paloalto
TECHDOCS

Strata Cloud Manager AIOps

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

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

Copyright

Last Revised

February 3, 2025

Table of Contents

AIOps for NGFW

En vous appuyant sur les données recueillies par le biais de la télémétrie des périphériques PAN-OS, AIOps 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.AIOps 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, AIOps 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 AIOps 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 AIOps pour NGFW vous permet également d'utiliser Strata Cloud Manager pour la* gestion du cloud pour les NGFW.

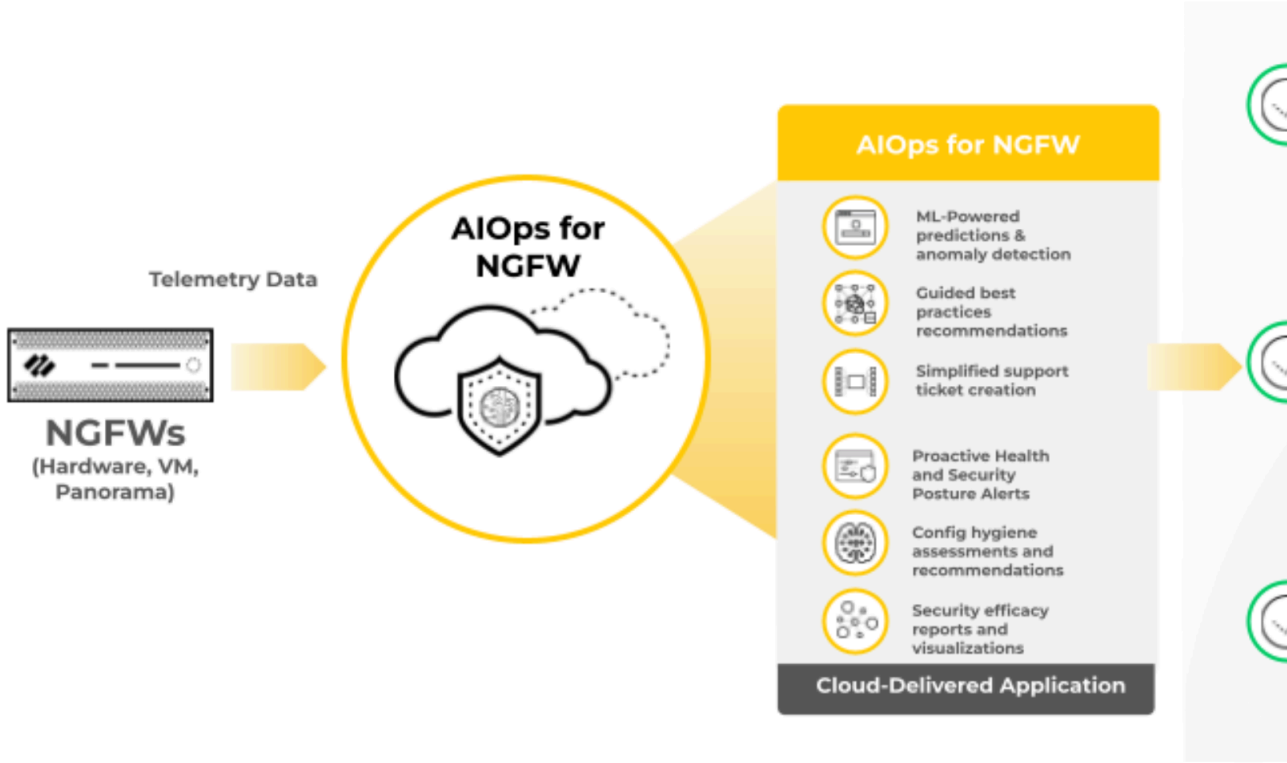
À partir d'octobre 2024, Strata Cloud Manager dispose de deux niveaux de licence : Strata Cloud Manager Essentials et Strata Cloud Manager Pro. Cette structure unifiée rationalise le déploiement des offres de sécurité réseau, notamment les AIOps pour NGFW, la gestion de l'expérience numérique autonome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

Mise en route :

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

- AIOps pour NGFW – Incidents et alertes



Régions pour AIOps 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 : ☐ AIOps for NGFW Free ou Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium ou Strata Cloud Manager Pro

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

AIOps for NGFW n'est pas proposé dans toutes les régions où l'infrastructure Strata Logging Service (SLS) est prise en charge. Le déploiement d'AIOps 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 AIOps n'est pas prise en charge, elles seront traitées par une instance AIOps 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 AIOps 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 : ☐ AIOps for NGFW Free ou Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium ou Strata Cloud Manager Pro

AIOps 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 pare-feu
- 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

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 Vérifier *les licences et autres exigences pour utiliser la visionneuse de journaux.*	Oui	Oui
• 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 AIOps 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 : ☐ AIOps for NGFW Free ou Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium ou Strata Cloud Manager Pro

Voici les différents scénarios pour activer AIOps for NGFW :

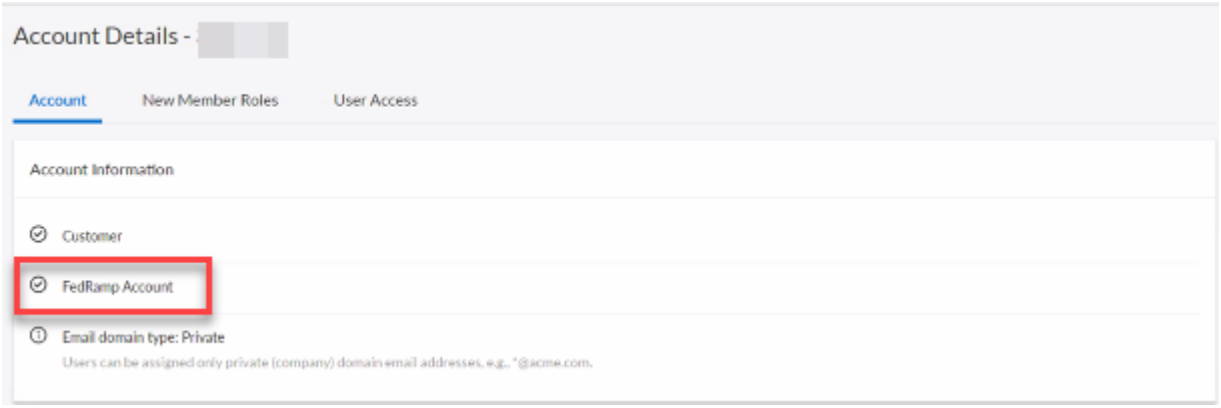
Scénario	Plan
Activation de AIOps for NGFW Gratuit	Activer AIOps for NGFW (Gratuit)
Activation de AIOps for NGFW Premium (utilisez l'appli Strata Cloud Manager)	Activer AIOps pour NGFW via les services communs
Intégration de nouveaux périphériques à l'instance AIOps for NGFW gratuite activée	Associer des périphériques à un locataire Activer la télémétrie sur les périphériques
Intégration de nouveaux périphériques à AIOps 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 AIOps for NGFW Premium	Activer le contrat de licence d'entreprise (ELA) AIOps pour NGFW Premium
Utilisation de Strata Cloud Manager (AIOps pour NGFW Premium) pour gérer VM-Series	Activer un contrat de licence de crédits NGFW logiciels
Utilisation de Strata Cloud Manager (AIOps 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 AIOps 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

Scénario	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, AIOps 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 AIOps 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 AIOps pour NGFW Premium et AIOps pour NGFW Gratuit reste prise en charge. Vous pouvez continuer à modifier, prolonger ou renouveler ces licences.

Les comptes FedRAMP ne peuvent pas utiliser AIOps 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 AIOps for NGFW.*



Activer AIOps for NGFW (Gratuit)

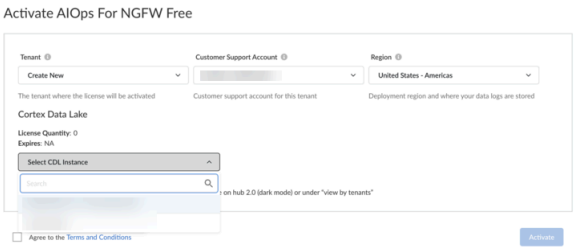
L'activation nécessite le rôle administrateur de compte ou d'appli.

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.

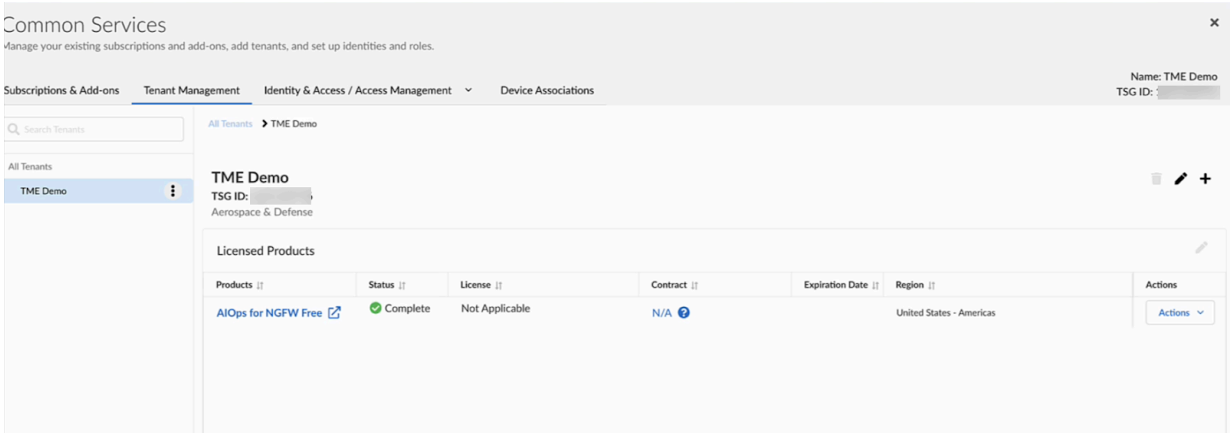
2. Recherchez AIOps for NGFW Gratuit et sélectionnez **Activate (Activer)**.
3. Remplissez le formulaire.



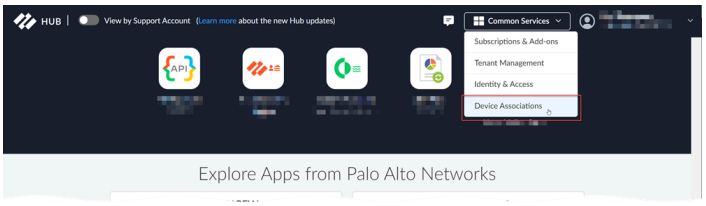
Locataire	Sélectionnez le locataire dans lequel vous activerez l'instance AIOps pour NGFW Gratuit. Si vous n'avez pas de locataire existant, sélectionnez **Create New (Créer un nouveau)**.
Compte de support client	Votre ID de compte sur le portail de support client.
Région	La région de déploiement et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

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

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



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 AIOps 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 AIOps 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.
   1. 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 AIOps 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 crédits NGFW logiciels	L'une des options suivantes : ☐ AIOps for NGFW Free ou Strata Cloud Manager Essentials ☐ AIOps 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 AIOps for NGFW avec vos autres produits et abonnements Palo Alto Networks et les gérer.

Pour lancer Strata Cloud Manager :

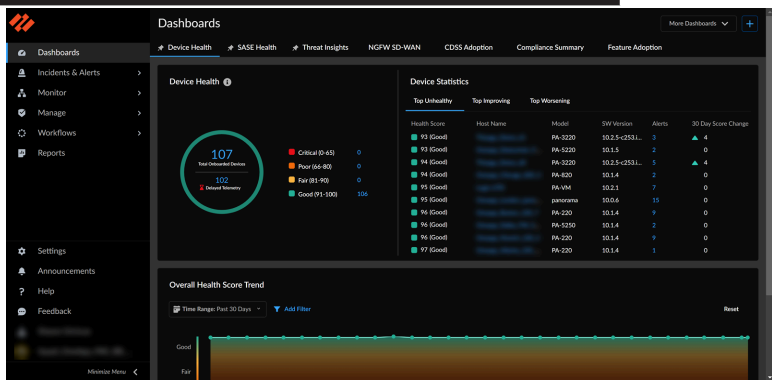
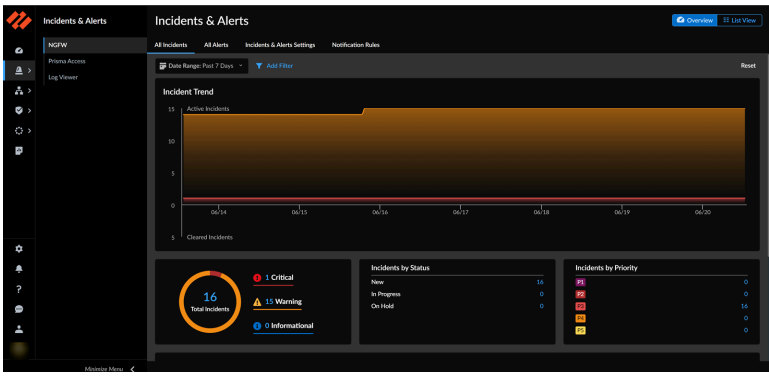
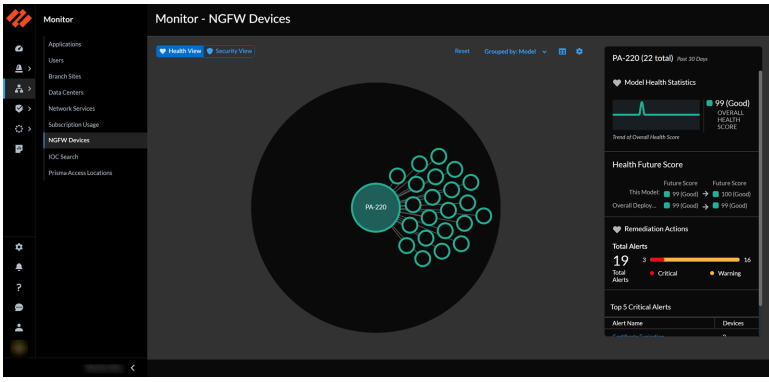
- Accédez au hub et lancez l'appli Strata Cloud Manager
- Rendez-vous directement à l'URL Strata Cloud Manager

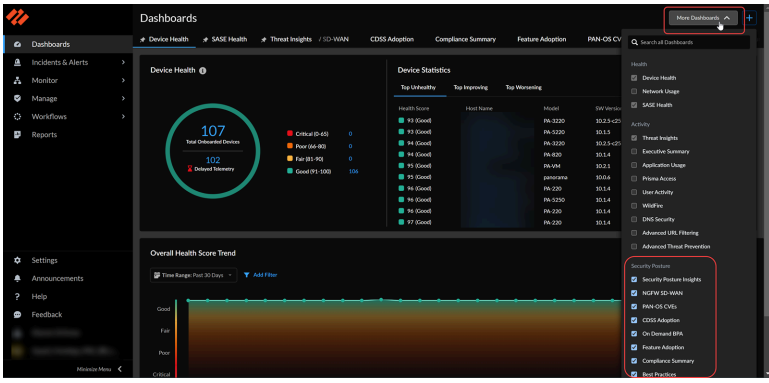
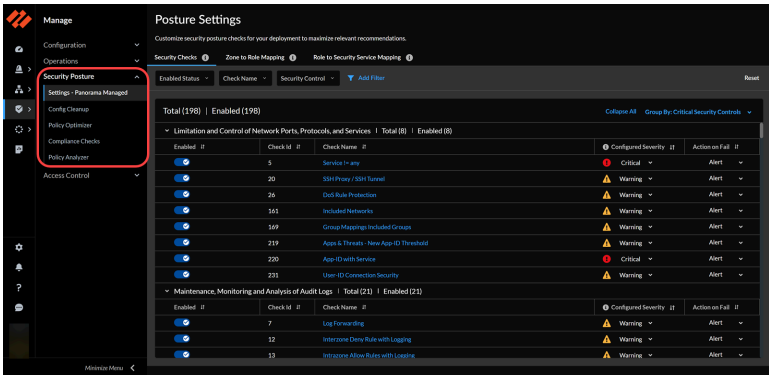
- Strata Cloud Manager *fournit une gestion et des opérations unifiées uniquement pour les NGFW utilisant la licence AIOps pour NGFW Premium. Le nom de la tuile de l'appli sur le hub pour AIOps pour NGFW (appli premium uniquement) est devenu désormais Strata Cloud Manager. Avec cette mise à jour, l'URL 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.*

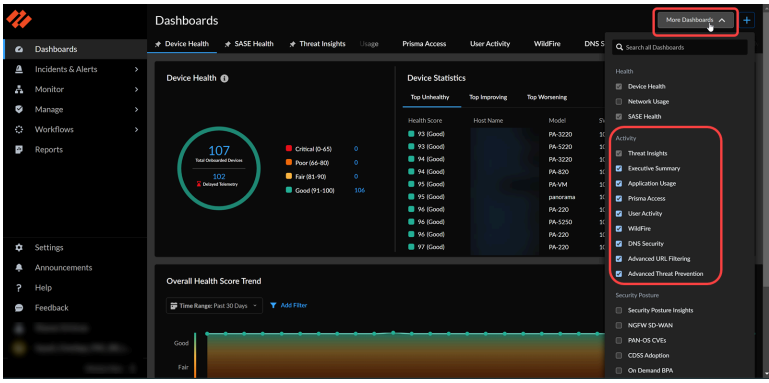
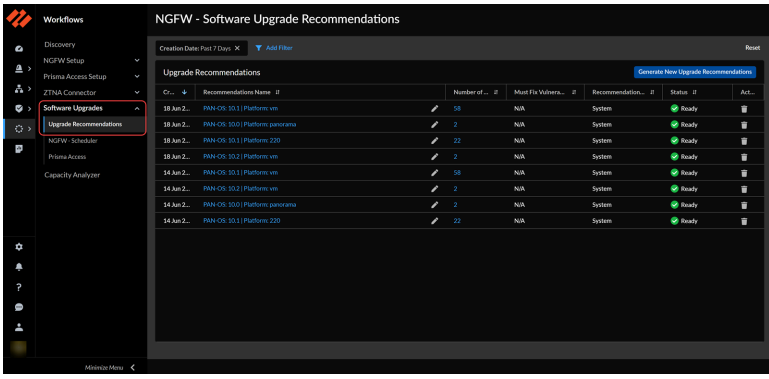
Si vous avez déjà utilisé l'appli AIOps for NGFW, voici où vous pouvez trouver vos fonctionnalités dans Strata Cloud Manager :

