paloalto
TECHDOCS

Mise en route de Strata Cloud Manager

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 6, 2025

Table of Contents

Présentation de Strata Cloud Manager

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Strata Cloud Manager de Palo Alto Networks vous offre une gestion et des opérations unifiées alimentées par l'IA pour l'ensemble de votre déploiement de sécurité réseau. Avec Strata Cloud Manager, vous pouvez facilement gérer l'ensemble de votre infrastructure de sécurité réseau Palo Alto Networks (vos environnements NGFW et SASE) à partir d'une interface utilisateur unique et rationalisée. Obtenez une vue d'ensemble des utilisateurs, des sites de filiales, des applications et des menaces sur tous les points d'application de la sécurité du réseau ; cela vous permet d'obtenir des informations exploitables, d'améliorer la sécurité et de faciliter le dépannage et la résolution des problèmes.

❑ **Prévoir et prévenir les perturbations du réseau**

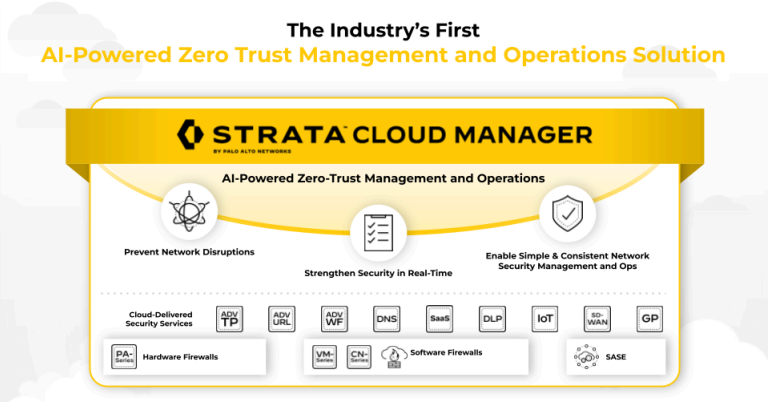
Strata Cloud Manager prédit et prévient les interruptions de réseau et résout rapidement les problèmes, afin que vous et vos utilisateurs puissiez continuer vos activités quotidiennes et rester productifs.

❑ **Renforcer la sécurité grâce aux meilleures pratiques en temps réel**

Strata Cloud Manager identifie les fonctionnalités de sécurité essentielles et sous-utilisées, et vous guide pour les activer sur la base des meilleures pratiques qui correspondent à vos besoins. Renforcez votre posture de sécurité grâce aux meilleures pratiques intégrées et aux fonctionnalités de remédiation en ligne optimisées par AIOps.

❑ **Gestion et opérations simples et cohérentes de la sécurité du réseau**

Strata Cloud Manager consolide vos outils de sécurité pour améliorer le fonctionnement et la visibilité, vous permettant ainsi d'adopter une expérience de gestion simple et cohérente pour l'ensemble de la pile de sécurité de votre réseau.



Renforcement de la sécurité grâce à Strata Cloud Manager

Maximiser l'utilisation des capacités de sécurité

- Découvrez les fonctionnalités de sécurité que vous utilisez et identifiez les failles dans l'adoption des fonctionnalités de sécurité dont vous pourriez tirer parti. → Adoption des fonctionnalités
- Consultez les taux d'adoption de vos abonnements aux services de sécurité. → Adoption du CDSS
- Découvrez comment vos fonctionnalités de sécurité respectent les meilleures pratiques ou où vous pouvez apporter des améliorations pour renforcer votre posture de sécurité.→ meilleures pratiques intégrées

Renforcer et optimiser la configuration existante

Améliorer et rationaliser votre politique de sécurité en fonction des données d'utilisation et des recommandations générées automatiquement.

- Supprimez les objets qui ne sont pas référencés dans la politique et les règles qui n'ont aucun impact sur le trafic. Ces objets et ces règles peuvent entraver les performances et compliquer la gestion de la politique. → Nettoyage de la configuration
- Les règles trop permissives introduisent des failles de sécurité, car elles autorisent des applications qui ne sont pas utilisées sur votre réseau. L'optimiseur de politique vous permet de convertir ces règles trop permissives en règles plus spécifiques et ciblées qui n'autorisent que les applications que vous utilisez réellement. → Optimiseur de politique

Guide en temps réel pour une configuration sécurisée

- Les garde-fous des meilleures pratiques vous permettent de valider en direct que vos règles de politique de sécurité sont conformes aux meilleures pratiques. → Vérifications de configuration en direct et en ligne des meilleures pratiques

Stratégies de Strata Cloud Manager pour prévoir et prévenir les perturbations du réseau

Une observabilité complète

- Découvrez comment votre réseau est protégé par l'infrastructure de sécurité. → Centre de commande
- Connaître l'état et les performances des utilisateurs, des sites distants, des applications et de l'infrastructure informatique, à partir de

  un seul tableau de bord. → Tableau de bord de l'état du SASE
- Consultez l'état et les performances des périphériques à partir d'un seul tableau de bord. → Tableau de bord de l'état du périphérique

Prévoir les perturbations et y remédier

Les prévisions automatiques préviennent les perturbations potentielles. Lorsque des problèmes sont détectés, des informations exploitables accélèrent la résolution des problèmes.

- Prédiction assistée par machine des pannes imminentes, avec recommandations pour les étapes de remédiation. → Prévisions et détection des défaillances
- Réduisez le temps de résolution grâce à l'analyse des causes probables. → Voir les causes probables

Élaborer un plan pour répondre à l'évolution des besoins en matière de sécurité

- Améliorez la stabilité en identifiant de manière proactive la capacité potentielle. Analyseur de capacité →

Découvrez comment Strata Cloud Manager fonctionne partout de manière cohérente

Configuration conforme

Appliquez des politiques conformes à tous les points d'application avec des processus rationalisés, et éliminez le besoin d'apporter des modifications individuelles pour les déploiements NGFW et SASE.

- Configurer et intégrer les NGFW, les utilisateurs mobiles Prisma Access et les réseaux distants, et planifier les mises à jour logicielles pour les NGFW. → Flux de travail dans Strata Cloud Manager
- Configurez une politique de sécurité partagée entre vos NGFW et Prisma Access. → Gestion partagée pour NGFW et Prisma Access

Organisation flexible de la configuration

Simplifiez la gestion de la configuration à grande échelle grâce à des flux de travail simples de gestion des dossiers et des périphériques.

- Appliquez les paramètres de configuration et renforcez la politique de manière globale dans l'ensemble de votre environnement, ou ciblez les paramètres et la politique sur certaines parties de votre organisation. → Portée de la configuration
- Regroupez logiquement vos pare-feu ou types de déploiement (utilisateurs mobiles Prisma Access, réseaux distants ou connexions de service) pour une gestion simplifiée de la configuration. → Gestion des dossiers
- Regroupez les configurations que vous pouvez rapidement pousser vers vos pare-feu ou déploiements. → Extraits
- Vous avez la possibilité de prendre en compte des valeurs de configuration uniques spécifiques à un périphérique ou à un déploiement. → Variables

Obtenez une visibilité unifiée sur les menaces

- Bénéficiez d'une visibilité complète sur le trafic réseau, les abonnements, les utilisateurs, les applications, les réseaux, les menaces, etc. Surveillance →
- Obtenez une vue interactive des applications, des périphériques ION, des menaces, des utilisateurs et des abonnements de sécurité utilisés dans votre réseau. Les tableaux de bord fournissent une visibilité sur l'état, la posture de sécurité et l'activité de votre déploiement, ce qui vous aide à prévenir ou à résoudre les lacunes en matière de performances et de sécurité de votre réseau.→ Tableaux de bord
- Obtenez des rapports sur les modèles de trafic réseau, l'utilisation de la bande passante, vos données d'abonnement à la sécurité et bien plus encore. Les rapports fournissent des informations exploitables sur votre réseau que vous pouvez utiliser à des fins de planification et de surveillance.→ Rapports

Produits pris en charge par Strata Cloud Manager

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Strata Cloud Manager fournit une gestion et des opérations unifiées et alimentées par l'IA pour votre réseau NGFW et SASE, et les fonctionnalités de Strata Cloud Manager disponibles dépendent de vos licences. Voici les licences qui permettent à Strata Cloud Manager de gérer les NGFW et SASE, et de débloquer les fonctionnalités de sécurité réseau Strata Cloud Manager. → Voici comment valider vos licences

Table 1:

Strata Cloud Manager Essentials	Strata Cloud Manager Essentials offre des fonctionnalités de gestion et de sécurité, et ces fonctionnalités sont disponibles gratuitement avec : • Pare-feu nouvelle génération (NGFW) • Prisma Access Strata Logging Service est disponible en option pour Strata Cloud Manager Essentials. *Strata Cloud Manager Essentials et Strata Cloud Manager Pro sont disponibles pour activer dans les comptes du portail de support client (CSP) qui n'ont pas : Strata Logging Service avec stockage de taille, AIOps pour NGFW Free ou Premium, ou Prisma Access.*
Strata Cloud Manager Pro	Strata Cloud Manager Pro est le niveau payant qui comprend toutes les fonctionnalités de Strata Cloud Manager Essentials,

	ainsi que des fonctionnalités avancées pour améliorer la santé opérationnelle, prévenir les perturbations du réseau, renforcer la posture de sécurité en temps réel et la gestion autonome de l'expérience numérique (ADEM) pour surveiller les performances de l'expérience utilisateur. Strata Cloud Manager Pro inclut Strata Logging Service avec un an de conservation des journaux et un stockage illimité, permettant une journalisation centralisée et une récupération transparente des données dans l'ensemble de votre déploiement. Vous pouvez acheter Strata Cloud Manager Pro pour les produits suivants : • Pare-feu nouvelle génération (NGFW) • VM-Series financée par Crédits NGFW logiciels • Prisma Access
AIOps pour NGFW Premium	Pour les NGFW titulaires d'une licence AIOps pour NGFW Premium, Strata Cloud Manager vous donne une vue globale de la santé et de la sécurité de vos NGFW, et peut imposer des contrôles proactifs pour combler les lacunes de sécurité. • **NGFW (Managed by PAN-OS or Panorama)** → Pour les NGFW gérés par PAN-OS et Panorama avec une licence AIOps pour NGFW Premium, utilisez Strata Cloud Manager pour superviser votre santé de déploiement et votre posture de sécurité. • **NGFW (Managed by Strata Cloud Manager)** → Avec une licence AIOps pour NGFW, vous pouvez également utiliser Strata Cloud Manager pour la **gestion du cloud des NGFW**. • *Contactez l'équipe de votre compte pour activer la gestion Cloud pour NGFWs à l'aide de Strata Cloud Manager.* • *Strata Cloud Manager offre une gestion et des opérations unifiées uniquement pour les NGFW utilisant la licence AIOps pour NGFW Premium. Continuez à utiliser l'application AIOps pour NGFW Free pour les NGFW embarqués sur AIOps pour NGFW Free.*
Crédits NGFW logiciels	Pour les VM-Series financées avec des crédits NGFW Software, Strata Cloud Manager prend en charge les fonctionnalités AIOps pour NGFW Premium, y compris la gestion du cloud pour les NGFW.

