Meilleures pratiques User-ID

10.0 (EoL)

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

- To ensure you are viewing the most current version of this document, or to access 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

November 16, 2020

Table of Contents

Meilleures pratiques User-ID

Commencer à utiliser les meilleures pratiques User-ID

User-ID™ met à profit le contexte utilisateur issu d'une large gamme de référentiels tels que les serveurs de répertoires, les contrôleurs LAN sans fil, les VPN, les NAC, les proxy, etc., pour vous permettre de :

- identifier les utilisateurs et appliquer le principe du moindre privilège envers les utilisateurs en fonction de leur niveau de confiance et de leur comportement, indépendamment des éléments suivants :
  - Emplacements des utilisateurs (par exemple, au bureau ou à la maison)
  - Les applications qu'ils utilisent (par exemple, IOS, appareils mobiles Android, macOS, Windows, bureaux Linux, ordinateurs portables, Citrix, Microsoft VDI ou serveurs de terminaux)
  - Les applications auxquelles les utilisateurs accèdent
- protéger vos identifiants d'entreprise d'une utilisation sur des sites web tiers et empêcher la réutilisation des identifiants volés en activant l'authentification à plusieurs facteurs (multi-factor authentification ; MFA) au niveau de la couche réseau pour n'importe quelle application sans modifier l'application.

La capacité d'identifier de manière constante les utilisateurs sur votre réseau indépendamment de leur emplacement offre une meilleure visibilité de l'activité des utilisateurs, permet une politique de sécurité basée sur les utilisateurs et sur les groupes et vous permet d'obtenir des données d'analyse plus instructives (journalisation, génération de rapports et investigation numérique). Utilisez les lignes directrices de meilleures pratiques suivantes pour apprendre comment planifier, déployer et maintenir User-ID sur votre réseau.

User-ID prend en charge plusieurs fonctionnalités ; ce guide couvre les fonctionnalités suivantes :

- GlobalProtect
- Surveillance Syslog
- Redistribution
- Mappage de groupe
- Groupe d'utilisateurs dynamiques

Les fonctionnalités supplémentaires qui ne sont pas encore couvertes par ce guide incluent :

- Accès à Prisma géré par Panorama
- Prévention contre le hameçonnage des informations d'identification
- Mappage nom d'utilisateur / adresse IP à partir de :
  - Périphériques de Network Access Control (contrôle d'accès au réseau – NAC)
  - Portail d'authentification
  - Active Directory

Meilleures pratiques User-ID pour GlobalProtect

Palo Alto Networks recommande GlobalProtect comme solution de meilleure pratique pour User-ID. Il offre une connectivité aux utilisateurs distants et utilise des passerelles internes pour rassembler des mappages pour les utilisateurs sur les réseaux internes. Étant donné que GlobalProtect demande aux utilisateurs de s'authentifier à l'aide de leurs informations d'identification lors d'un changement au niveau de la connectivité du réseau, de la position du périphérique ou de l'état d'authentification de l'utilisateur, il garantit des mappages d'utilisateur précis pour l'application des politiques basées sur les utilisateurs.

Planification des meilleures pratiques User-ID pour le déploiement de GlobalProtect

- Suivez le guide de configuration rapide GlobalProtect pour déterminer la manière optimale de déployer GlobalProtect. Pour User-ID, utilisez la configuration de VPN toujours active et la configuration mixte de passerelles externes et internes.
- Installez l'application GlobalProtect sur tous les terminaux lorsque vous souhaitez identifier des utilisateurs.
- Déterminez les attributs de répertoire pour les noms d'utilisateur (par exemple, UserPrincipalName, sAMAccountName ou common-name) que vous utilisez pour l'authentification GlobalProtect. Spécifiez ces attributs comme le nom d'utilisateur principal ou un nom d'utilisateur alternatif dans le profil de mappage de groupe.
- Si vous utilisez l'authentification de certificat client, le champ Subject Name (Nom de l'objet) du certificat doit identifier le nom d'utilisateur. User-ID ne prend pas en charge les certificats machine.
- Si vous n'avez qu'une seule passerelle interne mais que vous disposez d'autres pare-feu qui doivent apprendre les mappages de cette passerelle, planifiez la manière dont vous allez déployer la redistribution pour envoyer des mappages à d'autres pare-feu.
- Déterminez si vous recevez des mappages de plusieurs sources. Si tel est le cas, évaluez les sources à l'aide de l'interface web de la CLI pour déterminer si les mappages nom d'utilisateur / adresse IP collectés à partir de GlobalProtect peuvent être écrasés par des sources qui fournissent des mappages qui peuvent être moins précis ou moins rapides que GlobalProtect.