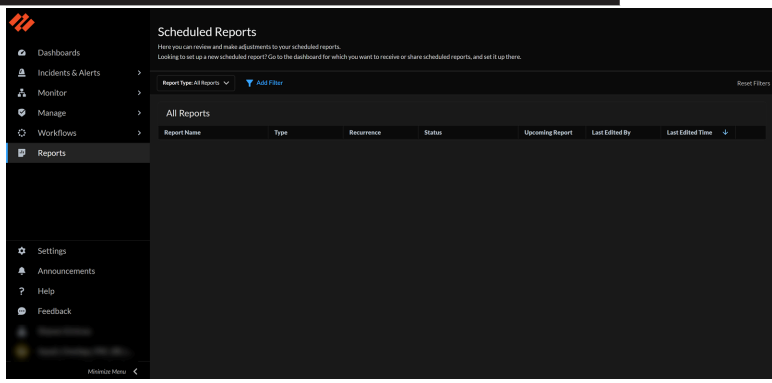
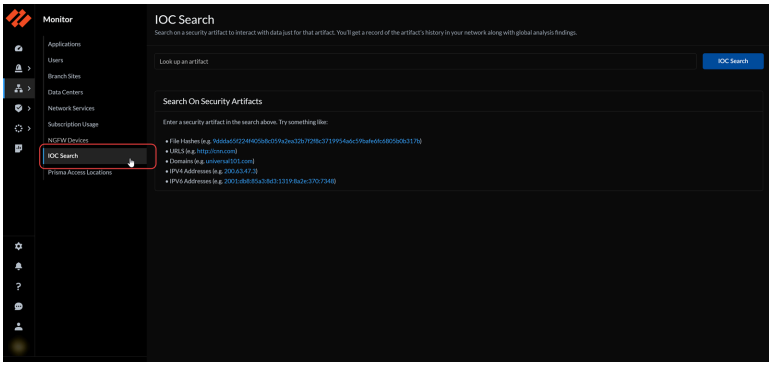
Table 1:

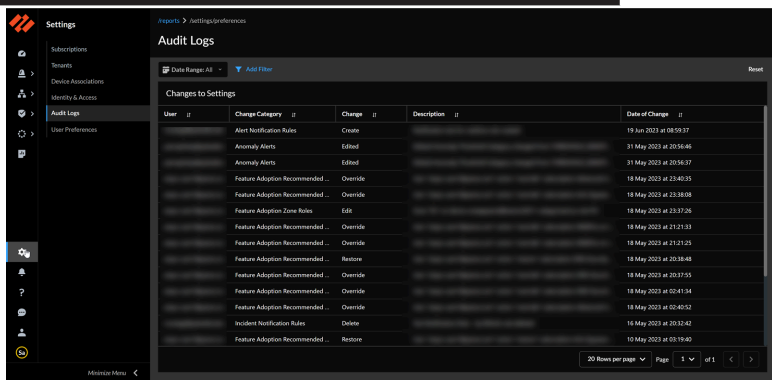
Appli AIOps for NGFW	Où trouver ces mêmes fonctionnalités dans Strata Cloud Manager :
Tableaux de bord	→ Accéder à →Tableaux de bord →Santé du périphérique

Appli AIOps for NGFW	Où trouver ces mêmes fonctionnalités dans Strata Cloud Manager :
	
Alertes	→ Accéder à →Incidents et alertes →NGFW 
Surveiller	→ Accéder à →Surveiller →Périphériques →NGFW 
Posture	→ Accédez aux tableaux de bord pour afficher : • Tableau de bord des meilleures pratiques • 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  → Accéder à →Gérer →Posture de sécurité pour trouver : • Paramètres - Panorama géré • Nettoyage de la configuration • Optimiseur de politique • Contrôles de conformité • Analyseur de politique 
Activité	→ 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 et alertes)** pour **Log Viewer (Visionneuse de journaux)**.
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)**. 
Rapports	→ Accédez à **Reports (Rapports)** pour planifier les rapports des tableaux de bord pris en charge.

Appli AIOps for NGFW	Où trouver ces mêmes fonctionnalités dans Strata Cloud Manager :
	
Recherche	→ Accédez à **Monitor (Surveiller)** pour la **IoC Search (recherche de l'IoC)**. 
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 AIOps for NGFW	Où trouver ces mêmes fonctionnalités dans Strata Cloud Manager :
	 → Accédez à **Manage (Gérer)** > **Security Posture (Posture de sécurité)** pour personnaliser **Settings - Panorama Managed (Paramètres - Panorama géré)**. → Accédez à **Help (Aide)** → **Export Tenant Metadata (Exporter les métadonnées des locataires)**.
–	**Vous cherchez à gérer les NGFW avec Strata Cloud Manager ?** Cela est pris en charge uniquement avec Strata Cloud Manager et AIOps for NGFW Premium, et n'est pas disponible dans l'appli AIOps 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 ?	De quoi ai-je besoin ?
• NGFW, y compris ceux financés par les crédits NGFW logiciels	❑ AIOps 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).

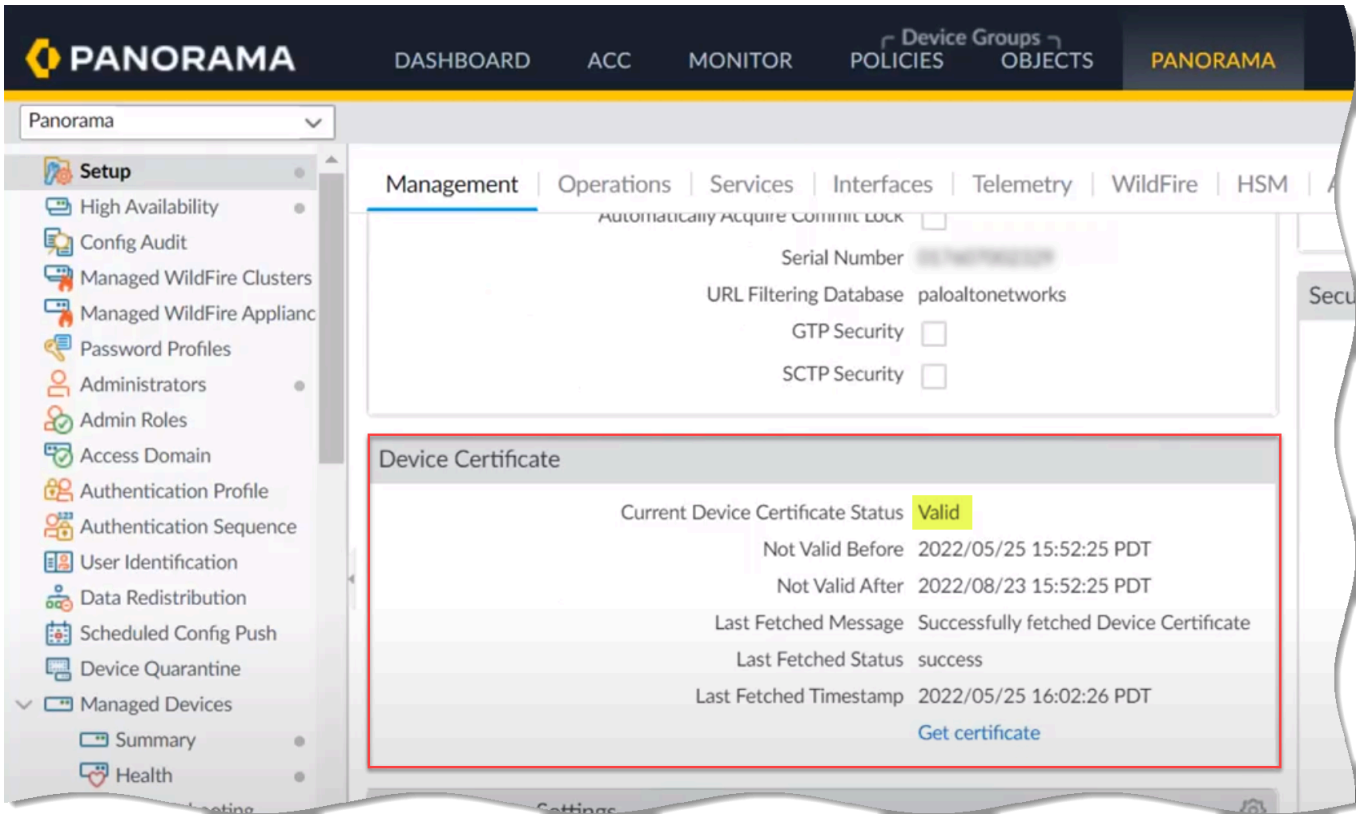
Pour y parvenir, l'Analyseur de politique de Strata Cloud Manager vous permet d'optimiser le temps et les ressources lors de la mise en œuvre d'une requête de modification. L'Analyseur de politique ne se contente pas d'analyser et de fournir des suggestions de consolidation ou de suppression éventuelle 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 AIOps 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.

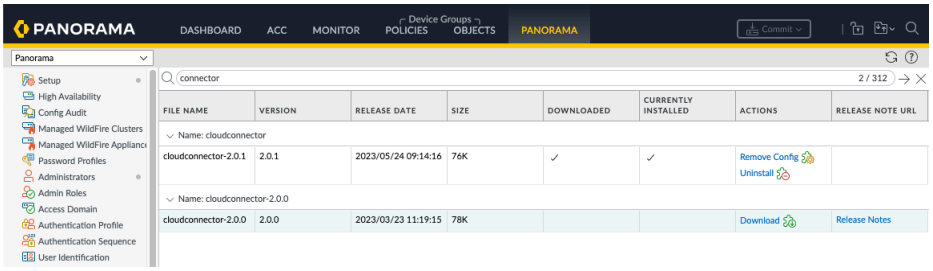
- Un Panorama avec un certificat de périphérique installé.



