition de stockage Panorama – NFS V3	Description
Serveur	Indiquez le nom de domaine complet ou l'adresse IP du serveur NFS.
Répertoire des journaux	Précisez le chemin d'accès complet du répertoire dans lequel les journaux seront stockés.
Protocole	Précisez le protocole (UDP ou TCP) de communication avec le serveur NFS.

Paramètres de partition de stockage Panorama – NFS V3	Description
Port	Précisez le port de communication avec le serveur NFS.
Taille de lecture	Précisez la taille maximum en octets (intervalle compris entre 256 et 32 768) des opérations de lecture NFS.
Taille d’écriture	Précisez la taille maximum en octets (intervalle compris entre 256 et 32 768) des opérations d’écriture NFS.
Copier lors de la configuration	Sélectionnez pour monter la partition NFS et pour copier les journaux existants dans le répertoire de destination sur le serveur au démarrage de Panorama.
Partition de journalisation test	Sélectionnez pour tester le montage de la partition NFS et afficher un message de réussite ou d’échec.

Panorama > Configuration > Interfaces

- Panorama > Configuration > Interfaces

Sélectionnez **Panorama** > **Setup (Configuration)** > **Interfaces** pour configurer les interfaces que Panorama utilise pour gérer les pare-feu et les Collecteurs de journaux, déployer des logiciels et des mises à jour de contenu sur les pare-feu et les Collecteurs de journaux, collecter les journaux des pare-feu et communiquer avec les Groupes de collecteurs. Par défaut, Panorama utilise l'interface de gestion MGT pour toutes les communications avec les pare-feu et les Collecteurs de journaux.

*Pour réduire le trafic sur l'interface MGT, configurez d'autres interfaces pour qu'elles déploient des mises à jour, collectent des journaux et communiquent avec les Groupes de collecteurs. Dans un environnement avec un trafic de journaux important, vous pouvez configurer plusieurs interfaces pour la collecte des journaux. De plus, pour améliorer la sécurité du trafic de gestion, vous pouvez définir un sous-réseau distinct (**Masque réseau** IPv4 ou **Longueur de préfixe** IPv6) pour l'interface MGT, qui est plus privé que les sous-réseaux pour les autres interfaces.*

Interface	Vitesse maximun	Appareil M-700	Appareil M-600	Appareil M-500	Appareil M-300	Appareil M-200	Appareil virtuel Panorama
Management (MGT)	1 Gbits/s	✓	✓	✓	✓	✓	✓
Ethernet1 (Eth1)	1 Gbits/s	✓	✓	✓	✓	✓	✓
Ethernet2 (Eth2)	1 Gbits/s	—	✓	✓	—	✓	✓
Ethernet3 (Eth3)	1 Gbits/s	—	✓	✓	—	✓	✓
Ethernet4 (Eth4)	10 Gbits/s	—	✓	✓	—	—	✓
Ethernet5 (Eth5)	10 Gbits/s	—	✓	✓	—	—	✓

Passez en revue les taux de journalisation de tous les modèles d'appareils de série M. Pour atteindre les taux de journalisation indiqués ci-dessous, l'appareil M-Series doit être un collecteur de journaux unique dans un groupe de collecteurs et vous devez installer tous les disques de journalisation pour votre modèle M-Series. À titre d'exemple, pour atteindre 30 000 journaux/seconde pour l'appareil M-500, vous devez installer les 12 disques de journalisation avec des disques de 1 To ou de 2 To.

Capacités et fonctionnalités du modèle	Appareil M-700	Appareil M-600	Appareil M-500	Appareil M-300	Appareil M-200
Taux de journalisation maximum pour Panorama en mode Gestion uniquement	Le stockage des journaux locaux n'est pas pris en charge				
Taux de journalisation maximal pour Panorama en mode Panorama	36 500 journaux / seconde	25 000 journaux / seconde	20.000 journaux / seconde	16 500 journaux / seconde	10 000 journaux / seconde
Taux de journalisation maximal pour Panorama en mode Collecteur de journaux	73 000 journaux / seconde	50 000 journaux / seconde	30 000 journaux / seconde	33 000 journaux / seconde	28 000 journaux / seconde
Stockage maximum de journaux sur le modèle	48 To (12 disques RAID de 8 To)	48 To (12 disques RAID de 8 To)	• 24 To (24 disques RAID de 2 To) • 12 To (24 disques RAID de 1 To)	16 To (4 disques RAID de 8 To)	16 To (4 disques RAID de 8 To)
Stockage par défaut de journaux sur le modèle	16 To (4 disques RAID de 8 To)	16 To (4 disques RAID de 8 To)	4 To (4 disques RAID de 2 To)	16 To (4 disques RAID de 8 To)	16 To (4 disques RAID de 8 To)
Stockage SSD sur le modèle (pour les journaux que les appareils de série M génèrent)	240 Go	240 Go	240 Go	240 Go	240 Go
Stockage de journaux attaché NFS	Non disponible				

Pour configurer une interface, cliquez sur le Nom de l'interface et configurez les paramètres décrits dans le tableau suivant.

Spécifiez toujours l'adresse IP, le masque réseau (pour IPv4) ou la longueur de préfixe (pour IPv6) ainsi que la passerelle par défaut pour l'interface MGT. Si vous omettez des valeurs pour certains paramètres (comme la passerelle par défaut), vous pouvez uniquement accéder à Panorama via le port de la console pour des modifications ultérieures de la configuration. Vous ne pouvez pas valider les configurations pour d'autres interfaces, sauf si vous spécifiez les trois paramètres. Cette exigence ne s'applique pas à un dispositif virtuel Panorama sur les supported cloud hypervisors (hyperviseurs compatibles avec le cloud)*, car seul DHCP prend en charge les interfaces.*

Paramètres de l'interface	Description
Eth1 / Eth2 / Eth3 / Eth4 / Eth5	Vous devez activer une interface pour la configurer. L'interface de gestion est une exception car elle est activée par défaut.
Adresse'A0;IP (IPv4)	Si votre réseau utilise des adresses IPv4, affectez une adresse IPv4 à l'interface.
Masque réseau (IPv4)	Si vous avez affecté une adresse IPv4 à l'interface, vous devez également saisir un masque réseau (par exemple, 255.255.255.0).
Passerelle par défaut (IPv4)	Si vous avez affecté une adresse IPv4 à l'interface, vous devez également affecter une adresse IPv4 à la passerelle par défaut (elle doit se trouver sur le même sous-réseau que l'interface).
Longueur du préfixe / de l'adresse IPv6	Si votre réseau utilise des adresses IPv6, affectez une adresse IPv6 à l'interface. Pour indiquer le masque réseau, saisissez une longueur de préfixe IPv6 (par exemple, 2001:400:f00::1/64). *Une adresse IPv6 est prise en charge pour l'interface MGT par tous les appareils M-Series et les appareils virtuels Panorama déployés dans un environnement de cloud privé (ESXi, vCloud Air, KVM, ou Hyper-V). Une adresse IPv6 n'est pas prise en charge pour l'interface MGT par un appareil virtuel Panorama déployé dans un environnement de cloud public (Amazon Web Services (AWS), AWS GovCloud, Microsoft Azure, ou Google Cloud Platform).*
Passerelle IPv6 par défaut	Si vous avez affecté une adresse IPv6 à l'interface, vous devez également affecter une adresse IPv6 à la passerelle par défaut (elle doit se trouver sur le même sous-réseau que l'interface).

Paramètres de l'interface	Description
	Une adresse IPv6 est prise en charge pour l'interface MGT par tous les appareils M-Series et les appareils virtuels Panorama déployés dans un environnement de cloud privé (ESXi, vCloud Air, KVM, ou Hyper-V). Une adresse IPv6 n'est pas prise en charge pour l'interface MGT par un appareil virtuel Panorama déployé dans un environnement de cloud public (Amazon Web Services (AWS), AWS GovCloud, Microsoft Azure, ou Google Cloud Platform).
Vitesse	Réglez la vitesse pour l'interface à 10 Mbit/s, 100 Mbit/s, 1 Gbit/s ou 10 Gbit/s (Eth4 et Eth5 uniquement) en duplex intégral ou semi-duplex. Utilisez le paramètre de négociation automatique par défaut pour que Panorama détermine la vitesse de l'interface. *Ce paramètre doit correspondre aux paramètres de l'interface de l'équipement réseau voisin. Pour assurer les paramètres de mappage, sélectionnez la négociation automatique si l'équipement voisin prend en charge cette option.*
MTU	Saisissez l'unité de transmission maximale (MTU) en octets par paquet envoyé sur cette interface (plage de 576 à 1 500 ; par défaut 1 500).
Gestion des périphériques et collecte des journaux de périphérique	Activez l'interface (activée par défaut sur l'interface MGT) pour gérer les pare-feu et les Collecteurs de journaux et collecter leurs journaux. Vous pouvez activer plusieurs interfaces pour effectuer ces fonctions.
Communication avec les groupes de collecteurs	Activez l'interface pour la communication de Groupe de collecteurs (l'interface par défaut est l'interface MGT). Seule une interface peut effectuer cette fonction.
Transfert Syslog	Activez l'interface pour le transfert de syslogs (l'interface par défaut est l'interface MGT). Seule une interface peut effectuer cette fonction.
Déploiement de périphériques	Activez l'interface pour le déploiement de logiciels et de mises à jour de contenu sur les pare-feu et les Collecteurs de journaux (l'interface par défaut est l'interface MGT). Seule une interface peut effectuer cette fonction.
Services de gestion administrative	• **HTTP** - Autorise l'accès à l'interface Web de Panorama. HTTP utilise du texte en clair, ce qui n'est pas aussi sécuritaire que le protocole HTTPS. *Activez le protocole **HTTPS** plutôt que le protocole HTTP pour le trafic de gestion sur l'interface.*

Paramètres de l'interface	Description
	• **Telnet** - Autorise l’accès à l’ILC (interface de ligne de commande) de Panorama. Telnet utilise du texte en clair, ce qui n'est pas aussi sécuritaire que le protocole SSH. • **HTTPS** - Autorise l’accès sécurisé à l’interface Web de Panorama.  *Activez le protocole **SSH** plutôt que le protocole de Telnet pour le trafic de gestion sur l’interface.* • **SSH** – Permet un accès sécurisé à l’interface de ligne de commande Panorama.
Services de connexion réseau	Le service **Ping** est disponible sur n’importe quelle interface. Vous pouvez utiliser le ping pour tester la connectivité entre l’interface Panorama et les services externes. Dans un déploiement haute disponibilité (HD), les pairs HA utilisent l'envoi de ping pour échanger de l'information sur la sauvegarde de pulsation. Les services suivants sont uniquement disponibles sur l’interface MGT : • **SNMP** - Permet à Panorama de traiter les requêtes de statistiques d’un gestionnaire SNMP. Pour plus de détails, voir Activation de la surveillance SNMP. • **User-ID** – Permet à Panorama de redistribuer les informations de mappage d’utilisateur reçues des agents User-ID.
Adresses IP autorisées	Saisissez les adresses IP à partir desquelles les administrateurs peuvent accéder à Panorama sur cette interface. Une liste vide (par défaut) indique que l’accès est possible à partir de n’importe quelle adresse IP.  *Ne laissez pas cette liste vide. Spécifiez les adresses IP des administrateurs Panorama (uniquement) pour empêcher tout accès non autorisé.*

Panorama > Haute disponibilité

Pour autoriser la haute disponibilité (HD) sur Panorama, configurez les paramètres comme décrits dans le tableau suivant.

Paramètres HA de Panorama	Description
setup Cliquez sur Modifier () pour configurer les paramètres suivants.	
Activer la HA	Sélectionnez cette action pour activer HA.
Adresse IP des HA homologues	Saisissez l’adresse IP de l’interface MGT de l'homologue.
Activer le chiffrement	Lorsque le chiffrement est activé, l'interface MGT crypte la communication entre les homologues HA. Avant d’activer le chiffrement, exportez la clé HA de chacun des homologues HA et importez-la vers l’autre homologue. Vous importez et exportez la clé HD sur la page **Panorama** > **Certificate Management (Gestion de certificats)** > **Certificates (Certificats)** (voir Gestion des certificats du pare-feu et de Panorama). *La connectivité HA utilise le port TCP 28 avec le chiffrement activé et le port TCP 28769 lorsque le chiffrement n’est pas activé.*
Temps d'attente pour la surveillance (ms)	Saisissez le nombre de millisecondes d’attente du système avant d’intervenir à la suite d’un échec de la liaison de contrôle (plage de 1 000 à 60 000 ; valeur par défaut de 3 000).
Paramètres de sélection Cliquez sur Modifier () pour configurer les paramètres suivants.	
Priorité (Obligatoire sur l’équipement virtuel Panorama)	Ce paramètre détermine l'homologue principal pour la réception des journaux du pare-feu. Désignez un homologue **Primary (Principal)** et un homologue **Secondary (Secondaire)** dans la paire HA. Lorsque vous configurez les Partitions de stockage des journaux pour un appareil virtuel Panorama en Mode hérité, vous pouvez utiliser son disque interne (par défaut) ou un système de fichiers réseau (NFS) pour le stockage des journaux. Si vous configurez un NFS, seul le destinataire principal reçoit

Paramètres HA de Panorama	Description
	les journaux du pare-feu. Si vous configurez la mémoire interne du disque, les pare-feu envoient par défaut des journaux à l'homologue primaire et secondaire, mais vous pouvez le modifier en activant **Only Active Primary Logs to Local Disk (Seulement les journaux actifs principaux sur le disque local)** dans les Paramètres de journalisation et de génération de rapports.
Préemptif	Sélectionnez cette option pour permettre à l'homologue Panorama principal de reprendre l'état actif après la récupération d'un échec. Si ce paramètre est désactivé, l'homologue Panorama secondaire reste actif même si l'homologue Panorama principal récupère d'un échec.
Paramètres du minuteur de haute disponibilité	Votre sélection détermine les valeurs des paramètres de sélection HA restants, qui contrôlent la vitesse de basculement : • **Recommended (Recommandé)** - Sélectionnez cette option pour les paramètres types du minuteur de basculement (par défaut). Pour visualiser les valeurs associées, sélectionnez **Advanced (Avancé)** et **Load Recommended (Charger le profil recommandé)**. • **Aggressive (Agressif)** - Sélectionnez cette option pour des paramètres plus rapides du minuteur de basculement. Pour visualiser les valeurs associées, sélectionnez **Advanced (Avancé)** et **Load Aggressive (Charger le profil agressif)**. • **Advanced (Avancé)** - Sélectionnez cette option pour afficher les paramètres de sélection HA restants et personnaliser leurs valeurs. Voir la valeur **recommandée** et **agressive** pour les paramètres suivants.
Délai de maintien de promotion (ms)	Saisissez le nombre de millisecondes (plage de 0 à 60 000) pendant lesquelles l'homologue Panorama secondaire attendra avant de prendre le relais après l'arrêt de l'homologue principal. La valeur recommandée (par défaut) est 2 000 ; la valeur du profil agressif est 500.
Intervalle Hello (ms)	Saisissez le nombre de millisecondes (plage de 8 000 to 60 000) entre chaque paquet Hello envoyé afin de vérifier que l'autre homologue est opérationnel. La valeur recommandée (par défaut) et la valeur du profil agressif est 8 000.
Intervalle de pulsation (ms)	Précisez la fréquence en millisecondes (plage de 1 000 to 60 000) à laquelle Panorama envoie des pings ICMP à l'homologue HA. La valeur recommandée (par défaut) est 2 000 ; la valeur du profil agressif est de 1 000.
Délai de maintien de préemption (min)	Ce champ s'applique uniquement si vous sélectionnez également l'option **Preemptive (Préemptif)**. Saisissez le nombre de minutes (plage de 1 à 60) pendant lesquelles l'homologue Panorama passif attendra avant de revenir à l'état actif après avoir récupéré d'un événement ayant entraîné

Paramètres HA de Panorama	Description
	un basculement. La valeur recommandée (par défaut) et la valeur du profil agressif est de 1.
Temps d'attente actif après l'échec de la surveillance (ms)	Précisez le nombre de millisecondes (plage de 0 à 60 000) pendant lesquelles Panorama attendra avant d'essayer de passer de nouveau à l'état passif après l'échec de surveillance du chemin. Pendant cette période, l'homologue passif ne peut pas prendre l'état actif en cas d'échec. Cet intervalle permet à Panorama d'empêcher un basculement dû au battement occasionnel de périphériques à proximité. La valeur recommandée (par défaut) et la valeur du profil agressif est de 0.
Temps d'attente actif principal supplémentaire (ms)	Précisez le nombre de millisecondes (plage de 0 à 60 000) pendant que lesquelles l'homologue de préemption reste à l'état passif avant de devenir l'homologue actif. La valeur recommandée (par défaut) est de 7 000 ; la valeur du profil agressif est de 5 000.
Surveillance des chemins Cliquez sur Modifier () pour configurer la Surveillance des chemins HA.	
Activé	Sélectionnez cette option pour activer la surveillance des chemins. La surveillance des chemins permet à Panorama de surveiller les adresses IP de destination définies en envoyant des messages ping ICMP afin de vérifier qu'elles répondent.
Condition d'échec	Sélectionnez cette option en cas d'échec lorsqu'**Any (Un)** ou **All (Tous)** les groupes de chemins surveillés ne répondent pas.
Groupe de chemins Pour créer un groupe de chemins pour la surveillance de chemins HA, cliquez sur **Add (Ajouter)** et remplissez les champs suivants.	
Name (Nom)	Donnez un nom au groupe de chemins.
Activé	Sélectionnez cette option pour activer le groupe de chemins.
Condition d'échec	Sélectionnez cette option en cas d'échec lorsqu'**Any (Une)** ou **All (Toutes)** les adresses de destination précisées ne répondent pas.
Intervalle des requêtes ping	Précisez le nombre de millisecondes entre les messages echo ICMP qui vérifient que le chemin vers l'adresse de destination est disponible (plage de 1 000 à 60 000 ; valeur par défaut de 5 000).

Paramètres HA de Panorama	Description
Nombre de requêtes ping	Précisez le nombre d’échecs de requêtes ping avant de déclarer un échec (plage de 3 à 10 ; valeur par défaut de 3).
Adresses IP de destination	Saisissiez une ou plusieurs adresses IP de destination à surveiller. Utilisez un point-virgule pour séparer plusieurs adresses.

Panorama > Clusters WildFire gérés

- Panorama > Clusters WildFire gérés
- Panorama > Appareils WildFire gérés

Vous pouvez gérer les appareils WildFire en clusters ou en tant qu'appareils autonomes, et ce depuis des appareils Panorama virtuels ou de série M. La gestion des clusters (**Panorama** > **Clusters WildFire gérés**) et la gestion des appareils autonomes (**Panorama** > **Appareils WildFire gérés**) ont en commun de nombreuses tâches administratives et de configuration courantes. Ainsi, ces deux gestions figurent dans les rubriques qui suivent.

Après avoir ajouté les appareils WildFire à Panorama, utilisez l'interface Web pour ajouter ces appareils et les gérer en tant que clusters ou pour les gérer en tant qu'appareils autonomes.

- Tâches des clusters WildFire gérés
- Tâches de l'appareil WildFire géré
- Informations WildFire gérées
- Cluster WildFire géré et administration de l'appareil

Tâches des clusters WildFire gérés

Vous pouvez créer et supprimer des clusters d'appareils WildFire à partir de Panorama. Vous pouvez également gagner du temps lors de la configuration en important des configurations d'un cluster à l'autre.

Tâche	Description
Créer un cluster	Si nécessaire, **Créez un cluster**, saisissez un nom pour le nouveau cluster, puis cliquez sur **OK**. Les clusters existants que vous avez configurés localement et ajoutés à Panorama en ajoutant les nœuds d'appareils WildFire individuels sont répertoriés avec leurs nœuds WildFire et les rôles des nœuds (**Panorama** > **Managed WildFire Appliances (Appareils WildFire gérés)**). Le nom du cluster doit être un nom de sous-domaine valide commençant par un caractère ou un chiffre minuscule. Ce nom ne peut contenir des traits d'union que s'ils ne correspondent pas au premier ou au dernier caractère du nom du cluster. Aucun espace ou autre caractère n'est autorisé. La longueur maximale d'un nom de cluster est de 63 caractères. Après avoir créé un cluster, vous pouvez ajouter des appareils WildFire gérés au cluster et les gérer sur Panorama. Lorsque vous ajoutez un appareil WildFire à Panorama, vous enregistrez automatiquement l'appareil avec Panorama. Vous pouvez créer un maximum de 10 clusters WildFire gérés sur Panorama ; chaque cluster peut contenir jusqu'à 20 nœuds d'appareils WildFire. Panorama peut gérer jusqu'à un total cumulatif de 200 appareils autonomes et nœuds de cluster.

Tâche	Description
Importer la config. du cluster	**Importer la Configuration du cluster** pour importer une configuration de cluster existante. Si vous sélectionnez un cluster avant d'**Importer la Configuration du cluster,** les informations appropriées pour le cluster sélectionné sont automatiquement renseignées dans le **Contrôleur** et le **Cluster**. Si vous ne sélectionnez pas un cluster avant d'**Importer la Configuration du cluster**, vous devez sélectionner le **Contrôleur** et le **Cluster** se complète automatiquement en fonction du nœud de Contrôleur que vous sélectionnez. Après avoir importé la configuration, **Validez sur Panorama** pour sauvegarder la configuration candidate importée dans la configuration d'exécution Panorama.
Supprimer de Panorama	Si vous n'avez plus besoin de gérer un cluster WildFire à partir de Panorama, cliquez sur **Supprimer de Panorama** et sélectionnez **Oui** pour confirmer votre action. Après avoir supprimé un cluster de la gestion de Panorama, vous pouvez gérer le cluster localement à partir d'un nœud de Contrôleur. Vous pouvez à tout moment rajouter le cluster dans l'appareil Panorama si vous souhaitez à nouveau gérer le cluster au niveau central plutôt que local.
Crypter les communications entre appareils au sein du cluster WildFire	Pour chiffrer la communication de données entre les appareils WildFire d'un cluster, **activez** le chiffrement sous **Secure Cluster Communication**. WildFire utilise un certificat prédéfini ou un certificat personnalisé pour communiquer entre les appareils. Les certificats personnalisés ne sont utilisés que lorsque vous **personnalisez la communication** serveur sécurisée et activez **le certificat personnalisé uniquement**. Le chiffrement est requis pour que les clusters WildFire fonctionnent en mode FIPS-CC. Les certificats personnalisés utilisés en mode FIPS-CC doivent répondre aux exigences FIPS-CC. Après avoir activé la communication sécurisée du cluster, vous pouvez ajouter des appareils WildFire gérées supplémentaires au cluster. Les appareils nouvellement ajoutés utilisent les paramètres de la communication sécurisée avec le cluster.

Tâches de l'appareil WildFire géré

Vous pouvez ajouter, supprimer et gérer des appareils WildFire autonomes sur un périphérique Panorama. Après avoir ajouté des appareils autonomes, vous pouvez les ajouter aux clusters d'appareils WildFire en tant que nœuds cluster ou vous pouvez les gérer en tant que périphériques autonomes individuels.

Tâche	Description
Ajouter un appareil	**Ajoutez un appareil** pour ajouter un ou plusieurs appareils WildFire à un appareil Panorama pour une gestion centralisée. Saisissez le numéro de série de chaque appareil WildFire sur une ligne séparée (nouvelle ligne).

Tâche	Description
	Panorama peut gérer jusqu'à un total cumulatif de 200 nœuds cluster WildFire et d'appareils WildFire autonomes. Sur chaque appareil WildFire que vous souhaitez gérer sur Panorama, configurez l'adresse IP ou FQDN de l'appareil Panorama (serveur Panorama) et, le cas échéant, le serveur Panorama de sauvegarde en utilisant les commandes suivantes de la CLI de l'appareil WildFire : **définir deviceconfig system panorama-server *<ip-address | FQDN>*** **définir deviceconfig system panorama-server-2 *<ip-address | FQDN>***
Importer la configuration	Sélectionnez un appareil WildFire et une **Configuration d'importation** pour importer (uniquement) vers Panorama la configuration en cours d'exécution pour cet appareil. Après avoir importé la configuration, **Validez sur Panorama** pour sauvegarder la configuration candidate importée dans la configuration d'exécution Panorama.
Supprimer	Si vous n'avez plus besoin de gérer un appareil WildFire à partir de Panorama, **Retirez** l'appareil et sélectionnez **Oui** pour confirmer votre action. Après avoir supprimé un appareil de la gestion de Panorama, vous pouvez gérer l'appareil localement à l'aide de sa CLI. Si nécessaire, vous pouvez rajouter l'appareil à tout moment à l'appareil Panorama si vous souhaitez gérer à nouveau l'appareil au niveau central plutôt que local.

Informations WildFire gérées

Sélectionnez **Panorama** > **Managed WildFire Clusters (Clusters WildFire gérés)** pour afficher les informations suivantes pour chaque cluster géré (vous pouvez également sélectionner des appareils autonomes à partir de cette page et afficher les informations s'y rapportant) ou sélectionnez **Panorama** > **Managed WildFire Appliances (Appareils WildFire gérés)** pour afficher les informations pour les appareils autonomes.

Sauf indication contraire, les informations reprises dans le tableau suivant s'appliquent tant aux clusters WildFire qu'aux appareils autonomes. Les informations précédemment configurées pour un cluster ou un appareil sont pré-renseignées.

Informations WildFire gérées	Description
Appareil	Le nom de l'appareil. L'affichage Clusters WildFire gérés indique les appareils regroupés par cluster, inclut les appareils autonomes qu'il est possible d'ajouter à un cluster

Informations WildFire gérées	Description
	et mentionne le numéro de série (entre parenthèses) avec le nom de l'appareil (le numéro de série ne fait pas partie du nom).
Numéro de série (affichage des appareils WildFire gérés uniquement)	Le numéro de série de l'appareil. L'affichage Clusters WildFire gérés indique le numéro de série dans la même colonne que le nom de l'appareil (le numéro de série ne fait pas partie du nom).
Version du logiciel	La version du logiciel installée et en cours d'exécution sur l'appareil.
Adresse IP	L'adresse IP de l'appareil.
Connected (Connecté)	Le statut de la connexion entre l'appareil et Panorama ; soit Connecté soit Déconnecté.
Nom du cluster	Le nom du cluster dans lequel l'appareil est inclus comme nœud ; dans le cas d'un appareil autonome, rien ne s'affiche.
Environnement d'analyse	L'environnement d'analyse (vm-1, vm-2, vm-3, vm-4 ou vm-5). Chaque environnement d'analyse représente un ensemble de systèmes d'exploitation et d'applications : • vm-1 prend en charge Windows XP, Adobe Reader 9.3.3, Flash 9, PE, PDF, Office 2003 et les versions antérieures d'Office ; • vm-2 prend en charge Windows XP, Adobe Reader 9.4.0, Flash 10n, PE, PDF, Office 2007 et les versions antérieures d'Office ; • vm-3 prend en charge Windows XP, Adobe Reader 11, Flash 11, PE, PDF, Office 2010 et les versions antérieures d'Office ; • vm-4 prend en charge Windows 7 32 bits, Adobe Reader 11, Flash 11, PE, PDF, Office 2010 et les versions antérieures d'Office. • vm-5 prend en charge Windows 7 64 bits, Adobe Reader 11, Flash 11, PE, PDF, Office 2010 et les versions antérieures d'Office.
Contenu	Le numéro de version de la version du contenu.
Rôle	Le rôle de l'appareil : • **Autonome** – L'appareil n'est pas un nœud de cluster. • **Contrôleur** – L'appareil est le nœud de Contrôleur du cluster. • **Sauvegarde Contrôleur du </** – L'appareil est le nœud de secours du Contrôleur du cluster. • **Subordonné** – L'appareil est un nœud dans le cluster.

Informations WildFire gérées	Description
État de config.	Le statut de la synchronisation de la configuration de l'appareil. L'appareil Panorama vérifie les paramètres de l'appareil WildFire et signale les différences de configuration entre la configuration de l'appareil et celle enregistrée sur Panorama pour cet appareil. • **Synchronisé** – La configuration de l'appareil est synchronisée avec sa configuration enregistrée sur Panorama. • **Désynchronisés** – La configuration de l'appareil n'est pas synchronisée avec sa configuration enregistrée sur Panorama. Vous pouvez placer votre souris sur la loupe pour afficher la cause de l'échec de la synchronisation.
État du cluster (page clusters WildFire gérés uniquement)	Le Statut du cluster affiche trois types d'informations pour chaque nœud de cluster : • services disponibles (conditions de fonctionnement normales) : • **wfpc** (WildFire Private Cloud) – Le service d'analyse et de rapportage d'échantillons de logiciels malveillants, • **signature** – Le service de génération de signature locale. • progression des opérations – Le nom de l'opération suivi de deux points (:) et du statut : • **opérations** – Statut de la désactivation, de la suspension et du redémarrage des opérations, • **statut de la progression** – Les notifications du statut de l'opération sont identiques pour chaque opération : demandée, en cours, refusée, réussie ou échouée. Par exemple, si vous suspendez un nœud et que l'opération est en cours, le Statut du cluster affichera `Suspension : en cours` ou, si vous redémarrez un nœud et que l'opération a été demandée, mais qu'elle n'a pas encore commencé, le Statut du cluster affichera `Redémarrage : demandé`. • conditions d'erreur : Le Statut du cluster affiche les conditions d'erreur suivantes : • **cluster** – `cluster : hors ligne` ou `cluster : split-brain`, • **service** – `service : suspendu` ou `service : aucun`.
État de la dernière validation	`Réussite de la validation` si la dernière validation a réussi ou `Échec de la validation` si la validation la plus récente a échoué. Visualisez les détails de la dernière validation en sélectionnant le statut.
Utilisation > Visualisation	

Informations WildFire gérées	Description
Vue	**Visionnez** les statistiques d'utilisation des clusters ou des appareils. Vous pouvez visualiser les appareils individuels uniquement (**Panorama** > **Managed WildFire Appliances (Appareils WildFire gérés)**) ou vous pouvez visualiser les statistiques du cluster uniquement (**Panorama** > **Managed WildFire Clusters (Clusters WildFire gérés)**). • **Appareil** – (affichage Appareil autonome uniquement) Le numéro de série de l'appareil. • **Cluster** – (affichage Cluster uniquement) Le nom du cluster. Vous pouvez également sélectionner un autre cluster à afficher. • **Durée** – Affiche la période pendant laquelle les statistiques sont recueillies et affichées. Vous pouvez sélectionner différentes durées: • **15 Min** • **Dernière heure** • **Dernière 24 heures (par défaut)** • **7 derniers jours** • **Tous** La **vue Utilisation** comporte quatre onglets et, sur chaque onglet, vous déterminez ce qui s'affiche en fonction de votre durée **configurée** .
Onglet Général	L'onglet **Général** affiche les statistiques d'utilisation des ressources agrégées pour un cluster ou un appareil. Les autres onglets affichent des informations plus granulaires concernant l'utilisation des ressources par type de fichier : • **Utilisation totale du disque** – L'utilisation totale du disque du cluster ou de l'appareil. • **Verdict** – Le nombre **Total** de verdicts, le nombre de verdicts de chaque type attribués aux fichiers (**Malveillant**, **Grayware** et **Bénin**) et combien de verdicts étaient des verdicts d'**Erreur**. • **Statistiques des échantillons** – Le nombre total d'échantillons **Soumis** et **Analysés** ainsi que le nombre d'échantillons **En attente** d'analyse. • **Analysis Environment & System Utilization (Environnement d'analyse et utilisation du système)** : • **Type de fichier analysé** – Le type de fichier qui a été analysé : **Exécutable**, **Non exécutable** ou **Liens**. • **Utilisation des machines virtuelles** – Le nombre de machines virtuelles utilisées pour chaque type de fichier analysé et le nombre de machines virtuelles disponibles pour analyser chaque type de fichier. Par exemple, pour les fichiers Exécutables, l'utilisation des machines virtuelles pourrait être de 6/10 (six machines virtuelles utilisées et dix disponibles).

Informations WildFire gérées	Description
	• **Fichiers analysés** – Le nombre de fichiers de chaque type qui ont été analysés.
Onglets Exécutables, Non exécutables et Liens	Les onglets **Executable (Exécutable)**, **Non-Executable (Non exécutable)** et **Links (Liens)** affichent des informations similaires à propos de chaque type de fichier : • **verdict** – Détails sur les verdicts par type de fichier. Vous pouvez filtrer les résultats : • **Barre de recherche** – Saisissez des termes de recherche pour filtrer les verdicts. La barre de recherche indique le nombre de types de fichiers (éléments) dans la liste. Après avoir saisi les termes de recherche, appliquez le filtre (→) ou effacez le filtre (×) et saisissez une autre suite de termes. • **Type de fichier** – Liste des fichiers par type. Par exemple, l'onglet **Exécutable** affiche les fichiers de type .exe et .dll ; l'onglet **Non exécutable** affiche les fichiers de type .pdf, .jar, .doc, .ppt, .xls, .docx, .pptx, .xlsx, .rtf, class et .swf; et l'onglet **Liens** affiche les informations des fichiers de type elink. • Le nombre total de verdicts pour les fichiers **Malveillants**, **Grayware** et **Bénins**, le nombre de verdicts d'**Erreur** et le nombre **Total** de verdicts sont affichés sous chaque onglet pour chaque **Type de fichier**. • **Statistiques des échantillons** – Détails à propos de l'analyse des échantillons par type de fichier. • **Barre de recherche** – Même chose que la barre de recherche pour les **Verdicts**. • **Type de fichier** – Même chose que le **Type de fichier** pour les **Verdicts**. • Le nombre total de fichiers **Soumis** pour analyse, le nombre total de fichiers **Analysés** et le nombre de fichiers **En attente** d'analyse sont affichés sous chaque onglet pour chaque **Type de fichier**.
Pare-feu connectés > Affichage	
Vue	**Affiche** des informations concernant les pare-feu connectés au cluster ou à l'appareil. Vous pouvez visualiser les appareils individuels uniquement (**Panorama** > **Managed WildFire Appliances (Appareils WildFire gérés)**) ou vous pouvez visualiser les statistiques du cluster uniquement (**Panorama** > **Managed WildFire Clusters (Clusters WildFire gérés)**).