Déploiement de GlobalProtect en suivant les meilleures pratiques pour User-ID

- Déployez les portails et passerelles GlobalProtect. Déployez des passerelles internes et externes pour identifier de manière constante les utilisateurs indépendamment de leur emplacement.
- Utilisez la méthode de connexion Pre-logon (Always On) (Pré-ouverture de session [Toujours activée]) ou User-log on (Always On) (Connexion utilisateur [Toujours Activée]) pour activer l'accès au réseau en utilisant des passerelles internes et externes.
- Si vous utilisez des certificats pour l'authentification, déployez des certificats clients spécifiques à l'utilisateur pour l'authentification au moyen du Simple Certificate Enrollment Protocol (Protocole de recrutement de certificat simple ; SCEP).
- Si vous utilisez des passerelles internes, utilisez la détection d'hôte interne pour que l'application GlobalProtect sache quand envoyer un utilisateur sur une passerelle interne.

- Activez l'identification utilisateur dans les zones sources uniquement. Par exemple, si vous utilisez une passerelle externe GlobalProtect, activez User-ID dans la zone associée à l'interface de tunnel (**Network (Réseau)** > **Zones** > *tunnel-zone (zone-tunnel)*).
- Si vous recevez des mappages d'utilisateurs de plusieurs sources, excluez les sous-réseaux GlobalProtect pour les passerelles GlobalProtect sur les agents User-ID afin que les mappages d'utilisateurs que GlobalProtect fournit ne soient pas écrasées par des sources qui fournissent des mappages moins précis ou moins rapides que GlobalProtect.
- Configurez la redistribution de manière à partager les mappages que les passerelles GlobalProtect collectent avec d'autres pare-feu.
- Spécifiez tous les formats de nom d'utilisateur qui permettent aux utilisateurs de s'authentifier auprès de GlobalProtect comme attributs de nom d'utilisateur principal ou comme nom d'utilisateur alternatif dans le profil de mappage de groupe. Activez **Allow matching usernames without domains (Autoriser la mise en correspondance des noms d'utilisateurs sans domaines)** (**Device [Périphérique]** > **User Identification [Identification de l'utilisateur]** > **User Mapping [Mappage d'utilisateur]** > **Palo Alto Networks User-ID Agent Setup [Configuration de l'agent User-ID Palo Alto Networks]**) si les utilisateurs ne fournissent pas le nom de domaine lors de l'authentification GlobalProtect.
- Créez vos propres règles de politique de sécurité et testez qu'elles correspondent aux flux de trafic utilisateur attendu.

Utilisation des meilleures pratiques GlobalProtect après le déploiement pour User-ID

- Maintenez et mettez à jour les applications GlobalProtect sur les terminaux. Si vous avez de nombreux terminaux à mettre à jour, hébergez les mises à jour de l'appli sur un serveur web pour réduire la charge sur le pare-feu lorsque les utilisateurs se connectent à et téléchargent l'appli, ou utilisez un outil de distribution de logiciel pour appliquer les mises à jour dans les hôtes gérés.
- Sur l'application GlobalProtect, confirmez que les utilisateurs peuvent se connecter à une passerelle externe.
- Vérifiez que le pare-feu reçoit les mappages nom d'utilisateur / adresse IP de GlobalProtect.
  - Sur l'interface web, sélectionnez **Monitor (Surveiller)** > **User-ID** et confirmez l'affichage des noms d'utilisateur dans la colonne **User (Colonne)**.
  - Utilisez des commandes CLI pour confirmer que le pare-feu reçoit correctement les mappages.

