

Strata Cloud Manager AlOps

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

Palo Alto Networks, Inc. www.paloaltonetworks.com

© 2023-2025 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

February 3, 2025

Table of Contents

	5
- Régions pour AIOps pour NGFW	7
Fonctionnalités des options Gratuit et Premium	9
Comment activer AIOps pour NGFW	13
Où sont mes fonctionnalités AIOps pour NGFW ?	19
Plug-in Panorama CloudConnector	25
Recevoir des notifications d'alerte	29
Résoudre les anomalies de connectivité et d'application des politiques des NGFW	31
Télémétrie du périphérique pour AlOps for NGFW	37
Domaines requis pour AIOps for NGFW	
Optimiser la posture de sécurité	41
Surveiller les informations sur la posture de sécurité	
Surveiller l'adoption des fonctionnalités	44
Surveiller les abonnements de sécurité	
Évaluer les vulnérabilités	
Surveiller le Résumé de la conformité	
Appliquer les vérifications de sécurité de manière proactive	56
Analyseur de politique	61
Types d'anomalies détectées par l'Analyseur de politique	62
Analyse des politiques préalable aux modifications	62
Rapports d'analyse de politique préalable aux modifications	66
Analyse de politique post-modification	68
État et gestion logicielle des NGFW	71
Voir Santé du périphérique	72
Obtenez des recommandations de mise à niveau	73
Analyser la capacité métrique	76
Meilleures pratiques dans les NGFW	89
Rapport BPA à la demande	93
Puis-je toujours générer des rapports BPA à partir du portail de suppor client ?	t
Meilleures pratigues	

TECH**DOCS**

AlOps for NGFW

En vous appuyant sur les données recueillies par le biais de la télémétrie des périphériques PAN-OS, AlOps for NGFW vous fournit un aperçu de la santé et de la sécurité de votre déploiement de pare-feu nouvelle génération pour vous aider à identifier les domaines d'amélioration et combler les lacunes en matière de sécurité.AlOps for NGFW tire les informations de santé des métriques de télémétrie du périphérique liées à l'état opérationnel de vos périphériques. Pour obtenir des informations de sécurité, AlOps for NGFW analyse la configuration de vos périphériques par rapport aux meilleures pratiques de Palo Alto Networks afin de signaler toute éventuelle lacune dans votre posture de sécurité.

AIOps pour NGFW Premium et Strata Cloud Manager

Strata Cloud Manager fournit une gestion et des opérations unifiées uniquement pour les NGFW utilisant la licence AIOps pour NGFW Premium.

- Les NGFW (gérés par PAN-OS et Panorama → Pour les NGFW gérés par PAN-OS et Panorama disposant d'une licence AlOps pour NGFW Premium, utilisez Strata Cloud Manager pour superviser la santé et la posture de sécurité de votre déploiement.
- Les NGFW (gérés dans le cloud) → Une licence AlOps pour NGFW vous permet également d'utiliser Strata Cloud Manager pour la gestion du cloud pour les NGFW.

À partir d'octobre 2024, Strata Cloud Manager dispose de deux niveaux de licence : Strata Cloud Manager Essentials et Strata Cloud Manager Pro. Cette structure unifiée rationalise le déploiement des offres de sécurité réseau, notamment les AIOps pour NGFW, la gestion de l'expérience numérique autonome (ADEM), la fonctionnalité de gestion du cloud et le service de journalisation Strata. Voir Licence Strata Cloud Manager.

Si vous utilisez déjà **l'application gratuite AlOps pour NGFW** ou Strata Cloud Manager avec une licence **AlOps pour NGFW Premium**, vos licences existantes ne sont pas affectées et vous pouvez continuer à les modifier, les prolonger ou les renouveler.

Mise en route :

- AlOps pour NGFW gratuit et Premium
- Activer AlOps pour NGFW
- Commencer à envoyer la télémétrie de périphérique à AlOps pour NGFW
- Nouvelles fonctionnalités
- Rapport BPA à la demande

• AlOps pour NGFW – Incidents et alertes



Régions pour AlOps pour NGFW

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
NGFW, y compris ceux financés par les crédits NGFW logiciels	L'une des options suivantes :
	AlOps for NGFW Free ou Strata Cloud Manager Essentials
	AlOps for NGFW Premium ou Strata Cloud Manager Pro

La région que vous sélectionnez lorsque vous activez AlOps for NGFW détermine l'emplacement physique dans lequel AlOps traite vos données.

AlOps for NGFW n'est pas proposé dans toutes les régions où l'infrastructure Strata Logging Service (SLS) est prise en charge. Le déploiement d'AlOps for NGFW s'étendra bientôt à d'autres régions pour correspondre aux destinations de données de télémétrie. À l'heure actuelle, si vous envoyez vos données de télémétrie vers une région où l'application AlOps n'est pas prise en charge, elles seront traitées par une instance AlOps for NGFW dans la région États-Unis-Amériques.

Lorsque vous activez AIOps for NGFW, ces restrictions sont appliquées automatiquement. Par exemple, si vous sélectionnez l'Allemagne comme région pour activer une instance AIOps for NGFW, seuls les locataires SLS basés en Allemagne peuvent être rattachés à cette instance.



Les mêmes régions qui prennent en charge AlOps pour NGFW prennent également en charge les NGFW dans Strata Cloud Manager.

Consultez le tableau suivant pour comprendre le traitement des données AIOps pour les diverses régions de destination de la télémétrie.

Région Strata Logging Service	Région prise en charge pour une instance AIOps for NGFW pour traiter les données
Allemagne	Allemagne
Royaume-Uni	Royaume-Uni
Pays-Bas - Europe	Pays-Bas - Europe
Italie - Europe	Italie - Europe
Espagne - Europe	Espagne - Europe
Suisse - Europe	Suisse - Europe

Région Strata Logging Service	Région prise en charge pour une instance AIOps for NGFW pour traiter les données
France - Europe	France - Europe
Pologne - Europe	Pologne - Europe
Corée	Corée
Indonésie	Indonésie
Israël	Israël
Taïwan	Taïwan
Qatar	Qatar
Singapour	Singapour
Australie	Australie
Inde	Inde
Japon	Japon
Canada	Canada
Régions SLS restantes	États-Unis - Amériques

Fonctionnalités des options Gratuit et Premium

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
 NGFW, y compris ceux financés par les crédits NGFW logiciels 	 L'une des options suivantes : AlOps for NGFW Free ou Strata Cloud Manager Essentials AlOps for NGFW Premium ou Strata Cloud Manager Pro

AlOps pour NGFW est disponible en deux niveaux de licence : gratuit et premium.

Les fonctionnalités de AIOps for NGFW Gratuit enrichissent votre compréhension du déploiement de votre pare-feu.

Fonctionnalités de la version gratuite :

- évaluer la configuration du pare-feu et identifier les domaines à améliorer
- fournir un accès facile aux données d'exécution et de télémétrie historiques à partir des parefeu
- détecter les problèmes du système (indépendamment de la méthode de détection)
- réduire les délais de résolution grâce aux flux de travail d'alerte / de notification
- fournir des tableaux de bord et des visualisations dynamiques pour plusieurs abonnements de sécurité

Une licence de niveau premium vous donne accès à des fonctionnalités gratuites et premium. Les fonctionnalités de l'option premium visent à garantir une utilisation complète et un résultat de sécurité maximal de vos pare-feu.

Fonctionnalités de l'option Premium :

• Gestion du cloud pour les NGFW



Contactez l'équipe de votre compte pour activer Gestion du cloud pour les NGFW à l'aide de Strata Cloud Manager.

- utiliser des techniques de ML avancées pour promouvoir une posture de sécurité toujours optimale qui répond à l'évolution des menaces et des paysages réseau, réduisant ainsi la surface d'attaque
- fournir des tableaux de bord et des visualisations dynamiques pour WildFire et la recherche d'IOC
- interagir avec les données et visualiser les relations entre les événements du réseau dans le centre de commande de Strata Cloud Manager pour révéler des anomalies ou rechercher des moyens d'améliorer la sécurité de votre réseau

F

Strata Cloud Manager dispose de deux niveaux de licence : Strata Cloud Manager Essentials et Strata Cloud Manager Pro. Cette structure unifiée rationalise le déploiement des offres de sécurité réseau, notamment les AIOps pour NGFW, la gestion de l'expérience numérique autonome (ADEM), la fonctionnalité de gestion du cloud et le service de journalisation Strata. Voir Licence Strata Cloud Manager.

Si vous utilisez déjà **AIOps pour NGFW Gratuit** ou Strata Cloud Manager avec une licence **AIOps pour NGFW Premium**, vos licences existantes ne sont pas affectées et vous pouvez continuer à les modifier, les prolonger ou les renouveler.

Ensemble de fonctionnalités	Gratuit	Premium (utilisez Strata Cloud Manager)
Renforcement de la posture de sécurité	Partiel	Oui
Informations sur la posture de sécurité	Oui	Oui
Adoptions de fonctionnalité	Oui	Oui
Paramètres de la posture de sécurité	Non	Oui
Recommandations de mise à niveau logicielle	Non	Oui
Adoption de CDSS	Oui	Oui
Analyseur de politique	Non	Oui
Rapport BPA à la demande	Oui	Oui
Plug-in Panorama CloudConnector	Non	Oui
Analyseur de capacité	Non	Oui
Tableau de bord NGFW SDWAN	Non	Oui
Tableau de bord Résumé de la conformité	Non	Oui
Résolution des interruptions de pare-feu de manière proactive	Partiel	Oui
Alertes et incidents	Partiel	Oui
Tableau de bord des CVE PAN-OS	Oui	Oui
Analyse des causes probables des alertes	Non	Oui
Dépannage avec les journaux	Oui	Oui

Ensemble de fonctionnalités	Gratuit	Premium (utilisez Strata Cloud Manager)
Affichage, interrogation et exportation des journaux dans la visionneuse de journaux	Oui	Oui
Vérifier les licences et autres exigences pour utiliser la visionneuse de journaux.		
• Exportation des métadonnées à des fins de dépannage	Oui	Oui
Affichage du journal d'audit	Oui	Oui
Optimisation de votre investissement dans la sécurité	Partiel	Oui
 Classement des périphériques en fonction de l'état et de la posture de sécurité 	Oui	Oui
• Tous les tableaux de bord et rapports, à l'exception du tableau de bord d'informations sur les menaces	Oui	Oui
Tableau de bord et rapport des informations sur les menaces	Non	Oui
Recherche d'artefacts de sécurité	Non	Oui
Création d'un tableau de bord personnalisé	Non	Oui
Centre de commande de Strata Cloud Manager	Non	Oui
Notifications	Partiel	Oui
Notifications par e-mail	Oui	Oui
Intégration ServiceNow	Non	Oui
Engagement et support	Non	Oui

Ensemble de fonctionnalités	Gratuit	Premium (utilisez Strata Cloud Manager)
 Capacité de création de tickets intégrée au produit pour les problèmes opérationnels nécessite un support de niveau Platinum sur le pare-feu (sauf pour les alertes de panne d'alimentation) 	Non	Oui

Les nouvelles fonctionnalités du produit, dans toutes les catégories de fonctionnalités, seront attribuées aux niveaux Gratuit et Premium à la seule discrétion de Palo Alto Networks.

Comment activer AlOps pour NGFW

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
NGFW, y compris ceux financés par les crédits NGFW logiciels	 L'une des options suivantes : AlOps for NGFW Free ou Strata Cloud Manager Essentials AlOps for NGFW Premium ou Strata Cloud Manager Pro

Voici les différents scénarios pour activer AlOps for NGFW :

Scénario	Plan
Activation de AlOps for NGFW Gratuit	Activer AlOps for NGFW (Gratuit)
Activation de AlOps for NGFW Premium (utilisez l'appli Strata Cloud Manager)	Activer AlOps pour NGFW via les services communs
Intégration de nouveaux périphériques à l'instance AIOps for NGFW gratuite activée	Associer des périphériques à un locataire Activer la télémétrie sur les périphériques
Intégration de nouveaux périphériques à AlOps for NGFW Premium activé (utiliser l'appli Strata Cloud Manager)	Associer des périphériques à un locataire Associer des périphériques du locataire à l'appli Activer la télémétrie sur les périphériques
Activation de l'ELA AlOps for NGFW Premium	Activer le contrat de licence d'entreprise (ELA) AlOps pour NGFW Premium
Utilisation de Strata Cloud Manager (AlOps pour NGFW Premium) pour gérer VM-Series	Activer un contrat de licence de crédits NGFW logiciels
Utilisation de Strata Cloud Manager (AlOps pour NGFW Premium) pour VM-Series Panorama géré	Activer une licence de crédits NGFW logiciels pour VM-Series Panorama géré
Conversion d'une licence d'essai AlOps pour NGFW Premium en licence de production	Convertir une licence d'essai en licence de production
Activer Strata Cloud Manager Essentials et Strata Cloud Manager Pro	 Activer Strata Cloud Manager Essentials Activer Strata Cloud Manager Pro

Scéna	rio	Plan
	Strata Cloud Manager Essentials et Strata Cloud Manager Pro peuvent être activés dans les comptes du portail support client (CSP) qui ne disposent pas des éléments suivants : Service de journalisation Strata avec stockage dimensionné, AlOps pour NGFW Gratuit ou Premium, ou Prisma Access.	

Strata Cloud Manager fournit une gestion et des opérations unifiées uniquement pour les NGFW utilisant la licence AIOps pour NGFW Premium. Continuez à utiliser l'appli gratuite AIOps pour NGFW pour les NGFW intégrés au AIOps pour NGFW Gratuit.

Strata Cloud Manager est disponible, avec deux niveaux de licence : Strata Cloud Manager Essentials et Strata Cloud Manager Pro. Cette structure unifiée rationalise le déploiement des offres de sécurité réseau, notamment les AlOps pour NGFW, la gestion de l'expérience numérique autonome (ADEM), la fonctionnalité de gestion du cloud et le service de journalisation Strata. Si vous utilisiez Strata Cloud Manager avant l'introduction de ces nouveaux niveaux de licence, votre licence existante pour AlOps pour NGFW Premium et AlOps pour NGFW Gratuit reste prise en charge. Vous pouvez continuer à modifier, prolonger ou renouveler ces licences.

Les comptes FedRAMP ne peuvent pas utiliser AlOps for NGFW. Pour vérifier si cela s'applique à vous, connectez-vous à votre compte sur le portail de support client et sélectionnez Account Management (Gestion de compte) > Account Details (Détails du compte). Si vous voyez un FedRamp Account (Compte FedRamp) répertorié, cela indique que vous ne pouvez pas utiliser AlOps for NGFW.

Account Details -
Account New Member Roles User Access
Account Information
⊘ Customer
FedRamp Account
Email domain type: Private Users can be assigned only private (company) domain email addresses, e.g., "@acme.com.

Activer AlOps for NGFW (Gratuit)

L'activation nécessite le rôle administrateur de compte ou d'appli.

1. Connectez-vous au hub avec la vue centrée sur le locataire.

Désactivez l'option **View by Support Account (Afficher par compte de support)** si vous êtes dans la vue Compte de support.



Si vous n'avez pas de locataire existant, connectez-vous au hub avec la vue du compte de support.

- 2. Recherchez AlOps for NGFW Gratuit et sélectionnez Activate (Activer).
- **3.** Remplissez le formulaire.

enant ()	Customer Support Account	0	Region ()	
Create New .		×	United States - Americas	~
e tenant where the license will be activated prtex Data Lake sense Quantity: 0 pires: NA	Customer support account f	or this tenant	Deployment region and where your dat	ta logs are stored
Select CDL Instance	^			
	Q, n hub 2.0 (dark r	node) or under "view by tenar	rts"	

Locataire	Sélectionnez le locataire dans lequel vous activerez l'instance AlOps pour NGFW Gratuit. Si vous n'avez pas de locataire existant, sélectionnez Create New (Créer un nouveau) .
Compte de support client	Votre ID de compte sur le portail de support client.
Région	La région de déploiement et la région où vos journaux de données sont stockés. Voir Régions pour AlOps pour NGFW.
Service de journalisation Strata	Le Strata Logging Service à partir duquel vous souhaitez envoyer des données à AlOps pour NGFW Gratuit. Si vous disposez d'un SLS de journalisation, vous pouvez l'associer à AlOps pour NGFW Gratuit. Sinon, vous pouvez l'ignorer.

4. Agree to the Terms and Conditions (Accepter les conditions générales) et Activate (Activer).

5. AlOps pour NGFW Gratuit est prêt lorsque l'option Statut (État) affiche Complete (Terminé).

Common Services x tanage your existing subscriptions and add-ons, add tenants, and set up identities and roles.								
Subscriptions & Add-ons	Tenant Mar	agement Identity & Access /	Access Managemen	t				Name: TME Demo TSG ID:
Q, Search Tenants		All Tenants > TME Demo						
All Tenants		TME Demo						= / +
TME Demo	•	TSG ID: Aerospace & Defense						
		Licensed Products						1
		Products 1	Status 1	License 1	Contract 1	Expiration Date 1	Region 1	Actions
		AlOps for NGFW Free	Complete	Not Applicable	N/A 😧		United States - Americas	Actions ~

- 6. Associez des périphériques à un locataire contenant votre instance AIOps pour NGFW Gratuit.
 - **1.** Connectez-vous au hub.
 - 2. Sélectionnez Common Services (Services communs) > Device Associations (Associations de périphériques).



- 3. Sélectionnez Add Device (Ajouter un périphérique).
- 4. Sélectionnez un ou plusieurs pare-feu ou appareils Panorama, puis Save (Enregistrer).

Vous devez associer Panorama au locataire contenant AlOps pour NGFW Gratuit si vous intégrez des déploiements gérés par Panorama. Assurez-vous d'associer tous les pare-feu gérés par Panorama individuellement au locataire.

Les périphériques que vous avez associés au locataire seront automatiquement ajoutés à AlOps pour NGFW Gratuit. Pour plus d'informations, voir Associer des périphériques à un locataire.

- Pour l'activation d'AIOps pour NGFW Gratuit, il n'est pas nécessaire d'associer des applis à des périphériques.
 - Vous pouvez associer des périphériques à un locataire au début de l'activation si vous disposez déjà d'un locataire existant.
 - Vous pouvez supprimer les associations de périphériques si, par exemple, vous retirez ou renvoyez un pare-feu ou un appareil Panorama, ou si vous souhaitez l'associer à un autre groupe de services aux locataires (TSG).
- 7. Activez la télémétrie sur les périphériques.
 - Confirmez que le périphérique est enregistré dans le portail de support client en vous connectant à support.paloaltonetworks.com, passez à votre compte (si nécessaire) et identifiez votre périphérique dans Assets (Ressources) > Devices (Périphériques).
 - 2. Installez un certificat de périphérique sur les périphériques que vous souhaitez intégrer.
 - 3. Activez le partage de télémétrie sur les périphériques.
 - Une fois que vous avez intégré les périphériques et activé la télémétrie, il faut environ quelques heures pour que la première série d'informations soit visible sur le tableau de bord AIOps pour NGFW. Le processus de génération et d'envoi de télémétrie du côté du périphérique se fait par lots, chaque métrique étant échantillonnée et collectée à une fréquence optimisée en fonction des cas d'utilisation pour lesquels elle est utilisée. Ce processus par lots peut entraîner un délai entre l'intégration du pare-feu et la disponibilité des informations. Il peut s'écouler plusieurs heures avant que toutes les informations associées à un périphérique nouvellement intégré s'affichent sur le tableau de bord AIOps pour NGFW.