Informations WildFire gérées	Description
	• **Appareil** – (affichage Appareil autonome uniquement) Le numéro de série de l'appareil. • **Cluster** – (affichage Cluster uniquement) Le nom du cluster ; vous pouvez également sélectionner un autre cluster à afficher. • **Actualiser** – Actualiser l'affichage.
Onglets Échantillons Enregistrés et En cours de soumission	L'onglet **Enregistrés** affiche des informations à propos des pare-feu enregistrés dans le cluster ou l'appareil, que les pare-feu soient en train de soumettre des échantillons ou non. L'onglet **Échantillons en cours de soumission** affiche des informations à propos des pare-feu qui soumettent activement des échantillons au cluster ou à l'appareil WildFire. Le type d'informations affichées sur ces onglets et la manière de filtrer ces informations sont identiques pour ces deux onglets : • **Barre de recherche** – Saisissez des termes de recherche pour filtrer la liste des pare-feu. La barre de recherche indique le nombre de pare-feu (éléments) dans la liste. Après avoir saisi les termes de recherche, appliquez le filtre (→) ou effacez le filtre (×) et saisissez une autre suite de termes. • **S/N** – Le numéro de série du pare-feu. • **Adresse IP** – L'adresse IP du pare-feu. • **Modèle** – Le numéro de modèle du pare-feu. • **Version du logiciel** – La version du logiciel installée et en cours d'exécution sur le pare-feu.

Cluster WildFire géré et administration de l'appareil

Sélectionnez **Panorama** > **Managed WildFire Clusters (Clusters WildFire gérés)** et sélectionnez un cluster à gérer ou sélectionnez un appareil WildFire (**Panorama** > **Managed WildFire Appliances (Appareils WildFire gérés)**) pour gérer un appareil autonome. L'affichage **Panorama** > **Managed WildFire Cluster (Clusters WildFire gérés)** reprend les nœuds cluster (appareils WildFire membres du cluster) et les appareils autonomes pour que vous puissiez ajouter des appareils disponibles à un cluster. Étant donné que c'est le cluster qui gère les nœuds, sélectionner un nœud cluster ne fournit qu'une capacité de gestion limitée.

Sauf contre-indication, les paramètres et les descriptions dans le tableau suivant s'appliquent tant aux clusters WildFire qu'aux appareils autonomes WildFire. Les informations précédemment configurées sur un cluster ou un appareil sont pré-renseignées. Vous devez d'abord valider les modifications et les ajouts

et les intégrer aux informations qui figurent dans Panorama, puis appliquer la nouvelle configuration aux appareils.

Paramètre	Description
Onglet Général	
Name (Nom)	Le cluster ou le **Name (Nom)** de l'appareil ou le numéro de série de l'appareil.
Activer DNS (Clusters WildFire uniquement)	**Enable DNS (Activez le service DNS)** pour le cluster.
Enregistrer le pare-feu sur	Le nom de domaine dans lequel vous enregistrez des pare-feu. Le format doit être le suivant : **`wfpc.service.<`***nom-du-cluster***`>.<`***domaine***`>`**. Par exemple, le nom de domaine par défaut est **`wfpc.service.mycluster.paloaltonetworks.com`**.
Serveur de mise à jour du contenu	Saisissez l'emplacement du **Content Update Server (Serveur de mise à jour de contenu)** ou utilisez la valeur par défaut **`wildfire.paloaltonetworks.com`** pour que le cluster ou l'appareil reçoive des mises à jour du contenu du serveur le plus proche au sein de l'infrastructure du Réseau de distribution de contenu. La connexion au cloud global vous permet d'accéder aux signatures et aux mises à jour en fonction de l'analyse des menaces de toutes les sources connectées au cloud, au lieu de se baser uniquement sur l'analyse des menaces locales.
Vérifier l'identité du serveur	**Check Server Identity (Vérifiez l'identité du serveur)** pour confirmer l'identité du serveur de mise à jour en faisant correspondre le nom commun (CN) dans le certificat avec l'adresse IP ou FQDN du serveur.
Serveur de cloud WildFire	Saisissez l'emplacement du **WildFire Cloud Server (Serveur de cloud WildFire)** global ou utilisez la valeur par défaut **`wildfire.paloaltonetworks.com`** pour que le cluster ou l'appareil puisse envoyer des informations au serveur le plus proche. Vous pouvez choisir si vous souhaitez envoyer des informations au nuage global et, si oui, quel type d'informations (**WildFire Cloud Services (Services de cloud WildFire)**).
Exemple d'image d'analyse	Sélectionnez l'image VM que le cluster ou l'appareil utilise pour l'analyse des échantillons (par défaut : vm-5). Vous pouvez Obtenir un fichier de test des logiciels malveillants (WildFire API) pour voir le résultat de l'analyse des échantillons.
Services de cloud WildFire	Si le cluster ou l'appareil est connecté au serveur de cloud global WildFire, vous pouvez choisir si vous souhaitez **Send Analysis Data (Envoyer des données d'analyse)**, **Send Malicious Samples (Envoyer des échantillons**

Paramètre	Description
	malveillants) ou **Send Diagnostics (Envoyer des diagnostics)** au nuage global ou à une combinaison des trois. Vous pouvez choisir d'effectuer une **Verdict Lookup (Vérification des verdicts)** dans le nuage global. L'envoi d'informations dans le cloud global profite à toute la communauté d'utilisateurs WildFire, car les informations partagées augmentent la capacité de chaque appareil à identifier le trafic malveillant et à l'empêcher de traverser le réseau.
Conservation des données des échantillons	Nombre de jours de conservation d'échantillons bénins, grayware ou malveillants : • échantillons **Benign/Grayware (bénins / Grayware)** – plage de 1 à 90, 14 par défaut ; • échantillons **Malicious (malveillants)** – minimum de 1 et il n'y a pas de durée maximale (indéterminée) ; durée indéterminée par défaut.
Services d'environnement d'analyse	**Environment Networking (Réseaux environnementaux)** permet aux machines virtuelles de communiquer avec Internet. Vous pouvez sélectionner **Anonymous Networking (Réseaux anonymes)** pour que la communication réseau soit anonyme, mais vous devez sélectionner **Environment Networking (Réseaux environnementaux)** avant de pouvoir activer **Anonymous Networking (Réseaux anonymes)**. Différents environnements de réseau produisent différents types de charges d'analyse selon que d'autres documents ou fichiers exécutables doivent être analysés. Vous pouvez configurer votre Environnement d'analyse préféré pour allouer davantage de ressources à **Executables (Exécutables)** ou à **Documents** en fonction des besoins de votre environnement. L'allocation **Default (Par défaut)** est répartie entre **Executables (Exécutables)** et **Documents**. La quantité de ressources disponibles dépend du nombre de nœuds WildFire présents dans le cluster.
Génération de signatures	Sélectionnez si vous souhaitez que le cluster ou l'appareil génère des signatures pour AV, DNS ou URL, ou toute combinaison des trois.
Onglet Appareil	
Nom d'hôte (Appareils WildFire autonomes uniquement)	Saisissez le nom d'hôte de l'appareil WildFire.
Serveur Panorama	Saisissez l'adresse IP ou le nom de domaine complet de l'appareil ou du Panorama principal qui gère le cluster.

Paramètre	Description
Serveur 2 de Panorama	Saisissez l'adresse IP ou le nom de domaine complet de l'appareil ou du Panorama de sauvegarde qui gère le cluster.
Domain (Domaine)	Saisissez le nom de domaine du cluster d'appareils ou de l'appareil.
Serveur DNS principal	Saisissez l'adresse IP du Serveur DNS principal.
Serveur DNS secondaire	Saisissez l'adresse IP du Serveur DNS secondaire.
Fuseau horaire	Sélectionnez le fuseau horaire à utiliser pour le cluster ou l'appareil.
Latitude (Appareils WildFire autonomes uniquement)	Saisissez la latitude de l'appareil WildFire.
Longitude (Appareils WildFire autonomes uniquement)	Saisissez la longitude de l'appareil WildFire.
Serveur NTP principal	Saisissez l'adresse IP du serveur NTP principal et définissez le Type d'authentification sur **None (Aucun)** (par défaut), **Symmetric Key (Clé symétrique)** ou **Autokey (Clé automatique)**. Définir le Type d'authentification sur **Symmetric Key (Clé symétrique)** révèle quatre champs supplémentaires : • **Key ID (ID de la clé)** – saisissez l'ID de la clé d'authentification ; • **Algorithm (Algorithme)** – définissez l'algorithme d'authentification sur **SHA1** ou sur **MD5**. • **Authentication Key (Clé d'authentification)** – saisissez la clé d'authentification ; • **Confirm Authentication Key (Confirmer la clé d'authentification)** – saisissez à nouveau la clé d'authentification pour la confirmer.
Serveur NTP secondaire	Saisissez l'adresse IP du serveur NTP secondaire et définissez le Type d'authentification sur **None (Aucun)** (par défaut), **Symmetric Key (Clé symétrique)** ou **Autokey (Clé automatique)**. Définir le Type d'authentification sur **Symmetric Key (Clé symétrique)** révèle quatre champs supplémentaires : • **Key ID (ID de la clé)** – saisissez l'ID de la clé d'authentification ;

Paramètre	Description
	• **Algorithm (Algorithme)** – définissez l'algorithme d'authentification sur **SHA1** ou sur **MD5**. • **Authentication Key (Clé d'authentification)** – saisissez la clé d'authentification ; • **Confirm Authentication Key (Confirmer la clé d'authentification)** – saisissez à nouveau la clé d'authentification pour la confirmer.
Bannière de connexion	Saisissez le message de bannière qui s'affichera lorsque les utilisateurs se connecteront au cluster ou à l'appareil.
Onglet Journaux (comprend l'onglet Système et l'onglet Configuration)	
Ajouter	**Add (Ajouter)** des profils de transfert des journaux (**Panorama** > **Managed WildFire Clusters (Clusters WildFire gérés)** > ***<cluster>*** > **Logging (Journalisation)** > **System (Système)** ou **Panorama** > **Managed WildFire Clusters (Clusters WildFire gérés)** > ***<cluster>*** > **Logging (Journalisation)** > **Configuration**) à transmettre : • journaux de système ou de configuration lorsque SNMP génère des pièges aux récepteurs de pièges SNMP ; • messages Syslog aux serveurs Syslog ; • notifications par courrier électronique aux serveurs de messagerie ; • requêtes HTTP aux serveurs HTTP. Aucun autre type de journal n'est pris en charge (voir Périphériques > Paramètres des journaux). Les profils de Transfert des journaux précisent les journaux à transmettre et les serveurs de destination. Pour chaque profil, procédez comme suit : • **Nom** – un nom qui identifie les paramètres des journaux (jusqu'à 31 caractères) uniquement composé de caractères alphanumériques et de traits de soulignement. Les espaces et les caractères spéciaux ne sont pas autorisés. • **Filtre** – par défaut, l'appareil Panorama transfère **Tous les journaux** du profil précisé. Pour transmettre un sous-ensemble de journaux, sélectionnez un filtre (**gravité EQ critique**, **gravité EQ élevée**, **gravité EQ informationnelle**, **gravité EQ basse** ou **gravité EQ moyenne**) ou sélectionnez **Générateur de filtrage** pour créer un nouveau filtre. • **Description** – saisissez une description (jusqu'à 1 023 caractères) pour expliquer le but du profil.
Ajouter > Filtre > Générateur de filtrage	Utilisez **Générateur de filtrage** pour créer de nouveaux filtres de journaux. Sélectionnez **Créer un filtre** pour élaborer des filtres et, pour chaque requête dans un nouveau filtre, mentionnez les paramètres suivants, puis **Ajoutez** la requête :

Paramètre	Description
	• **Connecteur** – Sélectionnez la logique de connecteur (**et** ou **ou**). Sélectionner **Refuser** si vous souhaitez appliquer un refus. Par exemple, pour éviter de transmettre un sous-ensemble de descriptions des journaux, sélectionnez **Description** en tant qu'Attribut, sélectionnez **Contient** en tant qu'Opérateur et saisissez la chaîne de description en tant que Valeur pour identifier la ou les description(s) que vous ne souhaitez pas transmettre. • **Attribute (Attribut)** – Sélectionnez un attribut de journal. Les options varient selon le type de journal. • **Opérateur** – Sélectionnez les critères qui déterminent comment un attribut s'applique (tel que « **contient** »). Les options varient selon le type de journal. • **Value (Valeur)** : indiquez la valeur de l'attribut à faire correspondre. • **Ajouter** – ajouter le nouveau filtre. Pour afficher ou exporter les journaux auxquels le filtre correspond, sélectionnez **Afficher les journaux filtrés**. • Pour trouver des entrées du journal correspondantes, vous pouvez ajouter des artefacts au champ de recherche, comme une adresse IP ou une plage horaire. • Sélectionnez la période de laquelle vous souhaitez voir les journaux : **Last 15 Minutes (15 dernières minutes)**, **Last Hour (Dernière heure)**, **Last 6 Hrs (6 dernières heures)**, **Last 12 Hrs (12 dernières heures)**, **Last 24 Hrs (24 dernières heures)**, **Last 7 Days (7 derniers jours)**, **Last 30 Days (30 derniers jours)** ou **All (Toutes)** (par défaut). • Les options situées à droite de la liste déroulante de période de temps vous permettent d'appliquer, d'effacer, d'ajouter, d'enregistrer et de charger des filtres : • **Appliquer des filtres** () – affiche les entrées des journaux qui correspondent aux termes renseignés dans le champ de recherche. • **Effacer les filtres** () – efface le champ de filtrage. • **Ajouter un nouveau filtre** () – définit un nouveau critère de recherche (vous atteignez Ajouter un filtre de journal, ce qui est la même chose que créer des filtres). • **Enregistrer un filtre** () – Saisissez un nom pour le filtre puis cliquez sur **OK**.

Paramètre	Description
	• **Utiliser un filtre enregistré** () – Ajouter un filtre enregistré au champ de filtre. • **Exporter vers CSV** () – exporte les journaux dans un rapport au format CSV, puis **Download file (Télécharge un fichier)**. Par défaut, le rapport comprend un maximum de 2 000 lignes de journal. Pour modifier le nombre maximum de lignes des rapports CSV générés, sélectionnez**Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **Logging and Reporting Settings (Paramètres de journalisation et de génération de rapports)** > **Log Export and Reporting (Exportation et génération de rapports de journaux)** et saisissez une nouvelle valeur **Max Rows in CSV Export (Nombre max. de lignes du rapport d'exportation CSV)**. Vous pouvez modifier le nombre et l'ordre des entrées affichées par page. Vous pouvez utiliser les commandes de pagination situées en bas à gauche de la page pour naviguer dans la liste des journaux. Les entrées du journal sont extraites par blocs de 10'A0;pages. • **par page** – utilisez le menu déroulant pour modifier le nombre d'entrées des journaux par page (**20**, **30**, **40**, **50**, **75** ou **100**). • **ASC** ou **DESC** – sélectionnez **ASC** pour classer les résultats dans l'ordre croissant (l'entrée des journaux la plus ancienne en premier) ou **DESC** pour les classer dans l'ordre décroissant (l'entrée des journaux la plus récente en premier). La valeur par défaut est **DESC**. • **Resolve Hostname (Résoudre un nom d'hôte)** – Sélectionnez pour résoudre des adresses IP externes en noms de domaines. • **Highlight Policy Actions (Surligner les actions de politique)** — Précisez une action et sélectionnez pour surligner les entrées des journaux qui correspondent à l'action. Les journaux filtrés sont surlignés dans les couleurs suivantes : • vert – autoriser ; • jaune – continuer ou forcer ; • rouge – refuser, abandonner, abandonner l'ICMP, réinitialiser le client, réinitialiser le serveur, réinitialiser les deux, bloquer-continuer, bloquer le forçage, bloquer l'URL, abandonner tout, entonnoir.
Supprimer	Sélectionnez puis **Supprimez** les paramètres de transfert des journaux que vous souhaitez supprimer de la liste des journaux du Système ou de la Configuration.
Onglet Authentification	

Paramètre	Description
Profil d'authentification	Sélectionnez un profil d’authentification configuré pour définir le service d’authentification qui valide les informations de connexion des administrateurs de l’appareil WildFire ou de Panorama.
Tentatives échouées	Saisissez le nombre d’échecs de tentatives de connexion que l’appareil WildFire autorise sur le CLI avant le verrouillage du compte administrateur (fourchette de 0 à 10 ; par défaut 10). Limitez les tentatives de connexion peut vous permettre de protéger le l’appareil WildFire contre les attaques en force. Une valeur de 0 indique un nombre illimité de tentatives de connexion. *Si vous définissez le champ **Failed Attempts (Tentatives échouées)** sur une valeur non nulle, mais que vous laissez le champ **Lockout Time (Durée de verrouillage)** sur 0, l’administrateur est verrouillé indéfiniment jusqu’à ce qu’un autre administrateur déverrouille manuellement l’administrateur. Si aucun autre administrateur n’a été créé, vous devez reconfigurer les paramètres de **Failed Attempts (Tentatives échouées)** et de **Lockout Time (Durée de verrouillage)** sur et transmettre les changements de configuration à l’appareil WildFire. Pour veiller à ce qu’un administrateur ne soit jamais verrouillé, utilisez la valeur par défaut (**0**) pour les **Failed Attempts (Tentatives échouées)** et la **Lockout Time (Durée de verrouillage)**.* *Définissez le nombre de **Failed Attempts (Tentatives échouées)** sur 5 ou moins pour permettre un nombre raisonnable de nouvelles tentatives en cas de fautes de frappe, tout en empêchant les systèmes malveillants de tenter des méthodes d’attaque par force pour se connecter à l’appareil WildFire.*
Durée de verrouillage (en min.)	Saisissez le nombre de minutes pendant lesquelles l’accès d’un administrateur à l’interface Web et la CLI est verrouillé par l’appareil WildFire si la limite de **Failed Attempts (Tentatives échouées)** est atteinte (plage de 0 à 60; 5 par défaut). Une valeur de 0 signifie que le verrouillage s’applique jusqu’à ce qu’un autre administrateur déverrouille manuellement le compte.

Paramètre	Description
	*Si vous définissez le champ **Failed Attempts (Tentatives échouées)** sur une valeur non nulle, mais que vous laissez le champ **Lockout Time (Durée de verrouillage)** sur 0, l'administrateur est verrouillé indéfiniment jusqu'à ce qu'un autre administrateur déverrouille manuellement l'administrateur. Si aucun autre administrateur n'a été créé, vous devez reconfigurer les paramètres de **Failed Attempts (Tentatives échouées)** et de **Lockout Time (Durée de verrouillage)** sur et transmettre les changements de configuration à l'appareil WildFire. Pour veiller à ce qu'un administrateur ne soit jamais verrouillé, utilisez la valeur par défaut (**0**) pour les **Failed Attempts (Tentatives échouées)** et la **Lockout Time (Durée de verrouillage)**.* *Définissez la **Lockout Time (Durée de verrouillage)** sur au moins 30 minutes pour empêcher les tentatives de connexion continues d'un acteur malveillant.*
Délai d'inactivité (en min.)	Saisissez, pour l'interface Web ou la CLI, le nombre de minutes d'inactivité maximum sur le CLI avant qu'un administrateur ne soit automatiquement déconnecté (la plage est comprise entre 0 et 1 440, la valeur par défaut est aucune). Une valeur égale à 0 signifie que l'inactivité n'entraîne pas une déconnexion automatique. *Définissez un **Idle Timeout (Délai d'inactivité)** de 10 minutes pour empêcher les utilisateurs non autorisés d'accéder à l'appareil WildFire si un administrateur laisse une session ouverte.*
Compte de session max.	Saisissez le nombre de sessions actives que l'administrateur peut ouvrir simultanément, par défaut 0, ce qui signifie que l'appareil WildFire peut avoir un nombre illimité de sessions actives simultanées.
Compte de session max.	Saisissez le nombre de minutes max. pendant lequel l'administrateur peut être connecté avant d'être automatiquement déconnecté. Le nombre par défaut est 0, ce qui signifie que l'administrateur peut être connecté indéfiniment même s'il est inactif.
Administrateurs locaux	Ajoutez et configurez de nouveaux administrateurs pour l'appareil WildFire. Ces administrateurs sont uniques pour l'appareil WildFire et sont gérés depuis cette page (**Panorama** > **Managed WildFire Appliances (Appareils WildFire gérés)** > **Authentication (Authentification)**).
Administrateurs de Panorama	Importez des administrateurs configurés dans Panorama. Ces administrateurs sont créés dans Panorama et importés dans l'appareil WildFire.

Paramètre	Description
Onglet Mise en cluster (clusters WildFire gérés uniquement) et onglet Interfaces (appareils WildFire gérés uniquement) Vous devez ajouter des appareils à Panorama pour gérer les interfaces et ajouter des appareils aux clusters pour gérer les interfaces de nœud.	
Appareil (onglet Mise en cluster uniquement)	Sélectionnez un nœud de cluster pour accéder aux onglets Appareils et Interfaces pour ce nœud. Les informations du nœud de l'onglet Appareil sont pré-renseignées et ne sont pas configurables, sauf pour le nom d'hôte. L'onglet Interfaces répertorie les nœuds d'interfaces. Sélectionnez une interface à gérer selon les descriptions présentées aux sections suivantes : • Nom de l'interface Gestion • Nom de l'interface Analyse Environnement Nom de l'interface réseau • Ethernet2 • Nom de l'interface Ethernet3
Gestion des noms de l'interface	L'interface de gestion est Ethernet0. Permet de configurer ou d'afficher les paramètres de l'interface de gestion : • **Speed and Duplex (Vitesse et Duplex)** – Sélectionnez **auto-negotiate (négocier automatiquement)** (par défaut), **10Mbps-half-duplex (semi-duplex 10 Mbits/s)**, **10Mbps-full-duplex (duplex intégral 10 Mbits/s)**, **100Mbps-half-duplex (semi-duplex 100 Mbits/s)**, **100Mbps-full-duplex (duplex intégral 100 Mbits/s)**, **1Gbps-half-duplex (semi-duplex 1 Gbit/s)** ou **1Gbps-full-duplex (duplex intégral 1 Gbit/s)**. • **Adresse IP** – Saisissez l'adresse IP de l'interface. • **Masque réseau** – Saisissez le masque réseau de l'interface. • **Passerelle par défaut** – Saisissez l'adresse IP de la passerelle par défaut. • **MTU** – Saisissez la MTU en octets (la plage est comprise entre 576 et 1 500 ; la valeur par défaut est 1 500). • **Management Services (Services de gestion)** – Activez les services de gestion que vous souhaitez prendre en charge. Vous pouvez activer **Ping**, **SSH** et les services **SNMP**. Configurez les paramètres proxy si vous utilisez un serveur proxy pour vous connecter à Internet : • **Serveur** – L'adresse IP du serveur proxy. • **Port** – Numéro de port configuré sur le serveur proxy pour écouter les requêtes des périphériques Panorama. • **Utilisateur** – Nom d'utilisateur configuré sur le serveur proxy pour l'authentification. • **Mot de passe** et **Confirmer le mot de passe** – Mot de passe configuré sur le serveur proxy pour l'authentification.

Paramètre	Description
	• **Services de mise en cluster** (onglet Mise en cluster uniquement) – Sélectionnez le service HD : • **HD** – S'il y a deux noeuds de Contrôleurs dans le cluster, vous pouvez configurer l'interface de gestion en tant qu'Interface HD pour que les informations de gestion soient disponibles pour les deux noeuds de Contrôleurs. Si le nœud de cluster que vous configurez est le noeud de Contrôleur principal, indiquez-le comme étant l'interface **HD**. En fonction de la façon dont vous utilisez les interfaces Ethernet de l'appareil WildFire, vous pouvez également configurer Ethernet 2 ou Ethernet 3 comme étant les interfaces HD et HD de sauvegarde, respectivement sur les noeuds de Contrôleur principal et de sauvegarde. Vous pouvez par exemple utiliser Ethernet 2 comme interface HD et HD de sauvegarde. Les interfaces HD et HD de sauvegarde doivent être les mêmes (gestion, Ethernet 2 ou Ethernet 3) sur les noeuds de Contrôleur principal et de sauvegarde. Vous ne pouvez pas utiliser Ethernet 1 comme interface HD/HD de sauvegarde. • **HD de sauvegarde** – Si le nœud de cluster que vous configurez est le noeud de Contrôleur de sauvegarde, indiquez-le comme étant l'interface **HD de sauvegarde**. Précisez les adresses IP autorisées sur l'interface : • **Barre de recherche** – Saisissez des termes de recherche pour filtrer la liste des adresses IP autorisées. La barre de recherche indique le nombre d'adresses IP (éléments) dans la liste pour vous informer de la longueur de cette liste. Après avoir saisi les termes de recherche, appliquez le filtre (→) ou effacez le filtre (×) et saisissez une autre suite de termes. • **Add (Ajouter)—Add (Ajouter)** une adresse IP autorisée. • **Supprimer** – Sélectionnez et **Supprimez** la ou les adresses IP dont vous souhaitez supprimer l'accès à l'interface de gestion.
Réseau environnemental d'analyse du nom de l'interface	Configurez les paramètres de l'interface du réseau environnemental de l'analyse du cluster d'appareils WildFire ou de l'appareil WildFire autonome (Ethernet 1, également appelé interface VM) : • **Speed and Duplex (Vitesse et Duplex)** – Définissez sur **auto-negotiate (négocier automatiquement)** (par défaut), sur **10Mbps-half-duplex (semi-duplex 10 Mbits/s)**, sur **10Mbps-full-duplex (duplex intégral 10 Mbits/s)**, sur **100Mbps-half-duplex (semi-duplex 100 Mbits/s)**, sur **100Mbps-full-duplex (duplex intégral 100 Mbits/s)**, sur **1Gbps-half-duplex (semi-duplex 1 Gbit/s)** ou sur **1Gbps-full-duplex (duplex intégral 1 Gbit/s)**.

Paramètre	Description
	• **Adresse IP** – Saisissez l'adresse IP de l'interface. • **Masque réseau** – Saisissez le masque réseau de l'interface. • **Passerelle par défaut** – Saisissez l'adresse IP de la passerelle par défaut. • **MTU** – Saisissez la MTU en octets (la plage est comprise entre 576 et 1 500 ; la valeur par défaut est 1 500). • **Serveur DNS** – Saisissez l'adresse IP du serveur DNS. • **État de liaison** – Définissez l'état des liaisons de l'interface sur **Ascendant** ou **Descendant**. • Services de gestion – Activez **Ping** si vous souhaitez que l'interface prenne en charge les services ping. Précisez les adresses IP autorisées sur l'interface : • **Barre de recherche** – Saisissez des termes de recherche pour filtrer la liste des adresses IP autorisées. La barre de recherche indique le nombre d'adresses IP (éléments) dans la liste pour vous informer de la longueur de cette liste. Après avoir saisi les termes de recherche, appliquez le filtre () ou effacez le filtre () et saisissez une autre suite de termes. • **Add (Ajouter)—Add (Ajouter)** une adresse IP autorisée. • **Supprimer** – Sélectionnez la ou les adresses IP dont vous souhaitez supprimer l'accès à l'interface de gestion, puis **Supprimez**.
Nom de l'interface Ethernet 2 Nom de l'interface Ethernet 3	Vous pouvez définir les mêmes paramètres pour les interfaces Ethernet 2 et Ethernet 3 : • **Speed and Duplex (Vitesse et Duplex)** – Définissez sur **auto-negotiate (négocier automatiquement)** (par défaut), sur **10Mbps-half-duplex (semi-duplex 10 Mbits/s)**, sur **10Mbps-full-duplex (duplex intégral 10 Mbits/s)**, sur **100Mbps-half-duplex (semi-duplex 100 Mbits/s)**, sur **100Mbps-full-duplex (duplex intégral 100 Mbits/s)**, sur **1Gbps-half-duplex (semi-duplex 1 Gbit/s)** ou sur **1Gbps-full-duplex (duplex intégral 1 Gbit/s)**. • **Adresse IP** – Saisissez l'adresse IP de l'interface. • **Masque réseau** – Saisissez le masque réseau de l'interface. • **Passerelle par défaut** – Saisissez l'adresse IP de la passerelle par défaut. • **MTU** – Saisissez la MTU en octets (la plage est comprise entre 576 et 1 500 ; la valeur par défaut est 1 500). • Services de gestion – Activez **Ping** si vous souhaitez que l'interface prenne en charge les services ping.

Paramètre	Description
	• **Services de Mise en cluster** – Sélectionnez les services de cluster : • **HD** – S'il y a deux noeuds de Contrôleurs dans le cluster, vous pouvez configurer l'interface Ethernet 2 ou Ethernet 3 comme une interface HD pour que les informations de gestion soient disponibles pour les deux noeuds de Contrôleurs. Si le nœud de cluster que vous configurez est le noeud de Contrôleur principal, indiquez-le comme étant l'interface **HD**. En fonction de la façon dont vous utilisez les interfaces Ethernet de l'appareil WildFire, vous pouvez également configurer l'interface de gestion (Ethernet 1) comme étant les interfaces HD et HD de sauvegarde, respectivement sur les noeuds de Contrôleur principal et de sauvegarde. Les interfaces HD et HD de sauvegarde doivent être les mêmes (gestion, Ethernet 2 ou Ethernet 3) sur les noeuds de Contrôleur principal et de sauvegarde. Vous ne pouvez pas utiliser Ethernet 1 comme interface HD/HD de sauvegarde. • **HD de sauvegarde** – Si le nœud de cluster que vous configurez est le noeud de Contrôleur de sauvegarde, indiquez-le comme étant l'interface **HD de sauvegarde**. • **Gestion des clusters** – Configurez l'interface Ethernet 2 ou Ethernet 3 comme l'interface utilisée pour la gestion et la communication à l'échelle du cluster.
Rôle (onglet Mise en cluster uniquement)	Lorsqu'un cluster possède des appareils membres, l'appareil peut avoir le rôle de Contrôleur, de Contrôleur de sauvegarde ou de Subordonné. Sélectionnez **Contrôleur** ou **Contrôleur de sauvegarde** pour modifier l'appareil WildFire utilisé pour chaque rôle à partir des appareils du cluster. La modification du Contrôleur entraîne une perte de données pendant le changement de rôle.
Parcourir (onglet Mise en cluster uniquement)	L'onglet **Mise en cluster** répertorie les nœuds de l'appareil WildFire dans le cluster. **Parcourir** pour afficher et ajouter des appareils WildFire autonomes que le périphérique Panorama gère déjà : • **Barre de recherche** – Saisissez des termes de recherche pour filtrer la liste des nœuds. La barre de recherche indique le nombre d'appareils (éléments) dans la liste pour vous informer de la longueur de cette liste. Après avoir saisi les termes de recherche, appliquez le filtre (→) ou effacez le filtre (×) et saisissez une autre suite de termes. • **Ajout de nœuds** — Ajoutez (⊕) des nœuds au cluster.

Paramètre	Description
	Le premier appareil WildFire que vous ajoutez à un cluster devient automatiquement le nœud de Contrôleur. Le deuxième appareil WildFire que vous ajoutez devient automatiquement le nœud de Contrôleur de sauvegarde. Vous pouvez ajouter jusqu'à 20 appareils WildFire à un cluster. Lorsque vous aurez ajouté les nœuds de Contrôleur et de Contrôleur de sauvegarde, tous les nœuds ajoutés par la suite seront des nœuds Subordonnés.
Supprimer (onglet Mise en cluster uniquement)	Sélectionnez un ou plusieurs appareils dans la liste des Appareils, puis **Supprimez**-les du cluster. Vous pouvez supprimer un nœud de Contrôleur uniquement s'il y a deux nœuds de Contrôleur dans le cluster.
Gérer le contrôleur (onglet Mise en cluster uniquement)	Sélectionnez **Gérer le contrôleur** pour définir un **Contrôleur** et un **Contrôleur de sauvegarde** parmi les nœuds d'appareils WildFire appartenant au cluster. Le nœud de Contrôleur et le nœud de Contrôleur de sauvegarde actuels sont sélectionnés par défaut. Le nœud de Contrôleur de sauvegarde ne peut pas être le même que le nœud de Contrôleur principal.
Onglet Communication	
Personnaliser la communication sécurisée avec le serveur	• **SSL/TLS Service Profile (Profil de service SSL/TLS)** – Sélectionnez un profil de service SSL/TLS à partir du menu déroulant. Ce profil définit le certificat et les versions SSL/TLS compatibles que les périphériques connectés utilisent pour communiquer avec WildFire. • **Certificate Profile (Profil de certificat)** – Sélectionnez un profil de certificat dans le menu déroulant. Ce profil de certificat définit le comportement de la vérification de la révocation du certificat et le certificat AC racine utilisé pour authentifier la chaîne de certificats présentée par le client. • **Custom Certificate Only (Certificat personnalisé uniquement)** – Lorsque cette option est activée, WildFire accepte uniquement des certificats personnalisés pour l'authentification avec des périphériques se connectant. • **Check Authorization List (Vérification de la liste des autorisations)** – Les périphériques clients connectés à WildFire sont vérifiés par rapport à la liste des autorisations. Un appareil ne doit correspondre qu'à un seul objet de la liste à autoriser. Si aucune correspondance n'est trouvée, le périphérique n'est pas autorisé. • **Authorization List (Liste d'autorisations)** – **Add (Ajoutez)** une liste d'autorisations et complétez les champs suivants pour définir les critères requis pour autoriser les périphériques clients. La Liste d'autorisations prend en charge un maximum de 16 entrées. • **Identifier (Identifiant)** – Sélectionnez **Subject (Objet)** ou **Subject Alt. (Autre nom d'objet)** en tant qu'identifiant d'autorisation.

Paramètre	Description
	• **Type** – Si vous avez choisi **Subject Alt. (Autre objet).** en tant qu'identifiant, puis sélectionnez **IP**, **hostname (nom d'hôte)** ou **e-mail** comme type d'identifiant. Si vous avez sélectionné **Subject (Objet)**, le nom commun est alors le type d'identifiant. • **Value (Valeur)** – Saisissez la valeur d'identifiant.
Communication sécurisée avec le client	L'utilisation de la **Secure Client Communication (Sécurisation des communications avec le client)** permet de s'assurer que WildFire utilise des certificats personnalisés configurés (plutôt que le certificat prédéfini par défaut) pour authentifier les connexions SSL avec un autre appareil WildFire. • **Predefined (Prédéfini)** – (par défaut) Aucun certificat de périphérique n'est configuré ; WildFire utilise le certificat prédéfini par défaut. • **Local** – WildFire utilise un certificat de périphérique local et la clé privée correspondante générée sur le pare-feu ou importée à partir d'un serveur PKI d'entreprise existant. • **Certificate (Certificat)** - Sélectionnez le certificat de périphérique local. • **Certificate Profile (Profil du certificat)** - Sélectionnez le Profil de certificat dans le menu déroulant. • **SCEP** – WildFire utilise un certificat de périphérique et une clé privée générée par un serveur Simple Certificate Enrollment Protocol (Protocole d'inscription de certificats simple ; SCEP). • **SCEP Profile (Profil SCEP)** - Sélectionnez un profil SCEP dans la liste déroulante. • **Certificate Profile (Profil du certificat)** - Sélectionnez le Profil de certificat dans le menu déroulant.
Communication sécurisée avec le cluster	Sélectionnez **Enable (Activer)** pour crypter les communications entre les appareils WildFire. Le certificat par défaut utilise le type de certificat prédéfini. Pour utiliser un certificat personnalisé défini par l'utilisateur, vous devez configurer la **Customize Secure Server Communication (Communication sécurisée avec le serveur)** et activer **Custom Certificate Only (Certificat personnalisé uniquement)**.