Prisma Access	Il existe deux façons de gérer Prisma Access : vous pouvez utiliser Strata Cloud Manager ou Panorama. Strata Cloud Manager fournit des fonctionnalités de visibilité Prisma Access. Celles-ci sont prises en charge quelle que soit l'interface de gestion que vous utilisez. Cela signifie que si vous utilisez Panorama pour gérer Prisma Access, vous pouvez toujours utiliser Strata Cloud Manager pour une surveillance complète de l'environnement Prisma Access. **Prisma Access (Managed by Strata Cloud Manager)** Utilisez Strata Cloud Manager pour l'intégration, la gestion et la surveillance complètes de votre environnement Prisma Access. Cela inclut l'utilisation de Strata Cloud Manager pour gérer et surveiller les services de sécurité fournis dans le cloud inclus avec Prisma Access. Strata Cloud Manager vous offre une surveillance, des alertes et une visibilité complètes sur votre environnement Prisma Access : • DEM autonome • Surveiller Prisma Access dans Strata Cloud Manager • Tableaux de bord Strata Cloud Manager Surveillance de • Strata Cloud Manager • Strata Cloud Manager Reports **Prisma Access (Managed by Panorama)** Si vous utilisez Panorama pour gérer Prisma Access, vous devez continuer à utiliser Panorama pour gérer votre environnement. Cependant, vous pouvez utiliser Strata Cloud Manager pour une surveillance complète, des alertes et une visibilité sur votre environnement Prisma Access : • DEM autonome alimenté par l'IA • Surveiller Prisma Access dans Strata Cloud Manager • Surveillance du tableau de bord Strata Cloud Manager • Strata Cloud Manager • Rapports Strata Cloud Manager
ADEM alimenté par l'IA	ADEM alimenté par l'IA est une licence complémentaire Prisma Access qui automatise les opérations informatiques complexes, pour augmenter la productivité et réduire le temps de résolution des problèmes. Strata Cloud Manager prend en charge ADEM alimenté par l'IA pour tous les utilisateurs Prisma Access (à la fois Panorama - Managed Prisma Access et Prisma Access Cloud Management).

	Si vous utilisez Panorama pour gérer Prisma Access, vous devez continuer à utiliser Panorama pour gérer votre environnement et pouvez utiliser Strata Cloud Manager pour la surveillance ADEM.
Prisma SD-WAN	Utilisez Strata Cloud Manager pour Prisma SD-WAN. Prisma SD-WAN est un service fourni dans le cloud qui met en œuvre un SD-WAN autonome et défini par des applications pour vous aider à sécuriser et connecter vos succursales, centres de données et grands sites de campus sans augmenter les coûts et la complexité. L'AppFabric connecte vos sites en toute sécurité avec la sensibilisation aux applications et vous donne la liberté d'utiliser n'importe quel WAN, n'importe quel cloud pour une solution de branche mince (sécurité depuis le cloud).
Services de sécurité fournis par le cloud (CDSS) : • **Prévention avancée des menaces** • **URL Filtering avancé** • **Advanced WildFire** • **Sécurité DNS** • **Enterprise DLP** • **IoT Security** • **Sécurité SaaS**	Si vous possédez une licence Prisma Access ou une licence AIOps pour NGFW Premium, vous pouvez utiliser Strata Cloud Manager pour gérer et surveiller vos abonnements de sécurité. Strata Cloud Manager offre les protections que vos abonnements de sécurité fournissent de manière cohérente dans le trafic de votre entreprise. Les fonctionnalités de Strata Cloud Manager mises à votre disposition pour les abonnements de sécurité dépendent de votre licence et peuvent inclure : • Des tableaux de bord et rapports Strata Cloud Manager • Gestion unifiée de Strata Cloud Manager pour les abonnements de sécurité. Si vous utilisez Strata Cloud Manager pour appliquer une politique de sécurité partagée entre les NGFW et/ou Prisma Access, vous pouvez utiliser une configuration unique et centralisée pour vos abonnements de sécurité.

Aperçu de Strata Cloud Manager

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Ceci est un premier aperçu de Strata Cloud Manager. L'interface utilisateur de Strata Cloud Manager fournit une vue complète de votre réseau et vous offre un flux de travail unifié pour gérer les NGFW et SASE. Parcourez la nouvelle navigation simplifiée et cohérente pour interagir avec toutes les données de votre réseau, obtenez des informations exploitables qui apparaissent automatiquement. Gérez et surveillez collectivement Prisma Access, vos NGFW et vos services de sécurité fournis par le cloud.

Explorez chaque menu de la barre de navigation de gauche. Ces chemins sont désormais standard pour tous les produits ou abonnements Palo Alto Networks que vous utilisez avec Strata Cloud Manager. Cela permet de faciliter :

- l'adoption de nouvelles fonctionnalités et abonnements
- l'intégration de nouveaux utilisateurs, périphériques, sites ou emplacements

car ils s'intégreront parfaitement dans votre configuration de gestion existante.

Important

Les fonctionnalités à votre disposition dans Strata Cloud Manager dépendent de vos abonnements Produits pris en charge par Strata Cloud Manager. *Vous pouvez consulter la documentation Strata Cloud Manager pour connaître les licences requises pour les fonctionnalités Strata Cloud Manager.*

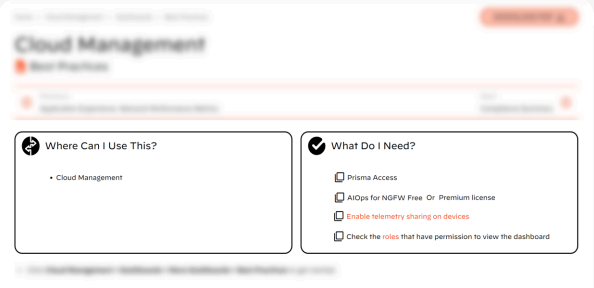
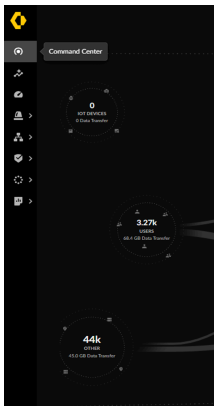
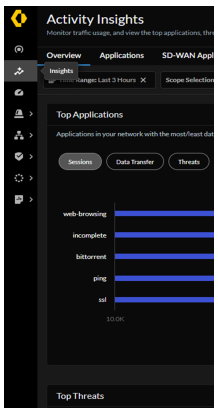
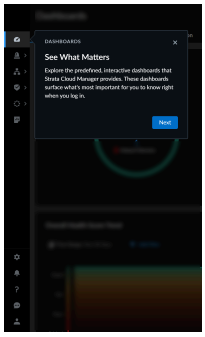
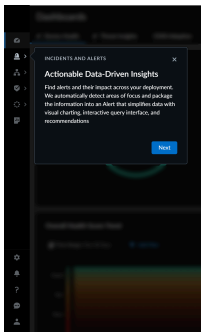
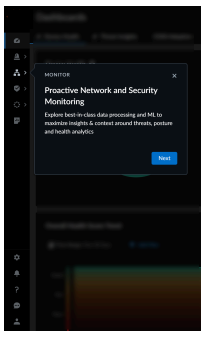
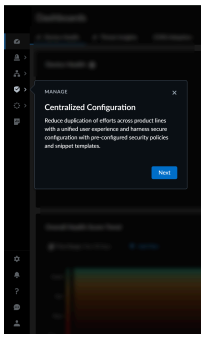
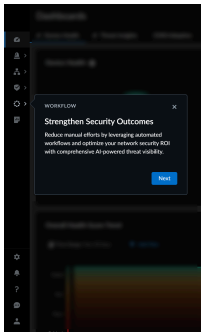
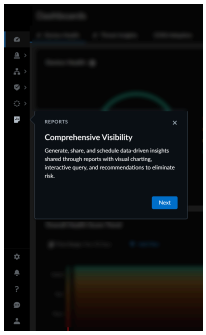
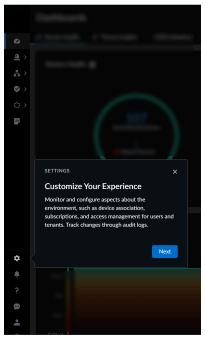


Table 2:

Centre de commande	**Votre premier arrêt pour évaluer l'état, la sécurité et l'efficacité de votre réseau** Le centre de commande est une vue d'ensemble de votre réseau et de votre infrastructure de sécurité. Il vous offre quatre vues différentes, chacune avec ses propres données suivies, ses métriques et ses informations exploitables à examiner et à utiliser. • Centre de commande : Strata Cloud Manager	
Informations sur l'activité	**Données unifiées sur le réseau, en un seul endroit** L'outil information sur l'activité vous offre une vue détaillée de vos activités réseau sur les déploiements Prisma Access et NGFW. L'outil information sur l'activité unifie vos données réseau telles que le trafic réseau, l'utilisation des applications, les menaces et les activités des utilisateurs en un seul endroit. • Informations : Informations sur l'activité	

Tableaux de bord	**Voir ce qui compte, tout de suite** Les tableaux de bord font apparaître ce qu'il est le plus important que vous sachiez, dès que vous vous connectez. Chaque tableau de bord est conçu pour mettre en évidence les domaines dans lesquels vous pouvez prendre des mesures pour améliorer votre posture de sécurité ou l'état de votre réseau. Explorez tous les tableaux de bord prédéfinis et interactifs fournis, ainsi vous pourrez épingler vos favoris. • Tableaux de bord : Strata Cloud Manager	
Incidents et alertes	**Informations exploitables basées sur des données** Strata Cloud Manager fournit un cadre unifié d'incidents et d'alertes. À partir d'un même point, vous pouvez visualiser, étudier et traiter les alertes ainsi que les incidents sur votre réseau, et accéder à vos journaux pour examiner l'activité associée. • Incidents et alertes : Strata Cloud Manager	
Surveiller	**Surveillance proactive du réseau et de la sécurité** Surveillez la santé et la sécurité de tout ce qui se trouve sur votre réseau et utilisez la recherche IoC pour étudier l'historique d'un artefact sur votre réseau et examiner les résultats de l'analyse globale. En fonction des abonnements et des produits que vous utilisez, vous pouvez surveiller : • Périphériques NGFW • Prisma Access • Applications • Utilisateurs • Sites de succursales • Centres de données	