8. Connectez-vous à AIOps pour NGFW Gratuit en cliquant sur son icône dans le hub.

Où sont mes fonctionnalités AlOps pour NGFW ?

Ce contenu est destiné à la gestion cloud des pare-feu nouvelle génération avec AIOps for NGFW et Strata Cloud Manager. Pour commencer à gérer les pare-feu nouvelle génération avec PAN-OS, cliquez ici.

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?		
• NGFW, y compris ceux financés par les	L'une des options suivantes :		
crédits NGFW logiciels	AlOps for NGFW Free ou Strata Cloud Manager Essentials		
	AlOps for NGFW Premium ou Strata Cloud Manager Pro		

Palo Alto Networks Strata Cloud Manager est une nouvelle plateforme unifiée de gestion de la sécurité réseau alimentée par l'IA. Désormais, vous pouvez utiliser Strata Cloud Manager pour interagir AlOps for NGFW avec vos autres produits et abonnements Palo Alto Networks et les gérer.

Pour lancer Strata Cloud Manager :

- Accédez au hub et lancez l'appli Strata Cloud Manager
- Rendez-vous directement à l'URL Strata Cloud Manager
 - Strata Cloud Manager fournit une gestion et des opérations unifiées uniquement pour les NGFW utilisant la licence AIOps pour NGFW Premium. Le nom de la tuile de l'appli sur le hub pour AIOps pour NGFW (appli premium uniquement) est devenu désormais Strata Cloud Manager. Avec cette mise à jour, l'URL de l'appli est également devenue stratacloudmanager.paloaltonetworks.com, et vous verrez également le logo Strata Cloud Manager sur le volet de navigation de gauche. Continuez à utiliser l'appli gratuite AIOps pour NGFW pour les NGFW intégrés au AIOps pour NGFW gratuit.
 - Contactez l'équipe de votre compte pour activer Gestion du cloud pour les NGFW à l'aide de Strata Cloud Manager.

Si vous avez déjà utilisé l'appli AlOps for NGFW, voici où vous pouvez trouver vos fonctionnalités dans Strata Cloud Manager :

Table 1:

Appli AlOps for NGFW	Où trouver ces mêmes fonctionnalités dans Strata Cloud Manager :			
Tableaux de bord	→ Accéder à →Tableaux de bord →Santé du périphérique			

Appli AlOps for NGFW	Où trouver ces mêmes fonctionnalités dans Strata Cloud Manager :				
	Dashboards Mer Cashaerk v +				
	• Dashbardt • Otskiel with • Marking • Markin				
Alertes	\rightarrow Accéder à \rightarrow Incidents et alertes \rightarrow NGFW				
	Notice & Avers Incidents & Alerts Notice Notice Alerts Notice Notice Notice Notice Notice Notice Notice Notice Notice <t< th=""></t<>				
Surveiller	→ Accéder à →Surveiller →Périphériques →NGFW				
	Instance Andread of the				
Posture	 → Accédez aux tableaux de bord pour afficher : Tableau de bord des meilleures pratigues 				
	 Tableau de bord des informations sur la posture de sécurité 				
	Tableau de bord NGFW SD-WAN				

Appli AIOps for NGFW	Où trouver ces mêmes fonctionnalités dans Strata Cloud Manager :
	 Tableau de bord Avis de sécurité (CVE PAN-OS)
	Tableau de bord Adoption des CDSS
	Tableau de bord BPA à la demande
	 Tableau de bord Adoption des fonctionnalités
	Tableau de bord Résumé de la conformité
	<figure></figure>
	pour trouver :
	Paramètres - Panorama géré
	Nettoyage de la configuration
	Optimiseur de politique
	Contrôles de conformité
	Analyseur de politique
	Manage Posture Settings a Configuration Catentise works pointer decks for and engineent to mainter network recommendation. b Configuration Catentise works pointer decks for and engineent to mainter network recommendation. b Configuration Catentise works pointer decks for and engineent to mainter network recommendation. configuration Configuration Catentise works pointer decks for and engineent to mainter network recommendation. configuration Configuration Configuration Configuration configuration Configuration Configuration Configuration configuration Total (1998) Enabled (198) Configuration
	Configurad Condex Configurad Condex Note Androws Configurad Condex Configurad Condex
Activité	\rightarrow Accédez aux tableaux de bord pour afficher :
	Utilisation du réseau
	Informations sur les menaces

Appli AIOps for NGFW	Où trouver ces mêmes fonctionnalités dans Strata Cloud Manager :
	Utilisation de l'application
	Advanced WildFire
	Sécurité DNS
	Récapitulatif
	Activité utilisateurs
	 → Accédez à Reports (Rapports) pour générer des rapports pour les tableaux de bord pris en charge. → Accédez à Incidents & Alerts (Incidents e les construction)
Flux de travail	 → Accédez à Workflows (Flux de travail) > Software Upgrades (Mises à niveau logicielles) pour utiliser les Upgrade Recommendations (Recommandations de mise à niveau).
	Workhow NGFW - Software Upgrade Recommendations Data System Notify Statute Phone Statute
Rapports	→ Accédez à Reports (Rapports) pour planifier les rapports des tableaux de bord pris en charge.

Appli AlOps for NGFW	Où trouver ces mêmes fonctionnalités dans Strata Cloud Manager :
	 Bahbards Bahbards Monitors Monitors Manage Workfloos Workfloos Reports
Recherche	→ Accédez à Monitor (Surveiller) pour la loC Search (recherche de l'loC).
	Martar Australia Australia Australia Australia
Paramètres	→ Accédez à Incidents & Alerts (Incidents et alertes) > NGFW > Incidents & Alerts Settings (Paramètres des incidents et alertes) pour afficher Forecast and Anomaly Incidents & Alerts (Prévisions et incidents et alertes d'anomalies).
	→ Accédez à Incidents & Alerts (Incidents et alertes) > NGFW pour définir Notification Rules (Règles de notification).
	→ Accédez à Settings (Paramètres) pour afficher :
	• Journaux d'audit
	Préférences de l'utilisateur

Appli AlOps for NGFW	Où trouver ces mêmes fonctionnalités dans Strata Cloud Manager :
	<pre>virtual control of the second of the s</pre>
-	 Vous cherchez à gérer les NGFW avec Strata Cloud Manager ? Cela est pris en charge uniquement avec Strata Cloud Manager et AlOps for NGFW Premium, et n'est pas disponible dans l'appli AlOps for NGFW. → Accédez à Manage (Gérer) > Configuration > NGFWs and Prisma Access (NGFW et Prisma Access) et Workflows (Flux de travail) > NGFW Setup (Configuration NGFW).

Plug-in Panorama CloudConnector

Où puis-je utiliser ceci ?

• NGFW, y compris ceux financés par les crédits NGFW logiciels

De quoi ai-je besoin?

AlOps for NGFW Premium ou Strata Cloud Manager Pro

Vous souhaitez vérifier de manière proactive que vos règles de politique sont conformes aux meilleures pratiques ? Vous ne devriez pas avoir à attendre de recevoir une alerte, puis de résoudre un problème après avoir appliqué vos règles de politique. Connectez AIOps pour NGFW ou Strata Cloud Manager à votre Panorama pour évaluer votre configuration par rapport à certaines vérifications des meilleures pratiques avant de le transmettre à vos pare-feu gérés. Voir Application proactive des vérifications de sécurité.

Les mises à jour de vos règles de politique de sécurité sont souvent sensibles au temps et nécessitent une action rapide. Cependant, vous devez vous assurer que toute mise à jour que vous effectuez à votre base de règles de politique de sécurité répond à vos exigences et n'introduit pas d'erreurs ou de mauvaises configurations (telles que des modifications qui entraînent des règles en double ou contradictoires).

Pour y parvenir, l'Analyseur de politique de Strata Cloud Manager vous permet d'optimiser le temps et les ressources lors de la mise en œuvre d'une requête de modification. L'Analyseur de politique ne se contente pas d'analyser et de fournir des suggestions de consolidation ou de suppression éventuelle de règles spécifiques pour répondre à votre intention, mais vérifie également les anomalies, telles que les zones d'ombre, les redondances, les généralisations, les corrélations et les consolidations dans votre base de règles.

Connectez AlOps pour NGFW ou Strata Cloud Manager à votre Panorama et utilisez l'Analyseur de politique pour ajouter ou optimiser votre base de règles de politique de sécurité. Voir Analyseur de politique.

Ces éléments vous seront nécessaires pour connecter votre AIOps for NGFW à votre Panorama :

 Instance AIOps pour NGFW ou Strata Cloud Manager : Vous n'avez pas besoin d'une licence AIOps pour NGFW Premium pour installer le plug-in Panorama CloudConnector. Cependant, la licence Premium est obligatoire pour utiliser les fonctionnalités premium telles que l'Analyseur de politique et l'évaluation des meilleures pratiques (BPA) proactive. • Un Panorama avec un certificat de périphérique installé.

🔶 PANORAMA	DASHBOARD	ACC	MONITOR	POLICIES	Groups _C OBJECTS	PANORAMA
Panorama 🗸						
 Setup High Availability Config Audit Managed WildFire Clusters Managed WildFire Applianc Password Profiles Administrators Admin Poles 	Management	Operation	IS Services aucany acquire con Seria URL Filtering GT SCT	Interfaces	Telemetry N	WildFire HSM A
 Access Domain Authentication Profile Authentication Sequence User Identification Data Redistribution Scheduled Config Push Device Quarantine Managed Devices Summary 	Device Certificate	Curr	ent Device Certific Not Va Not V Last Fetched Last Fetch Last Fetched T	ate Status <mark>Valid</mark> lid Before 2022 /alid After 2022 d Message Succe ned Status succe îmestamp 2022 Get c	/05/25 15:52:25 F /08/23 15:52:25 F essfully fetched De ess /05/25 16:02:26 F eertificate	PDT PDT evice Certificate
Health		ttings				18

 Le plug-in Panorama CloudConnector installé sur votre Panorama exécutant PAN OS 10.2.3 et supérieur.

Vous devez activer ce plug-in à l'aide de la commande :

> request plugins cloudconnector enable basic

🚺 PANORAMA	DASHBOARD		C Device C DR POLICIES	oroups – OBJECTS PAN	ORAMA		Commit ∽	î⊨ 18- Q
Panorama V								G (?
No Setup 🔹	Q connector							$2/312 \rightarrow \times$
High Availability Config Audit	FILE NAME	VERSION	RELEASE DATE	SIZE	DOWNLOADED	CURRENTLY	ACTIONS	RELEASE NOTE URL
Managed WildFire Clusters	✓ Name: cloudconner	tor						
Password Profiles	cloudconnector-2.0.1	2.0.1	2023/05/24 09:14:16	76K	~	~	Remove Config S	
Admin Roles	✓ Name: cloudconnet	tor-2.0.0						
Authentication Profile	cloudconnector-2.0.0	2.0.0	2023/03/23 11:19:15	78K			Download 5	Release Notes
Authentication Sequence								



- Pour aider les clients, nous avons préinstallé ce plug-in avec les versions plus récentes de Panorama (11.0.1 et supérieures).
- Si vous avez déjà installé le plug-in AlOps et le plug-in CloudConnector, désinstallez le plug-in AlOps, car ils sont identiques et seul le nom a été modifié. Vérifiez que vous n'avez qu'un seul plug-in installé, qui doit être la version la plus récente du plug-in CloudConnector.

Si vous avez installé le plug-in AlOps sur PAN-OS 10.2.3, puis effectué une mise à niveau vers PAN-OS 11.0.1 ou une version ultérieure, une version par défaut du plug-in sera installée avec la nouvelle version de PAN-OS. Par conséquent, les deux plug-ins sont présents sur Panorama. Dans ce cas, suivez les étapes suivantes :

- 1. Dans l'interface Web de Panorama, sélectionnez Panorama > Plugins (Panorama > Plug-ins) et Uninstall (Désinstallez) le plug-in AlOps.
- 2. Activer le plug-in CloudConnector :
 - > request plugins cloudconnector enable basic

Le plug-in CloudConnector 2.2.0 prend en charge les paramètres de configuration de proxy de Panorama. Ces paramètres ne prennent effet qu'après une validation. Voici les scénarios :

- Configuration des paramètres de proxy : Lorsque vous configurez les paramètres de proxy et effectuez une validation, le plug-in CloudConnector ne reconnaîtra pas les paramètres du nouveau proxy pendant cette validation. Après la validation, le plug-in utilisera la configuration du proxy pour les interactions futures avec le cloud.
- Suppression des paramètres du proxy : Lorsque vous supprimez les paramètres du proxy et effectuez une validation, le plug-in CloudConnector ne reconnaîtra pas les paramètres supprimés du proxy pendant la validation. Après la validation, le plug-in n'utilisera plus la configuration du proxy pour les interactions futures avec le cloud.

• Télémétrie du périphérique activée sur votre Panorama.

🚺 PANORAMA	DASHBOARD	ACC	MONITOR	C Device	Groups _– OBJECTS	PANORAMA	
Panorama 🗸							
Setup High Availability Config Audit Massaged MildEire Chusters	Management	Operations	Services	Interfaces	Telemetry	WildFire HSM	ACE
 Managed WildFire Clusters Managed WildFire Applianc Password Profiles Administrators Admin Roles Access Domain Authentication Profile 		Device Health	Threat Prevention and Performance Product Usage Telemetry Region Certificate Status	Americas Device Certifica	ate is valid		
Authentication Sequence	Product Usage						Th

• Une règle de politique de sécurité qui autorise la communication entre Panorama et le FQDN correspondant à votre région hôte Strata Logging Service :

Amériques (americas)	https://prod.us.secure-policy.cloudmgmt.paloaltonetworks.com/
Australie (au)	https://prod.au.secure-policy.cloudmgmt.paloaltonetworks.com/
Canada (ca)	https://prod.ca.secure-policy.cloudmgmt.paloaltonetworks.com/
Europe (europe)	https://prod.eu.secure-policy.cloudmgmt.paloaltonetworks.com/
FedRAMP (gov)	https://prod.gov.secure-policy.cloudmgmt.paloaltonetworks.com/
Allemagne (de)	https://prod.de.secure-policy.cloudmgmt.paloaltonetworks.com/
Inde (in)	https://prod.in.secure-policy.cloudmgmt.paloaltonetworks.com/
Japon (jp)	https://prod.jp.secure-policy.cloudmgmt.paloaltonetworks.com/
Singapour (sg)	https://prod.sg.secure-policy.cloudmgmt.paloaltonetworks.com/
Royaume-Uni (uk)	https://prod.uk.secure-policy.cloudmgmt.paloaltonetworks.com/

Recevoir des notifications d'alerte

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?			
 NGFW, y compris ceux financés par les crédits NGFW logiciels 	 L'une des options suivantes : AlOps for NGFW Free ou Strata Cloud Manager Essentials AlOps for NGFW Premium ou Strata Cloud Manager Pro 			

L'intégration de Strata Cloud Manager à vos opérations existantes implique la configuration d'alertes proactives, vous permettant de détecter et de gérer les problèmes potentiels avant qu'ils ne dégénèrent en complications graves. Ces alertes peuvent être adaptées pour correspondre au protocole de gestion des cas de votre équipe d'opérations, comme les P1 ou P2 couramment utilisés.

Par exemple, vous pouvez configurer un système d'alerte dans lequel les alertes critiques, qui représentent les problèmes les plus critiques, sont instantanément transmises à votre équipe de sécurité pour une attention immédiate. D'un autre côté, les alertes d'avertissement, qui sont moins urgentes, mais toujours importantes, peuvent être organisées pour un examen quotidien. Un tel arrangement assure une gestion efficace des incidents tout en maintenant le bon déroulement de vos opérations.

Une autre option consiste à acheminer les alertes en fonction des équipes ; certaines catégories d'alertes, voire des alertes spécifiques, peuvent être acheminées vers différentes équipes qui seront les mieux équipées pour les traiter. Vous pouvez définir des préférences de notification, notamment des alertes qui déclenchent des notifications, la façon dont vous recevez les notifications et la fréquence à laquelle vous les recevez ; et ce en créant une règle de notification.

Voici une vidéo qui montre comment créer une règle de notification.

- **STEP 1** Sélectionnez Incidents & Alerts (Incidents et alertes) > Incident & Alert Settings (Paramètres d'incident et d'alerte) > Notification Rules (Règles de notification) > + Add Notification Rule (Ajouter une règle de notification)
- **STEP 2** | Saisissez un nom et une description.
- **STEP 3** Add New Condition (Ajoutez une nouvelle condition) pour spécifier les conditions de la règle qui déclencheront la notification.

Par exemple, pour créer une notification pour les alertes matérielles, sélectionnez **subCategory** (Sous-catégorie), Equals (Égale) et Hardware (Matériel).

- **STEP 4** Sélectionnez le type de notification et destinataires de la notification.
 - 1. Si vous choisissez **Email (E-mail)**, sélectionnez un groupe d'e-mail, c'est-à-dire un groupe d'utilisateurs qui recevront les notifications par e-mail. Vous pouvez aussi choisir **Create** a New Email Group (Créer un nouveau groupe d'e-mail).
 - **1.** Si vous créez un nouveau groupe d'e-mail, saisissez un nom de groupe d'e-mail et commencez à saisir les adresses e-mail des personnes que vous souhaitez ajouter au groupe. Appuyez sur la touche Retour après avoir renseigné chaque adresse e-mail.
 - 2. Sélectionnez Next (Suivant).
 - 3. Sélectionnez la fréquence à laquelle vous souhaitez envoyer ces notifications :
 - Immédiatement
 - Groupé et envoyé toutes les 4 heures
 - Groupé et envoyé une fois par jour
 - 2. Si vous choisissez **ServiceNow**, saisissez l'URL ServiceNow, les informations d'identification du client, les informations d'identification ServiceNow et la version de l'API ServiceNow.
 - 1. Test (Testez) votre connexion pour vous assurer que l'intégration fonctionne.
 - 2. Sélectionnez Next (Suivant).
- **STEP 5** | Save Rule (Enregistrez la règle).