Panorama > Clusters de pare-feu

- **Panorama** > **Clusters de pare-feu**

Affichez le résumé des clusters de pare-feu de la série CN et les informations de surveillance dans l'interface Web de Panorama sous Clusters de pare-feu.

(Only available on the CN-Series firewalls (Disponible uniquement sur les pare-feu de la série CN)) Depuis la liste**Panorama** > **Admin roles (rôles d'admin)** > **Web UI (Interface utilisateur web)**, sélectionnez **Firewall Clusters (Clusters de pare-feu)**, puis **Enable (Activer)** pour accéder aux clusters de pare-feu. Après avoir ajouté des clusters de pare-feu à Panorama, utilisez l'interface Web pour afficher les détails des clusters de pare-feu de la série CN.

*Vous devez installer le plug-in de clustering à partir de **Device (Appareil)** > **Plugins** pour afficher les détails du cluster sous **Firewall Clusters (clusters de pare-feu)**.*

- Vue récapitulative
- Surveillance

Vue récapitulative

Affichez les informations concernant les clusters CN-Series capturés par le pare-feu au cours des cinq dernières minutes. Cliquez sur le bouton d'actualisation pour charger les derniers détails.

Champ	Description
Nom du cluster	Nom du cluster de pare-feu.
Version du logiciel	Version PAN-OS.
Plug-ins utilisés sur le cluster	Liste des plugins utilisés sur le cluster. *Seuls les plug-ins de pare-feu CN-Series sont pris en charge.*
Pile de modèles	Nom de la pile de modèles associée au cluster.
Groupe de périphériques	Nom du groupe de périphériques associé au cluster.
État du cluster	Indique si le cluster est affecté ou non.
Type de cluster	Type de cluster.

Champ	Description
	Seuls les types de clusters de pare-feu CN-Series sont pris en charge.
Membres touchés	Nombre de membres du cluster affectés et leurs noms.
Détails du journal système	Affiche les détails des événements système.
Erreur spécifique	Liste des erreurs spécifiques dans le cluster. Cliquez sur le lien pour afficher plus de détails sur l'erreur sous **Monitor (Surveiller)** > **Logs (journaux)** > **System (système)** où vous pouvez view logs (afficher les journaux).
Nom du pod	Nom du pod.
Nombre de CPU	Nombre de processeurs utilisés.

Surveillance

Affichez les informations d'intégrité du cluster de pare-feu de la série CN.

Champ	Description
Cluster de logiciels gérés	Sélectionnez un cluster de pare-feu. *Seuls les types de clusters de pare-feu CN-Series sont pris en charge.*
Touchés	Liste des clusters de pare-feu affectés. • **CN-Clusters (Clusters CN)** – Nombre de clusters de pare-feu CN-Series affectés. • **Clusters Impacted (Clusters affectés)** – Affiche la liste des clusters affectés. Cliquez pour afficher des informations détaillées sur les clusters dans les tableaux de bord **Interconnect Status (État de l'interconnexion)** et **Cluster Utilization (Utilisation du cluster)**.
OK	Liste des clusters de pare-feu qui ne sont pas affectés. • **Clusters CN** : nombre de clusters de pare-feu de la série CN qui ne sont pas affectés. • **Clusters impacted (Clusters concernés)**: affiche la liste des clusters qui ne sont pas affectés.

Champ	Description
	Cliquez pour afficher des informations détaillées sur les clusters dans les tableaux de bord **Interconnect Status (État de l'interconnexion)** et **Cluster Utilization (Utilisation du cluster)**.
État de l'interconnexion	Affichez les détails d'interconnexion du cluster pour une période sélectionnée. Sélectionnez **Last 5 Mins (5 dernières minutes)** pour afficher les détails suivants. • **Cluster Name (Nom du cluster)** – Nom du cluster de pare-feu. • **Cluster Type (Type de cluster)** – Type de cluster.  *Seuls les types de clusters de pare-feu CN-Series sont pris en charge.* • **Cluster Creation Time (Heure de création du cluster)** – Heure de création du cluster. • **Current Cluster State (État actuel du cluster)** – Indique si le cluster est affecté ou non. • **Current Cluster Detail (Détails du cluster actuel)** : cliquez sur le lien État actuel du cluster pour afficher plus de détails sur le cluster concerné. • **Cluster Interconnect Status (État d'interconnexion du cluster)** : indique si le cluster est affecté ou non. • **Current Cluster Detail (Détail du cluster actuel)** : cliquez sur le lien État actuel de l'interconnexion pour afficher plus de détails sur le cluster affecté. • **Traffic Interconnect (Interconnexion du trafic)** – État de l'interconnectivité du trafic. • **External Connection (Connexion externe)** – État de la connectivité externe. • **Impacted Links (Liaisons affectées)** – Nombre de liaisons affectées. • **Management Connectivity (Connectivité de gestion)** – Nombre de connexions de gestion. • **Impacted Cluster Member (Membre de cluster affecté)** – Liste des membres de cluster affectés. • **Time Stamp Hi-Res Uptime (Horodatage haute résolution du temps de disponibilité)** – Horodatage du temps de disponibilité. • **Time Stamp Hi-Res Downtime (Horodatage haute résolution du temps d'interruption)** – Horodatage du temps d'interruption. En cas de sélection de toute autre période, seules les informations suivantes apparaissent. • **Nom du cluster** • **Type de cluster** • **Temps de création du cluster** • **État actuel du cluster**

Champ	Description
	• **État de l’interconnexion du cluster** • **Interconnexion du trafic** • **Connexion externe**
Utilisation du cluster	Affichez le débit, la mémoire et l’utilisation des données du cluster de pare-feu. • **Cluster Name (Nom du cluster)** : nom du cluster de pare-feu. • **Cluster Details (Détails du cluster)** : cliquez sur le lien du nom du cluster pour afficher les détails du débit, de la mémoire et de l’utilisation des données du cluster sélectionné. • **Cluster Type (Type de cluster)** – Type de cluster. *Seuls les types de clusters de pare-feu CN-Series sont pris en charge.* • **Cluster State (État du cluster)** – Affiche l’état de santé du cluster. • **Cluster Throughput (gbps) (Débit du cluster [Gbit/s])** – Débit du cluster de pare-feu en Gbit/s. • **CPS** – Nombre de connexions par seconde. • **Session Count (Sessions) (Nombre de sessions [Sessions])** – Nombre de sessions. • **Average Data Plane (%) Within Health Threshold (Plan de données moyen [%] dans le seuil de santé)** – Seuil moyen du plan de données en pourcentage. • **Management Plane CPU (%) (Processeur du plan de gestion [%])** – Utilisation du processeur du plan de gestion en pourcentage. • **Management Plane Mem (%) (Mémoire du plan de gestion [%])** –Utilisation de la mémoire du plan de gestion en pourcentage. • **Logging Rate (Log/Sec) (Taux de journalisation [Journaux/s])** – Taux auquel les journaux sont générés sur le cluster. • **DP Auto-Scale Status (État de mise à l’échelle automatique DP)** – Détails de la mise à l’échelle automatique du plan de données.

Panorama > Administrateurs

Sélectionnez **Panorama** > **Administrators (Administrateurs)** pour créer et gérer des comptes pour les administrateurs Panorama.

Si vous vous connectez à Panorama en tant qu'administrateur avec un rôle de super-utilisateur, vous pouvez débloquer les comptes d'autres administrateurs en cliquant sur les icônes de verrouillage dans la colonne Utilisateur verrouillé. Un administrateur bloqué ne peut pas accéder à Panorama. Panorama verrouille les administrateurs qui dépassent le nombre autorisé de tentatives successives échouées pour accéder à Panorama tel que défini dans le **Authentication Profil (Profil d'authentification)** affecté à leurs comptes (voir Périphérique > Profil d'authentification).

Pour créer un compte administrateur, cliquez pour **Ajouter** et configurez les paramètres comme décrits dans le tableau suivant.

Paramètres du compte administrateur	Description
Name (Nom)	Donnez un nom d'utilisateur de connexion à l'administrateur (15 caractères maximum). Le nom est sensible à la casse, doit être unique et ne peut contenir que des lettres, des chiffres, des traits d'union et des caractères de soulignement.
Profil d'authentification	Sélectionnez un profil ou une séquence d'authentification pour authentifier cet administrateur. Pour plus de détails, voir Périphérique > Profil d'authentification ou Périphérique > Séquence d'authentification.
Utiliser uniquement l'authentification du certificat client (Web)	Sélectionnez cette option pour utiliser l'authentification du certificat du client pour l'accès à l'interface Web. Si vous choisissez cette option, un nom d'utilisateur (**Name (Nom)**) et un **Password (Mot de passe)** ne sont pas nécessaires.
Mot de passe/Confirmer le mot de passe	Saisissez et confirmez un mot de passe sensible à la casse pour l'administrateur (16 caractères maximum). Pour garantir la sécurité, Palo Alto Networks recommande que l'administrateur change son mot de passe régulièrement en utilisant des lettres en minuscules, en majuscules et des chiffres. Veillez à respecter les pratiques exemplaires en matière de robustesse des mots de passe pour vous assurer de créer un mot de passe fort. Les administrateurs de groupes de périphériques et de modèles ne peuvent pas accéder à **Panorama** > **Administrators (Administrateurs)**. Pour modifier leur mot de passe local, ces administrateurs doivent cliquer sur leur nom d'utilisation (à côté de **Logout (Déconnexion)** en bas de l'interface Web). Ce processus s'applique également aux administrateurs ayant un rôle Panorama personnalisé pour lequel l'accès à **Panorama** > **Administrators (Administrateurs)** est désactivé.

Paramètres du compte administrateur	Description
	Vous pouvez utiliser l'authentification de mots de passe conjointement avec un **Authentication Profile (Profil d'authentification)** (ou une séquence) ou pour l'authentification de base de données locale. Vous pouvez définir les paramètres d'expiration du mot de passe en sélectionnant un **Profil de mot de passe** (voir Périphérique > Profils de mots de passe) et en définissant des paramètres de Complexité minimale du mot de passe (voir Périphérique > Configuration > Gestion), mais uniquement pour les comptes administratifs que Panorama authentifie localement.
Utiliser l'authentification à clef publique (SSH)	Sélectionnez pour utiliser Authentification de clé publique SSH : cliquez sur **Importer la clé**, puis sur **Navigateur** pour sélectionner le fichier de clé publique, puis cliquez sur **OK**. La boîte de dialogue Administrateur affiche la clé chargée dans la zone de texte en lecture seule. Les formats de fichier de clé pris en charge sont IETF SECSH et OpenSSH. Les algorithmes de clé pris en charge sont DSA (1024 bits) et RSA (768 à 4096 bits). *Si l'authentification de la clé publique échoue, Panorama présente une invite de saisie du nom d'utilisateur et du mot de passe.*
Type d'administrateur	Le type sélectionné détermine les options du rôle administrateur : • **Dynamique** - Rôles qui offrent l'accès à Panorama et aux pare-feu gérés. Lors de l'ajout de nouvelles fonctionnalités, Panorama met automatiquement à jour les définitions des rôles dynamiques. Vous ne devez les jamais les mettre à jour manuellement. • **Admin Panorama personnalisé** - Rôles configurables qui disposent d'un accès en lecture / écriture, d'un accès en lecture seule ou d'aucun accès aux fonctionnalités de Panorama. • **Admin groupe de périphériques et modèle** - Rôles configurables qui disposent d'un accès en lecture / écriture, d'un accès en lecture seule ou d'aucun accès aux fonctionnalités pour les groupes de périphériques et les modèles affectés aux domaines d'accès que vous sélectionnez pour cet administrateur.
Rôle admin (Type d'administrateur dynamique)	Sélectionnez un rôle prédéfini : • **Superuser (Super utilisateur)** : accès complet en lecture/écriture à Panorama et à tous les groupes de périphériques, modèles et pare-feu gérés.

Paramètres du compte administrateur	Description
	• **Superuser (Read Only) (Super utilisateur (Lecture seule))** : accès en lecture seule à Panorama et à tous les groupes de périphériques, modèles et pare-feu gérés. • **Panorama administrator (Administrateur Panorama)** : accès complet à Panorama, à l'exception des actions suivantes : • Créer, modifier ou supprimer des administrateurs de Panorama ou de pare-feu et des rôles. • Exporter, valider, rétablir, enregistrer, charger ou importer une configuration (**Device (Périphérique)** > **Setup (Configuration)** > **Operations (Opérations)**). • Configurer une **Scheduled Config Export (Exportation programmée des configurations)** dans l'onglet **Panorama**.
Profil (Type d’administrateur Admin Panorama personnalisé)	Sélectionnez un rôle Panorama personnalisé (reportez-vous à la section Panorama > Périphériques gérés > Récapitulatif).
Domaine d'accès au rôle administrateur (type d'administrateur Groupe de périphériques et modèle Admin)	Pour chaque domaine d’accès (jusqu’à 25) que vous souhaitez affecter à l’administrateur, **Add (Ajoutez)** un **Access Domain (Domaine d’accès)** à partir de la liste déroulante (reportez-vous à la section Panorama > Domaines d’accès), cliquez sur la cellule adjacente au Rôle Administrateur, puis sélectionnez un rôle administrateur de groupe de périphériques et de modèle personnalisé à partir de la liste déroulante (reportez-vous à la section Panorama> Périphériques gérés > Récapitulatif). Lorsque des administrateurs disposant d’un accès à plusieurs domaines se connectent à Panorama, un menu déroulant **Domaine d’accès** apparaît dans le pied de page de l’interface Web. Les administrateurs peuvent sélectionner n'importe quel **Access Domain (Domaine d'accès)** affecté pour filtrer les données de surveillance et de configuration affichées par Panorama. La sélection **Access Domain (Domaine d'accès)** filtre également les pare-feu qui sont affichés dans la liste déroulante **Context (Contexte)**. *Si vous utilisez un serveur RADIUS pour authentifier les administrateurs, vous devez mapper les rôles d’administrateur et les domaines d’accès aux VSA RADIUS. Les chaînes VSA prenant en charge un nombre limité de caractères, si vous configurez le nombre maximum de paires de domaine d'accès/ rôle (25) pour un administrateur, les valeurs Nom de chaque domaine d'accès et de chaque rôle ne doivent pas dépasser une moyenne de 9 caractères.*

Paramètres du compte administrateur	Description
Profil de mot de passe	Sélectionnez un **Profil de mot de passe** (voir Périphérique > Profils de mots de passe).

Panorama > Rôles admin

Les profils de rôle d'administrateur sont des rôles personnalisés qui définissent les privilèges d'accès et les responsabilités des administrateurs. Par exemple, les rôles attribués à un administrateur contrôlent quels rapports il peut générer et quel groupe de périphériques ou quelles configurations de modèle l'administrateur peut afficher ou modifier.

Pour un administrateur de groupe de périphériques et de modèle, vous pouvez attribuer un rôle distinct pour chaque domaine d'accès qui est affecté au compte administratif (voir Panorama > Domaines d'accès). Le recensement des rôles pour accéder aux domaines vous permet d'obtenir un contrôle très important sur les informations auxquelles les administrateurs peuvent accéder sur Panorama. Par exemple, imaginez un scénario où vous configurez un domaine d'accès qui inclut tous les groupes de périphériques pour les pare-feu dans vos centres de données et où vous attribuez ce domaine d'accès à un administrateur qui est autorisé à surveiller le trafic du centre de données, mais qui n'est pas autorisé à configurer les pare-feu. Dans ce cas, vous pouvez schématiser le domaine d'accès à un rôle qui active tous les privilèges de surveillance, mais qui désactive l'accès aux paramètres du groupe de périphériques.

Pour créer un profil de rôle administrateur, cliquez pour **Ajouter** un profil et configurez les paramètres comme décrits dans le tableau suivant.

Si vous utilisez un serveur RADIUS pour authentifier les administrateurs, mappez les rôles administrateur et les domaines d'accès avec les attributs spécifiques au fournisseur (VSA) RADIUS.

Paramètres du rôle administrateur de Panorama	Description
Name (Nom)	Saisissez un nom pour identifier ce rôle administrateur (31 caractères maximum). Le nom est sensible à la casse, doit être unique et ne peut contenir que des lettres, des chiffres, des espaces, des traits d'union et des caractères de soulignement.
Description	(Facultatif) Saisissez une description du rôle.
Rôle	Sélectionnez la portée des responsabilités administratives : **Panorama** ou **Device Group and Template (Groupe de périphériques et modèle)**.
UI Web	Sélectionnez l'une des options suivantes pour définir le type d'accès autorisé pour des fonctions spécifiques dans le contexte de Panorama (**liste UI Web**) et le contexte de pare-feu (**liste IU de commutation de contexte**) : • **Enable (Activer)(** ) - Accès en lecture/écriture

Paramètres du rôle administrateur de Panorama	Description
	• **Read Only (Lecture seule)** () - Accès en lecture seule • **Disable (Désactiver)** () - Aucun accès
Api XML (rôle Panorama uniquement)	Sélectionnez le type d'accès à l'API XML/REST (**Enable (Activer)**, ou **Disable (Désactiver)**) pour Panorama et pour les pare-feu gérés : • **Rapport** - Accès à Panorama et aux rapports du pare-feu. • **Journal** - Accès à Panorama et aux journaux du pare-feu. • **Configuration** - Autorisations pour récupérer ou modifier les configurations de Panorama et pare-feu. • **Requêtes opérationnelles** - Autorisations pour exécuter des commandes opérationnelles sur Panorama et sur les pare-feu. • **Valider** - Autorisations pour valider les configurations de Panorama et du pare-feu. • **Agent User-ID** - Accès à l'agent User-ID. • **Exporter** - Autorisations pour exporter des fichiers depuis Panorama et les pare-feu (tels que des configurations, des pages de blocage ou de réponse, des certificats et des clés). • **Importer** - Autorisations pour importer des fichiers dans Panorama et les pare-feu (tels que des mises à jour logicielles, des mises à jour de contenu, des licences, des configurations, des certificats, des pages de blocage et des journaux personnalisés).
Ligne de commande (rôle Panorama uniquement)	Sélectionnez le type de rôle d'accès à la CLI : • **Aucun** - (par défaut) L'accès à CLI (interface de ligne de commande) de Panorama n'est pas autorisé. • **Super utilisateur** - Accès complet à **Panorama**. • **Super lecteur** - Accès en lecture seule à **Panorama**. • **Admin Panorama** - Accès complet à **Panorama**, à l'exception des actions suivantes : • Créer, modifier ou supprimer des administrateurs de Panorama et des rôles. • Exporter, valider, rétablir, sauvegarder, charger ou importer une configuration. • Planification de l'exportation de la configuration

Paramètres du rôle administrateur de Panorama	Description
REST API (rôle Panorama uniquement)	Sélectionnez le type d’accès (**Enable (Activer)**, **Read Only (Lecture seule)**, ou **Disable (Désactiver)**) qui s’applique à chaque terminal REST API pour Panorama et pour les pare-feu gérés : Vous pouvez attribuer un accès au rôle terminaux dans les catégories suivantes. • Objets • Politiques • Réseau • Périphérique
Changement de contexte	
Rôle d'administrateur du périphérique	Entrez le device admin role (nom du rôle d'administrateur du périphérique) pour permettre à un administrateur **Panorama** de basculer entre l'interface Web Panorama et le pare-feu géré.

Panorama > Domaines d'accès

Les domaines d’accès contrôlent l’accès dont disposent les administrateurs de groupe de périphériques et de modèles à des groupes de périphériques (pour gérer des politiques et des objets), à des modèles (pour gérer les paramètres de réseau et de périphérique), à l’interface Web des pare-feu gérés (à travers le changement de contexte) spécifiques et pour le REST API des pare-feux gérés. Vous pouvez définir jusqu’à 4 000 domaines d’accès et les gérer localement ou à l’aide d’attributs spécifiques au fournisseur (VSA) RADIUS, de VSA TACACS+ ou d’attributs SAML. Pour créer un domaine d’accès, cliquez pour **Ajouter** un domaine et configurez les paramètres comme décrits dans le tableau suivant.

Paramètres du domaine d’accès	Description
Name (Nom)	Donnez un nom au domaine d’accès (31 caractères maximum). Le nom est sensible à la casse, doit être unique et ne peut contenir que des lettres, des chiffres, des traits d’union et des caractères de soulignement.
Objets partagés	Sélectionnez un des privilèges d'accès suivants pour les objets dont les groupes de périphériques de ce domaine d'accès héritent à partir de l'emplacement Partagé. Quel que soit le privilège, les administrateurs ne peuvent pas appliquer un contrôle prioritaire sur des objets partagés ou par défaut (prédéfinis). • **Lecture** : les administrateurs peuvent afficher et cloner des objets partagés mais ne peuvent pas effectuer d'autres opérations sur ceux-ci. Lors de l'ajout d'objets non partagés ou du clonage d'objets partagés, la destination doit être un groupe de périphériques du domaine d'accès, non partagé. • **write (écriture)** : les administrateurs peuvent effectuer toutes les opérations sur des objets partagés. Il s'agit de la valeur par défaut. • **shared-only (partagé uniquement)** : les administrateurs peuvent ajouter des objets à Partagé uniquement. Les administrateurs peuvent également afficher, modifier et supprimer des objets partagés, mais ne peuvent pas les déplacer ou les cloner. Le choix de cette valeur a pour conséquence que les administrateurs ne peuvent pas effectuer d'opérations sur des objets non partagés autres que leur affichage.
Groupes de périphériques	Activez ou désactivez l’accès en lecture/écriture sur des groupes de périphériques donnés dans le domaine d’accès. Vous pouvez également cliquer sur **Enable All (Activer tout)** ou **Disable All (Désactiver tout)**. L'autorisation de l'accès en lecture/écriture sur un groupe de périphériques active automatiquement le même accès sur ses descendants. Si vous désactivez manuellement un descendant, l'accès sur son ancien le plus élevé passe automatiquement à lecture seule. Par défaut, l'accès est désactivé pour tous les groupes de périphériques.

Paramètres du domaine d’accès	Description
	Si vous souhaitez que la liste affiche uniquement des groupes de périphériques spécifiques, sélectionnez les noms des groupes de périphériques et le **Filtre sélectionné**. *Si vous définissez l’accès aux objets partagés sur **Partagés seulement**, Panorama applique l’accès en lecture seule à tous les groupes de périphériques pour lesquels vous spécifiez un accès en lecture / écriture.*
Modèles	Pour chaque modèle ou pile de modèles que vous souhaitez affecter, cliquez sur **Add (Ajouter)**, puis sélectionnez-le (ou la) dans la liste déroulante.
Contexte du périphérique (Correspond à la colonne Périphériques / Systèmes virtuels qui figure à la page Domaine d’accès)	Sélectionnez les pare-feu pour lesquels l’administrateur peut changer le contexte afin d'effectuer la configuration locale. Si la liste est longue, vous pouvez la filtrer par **Device State (État du périphérique)**, **Platforms (Plates-formes)**, **Device Groups (Groupes de périphériques)**, **Templates (Modèles)**, **Tags (Étiquettes)** ou **HA Status (État HA)**.
Groupes de collecteurs de journaux	Pour chaque groupe de collecteurs que vous souhaitez affecter, cliquez sur **Add (Ajouter)**, puis sélectionnez-le dans la liste déroulante.

Panorama > Transmission programmée des configurations

Pour simplifier l'opération de transmission des modifications de configuration aux pare-feux gérés, créez une transmission de configuration planifiée pour transmettre automatiquement les modifications à vos pare-feux gérés à une date et une heure spécifiées. Vous pouvez configurer une transmission de configuration planifiée pour qu'elle se produise une fois ou selon une planification récurrente.

Les rubriques suivantes fournissent des informations supplémentaires sur une transmission de configuration planifiée.

Que voulez-vous savoir ?	Reportez-vous à la section :
Ajouter une transmission planifiée de la configuration.	Planificateur de transmission programmée des configurations
Affichez l'historique de transmission de configuration planifiée.	Historique d'exécution de la transmission programmée des configurations

Informations de transmission de configuration planifiée	Description
Nom	Nom de la planification de transmission de configuration.
Étendue de l’administrateur	Ajoutez les modifications de configuration apportées par d’autres administrateurs à la configuration planifiée. La possibilité de transmettre des modifications de configuration pour d’autres administrateurs est définie dans le profil de rôle d’administrateur Panorama (Panorama > rôles d’administrateur). Cliquez sur le *<usernames>* lien pour sélectionner les administrateurs, puis cliquez sur **OK** pour afficher et sélectionner les modifications de configuration apportées par d’autres administrateurs. Même si votre rôle permet de transmettre les modifications d’autres administrateurs, l’étendue push inclut uniquement vos modifications par défaut.
Désactivation	Affiche si la configuration planifiée transmise est activée (non cochée) ou désactivée (cochée).
Date	Date (`YYY/MM/DD (AAAA/MM/JJ)`) prévue pour la prochaine transmission de configuration.
Récurrence	Si la transmission de configuration planifiée est une transmission unique ou une transmission programmée récurrente (`monthly (mensuelle)`, `weekly (hebdomadaire)` ou `daily (quotidienne)`).

Informations de transmission de configuration planifiée	Description
Période	Pour une planification récurrente, l'heure (`hh:mm`) et le jour où la transmission de configuration est planifiée. Pour une planification unique, l'heure (`hh:mm`) de la transmission de configuration planifiée est planifiée pour se produire.
État	Statut d'exécution de la dernière transmission de configuration planifiée. Cliquez pour afficher l'historique d'exécution complet de tous les pare-feux gérés associés à la transmission de configuration planifiée.
Périphériques	Pare-feux gérés impactés par la transmission de configuration programmée. Affiche les pare-feux impactés en fonction des modifications apportées au groupe de périphériques et au modèle.

Planificateur de transmission programmée des configurations

Créez une transmission programmée vers les pare-feu gérés en définissant les paramètres de planification pour quand et à quelle fréquence une transmission se produit, quels groupes d'appareils et configurations de modèles sont transmis, et vers quels pare-feu gérés transmettre. Panorama effectue la transmission planifiée de la configuration du groupe d'appareils et du modèle aux pare-feu gérés si l'état de la dernière validation des **Device Groups (groupes de périphériques)** ou des **Templates (modèles)** est `out-of-sync (pas synchronisé)`.

Paramètres de transmission de configuration planifiée	Description
Nom	Nom de la planification de transmission de configuration.
Désactivé	Vérifiez pour désactiver la transmission de configuration planifiée. Décochez cette case pour réactiver la transmission de configuration planifiée.
Type	Sélectionnez **One-time schedule (Planification unique)** pour planifier une transmission de configuration à une date et une heure spécifiques. Sélectionnez **Recurring schedule (Planification récurrente)** pour planifier une transmission de configuration
Date	Date à laquelle la prochaine transmission de configuration est planifiée.
Période	Heure (`hh:mm:ss`) à laquelle la transmission de configuration est planifiée pour se produire à la **Date** de transmission de configuration planifiée.

Paramètres de transmission de configuration planifiée	Description
Récurrence	Si la transmission de configuration planifiée est une transmission unique (**None (Aucune)**) ou une transmission planifiée récurrente (**Monthly (Mensuelle)**, **Weekly (Hebdomadaire)**, ou **Daily (Quotidien)**). Valeur par défaut : **Aucune**.
Sélection de l’étendue de la transmission	
Groupes de périphériques	Sélectionnez les pare-feu gérés associés à un ou plusieurs groupes d’appareils. • **Merge with Device Candidate Config (Fusionner avec la configuration candidate du périphérique)** (Selectionné par défaut) : fusionne les modifications de configuration transmises par Panorama en prenant en compte les modifications en attente mises en œuvre localement par les administrateurs sur le pare-feu cible. La transmission déclenche le logiciel PAN-OS® pour valider les modifications fusionnées. Si vous désélectionnez cette option, la validation exclut la configuration candidate sur le pare-feu. • (Sélectionné par défaut) **Include Device and Network Templates (Inclure les modèles de périphérique et de réseau)** (Sélectionné par défaut) : Applique les changements de groupe de périphériques et les modifications du modèle associé aux pare-feu et aux systèmes virtuels sélectionnés en une seule opération. Pour appliquer ces modifications en tant qu’opérations distinctes, désélectionnez cette option.
Modèles	Sélectionnez les pare-feu gérés associés à une ou plusieurs piles de modèles. • **Merge with Device Candidate Config (Fusionner avec la configuration candidate du périphérique)** (Selectionné par défaut) : fusionne les modifications de configuration transmises par Panorama en prenant en compte les modifications en attente mises en œuvre localement par les administrateurs sur le pare-feu cible. Le transmission déclenche le logiciel PAN-OS pour valider les modifications fusionnées. Si vous désélectionnez cette option, la validation exclut la configuration candidate sur le pare-feu.

Historique d'exécution de la transmission programmée des configurations

Affichez l'historique d'exécution de la transmission de configuration planifiée pour comprendre quand la dernière transmission pour une programmation spécifique s'est produite et pour voir combien de pare-feux gérés ont été touchés. À partir du nombre total de pare-feux gérés impactés, vous pouvez voir combien de transmission de configuration vers des pare-feux gérés ont réussi et combien ont échoué. Parmi les transmissions ayant échoué, vous pouvez afficher le nombre total de pare-feux gérés avec des configurations automatiquement rétablies en raison d'une connexion interrompue ou interrompue entre le pare-feu géré et Panorama.

Informations sur l'historique d'exécution	Description
Heure de la dernière transmission	Heure à laquelle le push de configuration planifié s'est produit (`MM (MM)/YYY (AAAA) HH:MM:SS`).
Périphériques	Nombre total de pare-feux gérés associés à la transmission de configuration planifiée.
Réussite	Nombre total de pare-feux gérés associés à la transmission de configuration planifiée pour lesquels la transmission a réussi.
Échec	Nombre total de pare-feux gérés associés à la transmission de configuration planifiée pour lesquels la transmission a échoué.
Rétablir	Nombre total de pare-feux gérés pour lesquels la transmission de configuration planifiée a échoué et la configuration a été rétablie.
Tâches	Affichez le gestionnaire de tâches Panorama et les tâches associées à la transmission de configuration.

Panorama > Périphériques gérés > Récapitulatif

Un pare-feu Palo Alto Networks géré par Panorama est appelé un *périphérique géré*. Panorama peut gérer des pare-feux exécutant la même version majeure ou des versions majeures antérieures, mais pas des pare-feux exécutant une version majeure ultérieure. Par exemple, Panorama utilisant PAN-OS 11.0 peut gérer les pare-feux utilisant PAN-OS 11.0 et ses versions antérieures. De plus, il n'est pas recommandé de gérer des pare-feux utilisant une version plus récente que Panorama puisque cela peut faire en sorte que certaines fonctionnalités ne fonctionnent pas comme prévu. Par exemple, il n'est pas recommandé de gérer des pare-feux utilisant PAN-OS 10.0.1 ou une version ultérieure si Panorama utilise PAN-OS 10.0.0. Pour plus d'informations reportez-vous à la section Release Notes (Notes de version) de PAN-OS 11.0. Pour plus d'informations sur les versions de PAN-OS prises en charge, reportez-vous à End-of-Life Summary (Récapitulatif de fin de vie).

- Administration du pare-feu géré
- Informations sur les pare-feu gérés
- Mises à jour logicielles et de contenu du pare-feu
- Sauvegardes du pare-feu

Administration du pare-feu géré

Vous pouvez effectuer les tâches administratives suivantes sur les pare-feu.

Tâche	Description
Ajouter	Cliquez sur **Ajouter** et saisissez les numéros de série des pare-feu (un par ligne) pour les ajouter en tant que périphériques gérés. Ensuite, la fenêtre **Périphériques gérés** affichera les Informations sur les pare-feu gérés, y compris l'état de la connexion, les mises à jour installées et les propriétés qui ont été définies lors de la configuration initiale. Cochez la case **Associate Devices (Périphériques associés)** pour associer les pare-feu à un groupe de périphériques ou à une pile de modèles. **Import (Importez)** plusieurs pare-feu au format CSV qui doivent être gérés par le serveur de gestion Panorama. Un fichier CSV type peut être téléchargé. Saisissez ensuite l'adresse IP du serveur de gestion Panorama sur chaque pare-feu (voir Périphérique > Configuration > Gestion) afin que Panorama puisse gérer les pare-feu. *le pare-feu s'enregistre auprès de Panorama via une connexion SSL en utilisant un chiffrement AES-256. Panorama et le pare-feu s'authentifient mutuellement à l'aide de certificats 2 048 bits et utilisent la connexion SSL pour la gestion de la configuration et la collecte des journaux.*
Réassocier	Réaffecter un ou plusieurs pare-feu sélectionnées à un autre groupe de périphériques ou à une autre pile de modèles.

Tâche	Description
Supprimer	Sélectionnez un ou plusieurs pare-feu, puis **Delete (Supprimez)**-les de la liste des pare-feu gérés par Panorama.
Étiquette	Sélectionnez un ou plusieurs pare-feu, cliquez sur **Tag (Étiquette)**, puis saisissez un texte de 31 caractères maximum ou sélectionnez une étiquette existante. sans espace Lorsque l'interface Web affiche une longue liste de pare-feu (dans la boîte de dialogue d'installation de logiciel, par exemple), les étiquettes permettent de filtrer la liste. Par exemple, vous pouvez utiliser une étiquette libellée Filiale pour définir un filtre pour tous les pare-feu des filiales de votre réseau.
Installer	**Install (Installez)** les mises à jour logicielles ou de contenu du pare-feu.
Regrouper les homologues HA	Sélectionnez **Regrouper les homologues HA** si vous voulez que la page **Périphériques gérés** regroupe les pare-feu homologues dans une configuration haute disponibilité (HA). Vous pouvez ensuite choisir d'effectuer uniquement des actions sur les deux homologues de chaque paire HA ou sur ni l'un, ni l'autre.
Gérer (les sauvegardes)	**Manage (Gérez)** les sauvegardes du pare-feu.
PDF/CSV	Les rôles administrateur qui sont au moins dotés de l’accès en lecture seule peuvent exporter le tableau des pare-feu gérés au format **PDF/CSV**. Vous pouvez appliquer des filtres pour créer des sorties du tableau de configuration plus précises, par exemple, pour effectuer des audits. Seules les colonnes qui sont visibles dans l’interface Web seront exportées. Reportez-vous à la section Exportation du tableau de configuration.
Déployer la clé principale	Déployez une nouvelle clé principale ou mettez à jour une clé principale existante d’un ou de plusieurs périphériques.
Demander l'OTP au CSP	Générez le One-Time Password (mot de passe à usage unique ; OTP) pour les pare-feux gérés. • **Custom selected devices (Appareils sélectionnés personnalisés)** : générez un OTP pour les pare-feu gérés sélectionnés afin d'installer un certificat d'appareil afin de tirer parti des services cloud de Palo Alto Networks. • **Select all devices without a certificate (Sélectionnez tous les appareils sans certificat)** : générez un OTP pour tout pare-feu géré sans certificat d'appareil installé avec succès afin de tirer parti des services cloud de Palo Alto Networks.
Télécharger OTP	Collez l'OTP généré à partir du portail de support client pour installer un certificat de périphérique pour tous les pare-feu gérés.

