Démarrage avec le BPA 9.1



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

- 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

Palo Alto Networks, Inc. www.paloaltonetworks.com

© 2019-2019 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised December 18, 2019

Table of Contents

Évaluation de l'adoption des fonctionnalités de la politique de	
sécurité	5
Examen du résumé de l'adoption	7
Identification des failles en matière d'adoption	10
Identification des règles à améliorer	15
Évaluation de la configuration des bonnes pratiques	17
Examen du résumé des bonnes pratiques	19
Examen de la configuration de la politique en matière de bonnes pratiques	21
Examen de la configuration des objets de bonnes pratiques	23
Examen de la configuration réseau des bonnes pratiques	24

Hiérarchisation des modifications des bonnes pratiques	
Renforcement de la posture de gestion des appareils	
Amélioration de la visibilité sur le trafic	
Mise en œuvre des contrôles initiaux des bonnes pratiques	
Ajustement et amélioration des contrôles des bonnes pratiques	

Évaluation de l'adoption des fonctionnalités de la politique de sécurité

L'outil Best Practice Assessment (BPA) vous aide à comprendre votre niveau actuel d'adoption des fonctionnalités de la politique de sécurité et à évaluer la maturité et l'efficacité de votre posture de sécurité. L'adoption de fonctionnalités telles que WildFire, la protection contre les vulnérabilités, le déchiffrement SSL, etc., contribue à la détection et à la prévention des attaques. Il est essentiel de bien comprendre comment et où utiliser chaque fonctionnalité dans différents environnements afin de mieux protéger votre réseau et ses précieux atouts.

Le Getting Started with Best Practices montre comment procéder à l'Accès et exécution du BPA. La section Capability Adoption Heatmaps du rapport BPA vous permet de vérifier l'adoption de ces fonctionnalités dans la base de règles de la politique de sécurité. Regardez la vidéo Introduction to Heatmaps pour en savoir plus sur les cartes thermiques et profiter de la Vidéothèque BPA pour en savoir plus sur l'outil.

Examinez et analysez les informations contenues dans les onglets Heatmap pour identifier les failles dans l'adoption des fonctionnalités de sécurité et déterminer ce que vous souhaitez améliorer :

- > Examen du résumé de l'adoption
- > Identification des failles en matière d'adoption
- > Identification des règles à améliorer

6 DÉMARRAGE AVEC LE BPA | Évaluation de l'adoption des fonctionnalités de la politique de sécurité

Examen du résumé de l'adoption

Après que vous ou votre représentant de Palo Alto Networks avez procédé à l'Exécution du BPA, le rapport HTML qui en résulte s'ouvre sur la page Heatmap (Carte thermique), dans le Adoption Summary (Résumé de l'adoption). La vue Adoption Summary (Résumé de l'adoption) fournit une vue d'ensemble de l'adoption globale des fonctionnalités de sécurité par votre équipement. Le rapport indique le pourcentage d'adoption actuel pour chaque indicateur (à l'exception d'Industry Average (Moyenne de l'industrie) qui fournit les moyennes d'adoption de votre secteur à comparer avec votre adoption), et entre parenthèses, le pourcentage de changement dans l'adoption depuis la dernière exécution du BPA sur le fichier de configuration de l'équipement (ou **No change** (Aucun changement) si la valeur est la même qu'à la dernière exécution du BPA).



Overall Adoption (Adoption globale) : adoption des profils de sécurité dans les règles d'autorisation de la politique de sécurité. Les pourcentages sont basés sur le nombre de règles d'autorisation pour lesquelles un ou plusieurs profils sont activés dans le cadre de la règle. Le BPA ne compte pas les règles désactivées ni les règles de blocage.

Industry Average (Moyenne du secteur) : adoption moyenne des profils de sécurité dans les règles d'autorisation pour le secteur de votre entreprise.

Best Practice Mode (Mode respectant les bonnes pratiques) : adoption des profils de sécurité configurés de la manière respectant les bonnes pratiques recommandée dans les règles d'autorisation. Le BPA ne compte que les règles dont les profils passent avec succès toutes les vérifications de bonnes pratiques.



App-ID Adoption (Adoption d'App-ID) : adoption d'App-ID dans les règles de politique de sécurité. La valeur en pourcentage est basée sur le nombre total de règles d'autorisation avec une ou plusieurs applications définies (l'application n'est pas **any** (tout)). Le BPA ne compte pas les règles désactivées.

User-ID Adoption (Adoption de User-ID) : adoption de User-ID dans les règles de politique de sécurité. La valeur en pourcentage est basée sur le nombre total de règles d'autorisation avec les utilisateurs (y compris les valeurs known-user (utilisateur connu) et **unknown** (inconnu)) ou des groupes d'utilisateurs. Le BPA ne compte pas les règles désactivées.

Service/Port Adoption (Adoption de service/port) : adoption du service/port dans les règles de politique de sécurité. La valeur en pourcentage est basée sur le nombre total de règles d'autorisation avec un service ou un port défini (le Service n'est pas **any** (tout)). Le BPA ne compte pas les règles désactivées.

Le BPA ne compte pas l'adoption d'App-ID, de User-ID ou de service/port pour les règles de blocage, car la logique de blocage varie d'une entreprise à l'autre. Le BPA ne peut donc pas faire de recommandations basées sur des règles de blocage.

Logging & Zone Protection Adoption Summary $_{\Theta}$		
Logging Adoption	Log Forwarding Adoption	Zone Protection Adoption
Logging Adoption	Log Forwarding Adoption	Zone Protection Adoption
100% (No change)	6.6% (No change)	96.5% (No change)

Logging Adoption (Adoption de la journalisation) : adoption de **Log at Session End** (Journaliser à la fin de la session) dans les règles de la politique de sécurité. La valeur en pourcentage est basée sur le nombre total de règles avec **Log at Session End** (Journaliser à la fin de la session) activée. Le BPA ne compte pas les règles désactivées.

Log Forwarding Adoption (Adoption du transfert de journaux) : adoption de profils de transfert de journaux dans les règles de la politique de sécurité. La valeur en pourcentage est basée sur le nombre total de règles avec un profil de transfert de journaux configuré. Le BPA ne compte pas les règles désactivées.

Zone Protection Adoption (Adoption de la protection de zone) : adoption de la protection de zone dans les règles d'autorisation de la politique de sécurité La valeur en pourcentage est basée sur le nombre total de règles d'autorisation dans lesquelles un profil de protection de zone est configuré dans la zone source. Le BPA ne compte pas les règles désactivées.

Pour chacun de ces indicateurs, la valeur entre parenthèses à côté de chaque pourcentage est le pourcentage de changement dans l'adoption depuis la dernière exécution du BPA sur le fichier de configuration de l'équipement (ou **No change** (Aucun changement) si la valeur est la même qu'à la dernière exécution du BPA).

Decryption Summary 🛛														
SSL Forward Proxy.	SSL Inbound Inspection	SSH Proxy	Decryption Profile Used											
URL Categories Exempted government, financial-services, any														

Decryption Summary (Résumé du déchiffrement) : indique si la configuration inclut des règles de politique de déchiffrement pour le proxy de transfert SSL, l'inspection SSL entrante et le proxy SSH. Le résumé indique également si la configuration inclut des profils de déchiffrement et identifie les catégories d'URL que l'équipement exclut du déchiffrement.



Si vous ne déchiffrez pas une catégorie d'URL, vous ne pouvez pas inspecter son trafic, car le pare-feu ne peut pas voir le contenu du trafic crypté. Le pare-feu peut uniquement inspecter le trafic que vous déchiffrez.

Étape suivante : Identification des failles en matière d'adoption pour comprendre les domaines dans lesquels vous pouvez améliorer la sécurité.