Résoudre les anomalies de connectivité et d'application des politiques des NGFW

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
 NGFW, y compris ceux financés par les crédits NGFW logiciels 	AlOps for NGFW Premium ou Strata Cloud Manager Pro
	La licence Strata Logging Service est obligatoire pour la journalisation
	 Si vous possédez une licence Prisma Access, vous pouvez utiliser la Gestion des dossiers pour afficher vos dossiers prédéfinis et activer la sécurité Web pour un dossier

Dépannez vos NGFW à partir de Strata Cloud Manager sans avoir à passer d'une interface de pare-feu à l'autre. Si vous rencontrez des problèmes de connectivité après le déploiement et la configuration de vos NGFW, vous pouvez obtenir une vue agrégée des états de vos routages et tunnels, et explorer jusqu'à arriver aux détails spécifiques afin de rechercher les anomalies et les configurations problématiques.

Dépannez les problèmes liés à vos règles de politique basées sur l'identité et à vos terminaux définis de manière dynamique. Vous pouvez vérifier l'état de NGFW spécifiques et exposer les éventuelles incohérences entre le fonctionnement attendu d'une politique et son application effective.

Le **Troubleshooting (Dépannage)** vous permet d'explorer les problèmes susceptibles de survenir au sein de ces fonctionnalités de réseau et d'identité, en traquant et résolvant les problèmes de connectivité ou les anomalies dans l'application des politiques :

Dépannage réseau

- NAT
- Proxy DNS

Dépannage des identités et des politiques

- Groupes d'utilisateurs
- Groupes d'adresses dynamiques
- Groupe d'utilisateurs dynamiques
- ID de l'utilisateur

Dépannage de pare-feu

• Navigateur de session

IAT	0											Push Co	nfig 🗸
NAT	Policy R	ules (1)	Q Search		T		Delete	Troubleshooting	Enable	Disable	Clone	Move 🕤 🗛	dd Rule
						Oriș	ginal Packet						
		Name		Tag		Zon	e	Address	Destination	Zone	Destin	ation Interfa	Destin
~ A	II Firewalls	Pre Rules (1)										
	2	nat-out				13-z	one-Ir-1	any	zone-out-v	m-network			any

Accédez à Manage (Gérer) > Configuration > NGFW and Prisma Access (NGFW et Prisma Access) > Operations (Opérations) > > Troubleshooting (Dépannage) > Session Browser (Navigateur de session) pour commencer à dépanner vos pare-feu.

Vous pouvez également accéder à la fonctionnalité que vous souhaitez dépanner et sélectionner le bouton **Troubleshooting (Dépannage)** pour commencer.

Affichez et triez les tâches de dépannage que vous avez exécutées par État, Action, Cible de recherche et Horodatage.

Fonctionnalité	Localisation des fonctionnalités	Actions disponibles	Portée de l'action	Sortie de tâche organisée par :
Navigateur de session (pare- feu)	Gestion > Configuration > NGFW et Prisma Access > de production > > Dépannage > Navigateur de session	 Filtrer par : Pare-feu Nom de la règle Zone source Adresse source Utilisateur source Port source Zone de destination Adresse de destination Port de destination App-ID 	Pare-feu que vous spécifiez	 ID de session Heure de début Zones Source Destination Ports Protocole Application Entrée Sortie bytes
Proxy DNS (réseau)	Gérer la configuration > NGFW et Prisma Access > Paramètres du périphérique > Proxy DNS	 Afficher le cache du proxy DNS Rechercher dans le cache du proxy DNS 	Pare-feu que vous spécifiez	 nom de domaine Adresse IP Type : enregistrement d'adresse IPv4 (A), enregistrement

Fonctionnalité	Localisation des fonctionnalités	Actions disponibles	Portée de l'action	Sortie de tâche organisée par :
				d'adresse IPv6 (AAAA), enregistrement de nom canonique (CNAME), enregistrement d'échange de courrier (MX) et pointeur vers un nom canonique (PTR) Classe : Internet (IN TCP/IP), Chaos (CH) et Hésiode (HS) Durée de vie (TTL) en secondes Correspondance : nombre de fois que l'enregistrement a été demandé depuis le dernier redémarrage
NAT (Réseau)	Gérer la configuration > NGFW et Prisma Access > Politiques réseau > NAT	Afficher le pool des IP de règles NAT	Pare-feu que vous spécifiez	 rule Type Utilisé Disponible Ratio de taille de la mémoire
Groupes d'utilisateurs (identité)	Gérer la configuration > NGFW et Prisma Access > Services d'identité	• Afficher le groupe d'utilisateurs	Pare-feu que vous spécifiez	Nom d'utilisateurGroupe

Fonctionnalité	Localisation des fonctionnalités	Actions disponibles	Portée de l'action	Sortie de tâche organisée par :
	> Moteur d'identité sur le cloud	 Rechercher des groupes d'utilisateurs 		
Groupes d'adresses dynamiques (identité)	Gérer la configuration > NGFW et Prisma Access > Objets > Adresse > Groupes d'adresses	 Afficher tous les groupes d'adresses dynamiques Rechercher un groupe d'adresses dynamiques (sélectionné dans une liste) 	Pare-feu que vous spécifiez	NomFiltreMembres
Groupes d'utilisateurs dynamiques (identité)	Gérer la configuration > NGFW et Prisma Access > Objets > Groupe d'utilisateurs dynamiques	 Recherche par groupe d'utilisateurs dynamiques Recherche par nom d'utilisateur 	Pare-feu que vous spécifiez	 Membres (Nom d'utilisateur) et/ou Groupe d'utilisateurs dynamiques
ID utilisateur (Identité)	Gérer la configuration > NGFW et Prisma Access > Services d'identité > Redistribution d'identité	 Afficher tous les mappages d'IP utilisateur Rechercher les mappages d'IP utilisateur 	Pare-feu que vous spécifiez	 Adresse IP Utilisateur De Délai d'inactivité Délai d'expiration maximum

Exportation des métadonnées à des fins de dépannage

Pour fournir au support technique les informations nécessaires pour mieux vous aider, AlOps for NGFW vous permet d'exporter vos données de déploiement vers votre ordinateur local. Ces données arrivent dans des fichiers JSON qui sont compressés au format gzip. 1. Sélectionnez Help > Export Tenant Metadata (Aide > Exporter les métadonnées du locataire).



2. Prepare Metadata (Préparer les métadonnées).



3. Donwload (Téléchargez) votre fichier de métadonnées.

Le nom du fichier de métadonnées contient votre ID de portail de support client (CSP), votre ID de locataire AIOps for NGFW et l'horodatage de l'exportation : *<csp-tenant-timestamp>*.gzip.
TECH**DOCS**

Télémétrie du périphérique pour AlOps for NGFW

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?			
 , y compris ceux financés par les crédits	L'une des options suivantes :			
NGFW logiciels	ou ou ou			

AlOps for NGFW évalue la santé des pare-feu de votre déploiement en analysant les données de télémétrie que vos périphériques PAN-OS envoient au Strata Logging Service. Pour envoyer ces données, vous devez avoir activé la télémétrie de périphérique sur vos périphériques.

Une fois la télémétrie configurée, vos pare-feu nouvelle génération envoient des données de télémétrie brutes au Strata Logging Service à des intervalles fixes. Strata Logging Service analyse et traduit ces données brutes afin que les AIOps for NGFW puissent vous fournir l'état du périphérique, des visualisations et des alertes.

Intégrez vos périphériques pour commencer à envoyer la télémétrie du périphérique à AIOps for NGFW.



Activer la télémétrie sur les périphériques

Suivez les étapes ci-dessous pour utiliser AlOps for NGFW avec vos périphériques PAN-OS.

Si votre trafic sortant passe par un proxy, assurez-vous d'avoir autorisé le Domaines requis pour AlOps for NGFW.



Vous devez intégrer Panorama sur AIOps pour NGFW si vous intégrez des déploiements gérés par Panorama.

- Confirmez que le périphérique est enregistré dans le portail de support client en vous connectant à support.paloaltonetworks.com, passez à votre compte (si nécessaire) et identifiez votre périphérique dans Assets (Ressources) > Devices (Périphériques).
- 2. Installez un certificat de périphérique sur les périphériques que vous souhaitez intégrer.
- 3. Activez le partage de télémétrie sur les périphériques.
 - Une fois que vous avez intégré les périphériques et activé la télémétrie, il faut environ quelques heures pour que la première série d'informations soit visible sur le tableau de bord AIOps pour NGFW. Le processus de génération et d'envoi de télémétrie du côté du périphérique se fait par lots, chaque métrique étant échantillonnée et collectée à une fréquence optimisée en fonction des cas d'utilisation pour lesquels elle est utilisée. Ce processus par lots peut entraîner un délai entre l'intégration du pare-feu et la disponibilité des informations. Il peut s'écouler plusieurs heures avant que toutes les informations associées à un périphérique nouvellement intégré s'affichent sur le tableau de bord AIOps pour NGFW.

Domaines requis pour AlOps for NGFW

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?			
 , y compris ceux financés par les crédits NGFW logiciels 	L'une des options suivantes :			
	ou ou			
	ou ou			

Si le trafic sortant de vos périphériques passe par un proxy, assurez-vous d'avoir autorisé les FQDN suivants pour garantir une utilisation réussie d'AlOps for NGFW.

Domaines pour accéder à AlOps for NGFW

Autorisez ces domaines afin d'accéder à l'application AlOps for NGFW, quelle que soit votre région géographique.

- *.prod.di.paloaltonetworks.cloud
- *.paloaltonetworks.com
- *.prod.di.paloaltonetworks.com
- *.prod.reporting.paloaltonetworks.com
- *.receiver.telemetry.paloaltonetworks.com
- https://storage.googleapis.com

ID d'applis et domaines pour l'envoi de télémétrie

Consultez les ports TCP et les FQDN requis par Strata Logging Service pour les ID d'applis et les ports que vous devez autoriser sur vos pare-feu Palo Alto Networks afin d'envoyer des données de télémétrie à AlOps for NGFW.

Sur votre serveur proxy, en plus d'autoriser les ports et FQDN requis, autorisez le domaine qui correspond à votre région géographique afin que vos périphériques puissent envoyer des données de télémétrie à AIOps for NGFW.

Région	Domaine				
États-Unis	http://br-prd1.us.cdl.paloaltonetworks.com/				
Europe	http://br-prd1.nl.cdl.paloaltonetworks.com/				
Royaume-Uni	http://br-prd1.uk.cdl.paloaltonetworks.com/				
Canada	http://br- prd1.ca1.ne1.cdl.paloaltonetworks.com/				
Singapour	http://br- prd1.sg1.se1.cdl.paloaltonetworks.com/				

Région	Domaine
Japon	http://br- prd1.jp1.ne1.cdl.paloaltonetworks.com/
Australie	http://br- prd1.au1.se1.cdl.paloaltonetworks.com/
Allemagne	http://br- prd1.de1.ew3.cdl.paloaltonetworks.com/
Inde	http://br- prd1.in1.as1.cdl.paloaltonetworks.com/

TECH**DOCS**

Optimiser la posture de sécurité

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?		
 , y compris ceux financés par les crédits 	L'une des options suivantes :		
NGFW logiciels	🗖 ou		
	🗖 ou		

En plus de vous aider à maintenir vos pare-feu en bon état de fonctionnement, AlOps for NGFW permet de vérifier qu'ils vous offrent une protection efficace contre les menaces de sécurité.

À l'heure actuelle, les évaluations de la posture de sécurité ne prennent pas en charge les systèmes virtuels multiples. Seul le système virtuel par défaut (vsys1) est pris en compte lors du traitement de la configuration.

- Surveiller les informations sur la posture de sécurité : Obtenez une visibilité sur l'état et la tendance de la sécurité de votre déploiement en fonction des postures de sécurité des périphériques NGFW intégrés.
- Surveiller l'adoption des fonctionnalités : Affichez les fonctionnalités de sécurité que vous utilisez dans votre déploiement.
- Surveiller les abonnements de sécurité : Consultez les abonnements recommandés aux services de sécurité fournis par le cloud (CDSS) et leur utilisation sur vos périphériques.
- Évaluer les vulnérabilités : Visualisez les vulnérabilités affectant un pare-feu et une version PAN-OS spécifique, pour vous aider dans votre processus de prise de décision quant à la nécessité d'une mise à niveau.
- Surveiller le Résumé de la conformité : Consultez l'historique des modifications apportées aux vérifications de sécurité pendant une période allant jusqu'à 12 mois, regroupées par les cadres du Center for Internet Security (CIS) et du National Institute of Standards and Technology (NIST).
- Appliquer les vérifications de sécurité de manière proactive : Prenez des mesures proactives contre les configurations non optimales en bloquant les validations qui ne passent pas des vérifications particulières des meilleures pratiques.
- Analyseur de politique : Obtenez des analyses et des suggestions pour une éventuelle consolidation ou suppression de règles de politique spécifiques afin de répondre à votre posture de sécurité prévue, ainsi que des vérifications d'anomalies, telles que des ombres, des redondances, des généralisations, des corrélations et des consolidations dans votre base de règles.

Surveiller les informations sur la posture de sécurité

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?				
 , y compris ceux financés par les crédits NGFW logiciels 	• L'une des options suivantes :				
	 ou ou 				
	Un rôle qui a l'autorisation d'afficher le tableau de bord				

Vous pouvez utiliser le tableau de bord **Security Posture Insights (Informations sur la posture de sécurité)** pour obtenir une visibilité sur l'état et la tendance de la sécurité de votre déploiement en fonction des postures de sécurité des périphériques NGFW intégrés. La gravité du score de sécurité (0-100) et son niveau de sécurité correspondant (bon, passable, mauvais, critique) déterminent la posture de sécurité d'un périphérique. Le score de sécurité est calculé sur la base de la priorité, de la quantité, du type et de l'état des alertes ouvertes.

1. Accédez à Dashboards (Tableaux de bord) > Security Posture Insights (Informations sur la posture de sécurité) pour commencer.



- 2. Affichez l'état de santé de vos périphériques à l'aide de **Device Security Posture (Posture de sécurité du périphérique)**. Vous pouvez consulter les éléments suivants :
 - Le nombre total de NGFW intégrés.
 - Le nombre de périphériques qui n'ont pas envoyé de données de télémétrie depuis plus de 12 heures.
 - La priorité du score de sécurité pour les périphériques intégrés dans votre déploiement. Pour connaître les détails du périphérique et les statistiques de sécurité, cliquez sur le lien du numéro.

Par exemple, vous pouvez afficher 7 risques critiques pour tous les périphériques.



Dans ce cas, vous pouvez cliquer sur les alertes critiques et voir les périphériques qui génèrent des alertes. Vous pouvez explorer davantage et remarquer que la « protection des informations d'identification de l'utilisateur » n'a pas été activée sur les pare-feu. Vous pouvez résoudre ce problème dans tous les périphériques pour éviter les attaques d'hameçonnage.

3. Examinez vos périphériques les plus défectueux et présentant les scores de sécurité les plus régressifs pendant les 30 derniers jours. Vous pouvez consulter l'état de santé de vos périphériques, y compris leur état opérationnel, la version du logiciel et d'autres métriques importantes.

Vous pouvez également remarquer si certains périphériques exécutent des versions de logiciel obsolètes. Dans ce cas, vous pouvez planifier une mise à niveau vers la dernière version recommandée, que vous pouvez rechercher dans les Recommandations de mise à niveau.

4. Vérifiez la tendance de la posture de sécurité de votre déploiement pour la période sélectionnée. Survolez le point de déclenchement pour connaître les périphériques et les alertes actives qui contribuent à la tendance de l'état de sécurité. Vous pouvez afficher les tendances d'un ou de plusieurs périphériques filtrés par nom d'hôte, modèle ou version de logiciel.

Pour plus d'informations, voir Tableau de bord : Informations sur la posture de sécurité.

Surveiller l'adoption des fonctionnalités

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?				
 , y compris ceux financés par les crédits NGFW logiciels 	 L'une des options suivantes : ou 				
	 ou Un rôle qui a l'autorisation d'afficher le tableau de bord 				

Dans **Dashboards (Tableaux de bord)** > **Feature Adoption (Adoption des fonctionnalités)**, vous pouvez afficher les fonctionnalités de sécurité que vous utilisez dans votre déploiement. Cela vous permet de vous assurer que vous tirez le meilleur parti de vos abonnements de sécurité et des fonctionnalités de pare-feu de Palo Alto Networks.



Ce tableau de bord montre les points forts de votre politique de sécurité et les lacunes dans l'adoption des capacités que vous pouvez vous efforcer d'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 meilleures pratiques. Évaluez votre posture actuelle par rapport à la base de référence pour identifier les lacunes dans l'adoption des capacités de la politique de sécurité.

Le résumé d'adoption permet d'identifier les périphériques, les zones et les domaines dans lesquels vous pouvez apporter des améliorations par l'adoption des capacités de la politique de sécurité. Vous pouvez examiner les informations sur l'adoption par Device Group (Groupe d'appareils), Serial Number & Vsys (Numéro de série et vsys), Zones, Areas of Architecture (Zones d'architecture), Tags (Étiquettes), Rule Details (Détails de la règle) et Zone Mappings (Mappages de la zone). Filtrez le Groupe d'appareils pour réduire le champ d'application et identifier les lacunes.

Dans **Feature Adoption (Adoption des fonctionnalités)**, vous pouvez également vérifier si vos fonctionnalités de sécurité sont configurées conformément aux meilleures pratiques de Palo Alto Networks en sélectionnant **Best practices (Meilleures pratiques)**.



• Pour vous concentrer sur la conformité aux meilleures pratiques pour un ensemble spécifique de pare-feu, vous pouvez filtrer le graphique en fonction du groupe d'appareils.

 Sélectionnez la section correspondant à une fonctionnalité dans le tableau pour afficher les règles de politique susceptibles d'être améliorées.



• Sélectionnez une règle pour afficher ses détails sans avoir à quitter l'appli.

Wildfire Analysis Profiles Add Filter						Introduction NAME Temporary FNF.Corp.Cognos/DB to any
Rules not Adoptin	g Best Practices in Wild	fire Analysis Profiles for Selec				
Location 11	Rule Name [†	Source Zone †	Source Address †	Source User 11	Destination	Source
	Temporary FNE.Corp.Co	-				
		-				ZONES any
			Q			ADDRESSES
		_				Addresses
		-	6 -		_	
		anv	-			
			ę			-
						·
_		-	Ģ			-
_		-	Ģ			
_		-	Ģ			
		-	Ģ			
		-	Ģ			—
						—

Pour plus d'informations, voir Tableau de bord : Adoptions de fonctionnalité.

Surveiller les abonnements de sécurité

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?				
 , y compris ceux financés par les crédits 	• L'une des options suivantes :				
INGEW logiciels	ou				
	🗖 ou				
	 Un rôle qui a l'autorisation d'afficher le tableau de bord 				

Dans Dashboard (Tableau de bord) > Posture > CDSS Adoption (Adoption de CDSS), vous pouvez afficher les abonnements des services de sécurité fournis par le cloud (CDSS) recommandés et leur utilisation sur vos périphériques. Cela vous permet d'identifier les failles de sécurité et de renforcer la posture de sécurité de votre entreprise. Une fois que vous avez accédé à cette page, une fenêtre contextuelle s'affiche, vous demandant de confirmer ou de mettre à jour vos rôles de zone dans les NGFW afin d'obtenir des recommandations précises sur les services de sécurité. Vous pouvez suivre le lien dans cette fenêtre contextuelle pour mapper les zones aux rôles.