Informations sur les pare-feu gérés

Sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)** pour afficher les informations suivantes pour chacun des pare-feu gérés.

Informations sur les pare-feu gérés	Description
Groupe de périphériques	Affiche le nom du groupe de périphériques dont le pare-feu est membre. Cette colonne est masquée par défaut, mais vous pouvez l'afficher en cliquant sur la liste déroulante dans un en-tête de colonne et en sélectionnant **Columns (Colonnes)** > **Device Group (Groupe de périphériques)**. La page affiche les pare-feu dans des clusters en fonction de leur groupe de périphériques. Chaque cluster comporte une ligne d'en-tête qui indique le nom du groupe de périphériques, le nombre total de pare-feu affectés, le nombre de pare-feu connectés, et le chemin du groupe de périphériques dans la hiérarchie. Par exemple, **Data center (2/4 Devices Connected) (Centre de données (2/4 périphériques connectés)) : Shared (Partagé)** > **Europe** > **Data center (Centre de données)** signifie qu'un groupe de périphériques nommé **Data center (Centre de données)** comporte quatre pare-feu membres (dont deux sont connectés) et qu'il est un enfant d'un groupe de périphériques nommé **Europe**. Vous pouvez réduire ou développer n'importe quel groupe de périphériques pour masquer ou afficher ses pare-feu.
Nom du périphérique	Affiche le nom d'hôte ou le numéro de série du pare-feu. Pour le pare-feu VM-Series édition NSX, le nom de pare-feu s'ajoute au nom d'hôte du hôte ESXi. Par exemple, PA-VM: host-NY5105
Virtual System (système virtuel - vsys)	Répertorie les systèmes virtuels disponibles sur un pare-feu en mode Plusieurs systèmes virtuels.
Modèle	Affiche le modèle du pare-feu.
Étiquettes	Affiche les étiquettes définies pour chaque pare-feu/système virtuel.
Numéro de série	Affiche le numéro de série du pare-feu.
Mode opérationnel	Affiche le mode opérationnel du pare-feu. Il peut s'agir de FIPS-CC ou Normal.
Adresse IP	Affiche l'adresse IP du pare-feu/système virtuel.
	IPv4 : adresse IPv4 du pare-feu/système virtuel.
	IPv6 : adresse IPv6 du pare-feu/système virtuel.
Variables	Crée des définitions de variables de périphérique spécifiques en les copiant d'un périphérique qui se trouve dans la pile de modèles, ou modifie des définitions de variables existantes afin de créer des variables uniques au périphérique. Cette colonne sera vide si le périphérique n'est pas associé à une pile de modèles. Par défaut, les

Informations sur les pare-feu gérés	Description
	variables sont héritées de la pile de modèles. Reportez-vous à la section Créer ou modifier les définitions de variables sur un appareil.
Modèle	Affiche la pile de modèles à laquelle le pare-feu appartient.
Status (État)	**État du périphérique** : indique l'état de la connexion entre Panorama et le pare-feu. Connecté ou déconnecté. Un pare-feu VM-Series peut présenter deux autres états : • **Désactivé** : indique que vous avez désactivé une machine virtuelle, soit directement sur le pare-feu, soit en sélectionnant **Deactivate VMs (Désactiver la VM)**(**Panorama** > **Device Deployment (Déploiement du périphérique)** > **Licenses (Licences)**) et supprimé toutes les licences et tous les droits sur le pare-feu. Un pare-feu désactivé n'est plus connecté à Panorama car le processus de désactivation supprime le numéro de série sur le pare-feu VM-Series. • **Partiellement désactivé** : indique que vous avez lancé le processus de désactivation de licence à partir de Panorama, mais que le processus n'est pas terminé car le pare-feu est hors ligne et que Panorama ne peut pas communiquer avec lui.
	État HA : indique si le pare-feu est : • **Actif** - État opérationnel de gestion du trafic normal. • **Passif** - État de sauvegarde normal. • **En cours d'initialisation** - Le pare-feu est dans cet état pendant 60 secondes maximum après le démarrage. • **Non fonctionnel** - État d'erreur. • **Suspendu** - Un administrateur a désactivé le pare-feu. • **Provisoire** - Pour un événement de surveillance des liaisons ou des chemins dans une configuration active/active.
	Politique partagée : indique si les configurations de politique et d'objet sur le pare-feu sont synchronisées avec Panorama.
	Modèle - Indique si les configurations réseau et de périphérique sur le pare-feu sont synchronisées avec Panorama.
État (suite)	**Certificat** – indique l'état du certificat client du périphérique géré. • **Prédéfini** – le périphérique géré utilise un certificat prédéfini pour s'authentifier avec Panorama. • **Déployé** – le certificat personnalisé est déployé avec succès sur le périphérique géré.

Informations sur les pare-feu gérés	Description
	• **Expire dans X jours X heures** – le certificat actuellement installé expire dans moins de 30 jours. • **Expire dans X minutes** – le certificat actuellement installé expire dans moins d'un jour. • **Vérification de l'identité du client réussie** – le nom commun du certificat correspond au numéro de série du périphérique de connexion. • **État OCSP inconnu** – Panorama ne parvient pas à obtenir le statut OCSP du répondeur OCSP. • **État OCSP non disponible** – Panorama ne parvient pas à contacter le répondeur OCSP. • **État CRL inconnu** – Panorama ne parvient pas à obtenir l'état de révocation de la base de données CRL. • **État CRL non disponible** – Panorama ne parvient pas à contacter la base de données CRL.
	• **État OCSP/CRL inconnu** – Panorama ne parvient pas à obtenir l'état OCSP ou de révocation lorsqu'ils sont tous les deux activés. • **État OCSP/CRL non disponible** – Panorama ne parvient pas à contacter la base de données OCSP ou CRL lorsqu'ils sont tous les deux activés. • **Émetteur non approuvé** – le périphérique géré dispose d'un certificat personnalisé, mais le serveur ne le valide pas. **État de la dernière validation** - Indique si la dernière validation a réussi ou non sur le pare-feu.
Version du logiciel | Applications et menaces | Antivirus | Filtrage des URL | Client GlobalProtect™ | WildFire	Affiche les versions logicielle et du contenu installées actuellement sur le pare-feu. Pour plus de détails, voir Mises à jour logicielles ou de contenu du pare-feu.
Sauvegardes	À chacune des validations du pare-feu, PAN-OS envoie automatiquement une sauvegarde de la configuration du pare-feu à Panorama. Cliquez sur **Manage (Gérer)** pour afficher les sauvegardes de configuration disponibles et, si vous le souhaitez, en charger une. Pour plus de détails, voir Sauvegardes de pare-feu.
Dernière clé principale transmise	Affiche l'état du déploiement de clé principale de Panorama au pare-feu.

Informations sur les pare-feu gérés	Description
	État : affiche l'état de la dernière transmission de la clé principale. L'état peut être `Success` ou `Failed`. `Unknown` s'affiche si aucune clé principale n'a été transmise au pare-feu depuis Panorama.
	Horodatage : affiche la date et l'heure de la dernière transmission de clé principale depuis Panorama.
Conteneurs : Si vous avez déployé le pare-feu CN-Series pour sécuriser les charges de travail de votre application conteneurisée sur des clusters Kubernetes, utilisez les colonnes suivantes.	
Nombre de nœuds du conteneur	Affiche le nombre de plans de données de pare-feu conteneurisés (CN-NGFW) qui sont connectés au Plan de gestion (CN-Mgmt) enregistré sur Panorama. La valeur peut être entre 0 et 30 cosses CN-NGFW pour chaque paire de cosses CN-Mgmt.
Notes de conteneur	Utilisation

Créer une définition de variable de périphérique

Lors du premier ajout d'un périphérique à une pile de modèles, vous avez la possibilité de créer des définitions de variables propres au périphérique que vous copiez à partir des périphériques qui se trouvent dans la pile de modèles. Vous pouvez également modifier les définitions des variables du modèle via **Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)**. Par défaut, toutes les définitions des variables sont héritées de la pile de modèles et vous ne pouvez remplacer (non pas supprimer) les définitions des variables d'un périphérique individuel. Vous pouvez vous servir de variables pour remplacer des objets d'adresses IP et des littéraux d'adresse IP (masque réseau IP, plage d'adresses IP, FQDN) dans toutes les zones de la configuration, des interfaces de la configuration de la passerelle IKE (Interface) et de la configuration HA (ID du groupe).

Informations sur la création d'une définition de variable de périphérique	Description
Cloner la définition de la variable du périphérique à partir d'un autre périphérique qui se trouve dans la pile de modèles ?	
Non	Affichez les définitions de variables existantes et modifiez-les au besoin. Voir Panorama > Modèles > Variables des modèles.
Oui	Sélectionnez un périphérique dans la liste déroulante à partir duquel cloner les définitions de variables, puis sélectionnez les définitions des variables que vous souhaitez cloner.

Mises à jour logicielles et de contenu du pare-feu

Pour installer une mise à jour logicielle ou de contenu sur un pare-feu géré, utilisez d'abord les pages **Panorama** > **Device Deployment (Déploiement du périphérique)** pour télécharger ou charger la mise à jour sur Panorama. Ensuite, sélectionnez la page **Panorama** > **Managed Devices (Périphériques gérés)**, cliquez sur **Install (Installer)** et complétez les champs suivants.

Pour réduire le trafic sur l'interface de gestion (MGT), vous pouvez configurer Panorama pour utiliser une interface distincte pour le déploiement de mises à jour (voir Panorama > Configuration > Interfaces*).*

Options d'installation des mises à jour logicielles / de contenu sur le pare-feu	Description
Type	Sélectionnez le type de mise à jour à installer. **Software (Logiciel)** PAN-OS, logiciel **GlobalProtect Client (Client GlobalProtect)**, signatures **Apps and Threats (Applications et menaces)**, signatures **Antivirus**, **WildFire** ou **URL Filtering (Filtrage des URL)**.
Classification	Sélectionnez l'image de mise à jour. La liste déroulante inclut uniquement des images que vous avez téléchargées ou chargées sur Panorama à l'aide des pages **Panorama** > **Device Deployment (Déploiement de périphérique)**.
Filtres	Sélectionnez Filtres pour filtrer la liste Périphériques.
Périphériques	Sélectionnez les pare-feu sur lesquels vous souhaitez installer l'image.
Nom du périphérique	Le nom du pare-feu.
Version actuelle	La version de mise à jour du **Type** sélectionné qui est actuellement installée sur le pare-feu.
État HA	Indique si le pare-feu est : • **Actif** - État opérationnel de gestion du trafic normal. • **Passif** - État de sauvegarde normal. • **En cours d'initialisation** - Le pare-feu est dans cet état pendant 60 secondes maximum après le démarrage. • **Non fonctionnel** - État d'erreur. • **Suspendu** - Un administrateur a désactivé le pare-feu. • **Provisoire** - Pour un événement de surveillance des liaisons ou des chemins dans une configuration active/active.
Regrouper les homologues HA	Sélectionnez pour regrouper les pare-feu homologues dans une configuration haute disponibilité (HA).

Options d’installation des mises à jour logicielles / de contenu sur le pare-feu	Description
Filtre sélectionné	Si vous souhaitez que la liste Périphériques n’affiche que des pare-feu spécifiques, sélectionnez les noms des périphériques correspondants et **Filter Selected (Filtre sélectionné)**.
Charger uniquement sur le périphérique	Sélectionnez pour télécharger l’image sur le pare-feu, mais n’activez pas le redémarrage automatique du pare-feu. L’image est installée lorsque vous redémarrez manuellement le pare-feu.
Redémarrer le périphérique après installation (Logiciel seulement)	Sélectionnez pour télécharger et installer l’image du logiciel. Le processus d'installation entraîne un redémarrage.
Désactiver les nouvelles applications dans la mise à jour de contenu (Applications et menaces uniquement)	Sélectionnez pour désactiver des applications de la mise à jour qui sont nouvelles par rapport à la dernière mise à jour installée. Cette façon de procéder vous protège contre les plus récentes menaces en vous offrant la souplesse d’activer les applications après avoir mis à jour les politiques. Ensuite, pour activer les applications, accédez au pare-feu, sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**, cliquez sur **Apps (Applications)** dans la colonne Features (Fonctions) pour afficher les nouvelles applications et cliquez sur **Enable/Disable (Activer / Désactiver)** pour chaque application que vous souhaitez activer.

Sauvegardes du pare-feu

- Panorama > Périphériques gérés

Panorama sauvegarde automatiquement chaque modification de la configuration que vous avez validée sur des pare-feu gérés. Pour gérer les sauvegardes sur un pare-feu, sélectionnez **Panorama** > **Managed Devices (Périphériques gérés)**, cliquez sur **Manage (Gérer)** dans la colonne Sauvegardes du pare-feu et exécutez l’une des tâches suivantes.

*Pour configurer le nombre de versions de sauvegarde de configuration du pare-feu à conserver sur Panorama, sélectionnez **Panorama** > **Setup (Configuration)** > **Management (Gestion)**, modifiez les Paramètres de journalisation et de génération de rapports, sélectionnez **Log Export and Reporting (Exportation et génération de rapports de journaux)** et saisissez le **Number of Versions for Config Backups (Nombre de versions pour les sauvegardes de configuration)** (la valeur par défaut est 100).*

Tâche	Description
Affiche des détails sur la configuration sauvegardée ou validée.	Dans la colonne Version correspondant à la sauvegarde, cliquez sur le fichier de configuration sauvegardé ou le numéro de

Tâche	Description
	version de configuration validé pour afficher le contenu du fichier XML associé.
Rétablissez une configuration sauvegardée ou validée vers la configuration candidate.	Dans la colonne Action correspondant à la sauvegarde, cliquez sur **Load (Charger)** et sur **Commit (Valider)**. Le chargement de la configuration du pare-feu rappelle la configuration du périphérique local et ne rappelle pas la configuration validée dans Panorama. Après avoir **Load (Téléchargé)** la sauvegarde du pare-feu, vous devez context switch (commuter le contexte) vers l'interface web du pare-feu oulaunch the firewall web interface (lancer l'interface web du pare-feu) pour **Commit (Valider)**.
Supprimer une configuration sauvegardée.	Dans la colonne Action correspondant à la sauvegarde, cliquez sur Supprimer (✕).

Panorama > Quarantaine du périphérique

La page **Panorama** > **Device Quarantine (Quarantaine des périphériques)** affiche les périphériques qui sont sur la liste de quarantaine. Les périphériques qui apparaissent dans cette liste suite aux actions suivantes :

- L'administrateur du système a ajouté le périphérique à cette liste manuellement.

  Afin de manuellement **Add (Ajouter)** un périphérique, saisissez le **Host ID** et, en option, le **Serial Number (Numéro de série)** du périphérique que vous devez mettre en quarantaine.
- L'administrateur du système a sélectionné la colonne d'identifiant de l'hôte depuis les journaux de Trafic, GlobalProtect ou des menaces, a sélectionné un périphérique dans cette colonne puis a sélectionné **Block Device**.
- Le périphérique a correspondu à une règle de politique de sécurité dont le profil de transfert des journaux possède une liste de correspondance comprenant une action intégrée de mise en **Quarantine (Quarantaine)**.

  *L'identifiant de l'hôte s'affiche dans les journaux GlobalProtect automatiquement. Pour que l'identifiant de l'hôte s'affiche dans les journaux de Trafic, des menaces ou Unifiés, l'appareil Panorama doit avoir au moins une règle de politique de sécurité dans le **Source Device (Périphérique source)** réglée sur **Quarantine (Quarantaine)**. Sans ce réglage dans la politique de sécurité, les journaux de Trafic, menaces ou Unifiés n'auront pas l'identifiant de l'hôte, et le profil de transfert des journaux n'entrera pas en vigueur.*
- L'appareil a été ajouté à la liste de quarantaine à l'aide d'un API.
- L'appareil Panorama a reçu la liste de quarantaine dans le cadre d'une saisie redistribuée (la liste de quarantaine a été redistribuée depuis un autre appareil ou pare-feu Panorama).

Le tableau de Quarantaine des périphériques comprend les champs suivants.

Champ	Description
ID d'hôte	Identifiant (ID) d’hôte de l’hôte qui est bloqué.
Motif	Le motif est que le périphérique est en quarantaine. Un motif **Admin Add (ajout par un admin)** signifie qu’un administrateur a manuellement ajouté le périphérique au tableau.
Horodatage	L’heure à laquelle l’administrateur ou la règle de politique de sécurité a ajouté le périphérique à la liste de quarantaine.
Périphérique/appli source	L’adresse IP de Panorama, du pare-feu ou de l’application tierce qui a ajoutée le périphérique à la liste de quarantaine.
Numéro de série	(En option) Le numéro de série du périphérique en quarantaine (s’il est disponible).
Nom d'utilisateur	(En option) Le nom d'utilisateur du client utilisateur de GlobalProtect qui était connecté au périphérique lorsque celui-ci a été mis en quarantaine.

Panorama > Périphériques gérés > État

Panorama™ vous permet de surveiller les ressources matérielles et la performance des pare-feu gérés. Panorama centralise les informations sur la performance (processeur, mémoire, CPS et débit), sur la performance de journalisation, sur l’environnement (comme les ventilateurs, l’état RAID et l’alimentation) en présentant leur évolution au fil du temps et met en corrélation les événements (comme les validations, les installations de contenu et les mises à niveau logicielles) avec les données sur l’état. Lorsqu’un pare-feu s’écarte de sa base de référence calculée, Panorama le signale comme Périphérique anormal pour aider à identifier, à diagnostiquer et à résoudre rapidement les problèmes matériels.

Vous pouvez utiliser cette page pour effectuer ce qui suit :

Afficher une Vue détaillée de l’état du périphérique.	Afficher les mesures sur l’état des périphériques gérés par Panorama.
Regrouper les homologues HA	Afficher les pare-feu qui sont regroupés pour faciliter l’identification de problèmes éventuels et pour déterminer si les pare-feu sont touchés par des problèmes liés à la performance ou aux ressources matérielles (et le cas échéant, lesquels).
PDF/CSV	Les rôles administrateur qui sont au moins dotés de l’accès en lecture seule peuvent exporter le tableau des pare-feu gérés au format **PDF/CSV**. Vous pouvez appliquer des filtres pour créer des sorties du tableau de configuration plus précises, au besoin, par exemple, pour effectuer des audits. Seules les colonnes qui sont visibles dans l’interface Web sont exportées. Consultez

	la section Exportation des données du tableau de configuration.

Panorama > Périphériques gérés > État > Tous les périphériques

Utilisez cette page pour consulter les informations suivantes pour chaque pare-feu.

Information sur l’état	Description
Nom du périphérique	Nom d’hôte ou numéro de série du pare-feu. Pour le pare-feu VM-Series édition NSX, le nom de pare-feu s'ajoute au nom d’hôte du hôte ESXi. Par exemple, PA-VM: host-NY5105
Modèle	Modèle du pare-feu.
Périphérique	
Débit (kilobits)	Le débit des données au fil du temps (moyenne sur cinq minutes) mesuré en kilobit par seconde.
CPS	Connexions par seconde totales pour le périphérique au fil du temps (moyenne sur cinq minutes).
Session	
Nombre de sessions	Compte de session total au fil du temps (moyenne sur cinq minutes).
Plan de données	
Processeur (%)	Utilisation totale du processeur sur le plan de données.
Plan de gestion	
Processeur (%)	Utilisation totale du processeur sur le plan de gestion.
MEM (%)	Utilisation totale de la mémoire sur le plan de gestion.
Taux de journalisation (journaux par seconde)	Taux de journalisation entrant du pare-feu géré.
Ventilateurs	Présente la présence, l’état actuel, le nombre de tours par minute et le dernier échec des ventilateurs de chaque support de ventilateur. L’état des ventilateurs s’affiche au format *A*/*B*, où *A* correspond au nombre de ventilateurs qui fonctionnent bien et *B* au nombre total de ventilateurs sur le pare-feu. Pour les pare-feu virtuels, `N/A` s'affiche.
Alimentation	Présente la présence, l’état actuel et l’horodatage du dernier échec. L’état de l’alimentation s’affiche au format *A*/*B*, où *A* correspond

Information sur l'état	Description
	au nombre de blocs d'alimentation qui fonctionnent bien et *B* au nombre total de blocs d'alimentation sur le pare-feu. Pour les pare-feu virtuels, `N/A` s'affiche.
du switch	Nombre total de ports utilisés sur le pare-feu. Les ports s'affichent au format *A*/*B*, où *A* correspond au nombre de ports qui fonctionnent bien et *B* au nombre total de ports sur le pare-feu.

Panorama > Périphériques gérés > État > Périphériques anormaux

L'onglet Périphériques anormaux présente les périphériques dont les mesures s'écartent de leur base de référence calculée ; les mesures divergentes sont indiquées en rouge. On obtient la base de référence de l'état de santé en calculant la moyenne de la performance de l'état pour une mesure donnée sur une période de sept jours plus l'écart type.

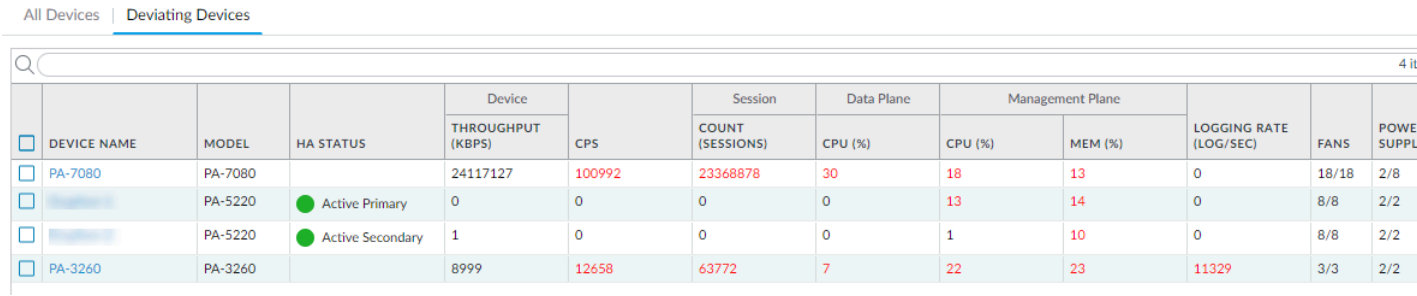


Figure 1: Exemple d'une mesure anormale

État détaillé des périphériques dans Panorama

Vous pouvez afficher un historique de l'état détaillé des périphériques d'un seul pare-feu en cliquant sur le Nom du périphérique dans l'onglet Tous les périphériques ou dans l'onglet Périphériques déviateurs. La Vue détaillée des périphériques présente l'historique de l'état de santé au moyen d'un filtre de temps et affiche les métadonnées associées au périphérique. Les informations sur l'état du périphérique s'affichent sous forme de tableau ou de widget, lorsque possible, afin de fournir une représentation graphique de l'évolution des données dans le temps.

Gestion de la Vue détaillée des périphériques

En plus des métadonnées descriptives associées au pare-feu, la Vue détaillée des périphériques affiche les informations sur l'état détaillé du pare-feu. Le cas échéant, vous pouvez configurer les Paramètres (⚙) des options supplémentaires du widget ou Maximiser le panneau (▭) pour agrandir le widget.

Champ	Description
Actions	
Filtre de temps	Sélectionnez le filtre pour afficher l'historique de l'état des périphériques dans la liste déroulante. Vous pouvez sélectionner

Champ	Description
	12 dernières heures, **24 heures**, **7 jours**, **15 jours**, **30 jours** ou **90 jours**.
Montrer la moyenne	Sélectionnez la moyenne et la distribution traditionnelle présentée pour les widgets dont l'évolution au fil du temps est analysée. Vous pouvez sélectionnez **Aucun**, **24 dernières heures**, **7 jours** ou **15 jours**.
Actualiser	Actualise les informations affichées en y intégrant les données les plus récentes.
Imprimer un PDF	Génère un PDF de l'onglet actuellement affiché. *Les fenêtres contextuelles doivent être activées pour sélectionner l'emplacement du téléchargement et pour accéder au PDF.*
Information système	
Information système	Les métadonnées associées au périphérique : adresse IP, version du logiciel, version de l'antivirus, état HA, numéro de série, version Appplications et menaces, version WildFire, mode VSYS, modèle et mode du périphérique.

Sessions

L'onglet Sessions affiche les informations sur les sessions qui traversent le pare-feu. Ces informations s'affichent sous la forme de six graphiques individuels.

Champ	Description
Débit	Le débit des données au fil du temps (moyenne sur cinq minutes) mesuré en kilobit par seconde (Kbit/s).
Compte de session	Compte de session total au fil du temps (moyenne sur cinq minutes).
Connexions par seconde	Connexions par seconde totales pour le périphérique au fil du temps (moyenne sur cinq minutes).
Paquets par seconde	Paquets par seconde totaux (moyenne sur cinq minutes) qui ont traversé le périphérique.
Pourcentage d'utilisation de la table de sessions	Le pourcentage d'utilisation de la table de sessions globale au fil du temps pour les pare-feu qui disposent d'une table de sessions globale (moyenne sur cinq minutes).

Champ	Description
globale (appareils PA-7000 et PA-5200 uniquement).	
Pourcentage d’utilisation de la table de sessions	Présente le pourcentage d’utilisation de la table de sessions pour chaque panneau de données du pare-feu au fil du temps (moyenne sur cinq minutes).
Informations sur les sessions SSL déchiffrées	Présente le nombre de sessions SSL déchiffrées au fil du temps (moyenne sur cinq minutes).
Pourcentage d’utilisation des sessions de proxy SSL	Présente le nombre de sessions de proxy au fil du temps (moyenne sur cinq minutes).

Environnements

L’onglet **Environnements** affiche la présence, l’état et les conditions de fonctionnement du matériel, par exemple l’alimentation électrique, le support de ventilateur et les disques durs. Cet onglet ne s’affiche que pour les pare-feu matériels :

Champ	Description
État des ventilateurs	Présente la présence, l’état actuel, le nombre de tours par minute et le dernier échec des ventilateurs de chaque support de ventilateur. L’état des ventilateurs s’affiche au format *A*/*B*, où *A* correspond au nombre de ventilateurs qui fonctionnent bien et *B* au nombre total de ventilateurs sur le pare-feu. Pour les pare-feu virtuels, `N/A` s'affiche.
Alimentation	Présente la présence, l’état actuel et l’horodatage du dernier échec. L’état de l’alimentation s’affiche au format *A*/*B*, où *A* correspond au nombre de blocs d’alimentation qui fonctionnent bien et *B* au nombre total de blocs d'alimentation sur le pare-feu. Pour les pare-feu virtuels, `N/A` s'affiche.
État thermique	Indique s’il y a des alarmes thermiques associées à chaque logement du périphérique. S’il existe une alarme active, le pare-feu affiche plus d’informations spécifiques concernant la température exacte et l'emplacement.
État du disque système	Affiche le pourcentage d’utilisation, d’espace disponible et d’espace utilisé sur les supports racine, pancfg, panlogs, and panrepo. L’État du disque système présente également le nom du disque, sa taille et l’état RAID des pare-feu compatibles RAID.

Interfaces

L’onglet Interfaces affiche l’état et les statistiques de l’ensemble des interfaces physiques du pare-feu.

Champ	Description
Nom de l'interface	Le nom de l'interface. Sélectionnez une Interface pour afficher les graphiques Débit binaire, Paquets par seconde, Erreurs et Abandons de l'interface sélectionnée.
État	L'état de l'interface : `Admin Up`, `Admin Down`, `Opérationnel` ou `Non Opérationnel`.
Débit binaire	Affiche le débit binaire (bps) des données reçues et transmises.
Paquets par seconde	Affiche le nombre de paquets par secondes correspondant aux données reçues et transmises.
Erreurs	Affiche le nombre d'erreurs applicables aux données reçues et transmises.
Abandons	Affiche le nombre de connexions abandonnées correspondant aux données reçues et transmises.

de journalisation

L'onglet Journalisation affiche les taux de journalisation et les connexions de l'ensemble des pare-feu gérés.

Champ	Description
Taux de journalisation	Affiche le taux moyen mesuré sur une période d'une minute pour les journaux de transfert vers Panorama ou vers un Collecteur de journaux du périphérique.
Connexions de journalisation	Présente toutes les connexions de transfert des journaux disponibles, y compris leur état actif ou inactif.
Transfert des journaux externe	Affiche le taux d'envoi, d'abandon et de transfert moyen (journaux par seconde) pour diverses méthodes de transfert des journaux externe.

Resources

L'onglet Ressources présente les statistiques relatives à la mémoire et au processeur du pare-feu.

Champ	Description
Mémoire du plan de gestion	Affiche la moyenne sur cinq minutes (selon une évolution au fil du temps) de la mémoire du plan de gestion sous forme de pourcentage.

Champ	Description
Mémoires tampons des paquets	Affiche la moyenne sur cinq minutes (selon une évolution au fil du temps) de l'utilisation de la mémoire tampon des paquets sous forme de pourcentage. Dans un système qui comporte plusieurs plans de données, cette vue présente différents plans de données, processeurs et mémoires tampons des paquets en diverses couleurs.
Descripteurs de paquet	Affiche la moyenne sur cinq minutes (selon une évolution au fil du temps) de l'utilisation du descripteur de paquet sous forme de pourcentage. Dans un système qui comporte plusieurs plans de données, cette vue présente différents plans de données, processeurs et mémoires tampons des paquets en diverses couleurs.
Plan de gestion du processeur	Affiche la moyenne sur cinq minutes (selon une évolution au fil du temps) du processeur sous forme de pourcentage.
Plan de données du processeur	Affiche la moyenne sur cinq minutes (selon une évolution au fil du temps) par utilisation essentielle du plan de données du processeur. Pour les systèmes qui comportent plusieurs plans de données, vous pouvez sélectionner le plan de données à afficher.
Supports	Affiche les informations sur le fichier système du périphérique. Le Nom du support, l'espace alloué (en Ko), l'espace utilisé (en Ko), et l'espace disponible (en Ko) ainsi que le pourcentage d'utilisation s'affichent.

Haute disponibilité

L'onglet Haute disponibilité présente l'état HA du pare-feu et de son homologue HA. Le widget supérieur affiche la configuration et la version de contenu du périphérique et de ses homologues. Le widget inférieur fournit des informations sur les basculements HA antérieurs ainsi que les motifs qui y sont associés et indique notamment le pare-feu qui a échoué.

Panorama > Modèles

Grâce aux onglets **Périphérique** et **Réseau**, vous pouvez déployer une configuration à base commune sur plusieurs pare-feu nécessitant des paramètres similaires à l'aide d'un modèle ou d'une pile de modèles (une combinaison de modèles). Lors de la gestion des configurations de pare-feu avec Panorama, vous utilisez une combinaison de groupe de périphériques (pour gérer les politiques et objets partagés) et de modèles (pour gérer les paramètres de périphérique et de réseau partagés).

En plus des paramètres disponibles depuis les boîtes de dialogue pour la création de Modèles ou de Piles de modèles, **Panorama** > **Modèles** affiche les colonnes suivantes :

- **Type** - Identifie les entrées qui sont figurent en tant que modèles ou piles de modèles.
- **Pile** - Énumère les modèles assignés à une pile de modèles.

Que souhaitez-vous faire ?	Reportez-vous à la section :
Ajouter, cloner, éditer ou supprimer un modèle	Modèles
Ajouter, modifier ou supprimer une pile de modèles	Piles de Modèles
Vous souhaitez en savoir plus ?	Modèles et piles de modèle
	Gérer les modèles et les piles de modèle

Modèles

Panorama prend en charge jusqu'à 1 024 modèles. Vous pouvez **Add (Ajouter)** un modèle et configurer les paramètres comme décrit dans le tableau suivant. Après avoir créé un modèle, vous devez également configurer une pile de modèles et ajouter les modèles et les pare-feu à la pile de modèles avant de pouvoir gérer vos pare-feu. Après avoir configuré un modèle, vous devez valider vos modifications dans Panorama (reportez-vous à la section Opérations de validation de Panorama).

La suppression d'un modèle n'entraînera pas la suppression des valeurs appliquées par Panorama au pare-feu.

Paramètres du modèle	Description
Nom	Donnez un nom au modèle (63 caractères maximum). Le nom est sensible à la casse, doit être unique et peut inclure uniquement des lettres, chiffres, espaces, traits d'union, points et traits de soulignement. Dans les onglets **Périphérique** et **Réseau**, ce nom apparaît dans la liste déroulante **Modèle.** Les paramètres que vous modifiez dans ces onglets s'appliquent uniquement au **Template (Modèle)** sélectionné.

Paramètres du modèle	Description
Description	Saisissez une description du modèle.

Piles de Modèles

Vous pouvez configurer une pile de modèles ou affecter des modèles à une pile de modèles. L'affectation de pare-feu à une piles de modèles vous permet de transmettre tous les paramètres nécessaires aux pare-feu plutôt que de devoir ajouter chaque paramètre à chaque modèle de manière individuelle. Panorama prend en charge jusqu'à 1 024 piles. Vous pouvez **Add Stack (Ajouter une pile)** pour créer une nouvelle piles de modèles et configurer les paramètres comme décrit dans le tableau suivant. Après avoir configuré une piles de modèles, vous devez valider vos modifications dans Panorama (reportez-vous à la section Opérations de validation de Panorama). De plus, après avoir configuré les paramètres du réseau et du périphérique des pare-feu affectés à la pile, vous devez effectuer une validation du modèle pour appliquer les paramètres aux pare-feu.

La suppression d'une pile de modèles ou la suppression d'un pare-feu d'une pile de modèles ne supprime pas les valeurs que Panorama a précédemment envoyées à ce pare-feu. Toutefois, lorsque vous supprimez un pare-feu d'une pile de modèles, Panorama n'envoie plus de nouvelles mises à jour à ce pare-feu.