	• Services réseau (comme GlobalProtect et DNS) • Vos abonnements Palo Alto Networks • Vos emplacements Prisma Access • Actifs • Prisma SD-WAN	
Gestion	**Configuration centralisée** Gérez une politique partagée pour l'ensemble de vos produits et abonnements de sécurité réseau ; dès le premier jour, vous pouvez démarrer avec une configuration sécurisée basée sur des politiques et des paramètres de meilleures pratiques prédéfinis, ainsi que sur des contrôles de meilleures pratiques en ligne. • Gestion : NGFW et Prisma Access • Gestion : Recommandation en matière de politique IoT • Gestion : Enterprise DLP • Gestion : Sécurité SaaS	
Flux de travail	**Renforcer les résultats en matière de sécurité** Lorsque vous accédez pour la première fois à vos flux de travail, le tableau de bord **Découverte** affiche les actions critiques et recommandées que vous pouvez entreprendre pour améliorer la posture de sécurité ou optimiser votre gestion de configuration, dès qu'elles sont à votre disposition. Continuez ici pour configurer et embarquer les NGFW, les utilisateurs mobiles Prisma Access et les réseaux distants, puis planifiez les mises à jour logicielles pour les NGFW. • Configurer Prisma Access • Configurer les NGFW	

	• Planificateur de mise à jour logicielle (AIOps pour NGFW)	
Rapports	**Visibilité complète** Générez, partagez et planifiez des informations basées sur les données partagées via des rapports avec des graphiques visuels, des requêtes interactives et des recommandations afin d'éliminer les risques. • Rapports : Strata Cloud Manager	
Paramètres	**Paramètres d'accueil et d'activation** Il s'agit des paramètres auxquels vous souhaiterez faire référence lorsque vous ajouterez de nouveaux utilisateurs, de nouvelles licences ou de nouveaux administrateurs, ou même lorsque vous commencerez à utiliser la fonctionStrata Cloud Manager: • Abonnements • Locataires • Associations de périphériques • Identité et accès • Journaux d'audit	

Lancement de Strata Cloud Manager

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

L'appli Strata Cloud Manager est disponible sur le hub Palo Alto Networks, et vous pouvez y accéder directement sur stratacloudmanager.paloaltonetworks.com.

Une licence Prisma Access, une licence AIOps pour NGFW Premium ou une licence Prisma SD-WAN est une exigence de base pour une gestion et des opérations unifiées Strata Cloud Manager. Si vous disposez d'au moins une de ces licences, vous pouvez accéder à Strata Cloud Manager pour avoir une visibilité sur votre/vos produit(s) ou le(s) gérer.

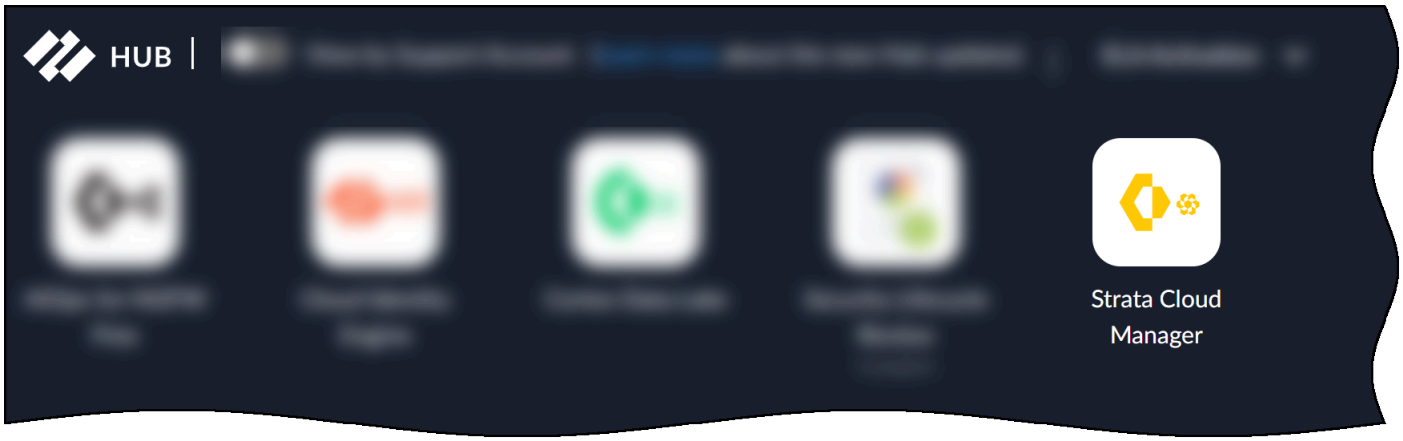
Si vous possédez plus d'une de ces licences, Strata Cloud Manager vous offre une interface unique pour interagir avec ces produits, ainsi que des licences supplémentaires ou des abonnements complémentaires (comme vos abonnements de sécurité Palo Alto Networks).
→ Voir les produits et licences pris *en charge pour la gestion et les opérations unifiées Strata Cloud Manager*

Pour lancer ou accéder aux Strata Cloud Manager :

- Si vous débutez avec Prisma Access, AIOps pour NGFW Premium ou Prisma SD-WAN en octobre 2023 ou plus tard, voici comment Lancer Strata Cloud Manager pour la première fois
- Si vous utilisiez précédemment des applis distinctes et autonomes sur le hub pour gérer vos produits, vous pouvez en savoir plus sur les points suivants Passer à une Strata Cloud ManagerAppli dédiée aux produits

Lancer Strata Cloud Manager pour la première fois

Après avoir activé une licence Prisma Access, AIOps pour NGFW Premium ou Prisma SD-WAN, l'appli Strata Cloud Manager sera disponible sur le hub Palo Alto Networks ou vous pouvez y accéder directement sur stratacloudmanager.paloaltonetworks.com.



Lancez l'appli et prenez une Aperçu de Strata Cloud Manager. Poursuivre l'intégration de votre produit :

- Démarrez avec AIOps pour NGFW Premium, y compris la Gestion du Cloud pour NGFWs
- Démarrez avec Prisma Access
- Démarrez avec Prisma SD-WAN

Passer à une Strata Cloud ManagerAppli dédiée aux produits

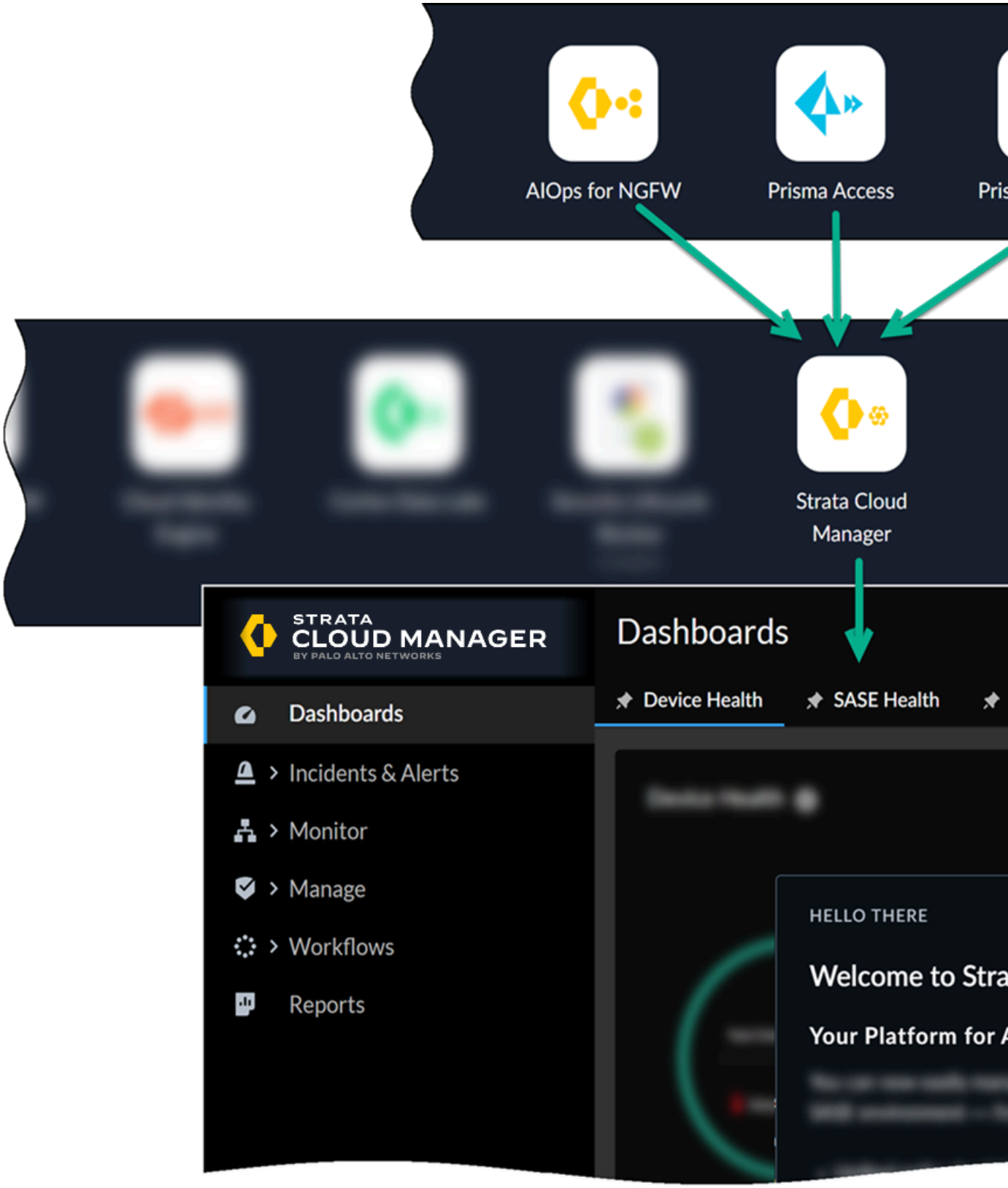
Important

Cette disposition ne s'applique que si vous utilisiez précédemment une appli autonome pour gérer ou interagir avec votre produit : l'appli Prisma Access, l'appli AIOps pour NGFW Premium ou l'appli Prisma SD-WAN. Ces applis ont été mises à jour (ou le seront bientôt) pour vous offrir une gestion et des opérations Strata Cloud Manager unifiées.

À quoi s'attendre lorsque vous passez à Strata Cloud Manager depuis une appli dédiée à un produit :

- Strata Cloud Manager fournit une gestion et des opérations unifiées basées sur la prise en charge des licences : voici les produits que vous pouvez surveiller ou gérer avec Strata Cloud Manager.
- Les notifications intégrées au produit vous informeront à l'avance qu'une mise à jour est imminente pour vous donner des Strata Cloud Manager.
- La mise à jour est transparente et n'a pas d'impact sur vos données, vos alertes ou vos actifs.