Meilleures pratiques User-ID pour la surveillance Syslog

Les pare-feu Palo Alto Networks peuvent analyser les messages Syslog pour obtenir des mappage nom d'utilisateur / adresse IP. Vous pouvez utiliser des événements d'authentification provenant de services réseau et de périphériques existants comme des solutions VPN, des solutions Network Access Control (contrôle d'accès au réseau – NAC) ou des systèmes de gestion des informations et des événements de sécurité (SIEM) tiers à l'aide de messages Syslog. Pour vous assurer que les mappages d'utilisateur sont à jour, vous pouvez également configurer le pare-feu pour qu'il analyse les messages syslog des événements de déconnexion pour supprimer automatiquement les mappages obsolètes.

Planification des meilleures pratiques User-ID pour le déploiement de la surveillance Syslog

- Examinez les formats que les expéditeurs syslog utilisent pour déterminer la syntaxe qu'ils utilisent, s'ils incluent les noms de domaine, et s'ils répondent aux critères.
- Déterminez si vous souhaitez surveiller les événements de connexion, les événements de déconnexion, ou les deux. Si vous souhaitez surveiller les événements de déconnexion, vérifiez que l'expéditeur syslog inclut l'adresse IP et le nom d'utilisateur dans le message.
- En fonction des messages syslog, déterminez si vous devez utiliser regex ou des identifiants de champ. Si le message syslog est constant et prévisible, utilisez des identifiants de champ. Si le message est plus complexe et moins prévisible, utilisez regex.
- Planifiez le déploiement de la de la surveillance Syslog à l'aide de l'agent User-ID intégré à PAN-OS sur le pare-feu et non l'agent User-ID de Windows.

Déploiement de la surveillance Syslog en suivant les meilleures pratiques pour User-ID

- Si les expéditeurs syslog utilisent des formats différents, configurez un profil d'analyse Syslog pour chaque format.
- Si vous souhaitez surveiller à la fois les événements de connexion et de déconnexion, configurez un profil d'analyse Syslog pour chaque type d'événement.
- Activez l'option **Allow matching usernames without domains (Autoriser la mise en correspondance des noms d'utilisateurs sans domaines)** si les messages syslog n'incluent pas le nom de domaine et si les noms d'utilisateur sont uniques pour tous les domaines.
- Sur l'agent User-ID intégré à PAN-OS, utilisez toujours SSL pour écouter les messages syslog, car le trafic est chiffré. Étant donné qu'UDP envoie le trafic en texte en clair, si vous devez utiliser 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 de confiance d'envoyer du trafic UDP au pare-feu.
- Vérifiez que tous les expéditeurs syslog que vous souhaitez surveiller sont inclus comme entrées dans la liste de surveillance du serveur, car le pare-feu ignore les messages Syslog issus d'expéditeur qui ne sont pas présents dans cette liste.
- Triez les entrées dans la liste de filtres par ordre de correspondance la plus probable. Par exemple, si vous pensez que 80 % des messages syslog correspondront à filter1 et 20 % à filter2, assurez-vous de placer filter1 avant filter2 dans la liste.

Utilisation des meilleures pratiques de surveillance syslog après le déploiement pour User-ID

- Validez le fait que les messages syslog correspondent aux profils d'analyse syslog et que le pare-feu reçoit le mappage nom d'utilisateur / adresse IP provenant des messages syslog.
- Utilisez la commande CLI `show user server-monitor statistics` pour valider le fait que le pare-feu reçoit les messages provenant des expéditeurs syslog et qu'il établit correctement les correspondances avec les utilisateurs.

Meilleures pratiques User-ID pour la redistribution

Sur des réseaux de grande envergure, vous pouvez optimiser l'utilisation des ressources en configurant des pare-feux pour qu'ils recueillent des données qui existent déjà sur d'autres pare-feu grâce à la redistribution, au lieu de configurer tous vos pare-feux pour qu'ils fassent des requêtes directes auprès des sources de données de mappage.