Identification des failles en matière d'adoption

La Heatmap (Carte thermique) vous montre les domaines dans lesquels votre politique de sécurité est forte et les domaines dans lesquels il existe des failles dans l'adoption des fonctionnalités de la politique de sécurité que vous pouvez chercher à améliorer. Pour obtenir une visibilité maximale sur le trafic et une protection maximale contre les attaques, définissez des objectifs pour l'adoption des fonctionnalités de sécurité et utilisez les recommandations suivantes comme base de référence respectant les bonnes pratiques. Évaluez votre posture actuelle par rapport à la situation de base afin d'identifier les failles dans l'adoption des fonctionnalités de la politique de sécurité.

Les Heatmaps (cartes thermiques) aident à identifier les équipements, les zones et les domaines dans lesquels vous pouvez améliorer l'adoption des fonctionnalités de la politique de sécurité. Vous pouvez examiner les informations sur l'adoption par Device Group (Groupe de périphériques), Serial Number (Numéro de série) & Vsys, Zones, Areas of Architecture (Zones d'architecture) et Tags (Étiquettes). Les **Column Filters** (Filtres de colonne) filtrent les groupes d'équipements, les équipements, les zones, les zones d'architecture et les balises afin de réduire la portée et d'identifier les failles.

🐠 paloalto		vice Group		lumber & Vs	iys Zones	Area of Arc	Area of Architecture Tags Rule Detail Zone Map			appings G	o to Best Practice	Assessment			Se	curity Poli	cy Capabi	ity Adoption	n Heatmaps
Help 😡																		.	iolumn Filters
					WildFire		Threat	Prevention (IPS)		URL	Filtering								
Source Area of Architecture	Destination Area of Architecture	Total Rule Count ↓₹	Allow Rule Count J↑	Deny Rule Count ↓↑	WildFire Adoption % 11	Anti- Spyware Adoption % 11	DNS Sinkhole Adoption % 1	Anti- Virus Adoption % ↓↑	Vulnerability Protection Adoption %	URL- Filtering Adoption % 1	Credential Theft Adoption % 11	File- Blocking Adoption % 11	Data- Filtering Adoption % 11	User ID Adoption % 11	App ID Adoption % 1	Service / Port Adoption % 11	Logging Adoption % 1	Log Forwarding Adoption %	Zone Protection Profile Adoption % 11
Internal Core	Datacenter	314	314	0	79.6	79.6	79.6	79.6	79.6	0.0	0.0	79.6	0.0	30.6	9.6	94.6	100.0	0.0	100.0
any	any	9	3	6	0.0	33.3	33.3	0.0	33.3	0.0	0.0	0.0	0.0	0.0	33.3	66.7	100.0	77.8	0.0
Remote Users/VPN, Internal Core	Internet	8	6	2	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	100.0	100.0	100.0	100.0	100.0	100.0
Internet	DMZ	3	3	0	66.7	0.0	0.0	66.7	100.0	0.0	0.0	33.3	0.0	0.0	100.0	100.0	100.0	66.7	100.0
Out-of-Band Management, Users, Remote Office/MPLS, Internal Core	IT Infrastructure	3	3	0	66.7	100.0	100.0	66.7	100.0	0.0	0.0	66.7	0.0	0.0	100.0	100.0	100.0	66.7	100.0
DMZ	Datacenter	2	2	0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	100.0	100.0	0.0	0.0
DMZ	Internet	2	2	0	50.0	50.0	50.0	100.0	50.0	0.0	0.0	0.0	0.0	0.0	100.0	100.0	100.0	100.0	0.0
Undefined	Undefined	2	2	0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	50.0	100.0	100.0	100.0	0.0	50.0
Web-tier	App-tier	1	1	0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	0.0	0.0	100.0	100.0	100.0	0.0	0.0
App-tier	DB-tier	1	1	0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	0.0	0.0	100.0	100.0	100.0	0.0	0.0
Remote Users/VPN, Internal Core	DMZ	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	100.0	100.0	100.0	100.0	100.0	100.0
Remote Office/MPLS	Internal Core	1	1	0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	0.0	0.0	0.0	0.0	100.0	0.0	0.0
Internal Core	Internet	1	0	1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	0.0	0.0	100.0	100.0	0.0
Remote Office/MPLS	PCI	1	1	0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	100.0	0.0	0.0
Internal Core	Remote Office/MPLS	1	1	0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	0.0	0.0	0.0	0.0	100.0	0.0	100.0
Grand Total:		350	341	9	78.0	78.0	78.0	78.3	78.9	2.1	2.1	77.4	0.0	30.6	16.0	94.1	100.0	6.6	96.5
Showing 1 to 15 of 15 entrie	es																		

Dans le Security Profile Adoption Summary (Résumé de l'adoption du profil de sécurité) de la Heatmap (Carte thermique), vérifiez les taux d'adoption des fonctionnalités suivantes et utilisez les recommandations comme critères d'identification des failles. Si le taux d'adoption réel ne correspond pas aux recommandations, prévoyez de remédier à la faille en procédant comme suit :

Previous 1 Next

verall Adoption		Industry Average		Best Practice Mode						
WildFire	78.0% (No change)	WildFire	36%	WildFire	77.4%					
Anti-Virus	78.3% (No change)	Anti-Virus	65.9%	Anti-Virus	77.1%					
Anti-Spyware	78.0% (No change)	Anti-Spyware	65.9%	Anti-Spyware	76.8%					
DNS Sinkhole	78.0% (No change)	DNS Sinkhole	33%	DNS Sinkhole	0.0%					
Vulnerability Protection	78.9% (No change)	Vulnerability Protection	66.4%	Vulnerability Protection	76.0%					
URL-Filtering	2.1% (No change)	URL-Filtering	23.1%	URL-Filtering	0.0%					
Credential Phishing Prevention	2.1% (No change)	Credential Phishing Prevention		Credential Phishing Prevention	2.1%					
File-Blocking	77.4% (No change)	File-Blocking	30.5%	File-Blocking	0.0%					
Data-Filtering	0.0% (No change)	Data-Filtering	8.9%							

Appliquez les profils de sécurité WildFire, Antivirus, Anti-Spyware, Vulnerability Protection (Protection contre les vulnérabilités) et File Blocking (Blocage des fichiers) à toutes les règles d'autorisation avec un objectif d'adoption de 100 % ou presque. Si vous n'appliquez aucun profil à une règle d'autorisation, vérifiez qu'il existe une bonne raison commerciale de ne pas appliquer le profil.

La configuration de profils de sécurité sur toutes les règles d'autorisation permet au pare-feu d'inspecter tout le trafic décrypté à la recherche de menaces, quels que soient l'application ou le service/port. Après la mise à jour de la configuration, exécutez le BPA pour mesurer les progrès et capter les nouvelles règles auxquelles aucun profil de sécurité n'est associé.



Vous pouvez appliquer des profils WildFire à des règles sans licence WildFire. La couverture est limitée aux fichiers PE, mais cela fournit néanmoins une visibilité utile sur les fichiers malveillants inconnus.

- Dans le profil Anti-Spyware, appliquez DNS Sinkhole à toutes les règles afin d'empêcher les hôtes internes compromis d'envoyer des requêtes DNS pour les domaines malveillants et personnalisés, d'identifier et de suivre les hôtes potentiellement compromis et d'éviter les interruptions de l'inspection DNS. L'activation de DNS Sinkhole protège votre réseau sans affecter la disponibilité. Vous pouvez et devez donc l'activer immédiatement.
- □ Appliquez la protection URL Filtering (Filtrage des URL) et Credential Phishing Prevention (Prévention de l'hameçonnage des informations d'identification) à tout le trafic Internet sortant.