- 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
  ```



  - *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 AIOps et le plug-in CloudConnector, désinstallez le plug-in AIOps, 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 AIOps 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 :

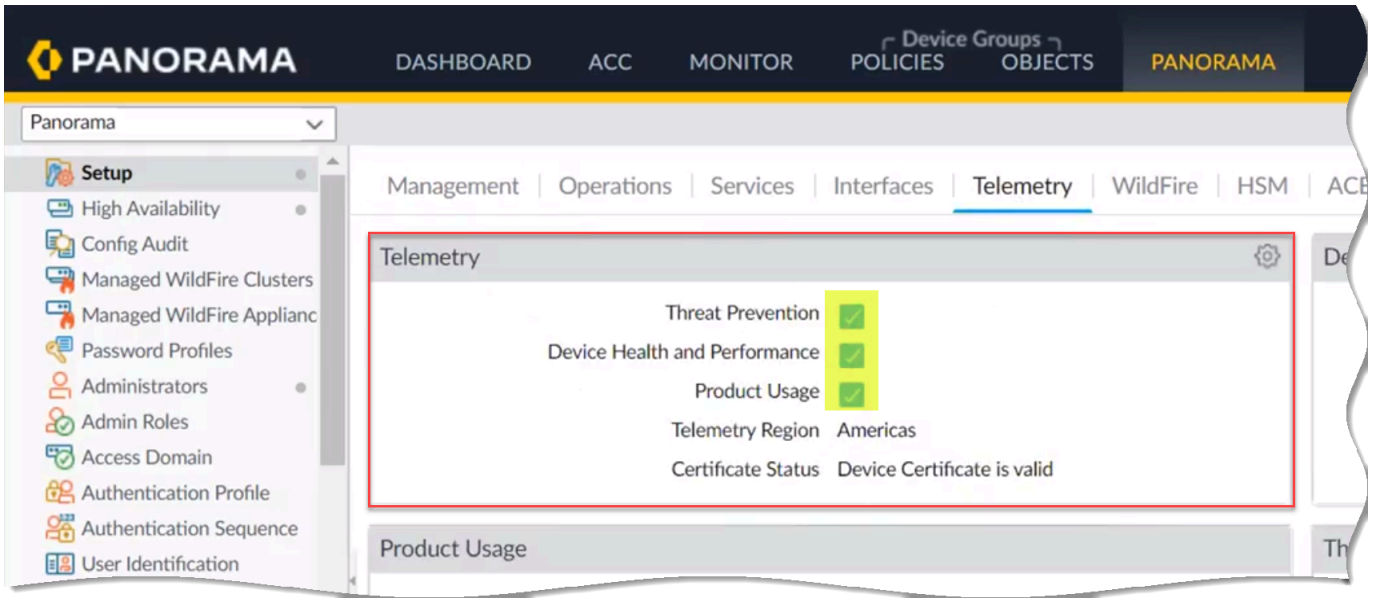
  1. Dans l'interface Web de Panorama, sélectionnez **Panorama > Plugins (Panorama > Plug-ins)** et **Uninstall (Désinstallez)** le plug-in AIOps.
  2. Activer le plug-in CloudConnector :

     ```
     > 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.



- 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 : ☐ AIOps for NGFW Free ou Strata Cloud Manager Essentials ☐ AIOps 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	❑ AIOps 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

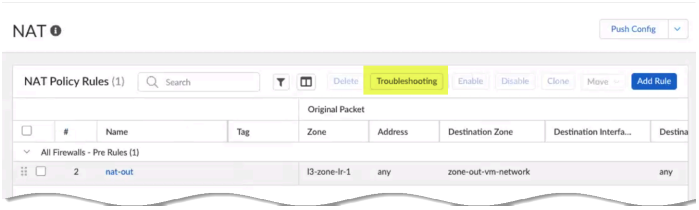
- NAT
- Proxy DNS

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



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

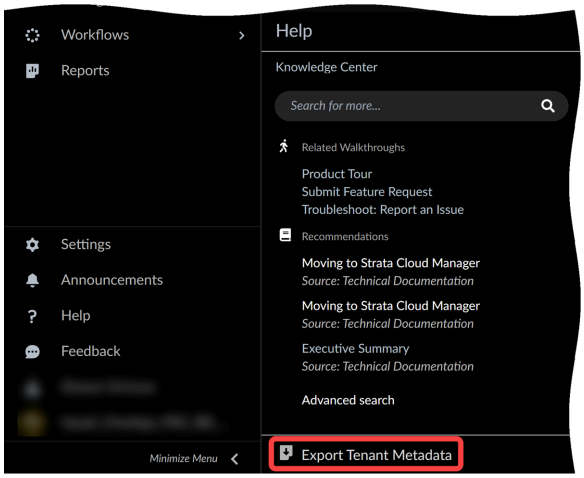
Fonctionnalité	Localisation des fonctionnalités	Actions disponibles	Portée de l'action	Sortie de tâche organisée par :
				d'adresse IPv6 (AAAA), enregistrement de nom canonique (CNAME), enregistrement d'échange de courrier (MX) et pointeur vers un nom canonique (PTR) • Classe : Internet (IN TCP/IP), 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'utilisateur • Groupe

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	• Nom • Filtre • Membres
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

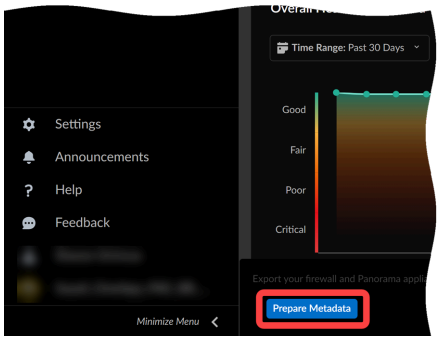
Exportation des métadonnées à des fins de dépannage

Pour fournir au support technique les informations nécessaires pour mieux vous aider, AIOps 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.

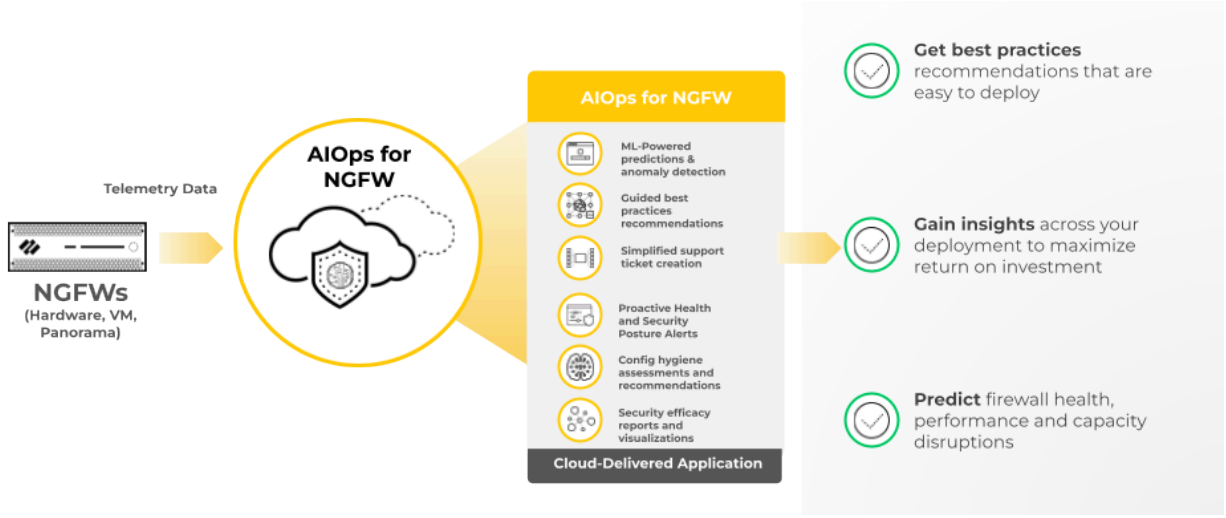
Télémétrie du périphérique pour AIOps for NGFW

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

AIOps 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 AIOps for NGFW avec vos périphériques PAN-OS.

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

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

1. 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 AIOps 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

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'AIOps for NGFW.

Domaines pour accéder à AIOps for NGFW

Autorisez ces domaines afin d'accéder à l'application AIOps 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 AIOps 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/

Optimiser 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

En plus de vous aider à maintenir vos pare-feu en bon état de fonctionnement, AIOps 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.

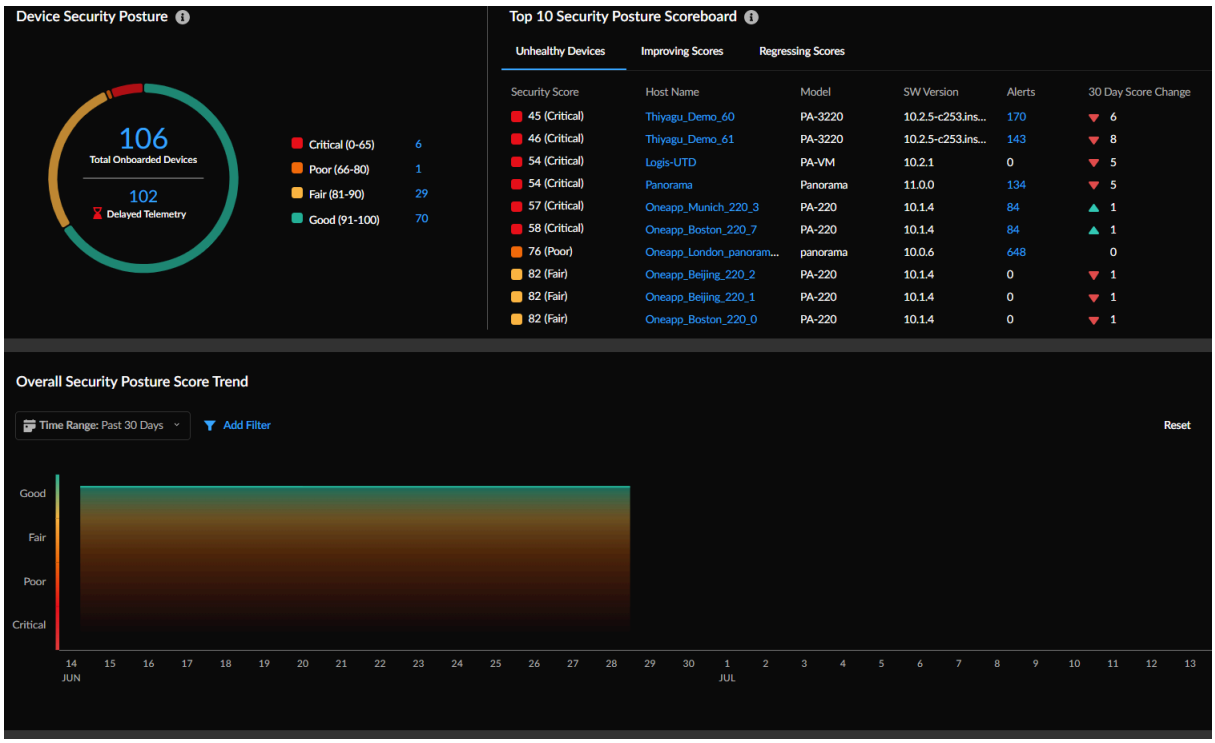