Actuellement, ce tableau de bord ne prend en charge que quatre abonnements de sécurité : Prévention avancée des menaces, filtrage avancé des URL, sécurité DNS et Wildfire.

- 1. En haut de la page Adoption de CDSS, vous pouvez afficher le nombre total de NGFW connus et le nombre de NGFW envoyant des données de télémétrie dans votre instance.
- 2. L'adoption de la CDSS implique la progression dans l'activation, la configuration et le respect des meilleures pratiques. Pour suivre la progression de chaque abonnement, il vous suffit de cliquer sur les chiffres dans le graphique pour afficher la liste des périphériques qui nécessitent des mises à jour tout au long de ce parcours. Dans ce cas, vérifions les NGFW dans lesquels la sécurité DNS n'est pas configurée.

Dashboards									More Dushb	oards 🗸 💽
# Device Health	📌 SASE Health	# Threat Insi	ghts CDSS Adoption	Feature Adoption	PAN-OS CVEs	On Demand BPA	NGFW SD-WAN	Best Practices		
NGPWE AT \sim										
Total Known NGFW	vis: 106 Total NGF	Ws Sending Teler	metry: 2						C Pie Chart	© Settings
		0	1. ACTIVATE		2. CONFIGURE		3. BEST PRACTICES			
		Advanced Threat Prevention	66 NGFWs : 54 Not Activated 12 License Expired		61 NGPWs Not Com	tgured on all rules	66 NGPWs Not P	ollowing Best Practices on all rules		
		Advanced URL Filtering	66 NGFWs: 66 Not Activated		61 NGFWs Not Com	tgured on all rules	66 NGFWs Not P	ollowing Best Practices on all rules		
		DNS Security	53 NGFWe : 53 Not Activated		65_NGFWs Not Cerr	taux of on oil rates	65 NGFWs Not P	ollowing Best Practices on all rules		
		WidFire	89 NGFWs : 84 Net Activated 5 License Expired		86 NGFWs Not Con	igured on all rules	86 NGPWs Not P	ollowing Best Practices on all rules		

3. Vérifiez les NGFW sur lesquels la configuration de la sécurité DNS est recommandée mais non configurée. **View details (Afficher les détails)** pour vérifier le rôle source et le rôle de destination.

🖈 Device Health 刘	SASE Health 📌 Thre	eat Insights CDSS A	doption Feature Adoption	PAN-OS CVEs On Demand BPA NGF	W SD-WAN Best Practices	
Host Name: All X	Add Filter					Reset
NGFWs on which	DNS Security configurat	ion is recommended (1	- 10 of 93)			Lat. Back to Graph View
Details	Host Name	Model II	PAN-OS Version	Recommended Security Services Not Configured on all	Security Services Configured on all	Overrides Last Update II
View Details		PA-3260	10.1.4	ADV-URL X (AS X) (AV X) (DNS X) (VP X) (WF X)		May 18, 2023, 2:14:16 PM
View Details		PA-5250	10.1.4	ADV-URL X (AS X) (AV X) (DNS X) (VP X) (WF X)		May 18, 2023, 2:24:26 PM
> View Details		PA-5250	10.1.4	DNS X	ADV-URL AS AV VP	May 18, 2023, 2:15:31 PM
> View Details		PA-5220	10.1.5	ADV-URL X (AS X) (AV X) (DNS X) (VP X) (WF X)		May 18, 2023, 2:17:22 PM
View Details		PA-5220	10.1.5	ADV-URL X AXX AV X DNS X		May 18, 2023, 2:15:37 PM

4. View Policies (Afficher les politiques) pour afficher les détails des règles et les zones source et de destination correspondantes.

De plus, vous pouvez cliquer sur le nom d'une règle pour afficher ses détails.

- **5.** Revenez au graphique en entonnoir. Vous pouvez également afficher les mêmes informations dans un format de graphique circulaire.
- 6. Si vous n'avez pas besoin d'un service de sécurité recommandé pour une raison quelconque, vous pouvez le remplacer. Dans ce cas, le service de sécurité DNS n'est plus nécessaire. Cliquez sur l'icône d'annulation à côté de **DNS**.

Host Name: All X	T Add Filter							Reset
NGFWs on which	DNS Security configuration	is recommended (1 ·	10 of 93)				🔛 Back to Graph View	•
Details	Host Name	Model II	PAN-OS Version	Recommended Security Services Not Configured on alL.	Security Services Configured on all.	Overrides	Last Update II	
 View Details 	Cheopp_Dallas_3260_1	PA-3260	10.1.4	ADV-URL X AS X AV X 015 3			May 18, 2023, 2:14:16	6 PM
 View Details 	Concepp_Dallas_FW_525	< PA-5250	10.1.4	ADV-URL X AS X AV X DNS X			May 18, 2023, 2:24:26	i PM
View Details	Concapp_Dallas_FW_525	C PA-5250	10.1.4	DNS X	ADV-URL AS AV VP		May 18, 2023, 2:15:31	I PM

7. Sélectionnez l'une des raisons de passer outre la recommandation.

NGFWs on which DNS Security configuration is recommended (1 - 10 of 93) It acts to coupt Weil Details Heir Nume Model II PANOS Wreinin III Recommended Security Services Not Configured on all. Overrides List Update III > View Details © Oncopy, Dalar, 1260,1 Hi-3200 10.1.4 Recommended Security Services Not Configured on all. Overrides May 18, 2022, 214:16 PM > View Details © Oncopy, Dalar, 17W, 521 Hi-3200 10.1.4 Recommended Security Services Not Configured on all. Overrides May 18, 2022, 224:16 PM > View Details © Oncopy, Dalar, FW, 521 Hi-3200 10.1.4 Recommended for Configured on all. May 18, 2022, 224:26 PM > View Details © Oncopy, Dalar, FW, 521 Hi-3200 Coverride the recommended for Configured on all. May 18, 2022, 224:26 PM > View Details © Oncopy, Dalar, FW, 522 Hi-3200 Coverride the recommended for Configured on all. May 18, 2022, 227:27 PM > View Details © Oncopy, Dalar, FW, 64-3220 This action or reliable for recommended for the cover of the security of all and the coverity of the cover of the security of all and the cover	Host Name: All X Y Add F	liter							Reset
Datalin Hold II Model II Model II Model III Recommended security services los Configured an all. Security Services Configured an all. Overrides Lat Update III > View Details If Omage, Data; 1280; 1 IA-5260 10.14 Introduction IIII Introduction IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	NGFWs on which DNS S	ecurity configuration is	recommended (1 - 10) of 93)				Back to Graph View	•
> View Detail: © Oncopy, Dalar, 1200, 1 No. 10.4 EV. View, View, X EV. View, View, View, X EV. View, View, View, View, X EV. View, View, View, X EV. View, View, X EV. View, View, View, View, X EV. View, View, X EV. View, View, X EV. View,	Details	Host Name	Model II	PAN-OS Version	Recommended Security Services Not Configured on all	Security Services Configured on all	Overrides	Last Update	
> View Detail: © Oncapy, Dalar, FW, 331: FM, 5203 10.1.4 EXCURLE, X, M, X, Y, DEEX May 18, 2003, 22.43.4 FM > View Detail: © Oncapy, Dalar, FW, 331: FM, 5203 Dot Excurring Excurring > View Detail: © Oncapy, Dalar, FW, 332: FM, 5203 Ocerride the recommendation for DNS Security? Excurring Excurring > View Detail: © Oncapy, Dalar, FW, 335: FM, 5203 Ocerride the recommendation for DNS Security? Excurring and FM view? May 18, 2003, 22.32.31 FM > View Detail: © Oncapy, Dalar, FW, FM, 5203 The action corrises the recommendation for DNS Security? Excurring and FW view? May 18, 2003, 23.23.31 FM > View Detail: © Oncapy, Dalar, FW, FM, 5203 The back innerview State Cool Manager, plasar Excurring and FW view? May 18, 2003, 23.23.37 FM > View Detail: © Oncapy, Dalar, VM, O FM view? May 18, 2003, 23.23.33 FM May 18, 2003, 23.23.33 FM > View Detail: © Oncapy, Dalar, VM, O FM view? May 18, 2003, 23.23.33 FM May 18, 2003, 23.23.33 FM > View Detail: © Oncapy, Dalar, VM, O FM view? May 18, 2003, 23.23.33 FM > View Detail: © Oncapy, Dalar, VM, O FM view? May 18, 2003, 23.23.33 FM > View Detail: © Oncapy, Dalar, VM, O FM view? May 18, 2003, 23.23.33 FM > View Detail: © Oncapy,	View Details	Oncapp_Dallas_3260_1	PA-3260	10.1.4	ADV-URL X AS X AV X DHS			May 18, 2023, 2:14:16	РМ
> View Details © Decays, Datas, FW, 321 FA 3250 Override the recommendation for DNS Security? > View Details © Decays, Datas, FW, 322 FA 3250 > View Details © Decays, Datas, FW, 323 FA 3250 > View Details © Decays, Datas, FW, 84-3220 This scill override the recommendation for DNS Security? > View Details © Decays, Datas, FW, 84-3220 This scill override the recommendation for DNS Security? > View Details © Decays, Datas, FW, 84-3220 This scill override the recommendation for DNS Security? > View Details © Decays, Datas, FW, 84-3220 This scill override the recommendation for DNS Security? > View Details © Decays, Datas, FW, 84-3220 This scill override the recommendation for datafiely DS security? > View Details © Decays, Datas, VI, 84 May 18, 2022, 213-37 FM > View Details © Decays, Datas, VI, 9 R4-VA1500 © Datas © Decays, Datas, VI, 9 R4-VA1500 > View Details © Decays, Datas, VI, 9 R4-VA1500 > View Details © Decays, Datas, VI, 9 R4-VA1500 > View Details © Decays, Datas, VI, 9 R4-VA1500 > View Details © Decays, Datas, VI, 9 R4-VA1500	View Details	Oneapp_Dallas_FW_5250	PA-5250	10.1.4	ADV-URL X AS X AV X DNS X			May 18, 2023, 2:24:26	PM
> Yiew Detail: © Oncopy. Distanter FW PA-5220 This action overfids the recommendation for DHS security and divices? We X We X <td>View Details</td> <td>Oneapp_Dallas_FW_525(</td> <td>PA-5250</td> <td>Override the recommendation</td> <td>on for</td> <td>ADV-URL AS AV VP</td> <td></td> <td>May 18, 2023, 2:15:31</td> <td>РМ</td>	View Details	Oneapp_Dallas_FW_525(PA-5250	Override the recommendation	on for	ADV-URL AS AV VP		May 18, 2023, 2:15:31	РМ
> View Details © Oncopy_Dublecrifter, FW_PR-5220 To help is improve Strata Cloud Manager, Hease for transfer between these zones. Str. S x (AV X) (BB X) May 18, 2023, 215.37 PM > View Details © Oncopy_Dublecrifter, FW_PR-5200 For transfer between these zones. W X W X BB X May 18, 2023, 215.37 PM > View Details © Oncopy_Dublecrifter, FW_PR-5200 Oncopy_Dublecrifter, FW_PR-5200 Win C May 18, 2023, 215.37 PM > View Details © Oncopy_Dublecrifter, VM_PR-5000 Others May 18, 2023, 215.37 PM > View Details © Oncopy_Dublecrifter, VM_PR-5000 May 18, 2023, 215.37 PM > View Details © Oncopy_Dublecrifter, VM_PR-5000 May 18, 2023, 215.37 PM > View Details © Oncopy_Dublecrifter, VM_PR-5000 May 18, 2023, 215.37 PM > View Details © Oncopy_Dublecrifter, VM_PR-5000 May 18, 2023, 215.37 PM	View Details	Oneapp_Datacenter_FW	PA-5220	This action overrides the recommend DNS Security on all devices?	dation for X AS X AV X DNS X			May 18, 2023, 2:17:22	РМ
Y Weer Details X Oncepter Details (VML) PALVMOD0 Totalise int vession X // // X // X // X // X // X // X //	View Details	Oneapp_Datacenter_FW	PA-5220	To help us improve Strata Cloud Man let us know the reason for disabling I for traffic between these zones.	DNS Security X AS X AV X DNS X			May 18, 2023, 2:15:37	РМ
Yew Details X Add a comment (optional) X Add a comment (optional) X May 18, 2023, 21305 PM May 18, 2023, 21305 PM	View Details	Oneapp_Dublin_VM_0	PA-VM300	Using a different vendor Others	X (AS X) (AV X) (DNS X)		WF C	May 18, 2023, 2:15:53	РМ
Unter Comment Pers.	View Details	Oneapp_Dublin_VM_1	PA-VM300	Add a comment (optional)	X AS X AV X DNS X		WF C	May 18, 2023, 2:15:05	РМ
Y Ver Desit X Oreage Duble, VM, 10 PAVM000 X Oreage Duble, VM, 10 PAVM	View Details	Oneapp_Dublin_VM_10	PA-VM300	Cancel				May 18, 2023, 2:13:01	РМ
Xew Details X Exp 2016 X Xex X Zer X <td>View Details</td> <td>Oneapp_Dublin_VM_11</td> <td>PA-VM300</td> <td>10.1.5</td> <td>ADV-URL X AS X AV X DNS X</td> <td></td> <td></td> <td>May 18, 2023, 2:16:32</td> <td>РМ</td>	View Details	Oneapp_Dublin_VM_11	PA-VM300	10.1.5	ADV-URL X AS X AV X DNS X			May 18, 2023, 2:16:32	РМ
Ver Details Z Oncourt, Outlin, VM, 12 PA-VM300 10.15 PAV-VMC AS AV VP Ver Details X Ver Details X Ver Details Ver Details Ver Details Ver Details May 18, 2023, 21214 PM	View Details	Concapp_Dublin_VM_12	PA-VM300	10.1.5	DNS X	ADV-URL AS AV VP		May 18, 2023, 2:13:16	PM

8. Cliquer Override (Remplacer).

Cela conclut l'affichage des abonnements CDSS recommandés et leur utilisation dans vos périphériques.

Pour plus d'informations, voir Tableau de bord : Adoption de CDSS.

Évaluer les vulnérabilités

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
 , y compris ceux financés par les crédits NGFW logiciels 	L'une des options suivantes :
	□ ou

Strata Cloud Manager vous indique les vulnérabilités qui affectent un pare-feu et une version PAN-OS donnés pour vous aider à décider si vous devez effectuer une mise à niveau. Accédez à **Incidents & Alerts (Incidents et alertes)** > **NGFW (NGFW)** > **All Alerts (Toutes les alertes)** et sélectionnez l'alerte **PAN-OS Known Vulnerability (Vulnérabilité connue de PAN-OS)** Alerte pour voir les Avis de sécurité les plus récents qui affectent le pare-feu qui a déclenché l'alerte.

Sélectionnez Vulnerabilities in this PAN-OS version (Vulnérabilités dans cette version de PAN-OS) pour afficher la fonctionnalité affectée d'une vulnérabilité dans la colonne Feature Affected (Fonctionnalité affectée). Cela vous permet de décider si vous devez mettre à niveau un pare-feu en fonction de la vulnérabilité et de son impact sur la fonctionnalité activée. Si une CVE n'est pas associée à une fonctionnalité, la valeur sous Feature Affected (Fonctionnalité affectée) est vide. Ce type de CVE affecte le pare-feu du modèle spécifié ou de la version spécifiée.

Par défaut, l'alerte **PAN-OS Known Vulnerability (Vulnérabilité connue de PAN-OS)** affiche toutes les vulnérabilités de la version PAN-OS du périphérique. Cependant, si vous avez activé la télémétrie d'utilisation du produit sur le pare-feu, vous pouvez choisir de n'afficher que les vulnérabilités qui affectent le pare-feu particulier en fonction de ses fonctionnalités activées. Cela vous permettra de mieux comprendre quelles vulnérabilités constituent un objet de préoccupation pour le pare-feu et de prendre une décision plus éclairée concernant la mise à niveau.