Dans le Application & User Control Adoption Summary (Résumé de l'adoption des contrôles d'applications et d'utilisateurs) de la Heatmap (Carte thermique), vérifiez les taux d'adoption des fonctionnalités suivantes. Utilisez les recommandations comme critères d'identification des failles. Si le taux d'adoption réel ne correspond pas aux recommandations, envisagez de remédier à la faille en procédant comme suit :



- Appliquez App-ID à 100 % ou le plus près possible de 100 % des règles. Appliquez User-ID à toutes les règles avec des zones sources ou des plages d'adresses ayant une présence utilisateur (certaines zones peuvent ne pas avoir de sources utilisateur ; par exemple, les sources des zones de centre de données doivent être des serveurs et non des utilisateurs). Utilisez App-ID et User-ID pour créer des politiques de liste blanche (règle d'autorisation) autorisant les utilisateurs appropriés sur les applications autorisées (et tolérées). Bloquez explicitement les applications malveillantes et indésirables.
- □ Ciblez une adoption de service/port à 100 % ou près de 100 %. N'autorisez pas les applications sur des ports non standard à moins que cela ne soit justifié par des raisons commerciales.

Dans le Logging & Zone Protection Adoption Summary (Résumé de l'adoption de la protection de zone et de la journalisation) de la Heatmap (Carte thermique), vérifiez les taux d'adoption des fonctionnalités suivantes. Utilisez les recommandations comme critères d'identification des failles. Si le taux d'adoption réel ne correspond pas aux recommandations, envisagez de remédier à la faille en procédant comme suit :



- Ciblez une adoption à 100 % ou près de 100 % pour Logging Adoption (Adoption de la journalisation) et Log Forwarding Adoption (Adoption du transfert de journaux).
- Configurez les profils de protection de zone sur toutes les zones.

En résumé :

Fonctionnalité	Objectif d'adoption
WildFire	Le plus près possible de 100 % des règles de la politique de sécurité
Antivirus	Le plus près possible de 100 % des règles de la politique de sécurité
Antispyware	Le plus près possible de 100 % des règles de la politique de sécurité
Vulnérabilité	Le plus près possible de 100 % des règles de la politique de sécurité
Blocage des fichiers	Le plus près possible de 100 % des règles de la politique de sécurité
URL Filtering (Filtrage des URL) et Credential Phishing Prevention (Prévention de l'hameçonnage des informations d'identification)	Tout le trafic Internet sortant

12 DÉMARRAGE AVEC LE BPA | Évaluation de l'adoption des fonctionnalités de la politique de sécurité

Fonctionnalité	Objectif d'adoption
App-ID	Le plus près possible de 100 % des règles de la politique de sécurité
User-id	Toutes les règles avec des zones sources ou des plages d'adresses ayant une présence utilisateur
Service/port	Le plus près possible de 100 % des règles de la politique de sécurité
de journalisation	Le plus près possible de 100 % des règles de la politique de sécurité
Transfert des journaux	Le plus près possible de 100 % des règles de la politique de sécurité
Zone protection (Protection de zones)	Toutes les zones

Utilisez **Column Filters** (Filtres de colonne) pour réduire la portée. Utilisez les informations obtenues pour identifier les failles dans les fonctionnalités de la politique de sécurité, les comparer aux critères d'identification des failles et affiner ou établir de nouveaux critères d'identification des failles pour une enquête plus approfondie. Par exemple, pour créer un filtre affichant l'adoption des règles contrôlant le trafic sur la Area of Architecture (Zone d'architecture) Internet, procédez comme suit :

- STEP 1 | Dans la section Heatmaps (Cartes thermiques) du BPA, cliquez sur **Areas of Architecture** (Zones d'architecture).
- STEP 2 | Cliquez sur Column Filters (Filtres de colonne) pour développer les options de filtrage.
- STEP 3 | Définissez la **Destination Area of Architecture** (Zone d'architecture de destination) sur **Internet**.
- STEP 4 | Cliquez sur Apply Filter (Appliquer le filtre).

Le BPA filtre les résultats :

paloalto	Arreadof Architecture Tags Rule Detail Zone Mappings											tice Assessmen			:	Security Po	olicy Capal	oility Adopt	ion Heatmaps
Device Group Nothing select * Apply Filters	Source Area Architecture Destination/Area Architecture Target Source Zone Destination/Zone Taget Control Control <th< th=""><th>Column Filters</th></th<>														Column Filters				
Help 🕢																			
WildFi		WildFire		Threat P	revention (IPS)		URL	Filtering											
Source Area of Architecture	Destination Area of Architecture	Total Rule Count ↓₹	Allow Rule Count 1	Deny Rule Count 1	WildFire Adoption % 11	Anti- Spyware Adoption % 11	DNS Sinkhole Adoption % I†	Anti- Virus Adoption % 11	Vulnerability Protection Adoption %	URL- Filtering Adoption % J1	Credential Theft Adoption %	File- Blocking Adoption %	Data- Filtering Adoption %	User ID Adoption % 11	App ID Adoption % I†	Service / Port Adoption % J1	Logging Adoption % 11	Log Forwarding Adoption % 1	Zone Protection Profile Adoption %
any	any	9	3	6	0.0	33.3	33.3	0.0	33.3	0.0	0.0	0.0	0.0	0.0	33.3	66.7	100.0	77.8	0.0
Remote Users/VPN, Internal Core	Internet	8	6	2	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	100.0	100.0	100.0	100.0	100.0	100.0
DMZ	Internet	2	2	0	50.0	50.0	50.0	100.0	50.0	0.0	0.0	0.0	0.0	0.0	100.0	100.0	100.0	100.0	0.0
Internal Core	Internet	1	0	1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	0.0	0.0	100.0	100.0	0.0
Grand Total		20	11	9	63.6	72.7	72.7	72.7	72.7	54.5	54.5	54.5	0.0	45.0	65.0	90.9	100.0	90.0	54.5
Showing 1 to 4 of 4 entries Export Data	5																	Previo	ous 1 Next

Interprétez les résultats en fonction de vos objectifs et critères de sécurité. Par exemple, si votre objectif est d'appliquer WildFire à 100 % de vos règles d'autorisation, la Heatmap (Carte thermique) filtrée révèle que seulement 50 % de vos règles d'autorisation DMZ ont des profils WildFire. Vous avez donc identifié une faille à améliorer.

STEP 5 | Étape suivante : Identification des règles à améliorer.

14 DÉMARRAGE AVEC LE BPA | Évaluation de l'adoption des fonctionnalités de la politique de sécurité

Identification des règles à améliorer

Une fois que vous avez identifié une faille dans l'adoption des fonctionnalités de la politique de sécurité, utilisez la vue **Rule Detail** (Détail des règles) pour répertorier les règles qui nécessitent une enquête ou une correction supplémentaire. Configurez Column Filters (Filtres de colonne) pour correspondre aux critères d'identification des failles que vous avez élaborés lorsque vous avez procédé à l'Identification des failles en matière d'adoption. Des listes de règles que vous pouvez exporter et transférer à l'équipe opérationnelle chargée de la politique de sécurité du pare-feu s'affichent alors.

Par exemple, pour créer un filtre Rule Detail (Détail des règles) afin d'identifier les règles qui autorisent tout le trafic et pour lesquelles aucun profil de protection contre les vulnérabilités n'a été configuré, procédez comme suit :

- STEP 1 | Dans la section Heatmaps (Cartes thermiques) du BPA, cliquez sur **Rule Detail** (Détail des règles).
- STEP 2 | Cliquez sur **Column Filters** (Filtres de colonne) pour développer les options de filtre, puis sélectionnez les filtres suivants :
 - Source Zone (Zone source) = any (tout)
 - Destination Zone (Destination source) = any (tout)
 - Source Address Configured (Adresse source configurée) = No (non)
 - Destination Address Configured (Adresse de destination configurée) = No (non)
 - Action = allow (autoriser)
 - Rule Enabled (Règle activée) = Yes (oui)
 - Vulnerability On (Vulnérabilité activée) = No (non)