- Surveiller les informations sur la posture de sécurité : Obtenez une visibilité sur l'état et la tendance de la sécurité de votre déploiement en fonction des postures de sécurité des périphériques NGFW intégrés.
- Surveiller l'adoption des fonctionnalités : Affichez les fonctionnalités de sécurité 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

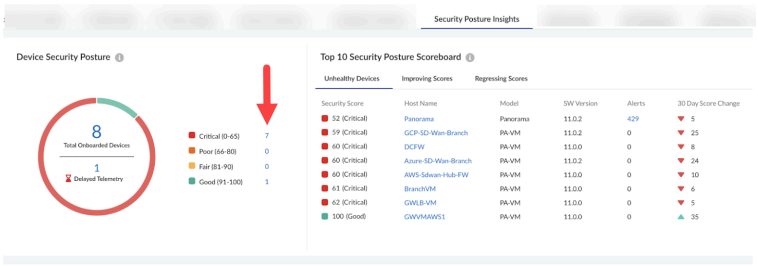
Vous pouvez utiliser le tableau de bord **Security Posture Insights (Informations sur la posture de sécurité)** pour obtenir une visibilité sur l'état et la tendance de la sécurité de votre déploiement en fonction des postures de sécurité des périphériques NGFW intégrés. La gravité du score de sécurité (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.

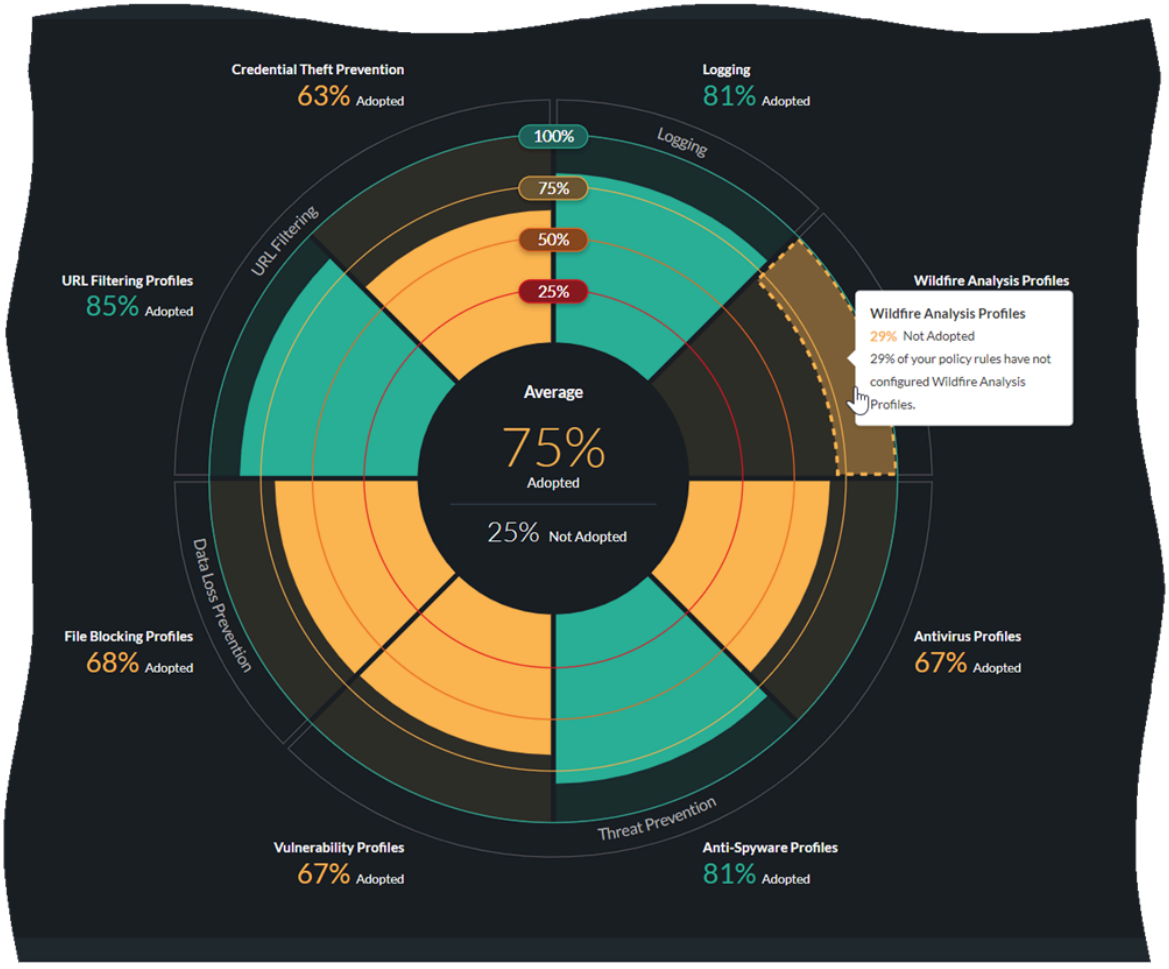
   Vous pouvez également remarquer si certains périphériques exécutent des versions de logiciel obsolètes. Dans ce cas, vous pouvez planifier une mise à niveau vers la dernière version recommandée, que vous pouvez rechercher dans les Recommandations de mise à niveau.
4. Vérifiez la tendance de la posture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



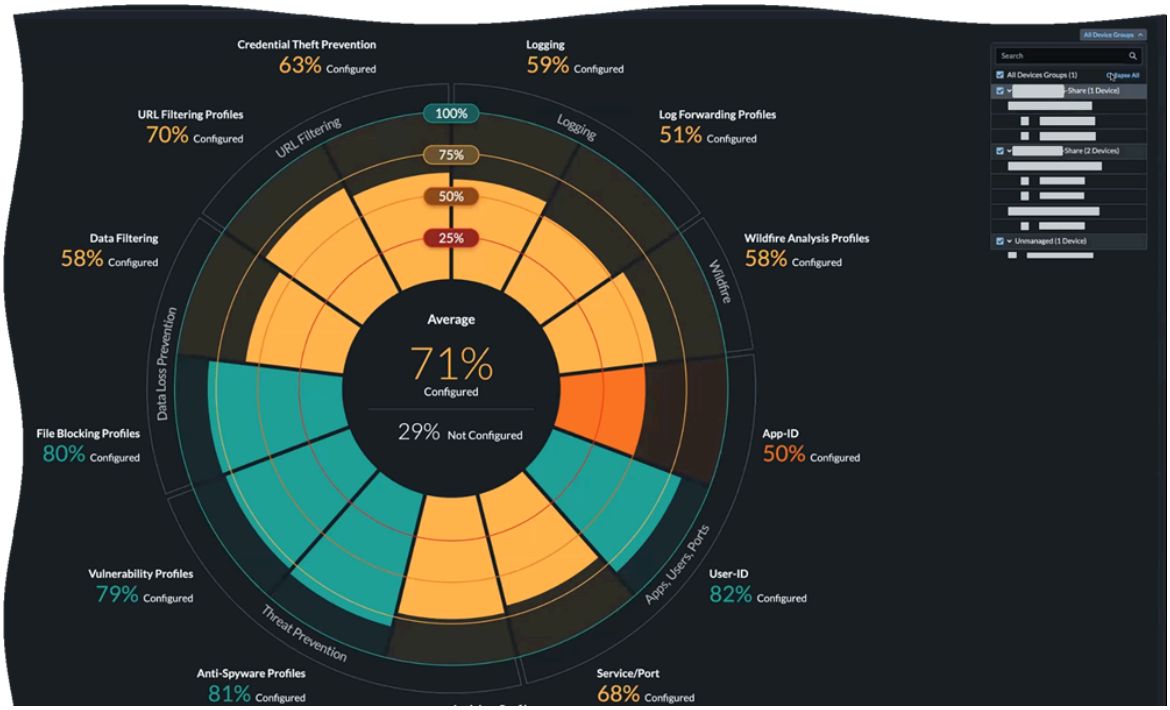
Ce tableau de bord montre les points forts de votre politique de sécurité et les lacunes dans l’adoption des capacités que vous pouvez vous efforcer d’améliorer. Pour obtenir une visibilité maximale sur le trafic et une protection maximale contre les attaques, définissez des objectifs

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.

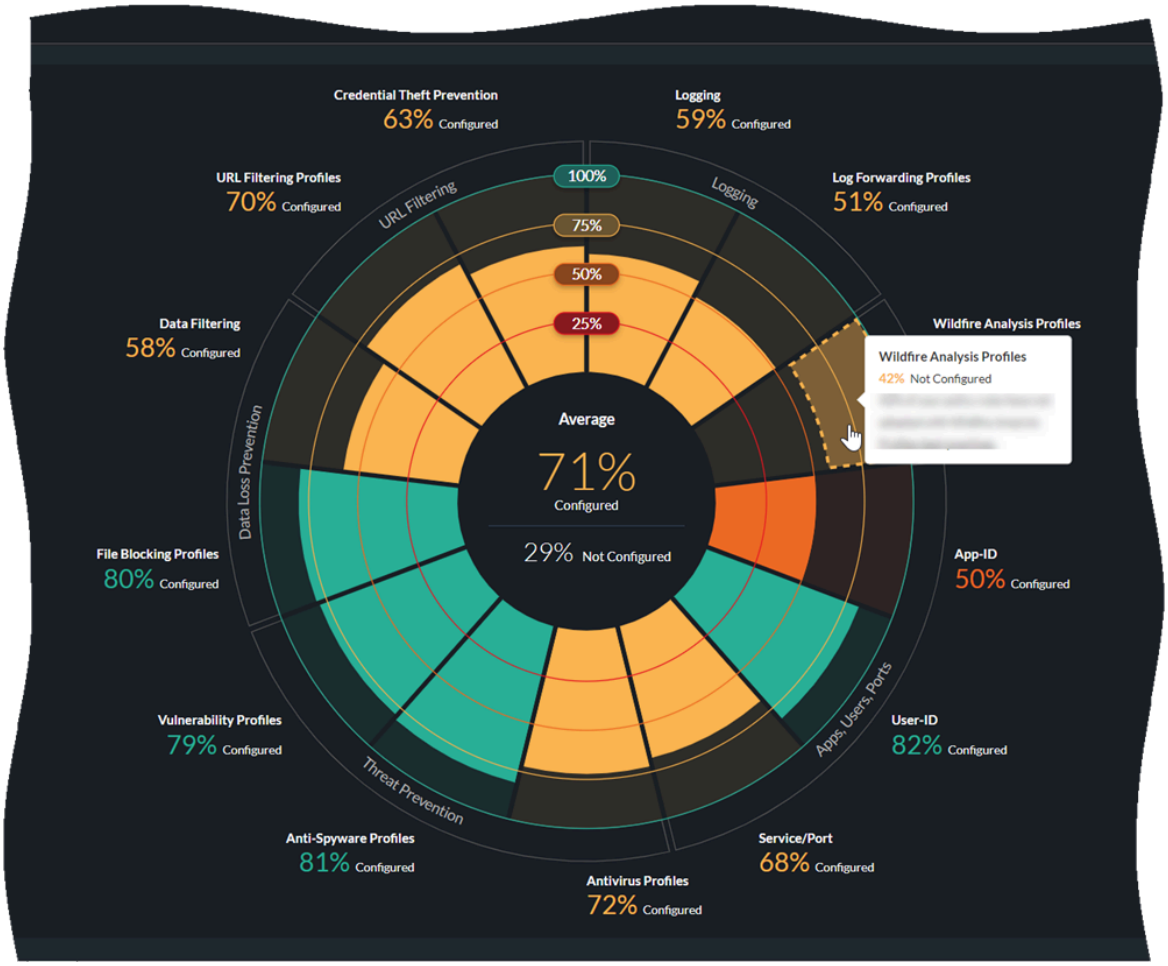
Le résumé d'adoption permet d'identifier les périphériques, les zones et les domaines dans lesquels vous pouvez apporter des améliorations par l'adoption des capacités de la politique de sécurité. Vous pouvez examiner les informations sur l'adoption par Device Group (Groupe d'appareils), Serial Number & 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)**.

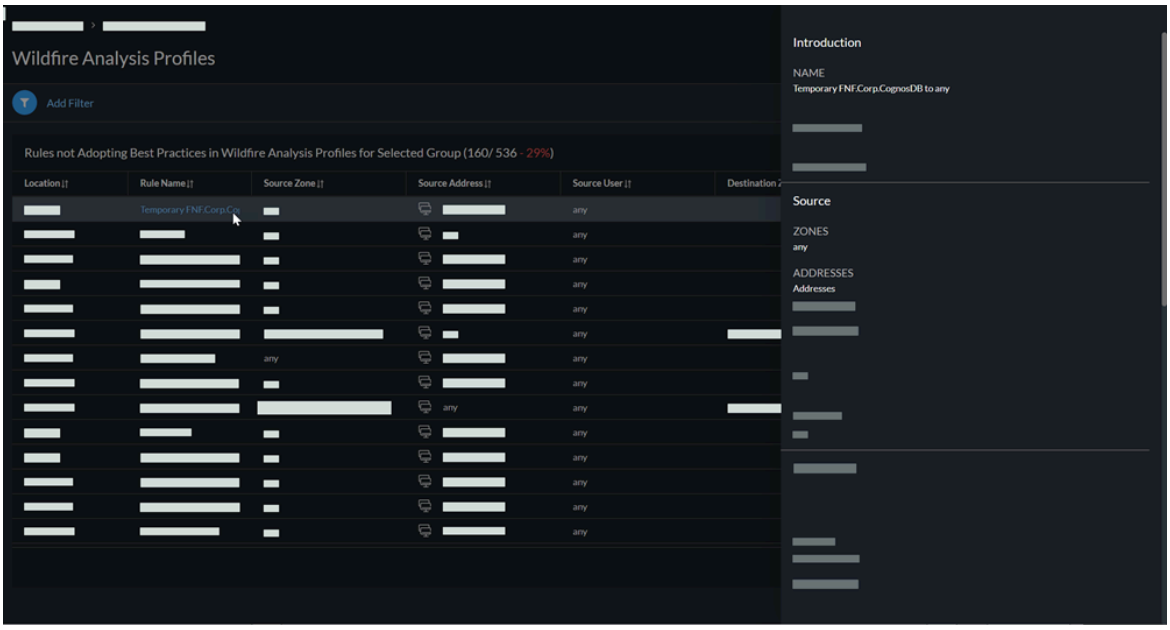
- Pour vous concentrer sur la conformité aux meilleures pratiques pour un ensemble spécifique de pare-feu, vous pouvez filtrer le graphique en fonction du groupe d'appareils.



- 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.



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

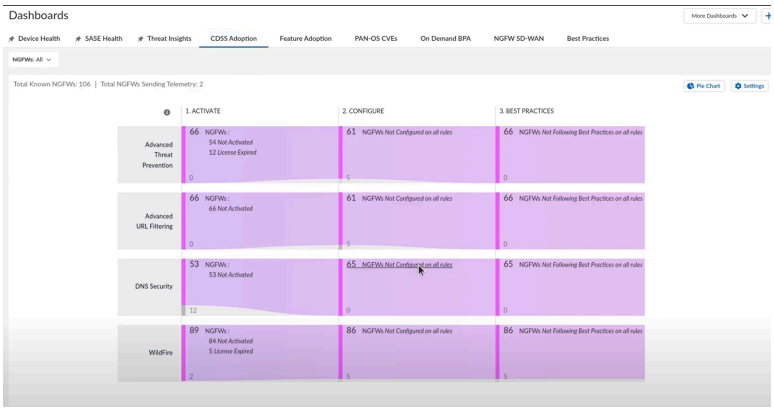
Surveiller les abonnements de sécurité

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

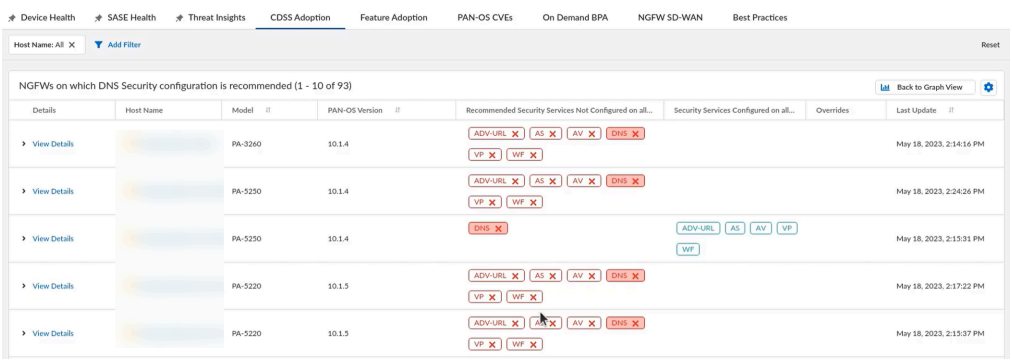
Dans **Dashboard (Tableau de bord)** > **Posture** > **CDSS Adoption (Adoption de CDSS)**, vous pouvez afficher les abonnements des services de sécurité fournis par le cloud (CDSS) recommandés et leur utilisation sur vos périphériques. Cela vous permet d'identifier les failles de sécurité et de renforcer 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.