Paramètres de la pile de modèles	Description
Name (Nom)	Donnez un nom à la pile (31 caractères maximum). Le nom est sensible à la casse, doit être unique, doit commencer par une lettre et ne peut contenir que des lettres, des chiffres et des caractères de soulignement. Dans les onglets **Device (Périphérique)** et **Network (Réseau)**, la liste déroulante **Template (Modèle)** affiche le nom de la pile et les modèles qui lui sont affectés.
Description	Saisissez une description de la pile.
Transférer automatiquement le contenu lorsque le périphérique logiciel s'enregistre dans Panorama	Activez cette option lors de l'intégration de pare-feu VM-Series ou CN-Series sur Panorama pour envoyer automatiquement les dernières mises à jour de contenu aux pare-feu.
Modèles	Vous pouvez **Ajouter** chaque modèle que vous voulez inclure dans la pile (jusqu'à 8). Si des modèles comportent des paramètres en double, Panorama n'applique que les paramètres du modèle le plus haut dans la liste lorsqu'il applique les paramètres aux pare-feu affectés. Par exemple, si Modèle_A est situé au-dessus de Modèle_B dans la liste et que les deux modèles définissent l'interface ethernet1/1, Panorama applique alors la définition ethernet1/1 du Modèle_A et non celle du Modèle_B. Pour modifier l'ordre des modèles dans la

Paramètres de la pile de modèles	Description
	liste, vous devez sélectionner un modèle et **Move Up (Déplacer en haut)** ou **Move Down (Déplacer en bas)**. *Panorama ne valide pas les combinaisons de modèles dans les piles, planifiez donc l'ordre de vos modèles pour éviter de générer des relations incorrectes.*
Périphériques	Sélectionnez chacun des pare-feu que vous voulez ajouter à la pile. Si la liste de pare-feu est longue, vous pouvez la filtrer par **Platforms (Plates-formes)**, **Device Groups (Groupes de périphériques)**, **Tags (Étiquettes)** ou **HA Status (État HA)**. *Vous pouvez affecter des pare-feu dont les modes ne correspondent pas (VPN, systèmes virtuels multiples ou opérationnel) à la même pile. Panorama applique les paramètres spécifiques des modes aux pare-feu prenant en charge ces modes uniquement.*
Sélectionner tout	Sélectionne chacun des pare-feu qui figurent dans la liste.
Désélectionner tout	Sélectionne chacun des pare-feu qui figurent dans la liste.
Regrouper les homologues HA	Regroupe les pare-feu qui sont des homologues haute disponibilité (HA). Cela vous permet d'identifier facilement les pare-feu présentant une configuration HA. Lors de l'application des paramètres de la pile de modèles, vous pouvez les appliquer à la paire regroupée plutôt qu'à chaque des pare-feu individuellement.
Filtre sélectionné	Pour n'afficher que des pare-feu spécifiques, sélectionnez-les, puis l'option **Filter Selected (Filtre sélectionné)**.
Périphérique principal de User-ID	Configurez Panorama en tant que périphérique maître d'ID utilisateur pour les mappages.
Moteur d'identité sur le cloud	**Ajoutez** une instance Cloud Identity Engine pour authentifier les utilisateurs à l'aide du profil d'authentification que vous configurez dans Cloud Identity Engine.
Modèles	**Ajouter** ou **supprimer** un modèle préconfiguré. **Déplacez vers le haut** ou **déplacez vers le bas** les modèles pour modifier la priorité. Le modèle en haut a la priorité la plus élevée.

Panorama > Modèles > Variables des modèles

- Création de nouvelles variables de modèles
- Modifier les variables de modèles existantes
- Créer ou modifier les définitions de variables sur un périphérique

Vous pouvez définir des variables (**Panorama** > **Templates (Modèles)**) pour des modèles ou des piles de modèles ou vous pouvez modifier les variables existantes d'un appareil individuel (**Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)**). Les variables sont des éléments de la configuration définis sur le modèle ou sur la pile de modèles qui procurent souplesse et la possibilité de réutilisation lorsque vous utilisez Panorama pour gérer les configurations d'un pare-feu. Vous pouvez utiliser les variables pour remplacer :

- Une adresse IP (notamment un masque réseau IP, une plage d'adresses IP et un FQDN) dans toutes les zones de configuration.
- Des interfaces dans une configuration de passerelle IKE (Interface) et dans une configuration HA (ID du groupe).
- Eléments de configuration de votre configuration SD-WAN (Numéro AS, Profil QoS, Sortie max., Étiquette de liens).

Lorsque vous ajoutez des pare-feu à une piles de modèles, ceux-ci héritent automatiquement des variables que vous avez créées pour un modèle ou une piles de modèles.

Informations sur les variables des modèles	Description
Name (Nom)	Nom de la définition de la variable.
Modèle (périphérique et piles de modèles)	Affiche le nom du modèle auquel la définition de la variable appartient.
Type	Affiche le type de définition de la variable : • **IP Netmask (Masque réseau IP)** : définit une adresse ou une adresse IP statique. • **IP Range (PLage d'adresses IP)** Range IP : définir une plage d'adresses IP. Par exemple, 192.168.1.10-192.168.1.20. • **FQDN (FQDN)** : définit un Fully Qualified Domain Name (nom de domaine complet ; FQDN). • **Group ID (ID du groupe)** : définit l'ID du groupe haute disponibilité. Pour obtenir de plus amples renseignements, reportez-vous à la section Directives concernant les configurations HA actives/passives. • **Priorité du périphérique** : Définissez la priorité du périphérique afin d'indiquer une préférence pour laquelle un pare-feu doit assumer un rôle dans une configuration de haute disponibilité (HA) active-passive.

Informations sur les variables des modèles	Description
	• **Device ID (ID du périphérique)**: Définissez l'IDE du périphérique à utiliser pour attribuer une valeur de priorité de périphérique dans une configuration de haute disponibilité (HA) active-passive. • **Interface** : définit une interface de pare-feu sur le pare-feu. Ne peut être utilisée que pour une configuration de passerelle IKE. • **AS Number (Numéro AS)** : Définissez un numéro de système autonome à utiliser dans votre configuration BGP. • **QoS Profile 'Profile QoS)**: Définissez un profil Quality of Service (Qualité de service - QoS) à utiliser dans les configurations. • **Egress Max (Sortie max.)** : Définissez une valeur de sortie max. à utiliser dans la configuration de profil QoS. • **Link Tag (Étiquette de liens)** : Définissez une étiquette de liens à utiliser dans votre configuration SD-WAN.
Valeur	Affiche la valeur qui a été configurée pour la définition de la variable.
Ajouter (modèle et piles de modèles)	Ajoute une nouvelle définition de la variable d'un modèle.
Supprimer	Supprime une définition de variable d'un modèle existante.
Cloner	Clone une définition de variable d'un modèle existante.
Remplacer (pile de modèles et périphérique)	Remplace la définition d'une variable d'un modèle existante héritée de la pile de modèles ou du périphérique. Vous ne pouvez modifier le nom de la variable, ni son type, et vous ne pouvez pas remplacer les variables propres aux périphériques.
Rétablir (pile de modèles et périphérique)	Pour supprimer les valeurs remplacées au niveau de la pile de modèles ou du périphérique ; rétablit la variable remplacée par la définition de la variable du modèle initiale.
Obtenir les valeurs utilisées sur le périphérique uniquement (périphérique uniquement)	Renseigne la variable sélectionnée par la valeur utilisée sur le pare-feu. Il faut que la variable d'un modèle ou d'une pile de modèles soit déjà définie et appliquée au pare-feu avant que Panorama puisse récupérer la valeur. Les valeurs tirées du pare-feu **Override (remplaceront)** la variable du modèle ou de la pile de modèles afin de créer une variable propre au périphérique. Si aucune définition de variable n'a été appliquée au pare-feu, Panorama renvoie le message `Value not found` pour cette variable.

Création de nouvelles variables de modèles

Add (Ajoutez) une nouvelle définition de la variable d'un modèle.

Informations sur la définition d'une nouvelle variable d'un modèle	Description
Name (Nom)	Nommez la définition de la variable. Tous les noms des définitions de variables doivent commencer par le symbole du dollar ($).
Type	Sélectionnez le type de définition de la variable : **IP Netmask (Masque réseau de l'IP)**, **IP Range (Fourchette d'IP)**, **FQDN**, **Group ID (ID de groupe)**, **Device Priority (Priorité du périphérique)**, **Device ID (ID du périphérique)**, **Interface**, **AS Number (Numéro AS)**, **QoS Profile (Profil QoS)**, **Egress Max (Sortie max.)**, ou **Link Tag (Étiquette de liens)**.
Valeur	Entrez la valeur souhaitée pour la définition de la variable.

Modifier les variables de modèles existantes

Vous pouvez modifier la définition d'une variable d'un modèle en tout temps après la création de la variable (**Panorama** > **Templates (Modèles)**). **Manage (Gérez)** les variables du modèle pour sélectionner une variable et modifier les valeurs disponibles, au besoin.

Créer ou modifier les définitions de variables sur un périphérique

Allez à **Panorama** > **Managed Devices (Périphériques gérés)** > **Summary (Récapitulatif)** pour créer des définitions de variables ou pour remplacer des variables de modèles qui ont été appliquées à partir d'un modèle ou d'une pile de modèles Panorama. Voici des exemples de variables de modèles :

- Une adresse IP (masque réseau IP, plage d'adresses IP ou FQDN) dans toutes les zones de configuration.
- Des interfaces dans une configuration de passerelle IKE (Interface) ou dans une configuration HA (ID du groupe).
- Eléments de configuration de votre configuration SD-WAN (Numéro AS, Profil QoS, Sortie max., Étiquette de liens).

La création d'une variable de périphérique vous permet de copier des variables propres à un périphérique qui ont été remplacées à partir d'un périphérique qui se trouve dans la même pile de modèles sans que vous ayez à les créer de nouveau. Par défaut, toutes les définitions des variables sont héritées du modèle ou de la piles de modèles et ne peuvent être remplacées (vous ne pouvez pas supprimer les définitions des variables d'un périphérique individuel ni en créer de nouvelles).

Create (Créez) des définitions de variables de périphérique en copiant des définitions de variables à partir des périphériques qui se trouvent dans la pile de modèles ou **Edit (Modifiez)** les définitions de variables existantes.

Panorama > Groupes de périphériques

Les groupes de périphériques sont constitués de pare-feu et de systèmes virtuels que vous souhaitez gérer en tant que groupe, tels que les pare-feu qui gèrent un groupe de succursales ou de services dans une entreprise. Panorama traite ces groupes comme des unités individuelles lors de l'application de politiques. Un pare-feu ne peut appartenir qu'à un seul groupe de périphériques. Cependant, les systèmes virtuels étant des entités distinctes dans Panorama, vous pouvez attribuer des systèmes virtuels d'un pare-feu à différents groupes de périphériques.

Vous pouvez imbriquer des groupes de périphériques à une hiérarchie d'arborescence pouvant comporter jusqu'à quatre niveaux sous l'emplacement partagé afin de mettre en œuvre une approche en couche pour gérer les politiques au sein de votre réseau de pare-feu. Au niveau inférieur, un groupe de périphériques peut avoir des groupes de périphériques parents, grands-parents et arrière-grands-parents à des niveaux supérieurs successifs (collectivement appelés *anciens*) dont le groupe de périphériques de niveau inférieur hérite des politiques et objets. Au niveau supérieur, un groupe de périphériques peut avoir des groupes de périphériques enfants, petits-enfants et arrière-petits-enfants — collectivement appelés *descendants*. Lorsque vous sélectionnez **Panorama** > **Device Groups (Groupes de périphériques)**, la colonne Nom affiche cette hiérarchie de groupe de périphériques.

Après avoir ajouté, modifié ou supprimé un groupe de périphériques, vous devez effectuer une validation de Panorama et une validation du groupe de périphériques (reportez-vous à la section Opérations de validation de Panorama). Panorama diffuse ensuite les modifications de configuration aux pare-feu affectés au groupe de périphériques. Panorama prend en charge jusqu'à 1 024 groupes de périphériques.

Pour configurer un groupe de périphériques, vous devez en **Ajouter** un et configurer les paramètres comme décrit dans le tableau suivant.

Paramètres du groupe de périphériques	Description
Name (Nom)	Saisissez un nom pour identifier le groupe (31 caractères maximum). Le nom est sensible à la casse, doit être unique sur l'ensemble de la hiérarchie du groupe de périphériques et ne peut contenir que des lettres, des chiffres, des espaces, des points, des traits d'union et des caractères de soulignement.
Description	Saisissez une description du groupe de périphérique.
Périphériques	Sélectionnez chacun des pare-feu que vous voulez ajouter au groupe de périphériques. Si la liste de pare-feu est longue, vous pouvez filtrer par **Device State (État du périphérique)**, **Platforms (Plates-formes)**, **Templates (Modèles)** ou **Tags (Étiquettes)**. La section Filtres affiche (entre parenthèses) le nombre de pare-feu gérés pour chacune de ces catégories. Si l'objectif d'un groupe de périphériques est purement organisationnel (à savoir qu'il est conçu pour contenir d'autres groupes de périphériques), vous ne devez pas nécessairement lui affecter des pare-feu.
Sélectionner tout	Sélectionne chaque pare-feu et système virtuel de la liste.

Paramètres du groupe de périphériques	Description
Désélectionner tout	Désélectionne chaque pare-feu et système virtuel de la liste.
Regrouper les homologues HA	Sélectionnez pour regrouper les pare-feu homologues dans une configuration haute disponibilité (HA). La liste affiche alors le pare-feu actif (ou actif/principal dans une configuration active/active), suivi du pare-feu passif (ou actif/secondaire dans une configuration active/active) entre parenthèses. Ceci vous permet d'identifier facilement les pare-feu en mode HA. Lors de l'application de politiques partagées, vous pouvez l'appliquer à la paire regroupée plutôt qu'à chaque homologue. *Pour les homologues HA dans une configuration active/passive, pensez à ajouter les deux pare-feu ou leurs systèmes virtuels au même groupe de périphériques. Ceci vous permet d'appliquer la configuration aux deux homologues simultanément.*
Filtre sélectionné	Si vous souhaitez que la liste Périphériques n'affiche que des pare-feu spécifiques, sélectionnez les pare-feu, puis **Filter Selected (Filtre sélectionné)**.
Groupe de périphériques parent	En fonction du groupe de périphériques que vous définissez, sélectionnez le groupe de périphériques (ou l'emplacement Partagé) situé juste au-dessus de lui dans la hiérarchie (**Shared (Partagé)** est défini par défaut).
Périphérique principal	Pour configurer les règles de politique et les rapports en fonction des noms d'utilisateur et des groupes d'utilisateurs, vous devez sélectionner un **Master Device (Périphérique principal)**. Il s'agit du pare-feu à partir duquel Panorama reçoit des noms d'utilisateur, des noms de groupe d'utilisateurs et des informations de mappage de nom d'utilisateur à un groupe. *Lorsque vous modifiez le **Master Device (Périphérique principal)** ou que vous le configurez sur **None (Aucun)**, Panorama perd toutes les informations d'utilisateur et de groupe reçues par ce pare-feu.*
Stocker les utilisateurs et les groupes à partir du périphérique principal	Cette option s'affiche uniquement si vous sélectionnez un **Master Device (Périphérique principal)**. L'option permet à Panorama de stocker localement les noms d'utilisateur, les noms des groupes d'utilisateurs et les informations de mappage de nom d'utilisateur à un groupe qu'il reçoit par le **Master Device (Périphérique principal)**. Pour activer le stockage local, vous devez également sélectionner **Panorama** > **Setup (Configuration)** > **Management (Gestion)**, modifier les paramètres de Panorama et Activer les rapports et le filtrage sur les groupes.
Propriétés du périphérique ajoutées dynamiquement – Lorsqu'un nouveau périphérique est ajouté au groupe de périphériques, Panorama applique dynamiquement le code d'autorisation spécifié et la	

Paramètres du groupe de périphériques	Description
version du logiciel PAN-OS au nouveau périphérique. Cela s’affiche uniquement après qu’un groupe de périphériques a été associé à une définition de service NSX dans Panorama.	
Code d'autorisation	Saisissez le code d’autorisation à appliquer aux périphériques ajoutés à ce groupe de périphériques.
Version du logiciel	Sélectionnez la version de logiciel à appliquer aux périphériques ajoutés à ce groupe de périphériques.

Panorama > Collecteurs gérés

Le serveur de gestion Panorama (appareil de série M ou appareil virtuel Panorama en mode Panorama) peut gérer les Collecteurs de journaux dédiés (appareils de série M ou appareil virtuel Panorama en mode Collecteur de journaux). Chaque serveur de gestion Panorama possède également un Collecteur de journaux local prédéfini (nommé par défaut) afin de traiter les journaux qu'il reçoit directement depuis les pare-feu. (Un équipement virtuel Panorama en Mode hérité stocke les journaux reçus directement des pare-feu sans utiliser un collecteur de journaux dédié.)

Si vous souhaitez utiliser Panorama pour la gestion d'un collecteur de journaux dédié, vous devez ajouter le collecteur de journaux en tant que *collecteur géré*.

Que souhaitez-vous faire ?	Reportez-vous à la section :
Afficher les informations des collecteurs de journaux	Informations sur les collecteurs de journaux
Ajouter, modifier ou supprimer un Collecteur de journaux	Configuration du Collecteur de journaux
Mettre à jour le logiciel Panorama sur un Collecteur de journaux	Mises à jour logicielles pour les collecteurs de journaux dédiés
Vous souhaitez en savoir plus ?	Journalisation centralisée et génération de rapports
	Configurer un collecteur géré

Informations sur les collecteurs de journaux

Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** pour afficher les informations suivantes pour les Collecteurs de journaux. Vous pourrez configurer d'autres paramètres lors de la Configuration du Collecteur de journaux.

Informations sur les collecteurs de journaux	Description
Nom du collecteur	Le nom qui identifie ce collecteur de journaux. Ce nom s'affiche en tant que nom d'hôte du collecteur de journaux.
Numéro de série	Le numéro de série de l'équipement Panorama qui agit en tant que Collecteur de journaux. Si le Collecteur de journaux est local, il s'agit du numéro de série du serveur de gestion Panorama.

Informations sur les collecteurs de journaux	Description
Version du logiciel	La version du logiciel Panorama installée sur le collecteur de journaux.
Adresse IP	L’adresse IP de l’interface de gestion installée sur le collecteur de journaux.
Connected (Connecté)	L'état de la connexion établie entre le collecteur de journaux et Panorama.
État/Détail de la configuration	Indique si la configuration sur le collecteur de journaux est synchronisée avec Panorama.
État/Détail d’exécution	L'état de la connexion établie entre ce collecteur de journaux et les autres collecteurs de journaux qui font partie du groupe de collecteurs.
État de la redistribution des journaux	Certaines actions (par exemple, ajout de disques) entraîneront la redistribution, par le collecteur de journaux, des journaux entre ses paires de disques. Cette colonne indique l'état d'achèvement du processus de redistribution en pourcentage.
État de la dernière validation	Indique si la dernière validation du groupe de collecteurs effectuée à l'égard du collecteur de journaux a échoué ou réussi.
Santé	Indique l’état d’intégrité du collecteur de journaux en fonction de l’état d’intégrité du processus de collecte des journaux. S’affiche  lorsque le collecteur de journaux est sain et  si un ou plusieurs processus de collecte de journaux connaissent une dégradation de l’intégrité. • **logd:** processus responsable de l’ingestion des journaux reçus du pare-feu géré et du transfert des journaux ingérés vers le vldmgr. • **vldmgr :**processus responsable de la gestion des processus vld. • **vlds :**processus responsable de la gestion des disques de journalisation individuels, de l’écriture des journaux sur les disques de journalisation et de l’ingestion des journaux dans ElasticSearch. • **es :**processus ElasticSearch exécuté sur le collecteur de journaux.
Statistiques	Après avoir terminé la Configuration du Collecteur de journaux, cliquez sur **Statistiques** pour afficher les informations sur le disque, les performances du processeur et le taux moyen de journalisation (journaux / secondes). Afin de mieux

Informations sur les collecteurs de journaux	Description
	comprendre la plage de journaux affichée, vous pouvez également consulter les informations du journal le plus ancien que le collecteur a reçu. *Si vous utilisez un Gestionnaire SNMP pour un suivi centralisé, vous pouvez également consulter les statistiques de journaux dans l'objet de la MIB panLogCollector.*

Configuration du Collecteur de journaux

Sélectionnez **Panorama** > **Managed Collectors (Collecteurs gérés)** pour gérer les Collecteurs de journaux. Lorsque vous **Ajoutez** un nouveau Collecteur de journaux en tant que collecteur géré, les paramètres que vous configurez varient selon l'emplacement du Collecteur de journaux et le déploiement ou non de Panorama dans une configuration haute disponibilité (HD) :

- **Collecteur de journaux dédié** – lorsque vous ajoutez le Collecteur de journaux, l'onglet **Interfaces** ne s'affiche pas dans un premier temps. Vous devez saisir le numéro de série (**Collecteur S/N**) du Collecteur de journaux, cliquer sur **OK**, puis éditer le Collecteur de journaux pour afficher les paramètres de l'interface.
- **Collecteur de journaux par défaut local pour le serveur de gestion Panorama solitaire (non HD) ou actif (HD)** – après avoir saisi le numéro de série (**Collecteur S / N**) du serveur de gestion Panorama, la boîte de dialogue Collecteur affiche uniquement les **Disques**, les paramètres de **Communication** et un sous-ensemble de paramètres **Généraux.** Pour tous les autres paramètres, le Collecteur de journaux dérive ses valeurs de la configuration du serveur de gestion Panorama.
- (HD uniquement) **Collecteur de journaux par défaut local au serveur de gestion Panorama passif –** Panorama traite ce Collecteur de journaux comme s'il était situé à distance : vous devez donc le configurer comme vous le feriez pour un Collecteur de journaux dédié.

La procédure complète pour la configuration d'un Collecteur de journaux exige l'accomplissement de tâches supplémentaires.

Que voulez-vous faire ?	Reportez-vous à la section :
Identifier le Collecteur de journaux et définir ses connexions au serveur de gestion Panorama et aux services externes.	Paramètres généraux du collecteur de journaux
Configurer l'accès à la CLI du collecteur de journaux.	Paramètres d'authentification des collecteurs de journaux
Configurez les interfaces que le Collecteur de journaux dédié utilise pour le trafic de gestion, la communication du Groupe	Paramètres d'une interface de collecteur de journaux

Que voulez-vous faire ?	Reportez-vous à la section :
de collecteurs et la collecte des journaux.	
Configurer les disques RAID qui stockent les journaux recueillis à partir des pare-feu.	Paramètres du disque RAID du collecteur de journaux
Configurez le Collecteur de journaux pour vous authentifier avec les agents User-ID Windows.	Sécurité de la connexion
Configurez les paramètres de sécurité pour la communication avec Panorama, les autres Collecteurs de journaux et les pare-feu.	Paramètres de communication

Paramètres généraux du collecteur de journaux

- Panorama > Collecteurs gérés > Général

Configurez les paramètres comme décrits dans le tableau suivant pour identifier le Collecteur de journaux et définissez ses connexions au serveur de gestion Panorama, aux serveurs DNS et aux serveurs NTP.

Paramètres généraux des collecteurs de journaux	Description
N° de série du collecteur	(Requis) Saisissez le numéro de série de l'équipement Panorama qui agit en tant que Collecteur de journaux. Si le Collecteur de journaux est local, saisissez le numéro de série du serveur de gestion Panorama.
Nom du collecteur	Saisissez un nom pour identifier ce Collecteur de journaux (31 caractères maximum). Le nom est sensible à la casse, doit être unique et peut inclure uniquement des lettres, chiffres, espaces, traits d'union et traits de soulignement. Ce nom s'affiche en tant que nom d'hôte du collecteur de journaux.
Certificat entrant pour Syslog sécurisé	Sélectionnez le certificat que le collecteur géré doit utiliser pour ingérer les journaux du serveur Traps ™ ESM de manière sécurisée. Ce certificat est appelé un certificat entrant car Panorama / le Collecteur géré est le serveur auquel le Traps ESM (client) envoie des journaux. Le certificat est requis si le protocole de **Transport** pour le profil d'ingestion des journaux est **SSL**.
Certificat pour Secure Syslog	Sélectionnez un certificat pour le transfert sécurisé des journaux système à un serveur Syslog externe. L'option **Certificate for Secure Syslog (Certificat pour Secure Syslog)** doit être sélectionnée sur le certificat (voir Gestion des certificats

Paramètres généraux des collecteurs de journaux	Description
	du pare-feu de Panorama). Lorsque vous affectez un profil de serveur Syslog au Groupe de collecteurs qui inclut ce Collecteur de journaux (voir Panorama > Groupe de collecteurs, **Panorama** > **Collector Groups (Groupes de collecteurs)** > **Collector Log Forwarding (Transfert de collecteurs de journaux)**), le protocole de **Transport** du profil du serveur doit être **SSL** (voir (Device (Périphérique) > Server Profiles (Profils de serveur) > Syslog).
Serveur IP de Panorama	Indiquez l'adresse IP du serveur de gestion Panorama qui gère ce collecteur de journaux.
Serveur IP 2 de Panorama	Indiquez l'adresse IP du homologue secondaire si le serveur de gestion Panorama est déployé dans une configuration haute disponibilité (HA).
Domain (Domaine)	Saisissez le nom de domaine du Collecteur de journaux.
Serveur DNS principal	Saisissez l'adresse IP du serveur DNS principal. Le Collecteur de journaux utilise ce serveur pour les recherches DNS (pour rechercher le serveur de gestion Panorama, par exemple).
Serveur DNS secondaire	(Facultatif) Saisissez l'adresse IP d'un serveur DNS secondaire à utiliser si le serveur principal n'est pas disponible.
Serveur NTP principal	Saisissez l'adresse IP ou le nom d'hôte du serveur NTP principal (le cas échéant). Si vous n'utilisez pas de serveurs NTP, vous pouvez définir l'heure du Collecteur de journaux manuellement.
Serveur NTP secondaire	(Facultatif) Saisissez l'adresse IP ou le nom d'hôte de serveurs NTP secondaires à utiliser si le serveur principal n'est pas disponible.
Fuseau horaire	Sélectionnez le fuseau horaire du Collecteur de journaux.
Latitude	Saisissez la latitude (de -90,0 à 90,0) du collecteur de journaux. Les cartes du trafic et des menaces utilisent la latitude d'App Scope.
Longitude	Saisissez la longitude (de -180,0 à 180,0) du collecteur de journaux. Les cartes du trafic et des menaces utilisent la longitude d'App Scope.

Paramètres d'authentification des collecteurs de journaux

- Panorama > Collecteurs gérés > Authentification

Un appareil M-Series ou un appareil virtuel Panorama en mode Log Collector (Collecteurs de journaux dédiés) n'a pas d'interface web mais seulement un CLI. Vous pouvez utiliser le serveur de gestion Panorama pour configurer la plupart des paramètres sur un collecteur de journaux dédié. Certains

paramètres nécessitent toutefois un accès à la CLI. Pour configurer les paramètres d'authentification pour accéder à la CLI, configurez les champs comme décrits dans le tableau suivant.

Paramètres d'authentification des collecteurs de journaux	Description
Profil d'authentification	Sélectionnez un profil d'authentification configuré pour définir le service d'authentification qui valide les informations de connexion des administrateurs du Collecteur de journaux dédié ou de Panorama.
Tentatives échouées	Saisissez le nombre d'échecs de tentatives de connexion que le collecteur de journaux dédié autorise sur le CLI avant le verrouillage du compte administrateur (fourchette de 0 à 10 ; par défaut 10). Limitez les tentatives de connexion peut vous permettre de protéger le l'appareil WildFire contre les attaques en force. Une valeur de 0 indique un nombre illimité de tentatives de connexion. *Si vous définissez le champ **Failed Attempts (Tentatives échouées)** sur une valeur non nulle, mais que vous laissez le champ **Lockout Time (Durée de verrouillage)** sur 0, l'administrateur est verrouillé indéfiniment jusqu'à ce qu'un autre administrateur déverrouille manuellement l'administrateur. Si aucun autre administrateur n'a été créé, vous devez reconfigurer les paramètres de **Failed Attempts (Tentatives échouées)** et de **Lockout Time (Durée de verrouillage)** sur et transmettre les changements de configuration au collecteur de journaux. Pour veiller à ce qu'un administrateur ne soit jamais verrouillé, utilisez la valeur par défaut (**0**) pour les **Failed Attempts (Tentatives échouées)** et la **Lockout Time (Durée de verrouillage)**.* *Définissez le nombre de **Failed Attempts (Tentatives échouées)** sur 5 ou moins pour permettre un nombre raisonnable de nouvelles tentatives en cas de fautes de frappe, tout en empêchant les systèmes malveillants de tenter des méthodes d'attaque par force pour se connecter au Collecteur de journaux dédié.*
Durée de verrouillage (en min.)	Saisissez le nombre de minutes pendant lesquelles l'accès d'un administrateur à l'interface Web et la CLI est verrouillé par le collecteur de journaux dédié si la limite de **Failed Attempts (Tentatives échouées)** est atteinte (plage de 0 à 60; 5 par défaut). Une valeur de 0 signifie que le verrouillage s'applique jusqu'à ce qu'un autre administrateur déverrouille manuellement le compte.

Paramètres d'authentification des collecteurs de journaux	Description
	*Si vous définissez le champ **Failed Attempts (Tentatives échouées)** sur une valeur non nulle, mais que vous laissez le champ **Lockout Time (Durée de verrouillage)** sur 0, l'administrateur est verrouillé indéfiniment jusqu'à ce qu'un autre administrateur déverrouille manuellement l'administrateur. Si aucun autre administrateur n'a été créé, vous devez reconfigurer les paramètres de **Failed Attempts (Tentatives échouées)** et de **Lockout Time (Durée de verrouillage)** sur et transmettre les changements de configuration au collecteur de journaux. Pour veiller à ce qu'un administrateur ne soit jamais verrouillé, utilisez la valeur par défaut (**0**) pour les **Failed Attempts (Tentatives échouées)** et la **Lockout Time (Durée de verrouillage)**.* *Définissez la **Lockout Time (Durée de verrouillage)** sur au moins 30 minutes pour empêcher les tentatives de connexion continues d'un acteur malveillant.*
Délai d'inactivité (en min.)	Saisissez, pour l'interface Web ou la CLI, le nombre de minutes d'inactivité maximum sur le CLI avant qu'un administrateur ne soit automatiquement déconnecté (la plage est comprise entre 0 et 1 440, la valeur par défaut est aucune). Une valeur égale à 0 signifie que l'inactivité n'entraîne pas une déconnexion automatique. *Définissez un **Idle Timeout (Délai d'inactivité)** de 10 minutes pour empêcher les utilisateurs non autorisés d'accéder au collecteur de journaux dédié si un administrateur laisse une session du pare-feu ouverte.*
Compte de session max.	Saisissez le nombre de sessions actives que l'administrateur peut ouvrir simultanément, par défaut 0, ce qui signifie que le collecteur de journaux dédié peut avoir un nombre illimité de sessions actives simultanées.
Compte de session max.	Saisissez le nombre de minutes max. pendant lequel l'administrateur peut être connecté avant d'être automatiquement déconnecté. Le nombre par défaut est 0, ce qui signifie que l'administrateur peut être connecté indéfiniment même s'il est inactif.
Administrateurs locaux	Ajoutez et configurez de nouveaux administrateurs uniques pour le Collecteur de journaux dédié. Ces administrateurs sont uniques pour le Collecteur géré et sont gérés depuis cette page (**Panorama** > **Managed Collectors (Collecteurs gérés)** > **Authentication (Authentification)**).
Administrateurs de Panorama	Importez des administrateurs configurés dans Panorama. Ces administrateurs sont créés dans Panorama et importés vers le Collecteur de journaux dédié.

Paramètres d’une interface de collecteur de journaux

- Panorama > Collecteurs gérés > Interfaces

Par défaut, les Collecteurs de journaux dédiés (appareils de série M en mode Collecteur de Journaux) utilisent l’interface de gestion (MGT) pour le trafic de gestion, la collecte de journaux et la communication au Groupe de collecteurs. Toutefois, Palo Alto Networks vous recommande d’attribuer des interfaces distinctes pour la collecte des journaux et la communication du Groupe de collecteurs afin de réduire le trafic sur l’interface MGT. Vous pouvez améliorer la sécurité en définissant un sous-réseau distinct pour l’interface de gestion qui est plus privée que les sous-réseaux pour les autres interfaces. Pour utiliser des interfaces distinctes, vous devez d’abord les configurer sur le serveur de gestion Panorama (voir Périphérique > Configuration > Gestion). Les interfaces disponibles pour la collecte des journaux et la Communication du groupe de collecteurs varient en fonction du modèle d’appareil du Collecteur de journaux. Par exemple, l’appareil M-500 comporte les interfaces suivantes : Ethernet1 (1 Gbit/s), Ethernet2 (1 Gbit/s), Ethernet3 (1 Gbit/s), Ethernet4 (10 Gbit/s) et Ethernet5 (10 Gbit/s).

Pour configurer une interface, sélectionnez le lien et configurez les paramètres de la manière décrite dans le tableau suivant.

Pour procéder à la configuration de l’interface de gestion, vous devez indiquer l’adresse IP, le masque réseau (pour IPv4) ou la longueur de préfixe (pour IPv6) et la passerelle par défaut. Si vous validez une configuration partielle (par exemple, il se peut que vous omettiez la passerelle par défaut), vous pouvez accéder au pare-feu ou au Panorama uniquement par le biais du port de console afin d'apporter des modifications ultérieures à la configuration.

Validez toujours une configuration complète de l’interface MGT. Vous ne pouvez pas valider les configurations pour d’autres interfaces à moins d’indiquer l’adresse IP, le masque réseau (pour IPv4) ou la longueur de préfixe (pour IPv6) et la passerelle par défaut.

Paramètres d’une interface de collecteur de journaux	Description
Eth1 / Eth2 / Eth3 / Eth4 / Eth5	Vous devez activer une interface pour la configurer. L’interface de gestion est une exception car elle est activée par défaut.
Vitesse et duplex	Configurez un débit de données et une option de duplex pour l’interface. Les choix possibles sont : 10 Mbit/s, 100 Mbit/s et 1 Gbit/s et 10 Gbit/s (Eth4 et Eth5 uniquement) en duplex intégral ou semi-duplex. Utilisez le paramètre de **négociation automatique** par défaut pour que le Collecteur de journaux détermine la vitesse de l’interface. *Ce paramètre doit correspondre aux paramètres d’interface de l’équipement réseau voisin.*
Adresse'A0;IP (IPv4)	Si votre réseau utilise des adresses IPv4, affectez une adresse IPv4 à l’interface.