Planification des meilleures pratiques User-ID pour le déploiement de la redistribution

- Planifiez l'architecture de redistribution. Voici certains facteurs à prendre en compte :
  - Quels pare-feu appliqueront les politiques pour tous les types de données (comme les mappages nom d'utilisateur / adresse IP ou les informations de mise en quarantaine des périphériques) et quels pare-feu doivent recevoir un sous-ensemble de données ?
  - Quelles plages d'IP nécessitent des mappages nom d'utilisateur / adresse IP ?
  - Si vous disposez d'une passerelle interne qui fournit un mappage d'utilisateur, quels autres périphériques ont besoin de ces données ? Quels seront leur fonction et leur rôle ?
  - Comment pouvez-vous limiter le nombre de sauts requis pour agréger toutes ces données ? Le nombre maximum de sauts autorisés pour les mappages nom d'utilisateur / adresse IP est de dix et le nombre maximum de sauts autorisés pour les mappages étiquette / nom d'utilisateur et les mappages étiquette / adresse IP est de un.
  - De quelle façon pouvez-vous minimiser le nombre de pare-feu qui interrogent les sources d'informations de mappage d'utilisateur ? Plus le nombre de pare-feu qui interrogent les sources d'informations est faible, plus la charge de traitement exercée sur les pare-feu et les sources est réduite.
- Déterminez la meilleure option pour votre concentrateur de redistribution :
  - Un pare-feu VM-Series dédié est idéal pour les déploiements User-ID à grande échelle. Si vous redistribuez uniquement des mappages d'utilisateurs, un VM-50 suffit. Si vous comptez également redistribuer des mappages étiquette / adresse IP, nous recommandons l'utilisation d'un VM-300 ou d'une série ultérieure.
  - Panorama est idéal pour les environnements de petite à moyenne échelle et si vous n'utilisez pas syslog ou la surveillance de serveur pour collecter des mappages d'utilisateurs.
- En fonction de vos exigences de serveur, déterminez le type de topologie que vous souhaitez utiliser :
  - Étoile pour une seule région
  - Étoile pour plusieurs régions
  - Hiérarchique

Déploiement de la redistribution en suivant les meilleures pratiques pour User-ID

- Configurez les sources des informations que vous souhaitez redistribuer :
  - Mappages nom d'utilisateur / adresse IP User-ID (y compris les agents User-ID Windows)
  - Mappages étiquette / adresse IP pour les groupes d'adresses dynamiques

- Mappages étiquette / nom d'utilisateur pour les groupes d'utilisateurs dynamiques
- Données pour la mise en œuvre des politiques basées sur HIP
- Informations de mise en quarantaine des périphériques

- Configurez les réseaux que vous souhaitez que le ou les agent(s) inclue(nt) dans la redistribution des données et les réseaux que vous souhaitez exclure de la redistribution des mappages étiquette / adresse IP ou des mappages nom d'utilisateur / adresse IP.
- 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.
- Configurez les réseaux ou les ressources qui reçoivent des types de données spécifiques par le biais de la redistribution.
- Activez l'authentification avec des certificats personnalisés pour la redistribution pour utiliser un certificat personnalisé pour l'authentification réciproque entre les agents de redistribution et les clients.
- Utilisez un pare-feu VM-Series ou Panorama pour redistribuer les données. Étant donné que Panorama peut être un agent ou un client, utilisez **Panorama** > **Data Redistribution (Redistribution des données)** pour configurer la redistribution des données sur Panorama.
- Si un pare-feu qui applique la politique a besoin de mappages des utilisateurs distants et locaux parce qu'il est également une passerelle GlobalProtect et un centre de données, activez la redistribution bidirectionnelle.
- Pour garantir une résilience optimale, il est recommandé d'activer la redistribution bidirectionnelle uniquement dans une région, et pas entre les régions.

Utilisation des meilleures pratiques de redistribution après le déploiement pour User-ID

- Suivez les deux dernières étapes dans Configurer la redistribution des données pour vérifier que les agents redistribuent correctement les données aux clients.

Meilleures pratiques User-ID pour le mappage de groupe

La définition de règles de politique basées sur l'appartenance à un groupe d'utilisateurs plutôt que sur des utilisateurs individuels simplifie l'administration car vous ne devez pas mettre à jour les règles lorsque l'appartenance à un groupe change. Les meilleures pratiques suivantes sont recommandées pour configurer le mappage de groupe pour les déploiements de Lightweight Directory Access Protocol (protocole d'accès léger aux annuaires – LDAP).

Les sections suivantes décrivent les meilleures pratiques pour déployer le mappage de groupe pour les services de répertoire sur site.