Alertidetal	IIS					
AN-OS Kr	nown Vu	Inerability -				
ial Number:		Model: PA-VM SW Version: 9.1.3 IP Address:				
	Your curren	nt version of PAN-OS has known vulnerabilities.				
	IMPACI	r				
	The curren	t OS has known security vulnerabilities that have been patched	in newer versions.			
Events						
Active Histor	rv .					
Software Secu		o Detaile			Minimum Eived Version: 9113	
Software Secu	irity Advisoi	γ Details			Minimum Fixed Version: 9.1.13	
Software Secu Vulnerabilities on t	irity Advisoi	y Details Vulnerabilities in this PAN-OS version			Minimum Fixed Version: 9.1.13	✓ RECOMMENDATIONS See Software Security Advisory Details table for known vulnerabilities found on your current PAN-OS version.
Software Secu Vulnerabilities on t	irity Advisor this firewall Advisory S.	y Details Wulnerabilities in this PAN-OS version Title	Feature Affected	CVE Fixed Version	Minimum Fixed Version: 9.1.13	✓ RECOMMENDATIONS See Software Security Advisory Details table for known vulnerabilities found on your current PAN-OS version. Consider updating PAN-OS version based on CVE Field Version column. Monitor Palo Jol No Networks Security
Software Secu Vulnerabilities on t ID CVE-2022-0778	irity Advisor this firewall Advisory S. High	y Details Vulnerabilities in this PAN-OS version Title Impact of the OpenSSL Infinite Loop Vulnerability CVE	Feature Affected	CVE Fixed Version → 100.10	Minimum Fixed Version: 9.1.13 Updated Date 25 Jun 2022 at 00:40:12	✓ RECOMMENDATIONS See Software Security Advisory Details table for known vulnerabilities found on your current PAN-OS version. Consider updating PAN-OS version based on CVE Fiked Version column. Monitor Pah Jot No Networks Security Advisories for the latest vulnerabilities
Software Secu Vulnerabilities on t ID CVE-2022-0778 CVE-2022-0024	irity Advisor this firewall Advisory S. High High	y Details Vulnerabilities in this PAN-OS version Title Impact of the OpenSSL Infinite Loop Vulnerability CVE PAN-OS: Improper Neutralization Vulnerability Leads t	Feature Affected	CVE Fixed Version >= 10.0.10 >= 10.0.10	Minimum Fixed Version: 9.1.13 Updated Date 25 Jun 2022 at 00:40:12 11 May 2022 at 21:30:25	✓ RECOMMENDATIONS See Software Security Advisory Details table for known vulnerabilities found on your current PAN-OS version. Consider updating PAN-OS version based on CVE Fixed Version column. Monitor Pah Joh Not Networks Security Advisories for the latest vulnerabilities
Software Secu Vulnerabilities on t ID CVE-2022-0778 CVE-2022-0024 CVE-2022-0024	rity Advisor this firewall Advisory S. High High Medium	y Details Vulnerabilities in this PAN-OS version Title Impact of the OpenSSL Infinite Loop Vulnerability CVE PAN-OS: Improper Neutralization Vulnerability Leads t PAN-OS: Denial-of-Service (DoS) Vulnerability in DNS	Feature Affected	CVE Fixed Version >= 10.0.10 >= 10.0.10 >= 10.0.10	Minimum Fixed Version: 9.1.13 Updated Date 25 Jun 2022 at 00:40:12 11 May 2022 at 21:30:25 13 Apr 2022 at 21:29:59	✓ RECOMMENDATIONS See Software Security Advisory Details table for known vulnerabilities found on your current PAN-OS version. Consider updating PAN-OS version based on CVE Fixed Version column. Monitor Palo Alto Networks Security Advisories for the latest vulnerabilities
Software Secu Vulnerabilities on t ID CVE-2022-0778 CVE-2022-0024 CVE-2022-0023 CVE-2022-0023	this firewall Advisory S. High High Medlum Medium	y Details Vulnerabilities in this PAN-OS version Title Impact of the OpenSSL Infinite Loop Vulnerability CVE PAN-OS: Improper Neutralization Vulnerability Leads t. PAN-OS: Denial-of-Service (DoS) Vulnerability in DNS PAN-OS: Use of a Weak Cryptographic Algorithm for St.	Feature Affected	CVE Fixed Version >= 10.0.10 >= 10.0.10 >= 10.0.10 >= 10.0.7	Minimum Fixed Version: 9.1.13 Updated Date 25 Jun 2022 at 00:40:12 11 May 2022 at 21:30:25 13 Apr 2022 at 21:29:59 09 Mar 2022 at 22:21:41	✓ RECOMMENDATIONS See Software Security Advisory Details table for known vulnerabilities found on your current PAN-OS version. Consider updating PAN-OS version based on CVE Fixed Version column. Monitor Palo Alto Networks Security Advisories for the latest vulnerabilities
Software Secu Vulnerabilities on t D CVE-2022-0778 CVE-2022-0024 CVE-2022-0023 CVE-2022-0022 CVE-2022-0022	rrity Advisor this firewall Advisory S. High High Medium Medium Medium	y Details Vulnerabilities in this PAN-OS version Title Impact of the OpenSSL Infinite Loop Vulnerability CVE PAN-OS: Improper Neutralization Vulnerability Leads t PAN-OS: Denial-of-Service (DoS) Vulnerability in DNS PAN-OS: Use of a Weak Cryptographic Algorithm for St PAN-OS: OS Command Injection Vulnerability in the C	Feature Affected DNS Proxy non-FIPS-CC operational	CVE Fixed Version >= 10.0.10 >= 10.0.10 >= 10.0.10 >= 10.0.7 >= 10.0.8	Updated Date 25 Jun 2022 at 00:40:12 11 May 2022 at 21:30:25 13 Apr 2022 at 21:29:59 09 Mar 2022 at 22:2:21:41 24 Nov 2021 at 00:38:07	✓ RECOMMENDATIONS See Software Security Advisory Details table for known vulnerabilities found on your current PAN-OS version. Consider updating PAN-OS version based on CVE Fixed Version column. Monitor Palo Alto Networks Security Advisories for the latest vulnerabilities
Software Secu Vulnerabilities on t ID CVE-2022-0778 CVE-2022-0024 CVE-2022-0023 CVE-2022-0022 CVE-20221-3061 CVE-2021-3054	rrity Advisor this firewall Advisory 5. High High Medium Medium Medium High	y Details Vulnerabilities in this PAN-OS version . Title Impact of the OpenSSL Infinite Loop Vulnerability CVE PAN-OS: Improper Neutralization Vulnerability Leads t PAN-OS: Unail-of-Service (DoS) Vulnerability in DNS PAN-OS: Use of a Weak Cryptographic Algorithm for St PAN-OS: Of a Weak Cryptographic Algorithm for St PAN-OS: OS Command Injection Vulnerability in the C PAN-OS: Unsigned Code Execution During Plugin Insta	Feature Affected DNS Proxy non-FIPS-CC operational	CVE Fixed Version >= 100.10 >= 100.10 >= 100.10 >= 100.7 >= 100.8 >= 100.7	Updated Date 25 Jun 2022 at 00:40:12 11 May 2022 at 21:30:25 13 Apr 2022 at 21:29:59 09 Mar 2022 at 22:2:141 24 Nov 2021 at 00:38:07 13 Sep 2021 at 21:52:33	✓ RECOMMENDATIONS See Software Security Advisory Details table for known vulnerabilities found on your current RAN-OS version. Consider updating PAN-OS version based on CVE Fixed Version column. Monitor Falo Alto Network Security Advisories for the latest vulnerabilities
Software Secu Vulnerabilities on t DCVE-2022-0778 CVE-2022-0024 CVE-2022-0023 CVE-2022-0022 CVE-2021-3051 CVE-2021-3054 CVE-2021-3050	rity Advisor this firewall Advisory S. High High Medium Medium High High	y Details Vulnerabilities in this PAN-OS version Title Impact of the OpenSSL Infinite Loop Vulnerability CVE PAN-OS: Improper Neutralization Vulnerability Leads t PAN-OS: Use of a Weak Cryptographic Algorithm for St PAN-OS: Use of a Weak Cryptographic Algorithm for St PAN-OS: Unsigned Code Execution Vulnerability in the C PAN-OS: Unsigned Code Execution During Plugin Insta PAN-OS: OS Command Injection Vulnerability in Meb I	Feature Affected DNS Proxy non-FIPS-CC operational	CVE Fixed Version >= 100.10 >= 100.10 >= 100.10 >= 100.7 >= 100.7 >= 100.7 >= 100.7	Minimum Fixed Version: 9.1.13 Updated Date 25 Jun 2022 at 00:40:12 11 May 2022 at 21:30:25 13 Apr 2022 at 21:29:59 09 Mar 2022 at 21:29:59 09 Mar 2022 at 21:21:41 24 Nov 2021 at 00:38:07 13 Sep 2021 at 21:52:33 11 Aug 2021 at 21:25:40	✓ RECOMMENDATIONS See Software Security Advisory Details table for known vulnerabilities found on your current PAN-OS version. Consider updating PAN-OS version based on CVE Fled Version column. Monitor Palo Alto Networks Security Advisories for the latest vulnerabilities

Vous pouvez également utiliser le tableau de bord **PAN-OS CVEs (CVE PAN-OS)** qui vous indique le nombre de périphériques touchés par une vulnérabilité spécifique en fonction des fonctionnalités activées sur les périphériques. Strata Cloud Manager analyse les fonctionnalités activées pour déterminer quels périphériques sont touchés par la CVE. La tâche suivante montre comment évaluer les vulnérabilités qui affectent les périphériques et générer des recommandations de mise à niveau pour corriger les vulnérabilités.

Dashboards						A
★ Device Health ★ Threat Insights	Security Posture Insights	NGFW SD-WAN	AN-OS CVEs	CDSS Adoption	Best Practice + More Dashboards	~
Y Add Filter					Reset	
Devices Impacted by Security Adv 0 out of 33 devices selected	visories			ations Select All	Expand All Sort by: Severity V	
CVE-2021-44228 Severity: 9.8 - Critical	Impact of Log4j Vulnerabilities CVE-2021- 44228, CVE-2021-45046, CVE-2021-45105, and CVE-2021-44832	Published Date: 10 Dec 2021	Updated I	Date: 22 Jan 2022	Devices Impacted: 1/101	
CVE-2021-3050 Z Severity: 0 8.8 - High	PAN-OS: OS Command Injection Vulnerability in Web Interface	Published Date: 11 Aug 2021	Updated I	Date: 11 Aug 2021	Devices Impacted: 1/101	
CVE-2021-3058 Severity: ● 8.8 - High	PAN-OS: OS Command Injection Vulnerability in Web Interface XML API	Published Date: 10 Nov 2021	Updated	Date: 10 Nov 2021	Devices Impacted: 1/101	
CVE-2022-0028 C Severity: 8.6 - High	PAN-OS: Reflected Amplification Denial-of- Service (DoS) Vulnerability in URL Filtering	Published Date: 10 Aug 2022	Updated	Date: 19 Aug 2022	Devices Impacted: 4/101	

Cette tâche montre comment évaluer les vulnérabilités qui impactent les périphériques et générer des recommandations de mise à niveau pour les corriger.

- STEP 1 | Dans Strata Cloud Manager, accédez à Dashboards (Tableaux de bord) > PAN-OS CVEs (CVE PAN-OS).
- **STEP 2** Développez une CVE pour afficher les périphériques affectés par celle-ci.
- **STEP 3** | Sélectionnez les périphériques que vous souhaitez mettre à niveau pour corriger les vulnérabilités.
- **STEP 4** Generate Upgrade Recommendations (Générer des recommandations de mise à niveau).
- **STEP 5** | Cliquez sur le rapport nouvellement généré pour les périphériques.
- STEP 6 | Sélectionnez l'une des options de mise à niveau pour afficher des détails sur New Features (Nouvelles fonctionnalités), PAN-OS Known Vulnerabilities (Vulnérabilités connues de PAN-OS), Changes of Behavior (Changements de comportement) et PAN-OS Known Issues (Problèmes connus de PAN-OS)

Vous pouvez Export (Exporter) les détails dans un fichier CSV et le télécharger.

Surveiller le Résumé de la conformité

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
 , y compris ceux financés par les crédits NGFW logiciels 	 ou Licence pour afficher les données du produit pris en charge dans le tableau de bord : Prisma Access

Pour accéder au tableau de bord Résumé de la conformité, accédez à **Tableaux de bord**, puis sélectionnez l'onglet **Résumé de la conformité**. Vous pouvez consulter l'historique des modifications apportées aux vérifications de sécurité effectuées jusqu'à 12 mois auparavant, regroupées par les cadres du Center for Internet Security et du National Institute of Standards and Technology (NIST). Pour chaque cadre, vous verrez une liste de contrôles ainsi que le pourcentage du taux de conformité actuel et moyen, le nombre total de vérifications des meilleures pratiques et le nombre de vérifications échouées pour chaque contrôle. Interagissez avec le graphique et la liste afin de voir la relation entre les contrôles et leurs statistiques historiques. Affichez les détails des contrôles individuels et de leurs vérifications associées, et sélectionnez une vérification des meilleures pratiques pour afficher la configuration du pare-feu dont la vérification a échoué. Le cadre des **contrôles de sécurité critiques du CIS** est un ensemble prioritaire de mesures recommandées et de meilleures pratiques qui permettent de protéger les organisations et leurs données contre les vecteurs de cyberattaque connus.



Vous pouvez consulter les résumés des contrôles pour 11 des 16 contrôles de base et fondamentaux du CIS :

- CSC 3 : Gestion continue des vulnérabilités
- CSC 4 : Utilisation contrôlée des privilèges administratifs
- CSC 6 : Maintenance, surveillance et analyse des journaux d'audit
- CSC 7 : Protection des messageries et des navigateurs Web
- CSC 8 : Défenses contre les logiciels malveillants
- CSC 9 : Limitation et contrôle des ports, protocoles et services réseau

- CSC 11 : Configuration sécurisée pour les périphériques réseau, comme les pare-feu, les routeurs et les commutateurs
- CSC 12 : Défense des limites
- CSC 13 : Protection des données
- CSC 14 : Accès contrôlé sur la base du besoin de connaître
- CSC 16 : Surveillance et contrôle des comptes

Le framework Contrôles du cadre de cybersécurité NIST SP 800-53 fournit des conseils aux organismes fédéraux et autres organisations pour mettre en œuvre et maintenir des contrôles de sécurité et de confidentialité pour leurs systèmes d'information. Vous pouvez afficher les résumés des vérifications pour huit familles de contrôles NIST :

- SC : Contrôle de l'accès
- AU : Audit et responsabilité
- CM : Gestion de la configuration
- CP : Plans d'urgence
- IA : Identification et authentification
- RA : Évaluation du risque
- SC : Protection des systèmes et des communications
- SI : Intégrité des systèmes et de l'information

Pour plus d'informations, voir Tableau de bord : Résumé de la conformité.

Appliquer les vérifications de sécurité de manière proactive

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
 , y compris ceux financés par les crédits NGFW logiciels 	ou

Vous pouvez personnaliser les contrôles de la posture de sécurité de votre déploiement afin de maximiser les recommandations pertinentes à l'aide des fonctionnalités ci-dessous.

• Vérifications de sécurité

Liste des vérifications des meilleures pratiques, vérifications utilisées par AlOps pour NGFW pour évaluer votre configuration. La configuration des pare-feu et de Panorama est comparée aux vérifications des meilleures pratiques de Palo Alto Networks pour évaluer la posture de sécurité de vos périphériques et générer des alertes de sécurité. Vous pouvez consulter la liste des vérifications des meilleures pratiques, qui sont utilisées pour évaluer votre configuration.

lci, vous pouvez :

- **1.** Définir le niveau de sévérité des vérifications pour identifier celles qui sont les plus critiques à votre déploiement.
- 2. Désactiver temporairement les vérifications.

Si vous choisissez de désactiver une vérification, vous pouvez spécifier la durée de la désactivation et laisser un commentaire pour en expliquer la raison.

- 3. Définir la réponse lors de l'échec d'une vérification.
- Mappage de zone sur un rôle

Mapper les zones dans les NGFW aux rôles pour obtenir des recommandations personnalisées.

• Mappage de rôle sur le service de sécurité

Gérer les services de sécurité nécessaires au trafic entre les zones et les rôles dans tous les NGFW.

Le plug-in Panorama CloudConnector vous permet de prendre des mesures proactives contre les configurations non optimales en bloquant les validations qui ne passent pas certaines vérifications particulières des meilleures pratiques. Lorsque vous indiquez dans AlOps for NGFW que vous souhaitez une vérification sur **Fail Commit (Échec de la validation)**, Panorama bloque automatiquement les validations de toute configuration qui ne passe pas cette vérification. Plutôt que d'attendre la réception d'une alerte concernant un échec de vérification des meilleures pratiques, utilisez le plug-in pour empêcher les problèmes de configuration de votre déploiement.

STEP 1 Assurez-vous desatisfaire toutes les conditions préalables et installez le plug-in.

- **STEP 2** | Spécifiez les vérifications des meilleures pratiques qui bloqueront les validations en cas d'échec.
 - 1. Sélectionnez Manage (Gérer) > Security Posture (Posture de sécurité) > Settings (Paramètres).
 - 2. Recherchez la vérification avec laquelle vous souhaitez bloquer les validations.
 - 3. Définissez une Action on Fail (Action en cas d'échec) pourFail Commit (Échec de la validation)

- **STEP 3** Vérifiez en essayant de valider une configuration qui ne passe pas la vérification.
 - 1. Connectez-vous à Panorama.
 - 2. Violez la vérification des meilleures pratiques que vous avez spécifiée dans Fail Commit (Échec de la validation).



3. Sélectionnez Commit (Valider) > Commit to Panorama (Valider sur Panorama) > Validate Configuration (Valider la configuration).

A contract of the second se					Sec.		lasteste	
	-			-	 			
E		(internal)	conservable in the second					
Renau Carlo		en inenti						

Une boîte de dialogue doit s'afficher, indiquant que la validation a échoué parce que la configuration n'a pas passé la vérification des meilleures pratiques.

Commit to Panor	ama		0 🗆
Doing a commit will over	Validate Status	?	
Commit All Changes COMMIT SCOPE shared-object	Operation Validate Status Completed Result Failed Details Plugin: alops name: rule security.001 location: shared checkMessage : Add meaningful description to security policy rule name: rule_security.0012-1 location: shared checkMessage : Add meaningful description to security policy rule Failed to initiate Plugin Phase1 commit Configuration is invalid Warnings		ADMINS
Preview Changes	Clos	•	t Cancel

La définition d'une vérification sur **Fail Commit (Échec de la validation)** entraîne l'échec de la vérification de la validation et de l'opération de validation proprement dite.

Voir Gérer : Paramètres de la posture de sécurité pour plus d'informations.

Analyseur de politique

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
NGFW (Panorama géré)	ou
 (Panorama géré) 	Plug-in Panorama CloudConnector pour les déploiements Panorama gérés

Les mises à jour de vos règles de politique de sécurité sont souvent sensibles au temps et nécessitent une action rapide. Cependant, vous devez vous assurer que toute mise à jour que vous effectuez à votre base de règles de politique de sécurité répond à vos exigences et n'introduit pas d'erreurs ou de mauvaises configurations (telles que des modifications qui entraînent des règles en double ou contradictoires).

L'Analyseur de politique dans Strata Cloud Manager vous permet d'optimiser le temps et les ressources lors de la mise en œuvre d'une requête de modification. L'Analyseur de politique ne se contente pas d'analyser et de fournir des suggestions de consolidation ou de suppression éventuelle de règles spécifiques pour répondre à votre intention, mais vérifie également les anomalies, telles que les zones d'ombre, les redondances, les généralisations, les corrélations et les consolidations dans votre base de règles.

Utilisez l'Analyseur de politique pour ajouter ou optimiser votre base de règles de politique de sécurité.

- Avant d'ajouter une nouvelle règle : vérifiez s'il est nécessaire d'ajouter de nouvelles règles. L'Analyseur de politique vous recommande la meilleure façon de modifier vos règles de politique de sécurité existantes pour répondre à vos besoins sans ajouter une autre règle, si possible.
- Rationalisez et optimisez votre base de règles existante : déterminez où vous pouvez mettre à jour vos règles pour réduire au minimum les proliférations et éliminer les conflits, et aussi pour vous assurer que l'application de la loi sur le trafic s'aligne sur l'intention de votre base de règles de politique de sécurité.

Analysez vos règles de politique de sécurité avant et après avoir validé vos modifications.

- Analyse des politiques préalable aux modifications : permet d'évaluer l'impact d'une nouvelle règle et d'analyser l'intention des nouvelles règles par rapport aux règles déjà existantes afin de recommander la meilleure façon d'y répondre.
- Analyse des politiques post-modification : permet de nettoyer la base de règles existante en identifiant les zones d'ombres, les redondances et autres anomalies accumulées au fil du temps.
 - L'Analyseur de politique nécessite le plug-in CloudConnector 1.1.0 ou une version ultérieure sur votre appareil Panorama. Vous devez activer ce plug-in à l'aide de la commande :

```
> request plugins cloudconnector enable basic
```

• L'Analyseur de politique nécessite que Panorama soit mis à jour vers PAN-OS version 10.2.3 ou une version ultérieure.

Types d'anomalies détectées par l'Analyseur de politique

L'Analyseur de politique détecte les types d'anomalies suivants dans votre base de règles de politique de sécurité :

• Ombres : règles qui ne sont pas respectées, car une règle située plus haut dans la base de règles couvre le même trafic.