Paramètres d'une interface de collecteur de journaux	Description
Masque réseau (IPv4)	Si vous avez affecté une adresse IPv4 à l'interface, vous devez également saisir un masque réseau (par exemple, 255.255.255.0).
Passerelle par défaut (IPv4)	Si vous avez affecté une adresse IPv4 à l'interface, vous devez également affecter une adresse IPv4 à la passerelle par défaut (elle doit se trouver sur le même sous-réseau que l'interface MGT).
Longueur du préfixe / de l'adresse IPv6	Si votre réseau utilise des adresses IPv6, affectez une adresse IPv6 à l'interface. Pour indiquer le masque réseau, saisissez une longueur de préfixe IPv6 (par exemple, 2001:400:f00::1/64).
Passerelle IPv6 par défaut	Si vous avez affecté une adresse IPv6 à l'interface, vous devez également affecter une adresse IPv6 à la passerelle par défaut (elle doit se trouver sur le même sous-réseau que l'interface).
MTU	Saisissez l'unité de transmission maximale (MTU) en octets par paquet envoyé sur cette interface (plage de 576 à 1 500 ; par défaut 1 500).
Collecte des journaux de périphérique	Activez l'interface pour collecter les journaux à partir des pare-feu. Pour un déploiement avec un trafic de journaux élevé, vous pouvez activer plusieurs interfaces pour effectuer cette fonction. Cette fonction est activée par défaut sur l'interface MGT.
Communication avec les groupes de collecteurs	Activez l'interface pour la communication de Groupe de collecteurs (l'interface par défaut est l'interface MGT). Seule une interface peut effectuer cette fonction.
Transfert Syslog	Activez l'interface pour le transfert de syslogs (l'interface par défaut est l'interface MGT). Seule une interface peut effectuer cette fonction.
Services de connexion réseau	Le service **Ping** est disponible sur toutes les interfaces et vous permet de tester la connectivité entre l'interface du Collecteur de journaux et les services externes. Les services suivants sont uniquement disponibles sur l'interface MGT : • **SSH** – Permet un accès sécurisé à l'interface de ligne de commande Panorama. • **SNMP** – Permet à l'interface de recevoir des requêtes de statistiques en provenance d'un gestionnaire SNMP. Pour plus de détails, voir Activation de la surveillance SNMP. • **User-ID** – permet au Collecteur de journaux de redistribuer les informations de mappage des utilisateurs reçues des agents User-ID.

Paramètres d'une interface de collecteur de journaux	Description
Adresses IP autorisées	Saisissez les adresses IP des systèmes clients qui peuvent accéder au Collecteur de journaux via cette interface. Une liste vide (par défaut) indique que tous les systèmes clients peuvent y accéder. *Palo Alto Networks vous recommande de ne pas laisser cette liste vide ; précisez les systèmes clients des administrateurs Panorama (uniquement) afin d'éviter tout accès non autorisé.*

Paramètres du disque RAID du collecteur de journaux

- Panorama > Collecteurs gérés > Disques

Après avoir configuré les disques de journalisation sur l'Appareil M-Series ou l'Appareil virtuel Panorama, vous pouvez les **Ajouter** à la configuration du Collecteur de journaux.

Par défaut, les appareils de la série M sont fournis avec la première paire RAID 1 installée dans les baies A1 et A2. Dans le logiciel, la paire de disques des baies A1 et A2 est nommée Paire de disques A. Les baies restantes sont nommées de manière séquentielle : paire de disques B, paire de disques C, etc. Par exemple, l'appareil M-500 prend en charge un maximum de 12 paires de disques. Vous pouvez Installer des paires de disques de 2 To ou 1 To dans le même appareil ; cependant, les deux lecteurs doivent faire la même taille dans chaque paire.

L'appareil virtuel Panorama prend en charge jusqu'à 12 disques de journalisation virtuels pour une capacité de stockage de 24 To.

Une fois les paires de disques ajoutées, le collecteur de journaux redistribue ses journaux existants sur tous les disques, ce qui peut prendre des heures pour chaque téraoctet de journaux. Pendant le processus de redistribution, le taux maximum d'ingestion des journaux est réduit. Dans la page **Panorama** > **Managed Collectors (Collecteurs gérés)**, la colonne État de la redistribution des journaux indique l'état de la progression du processus en pourcentage.

Si vous utilisez un Gestionnaire SNMP pour un suivi centralisé, vous pouvez consulter les statistiques de journaux dans l'objet de la MIB panLogCollector.

Sécurité de la connexion

- **Périphérique** > **Identification utilisateur** > **Sécurité de la connexion**
- **Panorama** > **Identification utilisateur** > **Sécurité de la connexion**

Pour configurer un profil de certificat utilisé par le Collecteur de journaux pour valider le certificat présenté par les agents User-ID Windows. Le Collecteur de journaux utilise le profil de certificat sélectionné pour vérifier l'identité de l'agent User-ID en validant le certificat de serveur présenté par l'agent.

Tâche	Description
Profil de certificat de User-ID	Dans le menu déroulant, sélectionnez le profil de certificat utilisé pour l'authentification avec les agents User-ID Windows par le pare-feu ou Panorama ou sélectionnez **Nouveau profil de certificat** pour en créer un. Sélectionnez **Aucun** pour supprimer le profil de certificat.

Paramètres de communication

- Panorama > Collecteurs gérés > Communication

Pour configurer l'authentification basée sur certificat personnalisée entre les Collecteurs de journaux et Panorama, les pare-feu et les autres Collecteurs de journaux, configurez les paramètres comme décrit dans le tableau suivant.

Paramètres de communication	Description
Communication sécurisée avec le serveur – Activer **Communication sécurisée avec le serveur** valide l'identité des périphériques clients se connectant au Collecteur de journaux.	
Profil de service SSL/TLS	Sélectionnez un profil de service SSL/TLS dans la liste déroulante. Ce profil définit le certificat présenté par le Collecteur de journaux et indique la plage de versions SSL/TLS acceptables pour la communication avec le Collecteur de journaux.
Profil du certificat	Sélectionnez un profil de certificat dans le menu déroulant. Ce profil du certificat définit le comportement de vérification de la révocation du certificat et l'autorité de certification racine utilisée pour authentifier la chaîne de certificats présentée par le client.
Certificat personnalisé uniquement	Lorsqu'il est activé, le Collecteur de journaux n'accepte que les certificats personnalisés pour l'authentification avec des pare-feu gérés et des Collecteurs de journaux.
Autoriser les clients en fonction de leur numéro de série	Le Collecteur de journaux autorise les périphériques clients en fonction de l'utilisation d'un hachage de leur numéro de série.
Vérifier la liste d'autorisation	Les périphériques clients ou les groupes de périphériques se connectant à ce Collecteur de journaux sont vérifiés par rapport à la liste d'autorisations.
Délai d'attente de déconnexion (min)	Le laps de temps pendant lequel le Collecteur de journaux attend avant d'interrompre la connexion actuelle avec ses périphériques gérés. Le Collecteur de journaux rétablit ensuite les connexions avec ses périphériques gérés en utilisant les paramètres de communications sécurisées avec le serveur configurés. Le temps d'attente commence après la validation de la configuration des communications sécurisées avec le serveur.

Paramètres de communication	Description
Liste d'autorisation	**Liste d'autorisations** – Sélectionnez Ajouter et renseignez les champs suivants pour définir les critères. • **Identifiant** – Sélectionnez **Objet** ou **Autre nom d'objet** en tant qu'identifiant d'autorisation. • **Type** – Si Autre nom d'objet est sélectionné en tant qu'Identifiant, sélectionnez **IP**, **nom d'hôte**, ou **e-mail** en tant que type d'identifiant. Si Objet est sélectionné, le nom commun est utilisé en tant que type d'identifiant. • **Valeur** – Saisissez la valeur d'identifiant.
Communication sécurisée avec le client – Activer **Communication sécurisée avec le client** garantit que le certificat client indiqué est utilisé pour authentifier les connexions Collecteur de journaux sur SSL avec Panorama, les pare-feu ou d'autres Collecteurs de journaux.	
Type de certificat	Sélectionnez le type de certificat de périphérique (Aucun, Local ou SCEP) utilisé pour sécuriser la communication
None	Si **Aucun** est sélectionné, aucun certificat de périphérique n'est configuré et la communication sécurisée avec le client n'est pas utilisée. Il s'agit de la sélection par défaut.
Local	Le Collecteur de journaux utilise un certificat de périphérique local et la clé privée correspondante générée sur le Collecteur de journaux ou importée à partir d'un serveur PKI d'entreprise existant.
	Certificat – Sélectionnez le certificat de périphérique local. Ce certificat peut être unique pour le pare-feu (basé sur un hachage du numéro de série du Collecteur de journaux) ou un certificat de périphérique commun utilisé par tous les Collecteurs de journaux se connectant à Panorama.
	Profil de certificat – Sélectionnez le Profil de certificat dans le menu déroulant. Ce profil du certificat est utilisé pour définir l'authentification du serveur avec le Collecteur de journaux.
SCEP	Le Collecteur de journaux utilise un certificat de périphérique et un serveur de Protocole d'inscription de certificat simple (SCEP) généré par une clé privée.
	Profil SCEP – Sélectionnez le Profil SCEP dans le menu déroulant.
	Profil de certificat – Sélectionnez le Profil de certificat dans le menu déroulant. Ce profil du certificat est utilisé pour définir l'authentification du serveur avec le Collecteur de journaux.

Paramètres de communication	Description
Vérifier l'identité du serveur	Le périphérique client confirme l’identité du serveur en faisant correspondre le nom commun (CN) avec l’adresse IP ou le FQDN du serveur.

Mises à jour logicielles pour les collecteurs de journaux dédiés

- Panorama > Collecteurs gérés

Pour installer une image logicielle sur un Collecteur de journaux dédié, téléchargez ou chargez l’image sur Panorama (voir Panorama > Déploiement du périphérique), cliquez sur **Installer**, puis remplissez les champs suivants.

Étant donné que le serveur de gestion Panorama partage son système d’exploitation avec le Collecteur de journaux par défaut local, vous les mettez tous deux à niveau lors de l’installation d’une mise à jour logicielle sur le serveur de gestion Panorama (voir Panorama > Logiciel*).*

Pour les Collecteurs de journaux dédiés, vous pouvez également sélectionner ***Panorama*** *>* ***Déploiement de périphériques*** *>* ***Logiciel*** *pour installer des mises à jour (voir* Gestion des mises à jour logicielles et de contenu*).*

Pour réduire le trafic sur l’interface de gestion (MGT), vous pouvez configurer Panorama pour utiliser une interface distincte pour le déploiement de mises à jour (voir Panorama > Configuration > Interfaces*).*

Champs pour l’installation d’une Mise à jour logicielle sur un Collecteur de journaux	Description
Classification	Sélectionnez une image logicielle chargée ou téléchargée.
Périphériques	Sélectionnez les collecteurs de journaux sur lesquels installer le logiciel. Le dialogue affiche les informations suivantes pour chacun des collecteurs de journaux : • **Nom du périphérique** – Le nom du Collecteur de journaux dédié. • **Version actuelle** - La version du logiciel Panorama actuellement installée sur le collecteur de journaux. • **État HA** - Cette colonne ne s’applique pas aux collecteurs de journaux. Les collecteurs de journaux dédiés ne prennent pas en charge la haute disponibilité.

Champs pour l’installation d’une Mise à jour logicielle sur un Collecteur de journaux	Description
Filtre sélectionné	Pour n'afficher que des collecteurs de journaux spécifiques, sélectionnez les collecteurs de journaux, puis **Filter Selected (Filtre sélectionné)**.
Charger sur le périphérique uniquement (ne pas Installer)	Sélectionnez pour charger le logiciel sur le Collecteur de journaux sans le redémarrer automatiquement. L’image n’est pas installée tant que vous n’avez pas redémarré manuellement en vous connectant à la CLI du Collecteur de journaux et en exécutant la commande opérationnelle **`request restart system`**.
Redémarrer le périphérique après l’Installation	Sélectionnez pour télécharger et installer automatiquement le logiciel. Le processus d’installation redémarre le collecteur de journaux.

Panorama > Groupes de collecteurs

Chaque groupe de collecteurs peut être composé d'un maximum de 16 collecteurs de journaux, auxquels vous pouvez assigner des pare-feu pour le transfert des journaux. Vous pouvez ensuite utiliser Panorama pour effectuer une recherche sur les collecteurs de journaux afin d'afficher ou d'interroger les journaux cumulés.

Le groupe de collecteurs prédéfini nommé par défaut contient le collecteur de journaux prédéfini qui est local au serveur de gestion Panorama.

- Configuration du groupe de collecteurs
- Information sur les groupes de collecteurs

Configuration du groupe de collecteurs

Pour configurer un Groupe de collecteurs, cliquez sur **Ajouter** et renseignez les champs suivants.

Paramètres de groupe de collecteurs	Configuré dans	Description
Nom	**Panorama** > **Groupes de collecteurs** > **Général**	Saisissez un nom pour identifier ce Groupe de collecteurs (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d'union et de soulignement.
Stockage des journaux		Indique le quota de stockage total des journaux de pare-feu reçus par le Groupe de collecteurs et l'espace disponible. Cliquez sur le lien de quota de stockage pour définir le **Quota (%)** de stockage et la période d'expiration (**Jours max**) pour les types de journaux suivants : • **Journaux détaillés du pare-feu** – Inclut tous les types de journaux dans **Périphérique** > **Configuration** > **Paramètres de journalisation et de génération de rapports**, comme le trafic, la menace, la correspondance HIP, les adresses IP enregistrées de manière dynamique (indicateur d'adresses IP), les PCAP étendus, le GTP et le Tunnel, les Statistiques de l'application, etc. • **Journaux récapitulatifs du pare-feu** – Inclut tous les journaux récapitulatifs inclus dans **Périphérique** > **Configuration** > **Paramètres de journalisation et de génération de rapports**, comme le récapitulatif du trafic, le récapitulatif

Paramètres de groupe de collecteurs	Configuré dans	Description
		des menaces, le récapitulatif des URL et le récapitulatif GTP et des tunnels. • **Infrastructure and Audit Logs (Journaux d'infrastructure et d'audit)** – Inclut les journaux de configuration, de système, de User-ID et d'authentification. • **Journaux de la plate-forme Palo Alto Networks** – Inclut les journaux de Traps et d'autres produits Palo Alto Networks. • **Journaux tiers externes** – Inclut les journaux provenant des intégrations d'un autre fournisseur fournies par Palo Alto Networks. Pour utiliser les paramètres par défaut, cliquez sur **Rétablir les valeurs par défaut**.
Période de conservation minimale (jours)		Saisissez la période de conservation minimale des journaux (de 1 à 2 000 jours) appliquée par Panorama sur tous les collecteurs de journaux du groupe de collecteurs. Si la date actuelle moins la date du plus ancien journal est inférieure à la période de conservation minimale, Panorama génère un journal système à titre d'alerte de violation.
Membres du groupe de collecteurs		Veuillez **Ajouter** les Collecteurs de journaux qui font partie de ce Groupe de collecteurs (jusqu'à 16). Vous pouvez ajouter n'importe quel Collecteur de journaux disponibles dans la page **Panorama** > **Collecteurs gérés**. Tous les Collecteurs de journaux d'un Groupe de collecteurs particulier doivent être du même modèle : par exemple, tous les appareils M-500 ou toutes les applications virtuelles Panorama.

Paramètres de groupe de collecteurs	Configuré dans	Description
		*Une fois des collecteurs de journaux ajoutés à un groupe de collecteurs existant, Panorama redistribue ses journaux existants sur tous les collecteurs de journaux, ce qui peut prendre des heures pour chaque téraoctet de journaux. Pendant le processus de redistribution, le débit de journalisation maximum est réduit. Dans la page **Panorama** > **Groupes de collecteurs**, la colonne État de la redistribution des journaux indique l'état de la progression du processus en tant que pourcentage.*
Activer la redondance des journaux parmi les collecteurs		Si vous sélectionnez cette option, chaque journal du groupe de collecteurs aura deux copies et chaque copie se trouvera sur un collecteur de journaux distinct. Cette redondance garantit qu'aucun journal n'est perdu en cas d'indisponibilité d'un collecteur de journaux : vous pouvez voir tous les journaux transférés au groupe de collecteurs et générer des rapports sur toutes les données de journal. La redondance des journaux est disponible uniquement si le groupe de collecteurs comprend plusieurs collecteurs de journaux et si chaque collecteur de journaux inclut le même nombre de disques. La redondance des journaux s'applique uniquement aux journaux nouvellement ingérés une fois le paramètre activé et non aux journaux existants. Dans la page **Panorama** > **Collector Groups (Groupes de collecteurs)**, la colonne Log Redistribution State (État de la redistribution des journaux) indique l'état de la progression du processus en tant que pourcentage. Tous les Collecteurs de journaux d'un Groupe de collecteurs particulier doivent être du même modèle : par exemple, tous les appareils M-500 ou toutes les applications virtuelles Panorama.

Paramètres de groupe de collecteurs	Configuré dans	Description
		L'activation de la redondance générant un plus grand nombre de journaux, cette configuration nécessite une capacité de stockage supérieure. L'activation de la redondance multiplie par deux le trafic de traitement des journaux dans un groupe de collecteurs, réduisant ainsi de moitié son débit de journalisation maximum car chaque collecteur de journaux doit distribuer une copie de chaque journal qu'il reçoit. (Lorsque l'espace vient à manquer sur un groupe de collecteurs, il supprime les journaux antérieurs.)
Transférer à tous les collecteurs de la liste des favoris		Sélectionnez cette option pour envoyer des journaux à chaque Collecteur de journaux dans la liste de préférences. Panorama utilise l'équilibrage de charge de la permutation circulaire pour sélectionner quel Collecteur de journaux reçoit les journaux à un moment donné. Cette option est désactivée par défaut : les pare-feu n'envoient les journaux qu'au premier Collecteur de journaux de la liste, à moins que ce Collecteur de journaux ne soit indisponible (voir Périphériques / collecteurs).
Activer la Communication sécurisée entre les collecteurs de journaux		Active l'utilisation de certificats personnalisés pour l'authentification SSL mutuelle entre les Collecteurs de journaux d'un Groupe de collecteurs.
Emplacement	**Panorama** > **Groupes de collecteurs** > **Surveillance**	Indiquez l'emplacement du Groupe de collecteurs.
Contact		Précisez un contact de messagerie électronique (par exemple, l'e-mail de l'administrateur SNMP qui surveillera les collecteurs de journaux).
Version		Précisez la version SNMP qui doit communiquer avec le serveur de gestion Panorama : **V2c** ou **V3**. SNMP vous permet de recueillir des informations sur les collecteurs de journaux, notamment : l'état de la connexion, les statistiques des lecteurs de disque, la version du logiciel, les performances moyennes du processeur, le nombre moyen de journaux/s et la durée

Paramètres de groupe de collecteurs	Configuré dans	Description
		de stockage par type de journal. Les informations SNMP sont disponibles sur la base du groupe de collecteurs.
La chaîne de communauté SNMP (V2c uniquement)		Saisissez la **SNMP Community String (chaîne de communauté SNMP)**, qui identifie une communauté de gestionnaires SNMP et de périphériques surveillés (collecteurs de journaux dans le cas présent), et qui sert de mot de passe pour authentifier les membres de la communauté entre eux. *N'utilisez pas la chaîne de communauté publique définie par défaut ; elle est connue et, par conséquent, n'est pas sécurisée.*
Vues (V3 uniquement)		**Ajoutez** un groupe de vues SNMP et, dans **Vues**, donnez un nom au groupe. Chaque vue est constituée d'une paire identifiant d'objet (OID)/masque de niveau bit : l'OID définit une base d'information géré (MIB) et le masque (au format hexadécimal) définit les objets SNMP qui sont accessibles à l'intérieur (inclure correspondance) ou à l'extérieur (exclure correspondance) de ce MIB. Pour chaque vue du groupe, **Ajoutez** les paramètres suivants : • **Vue** – Saisissez un nom pour une vue. • **OID** - Saisissez l'OID. • **Option** (inclure ou exclure) - Choisissez si la vue doit exclure ou inclure l'OID. • **Masque** - Précisez une valeur de masque pour un filtre sur l'OID (par exemple, 0xf0).
Utilisateurs (V3 uniquement)		**Ajoutez** les paramètres suivants pour chaque utilisateur SNMP : • **Utilisateurs** - Saisissez le nom d'utilisateur qui permettra de l'authentifier auprès du gestionnaire SNMP. • **Vue** – Sélectionnez un groupe de vues de l'utilisateur.

Paramètres de groupe de collecteurs	Configuré dans	Description
		• **Authpwd** – Saisissez un mot de passe pour authentifier l'utilisateur auprès du gestionnaire SNMP (huit caractères minimum). Seul l'algorithme SHA (Secure Hash Algorithm/algorithme de hachage sécurisé) est pris en charge. • **Privpwd** – Saisissez un mot de passe de confidentialité pour crypter les messages SNMP envoyés au gestionnaire SNMP (huit caractères minimum). Seule la norme AES (Advanced Encryption Standard/norme de chiffrement avancé) est prise en charge.
Dispositifs / collecteurs	**Panorama** > **Groupes de collecteurs** > **Transfert des journaux du périphérique**	La liste des préférences de transfert de journaux contrôle quels pare-feu transmettent les journaux à quels Collecteurs de journaux. Pour chaque saisie que vous allez **Ajouter** à la liste, il faut **Modifier** la liste des Périphériques pour affecter un ou plusieurs pare-feu et **Ajouter** un ou plusieurs Collecteurs de journaux dans la liste des Collecteurs. Par défaut, les pare-feu que vous affectez dans une entrée de liste envoient les journaux uniquement au principal (premier) Collecteur de journaux tant que celui-ci est disponible. En cas d'échec du Collecteur de journaux principal, les pare-feu envoient les journaux au Collecteur de journaux secondaire. En cas d'échec du Collecteur de journaux secondaire, les pare-feu envoient les journaux au Collecteur de journaux tertiaire, et ainsi de suite. Pour changer l'ordre, sélectionnez un collecteur de journaux, puis cliquez sur **Déplacer en haut** ou sur **Déplacer en bas**. *Vous pouvez remplacer le comportement de transfert des journaux par défaut pour les pare-feu de la série PA-5200 et de la série PA-7000 en sélectionnant* Forward to all collectors in the preference list (Transférer à tous les collecteurs dans la liste des préférences) *dans l'onglet* ***General (Général)***.
Système Configuration	**Panorama** > **Groupes de collecteurs** > **Transfert des journaux du collecteur**	Pour chaque type de journaux du pare-feu que vous souhaitez transférer de ce Groupe de collecteurs vers des services externes, il est nécessaire d'**Ajouter** un ou plusieurs profils de liste de correspondance. Les profils

Paramètres de groupe de collecteurs	Configuré dans	Description
Correspondance HIP		indiquent les journaux à transférer et les serveurs de destination. Pour chaque profil, procédez comme suit : • **Name (Nom)**: entrez un nom de 31 caractères maximum pour identifier le profil de la liste de correspondance. • **Filtre** – Par défaut, le pare-feu transfère **Tous les journaux** du type auquel s'applique ce profil de liste de correspondance. Pour transmettre un sous-ensemble de journaux, sélectionnez un filtre existant ou sélectionnez **Générateur de filtrage** pour ajouter un nouveau filtre. Pour chaque requête d'un nouveau filtre, spécifiez les champs suivants et **Ajoutez** la requête : • **Connecteur**: sélectionnez la logique du connecteur (et/ou). Sélectionner **Refuser** si vous souhaitez appliquer un refus. Par exemple, pour éviter de transférer les journaux à partir d'une zone non approuvée, sélectionnez **Inverser**, sélectionnez **Zone** en tant qu'attribut, sélectionnez **égal** en tant qu'Opérateur et saisissez le nom de la Zone non approuvée dans la colonne Valeur. • **Attribute (Attribut)** – Sélectionnez un attribut de journal. Les options varient selon le type de journal. • **Opérateur** – Sélectionnez des critères qui déterminent la manière dont un attribut s'applique (comme « **égal** »). Les options varient selon le type de journal. • **Valeur (Value)** : spécifiez la valeur d'attribut à faire correspondre. Pour afficher ou exporter les journaux auxquels le filtre correspond, sélectionnez **Afficher les journaux filtrés**. Cet onglet propose les mêmes options que les pages de l'onglet **Monitoring (Surveillance)** (telles que **Monitoring (Surveillance)** > **des Logs (Journaux)** > **de Traffic (Trafic)**). • **Description** – Saisissez une description pouvant contenir jusqu'à 1 023 caractères pour expliquer l'objectif de ce profil de liste de correspondance.
Trafic		
Prévention		
URL		
Données		
WildFire		
Corrélation		
GTP		
SCTP		
Authentification		
User-id		
Tunnel		
Indicateur d'adresse IP		
Déchiffrement		
GlobalProtect		

Paramètres de groupe de collecteurs	Configuré dans	Description
		• Serveurs de destination – Pour chaque type de serveur, veuillez **Ajouter** un ou plusieurs profils de serveur. Pour configurer les profils de serveur, voir Périphérique > Profils de serveur > Trap SNMP, Périphérique > Profils de serveur > Syslog, Périphérique > Profils de serveur > E-mail ou Périphérique > Profils de serveur > HTTP. • Actions intégrées : vous pouvez **ajouter des** actions pour tous les types de journaux, à l'exception des journaux système et de configuration : • entrez un nom descriptif pour l'action . • Sélectionnez l'adresse IP que vous souhaitez identifier – **Adresse source** ou **Adresse de destination**. Vous pouvez identifier uniquement l'adresse IP source dans les journaux de Corrélation et les journaux de Correspondance HIP. • Sélectionnez l'action – **Add Tag (Ajouter une étiquette)** ou **Remove Tag (Supprimer une étiquette)**. • Indiquez si vous souhaitez enregistrer la balise auprès de l'agent d'ID utilisateur local sur ce panorama ou auprès d'un agent d'ID utilisateur distant. Pour enregistrer des balises auprès d'un **agent**, d'ID utilisateur de périphérique distant, sélectionnez le profil de serveur HTTP qui activera le transfert. • Configurez le **Timeout (Délai)**, en minutes, de l'indicateur d'adresse IP à définir, la période de temps pendant laquelle le mappage adresse IP/ étiquette est maintenu. La définition du délai d'expiration sur 0 signifie que le mappage IP-Tag n'expire pas (plage comprise entre 0 et 43200 (30 jours) ; la valeur par défaut est 0). *Vous ne pouvez configurer un délai d'expiration qu'avec l'action **Ajouter une balise** .* • Saisissez ou sélectionnez les **Tags (Étiquettes)** que vous souhaitez appliquer ou supprimer de la source cible ou de l'adresse IP de destination.

Paramètres de groupe de collecteurs	Configuré dans	Description
Profil d'ingestion	**Panorama** > **Groupes de collecteurs** > **Ingestion de journaux**	Veuillez **Ajouter** un ou plusieurs profils d'ingestion de journaux qui permettent à Panorama de recevoir des journaux à partir du serveur Traps ESM. Pour configurer un nouveau profil d'ingestion de journaux, voir Panorama > Profil d'ingestion des journaux.
Activité de l'administrateur des journaux	**Panorama** > **Groupes de collecteurs** > **Audit**	Configurez le Collecteur de journaux pour générer et transférer les journaux d'audit de l'activité de l'administrateur au serveur syslog sélectionné. • **Operational Commands (Commandes opérationnelles)**(désactivées par défaut) : génère un journal d'audit lorsqu'un administrateur exécute une commande opérationnelle ou de débogage dans l'interface de ligne de commande. Consultez la CLI Operational Command Hierarchy (hiérarchie des commandes opérationnelles) de l'interface de ligne de commande pour obtenir la liste complète des commandes opérationnelles et de débogage de PAN-OS. • **Syslog Server (Serveur Syslog)** : sélectionnez un profil de serveur syslog cible pour transférer les journaux d'audit.

Information sur les groupes de collecteurs

Sélectionnez **Panorama** > **Groupes de collecteurs** pour afficher les informations suivantes pour les Groupes de collecteurs. Des champs supplémentaires sont configurables après avoir effectué la Configuration des collecteurs de journaux.

Information sur les groupes de collecteurs	Description
Nom	Un nom qui identifie le groupe de collecteurs.
Redondance activée	Indique si la redondance des journaux est activée pour le groupe de collecteurs. Vous pouvez activer la redondance de journaux pour un groupe de collecteurs après avoir effectué ou modifié la Configuration des collecteurs de journaux.
Collecteurs	Les collecteurs de journaux affectés au groupe de collecteurs.

Information sur les groupes de collecteurs	Description
État de la redistribution des journaux	Certaines actions (par exemple, activer la redondance des journaux) entraîneront la redistribution, par le collecteur de journaux, des journaux parmi ses collecteurs de journaux. Cette colonne indique l'état d'achèvement du processus de redistribution en pourcentage.

Panorama > Plug-ins

- **Panorama** > **Plug-ins**
- **Périphérique** > **Plug-ins**

Sélectionnez **Panorama** > **Plug-ins** pour installer, supprimer et gérer les plug-ins qui prennent en charge les intégrations de tiers sur Panorama.

(Seulement disponible sur les pare-feu VM-Series) Sélectionnez **Device (Périphériques)** > **Plugins** pour installer, supprimer et gérer les plug-ins des pare-feu VM-Series.

Plug-ins	Description
Télécharger	Vous permet de télécharger un fichier d'installation de plug-in à partir d'un répertoire local. Cela n'installe pas le plug-in. Après avoir téléchargé le fichier d'installation, le lien d'Installation devient actif.
File Name (Nom du fichier)	Le nom du fichier du plug-in. Lorsque vous installez le plug-in **vm_series** sur Panorama, la page **Device (Périphérique)** > **VM-Series** devient disponible pour la gestion et la validation des configurations du modèle sur les pare-feu VM-Series déployées sur les environnements de cloud public : AWS, Azure et Google.
Version	Le numéro de version du plug-in.
Platform (Plateforme)	Les modèles sur lesquels le plug-in est pris en charge.
Date de publication	La date de sortie de cette version du plug-in.
Taille	La taille du fichier du plug-in.
Installée	Fournit l'état actuel de l'installation de chaque plug-in sur Panorama.
Actions	• **Install (Installer)** : Installe la version spécifiée du plug-in. L'installation d'une nouvelle version du plug-in écrase la version précédemment installée. • **Effacer** – Supprime le fichier de plug-in spécifié. • **Supprimer la configuration** – Supprime toutes les configurations liées au plug-in. Afin de supprimer totalement toutes les configurations en lien avec un plug-in, vous devez aussi effectuer une **Uninstall (désinstallation)** après avoir utilisé **Remove Config (Suppression de configuration)**. Lors de la suppression de la configuration du plug-in Panorama pour VMware NSX, cette action supprime uniquement les définitions de service et le ou les gestionnaires de services. Il ne supprime pas les autres configurations associées, telles que la zone, les groupes de périphériques ou les modèles. En outre, pour

Plug-ins	Description
	effectuer cette action dans un déploiement Panorama HA, vous devez d'abord supprimer la configuration sur l'actif, lancer un basculement pour rendre le secondaire actif, puis supprimer la configuration sur le nouvel homologue actif. • **Uninstall (Désinstaller)** : Supprime l'installation actuelle du plug-in. Cela ne supprime pas le fichier du plug-in de Panorama. Si vous désinstallez le plug-in, vous perdez toute configuration liée à ce plug-in. N'utilisez que lorsque vous supprimez complètement la configuration connexe.

Panorama > SD-WAN

Téléchargez et installez le plug-in Panorama SD-WAN afin de gérer, surveiller et générer des rapports de façon centralisée. Configurez la topologie SD-WAN depuis Panorama en ajoutant et en associant des branches à leurs plate-formes appropriées et associez les périphériques de cette branche et de cette plate-forme aux zones appropriées. Après avoir configuré la topologie SD-WAN, vous pouvez surveiller les mesures de santé du chemin d'accès sur tous les périphériques et les chemins d'accès afin d'isoler ls problèmes d'application et de lien et comprendre la performance de votre lien dans le temps. De plus, vous pouvez générer des rapports pour des besoins d'audit.

Que souhaitez-vous faire ?	Reportez-vous à la section :
Ajouter, modifier ou supprimer des périphériques de branche et de plate-forme.	Ajouter des Périphériques SD-WAN
Ajouter, modifier ou supprimer un cluster VPN	Clusters VPN SD-WAN
Surveiller la santé du chemin d'accès	Surveillance SD-WAN
Générer des rapports de santé	Rapports SD-WAN

Ajouter des Périphériques SD-WAN

- **Panorama** > **SD-WAN** > **Périphériques**

Les périphériques SD-WAN sont des branches ou des plate-formes qui forment votre cluster VPN et la topologie SD-WAN.