.,j//	paloalto				ture Tags Rule Det	Zone Mappings G	o to Best Practice Assessmer	e Assessment Security Policy Capability Adoption Heatmaps							
P	ule Attribute Filters											Column Filters			
De	vice Group	Target	Rulebase	Source Zone	Destination Zone	Source Addresses Configured	Destination Addresses	Application	Action	Source Area of Architecture	Destination Area of Architecture				
	Nothing selected *	Nothing selected *	Nothing selected *	any 💌	any •	No 💌	No •	Nothing selected *	allow •	Nothing selected *	Nothing selected 👻				
Lo	Nothing selected -	Nothing selected -	Nothing selected ~	Nothing selected +	Nothing selected +	Rule Enabled	Nothing selected ~								
Cap	ability Adoption Filters														
w	ldFire On	File Blocking On	Anti-Virus On	Anti-Spyware On	DNS Sinkhole On	Vulerability On	Data Filtering On	URL Filtering On	Credential Theft On	AppID On	UserID On				
	Nothing selected 👻	Nothing selected 👻	Nothing selected 👻	Nothing selected 👻	Nothing selected 👻	No •	Nothing selected 👻	Nothing selected 👻	Nothing selected 👻	Nothing selected 👻	Nothing selected 👻				
Dred	le Ellers														
PIO	lie Filters														
6	georwarding	Prome Group	wildfire	File stocking	Ante-virus	Anti-opyware	Data Hittering	OKLEHtering	vunerability						
	Nothing selected *	Nothing selected *	Nothing selected *	Nothing selected *	Nothing selected *	Nothing selected *	Nothing selected *	Nothing selected *	Nothing selected *						

STEP 3 | Cliquez sur Apply Filter (Appliquer le filtre).

Le BPA répertorie les règles correspondant aux filtres :

_										_										_
"/P pal	loalto						ecture Tags	Rule Detai	Zone Mappir	ngs Go	to Best Practice Assessmen	t				Security Po	olicy Capa	bility Ado	ption Heat	map
																			Column Fil	ters
Rule Attr	ibute Filters																			_
Device G	p	Target		Rulebase	Source Z	one	Destination Zo	9 4	Source Addresses Con	figured	Destination Addresses Configured	Application	Action		Source Area of Archite	ecture Destin	tion Area of Archi	tecture		
Nothin	g selected *	Nothin	g selected 👻	Nothing selected	* any	•	any	•	No	•	No *	Nothing selected	allow	•	Nothing selec	ted * No	thing selected	1 *		
Log Session S	Start	Log Session E	nd	Service Port Configured	Tags		Service		Rule Enabled		Source Zone Using ZPP									
Nothin	g selected 👻	Nothin	g selected 👻	Nothing selected	* Not	hing selected 👻	Nothing	selected +	Yes	•	Nothing selected +									
Capability A	Adoption Filters																			
WildFire On		File Blocking	On	Anti-Virus On	Anti-Spy	ware On	DNS Sinkhole C	'n	Vulerability On		Data Filtering On	URL Filtering On	Credential The	ft On	AppID On	UserID	On			
Nothin	g selected 👻	Nothin	g selected 👻	Nothing selected	- Not	hing selected 👻	Nothing	selected -	No	-	Nothing selected 👻	Nothing selected	- Nothing	selected -	Nothing selec	ted - No	thing selecter	1 × 1		
Profile Filte	rs																			
Log Forwardi	ing	Profile Group		Wildfire	File Block	king	Anti-Virus		Anti-Spyware		Data Filtering	URL Filtering	Vulnerability							
Nothin	g selected 👻	Nothin	g selected 👻	Nothing selected	* Not	hing selected *	Nothing	selected *	Nothing select	ted *	Nothing selected *	Nothing selected	Nothing	selected *						
Apply Fil	Iters	Clear Fil	ers																	
search:																				
Device Group ↓1	Target		Source Area Of Architecture	Dest Area Of Architecture	Rulename 1	Tags	Service 🕼	Rulebase ↓↑	Source Zone 11	Source U	lser		Dest Zone 1	Source Addresses 1	Dest Addresses ↓↑	Application 1	Action 1	Rule Enabled ↓↑	Wildfire Enabled 1	File Bloc Enal
Branch Offices	0153000022 0153000022 0153000224 0153000225 0153000226 0153000226	2:no-vsys, 3:no-vsys, :no-vsys, :no-vsys, :no-vsys, :no-vsys	any	any	Panorama Allow All	NO_TAG	application- default	post- rulebase	any	any	ny		any	no	no	any	allow	yes	no	no
shared	007200009 0072000015 0072000015 0072000015 0072000015 0072010003 0153000022 0153000022 0153000224	98:no-vsys, 91:no-vsys, 92:no-vsys, 93:no-vsys, 94:no-vsys, 97:no-vsys, 2:no-vsys, 3:no-vsys, :no-vsys,	any	any	intrazone- default	NO_TAG	any	post- rulebase	any	any			any	no	no	any	allow	yes	no	no

STEP 4 | Pour exporter la liste des règles filtrées dans un fichier .csv, cliquez sur **Export data** (Exporter les données).

🐙 palog	Tren	ding Devic	e Group Se	rial Number & Vsys	Zones Area of Architecture Tags	Rule Detai	Zone Mappin	Go to Best	Practice Assessr	nent					Securi	ty Policy Capa	ability Ado	otion Heatmag	os
Search:					•													Column Filters	
Rulename 1	Tags .↓↑	Service 1	Rulebase 1	Source Zone ↓†	Source User		Dest Zone	Source Addresses ↓↑	Dest Addresses ↓↑	Application 1	Action 1	Rule Enabled 1	Wildfire Enabled 1	File Blocking Enabled 1	Antivirus Enabled 1	Antispyware Enabled 1	Dns Sinkhole Enabled ↓↑	Vulnerability Enabled	L F E
Panorama Allow All	NO_TAG	application- default	post- rulebase	any	any		any	no	no	any	allow	yes	no	no	no	no	no	no	1
Intrazone- default	NO_TAG	any	post- rulebase	any	any		any	no	no	any	allow	yes	no	no	no	no	no	no	1
Showing 1 to 2 of Export Data	f 2 entries																Pre	vious 1 Next	L

STEP 5 | Étape suivante : Évaluation de la configuration des bonnes pratiques.

Évaluation de la configuration des bonnes pratiques

L'outil Best Practice Assessment (BPA) vous aide à comprendre le niveau actuel de configuration de votre politique de sécurité vis à vis des bonnes pratiques afin que vous puissiez évaluer la maturité de votre posture de sécurité. Regardez la vidéo Introduction au BPA pour en savoir plus sur le BPA et profiter de la Vidéothèque BPA pour en savoir encore plus sur l'outil.

Lorsque vous ouvrez le rapport BPA pour la première fois, il s'ouvre dans la section Heatmap (Carte thermique). Cliquez sur **Go to Best Practice Assessment** pour aller à la section BPA du rapport qui se concentre sur l'adoption des bonnes pratiques en matière de configuration pour les pare-feux nouvelle génération et Panorama.

we paloatto and an and a second and a second

Outre cette documentation, vous pouvez visionner la Démonstration BPA et une courte vidéo sur Comment exécuter un BPA pour en savoir plus sur l'utilisation du BPA.