Les règles de politique de sécurité sont évaluées dans la base de règles de haut en bas, de sorte que des ombres sont créées lorsqu'une règle située plus haut dans la base de règles correspond au même trafic qu'une règle située plus bas dans l'ordre et que les règles sont configurées avec une action différente. Si vous supprimez la règle située plus bas dans l'ordre, la politique de sécurité ne change pas.

- Redondances : deux règles ou plus qui correspondent au même trafic et sont configurées avec la même action.
- Généralisations : lorsqu'une règle située plus bas dans la base de règles correspond au trafic d'une règle située plus haut dans la base de règles, mais pas l'inverse, et que les règles effectuent une action différente. Si l'ordre des deux règles de politique est inversé, la politique de sécurité est impactée.
- Corrélations : règles qui sont en corrélation avec une autre règle lorsqu'une règle correspond à certains paquets de l'autre règle, mais entraîne une action différente. Si l'ordre des deux règles est inversé, la politique de sécurité est impactée.
- Consolidations : règles pouvant être consolidées en une seule règle, car l'action est la même et un seul attribut est différent. Vous pouvez fusionner les règles en une seule règle en modifiant les attributs de l'une des règles et en supprimant les autres.

Analyse des politiques préalable aux modifications

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
NGFW (Panorama géré)	ou
 (Panorama géré) 	Plug-in Panorama CloudConnector pour les déploiements Panorama gérés

L'analyse préalable aux modifications de la règle de politique de sécurité effectue l'analyse de satisfaction de la nouvelle intention :

• Analyse de la satisfaction des nouvelles intentions : vérifie si l'intention d'une nouvelle règle de politique de sécurité est déjà couverte par une règle existante.

Avant de commencer :

1. Accédez à Manage (Gérer) > Security Posture (Posture de sécurité) > Policy Analyzer (Analyseur de politique) > Pre-change Policy Analysis (Analyse de politique préalable aux modifications). **2.** En haut de la page Analyseur de politique, sélectionnez l'instance Panorama contenant les règles de politique que vous devez analyser.



3. Start a Security Policy Analysis (Démarrer une analyse de la politique de sécurité).

Pour démarrer une nouvelle analyse, procédez comme suit :

STEP 1 | Saisissez Analysis Name (Nom de l'analyse) et Analysis Description (Description de l'analyse).

IntentDemo Define the parameters of your new policy below. The Analysis Report shows you	u if any existing policies already cover	the intent.	
Step 1: General Information You can add a description to make it easier to locate the report later.			
Analysis Name	Analysis Description (Optional)		
IntentDemo	Placeholder		
Step 2: Specify Existing Security Policy Select as many as needed to include in your analysis.			
SELECT SECURITY POLICY		SELECTION SUMMARY	
Saarch		Panorama Instance:	panorama-e2e
Search		Security policy layer:	
Security Policy		Security Policies for Analysis	
panorama-e2e ∨			
Shared 🗸			
O NGFW-Legacy-FWs >			
Container-FWs >			

Sur un appareil Panorama, les groupes d'appareils sont hiérarchiques. Vous pouvez créer quatre niveaux de groupes d'appareils et vous pouvez attribuer des NGFW au groupe d'appareils au niveau le plus bas de la hiérarchie. La politique que vous créez à un niveau supérieur est ensuite héritée par tous les groupes d'appareils qui y sont inférieurs.

Vous pouvez exécuter l'analyse pour un maximum de 10 groupes d'appareils ayant des NGFW qui leur ont été directement attribués, ce qui vous permet d'analyser toutes les règles de politique transmises à cet ensemble de NGFW directement attribués.

STEP 2 | Sélectionnez un ensemble de politiques de sécurité existant à analyser.

Vous pouvez sélectionner un maximum de 10 groupes d'appareils par analyse.

STEP 3 | Spécifiez le type d'analyse en sélectionnant un ou plusieurs types d'analyse :

• Analyse de satisfaction des nouvelles intentions

Add New Security Rule Intent (Ajouter l'intention de la nouvelle règle de sécurité) pour analyse.

Step 3: Specify Analysis Select all of the analyses you'd like to run.		
 New Intent Satisfaction Analysis Check if new security rule intent is already satisfied by existing security rules. Add New Security Rule Intent 		
Security Policy Anomaly Analysis Check if existing Security Policy has Shadows/Redundancies or other anomalies.		
	Cancel Save As Draft	Submit Analysis Request

Spécifiez des informations sur la nouvelle règle de sécurité, et AIOps for NGFW peut vérifier si les règles existantes couvrent l'intention.

Policy Analyzer > New Analysis	New Security Rule Intent X Specify new security rule additions below, and AIOps can tell you whether the intent is already met w
IntentDemo	
Define the parameters of your new policy below. The Analysis Report shows you if any existing policies already cover the intent.	Basic Info ^
NGFW-Legacy-FWs > Container-FWs >	New Security Rule Name DemoRule1 New Security Rule Description (Optional)
	Placeholder
	Source ^
	Zones (Any Zone)
Step 3: Specify Analysis Select all of the analyses you'd like to run.	Addresses (Any Address)
	+ Address
New Intent Satisfaction Analysis Check if new security rule intent is already satisfied by existing security rules.	+ Address Group
+ Add New Security Rule Intent	+ Region
Security Policy Anomaly Analysis Check if existing Security Policy has Shadows/Redundancies or other anomalies.	Users (Any User)
	Destination

Saisissez les valeurs des composants d'une règle de politique de sécurité. La valeur par défaut des champs liés à une règle de sécurité est « Tout ».

Save (Enregistrer) les paramètres.

Consultez le résumé de l'intention de la nouvelle règle de sécurité.

IntentDemo Define the parameters of your new + Add New Security Rule Inter	bolicy below. The Analysis Report shows you if any exist	ting policies already cover the intent.		
SUMMARY OF NEW SPECIFI Security Rule	ED SECURITY RULE INTENT (1)			Action
 DemoRule1 Description: 		Applications:	Any	∕ [] 亩
Source Zones:	Any	Service Entities:	Any	
Source Addresse	s: Any	URLs:	Any	
Source Users:	Any	Action:	Deny	
Destination Zon	es: Any			
Destination Add	resses: Any			
Security Policy Anomaly Ana Check if existing Security Policy h	lysis s Shadows/Redundancies or other anomalies.			
			Canc	el Save As Draft Submit Analysis Request

Vous pouvez créer jusqu'à 10 nouvelles règles de sécurité ou copier une règle et la modifier.

STEP 4 | Submit Analysis Request or Save As Draft (Soumettre une requête d'analyse ou enregistrer en tant que brouillon) pour modifier la règle ultérieurement.

Affichez l'état d'une analyse sur la page Analyseur de politique sous Requêtes d'analyse.

Policy Analyzer	panorama-e2e							
Pre-Change Policy Analysis	Post-Change Policy Analysis							
Analysis Request	ts (17)							
Q Search	Analysis Type 🗙	Status × Y Add Filter					Res	set
Analysis Name	Description		Analysis Type	Submission Time	Operator	Status	End Time	
IntentDemo			Intent Satisfaction	Oct 10, 2022 06:50 AM		In Progress (71% complete)	Oct 10, 2022	:
			Intent Satisfaction	Oct 06, 2022 06:25 PM		Completed	Oct 06, 2022	:
			Intent Satisfaction	Oct 03, 2022 04:10 PM		Completed	Oct 03, 2022	:
			Intent Satisfaction	Oct 01, 2022 01:27 AM		Partially Completed	Oct 01, 2022	:
			Intent Satisfaction			() Draft	Oct 10, 2022	:
			Intent Satisfaction	Sep 28, 2022 07:44 PM		Partially Completed	Sep 28, 2022	:
			Intent Satisfaction	Sep 28, 2022 07:39 PM		Partially Completed	Sep 28, 2022	:
			Intent Satisfaction	Sep 28, 2022 06:26 PM		Partially Completed	Sep 28, 2022	:
			Intent Satisfaction	Sep 28, 2022 04:45 PM		Partially Completed	Sep 28, 2022	:
			Intent Satisfaction	Sep 28, 2022 05:42 AM		Partially Completed	Sep 28, 2022	:
						10 Rows ~ Page 1 ~	of 2 <	>

Vous pouvez annuler une règle dont l'état est En cours et elle sera affichée comme Annulée. Une fois l'analyse terminée, affichez le rapport d'analyse.

Rapports d'analyse de politique préalable aux modifications

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
NGFW (Panorama géré)(Panorama géré)	 ou Plug-in Panorama CloudConnector pour les
•	deploiements Panorama geres

Sélectionnez un rapport d'analyse dont l'état est terminé pour afficher les résultats de l'analyse de politique. Vous pouvez consulter les résultats de l'analyse.

Résultats de satisfaction de l'intention

Dans la liste des analyses sous Requêtes d'analyse, cliquez sur une analyse pour afficher ses résultats d'analyse. Ces résultats comprennent :

- 1. Un résumé de l'analyse avec des détails sur les groupes d'appareils et le nombre d'anomalies.
- **2.** Cliquez sur le nom d'un groupe d'appareils pour afficher le résultat de l'analyse de satisfaction de l'intention :
 - Intention entièrement atteinte : votre règle de sécurité est un doublon d'une des règles existantes dans le groupe d'appareils.
 - Intention partiellement atteinte : votre règle de sécurité répond partiellement à l'intention d'une des règles existantes du groupe d'appareils.
 - Intention non respectée : votre règle de sécurité est une règle unique qui n'est pas présente dans le groupe d'appareils. Vous pouvez ajouter cette règle au groupe d'appareils.



3. Affichez les résultats de l'analyse pour connaître l'intention de la nouvelle règle de sécurité.

Security Policy Analysis > new-demo-inte	nt-5		
Analysis Reports View your analysis results below			
Intent Satisfaction Results Securit	Policy Anomaly Results		
V DGL1		2	2 Security Policy Analysis found in DG1_1 1 Intent Fully Met 1 Intent Partially Met 0 Intent Not Met
DG1_1 Analysis Summary	Intent Type X Y Add Filter		Reset
# Security R	le Intent	Result	
1 intent rule		There are existing rules that fully meet your new r	rule intent, (and no higher order rules that contradict it)
2 Copy of int		⚠️ There are existing rules that partially meet your n	new rule intent but there are higher order rules that fully contradict it
2 Results			10 Rows > Page 1 > of1 < >
	Please selec	t a rule from the table above to view the details.	

Cet exemple comporte deux règles. L'intention de la première règle correspond pleinement aux règles existantes et l'intention de la deuxième règle correspond partiellement aux règles existantes.

4. Affichez les détails de la nouvelle règle de sécurité et vérifiez les résultats de la satisfaction de l'intention.

Capy of intent rule 1 Results 10 Rows ~ Page 10 Rows ~ P														
Results 10 Rows Page 1 of 1 0 Intern rule 1 4 CIFIED NEW SECURITY RULE Q Search Action X Adf Filter Resultation Zone Destination Zone Destination Address URL Category Application-Group1 Rule Name Action Source Zone Source Address Source User Destination Address URL Category Application-Group1 Intern Rule 1 © Allow Trusted Ipv6, Address, 169:254 Any Any 169:25 Any Application-Group1 Intern SattisFACTION RESULTS Intern Saturs X Adf Filter Reserve Reserve Reserve Reserve		Copy of intent rule 1	Copy of intent rule 1 A There ar			existing rules that p	artially meet your new ru	ile intent but ti	here are higher ord	er rules tha	t fully contra	adictit		
. intent rule 1 4 • There are existing rules that fully meet your new rule intent, (and no higher order rules that contradict in the rule of the the rules that contradict in the rule of	Results									10 Rows ~	Page		of 1 <	
Action X Add Filter Rule Name Action Source Zone Source Address Source User Destination Address URL Category Application Intent Rule 1 Allow Trusted Ipv6, Address, 169,254 Any Any 10 Rows > Page	. intent rule 1		4	1			There are	e existing rules that fully r	neet your new	rule intent, (and no	higher ord	er rules that	contradict i	t) ^
C Search Action X< T Add Filter	PECIFIED NEW SE	CURITY RULE												
Rule Name Action Source Zone Source Address Source User Destination Zone Destination Address URL Category Application Intent Rule 1 Allow Trusted Ipv6, Address, 169,254 Any Any 169,25 Any Application-Group 1 Intent Rule 1 Allow Trusted Ipv6, Address, 169,254 Any Any 169,25 Any Application-Group 1 Intent Rule 1 Allow Trusted Ipv6, Address, 169,254 Any Any 169,25 Any Application-Group 1 Intent Rule 1 Intent Rule 1 Intent Rule 1 Intent Rule 1 Intent Rule 1 Any Any 169,25 Any Application-Group 1 Intent Rule 1 Intent Rule 1 Intent Rule 1 Intent Rule 1 Intent Rule 1 Intent Rule 1 Any Any Any 169,25 Any Application-Group 1 Intent Rule 1	Q Search		Action ×	▼ Add Filter										eset
Intert Rule 1 Image: Allow Trusted Ipv6, Address, 169,254 Any Any 169,25 Any Application-Group1 10 Rows > Page 1 > of 1 Image: Compare 1 of 1 Image: Compare 1 of 1 Image: Compare 1 NTENT SATISFACTION RESULTS Status X T Add Filter Real Name Satisfaction Status Policy Layer Action Source Zone Source User Destination Zone Destination Zone	Rule Name	Action	Source	Zone	Source Address	Source User	Destination 2	Zone Destinat	ion Address	URL Categor	/	Applica	tion	
10 Rows v Page 1 v of 1 <	Intent Pule 1	Aller:	Truster		Ipv6, Address, 169.254	Any	Any	169.25		Any		Applicat	ion-Group1	
Status X Y Add Filter Re Rule Name Satisfaction Status Policy Layer Action Source Zone Source User Destination Zone Destinatination Zone <	Intent Kule 1	Allow	Irusted											
Rule Name Satisfaction Status Policy Layer Action Source Zone Source Address Source User Destination Zone Dest	NTENT SATISFACT	ON RESULTS	Irüsted							10 Rows ~	Page	1 × of :		
	NTENT SATISFACT	ON RESULTS	Status ×	▼ Add Filter						10 Rows >	Page	1 × of 1		> eset
Shared Rule 1 🗸 Meets New Security Rule Intent Shared 🕐 Allow Any Any Any Any Any Any	NTENT SATISFACT Q Search Rule Name	ION RESULTS Satisfaction Status	Status X	▼ Add Filter Policy Laye	r Action	Source	e Zone	Source Address	Source	10 Rows V	Page Destinat	1 V of 1	L < R Dest	> eset ination
1 Results 10 Rows V Page 1 V of 1 C	NTENT SATISFACT Q Search Rule Name Shared Rule 1	CN RESULTS Satisfaction Status	Status X	▼ Add Filter Policy Laye Shared	r Action	Source	e Zone	Source Address Any	Source I Any	10 Rows V	Page Destinati	1 V of 1	L < Ri Dest	> eset ination

Dans cet exemple, tous les attributs de la nouvelle règle, la règle d'intention 1 correspondent aux attributs de la règle existante, la règle partagée 1. L'intention de la nouvelle règle correspond pleinement à celle de la règle existante. Par conséquent, vous n'avez pas besoin d'ajouter cette nouvelle règle à la configuration.

Analyse de politique post-modification

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
NGFW (Panorama géré)(Panorama géré)	 ou Plug-in Panorama CloudConnector pour les
•	déploiements Panorama gérés

Lorsque vous validez une configuration sur Panorama, celle-ci est disponible pour analyse via le plug-in à Strata Cloud Manager. Policy Analyzer analyse cette configuration pour détecter les ombres, les redondances et autres anomalies, et les résultats sont disponibles pour examen dans Manage (Gérer) > Security Posture (Posture de sécurité) > Policy Analyzer (Analyseur de politique) > Post-change Policy Analysis (Analyse de politique post-modification).

Vous pouvez consulter les informations suivantes :

 Affiche le résumé de l'analyse dans tous les ensembles de politiques, c'est-à-dire tous les groupes d'appareils avec des NGFW qui leur sont directement attribués. Vous pouvez afficher les anomalies ou les anomalies en fonction de la priorité élevée. Les valeurs indiquées dans ce rapport montrent le nombre unique d'anomalies trouvées dans tous les groupes d'appareils. Les couleurs du graphique indiquent les différents types d'anomalies.

Policy Analyzer	panorama-e2e ×				
Pre-Change Policy Analysis Post-Cha	nge Policy Analysis				
Policy Analysis Summar	y 1			2	Priority High All
287 total anomalies found	287	O Shadows S4 Redundancies O Ceneralizations 139 Correlations 94 Consolidations	Existing Security Policy Snapshot Tim Analysis Start Time: Completion Time: Analysis Runtime:	*	Sep 30, 2022 09:51 PM Sep 30, 2022 09:51 PM Sep 30, 2022 10:21 PM 30 minutes 20 seconds

- 2. Horodatages pour l'analyse qui comprend :
 - Instantané de politique de sécurité existante : horodatage lorsque la configuration a été marquée comme étant exécutée dans Panorama après une validation.
 - Analyse de temps commencée
 - Analyse de temps terminée
 - Temps nécessaire pour terminer l'analyse
- **3.** Affichez l'état de la politique de sécurité et le nombre d'anomalies pour chaque politique.
- **4.** Affichez une ventilation des anomalies d'une politique de sécurité sélectionnée.

5. Affichez les détails des anomalies pour chaque règle d'une politique de sécurité.

Policy Analyz	er panorama-e2e ×			
Pre-Change Policy Ana	alysis Post-Change Policy Analysis			
Policy Analy	/sis 3			
Status	Security Policy 1	Anomaly Count 1	Anomalies in BND LAN 🔶 🗸	
Q Search				
			115 Security Policy Anomalies found in BND LAN	
	BND LAN		😢 0 Shadows	
		44	115 8 1 Redundancies	
			▲ 0 Generalizations	
		30	107 Correlations	
		17	▲ 7 Consolidations	
		45		
Anomaly De	etails in BND LAN 🔶 5	5		
Q Search	Anomaly Type × Y Add			Reset
*	Security Policy Rule		Security Policy Anomaly	
			8 Redundancy: Allow security rule is covered by a higher order allow security rule	
			A Correlation: Block security rule is correlated with higher order allow security rule	
			▲ Correlation: Block security rule is correlated with higher order allow security rule	
			▲ Correlation: Block security rule is correlated with higher order allow security rule	

6. Affichez les attributs d'une règle sélectionnée et les détails de l'anomalie.

hange Policy Analys	is Post-Change Poli	Post-Change Policy Analysis BND Correlation: Block security rule is correlated with hisher order allow security rule								
<u> </u>			Correlation: Block security rule is correlated with higher order allow security rule							
.0					E BIOCK SECURITY FUILE IS CORN	elated with higher order all	ow security rule			
15 Results							10 Rows V Page	1 ~ of 12		
. BND	-	- 6				8 Redundancy: Allow :	ecurity rule is covered by a high	er order allow securi	ty rule 🔨	
Q Search		Action × Y Add Filter							Reset	
Rule Type	Rule Name	Location	Action	Source Zone	Source Address	Source User	Destination Zone	Destination Ad	ldress	
Covering Rule	BND		Allow	BND-Lan, Untrust	BND	Any	Untrust			
Covered Rule	BND Users		😒 Allow	BND-Lan	BND	Any	Untrust	10.		
							10 Rows V Page	1 × of 1 <		
Suggested N Option 1: If you want Remove the covered	lext Steps ^ <	red rule to be allowed with	same security inspection	as covering rule then the	covered rule is redund	ant. Consider following	changes:			
Option 2: If you want Change the security	ted traffic matching cover / profile field in the cover- ule to a higher order thar	red rule to have a different ed rule to reflect the inspec o the covering rule	security inspection versu tions of interest	us traffic matching the cov	vering rule then conside	r following changes:				
iviove the covered r										

Cette image illustre un exemple de l'anomalie de redondance. Dans cet exemple, la règle BND est déjà couverte par une autre règle d'utilisateurs BND. Par conséquent, la règle BND peut être supprimée.