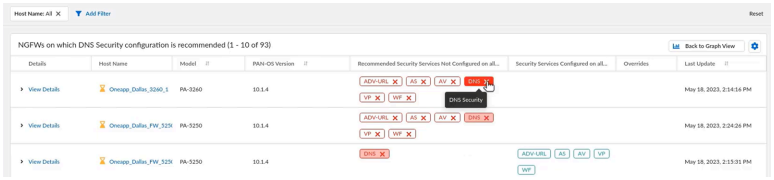
3. Vérifiez les NGFW sur lesquels la configuration de la sécurité DNS est recommandée mais non configurée. **View details (Afficher les détails)** pour vérifier le rôle source et le rôle de destination.



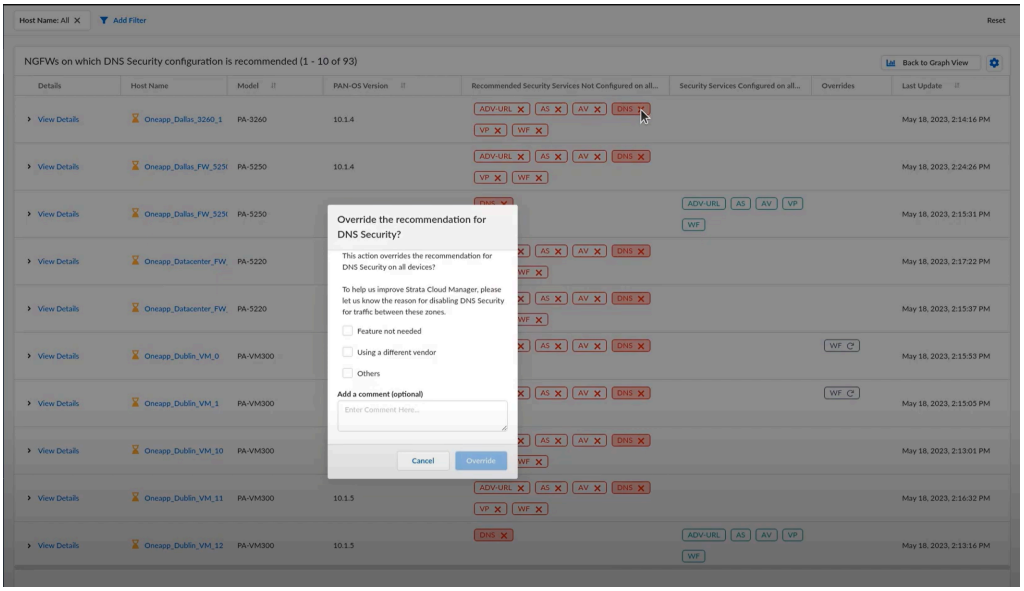
4. **View Policies (Afficher les politiques)** pour afficher les détails des règles et les zones source et de destination correspondantes.

   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**.



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



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.

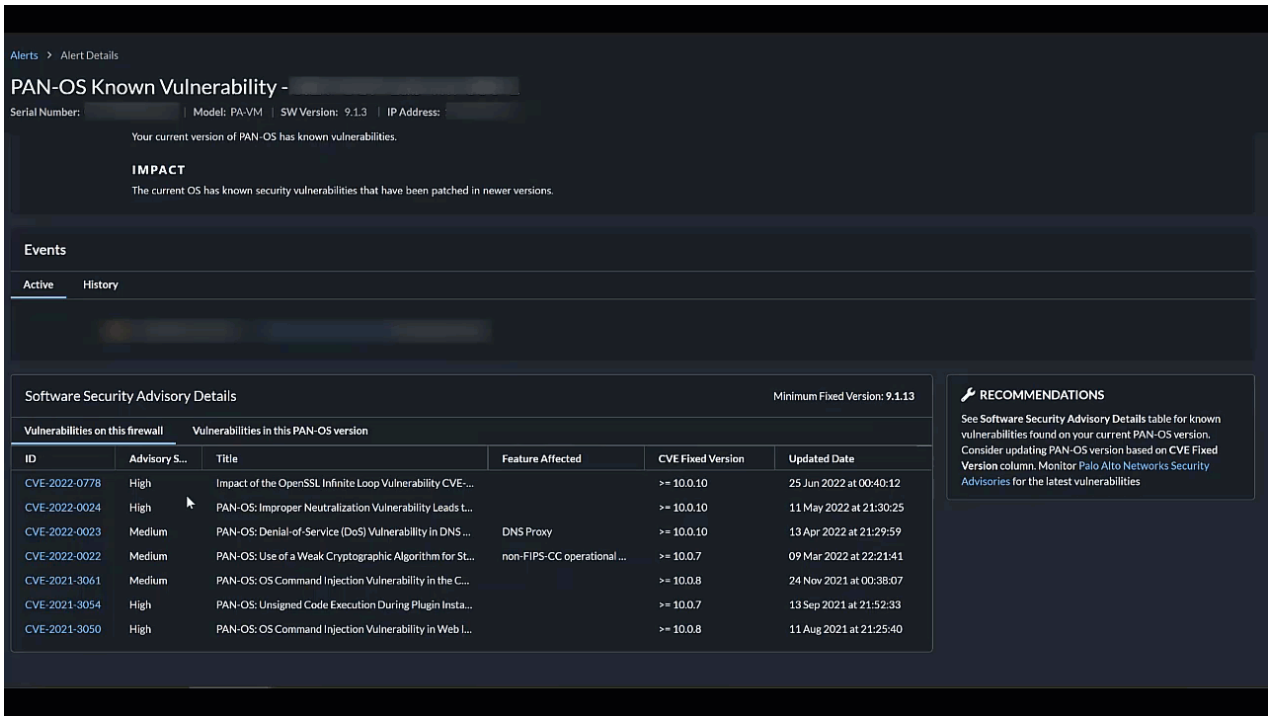
Évaluer les vulnérabilités

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 ❑ ou

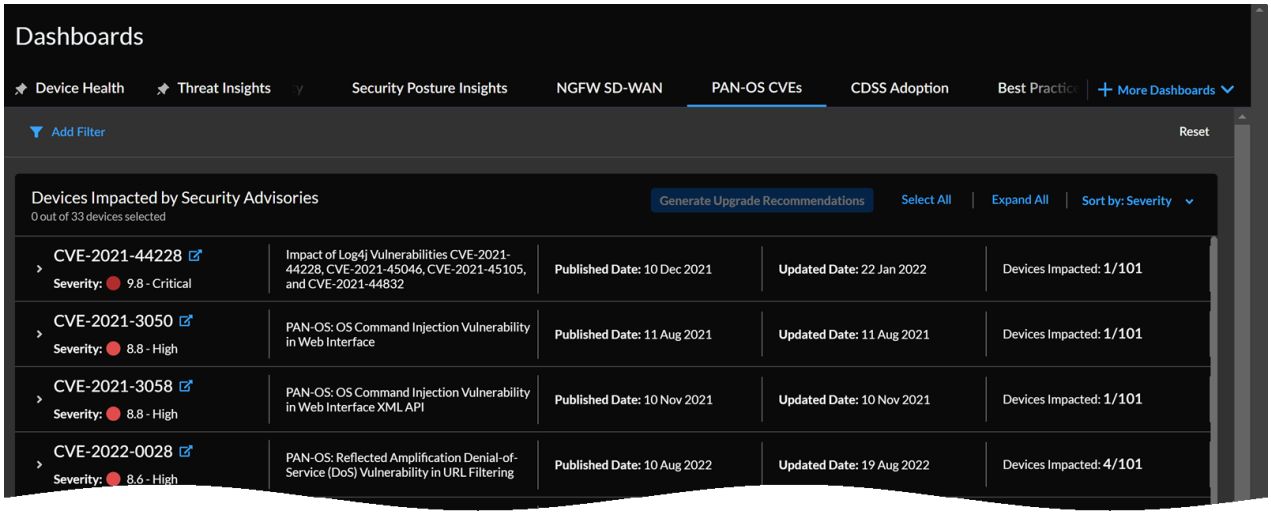
Strata Cloud Manager vous indique les vulnérabilités qui affectent un pare-feu et une version PAN-OS donnés pour vous aider à décider si vous devez effectuer une mise à niveau. Accédez à **Incidents & Alerts (Incidents et alertes)** > **NGFW (NGFW)** > **All Alerts (Toutes les alertes)** et sélectionnez 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.



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.



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.

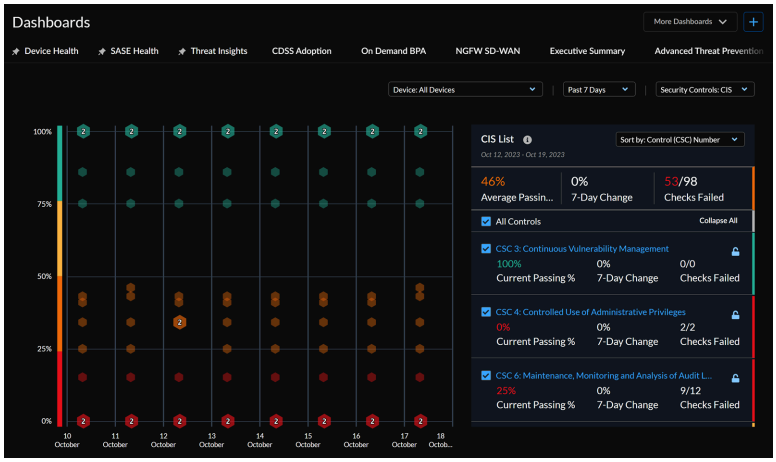
STEP 6 | Sélectionnez l'une des options de mise à niveau pour afficher des détails sur **New Features (Nouvelles fonctionnalités)**, **PAN-OS Known Vulnerabilities (Vulnérabilités connues de PAN-OS)**, **Changes of Behavior (Changements de comportement)** et **PAN-OS Known Issues (Problèmes connus de 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 AIOps 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.

  Ici, 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 AIOps 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.

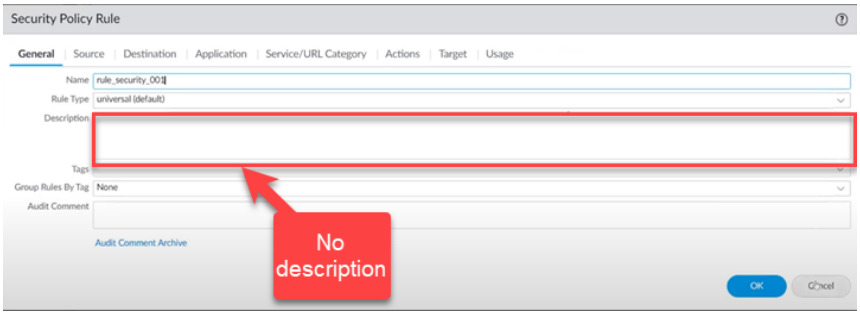
STEP 1 | Assurez-vous desatisfaire toutes les conditions préalables et installez le plug-in.

STEP 2 | Spécifiez les vérifications des meilleures pratiques qui bloqueront les validations en cas d'échec.

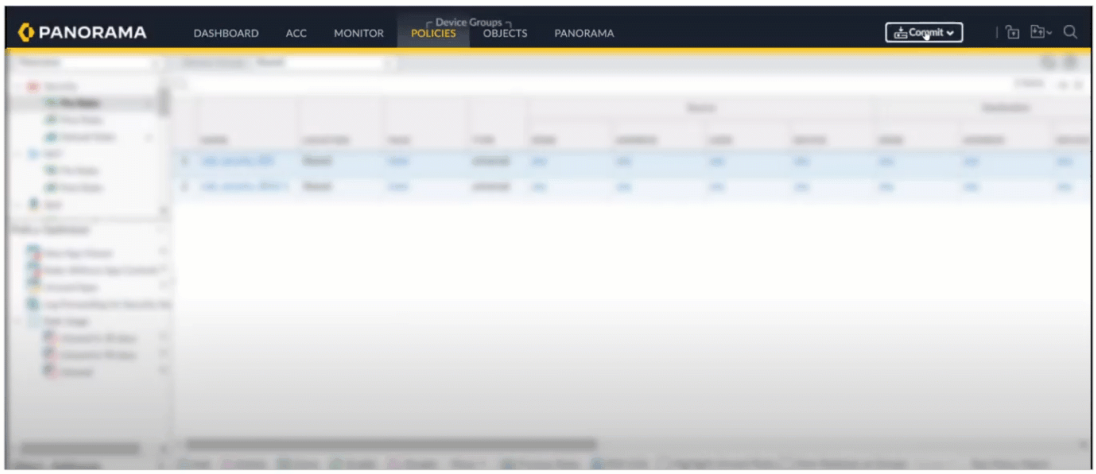
1. Sélectionnez **Manage (Gérer)** > **Security Posture (Posture de sécurité)** > **Settings (Paramètres)**.
2. Recherchez la vérification avec laquelle vous souhaitez bloquer les validations.
3. Définissez une **Action on Fail (Action en cas d'échec)** pour**Fail Commit (Échec de la validation)**

STEP 3 | Vérifiez en essayant de valider une configuration qui ne passe pas la vérification.

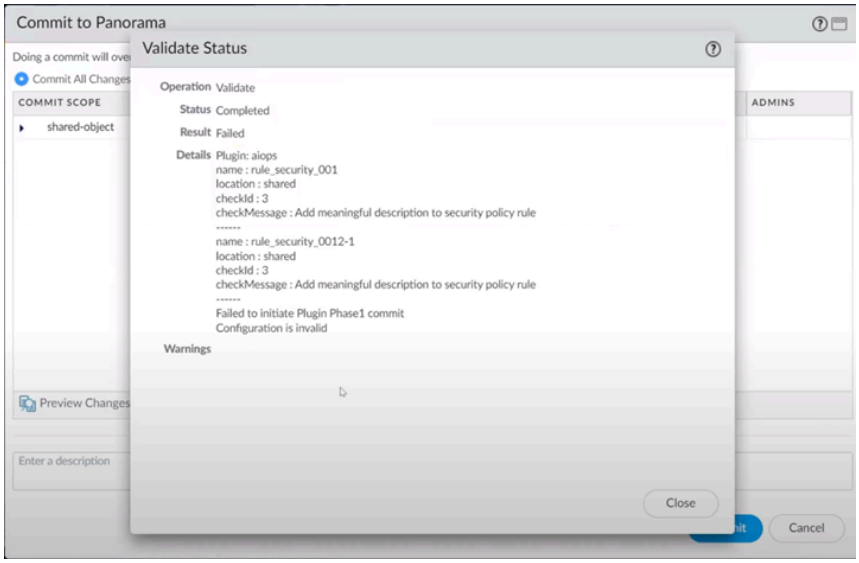
1. Connectez-vous à Panorama.
2. Violez la vérification des meilleures pratiques que vous avez spécifiée dans **Fail Commit (Échec de la validation)**.



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



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.