Un rapport BPA évalue un fichier de configuration du pare-feu prochaine génération ou Panorama avec plus de 200 vérifications des bonnes pratiques. Le BPA regroupe les résultats de l'évaluation en fonction des informations sur les politiques, objets, réseau et équipement/ Panorama de la même manière que sur l'interface utilisateur PAN-OS. Examinez et analysez les informations pour trouver les domaines à améliorer sur lesquels vous concentrer :

- > Examen du résumé des bonnes pratiques
- > Examen de la configuration de la politique en matière de bonnes pratiques
- > Examen de la configuration des objets de bonnes pratiques
- > Examen de la configuration réseau des bonnes pratiques
- Examen de la configuration de la gestion des équipements et de Panorama relative aux bonnes pratiques

18 DÉMARRAGE AVEC LE BPA | Évaluation de la configuration des bonnes pratiques

Examen du résumé des bonnes pratiques

Lorsque vous passez de la vue Heatmaps (Cartes thermiques) à BPA report (Rapport BPA), cette dernière affiche le Best Practice Summary (Résumé des bonnes pratiques).

paloalto Policies 20 Objects	29 Network 22 Device 127 Panorama 20 Go to Heatmaps	Best Practice Assessment for F
Best Practice Summary		
Device Info	Capability Summary Ø	Control Category Summary O
Mapping Definitions	Corrective 64% (No change)	Configuration Management 49% (No change)
		Access Control 68% (+3 pts)
	Preventative 77% (+2 pts)	Audit and Accountability 55% (+1 pt)
		Contingency Planning 8% (No change)
	Performance Toose (No change)	System and information integrity 89% (+1 pt)
	Recovery 8% (No change)	Identification and Authentication 47% (No change)
		System and Communication Protection 39% (+1 pt)
	Detective 25% (+5 pts)	Risk Assessment 75% (No change)
	Class Summary	
	Technical	Operational Management
	61% (+2 pts)	51% (+1 pt) 75% (No change)
	-7-	-
	A technical control is one that uses technology to reduce vulnerabilities. An administrator installs and configures a technical control, and the technical control then provides the protection automatically.	Operational controls help ensure that day-to-day operations of an organization comply with their overall security plan. People (not technology) implement these controls.
	CIS Critical Security Controls 6.0 Summary O	

Le résumé présente les résultats de la vérification de la configuration des bonnes pratiques correspondant aux catégories de contrôles des normes du secteur, telles que les contrôles de sécurité critiques du Centre pour la sécurité Internet (CIS) et la publication du National Institute of Standards and Technology (NIST) sur les contrôles de sécurité et les procédures d'évaluation. L'objectif de ces informations est de fournir un bon moyen d'apprendre comment les vérifications BPA sont liées aux normes du secteur, et non de servir d'audit.

Comme le Résumé de l'adoption, le Best Practice Summary (Résumé des bonnes pratiques) inclut des mesures indiquant votre taux d'adoption actuel et la progression de l'adoption (entre parenthèses) depuis la dernière génération du BPA sur la configuration de l'équipement.

Cliquez sur **Mapping Definitions** (Définitions de mappage) (barre latérale gauche) pour voir une liste complète de toutes les vérifications mappées et de leurs scores individuels. Cliquez sur Show Filters (Afficher les filtres) pour définir des filtres, **Apply Filters** (Appliquer les filtres) pour appliquer des filtres au fichier généré et **Export mappings** (Exporter des mappages) pour exporter les mappages dans un fichier .csv.

ping Definitions	T	Nothing selected	Nothing selected	Cap	ability othing selected •	Class Nothing selected	*	Nothing selecte	/ d ~	CSC Con Nothing	trols	*
	Show	Apply Filters	Clear Filters					Select All Configuration	Deselect	: All	rch:	
	ļi ID	Best Practice Check Name		Top ↓† Nav	Left Nav	↓† Capability	Class	Audit and Acco	ountability		CSC 1 Controls	Passing %
	3	Description Populated		Policies	Security	Corrective	Operational	System and Inf	ormation Integrity		N/A	0
	4	Source/Destination = any/any		Policies	Security	Preventative, Corrective	Technical	Identification a	and Authentication		11.1, 12.1	99.7
	5	Service != any		Policies	Security	Preventative, Corrective	Technical	System and Co	mmunication Protecti	on	9.6, 13.3	94.6
	6	Log at Start of Session		Policies	Security	Performance	Technical	Risk Assessme	nt		N/A	99.7
	7	Log Forwarding		Policies	Security	Recovery, Detective	Operational, Technical	Contingency Pla	nning, Audit and Acco	untability	6.2, 6.6, 10.1	6.8
	8	Expired Non-Recurring Schedules		Policies	Security	Preventative	Operational	Configuration M	anagement		N/A	100
	9	Disable Server Response Inspection		Policies	Security	Preventative	Operational	System and Info	rmation Integrity		8.1, 8.5, 11.1	100
	11	Disabled Rules		Policies	Security	Preventative	Operational	Configuration M	anagement		N/A	55.6
	12	Interzone Deny Rule with Logging		Policies	Security	Preventative, Detective	Technical	Audit and Accou Information Inte	ntability, System and grity		6.2, 6.4, 6.6	100
	13	Intrazone Allow Rules with Logging		Policies	Security	Preventative, Detective	Technical	Audit and Accou Information Inte	ntability, System and grity		6.2, 6.6, 8.1	0
											Total	62.8
	Show	ving 1 to 10 of 202 entries port Mappings							Previous 1	2 3 4	4 5	21 Ne

Étape suivante : Examen de la configuration de la politique en matière de bonnes pratiques.

Examen de la configuration de la politique en matière de bonnes pratiques

L'onglet **Policies** (Politiques) affiche toutes les vérifications liées aux différents types de politiques de parefeu. Sélectionnez le type de politique que vous voulez examiner pour identifier les améliorations potentielles des règles. La vue de la politique Security (Sécurité) affiche les résultats de la vérification basés sur une règle (**Security Rule Checks** (Vérifications des règles de sécurité)). Cliquez sur **Show Filters** (Afficher les filtres) pour configurer des filtres qui limitent les résultats aux règles pour lesquelles une ou plusieurs vérifications particulières ont échoué. Vous pouvez cliquez sur **Export data** (Exporter les données) pour exporter la liste dans un fichier .csv pour une analyse de la correction.

Cliquez sur l'aide (?) pour afficher la description et la justification de chaque vérification, ainsi qu'un lien vers la documentation technique relative à la fonctionnalité que chaque vérification examine.

paloalto Policies (19) Objects (52)	Network 🛃 Device 🐻 Go	to Heatmaps								Best Pr	actice Assessment for N
Security 2	Security Rule Checks										
Policy Based Forwarding	Show Filters										
Decryption Rulebase 1	Rest Practice Check Results (
Decryntion (3)	Search										
Application Override 7	Rule Name	Li Rule ↓↑ Enabled	Description Populated	Source/Destination	Service 1 != any	Application 1 != any	APP-ID with 1 Service	of Session	Log 1 Forwarding	Expired Non-Recurring Schedules	Disable Server Response 1 Inspection
Captive Portal 🚯	all-default-profiles	true	×	×	~	×	-	~	×	~	× *
DoS Protection	Allow-Dev-Users	true	×	~	×	×	-	×	×	~	×
	Block-apps	true	×	×	×	-	~	×	×	×	×
	Block-Apps	false	×	×	×	-	×	~	×	×	×
	Block-Qk	true	×	×	×	-	×	×	×	×	×
	Block-Region	true	×	×	×	-	-	×	×	×	×
	Block-region	true	×	×	×	-	-	×	×	×	×
	Byod-users	true	×	×	×	×	-	×	×	×	×
	Commerce-E	true	×	×	×	×	×	×	×	×	×
	dummy-deny	true	×	×	×	-	-	×	×	×	×
	E-comm	true	×	×	×	×	×	×	×	×	×
	Guest-traffic	true	×	×	×	×	-	×	×	×	×
	High-risk IPS	true	×	×	×	-	×	×	×	×	×
	Hip-check	true	×	×	× .	×	-	×	×	×	×
	interzone-default	true	-	-	-	-	-	×	×	-	-
	N rule	true	×	×	×	×	-	×	×	×	×
	Network	true	×	×	×	×	×	×	×	×	×
	Networking	true	×	×	×	×	×	×	×	×	× *
	4										•
		Passing %	0%	73.3%	93.3%	33.3%	84.6%	87%	9.6%	96.6%	90%

Dans **Security Rule Checks** (Vérifications des règles de sécurité), les **Security Rulebase Checks** (Vérifications de la base de règles de sécurité) résument les résultats de la vérification des bonnes pratiques par groupe d'appareils, avec un statut Pass (Réussite)/Fail (Échec) et des recommandations sur les mesures à prendre pour les échecs de vérification. Cliquez sur l'aide pour afficher la description et la justification de chaque résultat, ainsi qu'un lien vers la documentation technique.