7. Consultez les étapes suivantes proposées pour corriger une anomalie.

TECH**DOCS**

État et gestion logicielle des NGFW

Ce chapitre décrit la manière de gérer l'état de santé et les mises à niveau logicielles du NGFW.

- Afficher l'état de santé du périphérique Affichez l'état de santé cumulé et les performances de votre déploiement en fonction des scores de santé des NGFW intégrés.
- Recommandations de mise à niveau Créez des recommandations pour déterminer la meilleure version du logiciel de vos périphériques pouvant être mis à niveau.
- Analyser la capacité métrique Analysez et surveillez la capacité des ressources de vos périphériques en suivant leur utilisation des métriques en fonction de leurs types de modèles.

Voir Santé du périphérique

De quoi ai-je besoin ?
L'une des options suivantes :
ou

Le tableau de bord **Device Health (État de santé du périphérique)** vous montre l'état de santé cumulatif et les performances de votre déploiement en fonction des scores de santé des NGFW embarqués. L'état de santé du périphérique est déterminé par la gravité du score de santé (0-100) et son niveau de santé correspondant (bon, passable, mauvais, critique). Le score de santé est calculé sur la base de la priorité, de la quantité, du type et de l'état des alertes ouvertes.

Ce tableau de bord vous permet de :

- comprendre les améliorations apportées au déploiement sur une période donnée en examinant les données historiques du score de santé.
- répertorier les périphériques qui nécessitent une attention particulière dans votre déploiement et prioriser les problèmes en vue de les résoudre.



Pour plus d'informations, voir Tableau de bord : État de santé du périphérique.
NGFW logiciels

Obtenez des recommandations de mise à niveau

Où puis-je utiliser ceci ?De quoi ai-je besoin ?• , y compris ceux financés par les créditsI ou

Sélectionnez Workflows (Flux de travail) > Software Upgrades (Mises à niveau de logiciel) > Upgrade Recommendations (Recommandations de mise à niveau) pour utiliser Strata Cloud Manager afin d'analyser les fonctionnalités activées sur vos pare-feu et de créer une recommandation personnalisée qui fournit des informations spécifiques pour votre réseau :

- La meilleure version du logiciel à exécuter sur vos périphériques.
- Informations sur les nouvelles fonctionnalités, les changements de comportement, les vulnérabilités et les problèmes logiciels dans chaque version logicielle recommandée.

Types de recommandations de mise à niveau :

- Recommandations générées par le système à partir des données de télémétrie du périphérique deux fois par semaine.
- Recommandations personnalisées générées par l'utilisateur lorsque vous sélectionnez des périphériques pour des CVE PAN-OS spécifiques.
- Recommandations générées par l'utilisateur que vous générez en chargeant un fichier de support technique (TSF) d'un pare-feu.

NGFW - Software Upgrade Recommendations									
Creation Date: Past 7 Days X	▼ Add Filter					Reset			
Upgrade Recommendations Generate On Demand Upgrade Recommendations									
Creation Date 🔸	Recommendations Name 11		Number o 👔	Must Fix Vulner 1	Recommendatio 1	Status 🛔			
Dec 17, 2023, 3:30:	PAN-OS: 10.2 Platform: vm	1		N/A	System	🥪 Ready			
Dec 17, 2023, 3:30:	PAN-OS: 10.1 Platform: 220	r		N/A	System	🤣 Ready			
Dec 17, 2023, 3:30:	PAN-OS: 10.1 Platform: vm	1		N/A	System	🤣 Ready			
Dec 17, 2023, 3:30:	PAN-OS: 11.0 Platform: pc	r		N/A	System	🤣 Ready			
Dec 17, 2023, 3:30:	PAN-OS: 11.0 Platform: vm	r		N/A	System	🤣 Ready			
Dec 15, 2023, 1:44:	Custom Recommendations: PA-VM	r		CVE-2023-6790		🥪 Ready			
Dec 15, 2023, 5:17:	Custom Recommendations	r		CVE-2021-44228		🤣 Ready			
Dec 15, 2023, 5:17:	Custom Recommendations	r		CVE-2021-44228		🤣 Ready			
Dec 14, 2023, 8:20:	Custom Recommendations	1		CVE-2021-44228		🤣 Ready			
Dec 14, 2023, 7:34:	Custom Recommendations	1		CVE-2021-44228		🤜 Ready			
Dec 14, 2023, 10:49	Custom Recommendations	1		CVE-2022-0778		🤜 Ready			
Dec 14, 2023, 6:54:	Custom Recommendations	1		CVE-2022-0778	and the second sec	🤜 Ready			
Dec 13, 2023, 3:30:	PAN-OS: 10.1 Platform: vm	1		N/A	System	🤜 Ready			
Dec 13, 2023, 3:30:	PAN-OS: 10.2 Platform: vm	1		N/A	System	🤜 Ready			

Vous pouvez effectuer les tâches suivantes pour chaque recommandation.

• Affichez le nombre de périphériques nécessitant une mise à niveau et les vulnérabilités à corriger.

- Modifiez le nom d'une recommandation pour faire la distinction entre les recommandations personnalisées.
- Filtrez les recommandations par date de création, nom des recommandations et recommandations générées par.
- Supprimez les recommandations qui ont échoué ou qui ne sont plus appropriées.

Générer des recommandations de mise à niveau à la demande

- 1. Generate On Demand Upgrade Recommendations (Générez des recommandations de mise à niveau à la demande).
- 2. Select (Sélectionnez) un fichier de support technique (TSF) et Upload (Chargez) le.
 - Vous pouvez charger le TSF d'un seul périphérique à la fois et le TSF doit être au format .tgz.
 - Vous pouvez générer des recommandations de mise à niveau logicielle uniquement à partir d'un TSF que vous générez et chargez à partir d'un pare-feu exécutant la version PAN-OS 9.1 ou une version ultérieure.

NGFW - Software Upgrade Recommendations										
Creation Date: Past 7 Days X Y Add Filter										
Upgrade Recommend	Upgrade Recommendations Generate On Demand Upgrade Recommendations									
Creation Date 🔸	Recommendations N				Number o 👔	Must Fix Vulner 🛔	Recommendatio _{↓†}			
Dec 17, 2023, 3:30:			ľ				System	< Ready		
Dec 17, 2023, 3:30:		Upload Tech Support File (TSF)	×				System	< Ready		
Dec 17, 2023, 3:30:		Upload Tech Support File 📝 to generate an Upgrade	p				System	< Ready		
Dec 17, 2023, 3:30:		Recommendations.	8				System	🖌 Ready		
Dec 17, 2023, 3:30:		Note: Only for PAN-OS 9.1 or above devices.	p				System	< Ready		
Dec 15, 2023, 1:44:		NGFW or Panorama TSF	P					< Ready		
Dec 15, 2023, 5:17:		Select						< Ready		
Dec 15, 2023, 5:17:		File type: .tgz	8					< Ready		
Dec 14, 2023, 8:20:		Note: TSF uploads disabled Cancel	pload					< Ready		
Dec 14, 2023, 7:34:		for demo.	piouu					< Ready		
Dec 14, 2023, 10:49			ľ					< Ready		
Dec 14, 2023, 6:54:			P					Ready		
Dec 13, 2023, 3:30:			ľ				System	🖌 Ready		
Dec 13, 2023, 3:30:			ľ				System	Ready		

3. Affichez les recommandations de mise à niveau logicielle une fois que l'état devient Prêt.

Vous pouvez également consulter l'état pour voir s'il y a des erreurs liées au chargement, au format de fichier ou au traitement du fichier TSF.

Afficher le rapport sur les recommandations de mise à niveau logicielle

Cliquez sur une recommandation pour afficher le rapport détaillé avec les options de mise à niveau de vos périphériques. Sélectionnez une option de mise à niveau pour afficher les détails concernant **New Features (Nouvelles fonctionnalités)**, **Changes of Behavior (Changements**

de comportement), Vulnerabilities Based on Enabled Features (Vulnérabilités basées sur des fonctionnalités activées) et PAN-OS Known Issues (Problèmes de PAN-OS connus). Vous pouvez également Export (Exporter) ce rapport au format CSV.



- Le rapport de recommandation inclut des informations spécifiques aux fonctionnalités activées sur vos périphériques.
- Pour **PAN-OS Known Issues (Problèmes de PAN-OS connus)**, le nombre de cas associés représente le nombre de clients ayant signalé le problème.

NGFW - Software Upgrade Recommendations								
PAN-05:10.2 Platform: vm ≠ Dec 17,2023								
	This report is tablered to the PAN-CG features enabled or 21 devices. Choose a major version below to see further details about new features. Vulnerabilities Based on Enabled Features, and PAN-CG Known issues related to this upgrade.							
	Upgrade Option 1 - PAN-OS 10.2	Upgrade Option 2 - PAN-OS 11.0						
	haget Wender, 1927 Researcher, Neuer, 2023 Die Cherkense, Aug 27, 2023 Die Cherkensen, Neuer Neuer Anderense, Olicher Ausseller All Wannenschlicher, Olich kensten Eff Researcherer, Schlich kenster, Eff	Toget Weeker 11.02-32 Relate Data Social 2003 Ref Data New 1977 2004 The Performant Week New Foreness 28 Placet Automatiking 01: A Markanathing 01: Child A sides Cf Resemblisher 77 Nation Nation Cf						
Upgrade Option 2 - PAN OS 11.0 New Features (28) Changes of Behavior (1) Vuberabilities Based	on Enabled Features PNN-OS Known Issues (77)			🔓 Expert				
Y Add Filter				Reset				
Feature Group II Feature II	Detail II			Release Introduced II				
Networking Features Web Proxy	Some networks are designed around a proxy for complia	nce and other requirements. The Web Proxy capability available in PAN-C	05 11.0 allows these customers to	11.0				
	migrate to NGPW without changing their proxy network Also Networks helps you transition to a single, integrate	to secure web as well as non-web traffic. With web proxy available for b I security stack for web security across on-premises and cloud-delivered	oth NGFW and Prisma Access, Palo form factors. By configuring					

Analyser la capacité métrique

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
•	ou

Depuis Strata Cloud Manager, accédez à **Monitor (Surveiller)** > **Capacity Analyzer (Analyseur de capacité)**pour analyser et surveiller la capacité des ressources de vos périphériques en suivant l'utilisation de leurs métriques en fonction de leurs types de modèles. Vous pouvez analyser les métriques à l'aide des méthodes suivantes :

- Analyser la capacité métrique en fonction de la métrique, du modèle et du périphérique
- Analyser la capacité métrique en fonction des modèles de périphériques
- Analyser la capacité métrique en fonction des métriques

L'analyseur de capacité est amélioré pour prendre en charge les alertes qui vous aident à anticiper la consommation des ressources qui approche de leur capacité maximale et à déclencher des alertes. Voir Gérer les alertes de l'analyseur de capacité.



La fonctionnalité **Capacity Analyzer (Analyseur de capacité)** n'est pas prise en charge pour les pare-feu VM Series.

Analyser la capacité métrique en fonction de la métrique, du modèle et du périphérique

1. Sur la carte thermique de l'analyseur de capacité, faites passer votre curseur sur une cellule pour afficher l'utilisation de la capacité métrique de tous les périphériques appartenant au modèle de périphérique correspondant.

Dans cet exemple, la fenêtre contextuelle affiche la capacité métrique de **ARP table size (Taille de la table ARP)** pour tous les périphériques appartenant au modèle **PA-220**.



2. Cliquez sur une cellule correspondant au modèle de périphérique et à la métrique pour vérifier l'utilisation de la capacité. Dans cet exemple, nous cliquons sur la taille de la table ARP pour le modèle de périphérique **PA-220**.

Capacity	Analyzer Heat-map 🖒 C	apacity Analyzer Trend	d			
Capa	acity Analyze	er 🚯				
Time: P	Past 30 Days Y	diction Time: Next 90	Days ~			
Met	ric ARP table size o	on device Afin_B	eijing_220	_1 [PA-220]		
			1.5 K (98	%)		
100	MAX CAPACITY(1	.5 K)				
75	5%					
50	0%					
25	5%					
(0% 10/15 10/22	10/29 11/05	11/12	11/19	11/26 12/03	12/10 12 Month/D
ARP	table size on all P	A-220				
	Host Name 🗍	Amount Used 🕌			Amou _{I1}	Alert Name 🛔
O	Afin_Beijing_220	1.5 K (99%)			19.0 (1%)	Approaching M
С	Afin_Munich_220	1.4 K (93%)			111.0 (7%)	Approaching M
С	Afin_Boston_220	1.4 K (92%)			126.0 (8%)	Approaching M
С	Afin_Munich_220	1.4 K (91%)			131.0 (9%)	Approaching M

Vous pouvez consulter les éléments suivants :

- Capacité métrique de taille de table ARP pour tous les périphériques appartenant au modèle **PA-220**.
- Sélectionnez l'un des noms d'hôte pour afficher la tendance de la capacité métrique.
- Les alertes déclenchées pour la métrique et la date à laquelle il est prévu que la métrique atteindra sa capacité maximale.
- Tendance prévue pour la métrique. Strata Cloud Manager prévoit la date à laquelle la métrique atteindra la capacité maximale. Vous pouvez faire passer votre curseur sur le graphique pour vérifier la capacité métrique à un moment précis.

Analyser la capacité métrique en fonction des modèles de périphériques

1. Dans la carte thermique de l'analyseur de capacité, sélectionnez un modèle de périphérique pour afficher toutes ses métriques associées.

Capacity Analyzer										
Metric: All	Mo	del Type: A	JI ~							
Capacity (Capacity Overview for All Metrics on All Models									
					Capacity F	0% ilter 0%				
	Configuration	on Resource	_							
PA-220										
PA-3260										
PA-5220										
PA-5250										
PA-820										
	ARP tab	GlobalP	GlobalP	IPSec VPN		Objects				
h	table site	Jientless	ect tumes	HEPeers Jo	N Tunnels Addre	55 Objects Ad	nes croups FOL	NA Address Servit	e objects servi	Le Groups
	Globalt	Glop.								

Capacity Analyzer Heat-map 🗲 Capacity Analyzer Table							
Capacity Analyzer 🛛							
Metric: All ~ Model Type: PA-220 ~							
PA-220 (Each row displays a metric's utili	zed and unutilized capacity, indicating the number	of resources used and unus					
 Configuration Resource 							
Metric Name 👔	Amount Used 👔	Alert Name 🔐					
Address Objects	2.5 K (99%)	Approaching Max					
Address Groups	123.0 (98%)	Approaching Max					
ARP table size	1.5 K (99%)	Approaching Max					
FQDN Address	1.9 K (96%)	Approaching Max					
Global Protect Clientless Tunnels	19.0 (95%)	Approaching Max					
Global Protect Tunnels	242.0 (97%)	Approaching Max					
IKE Peers	984.0 (98%)	Approaching Max					
VPN Tunnels	973.0 (97%)	Approaching Max					
NAT policies	384.0 (96%)	Approaching Max					
Security Policies	493.0 (99%)	Approaching Max					
Service Objects	989.0 (99%)	Approaching Max					
Service Groups	247.0 (99%)	Approaching Max					
✓ System Resource							
Metric Name 🕌	Amount Used 🕌	Alert Name 📊					

Chaque ligne affiche la capacité utilisée d'une métrique, indiquant le nombre de ressources utilisées pour cette métrique dans un périphérique. De plus, vous pouvez afficher les alertes déclenchées pour la métrique et la date à laquelle il est prévu que la métrique atteindra sa capacité maximale.

2. Dans le tableau Analyseur de capacité, sélectionnez une métrique pour afficher sa tendance sur un périphérique.

3. Sélectionnez un périphérique pour afficher la tendance de métrique correspondante.

Vous pouvez sélectionner l'**heure de prédiction** pour vérifier la tendance prévue pour la métrique. Strata Cloud Manager prévoit la date à laquelle la métrique atteindra la capacité maximale.

Vous pouvez faire passer votre curseur sur le graphique pour vérifier la capacité métrique à un moment précis.



Sous **Nom de l'alerte**, vous pouvez afficher les alertes déclenchées pour la métrique d'objets d'adresse correspondant à un nom d'hôte.

Analyser la capacité métrique en fonction des métriques

1. Dans la carte thermique de l'analyseur de capacité, sélectionnez une métrique pour afficher sa capacité dans tous les périphériques sous forme de tableau. Dans cet exemple, la métrique de la taille de la table ARP est sélectionnée.



Vous pouvez également sélectionner un type de métrique et explorer une métrique pour afficher sa capacité dans tous les périphériques dans un format tabulaire. Par exemple, **Configuration Resource (Ressource de configuration)** saisir la métrique > **Objects (Objets)** > **Address Objects (Objets d'adresse)**.