*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) • (Panorama géré) •	☐ ou ☐ 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) • (Panorama géré) •	❑ ou ❑ Plug-in Panorama CloudConnector pour les déploiements Panorama gérés

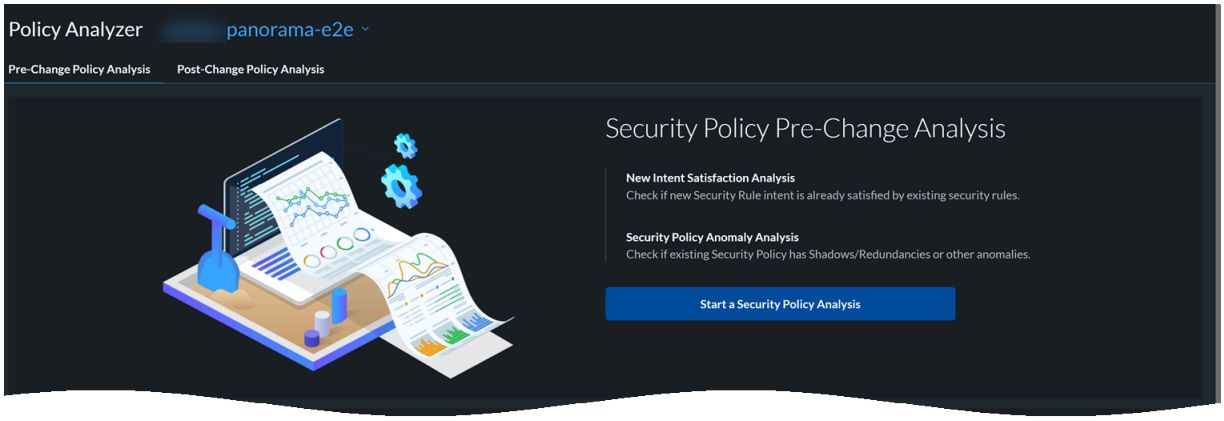
L'analyse préalable aux modifications de la règle de politique de sécurité effectue l'analyse de satisfaction de la nouvelle intention :

- **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)**.

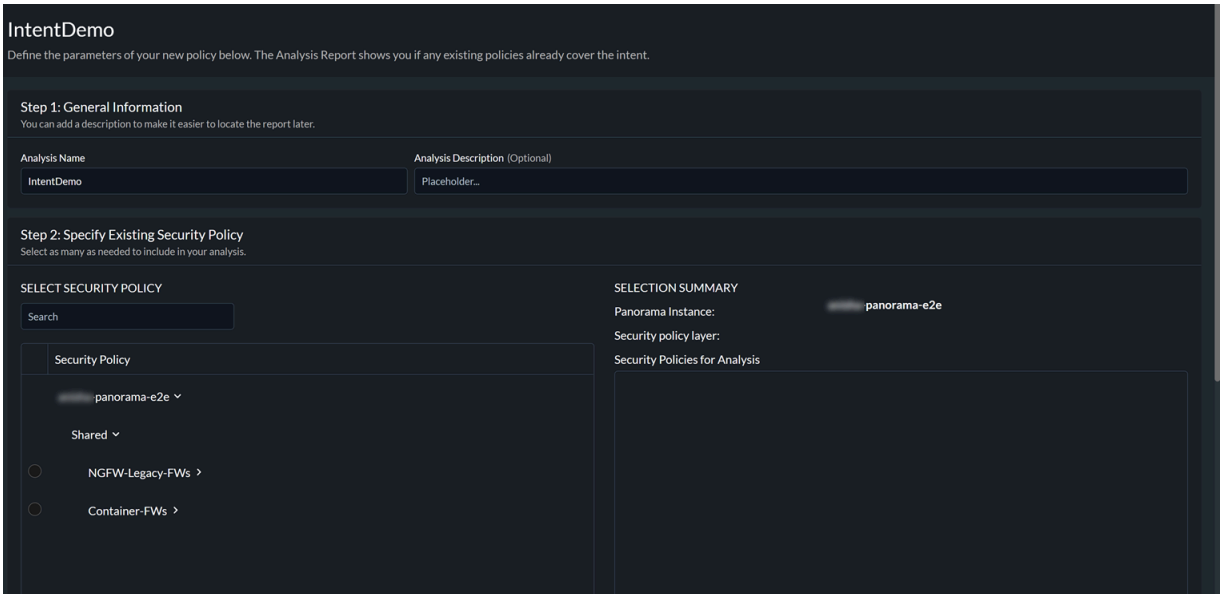
2. En haut de la page Analyseur de politique, sélectionnez l'instance Panorama contenant les règles de politique que vous devez analyser.



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)**.



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.

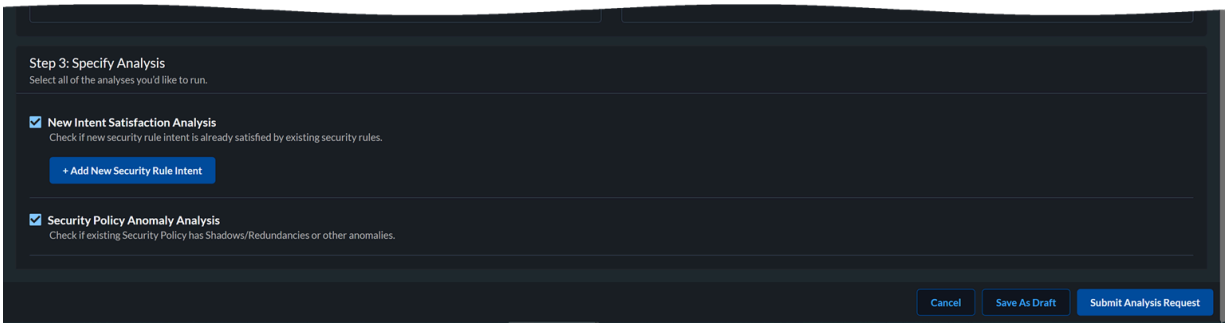
STEP 2 | Sélectionnez un ensemble de politiques de sécurité existant à analyser.

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

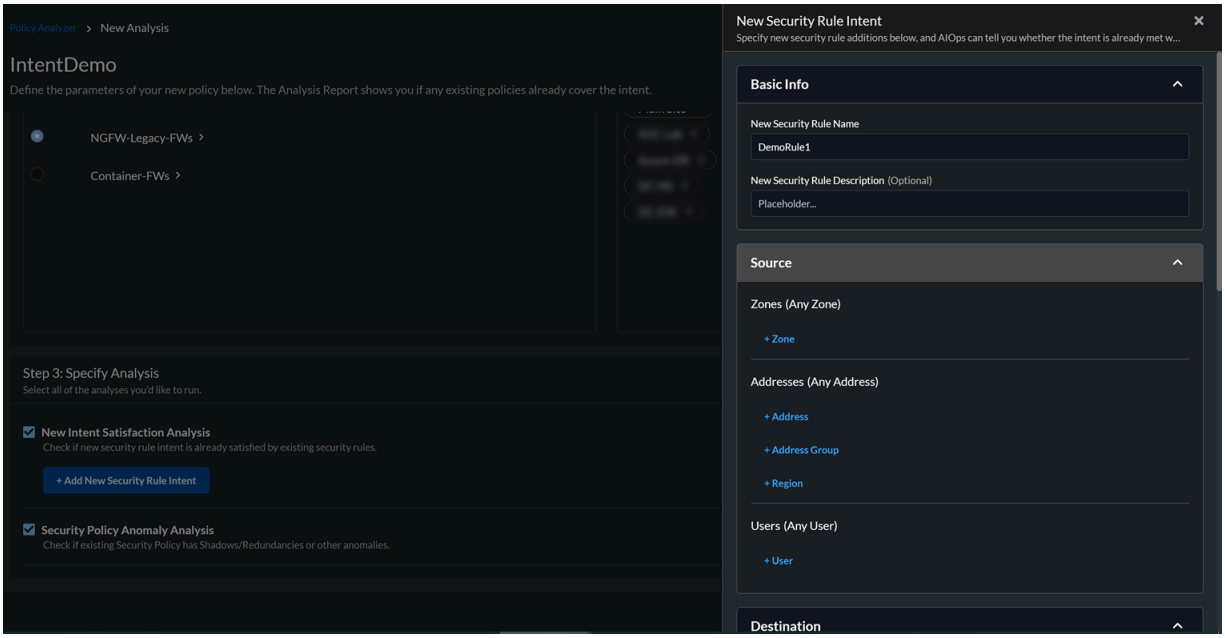
STEP 3 | Spécifiez le type d'analyse en sélectionnant un ou plusieurs types d'analyse :

- **Analyse de satisfaction des nouvelles intentions**

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



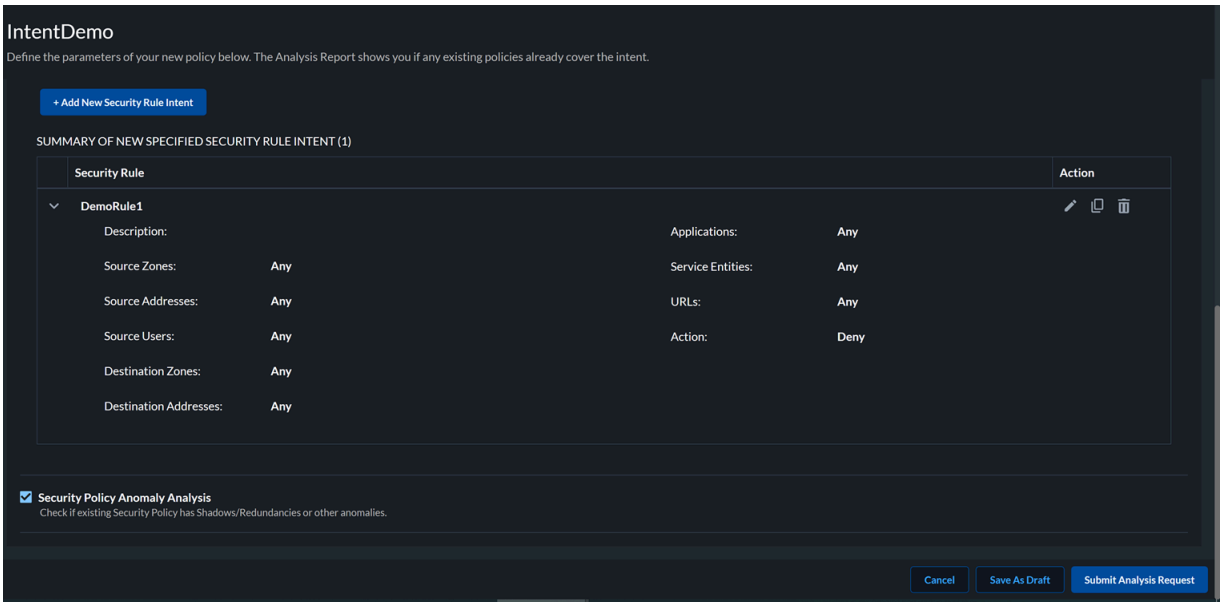
Spécifiez des informations sur la nouvelle règle de sécurité, et AIOps for NGFW peut vérifier si les règles existantes couvrent l'intention.



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.

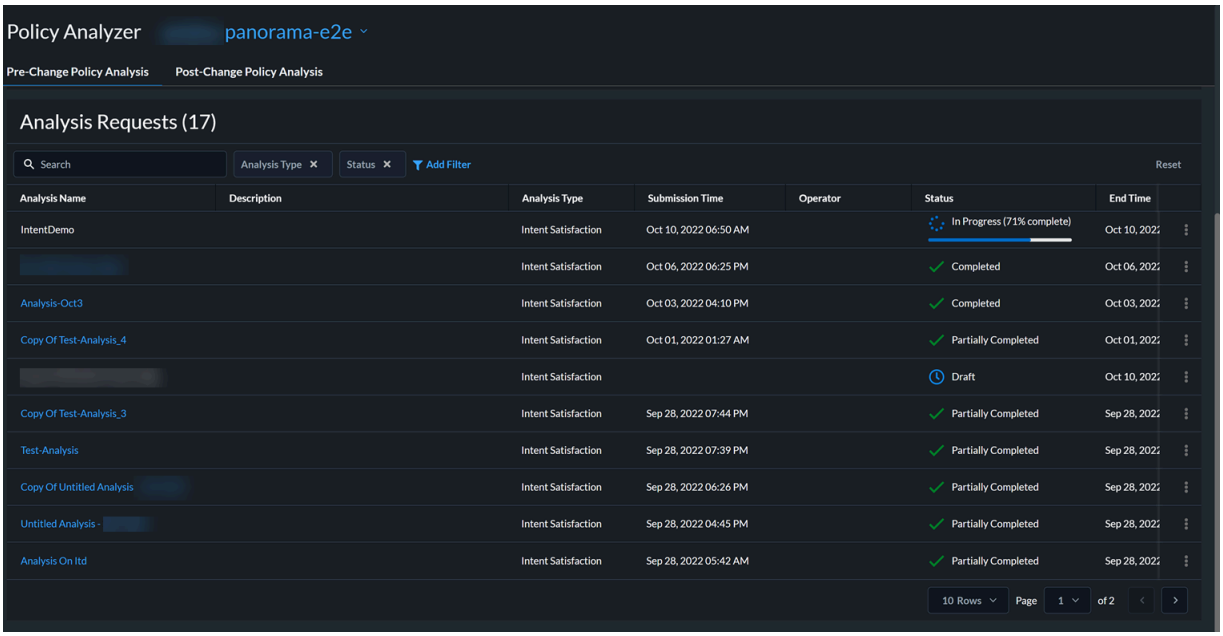
Consultez le résumé de l'intention de la nouvelle règle de sécurité.



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.



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

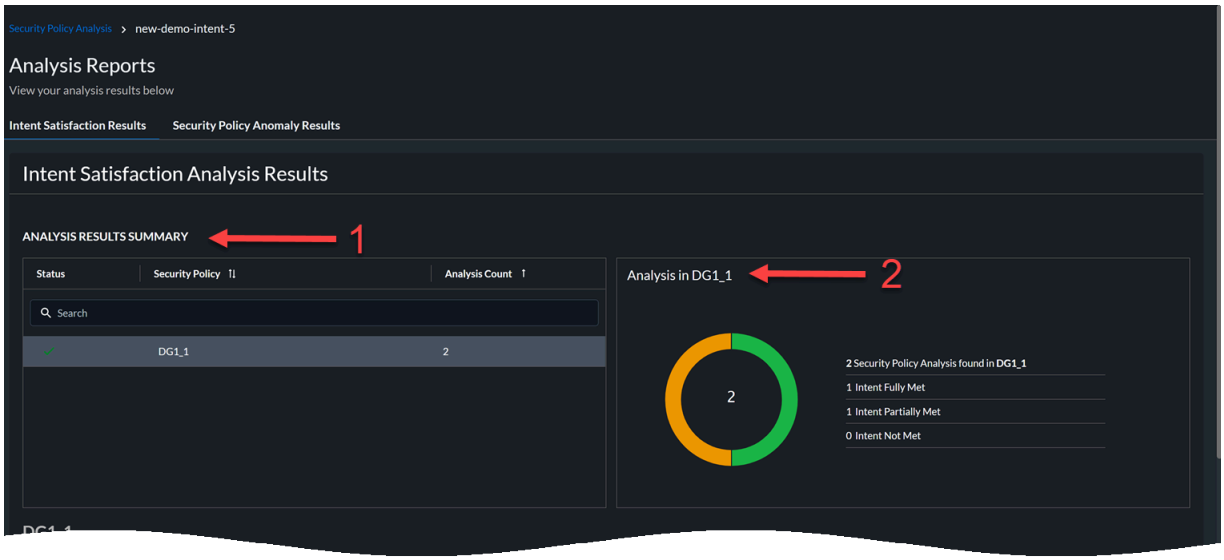
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Panorama géré) • (Panorama géré) •	❑ ou ❑ Plug-in Panorama CloudConnector pour les déploiements Panorama gérés

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.

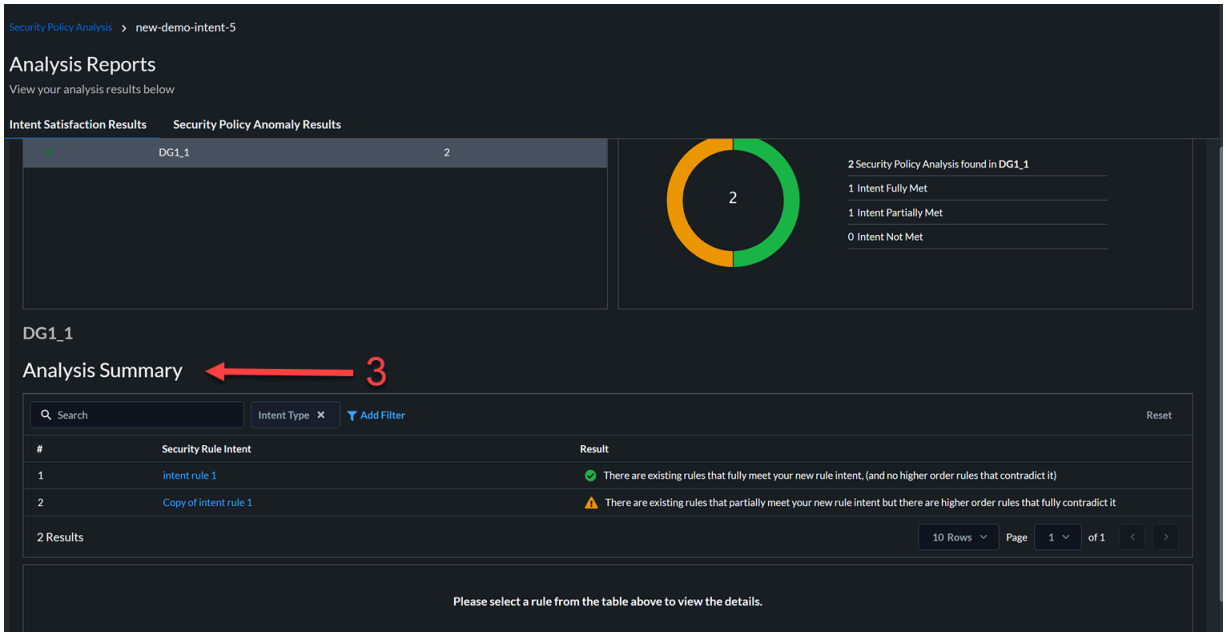
Résultats de satisfaction de l’intention

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.

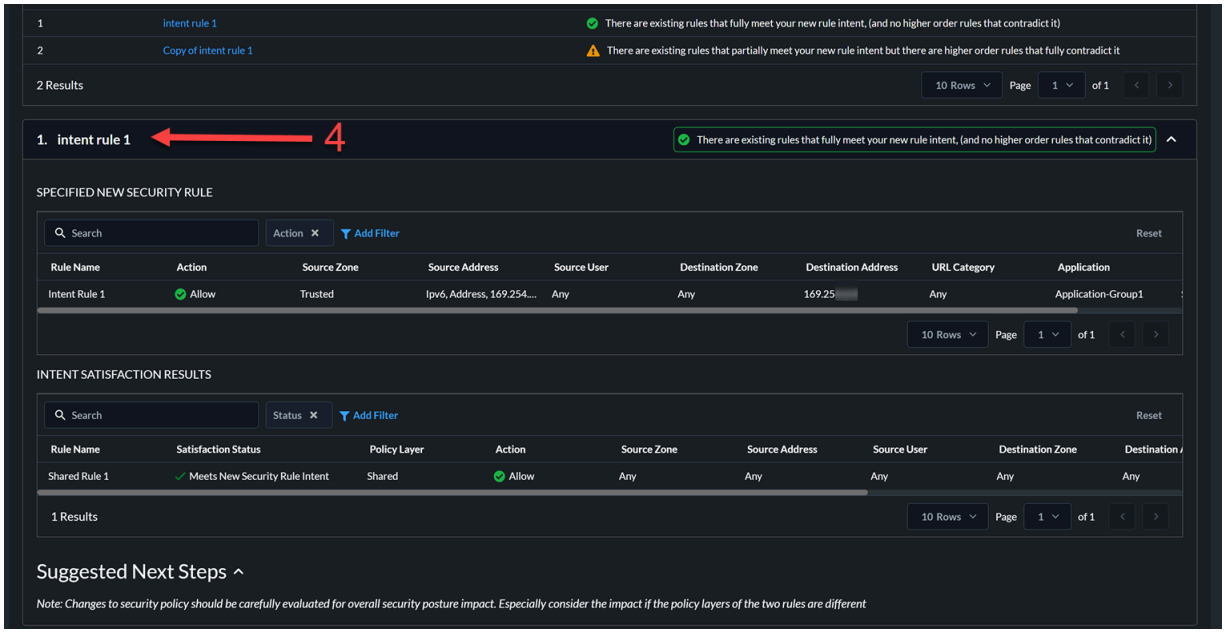


3. Affichez les résultats de l'analyse pour connaître l'intention de la nouvelle règle de sécurité.



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.



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.

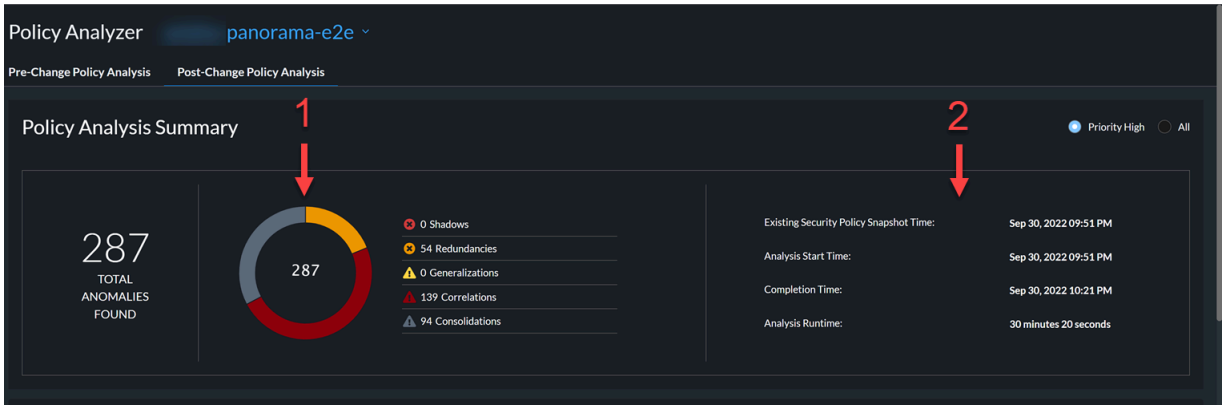
Analyse de politique post-modification

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)**.

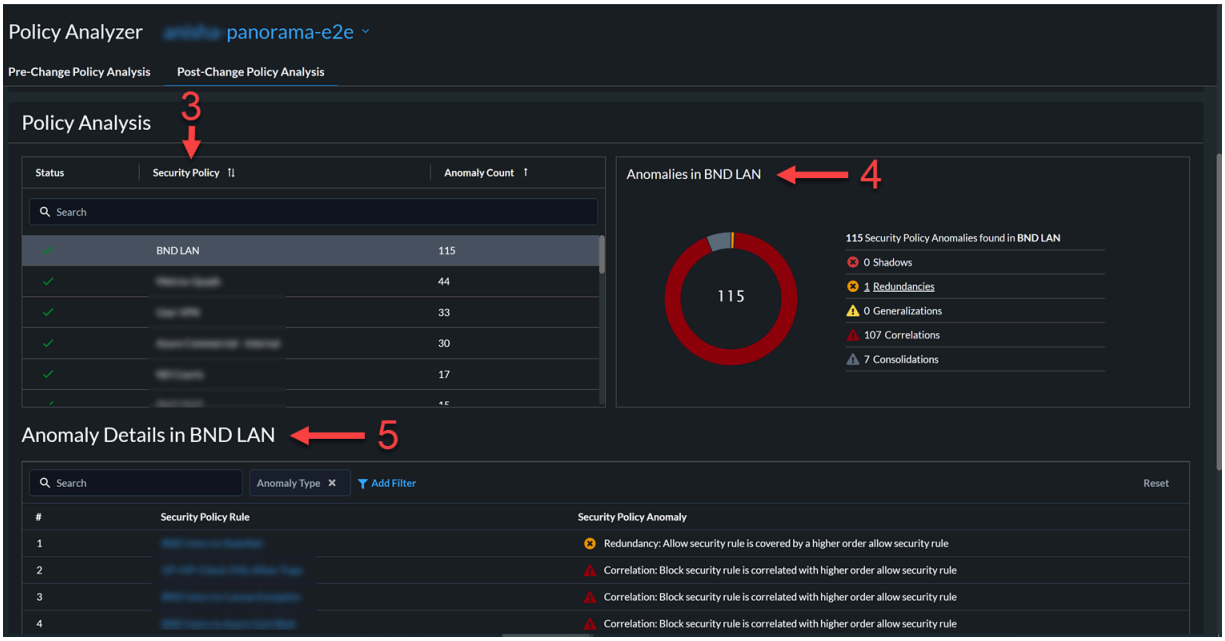
Vous pouvez consulter les informations suivantes :

1. 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.

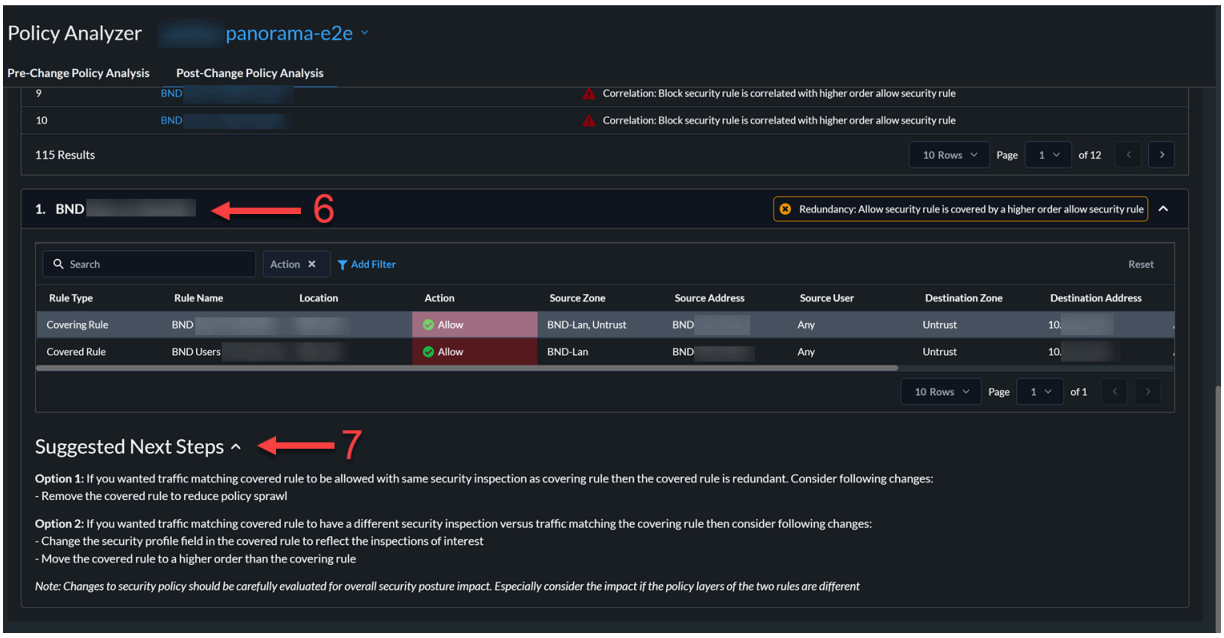


2. Horodatages pour l'analyse qui comprend :
   - Instantané de politique de sécurité existante : horodatage lorsque la configuration a été marquée comme étant exécutée dans Panorama après une validation.