Security Rulebase vsys: vsys1
Best Practice Check Results

- Disabled Rules (Fail): 1 disabled rules exist
 Interzone Deny Rule with Logging (Pass)
- Intrazone Allow Rules with Logging (Fail): It is recommended to override the intrazone-default rule with Action set to 'allow', Log at Session End enabled, and IPS capability enabled.
- HIP Profiles used in Rules (Pass)
 User ID Rules without User ID enabled on Zone (Pass)

Lorsque vous examinez les informations sur la **Policy** (Politique), examinez au minimum les éléments suivants pour vous aider à comprendre la portée de la correction de la politique (alternez entre les vues) :

- Security (Sécurité) : identifiez les règles qui échouent à la vérification Source/Destination != any/any (Source/Destination != tout/tout).
- Security (Sécurité) : identifiez les règles qui échouent à la vérification App-ID with Service (App-ID avec service).

- Security (Sécurité) : identifiez les règles User-ID qui échouent à la vérification User-ID Rules without User ID enabled on Zone (Règles de User-ID sans User-ID activé sur zone).
- **Decryption Rulebase** (Base de règles de déchiffrement) : vérifications du déchiffrement du proxy SSH.
- Decryption (Déchiffrement) : chaque règle de politique de déchiffrement doit avoir un profil de déchiffrement associé.
- Application Override (Contrôle prioritaire sur l'application) : les règles de contrôle prioritaire sur l'application qui utilisent une application personnalisée simple contournent l'inspection de couche 7 du trafic correspondant. Réduisez ou éliminez les règles de contrôle prioritaire sur l'application qui utilisent une application personnalisée simple pour pouvoir procéder à l'Amélioration de la visibilité sur le trafic et inspecter les applications et le contenu que ces règles contrôlent.

Étape suivante : Examen de la configuration des objets de bonnes pratiques.

Examen de la configuration des objets de bonnes pratiques

L'onglet **Objects** (Objets) affiche toutes les vérifications liées aux différents types d'objets de pare-feu. Sélectionnez le type d'objet à examiner pour comprendre la configuration existante et identifier les failles potentielles dans la configuration des bonnes pratiques liée aux Tags (Balises), GlobalProtect, Security Profiles (Profils de sécurité), Log Forwarding (Transfert des journaux) et Decryption profiles (Profil de déchiffrement). L'exemple suivant montre le résultat pour un Security Profil (Profil de sécurité) Antivirus.

paloatto Policies 22	Objects (22) Network (22) Device (127)	Panorama 20 Go to Heatmaps		Best Practice Assessment for Panorama
Tags GlobalProtect HIP Profiles	Device Group	Only show records with warnings		
Security Profiles Anth/sus Anth: Spyware Vulnerability Protection URL Filtering File Blocking WildFire Analysi:	Packet Capture Enabled Faile Decoders Name Action Wildfire Actio smtp reset-both alert pop3 alert alert imap alert alert thtp reset-both alert	• 		
DoS Protection (5) Log Forwarding (6) Decryption Profile (5)	Threat Exceptions None Best Practice Check Results •	Application Excep None 1 (Pass)	xtions Rules Using Pn 4 be set to either drop, reset-both, reset-client, or reset-server: smtp, smb, http.f	ofile
	✓ Antivirus Profile Packet Capture	Pass)		

Pour chaque profil, le rapport indique la configuration actuelle et le nombre de règles utilisant le profil. Le rapport affiche les résultats de la vérification des bonnes pratiques en dessous de la configuration actuelle avec le statut Pass (Réussite)/Fail (Échec) et des recommandations pour les échecs de vérification des bonnes pratiques. Cliquez sur l'aide pour afficher la justification de chaque vérification et sur les liens vers la documentation sur les bonnes pratiques.

Lorsqu'une ou plusieurs vérifications échouent, l'intitulé du profil devient rouge. Le rapport répertorie les profils inutilisés en bas avec un intitulé jaune.

Lorsque vous examinez l'onglet **Objects** (Objets), examinez au minimum les éléments suivants pour vous aider à comprendre la portée potentielle de la correction :

- **Antivirus** : actions du décodeur pour Antivirus et WildFire.
- Anti-Spyware : profil Strict, DNS Sinkhole.
- **Vulnerability Protection** (Protection contre les vulnérabilités) : profil Strict.
- URL Filtering (Filtrage des URL) : pour savoir si les catégories connues comme malveillantes sont bloquées.
- WildFire Analysis (Analyse WildFire) : types de fichiers de profil (tous les types doivent être envoyés à WildFire pour analyse).
- Log Forwarding (Transfert des journaux) : pour savoir si tous les types de journaux sont transférés (transfère tous les types de journaux).

Étape suivante : Examen de la configuration réseau des bonnes pratiques.

Examen de la configuration réseau des bonnes pratiques

L'onglet **Network** (Réseau) affiche toutes les vérifications de la configuration liée au réseau. Dans le menu de gauche, sélectionnez la vérification de réseau que vous souhaitez examiner pour comprendre la configuration existante et identifier les failles potentielles dans la configuration des bonnes pratiques liée aux Zones, GlobalProtect ainsi qu'aux profils IPsec Crypto (Crypto IPSec) et Zone Protection (Protection de zone). L'exemple suivant montre le résultat pour les Zones.

paloalto	Policies 22 Objects	29 Network 22	Device 127	Panorama 🙆	Go to Heatmaps				Best Practice Assessment for Panorama
Zones 19		Device Group	¥	Template	¥	Only show records with warnings			
GlobalProtect Portals		Internet device gr							
Gateways Network Profiles IPSec Crypto		User Id Enabled True Packet Buffer Prote True	ction Enabled			Using Acl Include List False		Zone Protection Profile zpp-hq-internet	
Zone Protection (3)		Best Practice Check Results ① ✓ Enable Packet Buffer Protection (Pass) X ACL Indude List for User (DI Failt: When User ID is enabled, you should also be using an ACL Include List ✓ Zone Protection Profile Applied to Zone (Pass) Notes P User ID on Untrusted Zones: Only enable User ID on trusted zones							
		User Id Enabled True Packet Buffer Prote False	ction Enabled			Using Acl Include List False		Zone Protection Profile None	
		Kerker Practice Uneck R Enable Packet Bu ACL Include List Zone Protection i Notes User ID on Untru	ffer Protection (I ior User ID (Fail): Profile Applied to sted Zones: Only	Fail): It is recommend When User ID is ena Zone (Fail): Zone sh renable User ID on tr	ed to enable Packet I bled, you should also ould have a zone pro- usted zones	Buffer Protection. be using an ACL Include List tection profile applied			
		GlobalProtect d	evice group: vsy	s1 template : Perime	ter				
		User Id Enabled True				Using Acl Include List False		Zone Protection Profile None	

Le rapport affiche la configuration actuelle pour chaque élément. Les résultats de la vérification des bonnes pratiques pour chaque élément apparaissent sous sa configuration actuelle. Vous pouvez spécifier un **Device Group** (Groupe d'équipementd) et/ou un **Template** (Modèle) pour limiter la portée des informations affichées.

Chaque vérification a le statut Pass (Réussite)/Fail (Échec) et des recommandations pour les échecs de vérification des bonnes pratiques. Cliquez sur l'aide pour afficher la justification de chaque vérification et sur les liens vers la documentation sur les bonnes pratiques. Lorsqu'une ou plusieurs vérifications échouent, l'intitulé de l'élément devient rouge.

Lorsque vous examinez l'onglet **Network** (Réseau), examinez au minimum les éléments suivants pour vous aider à comprendre la portée potentielle de la correction :

- **Zones** : pour savoir si la Packet Buffer Protection (Protection de la mémoire tampon de paquets) est activée dans chaque zone et si son profil est Zone Protection (Protection de zone).
- Zone Protection (Protection de zone) : pour savoir si Flood Protection (Protection contre les inondations) et la Packet-Based Attack Protection (Protection contre les attaques basées sur des paquets) sont activées.