- Une fois la mise à jour effectuée, vous vous connecterez à l'appli Strata Cloud Manager sur le hub ; vous n'utiliserez plus d'applis distinctes sur le hub pour Prisma Access, AIOps pour NGFW Premium ou Prisma SD-WAN.



- Votre appli de produit vous redirige automatiquement vers stratacloudmanager.paloaltonetworks.com. Il s'agit de l'URL de Strata Cloud Manager.

  Si vous utilisiez précédemment plus d'une appli de produit mise à jour pour Strata Cloud Manager, les applis de produit mises à jour seront toutes redirigées vers la même instance de Strata Cloud Manager.

- Strata Cloud Manager vous offre une toute nouvelle interface de navigation commune à l'ensemble de vos produits de sécurité réseau. Jetez un premier coup d'œil à Strata Cloud Manager et explorez la nouvelle expérience de navigation et les nouvelles fonctionnalités.
- **Retrouvez les fonctionnalités de votre produit dans la nouvelle interface de gestion unifiée :**
  - AIOps pour NGFW : Où se situent mes fonctionnalités dans Strata Cloud Manager ?
  - Prisma SD-WAN : Où se situent mes fonctionnalités dans Strata Cloud Manager ?
  - Prisma Access Insights : Où se situent mes fonctionnalités dans Strata Cloud Manager ?
  - Prisma Access : Où se situent mes fonctionnalités dans Strata Cloud Manager ?

Prise en main de Strata Cloud Manager

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Prisma SD-WAN ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Strata Cloud Manager vous offre une gestion et des opérations unifiées, alimentées par l'IA, pour vos NGFW et votre réseau SASE. Voici un aide-mémoire sur la prise en main de Strata Cloud Manager pour la première fois.

Si vous prévoyez d'utiliser Strata Cloud Manager pour embarquer et gérer Prisma Access, NGFW (nécessite AIOps pour NGFW Premium), ou les deux ensemble, cela inclut ce que vous devez savoir pour commencer avec Gestion partagée pour Prisma Access et les NGFW

☐ **(Dans le concentrateur) Activez vos licences**

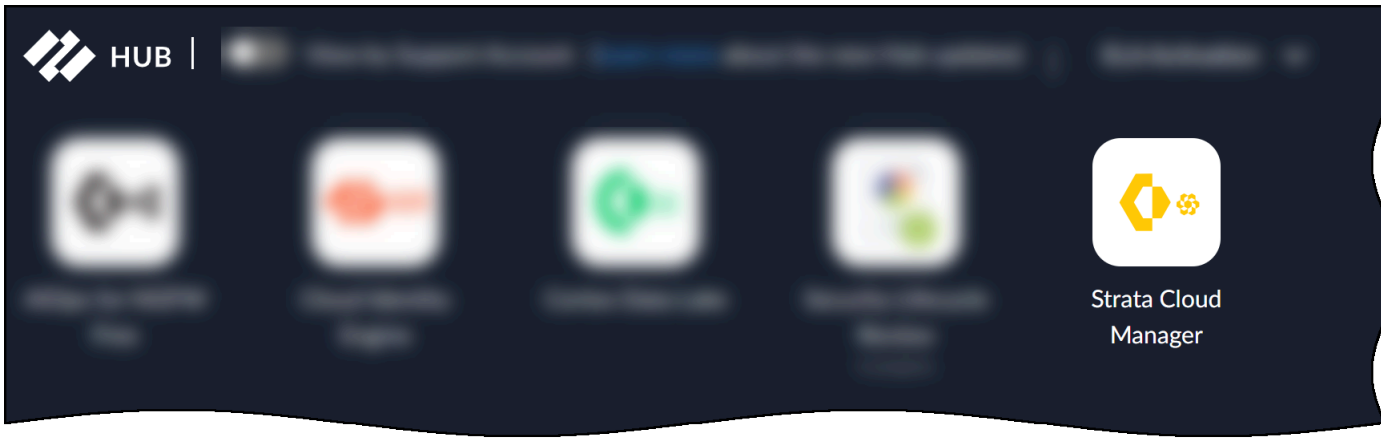
Après avoir acheté une licence, vous recevrez une adresse e-mail contenant un lien d'activation. Le lien lance un flux de travail guidé dans le concentrateur ; suivez le flux de travail d'activation pour chaque licence que vous souhaitez activer :

- Licence AIOps pour NGFW Premium
- Activer une licence Prisma Access
- Prisma SD-WAN

L'activation de l'une de ces licences active la Strata Cloud Manager. Après avoir activé au moins une de ces licences, activez ensuite les licences supplémentaires ou les abonnements complémentaires.

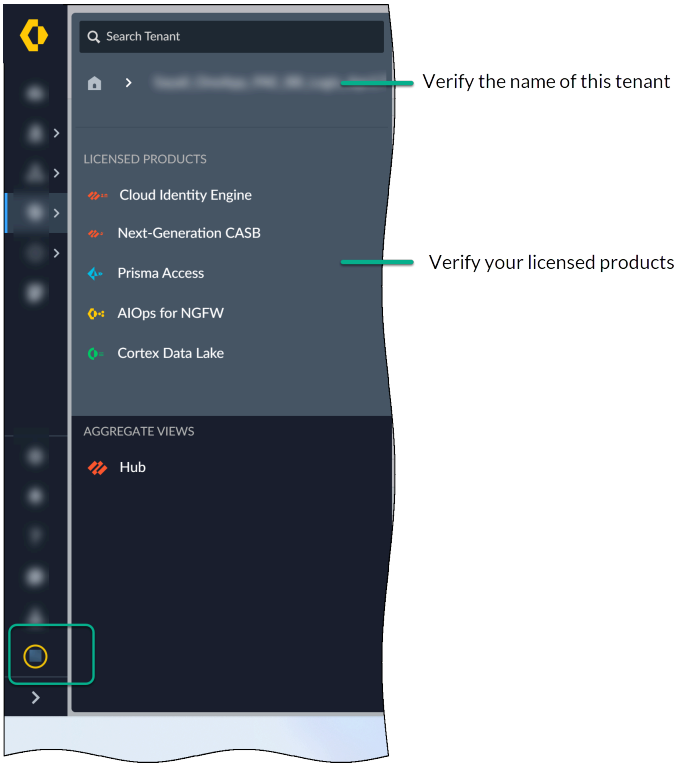
Lancement de Strata Cloud Manager

Après avoir activé une Prisma Access, AIOps pour NGFW Premium ou la licence Prisma SD-WAN, Strata Cloud Managerl'appli sera disponible sur le concentrateur Palo Alto Networks, ou vous pouvez y accéder directement sur stratacloudmanager.paloaltonetworks.com.



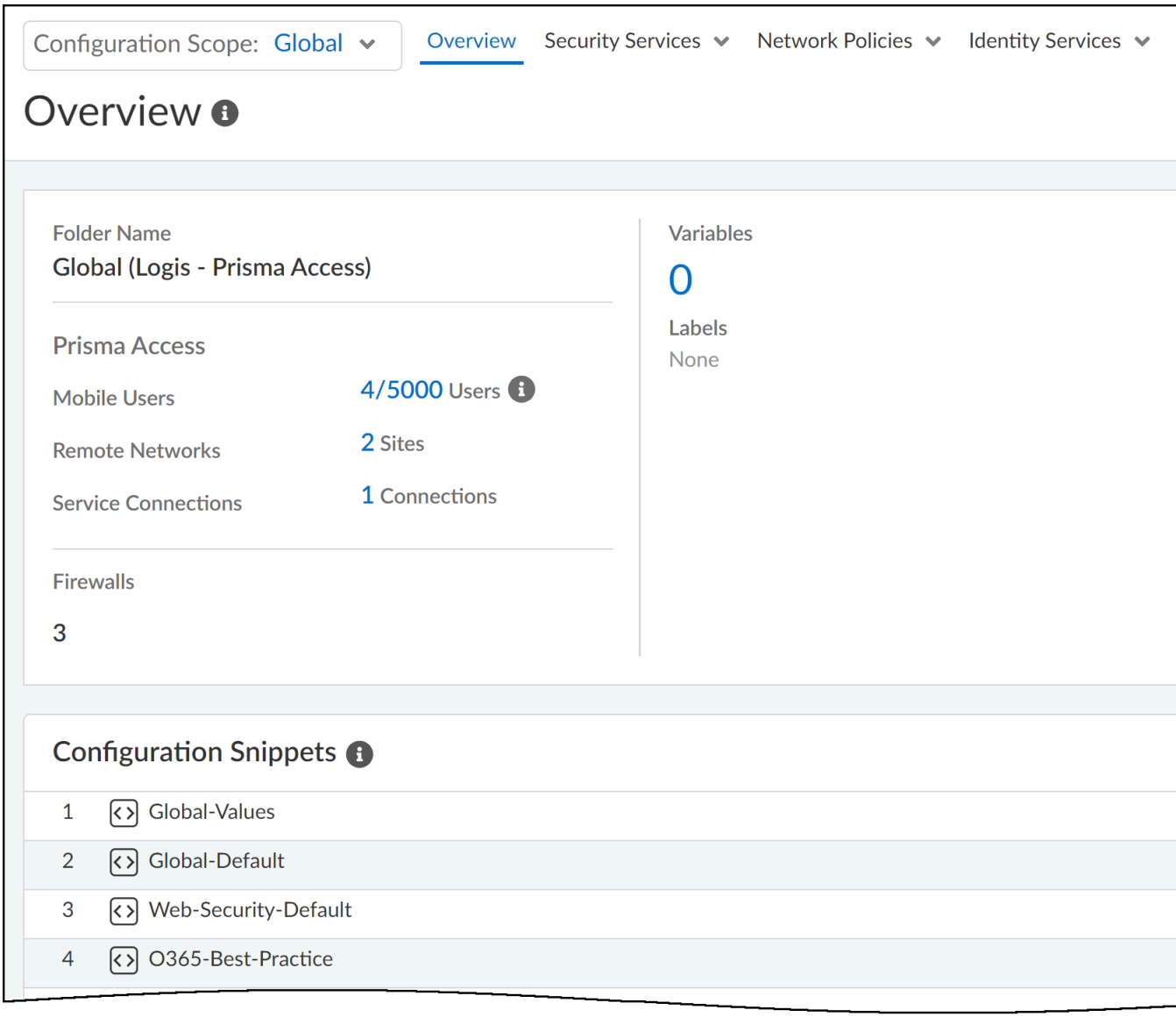
Valider vos licences

- Dans la partie inférieure du menu de navigation, sélectionnez les détails de votre locataire et vérifiez le nom du locataire que vous utilisez, ainsi que vos produits sous licence. En savoir plus sur la gestion des locataires et des abonnements.