Champ	Description
Name (Nom)	Saisissez un nom qui identifie le périphérique SD-WAN.
Type	Sélectionnez le type de périphérique SD-WAN : • **Hub (Plate-forme)** : Un pare-feu centralisé déployé dans un bureau ou un emplacement principal, comme un Centre de données ou le siège d'une entreprise, auquel tous les périphériques de la branche se connectent à l'aide d'une connexion VPN. Le trafic entre les branches passe par la plate-forme avant de continuer vers la branche cible. Les branches se connectent aux plate-formes pour obtenir l'accès à des ressources centralisées à l'emplacement de la plate-forme. Le périphérique de hub traite le trafic, applique les règles de politique et gère les inversions de liens au bureau ou emplacement principal. • **Branch (Branche)** : Un pare-feu déployé à l'emplacement physique de la branche qui connecte à la plate-forme à l'aide de la connexion VPN et qui

Champ	Description
	offre une sécurité au niveau de la branche. La branche se connecte à la plate-forme pour accéder aux ressources centralisées. Le périphérique de plateforme traite le trafic, applique les règles de politique et gère les inversions de liens à l'emplacement de la branche.
Nom du routeur	Sélectionnez le routeur virtuel ou logique à utiliser pour l'acheminement entre le hub et les branches SD-WAN. Par défaut, un routeur virtuel`sdwan-default` est créé et permet automatiquement à Panorama d'appliquer les configurations du routeur.
Site	Saisissez un nom convivial pour l nom du site qui identifie la plate-forme ou la branche. Par exemple, saisissez le nom de la ville où le périphérique de branche est déployé.
Étiquette de liens	(PAN-OS 10.0.3 and later releases (PAN-OS 10.0.3 et versions ultérieures)) Pour une plate-forme, sélectionnez l'Étiquette de lien que vous avez créée pour l'interface virtuelle d'une plate-forme afin que la plate-forme puisse participer à DIA AnyPath. Auto VPN applique cette étiquette de lien à la totalité de l'interface virtuelle de la plate forme, et non à un lien individuel. Vous référencez cette Etiquette de lien dans le Profil de distribution de trafic pour indiquer l'ordre de basculement vers cette interface de plate-forme virtuelle. Sur le périphérique de branche, Auto VPN utilise cette étiquette pour remplir le champ de l'étiquette de lien dans l'interface virtuelle SD-WAN qui se termine sur le périphérique de la plate-forme.
Zone Internet	**Add (Ajoutez)** une ou plusieurs zones de sécurité pour identifier le trafic qui va vers et provient de sources non fiables.
Zone Hub	**Add (Ajoutez)** une ou plusieurs zones de sécurité pour identifier le trafic qui va vers et provient de périphériques de plate-forme SD-WAN.
Zone Branche	**Add (Ajoutez)** une ou plusieurs zones de sécurité pour identifier le trafic qui va vers et provient de périphériques de branche SD-WAN.
Zone Internal	**Add (Ajoutez)** une ou plusieurs zones de sécurité pour identifier le trafic qui va vers et provient de périphériques fiables sur le réseau de l'entreprise.
Onglet BGP	
BGP	Activer BGP.
ID de routeur	Précisez l'ID du routeur BGP. Le routeur du protocole BGP (Border Gateway Protocol) doit être unique parmi tous les routeurs. *Utilisez l'adresse de bouclage en tant qu'ID du routeur.*

Champ	Description
Adresse de bouclage	Spécifiez une adresse de bouclage statique IPv4 pour les homologues BGP.
Numéro AS	Saisissez le numéro de système autonome pour définir une politique, règle, mesures d'itinéraire communément définie pour internet. Le numéro AS doit être unique pour chaque emplacement de hub et branche. *Utilisez un numéro AS BGP privé de 4 octets pour ne pas interférer avec un numéro AS routable publiquement.*
Nom du profil de redistribution	Sélectionnez ou créez un profil de redistribution pour contrôler quels préfixes locaux sont communiqués au routeur de la plate-forme depuis la branche. Par défaut, tous les préfixes internet connectés en local sont communiqués à l'emplacement de la plate-forme. *Palo Alto Networks ne redistribue pas les itinéraires par défaut des branches déduites de l'ISP.*
Onglet NAT en amont	
NAT en amont	Activez le NAT en amont.
Interface SD-WAN	Sélectionnez une interface configurée pour le SD-WAN.
Type d'adresse IP NAT	Sélectionnez l'une des options suivantes : • **IP statique :**pour un concentrateur ou une succursale SD-WAN qui se trouve derrière un périphérique exécutant NAT pour le concentrateur ou la branche. Vous devez spécifier l'adresse IP ou le nom de domaine complet de l'interface publique sur ce périphérique NAT en amont, afin que la configuration VPN automatique puisse utiliser cette adresse comme point de terminaison de tunnel du concentrateur ou de la branche. Sélectionnez **Adresse** IP et entrez une adresse IPv4 sans masque de sous-réseau, ou sélectionnez **Nom de domaine complet**. • **DDNS :**pour une branche SD-WAN qui se trouve derrière un périphérique qui exécute NAT pour la branche. Indique que l'adresse IP de l'interface sur le périphérique NAT est obtenue à partir du service DDNS de Palo Alto Networks.
Onglet Tunnel VPN	
Copier l'en-tête ToS	(PAN-OS 10.2.1 and later 11.0 releases (PAN-OS 10.2.1 et versions ultérieures 11.0)) Copiez le champ ToS (Type de service) (bits ToS ou marques DSCP [Differentiated Services Code Point]) de l'en-tête IPv4 interne vers l'en-tête VPN des paquets encapsulés afin de préserver les informations ToS d'origine. Cette option copie également le champ Notification explicite de congestion (ECN).

Clusters VPN SD-WAN

- **Panorama** > **SD-WAN** > **Clusters VPN**

Associez les périphériques de branche SD-WAN avec un ou plusieurs périphériques de plate-forme SD-WAN afin de permettre la sécurisation de la communication entre les emplacements de la branche et de la plate-forme. Lorsque vous associez des périphériques de branche et de plate-forme dans un cluster VPN SD-WAN, le pare-feu crée les connexions IKE et IPSec VPN nécessaires entre les sites basés sur le type de cluster VPN que vous indiquez.

Champ	Description
Name (Nom)	Saisissez un nom qui identifie le cluster VPN.
Type	Sélectionnez le type de cluster VPN SD-WAN. • **Hub Spoke (plate-forme en étoile)** : topologie SD-WAN dans laquelle un pare-feu centralisé dans un bureau ou un lieu principal agit en tant que passerelle entre les périphériques de la branche connectés qui utilisent une connexion VPN. Le trafic entre les branches passe par la plate-forme avant de continuer vers la branche cible.
Branches	**Add (Ajoutez)** un ou plusieurs périphériques de branche à associer avec une ou plusieurs plate-formes.
Plate-formes	**Add (Ajoutez)** un ou plusieurs périphériques de plate-forme à associer avec une ou plusieurs périphériques de branche. Si plusieurs plate-formes sont ajoutées, utilisez les mesures de qualité de la santé du chemin d'accès pour contrôler quelle plate-forme est la principale et quelle est la secondaire.

Surveillance SD-WAN

- **Panorama** > **SD-WAN** > **Surveillance**

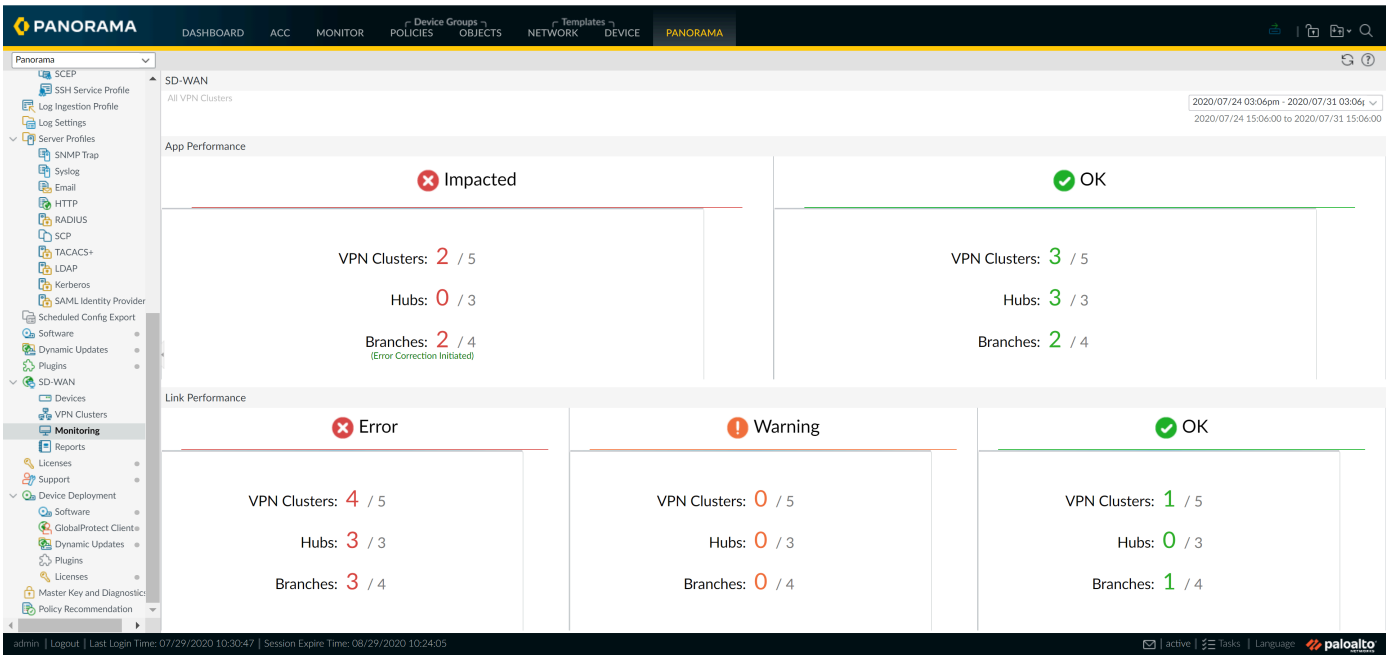
L'onglet de surveillance est un tableau de bord qui affiche des widgets de résumé de toutes vos mesures de la santé du périphérique SD-WAN. Cet outil offre une intelligence en matière de l'activité sur votre réseau SD-WAN, en vous de rapidement identifier les applications ou les liens qui ont des problèmes de performances. Vous pouvez afficher la qualité du chemin d'accès et la performance du lien de tous les clusters VPN, ou 'un Cluster VPN spécifique pour une période de temps donnée.

En un coup d'œil, vous pouvez voir le nombre total de Clusters VPN ayant des pare-feux de branche ou de plate-forme qui sont impactés par la performance de l'application et ceux qui sont sains. Vous pouvez afficher les états de santé des applications et liens suivants pour les Clusters VPN :

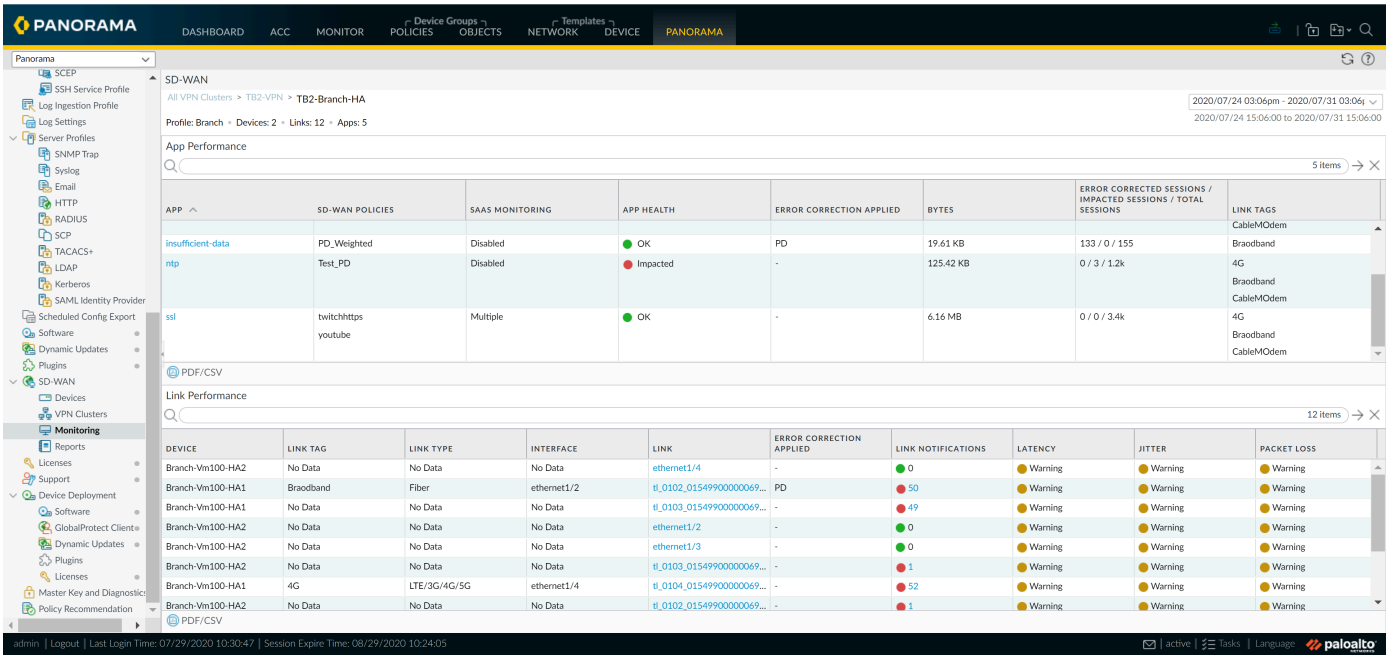
- Performance des applications
  - **Impacted** (impactée) — une ou plusieurs applications du Cluster VPN pour lequel aucun des chemins ne présente de performance suffisante, de gigue, latence ou perte de paquets, qui atteint ou est inférieur aux seuils indiqués dans le Profil de Qualité de chemin de la liste des chemins qui peuvent être choisis.

- **OK** : Applications dans le Cluster VPN qui sont saines et ne subisse aucune gigue, latence ou performance de perte de paquets.

- Performance des liens
  - **Error (erreur)** : une ou plusieurs applications du Cluster VPN pour lequel aucun des chemins ne présente de performance suffisante, de gigue, latence ou perte de paquets, qui atteint ou est inférieur aux seuils indiqués dans le Profil de Qualité de chemin de la liste des chemins qui peuvent être choisis.
  - **Warning (avertissement)** : un ou plusieurs sites du Cluster VPN qui ont des liens présentant des mesures de performance de gigue, latence ou perte de paquets qui ne peuvent être comparés de façon favorable avec la valeur de la moyenne flottante sur sept jours de la mesure.
  - **OK** : Liens dans le Cluster VPN qui sont saines et ne subisse aucune gigue, latence ou performance de perte de paquets.



Cliquez sur un widget pour avoir un aperçu plus détaillé de tous les clusters VPN de l'état de santé désiré. De plus, vous pouvez le filtre de sites pour afficher les clusters VPN sur la base des notifications de liens, déviations de latence, déviations de gigue, déviations de perte de paquets ou applications impactées.



Rapports SD-WAN

- **Panorama** > **SD-WAN** > **Rapports**

Générez un rapport de performance de l'application ou du lien pour les applications ou les liens principaux qui ont subi la fréquence la plus élevée de dégradation de santé au cours de la période indiquée des besoins d'audit. Après qu'un rapport ait été configuré, vous devez **Run now (lancer maintenant)** afin d'afficher le rapport. Les rapports peuvent être exportés la fonctionnalité ne fonctionne pas pour le moment; Dans quels formats les rapports peuvent-ils être exportés ?

Champ	Description
Name (Nom)	Saisissez un nom qui identifie l'objectif du rapport.
Types de rapport	Sélectionnez le type de rapport à lancer : • **App Performance (Performance de l'appli)** : Génère un rapport détaillant les mesures de santé de tout le trafic d'application dans le SD-WAN. • **App Performance (Performance de l'appli)** : Génère un rapport détaillant les mesures de santé de tout le trafic d'application dans le SD-WAN.
Cluster	Dans le menu déroulant, sélectionnez le cluster pour lequel vous voulez générer un rapport. Par défaut, **all** (tous) est sélectionné.
Site	Dans le menu déroulant, sélectionnez le site pour lequel vous voulez générer un rapport. Par défaut, **all** (tous) est sélectionné. Si **all (tous)** est sélectionné pour le cluster, alors vous devez générer un rapport pour tous les sites attribués au cluster. Si un cluster spécifique est sélectionné, alors vous pouvez sélectionner un site spécifique pour lequel générer un rapport.

Champ	Description
Application (Type d rapport de performance des applications uniquement)	Dans le menu déroulant, sélectionnez l'application pour laquelle vous voulez générer un rapport. Par défaut, **all** (tous) est sélectionné. Si **all (tous)** est sélectionné pour le Site, alors vous devez générer un rapport pour toutes les applications attribuées au site. Si un site spécifique est sélectionné, alors vous pouvez sélectionner une application spécifique pour laquelle générer un rapport.
Etiquette de liens (Type de rapport de performance de lien uniquement)	Dans le menu déroulant, sélectionnez une étiquette de lien pour laquelle vous voulez générer un rapport. Par défaut, **all** (tous) est sélectionné. Si **all (tous)** est sélectionné pour le Site, alors vous devez générer un rapport pour toutes les étiquettes de liens créées sur le site. Si un site spécifique est sélectionné, alors vous pouvez sélectionner une étiquette de lien spécifique pour laquelle générer un rapport.
Type de lien (Type de rapport de performance de lien uniquement)	Dans le menu déroulant, sélectionnez un type de lien pour laquelle vous voulez générer un rapport. Par défaut, **all** (tous) est sélectionné. Si **all (tous)** est sélectionné pour l'Étiquette de lien, alors vous devez générer un rapport pour tous les types de liens créées sous l'Étiquette de lien. Si une Etiquette de lien est sélectionnée, alors vous pouvez sélectionner une type de lien spécifique pour lequel générer un rapport.
Top N	Indiquez le nombre d'applications ou liens à inclure dans le rapport. Vous pouvez sélectionnez afin que le rapport inclue les 5, 10, 25, 50, 100, 250, 500, ou 1000 premiers applications ou liens performants. Par défaut, **5** est sélectionné.
Période de temps	Indiquez la durée pour laquelle le rapport est lancé. **None (Aucun)** est sélectionné par défaut, ce qui génère un rapport utilisant toutes les données de performance de l'application ou du lien.

Panorama > VMware NSX

Afin d'automatiser la configuration d'un pare-feu VM-Series Édition NSX, vous devez activer la communication entre NSX Manager et Panorama. Lorsque Panorama enregistre le pare-feu VM-Series en tant que service sur NSX Manager, ce dernier dispose des paramètres de configuration nécessaires pour configurer une ou plusieurs instances des pare-feu VM-Series sur chaque hôte ESXi du cluster.

Que voulez-vous savoir ?	Reportez-vous à la section :
Comment puis-je configurer un Groupe de notification ?	Configuration d'un groupe de notification
Comment puis-je définir la configuration du pare-feu VM-Series Édition NSX ?	Création de définitions de services
Comment puis-je configurer Panorama pour communiquer avec NSX Manager ?	Configuration de l'accès à NSX Manager
Comment puis-je définir les règles de redirection du pare-feu VM-série NSX Édition ?	Création de règles de redirection
Comment puis-je configurer le pare-feu afin d'appliquer uniformément la politique dans l'environnement vSphere dynamique ?	Sélectionnez Objets > Groupes d'adresses et Politiques > Sécurité Pour que Panorama et les pare-feu apprennent les changements qui surviennent dans l'environnement virtuel, utilisez les Groupes d'adresses dynamiques en tant qu'objets d'adresses source et destination dans les prérègles de politique de Sécurité.
Vous souhaitez en savoir plus ?	Voir Configuration d'un pare-feu série VM Édition NSX

Configuration d'un groupe de notification

- Panorama > Groupes de notification

Le tableau suivant décrit les paramètres du groupe de notification Panorama.

Paramètres du groupe de notification	Description
Nom	Saisissez un nom descriptif pour votre groupe de notification.
Informer le périphérique	Cochez les cases des groupes de périphériques qui doivent être informés des modifications ou des ajouts aux machines virtuelles déployées sur le réseau.

Paramètres du groupe de notification	Description
	Lorsque de nouvelles machines virtuelles sont configurées et les machines existantes sont modifiées, les modifications effectuées sur le réseau virtuel sont fournies comme mises à jour de Panorama. Lorsqu'il est configuré pour le faire, Panorama pré-remplit et met à jour les objets d'adresses dynamiques auxquels font référence les règles de politique afin que les pare-feu des groupes de périphériques précisés reçoivent les modifications apportées aux adresses IP enregistrées dans les groupes d'adresses dynamiques. pour activer les notifications, assurez-vous de sélectionner chacun des groupes de périphériques pour lesquels vous voulez activer les notifications. Si vous n'êtes pas en mesure de sélectionner un groupe de périphériques (aucune case à cocher disponible), le groupe de périphériques est automatiquement inclut parce qu'il fait partie d'une hiérarchie de groupe de périphériques. Ce processus de notification crée une sensibilité au contexte et garantit la sécurité des applications sur le réseau. Si, par exemple, vous disposez d'un groupe de pare-feu de périmètre matériels qui doit être averti lorsqu'une nouvelle application ou un nouveau serveur Web est déployé, ce processus actualise automatiquement les groupes d'adresses dynamiques du groupe de périphériques donné. De plus, toutes les règles de politique qui font référence à l'objet adresse dynamique incluent alors automatiquement toute nouvelle application ou tout nouveau serveur Web et peuvent être activées en toute sécurité en fonction de vos critères.

Création de définitions de services

- Panorama > VMware NSX > Définitions du service

Une définition de service vous permet d'enregistrer le pare-feu VM-Series en tant que service de sécurité partenaire sur NSX Manager. Vous pouvez définir un maximum de 32 définitions de service sur Panorama et les synchroniser sur NSX Manager.

Généralement, vous créerez une définition de service pour chaque client d'un cluster ESXi. Chaque définition de service précise l'OVF (version de PAN-OS) utilisé pour déployer le pare-feu et comprend la configuration des pare-feu VM-Series installés sur le cluster ESXi. Pour préciser la configuration, une définition de service doit avoir un modèle unique, un groupe de périphériques unique et les codes d'autorisation des licences pour les pare-feu qui seront déployés au moyen de la définition de service. Une fois le pare-feu déployé, ce dernier se connecte à Panorama et reçoit les deux paramètres de configuration (notamment la ou les zones pour chacun des clients ou des départements que le pare-feu sécurisera) et les paramètres de politique du groupe de périphériques indiqué dans la définition de service.

Pour ajouter une nouvelle définition de service, configurez les paramètres comme décrit dans le tableau suivant.

Champ	Description
Nom	Saisissez le nom du service que vous voulez afficher sur NSX Manager.
Description	(Facultatif) Saisissez une étiquette pour décrire l'objet ou la fonction de cette définition de service.
Groupe de périphériques	Sélectionnez le groupe de périphériques ou la hiérarchie de groupe de périphériques auquel ces pare-feu VM-Series seront affectés. Pour plus d'informations, voir Panorama > VMware NSX.
Modèle	Sélectionnez le modèle auquel les pare-feu VM-Series seront affectés. Pour plus d'informations, voir Panorama > Modèles. Chaque définition de service doit être assignée à un modèle unique ou à une pile de modèles unique. Des zones multiples (Zones de profil du service NSX pour NSX) peuvent être associées à un modèle. Pour un déploiement d'un client unique, créez une zone (Zone de profil du service du pare-feu NSX) dans le modèle. Si vous disposez d'un déploiement de locataires multiples, créez une zone par sous-client. Lorsque vous créez une nouvelle zone de profil du service du pare-feu NSX, celle-ci est automatiquement liée à une paire de sous-interfaces de câble virtuel. Pour plus d'informations, voir Réseau > Zones.
URL OVF VM-Series	Saisissez l'URL (adresse IP ou nom d'hôte et chemin d'accès) via laquelle NSX Manager peut accéder au fichier OVF pour configurer de nouveaux pare-feu VM-Series.
Groupes de notification	Sélectionnez un groupe de notification dans le menu déroulant.

Configuration de l'accès à NSX Manager

- Panorama > VMware NSX > Gestionnaires de service

Pour permettre à Panorama de communiquer avec le NSX Manager, vous devez **Ajouter** et configurer les paramètres comme décrit dans le tableau suivant.

Gestionnaires de service	Description
Nom du gestionnaire de services	Saisissez un nom permettant d'identifier le pare-feu VM-Series en tant que service. Ce nom s'affiche sur NSX Manager et est utilisé pour déployer le pare-feu VM-Series sur demande. Entrez 63 caractères maximum, n'utilisez que des lettres, chiffres, traits d'union et traits de soulignement.

Gestionnaires de service	Description
Description	(Facultatif) Saisissez une étiquette pour décrire l’objet ou la fonction de ce service.
URL de NSX Manager	Définissez l’URL que Panorama peut utiliser pour établir la connexion à NSX Manager.
Connexion au NSX Manager	Saisissez les informations d'identification d'authentification (nom d'utilisateur et mot de passe) configurées sur NSX Manager. Panorama utilise ces informations d’identification pour s’authentifier auprès de NSX Manager.
Mot de passe NSX Manager	
Confirmer le mot de passe NSX Manager	
Définitions du service	Spécifiez les définitions de service associées à ce gestionnaire de service. Chaque gestionnaire de service prend en charge jusqu’à 32 définitions de service.

Après avoir validé les modifications apportées à Panorama, la page VMware Service Manager affiche l’état de la connexion entre Panorama et NSX Manager.

Statut de synchronisation	Description
État	Affiche le statut de la connexion entre Panorama et NSX Manager. Lorsque la connexion a réussi, l'état affiché est Enregistré - Panorama et NSX Manager sont synchronisés et le pare-feu VM-Series est enregistré en tant qu’un service sur NSX Manager. Pour une connexion non réussie, l'état peut être : • **Erreur de connexion** - impossible d’atteindre/établir une connexion réseau avec NS Manager. • **Non autorisé** - Les informations d’identification d’accès (nom d’utilisateur et/ou mot de passe) ne sont pas correctes. • **Non enregistré** - Le gestionnaire de service, la définition de service ou le profil de service n’est pas disponible ou a été supprimé sur NSX Manager. • **Non synchronisé** - Les paramètres de configuration définis sur Panorama sont différents de ceux définis sur NSX Manager. Cliquez sur **Non synchronisé** pour connaître les détails de la raison de l’échec. Par exemple, NSX Manager peut disposer d’une définition de service ayant le même nom que celui qui est défini sur Panorama. Pour corriger l’erreur, utilisez le nom de la définition de service qui est indiqué dans le message d’erreur afin de valider la définition de service sur NSX Manager. Jusqu’à ce que la configuration sur Panorama et celle sur

Statut de synchronisation	Description
	NSX Manager soient synchronisées, vous ne pouvez pas ajouter de nouvelle définition de service sur Panorama.
Synchroniser les objets dynamiques	Cliquez sur **Synchroniser les objets dynamiques** pour actualiser les informations relatives à l'objet dynamique sur NSX Manager. La synchronisation des objets dynamiques vous permet de conserver le contexte des modifications dans l'environnement virtuel et vous permet d'activer des applications en toute sécurité grâce à la mise à jour automatique Groupes d'adresses dynamiques utilisés dans les règles de politique. *Sur Panorama, vous pouvez afficher uniquement les adresses IP enregistrées de manière dynamique à partir de NSX Manager. Panorama n'affiche pas les adresses IP enregistrées directement sur les pare-feu. Si vous utilisez des sources d'information de machine virtuelle (non prises en charge sur les pare-feu VM-Series Édition NSX) ou l'API XML pour enregistrer les adresses IP dynamiquement sur les pare-feu, vous devez vous connecter à chacun des pare-feu pour voir la liste complète des adresses IP dynamiques (celles que Panorama applique et celles qui sont enregistrées localement) sur le pare-feu.*
Synchronisation de la configuration NSX	Sélectionnez **Synchronisation de la configuration NSX** pour synchroniser les définitions de service configurées sur Panorama avec NSX Manager. Cette option n'est pas disponible si des validations sont en attente sur Panorama. Si la synchronisation échoue, affichez les détails du message d'erreur pour savoir si l'erreur s'est produite sur Panorama ou sur NSX Manager. Par exemple, si vous supprimez une définition de service sur Panorama, la synchronisation avec le NSX Manager échoue si une règle de NSX Manager y fait référence. Utilisez l'information présentée dans le message d'erreur pour déterminer la raison de l'échec ainsi que l'emplacement où les mesures correctives doivent être prises (sur Panorama ou sur NSX Manager).

Création de règles de redirection

- Panorama > VMware NSX > Règles de redirection

Les règles de redirection déterminent le trafic de quels invités du cluster est redirigé vers le pare-feu VM-Series.

Champ	Description
Générer automatiquement	Génère les règles de redirection en fonction d'une règle de sécurité configurée comme suit :

Champ	Description
les règles de redirection	• appartient à un groupe de périphériques parent ou enfant enregistré auprès d'un gestionnaire de services NSX ; • présente la même zone que la source et la destination (pas indifférent pour indifférent) ; • n'a qu'une seule zone ; • n'a aucun groupe d'adresses statiques, plage d'adresses IP ou masque de réseau configuré pour la politique. Par défaut, les règles de redirection générées au moyen de Panorama n'ont pas de services NSX configurés et la Direction du trafic NSX est définie sur entrée-sortie. Après avoir généré des règles de redirection, vous pouvez mettre à jour les règles de redirection individuelles pour modifier la Direction du trafic NSX ou ajouter des services NSX. Panorama renseigne automatiquement les champs suivants (sauf Description et services NSX) lorsque vous générez automatiquement les règles de redirection.
Nom	Saisissez le nom de la règle de direction que vous voulez afficher sur NSX Manager. Lorsqu'il est généré automatiquement, Panorama ajoute le préfixe « auto_ » à chaque règle de redirection et remplace tout espace dans le nom de la règle de politique de sécurité par un trait de soulignement (_).
Description	(Facultatif) Saisissez une étiquette pour décrire l'objet ou la fonction de cette définition de service.
Direction du trafic NSX	Indiquez la direction du trafic qui est redirigé vers le pare-feu VM-Series. • **Entrée-sortie** – Crée une règle ENTRÉE-SORTIE sur NSX. Le trafic du type spécifié se trouvant entre la source et la destination est redirigé vers le pare-feu VM-Series. Panorama utilise cette direction de trafic pour les règles de redirection générées automatiquement. • **Entrée** – Crée une règle ENTRÉE sur NSX. Le trafic du type spécifié se dirigeant vers la source depuis la destination est redirigé vers le pare-feu VM-Series. • **Sortie** – Crée une règle SORTIE sur NSX. Le trafic du type spécifié se dirigeant vers la destination depuis la source est redirigé vers le pare-feu VM-Series.
Services NSX	Sélectionnez le trafic de l'application (serveur Active Directory, HTTP, DNS, etc.) à rediriger vers le pare-feu VM-Series.
Groupe de périphériques	Sélectionnez un groupe de périphériques dans le menu déroulant. Le groupe de périphériques choisi détermine les politiques de sécurité qui sont appliquées à la règle de redirection. Les groupes de périphériques doivent être associés à une définition du service NSX.

Champ	Description
Politique de Sécurité	La règle de politique de sécurité sur laquelle se base la règle de redirection générée automatiquement.

Panorama > Profil d’ingestion des journaux

Utilisez le profil d’ingestion de journaux pour permettre à Panorama de recevoir des journaux à partir de sources externes. Dans PAN-OS 8.0.0, Panorama (en mode Panorama) peut servir de récepteur Syslog qui peut ingérer des journaux du serveur Traps ESM à l’aide de Syslog. La prise en charge de nouvelles sources de journaux externes et les mises à jour pour les nouvelles versions de Traps ESM seront appliquées par des mises à jour de contenu.

Pour activer l’ingestion du journal, vous devez configurer Panorama comme un récepteur Syslog sur le serveur Traps ESM, définir un profil d’ingestion de journal sur Panorama et joindre le profil d’ingestion de journal à un groupe de collecteur de journaux.

Pour ajouter un nouveau profil d’ingestion Syslog externe, cliquez sur **Ajouter** un profil et configurez les paramètres comme décrits dans le tableau suivant.

Champ	Description
Name (Nom)	Saisissez le nom du profil d’ingestion Syslog externe. Vous pouvez ajouter jusqu’à 255 profils.
Nom de la source	Saisissez le nom ou l’adresse IP des sources externes qui enverront des journaux. Vous pouvez ajouter jusqu’à 4 sources dans un profil.
Port	Saisissez le port sur lequel Panorama sera accessible sur le réseau et celui qu’il utilisera pour communiquer et écouter. Pour Traps ESM, sélectionnez une valeur comprise entre 23 000 et 23 999. Vous devez configurer le même numéro de port sur le Traps ESM pour permettre la communication entre Panorama et l’ESM.
Transport	Sélectionnez TCP, UDP ou SSL. Si vous sélectionnez SSL, vous devez configurer un certificat entrant pour une communication Syslog sécurisée dans Panorama > Collecteurs gérés > Généralités.
Type de journal externe	Sélectionnez le type de journal dans le menu déroulant.
Version	Sélectionnez la version dans le menu déroulant.

Utilisez Surveillance > Journaux externes pour afficher les informations sur les journaux ingérés dans le serveur Traps ESM vers Panorama.

Panorama > Paramètres des journaux

Utilisez la page des **Paramètres du journal** pour transmettre les types de journaux suivants aux services externes :

- les journaux système, de configuration, d'User-ID et de corrélation que le serveur de gestion Panorama (appareil de la série M ou appareil virtuel panoramique en mode panoramique) génère localement ;
- les journaux de tous types qui sont générés localement par l'appareil virtuel Panorama en Mode hérité ou qui sont rassemblés à partir des pare-feu.

> *Pour les journaux que les pare-feu envoient aux collecteurs de journaux, terminez la* Configuration du collecteur de journaux *pour permettre le transfert vers des services externes.*

Avant de commencer, vous devez définir des profils de serveur pour les services externes (voir Périphérique > Profils de serveur > Traps SNMP, Périphérique > Profils de serveur > Syslog, Périphérique > Profils de serveur > E-mail, et Périphérique > Profils de serveur > HTTP). Vous pouvez ensuite **Ajouter** un ou plusieurs profils de liste de correspondance et configurer les paramètres comme décrits dans le tableau suivant.

Paramètres du profil de la liste de correspondance	Description
Name (Nom)	Saisissez un nom (jusqu'à 31 caractères) pour identifier le profil de la liste de correspondance.
Filtre	Par défaut, Panorama transfère **Tous les journaux** au type pour lequel vous ajoutez le profil de liste de correspondance. Pour transférer un sous-ensemble de journaux, ouvrez le menu déroulant et sélectionnez un filtre existant ou sélectionnez **Filter Builder (Générateur de filtre)** pour ajouter un nouveau filtre. Pour chaque requête dans un nouveau filtre, il vous faut renseigner les champs suivants et **Add (Ajouter)** la requête : • **Connector (Connecteur)** – Sélectionnez le connecteur logique (et/ou) pour la requête. Sélectionnez **Negate (Ignorer)** si vous ne voulez pas appliquer le connecteur logique. Par exemple, pour éviter de transférer les journaux à partir d'une zone non approuvée, sélectionnez **Negate (Ignorer)**, sélectionnez **Zone** en tant qu'attribut, sélectionnez **equal (égal)** en tant qu'Opérateur et saisissez le nom de la Zone non approuvée dans la colonne Valeur. • **Attribute (Attribut)** – Sélectionnez un attribut de journal. Les options dépendent du type de journal. • **Operator (Opérateur)** - Sélectionnez des critères pour déterminer si un attribut s'applique (comme =). Les options disponibles dépendent du type de journal. • **Valeur** - Indiquez la valeur de l'attribut à faire correspondre avec la requête.