Étape suivante : Examen de la configuration de la gestion des équipements et de Panorama relative aux bonnes pratiques.

Examen de la configuration de la gestion des équipements et de Panorama relative aux bonnes pratiques

Les onglets **Device** (Équipement) et **Panorama** affichent toutes les vérifications liées à la configuration de la gestion des équipements. Sélectionnez la vérification de la gestion des équipements que vous souhaitez examiner pour comprendre la configuration existante et identifier les failles potentielles dans la configuration des bonnes pratiques liée à la gestion des équipements Panorama et du pare-feu. L'exemple suivant montre le résultat des General Settings (Paramètres généraux) du pare-feu (cliquez sur **Panorama** pour voir les résultats de la vérification de Panorama).

	Objects 20 Network 22 Device 127 Panorama 20 Go to	Heatmaps	Best Practice Assess	ment for Panorama
Setup - Management General Settings 1	Template All Only show records	with warnings		
Authentication Settings 12	Template General Settings template: Perimeter			
Logging and Reporting Settings 3				
Secure Communication Settings (8)	Login Banner Enabled False	Auto Acquire Commit Lock Enabled False	Ssl TIs Service Profile None	
Management Interface Settings	Hostname None	Cert Expiration Check Enabled False		
Minimum Password Complexity 🔇	Best Practice Check Results 🛛			
Setup - Services 6	Automatically Acquire Commit Lock (Fail): It is recommended t Certificate Expiration Check (Fail): The SSL/TLS Service Profile Login Banner (Fail): It is recommended to have a descriptive Lo	o enable "Automatically Acquire Commit Lock" is not configured gin Banner		
Setup - Content-ID (8)				
Setup - WildFire 20	Template General Settings template: Internal Core			
Setup - Session 🖪				
Setup - Telemetry 🕢	Login Banner Enabled False	Auto Acquire Commit Lock Enabled False	Ssl TIs Service Profile None	
High Availability	Hostname None	Cert Expiration Check Enabled False		
Administrators	Best Practice Check Results 😧			
Admin Roles	 Automatically Acquire Commit Lock (Fail): It is recommended t Certificate Expiration Check (Fail): The SSL/TLS Service Profile 	o enable "Automatically Acquire Commit Lock" is not configured		
Authentication Profile (2)	 Login Banner (Fail): It is recommended to have a descriptive Lo. 	<mark>sin Banner</mark>		
Authentication Profiles (3)				
Authentication Sequence	Template General Settings template: Datacenter			
Authentication Sequences	Login Banner Enabled	Auto Acquire Commit Lock Enabled	Ssl TIs Service Profile	
User Identification	False Hostname	False Cert Expiration Check Enabled	None	
Log Settings	HORE	raise		
System 19	Best Practice Check Results Automatically Acquire Commit Lock (Fail): It is recommended t	o enable "Automatically Acquire Commit Lock"		
	 Common Common Charle Lottle The SST/TES Comice Proble 	ic not confidured		

Le rapport affiche la configuration actuelle pour chaque élément. Les résultats de la vérification des bonnes pratiques pour chaque élément apparaissent sous sa configuration actuelle. Lors de la visualisation d'informations pour un **Device** (Équipement), vous pouvez spécifier un **Template** (Modèle) pour limiter la portée des informations affichées.

Chaque vérification a le statut Pass (Réussite)/Fail (Échec) et des recommandations pour les échecs de vérification des bonnes pratiques. Cliquez sur le point d'interrogation pour obtenir la justification de chaque vérification et sur les liens vers la documentation sur les bonnes pratiques. Lorsqu'une ou plusieurs vérifications échouent, l'intitulé de l'élément devient rouge.

Lorsque vous examinez l'onglet **Device** (Équipement), ou **Panorama**, examinez au minimum les éléments suivants pour vous aider à comprendre la portée potentielle de la correction :

- Dynamic Updates (Mises à jour dynamiques) : mises à jour Antivirus, Apps, Threats (Menaces) et WildFire.
- Management Interface Settings (Paramètres de l'interface de gestion) : Network Connectivity Services (Services de connectivité réseau), Permitted IP Addresses (Adresses IP autorisées).
- Administrators (Administrateurs) : Local Admins (Administrateurs locaux), Administrator Password profil (profil de mot de passe administrateur). Vérifiez Device (Périphérique) > Administrators

(Administrateurs) ou Panorama > Administrators (Administrateurs) pour vous assurer que les mots de passe des administrateurs sont configurés avec la complexité minimale requise.

Minimum Password Complexity (Complexité minimale du mot de passe) : vérification des exigences de complexité minimale du mot de passe.

Étape suivante : Hiérarchisation des modifications des bonnes pratiques.

Hiérarchisation des modifications des bonnes pratiques

La quantité d'informations dans un rapport BPA peut être considérable. Ce chapitre fournit des recommandations pour vous aider à hiérarchiser les améliorations à apporter à votre configuration afin que vous puissiez remédier aux failles de sécurité, commencer par mettre en œuvre les améliorations les plus importantes et progresser vers une bonne pratique en matière de posture de sécurité.

Les rubriques suivantes traitent de la manière d'améliorer votre posture de sécurité dans l'ordre dans lequel les nouveaux déploiements sont généralement mis en œuvre, en commençant par la gestion, puis la visibilité, le contrôle et l'application. Les déploiements existants ont peut-être déjà atteint une certaine maturité dans chaque domaine.

- > Renforcement de la posture de gestion des appareils
- > Amélioration de la visibilité sur le trafic
- > Mise en œuvre des contrôles initiaux des bonnes pratiques
- > Ajustement et amélioration des contrôles des bonnes pratiques

28 DÉMARRAGE AVEC LE BPA | Hiérarchisation des modifications des bonnes pratiques

Renforcement de la posture de gestion des appareils

Le renforcement de votre posture de gestion des équipements sécurise le pare-feu en empêchant tout accès non autorisé qui pourrait le compromettre, en réduisant l'impact opérationnel de événements imprévus et en offrant une meilleure visibilité sur le fonctionnement du pare-feu.

- Suivez les Bonnes pratiques pour sécuriser l'accès administratif pour empêcher tout accès non autorisé et non sécurisé à l'interface de gestion de l'équipement.
- Procédez au Transfert de tous les journaux du système et de la configuration vers Panorama et aux Solutions de surveillance tierces pour suivre les événements liés au système et les modifications de configuration.
- Procédez à la Création d'un planning de sauvegarde de configuration pour pouvoir ainsi résoudre plus rapidement les problèmes liés à la configuration et les pannes du système.

Après avoir configuré les modifications, procédez à l'<u>Exécution du BPA</u> pour valider les modifications, mesurer les progrès et hiérarchiser les modifications suivantes.

Étape suivante : Amélioration de la visibilité sur le trafic.

Amélioration de la visibilité sur le trafic

Vous ne pouvez pas vous protéger contre les menaces que vous ne voyez pas. Vous devez donc vous assurer de toujours avoir une visibilité complète sur le trafic, sur tous les utilisateurs et toutes les applications. La première étape vers un contrôle informé des politiques est atteinte par l'obtention d'une visibilité complète sur les applications, les contenus et les utilisateurs de votre réseau :

- Maximisez l'adoption du profil de sécurité. Après avoir procédé à l'Examen du résumé de l'adoption et à l'Identification des failles en matière d'adoption, corrigez les failles à l'aide des étapes de transition en toute sécurité pour passer à la mise en œuvre d'un profil de sécurité complet respectant les bonnes pratiques.
- Maximisez l'adoption de la journalisation (notamment le Transfert des journaux) à travers la base de règles de la politique de sécurité pour inspecter *tout* le trafic.
- Procédez à la Configuration des bonnes pratiques pour les mises à jour de contenu dynamiques pour vous assurer que le pare-feu dispose des dernières signatures d'applications et de menaces pour protéger votre réseau et que vous déployez des mises à jour en fonction des exigences de sécurité et de disponibilité de votre réseau.
- Procédez à la Planification du déploiement de votre déchiffrement SSL en fonction des bonnes pratiques.
- Procédez à l'Activation de User-ID dans les zones utilisateur (zones de confiance internes à partir desquelles les utilisateurs génèrent du trafic) pour mapper le trafic des applications et les menaces associées pour les utilisateurs et les périphériques.