- Accédez à **Manage (Gestion)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** pour vérifier l'état et les détails de votre licence Prisma Access, et voir quels autres détails pourraient être disponibles.

> *Il se peut que vous ne voyiez pas encore beaucoup de données ici si vous n'avez pas encore embarqué les NGFW ou si votre environnement Prisma Access est encore en cours de provisionnement. Si tel est le cas, revenez bientôt et après avoir terminé le reste des étapes ici.*



- **Surveillance et visibilité avec Strata Cloud Manager**
  - Explorez une représentation visuelle de votre réseau et de votre infrastructure de sécurité avec le Centre de Commandes.
  - Examinez les données réseau importantes dans Informations sur l'activité.
  - Explorez les Strata Cloud Manager tableaux de bord mis à votre disposition. De nombreux tableaux de bord prennent également en charge les rapports que vous pouvez planifier ou partager avec les parties prenantes.
  - Surveiller votre environnement Prisma Access, Prisma SD-WAN et vos NGFW.
  - Examinez vos incidents et alertes sur Prisma Access, NGFWs et Prisma SD-WAN.
- **Les meilleures pratiques recommandées et les flux de travail en ligne**

  Apprenez-en davantage sur les meilleurs pratiques et automatisations intégrés directement dans Strata Cloud Manager.

- **Paramètres d'intégration Strata Cloud Manager**

  Strata Cloud Manager regroupe les services communs dans le menu **Settings (Paramètres)**. Allez dans **Settings (Paramètres)** pour gérer :

  - Rôles et autorisations : en savoir plus sur les rôles disponibles sur Strata Cloud Manager et les autorisations associées.
  - Associations de périphériques : associez des applications cloud prises en charge à vos périphériques.
  - Gestion des locataires : créez et gérez votre hiérarchie d'organisations et d'unités professionnelles, représentées par des locataires.

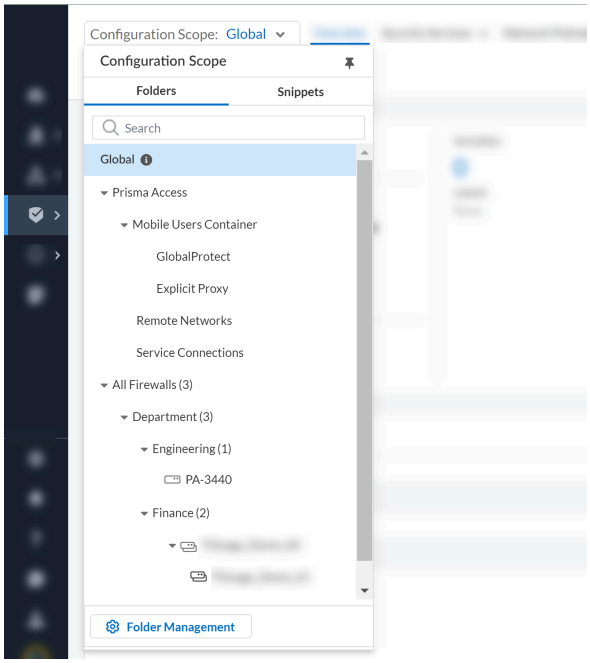
Gestion partagée pour Prisma Access et les NGFW

Pour Prisma Access et les NGFW, Strata Cloud Manager fournit une gestion partagée ; les utilisateurs embarqués de NGFW et Prisma Access, les réseaux distants et les connexions de service pour Strata Cloud Manager et appliquer une politique de sécurité commune.

- **Intégration des NGFW et Prisma Accès aux Strata Cloud Manager**
  - Configurer Prisma Access et les utilisateurs mobiles embarqués, les réseaux distants et les connexions de service :
    - Mise en place de l'infrastructure du service
    - Configurer les utilisateurs mobiles de Prisma Access, y compris les connexions GlobalProtect et Proxy explicit.
    - Configurer les réseaux distants
    - Configurer les connexions
  - Intégrer et mettre en place des NGFW :
    - Intégration et configuration pour la Gestion NGFW dans le cloud
- **Organiser votre configuration**

  Lorsque vous travaillez dans les paramètres de configuration Strata Cloud Manager, l'actuel Gestion : Portée de la configuration est toujours visible pour vous, et vous pouvez basculer votre vue pour gérer une configuration plus large ou plus granulaire. L'étendue de

configuration vous permet d'appliquer des politiques à l'échelle mondiale ou de fournir une application ciblée à certains déploiements NGFW ou Prisma Access.



Voici comment commencer à organiser la configuration de votre Strata Cloud Manager :

- **Flux de travail : Gestion des dossiers**

  Les dossiers permettent de regrouper logiquement les NGFW afin de simplifier la gestion de la configuration. Les dossiers Prisma Access sont prédéfinis en fonction du type de déploiement. Vous pouvez également activer Web Security (une expérience de gestion simplifiée pour les administrateurs gérant l'accès à Internet et aux applications SaaS) au niveau des dossiers.

- **Gestion : Extraits**

  Utilisez des extraits pour regrouper les configurations que vous pouvez rapidement intégrer à vos déploiements NGFW ou Prisma Access.

- **Gestion : Variables**

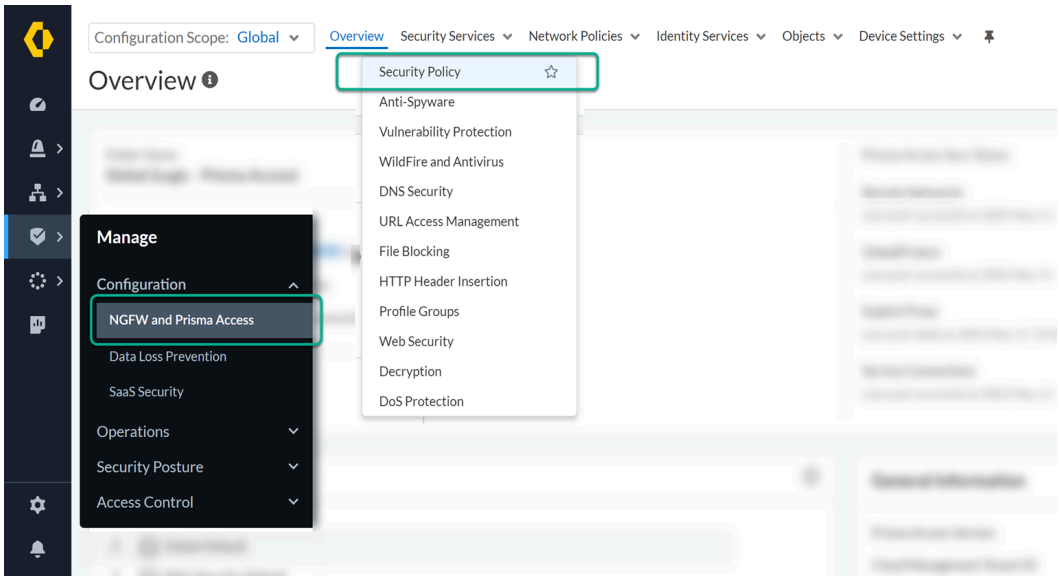
  Faites appel à des variables pour vos configurations afin de prendre en compte les objets de configuration spécifiques à un périphérique ou à un déploiement.

- **Politique de sécurité partagée pour les NGFW et Prisma Access**

  Strata Cloud Manager vous offre une gestion unifiée pour Prisma Access et vos NGFW. Votre politique de Strata Cloud Managervsécurité est partagée, et vous pouvez l'appliquer

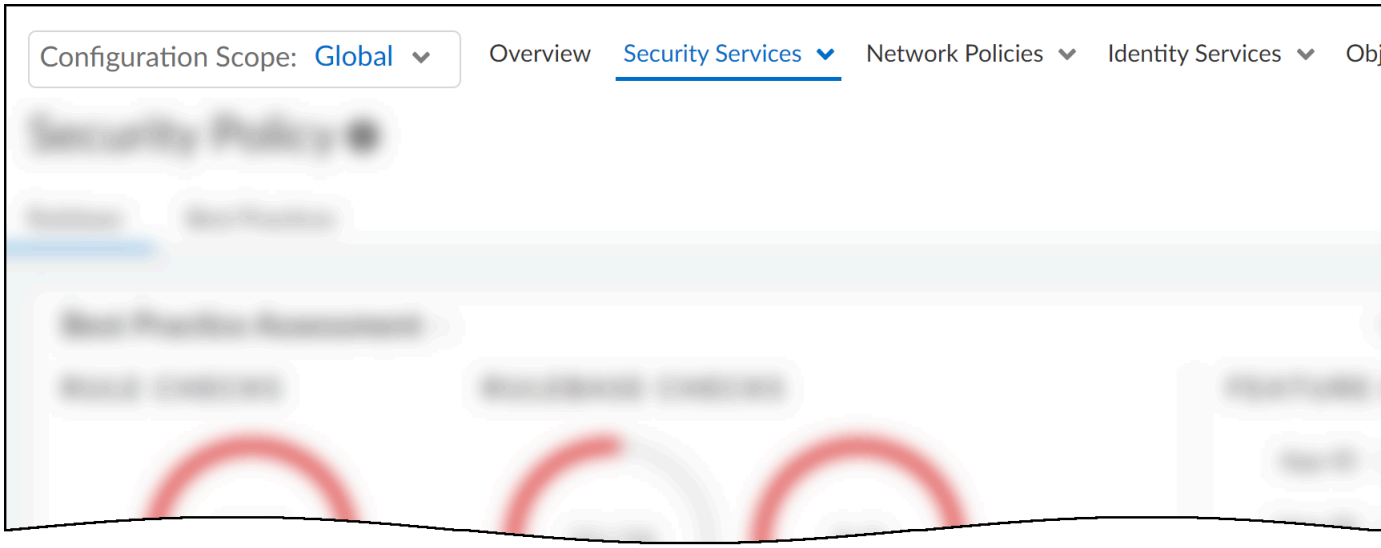
globalement sur Prisma Access et NGFW, ou cibler des paramètres spécifiques aux déploiements Prisma Access ou à des groupes spécifiques de pare-feux.

Accédez à **Gestion > Configuration > NGFW et Prisma Access** pour commencer.