Planification des meilleures pratiques User-ID pour le déploiement du mappage de groupe

- Identifiez vos services de répertoire (comme Active Directory ou un service basé sur LDAP comme OpenLDAP) et identifiez la topologie pour vos serveurs d'annuaire Voici quelques questions que vous devriez vous poser :
  - Combien y a-t-il de serveurs de répertoire, de centres de données et de contrôleurs de domaine ?
  - Quelles sont vos principales sources d'informations sur les groupes ?
  - Où se trouvent les contrôleurs de domaine par rapport à vos serveurs d'annuaire ?
  - Les serveurs de répertoire et les contrôleurs de domaine se trouvent-ils dans des régions différentes ?
  - Quelles ressources sont locales et quelles ressources sont régionalisées ?
- Pour les déploiements pour lesquels votre source principale pour les mappages de groupe est un serveur Active Directory :
  - Si vous avez un seul domaine, vous n'avez besoin que d'une configuration de mappage de groupe avec un profil de serveur LDAP qui connecte le pare-feu au contrôleur de domaine avec la meilleure connectivité. Ajoutez jusqu'à quatre contrôleurs de domaine au profil de serveur LDAP pour la redondance.
  - Si vous disposez de groupes universels, créez un profil de serveur LDAP pour vous connecter au domaine racine du serveur du Catalogue global sur le port 3268 ou 3269 pour SSL, puis créez un autre profil de serveur LDAP pour vous connecter aux contrôleurs du domaine racine à l'aide de LDAPS sur le port 636. Si vous n'utilisez pas TLS, utilisez le port 389. Vous vous assurez ainsi que les informations sur les groupes et les utilisateurs sont disponibles pour tous les domaines et sous-domaines.
  - Si vous ne disposez pas de groupes universels et si vous disposez de plusieurs domaines ou forêts, vous devez créer une configuration de mappage de groupe avec un profil de serveur LDAP qui connecte le pare-feu à un serveur de domaine dans chaque domaine / forêt. Assurez-vous que les noms d'utilisateurs sont uniques dans chaque forêt.
  - Avant d'utiliser le mappage de groupe, configurez un nom d'utilisateur principal pour les règles de politiques de sécurité basées sur l'utilisateur, car cet attribut identifie les utilisateurs dans la configuration de la politique, les journaux et les rapports.
- Pour créer un groupe personnalisé qui n'est pas déjà disponible dans votre répertoire LDAP, utilisez des attributs d'utilisateur pour créer des groupes personnalisés.

- Assurez-vous que les configurations de mappage de groupe ne contiennent pas de groupes superposés si vous créez plusieurs configurations de mappage de groupe qui utilisent le même Distinguished Name (nom unique – DN) de base ou le même serveur LDAP. Par exemple, la liste d'inclusion pour une configuration de mappage de groupe ne peut pas contenir un groupe qui est également compris dans une configuration de mappage de groupe différente.
- Assurez-vous que les noms d'utilisateur et les attributs de groupe sont uniques pour tous les utilisateurs et groupes dans chaque domaine.
- Récupérez uniquement les groupes que vous utiliserez dans votre politique de sécurité basée sur les groupes et dans votre configuration en utilisant la liste d'inclusion des groupes ou en appliquant un filtre de recherche personnalisé.
- Évaluez la fréquence à laquelle les groupes changent dans vos répertoires pour déterminer la valeur d'**intervalle de mise à jour** optimale pour votre profil de mappage de groupe. Par exemple, si vous groupes changent fréquemment, configurez une valeur plus faible, mais s'ils sont généralement statiques, saisissez une valeur plus importante.
- Déterminez l'attribut de nom d'utilisateur qui doit représenter les utilisateurs dans les journaux, rapports et dans la configuration de la politique. Si vos sources User-ID envoient des noms d'utilisateur dans différents formats, spécifiez ces noms d'utilisateur comme attributs alternatifs.

Assurez-vous que le nom d'utilisateur principal, le nom d'utilisateur alternatif et l'attribut d'e-mail sont uniques pour chaque utilisateur.