N'activez pas User-ID dans les zones externes non approuvées. Si vous activez User-ID (ou un sondage du client tel que WMI) sur une zone externe non approuvée, des sondages pourraient être envoyés en dehors de votre réseau protégé, ce qui entraînerait une divulgation des informations sur User-ID telles que le 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 de compromettre votre réseau.

- Réduisez ou éliminez les règles de contrôle prioritaire sur l'application afin de pouvoir inspecter les applications et le contenu contrôlé par ces règles (une règle de contrôle prioritaire sur l'application est une règle de couche 4 qui ne permet pas au pare-feu d'inspecter le trafic). Pour éliminer le besoin ou réduire la portée des règles de contrôle prioritaire sur l'application de base, procédez comme suit :
 - Confirmez que le cas d'utilisation de la règle existe toujours. Une règle de contrôle prioritaire sur l'application a souvent été créée pour résoudre un problème spécifique lié aux performances, aux décodeurs de protocole ou aux applications inconnues. Au fil du temps, les mises à jour PAN-OS, les mises à jour du contenu ou les mises à niveau matérielles peuvent supprimer le besoin d'avoir certaines règles de contrôle prioritaire sur l'application. Si vous exécutez PAN-OS 9.0 ou version ultérieure sur des pare-feu ou PAN-OS 9.0 ou version ultérieure sur un Panorama gérant des parefeux exécutant PAN-OS 8.1 (ou version ultérieure), vous pouvez utiliser Policy Optimizer pour transformer la règle en règle de couche 7.
 - Réduisez la portée de la règle de contrôle prioritaire sur l'application afin qu'elle n'affecte que la quantité de trafic la plus faible possible. Les règles définies de manière trop large peuvent avoir un contrôle prioritaire sur plus de trafic que nécessaire ou prévu. Définissez les zones, adresses et/ou ports source et de destination dans chaque règle de contrôle prioritaire sur l'application afin de limiter le plus possible la portée de la règle.
 - Créez des applications personnalisées de couche 7 pour les applications internes.
 - Créez des objets de Service avec valeurs de délai d'expiration personnalisées.
- Procédez à la Planification du déploiement de la protection DoS et de zone et à la Prise de mesures de référence des CPS pour pouvoir définir des seuils raisonnables de protection contre la saturation.

Lorsque vous mettez en œuvre ces fonctionnalités natives App-ID, Content-ID, User-ID et déchiffrement SSL, le pare-feu obtient une visibilité et peut inspecter tout votre trafic (applications, menaces et contenu) et lie les événements à l'utilisateur, quels que soient l'emplacement, le type de périphérique, le port, le chiffrement ou les techniques d'évasion d'un pirate.

L'amélioration de l'adoption de fonctionnalités telles que le déchiffrement SSL, la journalisation, la protection contre la saturation, les profils de sécurité, etc., peut entraîner une consommation supplémentaire des ressources de pare-feu. Comprenez la fonctionnalité de vos pare-feux et assurez-vous qu'ils sont correctement dimensionnés pour supporter toute charge supplémentaire. Votre SE ou CE de Palo Alto Networks peut vous aider à dimensionner le déploiement. Vous aurez peut-être également besoin d'espace de stockage supplémentaire dans les journaux.

Après avoir configuré les modifications, procédez à l'<u>Exécution du BPA</u> pour valider les modifications, mesurer les progrès et hiérarchiser les modifications suivantes.

Étape suivante : Mise en œuvre des contrôles initiaux des bonnes pratiques.

Mise en œuvre des contrôles initiaux des bonnes pratiques

Après avoir obtenu une visibilité et une meilleure perspective du trafic sur votre réseau (applications, contenu, menaces et utilisateurs), mettez en œuvre des contrôles stricts pour réduire la surface d'attaque et empêcher les menaces connues et inconnues afin de mener à bien la transition vers une configuration relative aux bonnes pratiques.

- Après avoir procédé à l'Examen du résumé de l'adoption et à l'Identification des failles en matière d'adoption, suivez les étapes de transition en toute sécurité pour passer aux profils de sécurité respectant les bonnes pratiques pour bloquer les menaces et réduire la surface d'attaque, notamment par la mise en place de contrôles stricts dans le centre de données afin de protéger les actifs les plus précieux de votre entreprise.
- Créez des règles de politique de sécurité basées sur une application pour le centre de données et les pare-feux de périmètre ; utilisez les recommandations relatives aux bonnes pratiques en matière de pare-feux de périmètre pour les autres pare-feu ne figurant pas dans le centre de données. Si vous exécutez PAN-OS 9.0 ou version ultérieure sur des pare-feux ou PAN-OS 9.0 ou version ultérieure sur un Panorama gérant des pare-feu exécutant PAN-OS 8.1 (ou version ultérieure), vous pouvez utiliser Policy Optimizer pour convertir les règles basées sur un port en règles basées sur une application.
- Procédez à la Création de politiques d'accès basées sur un utilisateur.
- Procédez au Déploiement des profils de protection de zone respectant les bonnes pratiques à toutes les zones.
- Procédez au Déploiement du déchiffrement SSL pour que le pare-feu puisse obtenir une visibilité (déchiffrer) et inspecter le trafic chiffré.

Une fois que vous avez mis en œuvre les fonctionnalités de contrôle, le pare-feu peut analyser tout le trafic autorisé et détecter et bloquer les exploitations de vulnérabilité des couches d'application et réseau, les dépassements de capacité de la mémoire tampon, les attaques DoS, les analyses de ports et les variantes de logiciels malveillants connues et inconnues. Le pare-feu contrôle l'accès aux applications et aux utilisateurs, ainsi que le blocage des applications malveillantes et indésirables.

Après avoir configuré les modifications, procédez à l'Exécution du BPA pour valider les modifications, mesurer les progrès et hiérarchiser les modifications suivantes.

Étape suivante : Ajustement et amélioration des contrôles des bonnes pratiques.

Ajustement et amélioration des contrôles des bonnes pratiques

Après avoir procédé à l'Mise implement control sur le trafic de votre réseau (applications, contenu, menaces et utilisateurs), commencez à ajuster les contrôles et à mettre en œuvre des fonctionnalités supplémentaires pour améliorer votre posture de sécurité.

- Si vous n'avez pas converti les applications internes en applications personnalisées pour obtenir une visibilité et un contrôle du trafic, convertissez les applications internes en Applications personnalisées.
- Adaptez les profils de sécurité aux bonnes pratiques après avoir utilisé les safe transition steps pour commencer la transition vers les best practice profiles.
- Procédez au blocage d'adresses IP malveillantes Block known malicious IP addresses en fonction des informations sur les menaces de Palo Alto Networks et des flux tiers réputés.
- Procédez au Deploy GlobalProtect ou au GlobalProtect Cloud Service pour étendre la plateforme de sécurité nouvelle génération aux utilisateurs et aux périphériques, quel que soit l'endroit où ils se trouvent.
- Activez la prévention contre le vol d'identifiants credential theft prevention.
- Configurez l'authentification multi-facteurs Multi-Factor Authentication basée sur le réseau.

Ensuite : procédez à l'Exécution du BPA pour valider les modifications, mesurer les progrès et hiérarchiser les modifications suivantes, en savoir plus sur les Bonnes pratiques et sur les nombreuses fonctionnalités de sécurité de Panorama et des pare-feux nouvelle génération de PAN-OS.

34 DÉMARRAGE AVEC LE BPA | Hiérarchisation des modifications des bonnes pratiques