- **Pousser les modifications de configuration aux NGFW et Prisma Access**

  Lors de la gestion de la configuration de votre Strata Cloud Manager, sélectionnez **Push Config (Transmettre la configuration)** afin de pousser les modifications de configuration à vos NGFW et Prisma Access :



Vous serez invité à définir la portée de la transmission de configuration, en fonction de vos dossiers Flux de travail : Gestion des dossiers. Voici comment procéder :

- Enregistrez les modifications de configuration
- Examinez l'état de la transmission de configuration
- Découvrez comment vous pouvez améliorer votre configuration

Meilleures pratiques intégrées dans Strata Cloud Manager

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Les meilleures pratiques de Palo Alto Networks sont conçues pour vous aider à obtenir le réseau le plus sécurisé possible en rationalisant le processus de vérification de la conformité de votre infrastructure réseau. Nous avons intégré les vérifications des meilleures pratiques directement dans Strata Cloud Manager, afin que vous puissiez obtenir une évaluation en direct de votre configuration. Renforcez votre posture de sécurité en vous alignant sur les meilleures pratiques. Vous pouvez tirer parti de Strata Cloud Manager 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.

Les conseils sur les meilleures pratiques visent à vous aider à renforcer votre posture de sécurité, mais aussi à gérer efficacement votre environnement et à favoriser au mieux la productivité des utilisateurs. Évaluez en permanence votre configuration par rapport à ces vérifications en ligne et, lorsque vous voyez une opportunité d'améliorer votre sécurité, prenez des mesures sur-le-champ.

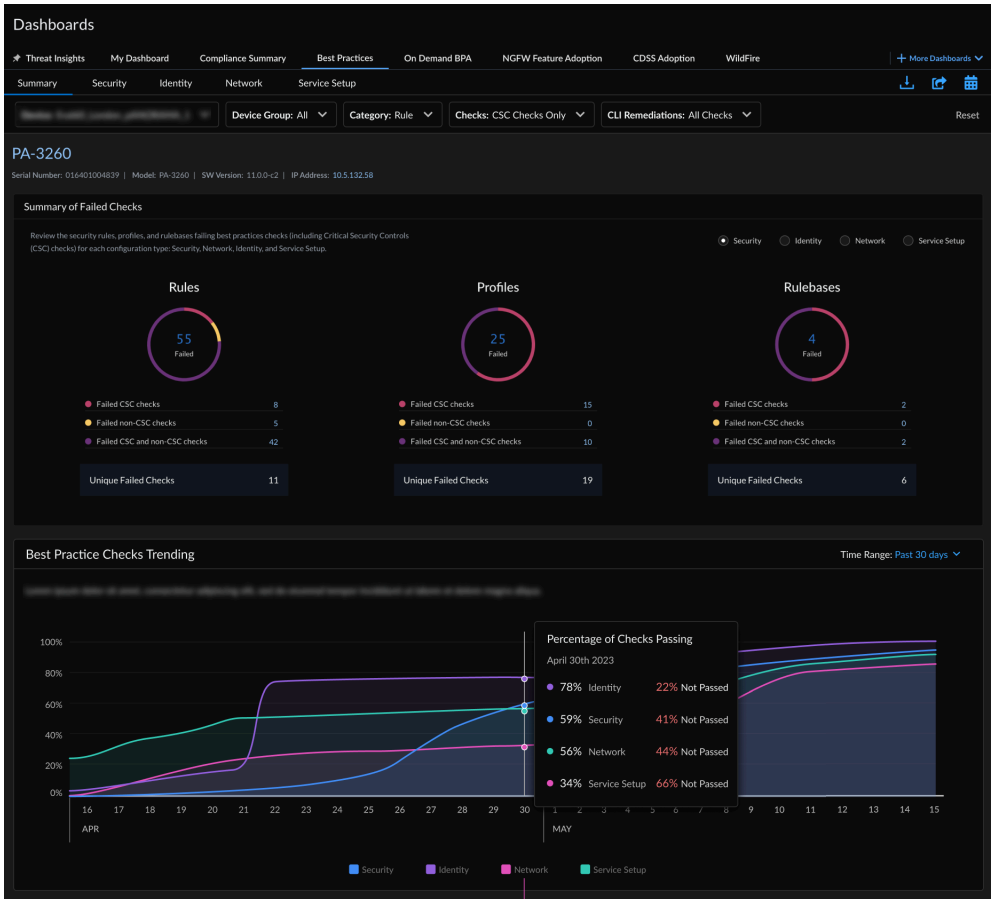
Visibilité sur l'adoption et la conformité des meilleures pratiques

Pour commencer, vous pouvez rapidement évaluer votre posture de sécurité globale en vérifiant les éléments suivants : **Dashboards (Tableaux de bord)**.

Voyez comment vous vous en sortez à un niveau élevé et identifiez les domaines dans lesquels vous pourriez commencer à agir.

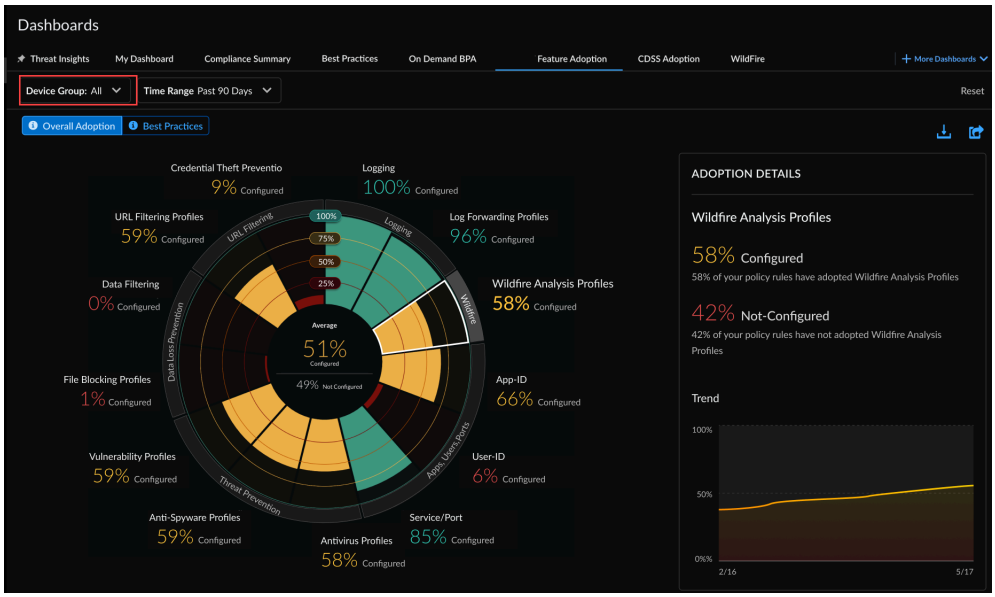
- Vérifiez le Tableau de bord : Meilleures pratiques tableau de bord pour les rapports quotidiens sur les meilleures pratiques, et leur mise en correspondance avec les contrôles de sécurité critiques (CSC) du Centre pour la sécurité internet. Ces rapports vous aideront à identifier les domaines dans lesquels vous pouvez apporter des changements 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 réception.

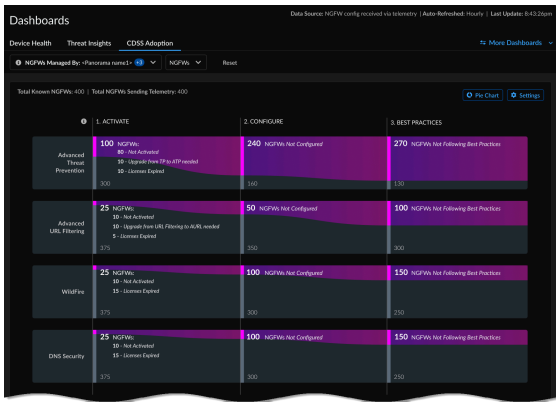


- Vérifiez le tableau de bord du Résumé de la conformité pour afficher un historique des modifications apportées aux contrôles de sécurité effectués jusqu'à 12 mois auparavant, regroupés par les cadres du Centre pour la sécurité Internet (CIS) et de l'Institut national des normes et de la technologie (NIST).

- Moniteur Tableau de bord : Adoptions de fonctionnalité et restez au courant des fonctionnalités de sécurité que vous utilisez dans votre déploiement et des lacunes potentielles dans la couverture.



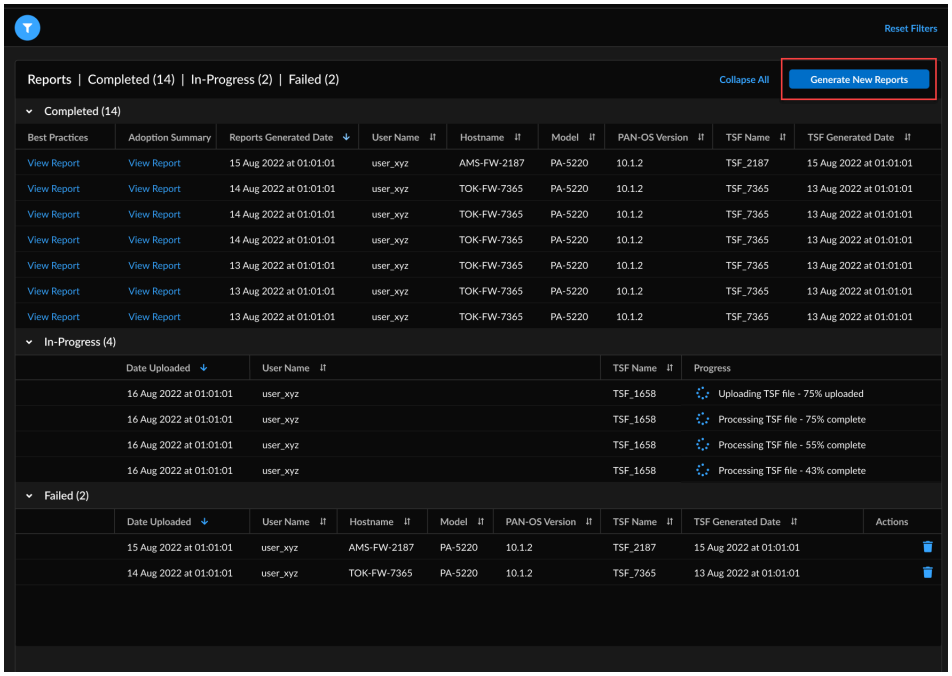
- Moniteur Tableau de bord : Adoption de CDSS : consultez les services de sécurité ou les abonnements aux fonctionnalités et leur utilisation des licences sur vos périphérique pour identifier les failles de sécurité et renforcer la posture de sécurité de votre entreprise.



- Obtenez une visibilité sur l'état et la tendance de la sécurité de votre déploiement en fonction des postures de sécurité des appareils NGFW intégrés avec Tableau de bord : Informations

sur la posture de sécurité et soyez alerté lorsque des incidents se produisent ou lorsque vos paramètres de sécurité peuvent nécessiter un examen plus approfondi.