Déploiement du mappage de groupe en suivant les meilleures pratiques pour User-ID

- Si vous utilisez uniquement des groupes personnalisés d'un répertoire, ajoutez un groupe inutilisé à la liste d'inclusion pour éviter que User-ID ne récupère tous les groupes à partir du répertoire.
- Utilisez la **liste d'inclusion de groupes** pour limiter des règles de politique à des groupes spécifiques. Vous pouvez également filtrer les groupes que le pare-feu suit pour le mappage de groupe en saisissant un **Search Filter (Filtre de recherche)** (requête LDAP) et une **Object Class (Classe d'objet)** (définition du groupe). Si vous ne disposez pas d'un groupe disponible dans votre répertoire LDAP, vous pouvez utiliser des attributs utilisateur pour créer des groupes personnalisés sur le pare-feu. Assurez-vous que les attributs utilisés pour former des groupes personnalisés sont des attributs indexés sur le répertoire.
- Spécifiez le nom d'utilisateur principal qui identifie les utilisateurs dans les rapports et dans les journaux.

Utilisation des meilleures pratiques de mappage de groupe après le déploiement pour User-ID

- Pour confirmer la connectivité au serveur LDAP, utilisez la commande CLI `show user group-mapping state all`.
- Pour afficher les membres des groupes, exécutez la commande `show user group name <group name>`.
- Confirmez que l'utilisateur existe dans un groupe avant d'utiliser ce groupe dans votre politique de sécurité. Pour vérifier les groupes que vous pouvez actuellement utiliser dans les règles de politiques, utilisez la commande CLI `show user group`.
- Si vous apportez des modifications au mappage de groupe, actualisez le cache manuellement. Pour actualiser manuellement le cache, exécutez la commande `debug user-id refresh group-mapping all`.

Meilleures pratiques User-ID pour les groupes d'utilisateurs dynamiques

Les groupes d'utilisateurs dynamiques vous permettent de réagir aux modifications du comportement des utilisateurs, des besoins commerciaux ou des menaces potentielles sans modifier manuellement les politiques ou créer et mettre à jour les groupes. Les groupes d'utilisateurs dynamiques vous permettent de créer une politique de sécurité qui offre :

- un accès aux ressources défini dans le temps pour les utilisateurs ;
- la capacité de remédier automatiquement aux comportements anormaux des utilisateurs et aux activités malveillantes tout en maintenant la visibilité de l'utilisateur.

Après avoir défini les critères du groupe à l'aide d'étiquettes et validé les modifications, l'adhésion au groupe d'utilisateurs dynamiques est automatiquement mise à jour en fonction des étiquettes de l'utilisateur.

Planification des meilleures pratiques User-ID pour le déploiement des groupes d'utilisateurs dynamiques

- ❑ En fonction de facteurs tels que les changements au niveau des besoins commerciaux ou des comportements utilisateur, identifiez la manière dont vous souhaitez que le pare-feu contrôle l'accès utilisateur :
  - ❑ Souhaitez-vous autoriser ou limiter l'accès par le biais d'une politique de sécurité ?
  - ❑ Souhaitez-vous exiger une MFA pour les utilisateurs ?
  - ❑ Souhaitez-vous déchiffrer le trafic de l'utilisateur pour bénéficier d'une meilleure visibilité concernant l'activité de l'utilisateur ?
- ❑ Déterminez la durée de l'adhésion de l'utilisateur à un groupe d'utilisateurs dynamiques spécifique.
  - ❑ Le pare-feu doit-il automatiquement supprimer l'utilisateur du groupe en fonction du temps (par exemple, le nombre d'heures dont un sous-traitant a besoin pour un accès temporaire aux ressources) ?
  - ❑ Le pare-feu doit-il exiger un événement spécifique pour associer ou dissocier des utilisateurs du groupe (par exemple, une activité malveillante) ?
- ❑ Évaluez quels événements générés par le pare-feu peuvent identifier une modification du comportement de l'utilisateur ou des besoins commerciaux. Vous pouvez attribuer des étiquettes par le biais de l'API, de l'auto-étiquetage ou manuellement à l'aide de l'interface web.
  - ❑ En fonction de vos cas pratiques, déterminez les étiquettes que vous utiliserez pour grouper les utilisateurs et la manière dont vous générerez l'étiquette.
  - ❑ Par exemple, évaluez le niveau de risque de l'utilisateur en fonction de leur comportement comme « risque élevé », « risque moyen » et « risque faible » selon les informations issues des périphériques et applications de sécurité et attribuez automatiquement des étiquettes aux utilisateurs en fonction de ces événements.
- ❑ Identifiez les sources des informations utilisateur pour les étiquettes :
  - ❑ Journaux du pare-feu
    - Pour les journaux d'authentification, de données, de trafic, d'inspection Tunnel, d'URL et de Wildfire, créez un profil de transfert des journaux et utilisez les actions intégrées.