   - Analyse de temps commencée
   - Analyse de temps terminée
   - Temps nécessaire pour terminer 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.



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



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.

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

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

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.

Obtenez des recommandations de mise à niveau

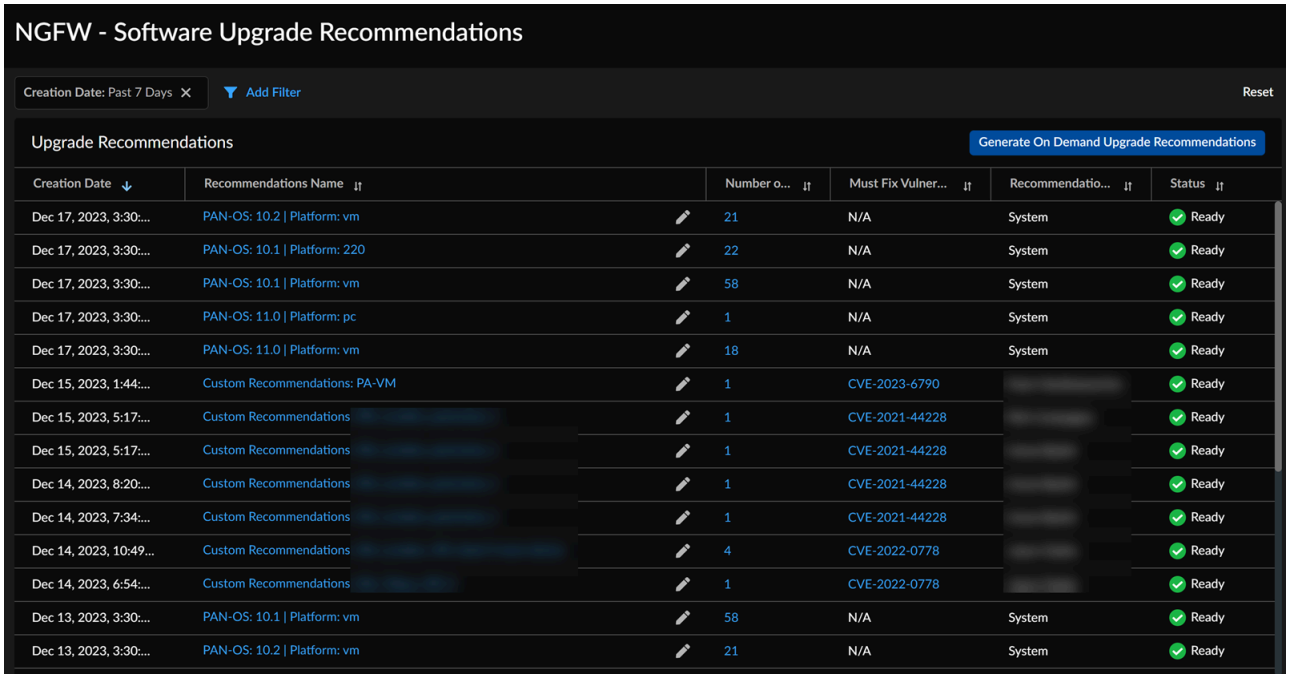
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• , y compris ceux financés par les crédits NGFW logiciels	❑ ou

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.



Vous pouvez effectuer les tâches suivantes pour chaque recommandation.

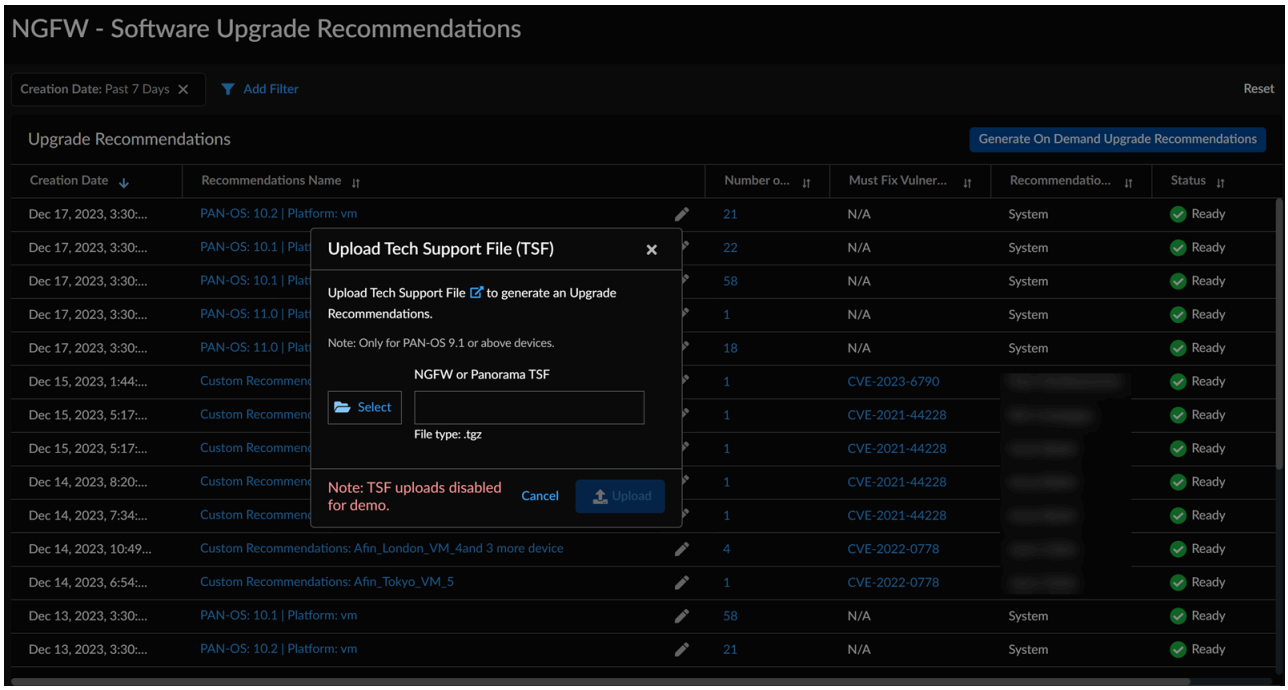
- Affichez le nombre de périphériques nécessitant une mise à niveau et les vulnérabilités à corriger.

- 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.*



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

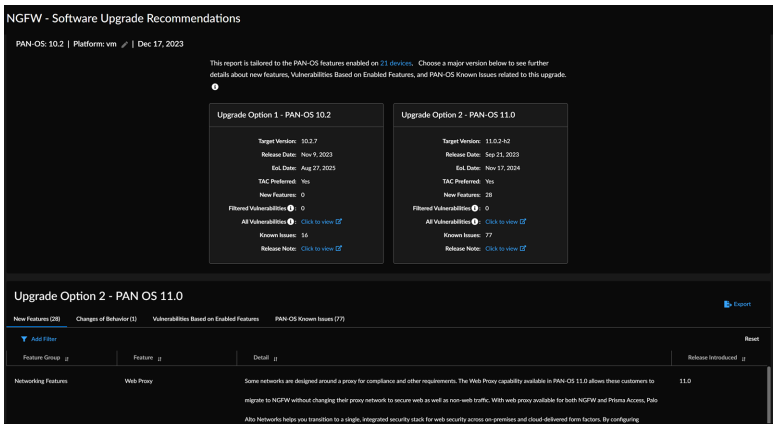
   Vous pouvez également consulter l'état pour voir s'il y a des erreurs liées au chargement, au format de fichier ou au traitement du fichier TSF.

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.*



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

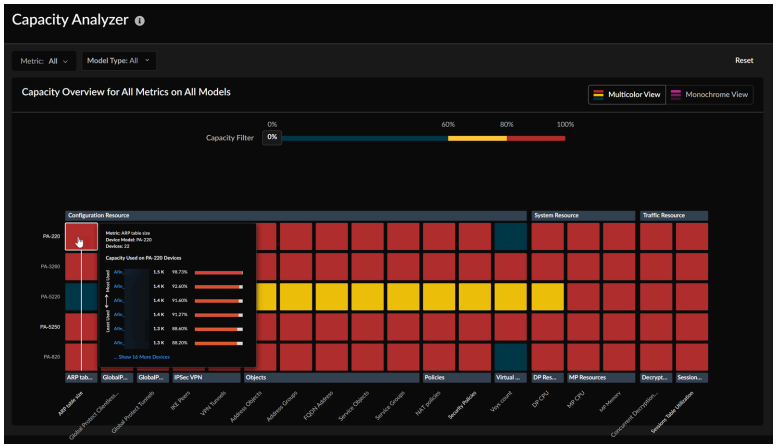
L'analyseur de capacité est amélioré pour prendre en charge les alertes qui vous aident à anticiper la consommation des ressources qui approche de leur capacité maximale et à déclencher des alertes. Voir Gérer les alertes de l'analyseur de capacité.

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

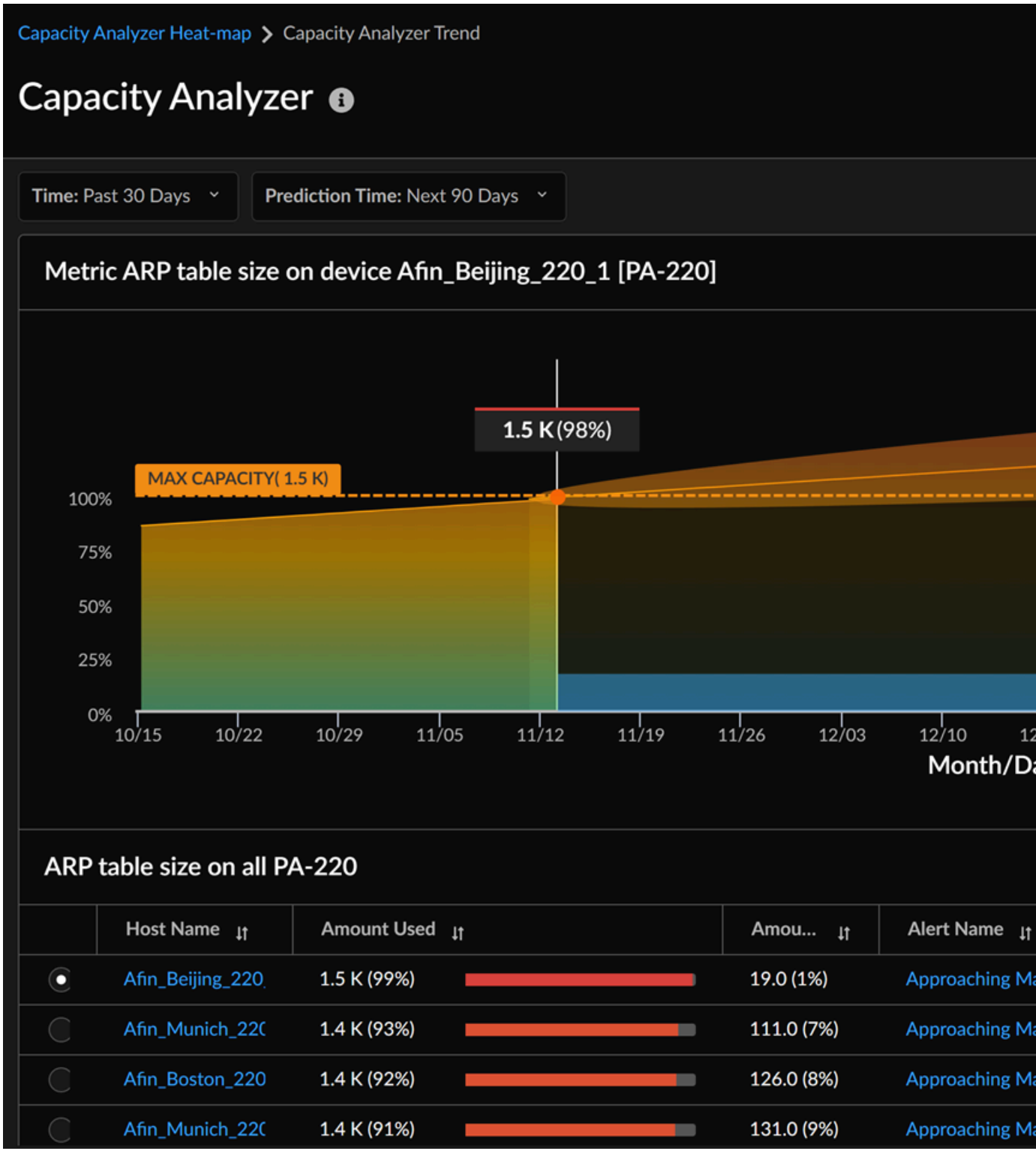
Analyser la capacité métrique en fonction de la métrique, du modèle et du périphérique

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**.

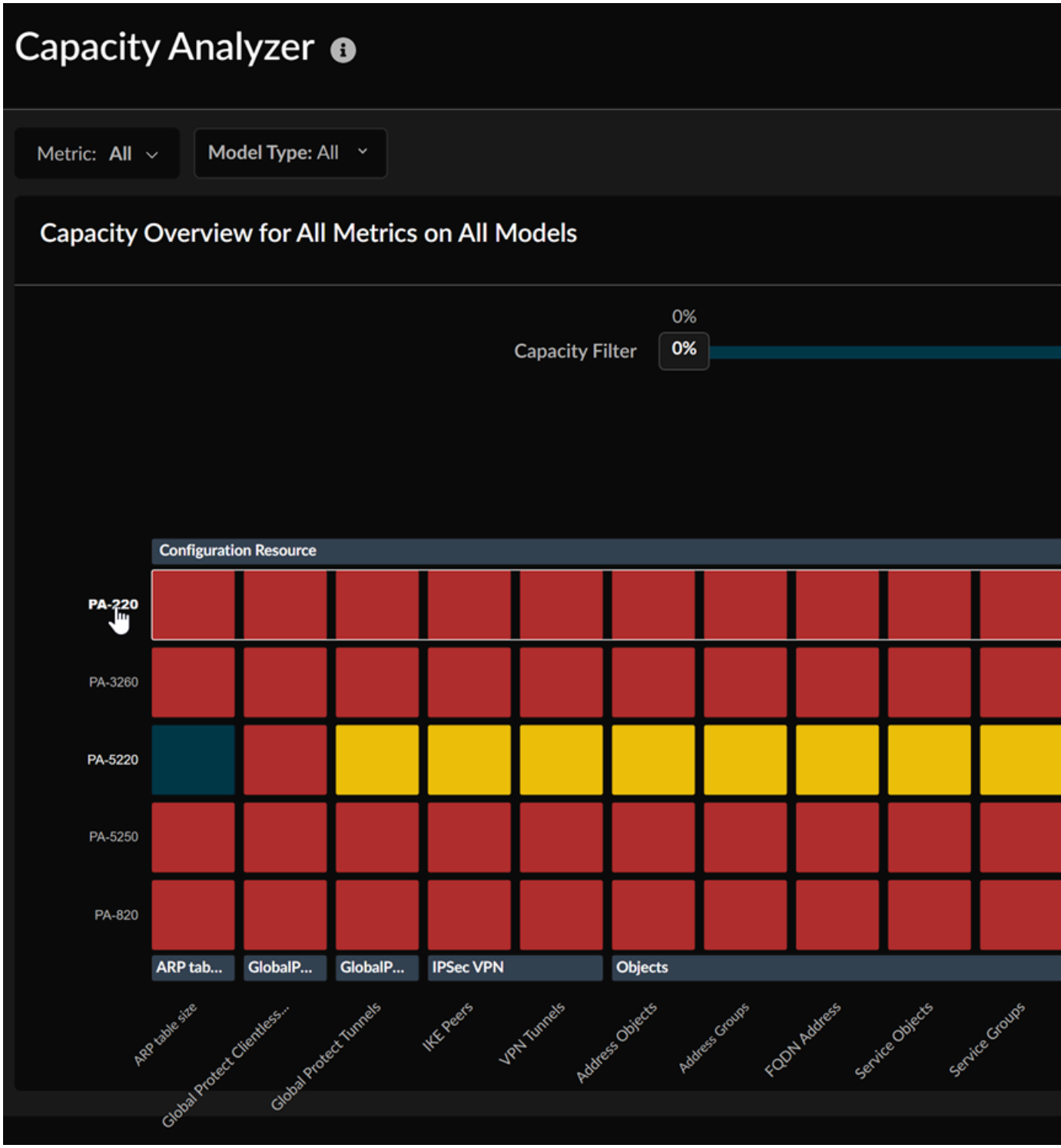


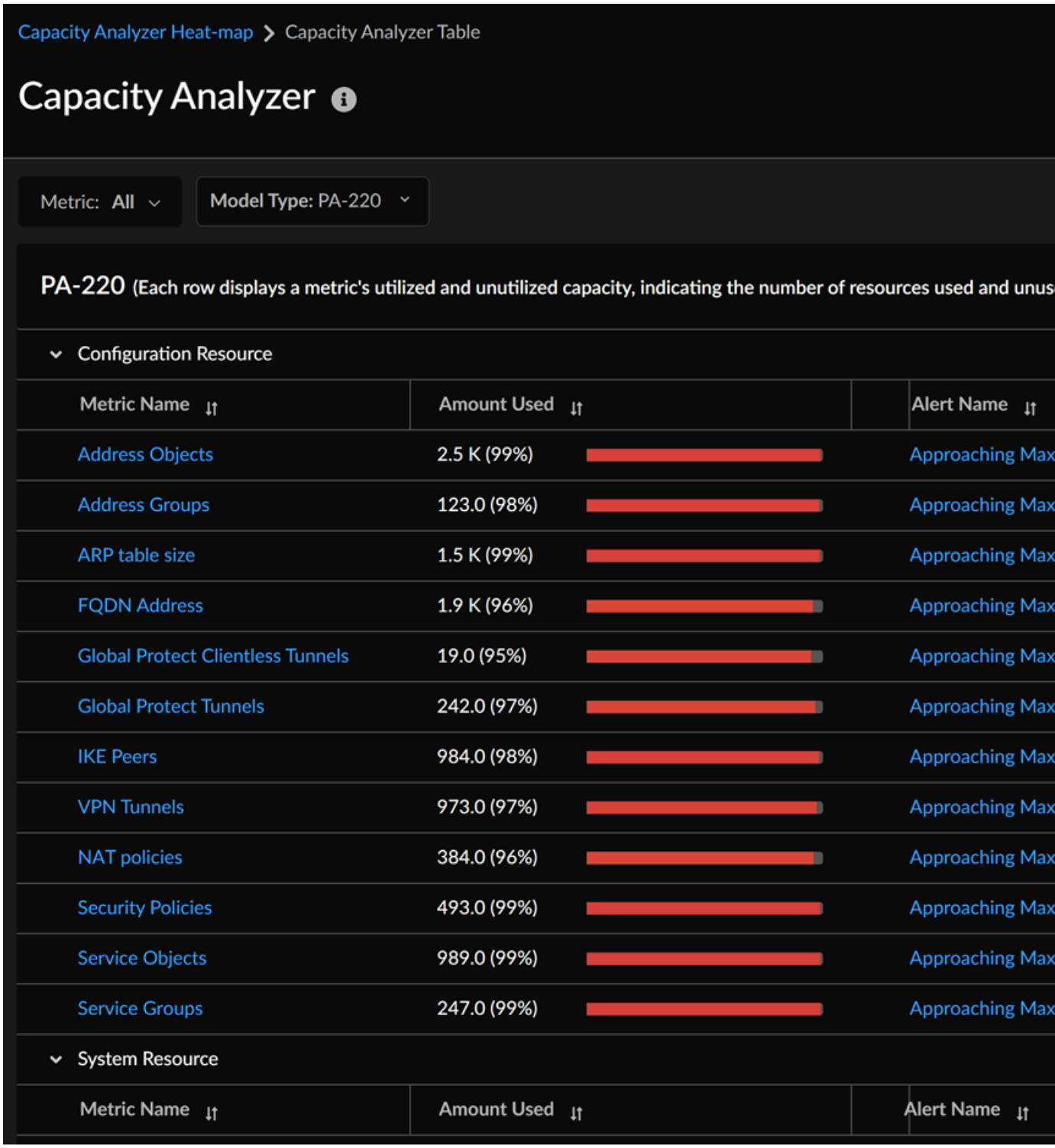
Vous pouvez consulter les éléments suivants :

- 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.





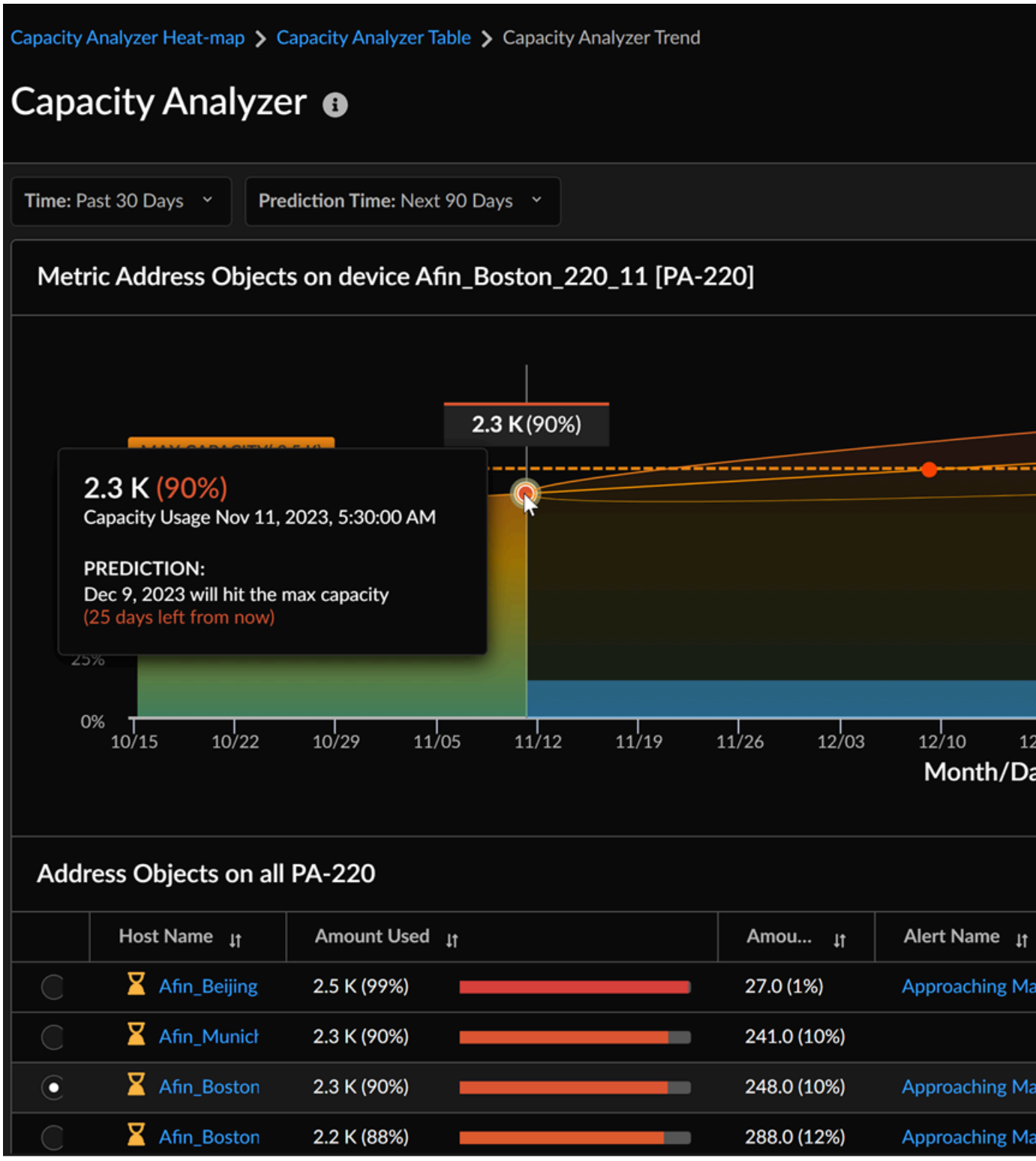
Chaque ligne affiche la capacité utilisée d'une métrique, indiquant le nombre de ressources utilisées pour cette métrique dans un périphérique. De plus, vous pouvez afficher les alertes déclenchées pour la métrique et la date à laquelle il est prévu que la métrique atteindra sa capacité maximale.

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.

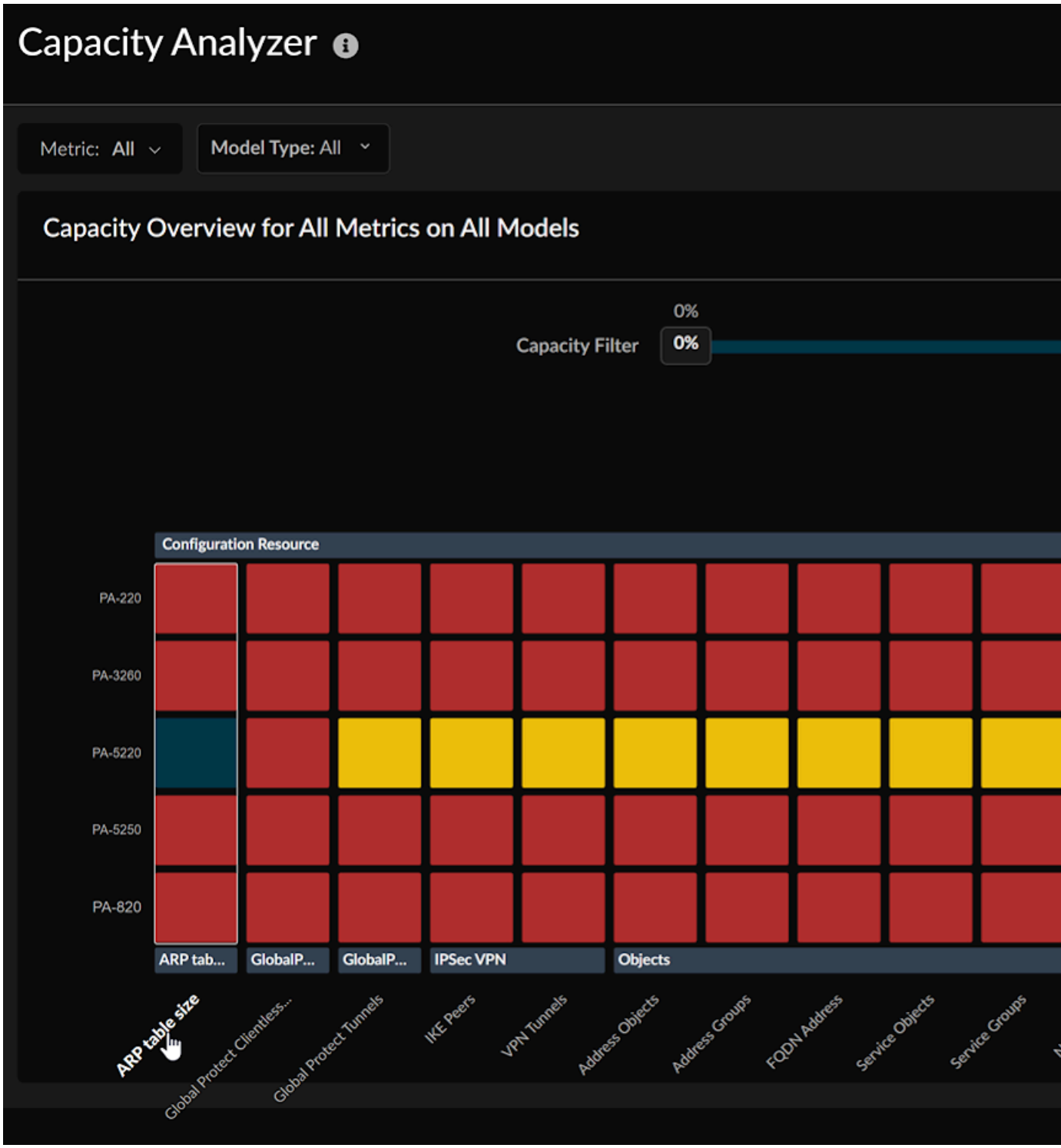


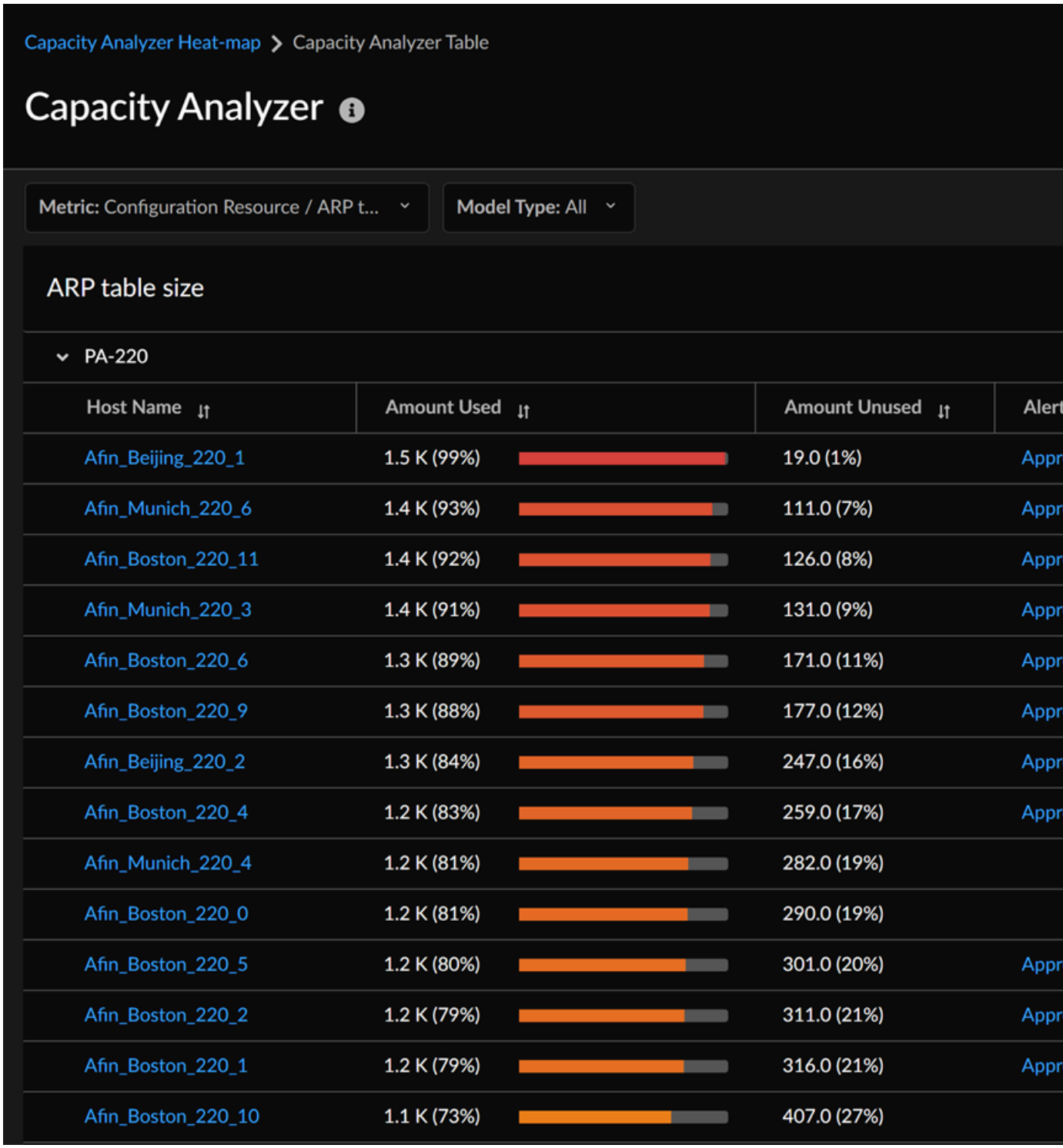
Sous **Nom de l'alerte**, vous pouvez afficher les alertes déclenchées pour la métrique d'objets d'adresse correspondant à un nom d'hôte.

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)****.*

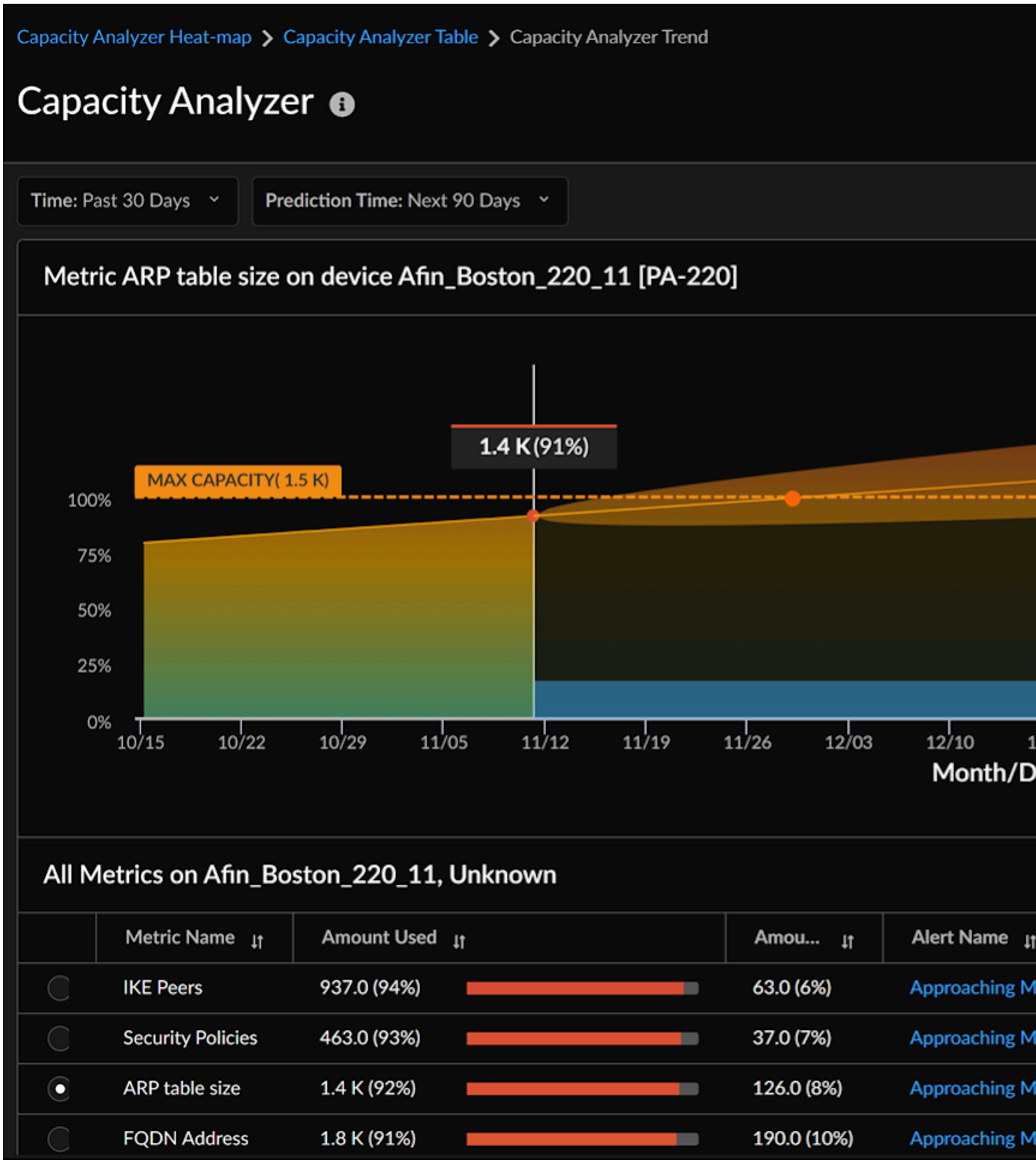