- Générer des rapports BPA pour les dispositifs PAN-OS (non télémétriques) fonctionnant à partir de la version 9.1, incluant désormais les mesures d'adoption des fonctionnalités.



Outils de meilleures pratiques pour renforcer la posture de sécurité

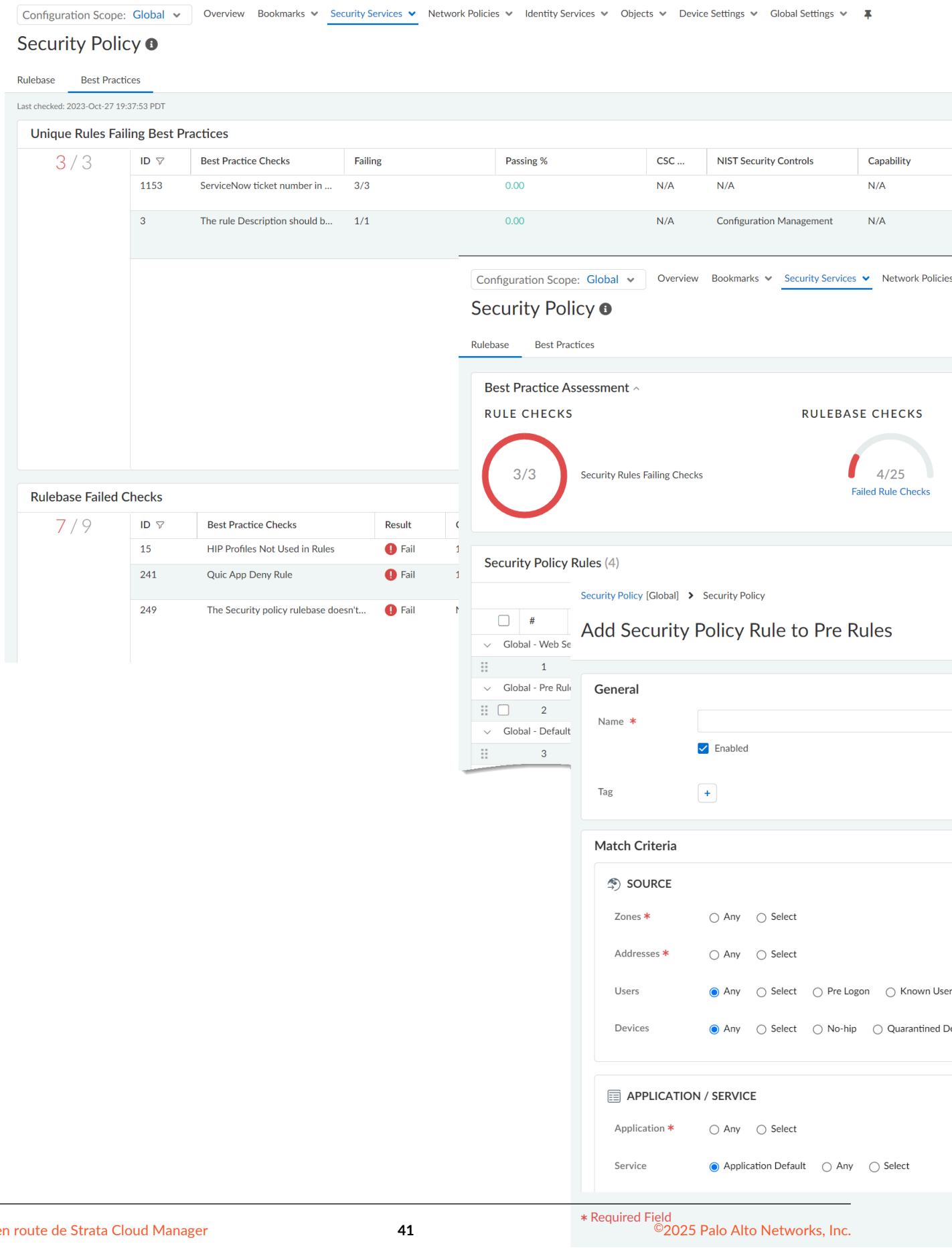
Trouver une collection d'outils pour vous aider à améliorer votre posture de sécurité.

- Personnalisez les contrôles liés à la posture de sécurité pour votre déploiement afin de maximiser les recommandations pertinentes dans Gestion : Paramètres de la posture de sécurité
- Utilisez Config Cleanup (Nettoyage de la configuration) pour identifier et supprimer les objets de configuration et les règles de politique inutilisées.
- Configurer Paramètres de l'optimiseur de politiques pour affiner et optimiser les règles de sécurité trop permissives afin qu'elles n'autorisent que les applications qui sont réellement utilisées dans votre réseau.

- Créez le vôtre Contrôles de conformité : personnalisez les vérifications des meilleures pratiques existantes, créez et gérez des exemptions spéciales pour mieux vous aligner sur les exigences commerciales de votre organisation.
- Utiliser Analyseur de politiques pour vous assurer rapidement que les mises à jour que vous apportez à vos règles de politique de sécurité répondent à vos besoins et n'introduisent pas d'erreurs ou de configurations erronées (telles que des modifications entraînant des règles en double ou contradictoires).

Vérifications de configuration en direct et en ligne des meilleures pratiques

Les conseils sur les meilleures pratiques visent à vous aider à renforcer votre posture de sécurité, mais aussi à gérer efficacement votre environnement et à favoriser au mieux la productivité des utilisateurs. Évaluez en permanence votre configuration par rapport à ces vérifications en ligne et, lorsque vous voyez une opportunité d'améliorer votre sécurité, prenez des mesures sur-le-champ.



- **Scores des meilleures pratiques**

  Les scores des meilleures pratiques sont affichés sur un tableau de bord de fonctionnalités (politique de sécurité, décryptage ou contrôle d'accès aux URL, par exemple). Ces scores vous donnent un aperçu rapide de la progression de vos meilleures pratiques. En un coup d'œil, vous pouvez identifier les domaines nécessitant une enquête plus approfondie ou les domaines dans lesquels vous souhaitez prendre des mesures pour améliorer votre posture de sécurité.
- **Meilleures pratiques en matière de vérifications sur le terrain**

  Les vérifications au niveau du champ vous montrent exactement où votre configuration ne correspond pas à une meilleure pratique. Des conseils sur les meilleures pratiques sont fournis en ligne, afin que vous puissiez agir immédiatement.
- **Évaluation des meilleures pratiques**

  Ici, vous pouvez obtenir une vue complète de la façon dont votre implémentation d'une fonctionnalité s'aligne aux meilleures pratiques. Examinez les vérifications ayant échoué pour voir où vous pouvez apporter des améliorations (vous pouvez également examiner les vérifications réussies). Les vérifications de la base de règles mettent en évidence les modifications de configuration que vous pouvez apporter en dehors des règles individuelles, par exemple à un objet de politique utilisé dans plusieurs règles.

Des vérifications des meilleures pratiques sont disponibles pour :

- **Votre base de règles de politique de sécurité**

  Les vérifications de la base de règles examinent l'organisation et la gestion de la politique de sécurité, y compris les paramètres de configuration qui s'appliquent à de nombreuses règles.
- **Règles de sécurité**
- **Profils de sécurité**
  - Logiciel anti-espion
  - Protection contre les vulnérabilités
  - WildFire et Antivirus
  - Gestion de l'accès à l'URL
  - Sécurité DNS
- **Authentification**
- **Déchiffrement**
- **GlobalProtect**

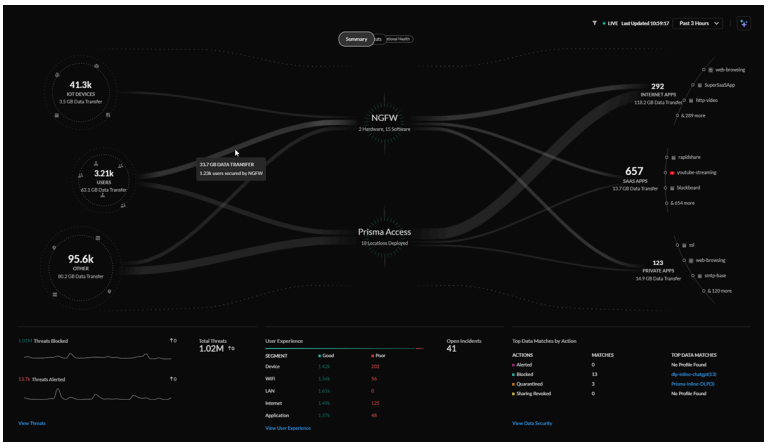
Vous souhaitez en savoir plus sur les meilleures pratiques de Palo Alto Networks ?

Voici la page d'accueil des meilleures pratiques, où vous trouverez des ressources pour vous aider à faire la transition vers les meilleures pratiques et à les mettre en œuvre.

Centre de commande : Strata Cloud Manager

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels • Prisma SD-WAN	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Pro ☐ Strata Cloud Manager Essentials ☐ Prisma SD-WAN Les autres licences et prérequis nécessaires pour accéder au Centre de commande : ☐ Strata Logging Service ☐ Une licence spécifique pour afficher certaines mesures dans le centre de commande qui est décrite ci-dessous ☐ Un rôle qui a l'autorisation d'afficher le → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Le Centre de commande Strata Cloud Manager est votre nouvelle page d'accueil NetSec. Il s'agit d'un résumé visuel interactif qui vous aidera à évaluer la santé, la sécurité et l'efficacité de votre réseau. Le centre de commande fournit une vue consolidée de la plate-forme NetSec et vous offre une visibilité complète sur vos sources, vos applications, le déploiement Prisma Access, vos NGFW et vos services de sécurité en un seul endroit.



Le centre de commande vous permet d'interagir avec les données et de visualiser les relations entre les événements sur le réseau. Aussi, de pouvoir prendre des mesures immédiates pour renforcer votre sécurité.

Le centre de commande est intégré aux nouveaux tableaux de bord Activity Insights **(Insights (Informations) > Activity Insights (Informations sur les activités))**, et mettra en évidence les anomalies détectées par vos licences et abonnements intégrés grâce à des informations exploitables, et fournira un chemin pour corriger ces anomalies.