- Pour les journaux User-ID, correspondance HIP, GlobalProtect et IP-étiquette, configurez les paramètres de journaux.

- Cortex XSOAR
- Informations de sécurité et systèmes de gestion des événements (SIEMS), comme Splunk
- Scripts d'API personnalisés

- Combinez des étiquettes issues de plusieurs sources pour définir les critères pour les groupes d'utilisateurs dynamiques. Par exemple, vous souhaitez peut-être interdire l'accès utilisateur uniquement si vous recevez des alertes de plusieurs applications de sécurité indiquant que les informations d'identification de l'utilisateur ont été compromises, au lieu d'une seule application, en fonction du niveau de confiance.

Déploiement de groupes d'utilisateurs dynamiques sur la base des meilleures pratiques User-ID

- Si vous souhaitez ajouter un grand nombre d'utilisateurs à un groupe d'utilisateurs dynamiques ou ajouter des utilisateurs en fonction d'événements issus d'autres applications de sécurité, utilisez des API pour ajouter les utilisateurs plutôt que l'interface web.
- Utilisez l'API ou définissez manuellement le **délai d'expiration** qui représente le moment où supprimer les utilisateurs de ce groupe (par exemple à l'expiration du contrat).
- Créez des règles de politique de sécurité qui utilisent le groupe d'utilisateurs dynamiques comme utilisateur source pour contrôler l'accès utilisateur, activer la MFA ou déchiffrer le trafic pour les utilisateurs membres de groupes d'utilisateurs dynamiques.
- Configurez les sources de manière à fournir des informations pour les étiquettes utilisateurs :
  - Si vous utilisez des journaux de pare-feu, configurez l'auto-étiquetage pour étiqueter l'utilisateur.
  - Si vous utilisez Splunk, vous pouvez attribuer des étiquettes aux utilisateurs à l'aide de l'application Palo Alto Networks pour Splunk.
  - Utilisez des programmes dans Cortex XSOAR ou d'autres plateformes d'orchestration de la sécurité, d'automatisation et de réponse (SOAR) pour appliquer des étiquettes aux utilisateur en fonction d'événements spécifiques.
  - Si vous utilisez des scripts personnalisés, modifiez le script pour remplir les étiquettes à l'aide de l'API.
  - Ajoutez des utilisateurs aux groupes manuellement à l'aide de l'interface web du pare-feu.

Utilisez les meilleures pratiques de groupes d'utilisateurs dynamiques après le déploiement pour User-ID

- Examinez les membres de votre groupe pour vous assurer que seuls les utilisateurs que vous souhaitez inclure sont membres du groupe. Si le groupe inclut des utilisateurs qui ne doivent pas en faire partie (par exemple des employés permanents dans le groupe « accès sous-traitant »), **désinscrivez les utilisateurs** pour supprimer leurs mappages étiquette / nom d'utilisateur et **supprimez**-les du groupe.
- Examinez les journaux User-ID pour vérifier que le pare-feu génère correctement des étiquettes pour les utilisateurs.
- Utilisez des commandes CLI pour en apprendre plus sur vos groupes d'utilisateurs dynamiques (par exemple, pour voir quels utilisateurs sont associés à ces groupes).
- Utilisez la colonne des groupes d'utilisateurs dynamiques dans les journaux de trafic et des menaces pour vous assurer que le pare-feu correspond aux groupes avec les politiques de sécurité attendues.

- Redistribuez les étiquettes d'utilisateur aux autres pare-feu pour vous assurer que tous les pare-feu appliquent la politique de sécurité de manière constante. Gardez à l'esprit que vous pouvez redistribuer les étiquettes d'utilisateur pour un seul saut.