Chaque ligne affiche les métriques de la **taille de table ARP** utilisées et inutilisées pour chaque hôte sous les modèles de périphériques. En outre, vous pouvez afficher les alertes déclenchées pour cette métrique pour chaque hôte et la date à laquelle il est prévu que la métrique atteindra sa capacité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



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

Meilleures pratiques dans les NGFW

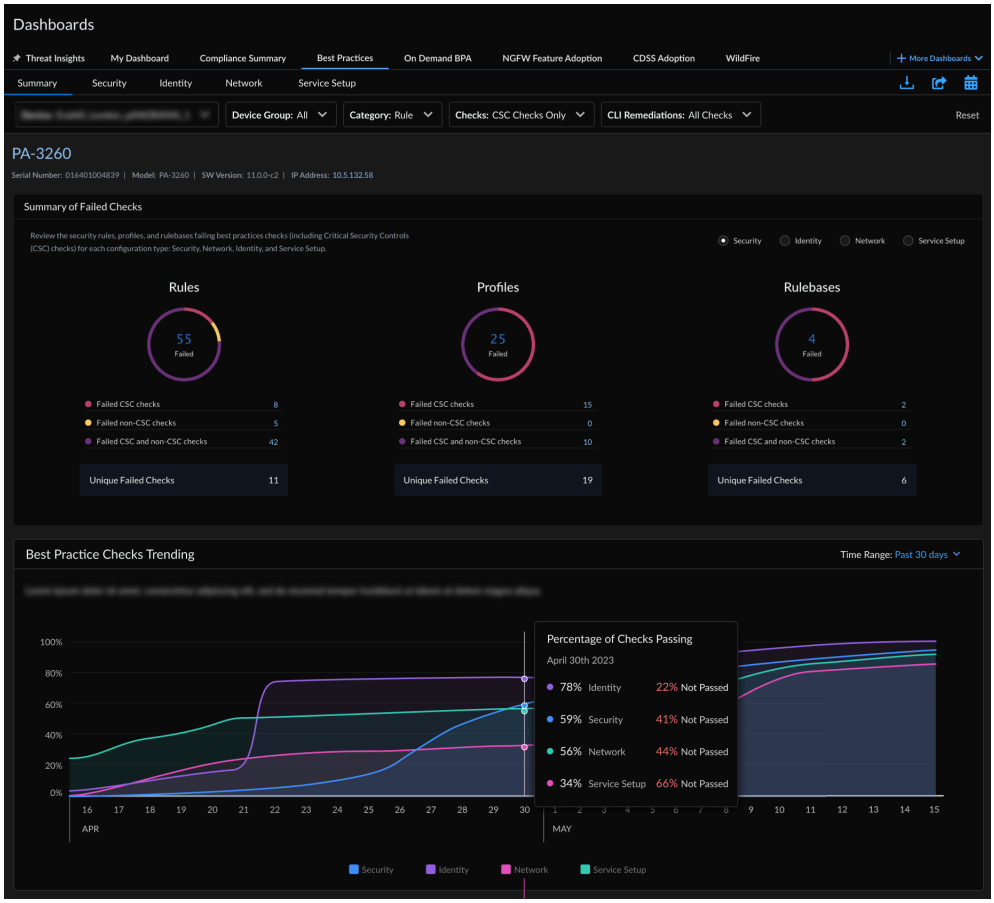
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• , y compris ceux financés par les crédits NGFW logiciels	L'une des options suivantes : ❑ ou ❑ ou

AIOps pour NGFW vous aide à renforcer la posture de sécurité en vous alignant sur les meilleures pratiques. Vous pouvez tirer parti d'AIOps 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. AIOps pour NGFW simplifie le processus de vérification de la conformité InfoSec sur votre infrastructure réseau.

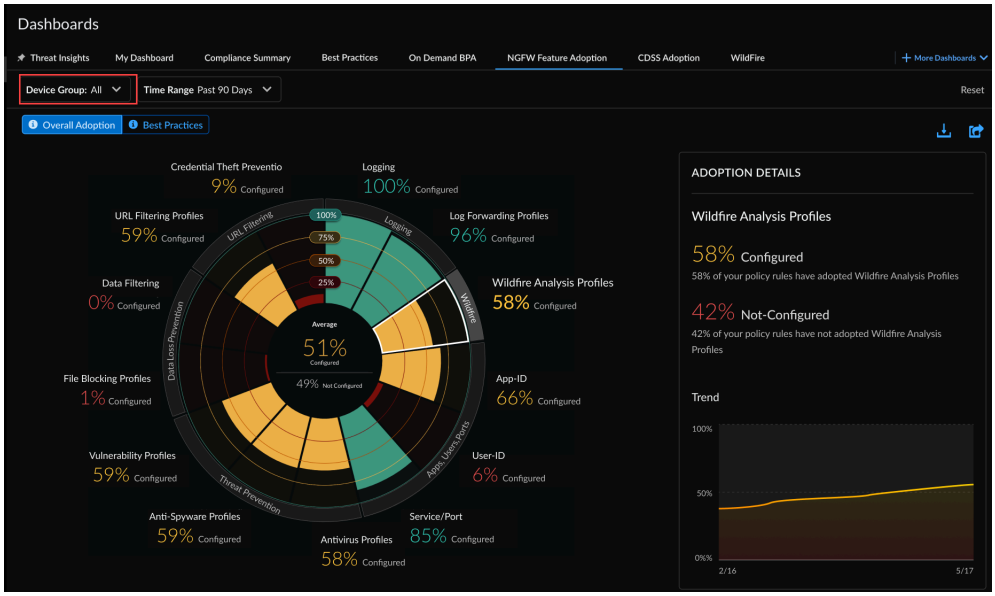
AIOps pour NGFW est gratuit, et les fonctionnalités d'évaluation des meilleures pratiques (BPA) d'AIOps suivantes sont disponibles sans licence AIOps Premium. Pour obtenir la liste complète des fonctionnalités des meilleures pratiques disponibles, voir Meilleures pratiques intégrées :

- 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.

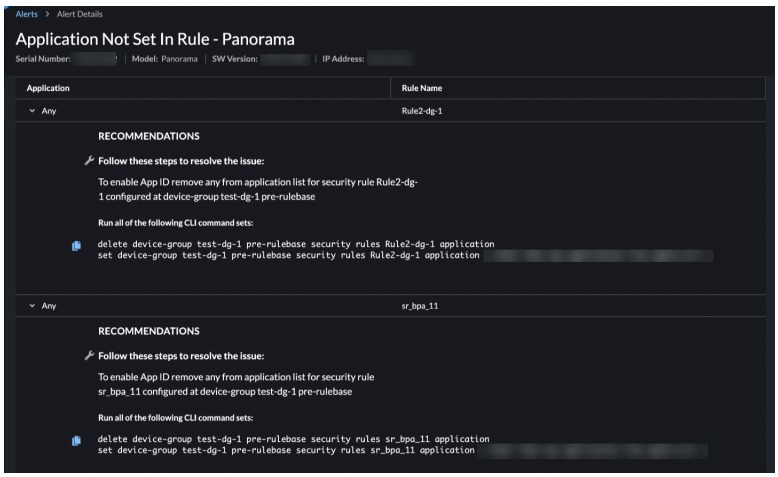


- Surveillez l'adoption des fonctionnalités et restez au courant des fonctionnalités de sécurité que vous utilisez dans votre déploiement et des lacunes potentielles dans la couverture.



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

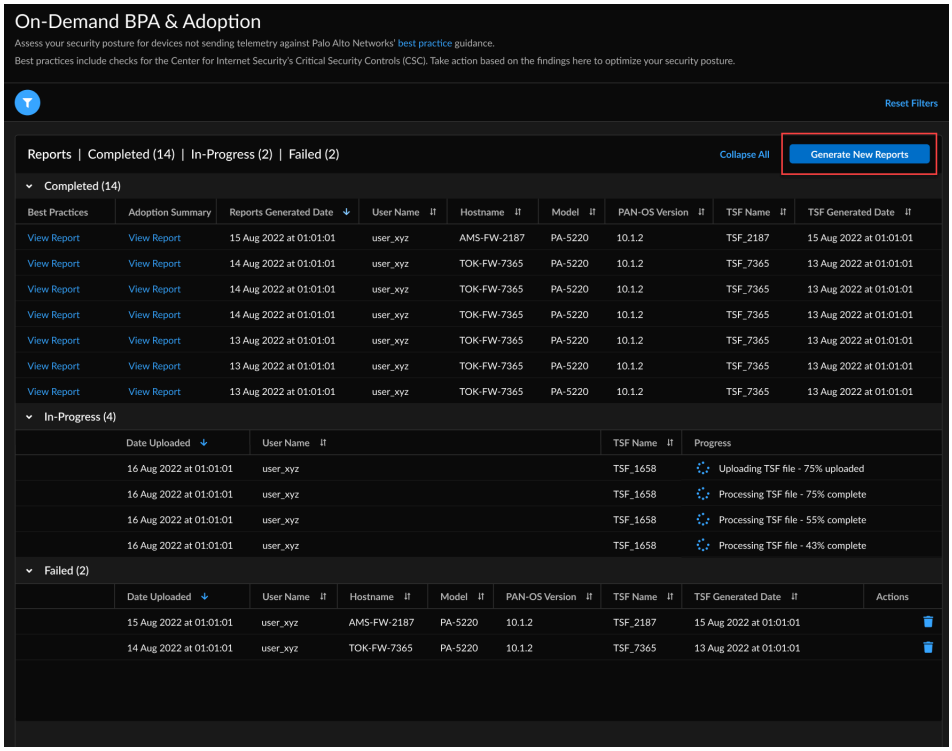
  Les corrections Command Line Interface (interface de ligne de commande - CLI) sont également disponibles dans AIOps pour NGFW sous **Alerts (Alertes)** > **Security (Sécurité)** > **Alert Details (Détails de l'alerte)**. Consultez les recommandations destinées à vous aider à corriger les problèmes qui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



  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.



Avec une licence Premium, AIOps 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

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 AIOps 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'AIOps, 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'AIOps.

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 AIOps 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.*

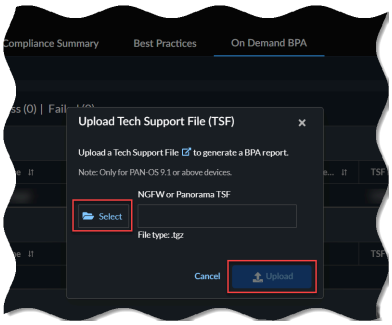
STEP 2 | Connectez-vous à votre instance AIOps pour NGFW activée. Les onglets suivants s'affichent, même sans Strata Logging Service :

- 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

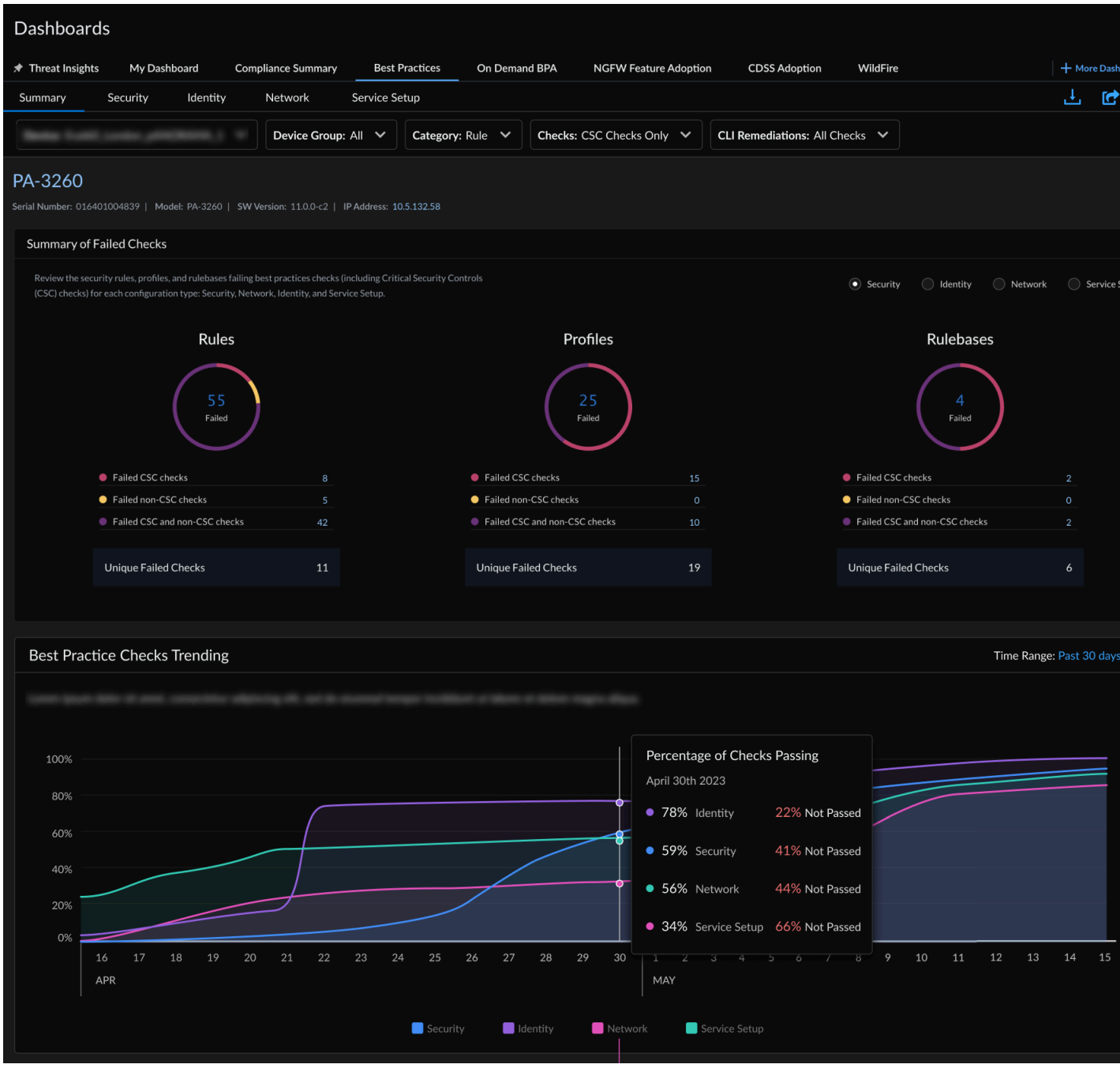
Que vous indique ce tableau de bord ?

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 :