Paramètres du profil de la liste de correspondance	Description
	Pour afficher ou exporter les journaux auxquels correspond le filtre, sélectionnez **Afficher les journaux filtrés**. Cet onglet propose les mêmes options que les pages de l'onglet **Monitoring (Surveillance)** (telles que **Monitoring (Surveillance)** > **Logs (Journaux)** > **Traffic (Trafic)**).
Description	Saisissez une description contenant jusqu'à 1 024 caractères afin d'expliquer le but de ce profil de liste de correspondance.
SNMP	Cliquez pour **Ajouter** un ou plusieurs profils de serveur pour transférer des journaux en tant que pièges SNMP (voir Périphérique > Profils de serveur > Piège SNMP).
Messagerie	Cliquez pour **Ajouter** un ou plusieurs profils de serveur de messagerie pour transférer des journaux en tant que notifications par e-mail (voir Périphérique > Profils de serveur > E-mail).
Syslog	Cliquez pour **Ajouter** un ou plusieurs profils de serveur Syslog pour transférer des journaux en tant que messages Syslog (voir Périphérique > Profils de serveur > Syslog).
HTTP	Cliquez pour **Ajouter** un ou plusieurs profils de serveur HTTP pour transférer des journaux en tant que requêtes HTTP (voir Périphérique > Profils de serveur > HTTP).
Actions intégrées	Tous les types de journaux, à l'exception des Journaux système et des Journaux de configuration, vous permettent de configurer des actions. • Cliquez pour **Ajouter** une action et saisissez un nom pour la décrire. • Sélectionnez l'adresse IP que vous souhaitez identifier – **Adresse source** ou **Adresse de destination**. • Sélectionnez l'action – **Add Tag (Ajouter une étiquette)** ou **Remove Tag (Supprimer une étiquette)**. • Choisissez si vous souhaitez distribuer l'étiquette à l'agent User-ID local de ce périphérique ou à un agent User-ID distant. • Pour distribuer des étiquettes à un **Agent User-ID de périphérique distant**, sélectionnez le profil du serveur HTTP qui permettra le transfert. • Configurez le **Timeout (Délai)**, en minutes, de l'indicateur d'adresse IP à définir, la période de temps pendant laquelle le mappage adresse IP/ étiquette est maintenu. Si vous définissez le délai sur 0, le mappage de

Paramètres du profil de la liste de correspondance	Description
	l’indicateur d'adresse IP n’expire jamais (la plage est définie entre 0 et 43 200 [30 jours] ; la valeur par défaut est 0). *Vous pouvez uniquement configurer un délai avec l’action **Add Tag (Ajouter une étiquette)**.* • Saisissez ou sélectionnez les **Tags (Étiquettes)** que vous souhaitez appliquer ou supprimer de la source cible ou de l’adresse IP de destination. Vous pouvez étiqueter l’adresse IP source uniquement dans les Journaux de corrélation et les Journaux de correspondance HIP.

Panorama > Profils de serveur > SCP

- Panorama > Profils de serveur > SCP

Sélectionnez **Panorama** > **Server Profiles (Profils de serveur)** > **SCP** pour configurer les paramètres du serveur Secure Copy Protocol (SCP) afin de copier et transférer en toute sécurité des fichiers sur votre réseau afin que vous puissiez télécharger et installer automatiquement des mises à jour du contenu sur les pare-feux gérés, Collecteurs de journaux, et appareils WildFire® gérés par un serveur de Panorama™ à air gap.

Paramètres d'un serveur SCP	Description
Name (Nom)	Saisissez un nom pour identifier le profil de serveur (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. Utilisez uniquement des lettres, nombres, espaces, traits d’union et de soulignement.
Serveur	Saisissez l’adresse IP ou le FQDN.
Port	Saisissez le port du serveur pour le transfert de fichiers (plage de 1 à 65 535 ; la valeur par défaut est de 22).
Username (Nom d’utilisateur)	Saisissez le nom d'utilisateur utilisé pour accéder au serveur SCP.
Mot de passe Confirmez le mot de passe	Saisissez et confirmez le mot de passe sensible à la casse pour le nom d'utilisateur utilisé pour accéder au serveur SCP.

Panorama > Exportation programmée des configurations

Pour planifier une exportation de toutes les configurations en cours d'exécution sur Panorama et les pare-feu, il vous faut **Ajouter** une tâche d'exportation et configurer les paramètres, comme décrit dans le tableau suivant.

Si Panorama est dans une configuration haute disponibilité (HD), vous devez suivre ces instructions sur chaque homologue pour vous assurer que les exportations planifiées continuent après un basculement. Panorama ne synchronise pas les exportations de configuration planifiées entre les homologues HD.

Paramètres d'exportation de configuration programmée	Description
Name (Nom)	Donnez un nom pour identifier la tâche d'exportation de configuration (31 caractères maximum). Celui-ci est sensible à la casse et doit être unique. N'utilisez que des lettres, chiffres, traits d'union et traits de soulignement.
Description	Saisissez une description (facultatif).
Activer	Sélectionnez cette option pour activer la tâche d'exportation.
Heure (quotidienne) de début de l'exportation programmée	Indiquez l'heure du jour de démarrage de l'exportation (horloge 24 heures, format HH:MM).
Protocole	Sélectionnez le protocole à utiliser pour l'exportation des journaux entre Panorama et un hôte distant. Secure Copy (**SCP**) est un protocole sécurisé ; **FTP** ne l'est pas.
Nom d'hôte	Saisissiez l'adresse IP ou le nom d'hôte du serveur SCP ou FTP cible.
Port	Saisissez le numéro de port du serveur cible.
Chemin d'accès	Indiquez le chemin d'accès au dossier ou au répertoire sur le serveur cible où les informations exportées seront enregistrées. Par exemple, si l'ensemble de configuration est conservé dans un dossier nommé exported_config dans un dossier racine nommé Panorama, la syntaxe de chacun des types de serveur est : • Serveur SCP : /Panorama/exported_config • Serveur FTP : //Panorama/exported_config Les caractères suivants : **.**(point), **+**, **{** et **}**, **/**, **-**, **_**, **0-9**, **a-z**, et **A-Z**. Les espaces ne sont pas pris en charge dans le fichier **Chemin d'accès**.

Paramètres d’exportation de configuration programmée	Description
Activer le mode passif FTP	Sélectionnez cette option pour utiliser le mode passif FTP.
Username (Nom d’utilisateur)	Indiquez le nom d’utilisateur requis pour l’accès au système cible.
Mot de passe/Confirmer le mot de passe	Indiquez le mot de passe requis pour l’accès au système cible. Utilisez un mot de passe d’une longueur maximale de 15 caractères. Si le mot de passe dépasse 15 caractères, la connexion SCP d’essai affichera une erreur, car le pare-feu chiffre le mot de passe lorsqu’il tente de se connecter au serveur SCP et la longueur du mot de passe chiffré peut comporter un maximum de 63 caractères.
Tester la connexion au serveur SCP	Sélectionnez cette option pour vérifier la communication entre Panorama et l’hôte / le serveur SCP. Une fenêtre contextuelle s'affiche vous obligeant à entrer un **Password (Mot de passe)** en texte clair, puis à **Confirm Password (Confirmer le mot) de passe** afin de tester la connexion au serveur SCP et de permettre le transfert sécurisé des données.Confirmer le mot de passe Si Panorama dispose d’une configuration HD, effectuez cette étape sur chaque homologue HD afin que chacun accepte la clé d'hôte du serveur SCP. Si Panorama peut se connecter avec succès au serveur SCP.

Panorama > Logiciel

Utilisez cette page pour gérer les mises à jour logicielles de Panorama sur le serveur de gestion Panorama.

- Gestion des mises à jour logicielles Panorama
- Affichage des informations sur les mises à jour logicielles Panorama

Gestion des mises à jour logicielles Panorama

Sélectionnez **Panorama** > **Software (Logiciel)** pour effectuer les tâches décrites dans le tableau suivant.

Par défaut, le serveur de gestion Panorama enregistre jusqu'à deux mises à jour logicielles. Pour libérer de l'espace pour les plus récentes mises à jour, le serveur supprime automatiquement la mise à jour la plus ancienne. Vous pouvez modifier le nombre d'images logicielles enregistrées par Panorama *et supprimer manuellement des images afin de libérer de l'espace.*

Pour obtenir plus d'informations sur la compatibilité des versions, reportez-vous à Installer les mises à jour de contenu et logicielles pour Panorama.

Tâche	Description
Vérifier maintenant	Si Panorama dispose d'un accès à Internet, cliquez sur **Vérifier maintenant** pour afficher les plus récentes informations sur les mises à jour (voir Affichage des informations sur les mises à jour logicielles Panorama). Si Panorama n'a pas accès au réseau externe, utilisez un navigateur pour vous rendre sur le site de Mise à jour logicielle pour des informations sur la mise à jour.
Télécharger	Pour télécharger une image logicielle lorsque Panorama ne dispose pas d'un accès à Internet, utilisez un navigateur pour vous rendre sur le site deMise à jour logicielle, trouvez la version désirée et téléchargez l'image logicielle vers un ordinateur auquel Panorama peut accéder. Sélectionnez **Panorama** > **Software (Logiciel)**, cliquez sur **Upload (Télécharger)**, **Browse (Rechercher)** et sélectionnez l'image logicielle, puis cliquez sur **OK**. Une fois que le téléchargement est terminé, la colonne Téléchargé affiche une coche et**Install (Installer)** s'affiche dans la colonne Action.
Valider	Si Panorama dispose d'un accès à Internet, **Validez** (colonne Action) pour obtenir la version souhaitée. Sélectionnez les appareils que vous souhaitez mettre à niveau (colonne Déployer), sélectionnez **Panorama** comme source de mise à niveau, puis cliquez sur **Télécharger**. Une fois le téléchargement terminé, la colonne Disponible affiche une coche.

Tâche	Description
	*Le **serveur SCP** et le **serveur de mise à jour** ne sont pas disponibles en tant que sources de téléchargement* *dans PAN-OS 10.2.0.*
Installer	**Installez** (colonne Action) l’image logicielle. À l'issue de l'installation, Panorama vous déconnecte lorsqu’il redémarre. *Panorama contrôle régulièrement l'intégrité du système de fichiers (FSCK) afin d'éviter une corruption des fichiers système de Panorama. Ce contrôle se produit après huit redémarrages ou lors d'un démarrage survenant 90 jours après le dernier FSCK. Un avertissement s'affiche sur l'interface Web et sur les écrans de connexion SSH si un contrôle FSCK est en cours et que vous ne pouvez pas vous connecter tant que celui-ci n'est pas terminé. La durée d’exécution de ce processus varie en fonction de la taille du système de stockage; si système est important, vous devrez probablement compter plusieurs heures avant de pouvoir vous reconnecter à Panorama. Pour consulter la progression, configurez l'accès de la console à Panorama.*
Notes de version	Si Panorama dispose d’un accès à Internet, vous pouvez accéder aux **Notes de version** de la version logicielle souhaitée et passer en revue les modifications apportées à la version, les correctifs, les problèmes connus, les problèmes de compatibilité et les changements apportés au comportement par défaut. Si Panorama n’a pas accès à Internet, utilisez un navigateur pour vous rendre sur le site de Mise à jour logicielle et téléchargez la version appropriée.
	Supprime une image logicielle qui n'est plus nécessaire ou si vous souhaiter libérer de l’espace pour stocker d'autres images logicielles.

Affichage des informations sur les mises à jour logicielles Panorama

Sélectionnez **Panorama** > **Software (Logiciel)** pour afficher les informations suivantes. Pour afficher les dernières informations de Palo Alto Networks, cliquez sur **Check Now (Vérifier maintenant)**.

Informations sur les mises à jour logicielles et de contenu	Description
Version	La version de logiciel Panorama
Taille	La taille en mégaoctets de l’image logicielle.

Informations sur les mises à jour logicielles et de contenu	Description
Date de version	Date et heure de disponibilité de la mise à jour auprès de Palo Alto Networks.
Disponible	Indique si l’image est disponible pour son installation.
Actuellement installé	Un crochet indique que la mise à jour est déjà installée.
Action (Action)	Indique les actions (**Download (Télécharger)**, **Install (Installer)**, ou **Reinstall (Réinstaller)**) qui sont disponible pour une image.
Notes de version	Cliquez sur **Release Notes (Notes de version)** pour accéder aux notes de version de la version logicielle souhaitée et passer en revue les modifications apportées à la version, les correctifs, les problèmes connus, les problèmes de compatibilité et les changements apportés au comportement par défaut.
	Supprime une mise à jour qui n'est plus nécessaire ou pour libérer de l’espace pour procéder à d'autres chargements ou téléchargements.

Panorama > Déploiement du périphérique

Vous pouvez utiliser Panorama pour déployer des mises à jour de logiciels et de contenu sur plusieurs pare-feu et collecteurs de journaux et pour gérer des licences de pare-feu.

Que voulez-vous faire ?	Reportez-vous à la section :
Déployer les mises à jour de logiciel et de contenu sur les pare-feu et les collecteurs de journaux.	Gestion des mises à jour logicielles et de contenu
Savoir quelles sont les mises à jour de logiciel et de contenu qui ont été installées ou qui sont disponibles pour le téléchargement et l'installation.	Affichage des informations sur les mises à jour logicielles et de contenu
Programmer des mises à jour de contenu automatiques pour les pare-feu et les collecteurs de journaux.	Planification des mises à jour de contenu dynamiques
Rétablir les version de contenu précédentes de un ou plusieurs pare-feu de Panorama.	Rétablissement des versions de contenu précédentes de Panorama
Afficher, activer, désactiver et actualiser les licences. Afficher l'état des licences du pare-feu.	Gestion des licences du pare-feu
Vous souhaitez en savoir plus ?	Gestion des licences et des mises à jour.

Gestion des mises à jour logicielles et de contenu

- Panorama > Déploiement du périphérique > Logiciel

Panorama propose les options suivantes pour déployer des mises à jour logicielles et de contenu sur les pare-feu et les Collecteurs de journaux.

Pour réduire le trafic sur l'interface de gestion (MGT), vous pouvez configurer Panorama pour utiliser une interface distincte pour le déploiement de mises à jour (voir Panorama > Configuration > Interfaces*).*

Options de Déploiement du périphérique Panorama	Description
Téléchargement	Pour déployer une mise à jour logicielle ou de contenu lorsque Panorama est connecté à l'Internet, cliquez sur **Download (Télécharger)** la mise à jour. Une fois le téléchargement terminé, la colonne Disponible affiche Téléchargé. Vous pouvez ensuite : • Installer la mise à jour logicielle ou de contenu PAN-OS / Panorama. • Activer la mise à jour logicielle de l'application GlobalProtect™ ou du client VPN SSL.
upgrade	Si une mise à jour de contenu pour le Filtrage des URL BrightCloud est disponible, cliquez sur **Upgrade (Mettre à niveau)**. Après avoir effectué la mise à niveau, vous pouvez procéder à l'Installation de la mise à jour sur les pare-feu.
Installer	Après avoir effectué le Téléchargement ou le Chargement d'un logiciel PAN-OS, d'un logiciel Panorama ou de contenu, cliquez sur **Install (Installer)** dans la colonne Action et sélectionnez : • **Devices (Périphériques)** - Sélectionnez les pare-feu ou les collecteurs de journaux sur lesquels installer la mise à jour. Si la liste est longue, utilisez les filtres. Sélectionnez **Regrouper les homologues HA** pour regrouper des pare-feu qui sont des homologues haute disponibilité (HA). Cela vous permet d'identifier facilement les pare-feu présentant une configuration HA. Pour n'afficher que des pare-feu spécifiques ou des collecteurs de journaux spécifiques, sélectionnez-les, puis sélectionnez l'option **Filter Selected (Filtre sélectionné)**. • **Upload only to device (Charger uniquement sur le périphérique)** (logiciel uniquement) – Sélectionnez pour charger le logiciel sans l'installer automatiquement. Vous devez installer le logiciel manuellement. • **Reboot device after install (Redémarrer le périphérique après installation)** (logiciel uniquement) – Sélectionnez si vous voulez que le processus d'installation redémarre automatiquement les pare-feu ou les Collecteurs de journaux. L'installation n'est terminée qu'après un redémarrage du pare-feu. • **Disable new apps in content update (Désactiver les nouvelles applis dans la mise à jour de contenu)** (Applications et Menaces uniquement) – Sélectionnez pour désactiver les applications dans la mise à jour qui sont nouvelles par rapport à la dernière mise à jour installée. Cette façon de procéder vous protège contre les plus récentes menaces en vous offrant la souplesse d'activer les applications après avoir mis à jour les politiques. Ensuite, pour activer les applications, accédez au pare-feu, sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**, cliquez sur **Apps (Applications)** dans la colonne Features (Fonctions) pour afficher les nouvelles applications et cliquez sur **Enable/Disable (Activer / Désactiver)** pour chaque application que vous souhaitez activer.

Options de Déploiement du périphérique Panorama	Description
	Vous pouvez également sélectionner ***Panorama*** > ***Managed Devices (Périphériques gérés)*** *pour installer* les mises à jour logicielles et de contenu du pare-feu *ou* ***Panorama*** > ***Managed Collectors (Collecteurs gérés)*** *pour installer* les mises à jour logicielles pour les Collecteurs de journaux dédiés.
Activate (Activer)	Après avoir effectué le Téléchargement ou le Chargement d'une mise à jour logicielle de l'application GlobalProtect, cliquez sur **Activate (Activer)** dans la colonne Action et sélectionnez les options comme suit : • **Devices (Périphériques)** - Sélectionnez les pare-feu sur lesquels activer la mise à jour. Si la liste est longue, utilisez les filtres. Sélectionnez **Regrouper les homologues HA** pour regrouper des pare-feu qui sont des homologues haute disponibilité (HA). Cela vous permet d'identifier facilement les pare-feu présentant une configuration HA. Pour n'afficher que des pare-feu spécifiques, sélectionnez-les, puis l'option **Filter Selected (Filtre sélectionné)**. • **Upload only to device (Charger uniquement sur le périphérique)** – Sélectionnez si vous ne voulez pas que PAN-OS active automatiquement l'image chargée. Vous devez vous connecter au pare-feu et l'activer.
Notes de version	Cliquez sur **Release Notes (Notes de version)** pour accéder aux notes de version de la version logicielle souhaitée et passer en revue les modifications apportées à la version, les correctifs, les problèmes connus, les problèmes de compatibilité et les changements apportés au comportement par défaut.
Documentation	Cliquez sur **Documentation** pour accéder aux notes de versions de la version de contenu souhaitée.
	Supprime les mises à jour logicielles ou de contenu qui ne sont plus nécessaires ou si vous souhaitez libérer de l'espace pour procéder à d'autres chargements ou téléchargements.
Vérifier maintenant	**Check Now (Vérifier maintenant)** pour Afficher les informations sur les mises à jour logicielles et de contenu.
Télécharger	Pour déployer une mise à jour logicielle ou de contenu lorsque Panorama n'est pas connecté à Internet, téléchargez la mise à jour vers votre ordinateur à partir du site Mises à jour logicielles ou Mises à jour dynamiques, sélectionnez la page **Panorama** > **Device Deployment (Déploiement du périphérique)** qui correspond au type de mise à jour, cliquez sur **Upload (Télécharger)**, sélectionnez le **Type** de mise à jour (mises à jour de contenu uniquement), sélectionnez le fichier chargé et cliquez sur **OK**. Les étapes suivantes d'installation ou d'activation de la mise à jour dépendent du type :

Options de Déploiement du périphérique Panorama	Description
	• **PAN-OS or Panorama software (PAN-OS ou logiciel Panorama)** : Une fois que le téléchargement est terminé, la colonne Téléchargé affiche une coche et vous pouvez voir que **Install (Installer)** s'affiche dans la colonne Action. • **Client GlobalProtect ou Logiciel du client VPN SSL** – Activez depuis le fichier. • **Mises à jour dynamiques** – Installation à partir du fichier.
Installer depuis le fichier	Après avoir effectué le téléchargement d'une mise à jour de contenu, cliquez sur **Install from File (Installer depuis le fichier)**, sélectionnez le **Type** de contenu, sélectionnez le nom de fichier de la mise à jour et sélectionnez les pare-feu ou les Collecteurs de journaux.
Activer depuis le fichier	Après avoir effectué le téléchargement de la mise à jour logicielle de l'application GlobalProtect, cliquez sur **Activate from File (Activer depuis le fichier)**, sélectionnez le nom de fichier de la mise à jour et sélectionnez les pare-feu.
Calendriers	Sélectionnez pour Planifier des mises à jour de contenu dynamiques.

Affichage des informations sur les mises à jour logicielles et de contenu

- Panorama > Déploiement du périphérique > Logiciel

Sélectionnez **Panorama** > **Device Deployment (Déploiement du périphérique)** > **Software (Logiciel)** pour afficher le **Software (Logiciel)** PAN-OS, le logiciel **GlobalProtect Client (Client GlobalProtect)** et les **Dynamic Updates (Mises à jour dynamiques)** (contenu) actuellement installés ou disponibles pour le téléchargement et l'installation. La page **Dynamic Updates (Mises à jour dynamiques)** regroupe l'information par type de contenu (Antivirus, Applications et menaces, Filtrage des URL et WildFire) et indique la date et l'heure de la dernière vérification des informations mises à jour. Pour afficher les dernières informations relatives aux mises à jour logicielles et de contenu de Palo Alto Networks, cliquez sur **Check Now (Vérifier maintenant)**.

Informations sur les mises à jour logicielles et de contenu	
Version	La version de la mise à jour logicielle ou de contenu.
File Name (Nom du fichier)	Le nom du fichier de mise à jour.
Platform (Plateforme)	Le pare-feu ou le modèle de Collecteur de journaux désigné pour la mise à jour. Un nombre indique un modèle de pare-feu matériel (par exemple, `7 000` indique le pare-feu de la série PA-7000), `vm` indique le pare-feu VM-Series et `m` indique l'équipement M-Series.

Informations sur les mises à jour logicielles et de contenu	
Caractéristiques	(Contenu seulement) Répertorie le type de signatures que la version du contenu peut contenir.
Type	(Contenu seulement) Indique si le téléchargement inclut une mise à jour complète ou incrémentielle de la base de données.
Taille	La taille du fichier de mise à jour.
Date de version	Date et heure de disponibilité de la mise à jour auprès de Palo Alto Networks.
Disponible	(logiciel PAN-OS ou Panorama seulement) Indique que la mise à jour a été chargée ou téléchargée.
Téléchargé	(logiciel client VPN SSL, logiciel client GlobalProtect ou de contenu seulement) Une coche indique que la mise à jour a été téléchargée.
Action (Action)	Indique l'action que vous pouvez effectuer sur la mise à jour : Télécharger, Mettre à niveau, Installer ou Activer.
Documentation	(Contenu seulement) Fournit un lien vers les notes de version relatives à la version de contenu souhaitée.
Notes de version	(Logiciel seulement) Fournit un lien vers les notes de version relatives à la version logicielle souhaitée.
	Supprime une mise à jour qui n'est plus nécessaire ou si vous souhaitez libérer de l'espace pour procéder à d'autres chargements ou téléchargements.

Planification des mises à jour de contenu dynamiques

- Panorama > Déploiement de périphérique > Mises à jour dynamiques

Pour programmer un téléchargement et une installation automatiques d'une mise à jour, cliquez sur **Schedules (Calendriers)**, cliquez sur **Add (Ajouter)**, puis configurez les paramètres comme décrits dans le tableau suivant.

Paramètres de planification des mises à jour dynamiques	
Name (Nom)	Saisissez un nom pour identifier la tâche planifiée (31 caractères maximum). Le nom est sensible à la casse, doit être unique et ne peut contenir que des lettres, des chiffres, des traits d'union et des caractères de soulignement.
Désactivé	Sélectionnez pour désactiver la tâche planifiée.

Paramètres de planification des mises à jour dynamiques	
Download Source (Source de téléchargement)	Sélectionnez la source de téléchargement pour la mise à jour du contenu. Vous pouvez choisir de télécharger des mise à jour du contenu depuis le **Updates Server (serveur de mises à jour)** Palo Alto Networks ou depuis un serveur **SCP**.
Profil SCP (SCP uniquement)	Sélectionnez un profil SCP configuré depuis lequel télécharger.
Chemin d'accès SCP (SCP uniquement)	Saisissez le chemin d'accès spécifique sur le serveur SCP depuis lequel télécharger la mise à jour du contenu.
Type	Sélectionnez le type de la mise à jour de contenu à planifier : **App (Applications)**, **App and Threat (Applications et menaces)**, **Antivirus**, **WildFire** ou **URL Database (Base de données des URL)**.
Récurrence	Sélectionnez l'intervalle auquel Panorama se connecte au serveur de mises à jour. Les options de récurrence varient selon le type de mise à jour.
Période	Pour une mise à jour **Daily (Quotidienne)**, sélectionnez **Time (Heure)** au format d'horloge 24 heures. Pour une mise à jour **Weekly (Hebdomadaire)**, sélectionnez le **Day (Jour)** de la semaine et **Time (Heure)** au format d'horloge 24 heures.
Désactiver les nouvelles applis dans la mise à jour de contenu	Vous pouvez désactiver les nouvelles applications des mises à jour de contenu uniquement si vous définissez le **Type** sur **App (Applications)** ou sur **App and Threat (Applications et menaces)** et uniquement **Action** est définie sur **Download and Install (Télécharger et Installer)**. Sélectionnez pour désactiver des applications de la mise à jour qui sont nouvelles par rapport à la dernière mise à jour installée. Cette façon de procéder vous protège contre les plus récentes menaces en vous offrant la souplesse d'activer les applications après avoir mis à jour les politiques. Ensuite, pour activer les applications, accédez au pare-feu, sélectionnez **Device (Périphérique)** > **Dynamic Updates (Mises à jour dynamiques)**, cliquez sur **Apps (Applications)** dans la colonne Features (Fonctions) pour afficher les nouvelles applications et cliquez sur **Enable/Disable (Activer / Désactiver)** pour chaque application que vous souhaitez activer.
Action (Action)	• **Download Only (Télécharger seulement)** - Panorama™ téléchargera la mise à jour planifiée. Vous devez installer manuellement la mise à jour sur les pare-feu et les Collecteurs de journaux. • **Download and Install (Télécharger et installer)** - Panorama téléchargera et installera automatiquement la mise à jour planifiée. • **Download and SCP (Téléchargement et SCP)**: Panorama téléchargera et transfèrera le package de mise à jour du contenu sur le serveur SCP indiqué.

Paramètres de planification des mises à jour dynamiques	
Périphériques	Sélectionnez **Devices (Périphériques)**, puis sélectionnez les pare-feu qui recevront les mises à jour de contenu planifiées.
Collecteurs de journaux	Sélectionnez **Log Collectors (Collecteurs de journaux)**, puis sélectionnez les collecteurs gérés qui recevront les mises à jour de contenu planifiées.

Rétablissement des versions de contenu précédentes de Panorama

- Panorama > Déploiement de périphérique > Mises à jour dynamiques

Revert Content (Rétablissez les versions de contenu précédentes) Applications, Applications et Menaces, Antivirus, WildFire et les mises à jour de contenu WildFire d'un ou plusieurs pare-feu à la version de contenu installée précédemment sur Panorama. La version de contenu que vous rétablissez doivent être antérieure à celle qui est actuellement installée sur le pare-feu. Le rétablissement du contenu précédent est disponible sur Panorama 8.1. Le contenu des pare-feu peut être rétabli tant que la fonction de rétablissement est disponible localement sur le pare-feu.

Champ	Description
Filtre	Filtrer les périphériques sur lesquels vous aimeriez rétablir la version de contenu précédente. Vous pouvez appliquer les filtres suivants : • État de l'appareil • Plateformes • Groupes de périphériques • Modèles • Étiquettes • État HA • Version du logiciel (PAN-OS) • Version du contenu actuel
Périphériques	Sélectionnez un ou plusieurs périphériques devant faire l'objet du rétablissement. Affiche les informations sur le périphérique suivantes : • Nom du périphérique : le nom du périphérique. • Version actuelle : la version de contenu actuellement installée sur le périphérique. Un 0 sera indiqué dans la colonne si aucune version de contenu n'est installée. • Version (de contenu) antérieure : la version de contenu précédemment installée sur les pare-feu exécutant la version 8.1 de PAN-

Champ	Description
	OS ou toute version ultérieure. La colonne sera vide si aucune version de contenu n'était précédemment installée ou si le pare-feu utilise une version de PAN-OS antérieure à 8.1. • Version du logiciel : la version de PAN-OS qui est actuellement installée sur le périphérique. • État HA : affiche l'état HA lorsqu'il s'agit d'une paire HA. La colonne sera vide si le périphérique ne fait pas partie d'une paire HA.
Regrouper les paires HA	Cochez cette case pour regrouper les homologues HA.

Lorsque vous avez sélectionné les périphériques devant faire l'objet du rétablissement, cliquez sur **OK**.

Gestion des licences du pare-feu

- Sélectionnez Panorama > Déploiement de périphérique > Licences

Sélectionnez **Panorama** > **Déploiement de périphérique** > **Licences** pour effectuer les tâches suivantes :

- Mettre à jour les licences des pare-feu qui ne disposent pas d'un accès direct à Internet – Cliquez sur Rafraichir.
- Activer une licence sur des pare-feu – Pour activer une licence sur des pare-feu, cliquez sur **Activer**, sélectionnez les pare-feu et, dans la colonne Code d'authentification, saisissez les codes d'autorisation que Palo Alto Networks a fournis pour les pare-feu.
- Désactiver toutes les licences et tous les abonnements / droits installés sur des pare-feu Série VM – Cliquez sur **Désactiver les VM**, sélectionnez les pare-feu (la liste affiche uniquement les pare-feu qui sont exécutés sur PAN-OS 7.0 ou une version ultérieure), et cliquez sur :
  - **Continue (Continuer)** - Désactive les licences et enregistre automatiquement les modifications sur le serveur de licences. Les licences sont recréditées sur votre compte et peuvent être réutilisées.
  - **Complete Manually (Terminer manuellement)** - Génère un fichier de jeton. Utilisez ceci si Panorama ne dispose d'aucun accès direct à Internet. Pour terminer le processus de désactivation, vous devez vous connecter au Portail d'assistance, sélectionnez **Actifs**, cliquez sur **Désactiver la (les) licence(s)**, téléchargez le fichier de jeton, et cliquez sur **Soumettre**. Terminez ensuite le processus de désactivation.

Vous pouvez également afficher l'état actuel de la licence pour les pare-feu gérés. Dans le cas de pare-feu qui disposent d'un accès direct à Internet, Panorama effectue automatiquement une vérification quotidienne sur le serveur de licences, obtient les mises à jour et les renouvellements des licences et les applique aux pare-feu. La vérification est codée strictement pour s'effectuer entre 1 h et 2 h ; vous ne pouvez pas changer cet horaire.

Informations sur les licences du pare-feu	
Périphérique	Le nom du pare-feu.

Informations sur les licences du pare-feu	
Virtual System (système virtuel - vsys)	Indique si le pare-feu prend en charge  ou non  des systèmes virtuels multiples.
Prévention contre les menaces URL Assistance Passerelle GlobalProtect Portail GlobalProtect WildFire	Indique si la licence est active  inactive  ou expirée  (ainsi que la date d’expiration).
Capacité de la série VM	Indique s'il s'agit  ou non  d'un pare-feu VM-Series.

Panorama > Clé d’autorisation de l’enregistrement du périphérique

Pour renforcer votre posture de sécurité lors de l’intégration de nouveaux pare-feux, Collecteurs de journaux et appareils WildFire à un serveur d’administration Panorama™, créez une clé d’authentification d’enregistrement de périphérique pour l’authentification mutuelle entre un nouveau périphérique et le serveur d’administration Panorama lors de la première connexion. Vous pouvez configurer une clé d’authentification avec des valeurs spécifiques : la durée de vie de la clé, le nombre de fois que vous pouvez utiliser la clé d’authentification d’enregistrement de l’appareil pour intégrer de nouveaux pare-feux, une liste d’un ou plusieurs numéros de série pour lesquels la clé d’authentification d’enregistrement du périphérique est valide et spécifier le type de périphériques pour lesquels la clé d’authentification est valide. Après avoir créé une clé d'authentification sur Panorama, vous devez l'ajouter au nouveau pare-feu, collecteur de journaux ou appareil WildFire lors de l'intégration à la gestion de Panorama.

Champs de la lé d’autorisation de l’enregistrement du périphérique	Description
Nom	Nom de la clé d’authentification d’enregistrement de l’appareil. Le nom est sensible à la casse, doit être unique sur l’ensemble de la hiérarchie du groupe de périphériques et ne peut contenir que des lettres, des chiffres, des espaces, des traits d’union et des caractères de soulignement.
Durée de vie	La durée de vie de la clé affiche le nombre de jours, d’heures et de minutes pendant les jours, la clé d’authentification d’enregistrement du périphérique est valide pour intégrer de nouveaux pare-feux, Collecteurs de journaux et appareils WildFire.
Nombre	Nombre de fois que vous pouvez utiliser la clé d’authentification d’enregistrement du périphérique pour intégrer de nouveaux pare-feux, Collecteurs de journaux et appareils WildFire.
Série	Numéro de série d’un ou de plusieurs nouveaux pare-feux, Collecteurs de journaux et appareils WildFire pour lesquels la clé d’authentification d’enregistrement de périphérique est valide.
Type	Type de périphérique pour lequel la clé d’authentification est valide (`Any (n’importe lequel)`,`Firewalls (Pare-feux)`, ou `Log Collectors (Collecteurs de journaux)`).

Ajouter une clé d’autorisation de l’enregistrement du périphérique

Ajoutez et configurez une clé d’authentification d’enregistrement de périphérique pour intégrer de nouveaux pare-feu, collecteurs de journaux et appareils WildFire à Panorama.

Paramètres de la clé d'autorisation de l'enregistrement du périphérique	Description
Nom	Entrez un nom pour identifier la clé d'authentification d'enregistrement de l'appareil. Le nom est sensible à la casse, doit être unique sur l'ensemble de la hiérarchie du groupe de périphériques et ne peut contenir que des lettres, des chiffres, des espaces, des traits d'union et des caractères de soulignement.
Durée de vie	Spécifiez la durée de vie de la clé pendant laquelle vous pouvez utiliser la clé d'authentification d'enregistrement de périphérique pour intégrer de nouveaux pare-feux, Collecteurs de journaux et appareils WildFire.
Nombre	Spécifiez le nombre de fois que vous pouvez utiliser la clé d'authentification pour intégrer de nouveaux pare-feux, Collecteurs de journaux et appareils WildFire.
Type de périphérique	Spécifiez pour quels périphériques vous pouvez utiliser la clé d'authentification d'enregistrement des périphériques : **Firewalls (Pare-feux)**, **Log Collectors (Collecteurs de journaux)**, ou **Any (n'importe lequel)** (par défaut).
Périphériques	Entrez les numéros de série du pare-feu, du Collecteur de journaux et de l'appareil WildFire pour spécifier les pare-feux, les Collecteurs de journaux et les appareils WildFire pour lesquels la clé d'authentification d'enregistrement de périphérique est valide.