Capacity	/ Ana	lyzer	i							
Metric: All	Mo	del Type: A	All ~							
Capacity (Overvie	w for All	Metrics	on All N	Aodels					
					Capacity F	09 Filter 09	6			
					Capacity					
	Configurati	on Resource								
PA-220										
PA-3260										
PA-5220										
PA-5250										
PA-820										
	ARP tab	GlobalP	GlobalP	IPSec VPN		Objects				
ARPE	able site	tientes. a Prot	ectTunnets	WE Peers	APH TUNNELS Add	Res Objects Ad	ues Goups FO	Jth Address servi	ce ^{Objects} seri	ice Groups
	GlobalP	Clop								

Capacity Analyzer Heat-map 🗲 Capacity Analyzer Table											
Capacity Analyzer											
Metric: Configuration Resource / ARP	t Y Model Type: All										
ARP table size											
✓ PA-220											
Host Name 👔	Amount Used _{J1}	Amount Unused 👔	Aler								
Afin_Beijing_220_1	1.5 K (99%)	19.0 (1%)	Аррг								
Afin_Munich_220_6	1.4 K (93%)	111.0 (7%)	Appr								
Afin_Boston_220_11	1.4 K (92%)	126.0 (8%)	Appr								
Afin_Munich_220_3	1.4 K (91%)	131.0 (9%)	Appr								
Afin_Boston_220_6	1.3 K (89%)	171.0 (11%)	Appr								
Afin_Boston_220_9	1.3 K (88%)	177.0 (12%)	Appr								
Afin_Beijing_220_2	1.3 K (84%)	247.0 (16%)	Appr								
Afin_Boston_220_4	1.2 K (83%)	259.0 (17%)	Appr								
Afin_Munich_220_4	1.2 K (81%)	282.0 (19%)									
Afin_Boston_220_0	1.2 K (81%)	290.0 (19%)									
Afin_Boston_220_5	1.2 K (80%)	301.0 (20%)	Appr								
Afin_Boston_220_2	1.2 K (79%)	311.0 (21%)	Appr								
Afin_Boston_220_1	1.2 K (79%)	316.0 (21%)	Appr								
Afin_Boston_220_10	1.1 K (73%)	407.0 (27%)									

Chaque ligne affiche les métriques de la **taille de table ARP** utilisées et inutilisées pour chaque hôte sous les modèles de périphériques. En outre, vous pouvez afficher les alertes déclenchées pour cette métrique pour chaque hôte et la date à laquelle il est prévu que la métrique atteindra sa capacité maximale.

2. Sélectionnez un nom d'hôte pour afficher la tendance graphique de la métrique sélectionnée.

Vous pouvez sélectionner l'**heure de prédiction** pour vérifier la tendance prévue pour la métrique. Strata Cloud Manager prévoit la date à laquelle la métrique atteindra la capacité maximale.

Capacity	Analyzer Heat-map 🗲 C	apacity Analyzer	Table 🗲 Capa	city Analyzer Tren	d	
Capa	icity Analyze	r 🚯				
Time: P	ast 30 Days Y	liction Time: Nex	t 90 Days 💙			
Metr	ic ARP table size o	n device Afir	_Boston_2	220_11 [PA-2	20]	
100	MAX CAPACITY(1.	5 K)	1.4 K (9	1%)		
75 50 25	5% 5% 5%					
c	^{0%} 10/15 10/22	10/29 11	/05 11/:	12 11/19	11/26 12/03	^{12/10} Month/[
All M	letrics on Afin_Bos	ton_220_11	, Unknown	1		
	Metric Name 🛯 🛔	Amount Used	1t		Amou _{I†}	Alert Name
С	IKE Peers	937.0 (94%)			63.0 (6%)	Approaching N
С	Security Policies	463.0 (93%)		-	37.0 (7%)	Approaching N
0	ARP table size	1.4 K (92%)			126.0 (8%)	Approaching N
С	FQDN Address	1.8 K (91%)			190.0 (10%)	Approaching N

Vous pouvez faire passer votre curseur sur le graphique pour vérifier la capacité métrique à un moment précis.

TECH**DOCS**

Meilleures pratiques dans les NGFW

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
 , y compris ceux financés par les crédits	L'une des options suivantes :
NGFW logiciels	ou ou ou

AlOps pour NGFW vous aide à renforcer la posture de sécurité en vous alignant sur les meilleures pratiques. Vous pouvez tirer parti d'AlOps pour NGFW pour évaluer vos configurations de sécurité Panorama, NGFW et Prisma Access Panorama géré par rapport aux meilleures pratiques et remédier aux vérifications des meilleures pratiques qui ont échoué. AlOps pour NGFW simplifie le processus de vérification de la conformité InfoSec sur votre infrastructure réseau.

AlOps pour NGFW est gratuit, et les fonctionnalités d'évaluation des meilleures pratiques (BPA) d'AlOps suivantes sont disponibles sans licence AlOps Premium. Pour obtenir la liste complète des fonctionnalités des meilleures pratiques disponibles, voir Meilleures pratiques intégrées :

• Consultez le Tableau de bord des meilleures pratiques pour les rapports quotidiens sur les meilleures pratiques, et leur mappage sur les vérifications des contrôles de sécurité critiques (CSC) du Center for Internet Security. Ces rapports vous aident à identifier les domaines dans lesquels vous pouvez apporter des modifications pour améliorer votre conformité

aux meilleures pratiques. Partagez le rapport sur les meilleures pratiques au format PDF et programmez-le pour qu'il soit régulièrement livré dans votre boîte de messagerie.

Dashboards			
* Threat Insights My Dashboard Compliance Summary Best I	Practices On Demand BPA NGFW Feature Adoptio	on CDSS Adoption WildFire	+ More Dashboards V
Summary Security Identity Network Service Se	etup		土 🖻 🛱
Device Group: All	Category: Rule 💙 Checks: CSC Checks Only 💙	CLI Remediations: All Checks Y	Reset
PA-3260 Serial Number: 016401004839 Model: PA-3260 SW Version: 11.0.0-c2 IP Address: 10			
Summary of Failed Checks			
Review the security rules, profiles, and rulebases failing best practices checks (including Criti (CSC) checks) for each configuration type: Security, Network, Identity, and Service Setup.		Security Identity) Network O Service Setup
Rules	Profiles	Rulebases	
55 Fraud	25 Failed	4 Failed)
Failed CSC checks 8	Failed CSC checks 15	Failed CSC checks	2
Failed non-CSC checks S	Failed non-CSC checks 0	Failed non-CSC checks	0
Falled USC and hon-USC checks 42	Failed CSC and non-CSC crecks 10	Failed LSC and non-CSC checks	2
Unique Failed Checks 11	Unique Failed Checks 19	Unique Failed Checks	6
Best Practice Checks Trending			ime Range: Past 30 days 🗸
	Percentage April 30th 2	e of Checks Passing	
	• 78% id	lentity 22% Not Passed	
60%	• 59% Se	ecurity 41% Not Passed	
40%	• 56% N	etwork 44% Not Passed	
20%	• 34% Se	ervice Setup 66% Not Passed	
0% 16 17 18 19 20 21 22 23 24 APR	4 25 26 27 28 29 30 1 2 MAY	3 4 5 6 7 8 9 10 11 12	13 14 15
	Security Identity Network S		

• Surveillez l'adoption des fonctionnalités et restez au courant des fonctionnalités de sécurité que vous utilisez dans votre déploiement et des lacunes potentielles dans la couverture.



• Recevez des alertes sur la posture de sécurité d'AlOps pour NGFW pour savoir quand vos paramètres de sécurité peuvent nécessiter un examen plus approfondi.

Les corrections Command Line Interface (interface de ligne de commande - CLI) sont également disponibles dans AIOps pour NGFW sous **Alerts (Alertes)** > **Security (Sécurité)** > **Alert Details (Détails de l'alerte)**. Consultez les recommandations destinées à vous aider à corriger les problèmes qui déclenchent une alerte.

Alerts > Alert De					
Applicatio	on Not Set In Rule - Panorama				
Serial Number:	Model: Panorama SW Version: IP Address:				
Application		Rule Name			
✓ Any		Rule2-dg-1			
	RECOMMENDATIONS				
	۶ Follow these steps to resolve the issue:				
	To enable Ago ID remove any from application list for security rule Rule2-dg- 1 configured at device-group test-dg-1 pre-rulebase				
	Run all of the following CLI command sets:				
	delete device-aroup test-da-1 pre-rulebase security rules RuleZ-da-1 application				
	set device-group test-dg-1 pre-rulebase security rules Rule	2-dg-1 application			
✓ Any		sr_bpa_11			
	RECOMMENDATIONS				
	Follow these steps to resolve the issue: مر				
	To enable App ID remove any from application list for security rule				
	sr_bpa_11 configured at device-group test-dg-1 pre-rulebase				
	Run all of the following CLI command sets:				
	delete device-group test-dg-1 pre-rulebase security rules s set device-group test-dg-1 pre-rulebase security rules sr_b	r_bpa_11 application pa_11 application			

- Les alertes de sécurité et les corrections CLI sont disponibles uniquement pour les périphériques partageant la télémétrie. Cette fonctionnalité ne prend pas en charge le chargement manuel du fichier de support technique (TSF) pour les périphériques PAN-OS exécutant les versions 9.1 et supérieures.
- Générez des rapports BPA pour les périphériques PAN-OS (non télémétriques) exécutant les versions 9.1 et supérieures, qui incluent désormais des métriques d'adoption de fonctionnalités. Si vous avez utilisé l'outil autonome BPA pour générer des rapports BPA, vous

pourriez vous demander « Puis-je toujours générer des rapports BPA à partir du portail de support client ? » Nous nous occupons également de cela.

On-Demand BPA & Adoption Assess your security posture for devices not sending telemetry against Palo Alto Networks' best practice guidance. Best practices include checks for the Center for Internet Security's Critical Security Controls (CSC). Take action based on the findings here to optimize your security posture.								
								Reset Filte
Reports Com	pleted (14) In-Pr	ogress (2) Failed (2)					Collapse All	Generate New Reports
 Completed (14) 	4)							
Best Practices	Adoption Summary	Reports Generated Date 🛛 🕹	User Name 41	Hostname It	Model 41	PAN-OS Version It	TSF Name 태	TSF Generated Date 41
		15 Aug 2022 at 01:01:01	user_xyz	AMS-FW-2187	PA-5220	10.1.2	TSF_2187	15 Aug 2022 at 01:01:01
		14 Aug 2022 at 01:01:01	user_xyz	TOK-FW-7365	PA-5220	10.1.2	TSF_7365	13 Aug 2022 at 01:01:01
		14 Aug 2022 at 01:01:01	user_xyz	TOK-FW-7365	PA-5220	10.1.2	TSF_7365	13 Aug 2022 at 01:01:01
		14 Aug 2022 at 01:01:01	user_xyz	TOK-FW-7365	PA-5220	10.1.2	TSF_7365	13 Aug 2022 at 01:01:01
		13 Aug 2022 at 01:01:01	user_xyz	TOK-FW-7365	PA-5220	10.1.2	TSF_7365	13 Aug 2022 at 01:01:01
		13 Aug 2022 at 01:01:01	user_xyz	TOK-FW-7365	PA-5220	10.1.2	TSF_7365	13 Aug 2022 at 01:01:01
		13 Aug 2022 at 01:01:01	user_xyz	TOK-FW-7365	PA-5220	10.1.2	TSF_7365	13 Aug 2022 at 01:01:01
 In-Progress (4) 								
	Date Uploaded 🛛 🕹	User Name It				TSF Name If Pro	gress	
	16 Aug 2022 at 01:01	:01 user_xyz				TSF_1658	Uploading TSF file	- 75% uploaded
	16 Aug 2022 at 01:01	:01 user_xyz				TSF_1658	Processing TSF file	- 75% complete
	16 Aug 2022 at 01:01	:01 user_xyz				TSF_1658	Processing TSF file	- 55% complete
	16 Aug 2022 at 01:01	:01 user_xyz				TSF_1658	Processing TSF file	- 43% complete
 Failed (2) 								
	Date Uploaded 🔸	User Name 41 F	lostname 41 N	Nodel It PAN-O	S Version 1	TSF Name 41 TSF	Generated Date	Actions
	15 Aug 2022 at 01:01	:01 user_xyz A	MS-FW-2187 P	PA-5220 10.1.2		TSF_2187 15	Aug 2022 at 01:01:0	1
	14 Aug 2022 at 01:01	:01 user_xyz T	OK-FW-7365 P	PA-5220 10.1.2		TSF_7365 13	Aug 2022 at 01:01:0	1

Avec une licence Premium, AlOps pour NGFW offre également des capacités avancées en matière de posture de sécurité. Les fonctionnalités de l'option Premium visent à garantir une utilisation complète et une sécurité maximale de vos pare-feu. Découvrez les offres des licences gratuite et premium.

Rapport BPA à la demande

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?	
 , y compris ceux financés par les crédits NGFW logiciels 	L'une des options suivantes : ou	
	ou ou	

Vous pouvez maintenant exécuter le résumé de l'évaluation des meilleures pratiques (EBP) et de l'adoption des fonctionnalités directement depuis Strata Cloud Manager. Il suffit de télécharger un fichier de support technique (TSF). Vous pouvez générer le rapport BPA à la demande pour les périphériques qui n'envoient pas de données télémétriques ou qui sont intégrés à AlOps pour NGFW.

Le BPA évalue votre posture de sécurité par rapport aux meilleures pratiques de Palo Alto Networks et priorise les améliorations à apporter aux périphériques. Les meilleures pratiques en matière de sécurité permettent de prévenir les menaces connues et inconnues, de réduire la surface d'attaque et de fournir une visibilité sur le trafic, afin que vous puissiez connaître et contrôler les applications, les utilisateurs et le contenu présents sur votre réseau. En outre, les meilleures pratiques comprennent des vérifications des contrôles de sécurité critiques (CSC) du Center for Internet Security. Consultez le Guide des meilleures pratiques pour renforcer la posture de sécurité et mettre en œuvre des améliorations.

Puis-je toujours générer des rapports BPA à partir du portail de support client ?

Avant l'existence d'AlOps, vous vous rendiez au Portail de support client pour accéder au BPA et l'exécuter. Aujourd'hui, la méthode préférée pour générer et télécharger un rapport d'évaluation des meilleures pratiques pour NGFW/Prisma Access Panorama géré est l'AlOps.

Après le 17 juillet 2023, vous ne pourrez plus accéder au BPA et l'exécuter à partir du portail de support client.

STEP 1 Rendez-vous dans le Hub et activez AlOps pour NGFW. C'est gratuit. Vous pouvez l'activer sans Strata Logging Service si vous ne souhaitez pas intégrer des périphériques avec télémétrie activée pour le moment.



Le tableau de bord des meilleures pratiques, les alertes de sécurité et les fonctionnalités de résumé de l'adoption ne sont pas disponibles pour les périphériques intégrés sans Strata Logging Service ou télémétrie activée.

- **STEP 2** | Connectez-vous à votre instance AlOps pour NGFW activée. Les onglets suivants s'affichent, même sans Strata Logging Service :
 - Posture
 - Activité
 - Paramètres

- STEP 3 Accédez aux Dashboards (Tableaux de bord) > On Demand BPA (BPA à la demande).
- **STEP 4** Generate New BPA Report (Générez un nouveau rapport BPA).
- **STEP 5** | Select TSF (Sélectionnez TSF) et Upload TSF (Téléchargez le fichier TSF).



Le temps de téléchargement dépend de la taille de votre fichier .tgz et de votre vitesse Internet. Le téléchargement du fichier peut prendre quelques minutes pour les fichiers volumineux. Développez la rubrique **In-Progress (En cours)** pour afficher l'état des fichiers TSF.

- Le BPA à la demande prend en charge uniquement les fichiers d'assistance technique (TSF) au format de fichier .tgz.
- Le BPA à la demande prend en charge les TSF des périphériques équipés de la version PAN-OS 9.1 ou supérieure pour la génération de rapports.
- **STEP 6** | Sélectionnez **View Report (Afficher le rapport)** sous **Completed (Terminé)** après le traitement de la TSF pour afficher le rapport BPA généré à partir de votre périphérique.

Meilleures pratiques

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
•	ou
•	□ Licence
	 Activer le partage de télémétrie sur les périphériques

Que vous indique ce tableau de bord ?

Le tableau de bord affiche les données agrégées par Prisma Access et NGFW/Panorama associés à votre locataire.

Accédez au tableau de bord **Strata Cloud Manager > Dashboards (Tableaux de bord) > More Dashboards (Plus de tableaux de bord) > Best practices (Meilleures pratiques)** pour mesurer votre posture de sécurité par rapport aux conseils de Palo Alto Networks sur les meilleures pratiques. Il est important de noter que l'évaluation des meilleures pratiques prévoit la vérification des contrôles de sécurité critiques (CSC) du Center for Internet Security. Les vérifications CSC sont présentés séparément des autres vérifications des meilleures pratiques afin de faciliter la sélection et la hiérarchisation des mises à jour qui vous permettront de vous conformer aux CSC.

Comment pouvez-vous utiliser les données du tableau de bord ?

Bien que les conseils sur les meilleures pratiques visent à vous aider à renforcer votre posture de sécurité, les résultats de ce rapport peuvent également vous aider à identifier les domaines nécessitant des modifications pour une gestion plus efficace de votre environnement.



Le tableau de bord des meilleures pratiques comporte cinq sections :

Résumé

Vous offre une vue complète de toutes les vérifications ayant échoué sur un périphérique dans toutes les configurations (sécurité, réseau, identité et configuration du service). Affiche des graphiques de tendance historiques pour les vérifications BPA et évalue votre taux d'adoption des meilleures pratiques pour les zones de fonctionnalités clés.

• Sécurité

Affiche les règles, les bases de règles ou les profils qui échouent aux meilleures pratiques et les vérifications CSC d'un périphérique et d'un emplacement sélectionnés. Lorsqu'elles sont

disponibles, les corrections CLI vous permettent de résoudre les problèmes liés aux règles de votre politique. Les corrections CLI sont générées à l'aide des données TSF que vous chargez lors de la génération d'un Rapport BPA à la demande.

• Bases de règles

Examine l'organisation de votre politique et vérifie si les paramètres de configuration qui s'appliquent à de nombreuses règles sont conformes aux meilleures pratiques (notamment les vérifications CSC).

Règles

Vous montre les règles qui échouent aux meilleures pratiques et aux vérifications CSC. Découvrez où vous pouvez prendre des mesures rapides pour corriger les échecs de vérifications. Les règles sont triées en fonction du nombre de sessions, ce qui vous permet de commencer par revoir et mettre à jour les règles qui ont le plus d'impact sur le trafic.

• Profils

Vous montre comment vos profils se comparent aux meilleures pratiques, notamment les vérifications CSC. Les profils effectuent une inspection avancée du trafic correspondant à une règle de sécurité ou de déchiffrement.

• Identité

Indique si les paramètres d'application de l'authentification (règle d'authentification, profil d'authentification et portail d'authentification) d'un périphérique sont conformes aux meilleures pratiques et aux vérifications CSC.

Réseau

Vérifie si les règles de contrôle prioritaire sur l'application et les paramètres réseau sont conformes aux meilleures pratiques et aux vérifications CSC.

• Configuration du service

Découvrez comment les abonnements que vous avez activés sur vos périphériques reflètent les meilleures pratiques et les vérifications CSC. Vous pouvez consulter la configuration de WildFire, du portail GlobalProtect et de la passerelle GlobalProtect ici et corriger les échecs de vérification.



Partager, télécharger et planifier des rapports pour un tableau de bord

Vous pouvez télécharger, partager et planifier des rapports couvrant les données affichées par le tableau de bord aux formats PDF et .csv, ainsi que les corrections CLI au format .txt. Retrouvez ces icônes dans le coin supérieur droit du tableau de bord :

Application Usage		L. C.	ŧ
		The later is	