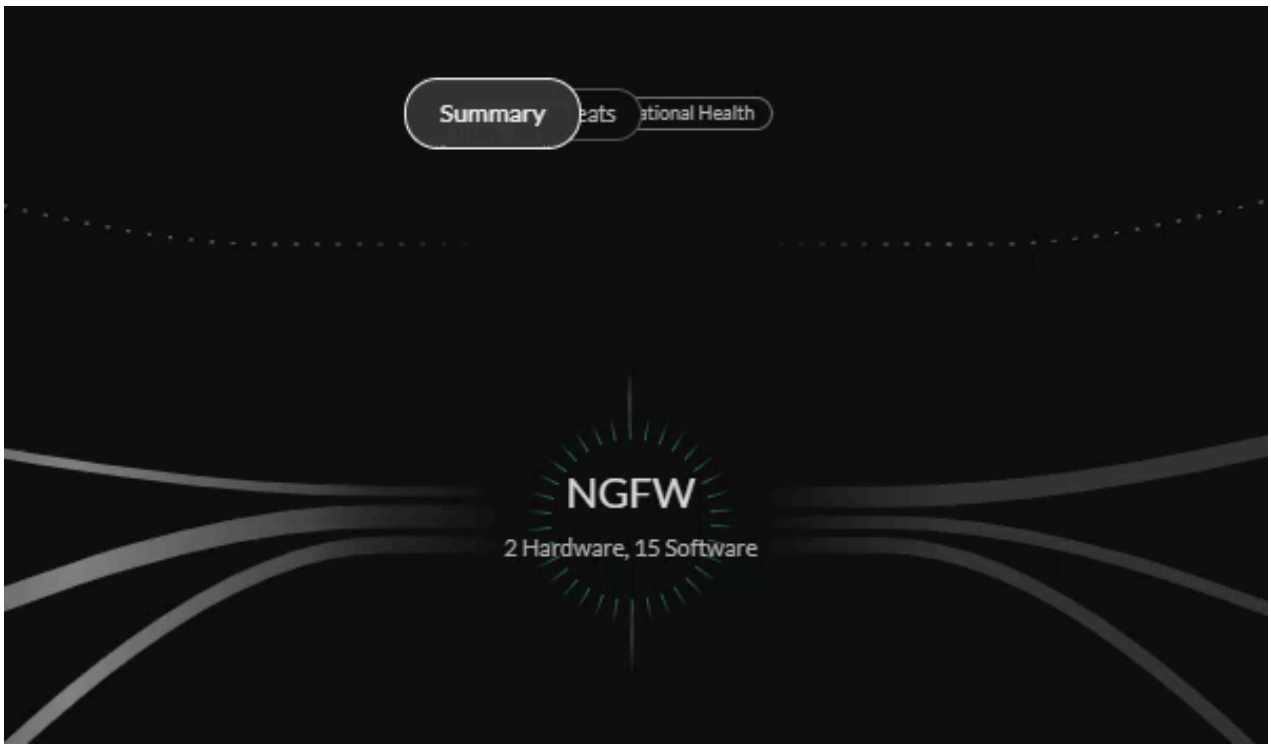
Depuis la nouvelle page d'accueil, vous pouvez voir :

- Une vue complète de tout le trafic sur votre réseau circulant entre les sources (utilisateurs, IoT, hôtes externes) vers les applications (Internet, SaaS, privées).
- Comment les actifs tels que les utilisateurs, les périphériques et les applications sont accessibles et sécurisés.
- Accédez à des tableaux de bord spécifiques avec contexte pour une compréhension plus approfondie des problèmes impactant votre réseau.
- Types de menaces rencontrées pendant que les utilisateurs travaillent.

Lancez Strata Cloud Manager et cliquez sur **Command Center (Centre de commandes) ( )** pour commencer.

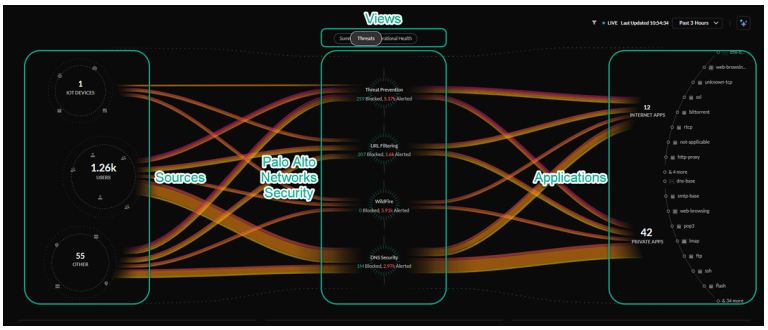
Comment interagir avec le centre de commande Strata Cloud Manager

Chaque vue du centre de commande décompose soigneusement toutes les informations dont vous auriez besoin pour évaluer la santé et la sécurité de votre réseau.



Les données du centre de commande sont actualisées toutes les 5 minutes et affichent par défaut les données des dernières 24 heures. Vous pouvez également filtrer ces données sur les 1 heure, 3 heures, 7 jours ou 30 derniers jours.

Chaque vue du centre de commande affiche différents types de données visuelles circulant des sources, via Prisma Access et NGFW ou des abonnements de sécurité déployés sur votre réseau, vers les différentes applications de votre réseau.



Les bulles Sources (travailleurs hybrides, utilisateurs bureautiques, périphériques IoT, etc.) sont à gauche et les bulles Applications (accessibles sur Internet, SaaS et hébergées sur site ou dans le cloud) sont à droite. Les bulles d'applications affichent les trois applications les plus utilisées dans chaque catégorie.

Sources :

- **IoT Devices (Périphériques IoT)** : périphériques découverts par une licence active IoT Security et activés,
- **Users (Utilisateurs)** : utilisateurs distants et Branchés.
- **Other (Autres)** : hébergeurs internes et externes accédant à des ressources sur Internet.

Les applications comprennent :

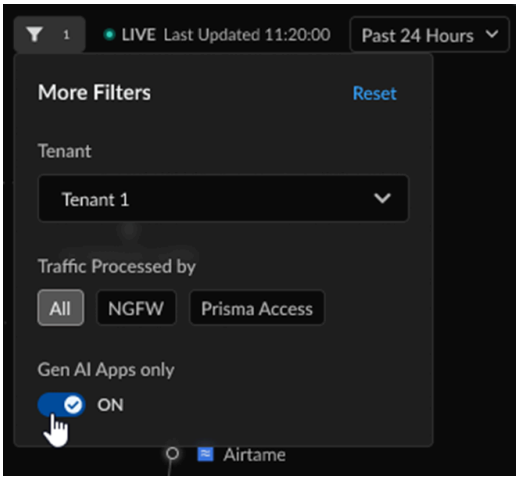
- **Internet Apps (Applications Internet)** ; applications accessibles à l'aide d'un navigateur Web.
- **SaaS Apps (Apps SaaS)** : applications cloud détenues et gérées par un fournisseur de services d'applications.
- **Private Apps (Applications privées)** : applications hébergées dans un centre de données.

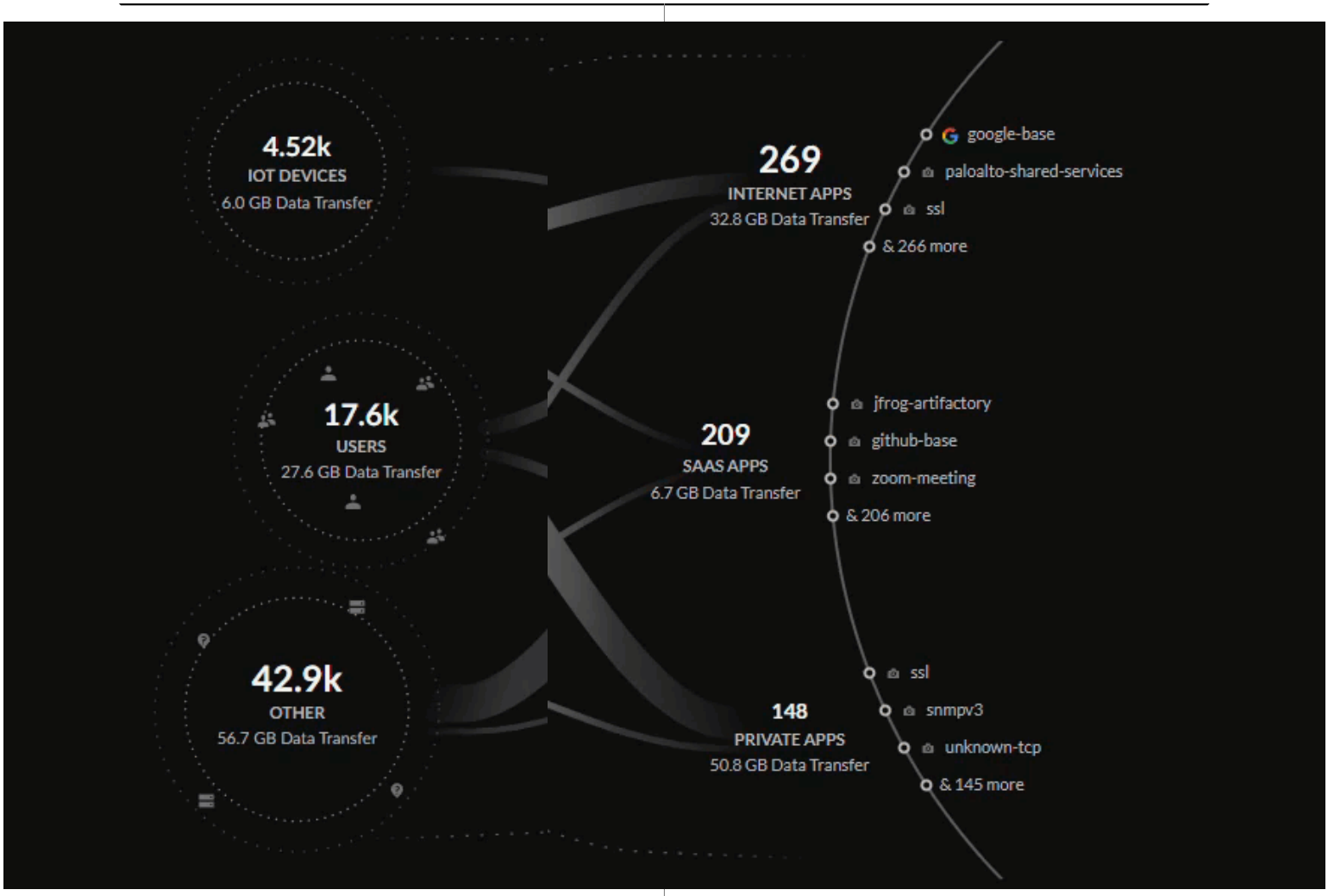
Vous pouvez filtrer les données dans la vue centrale en cliquant sur les bulles correspondant aux sources, déploiements ou applications. Cela vous donnera une vue plus détaillée des données suivies pour cette vue par rapport à la bulle sélectionnée.

En sélectionnant des filtres (▼), vous pouvez filtrer les données dans les vues du centre de commande par **Tenant (Locataire)** ou **NGFW** ou par données spécifiques de **Prisma Access**.

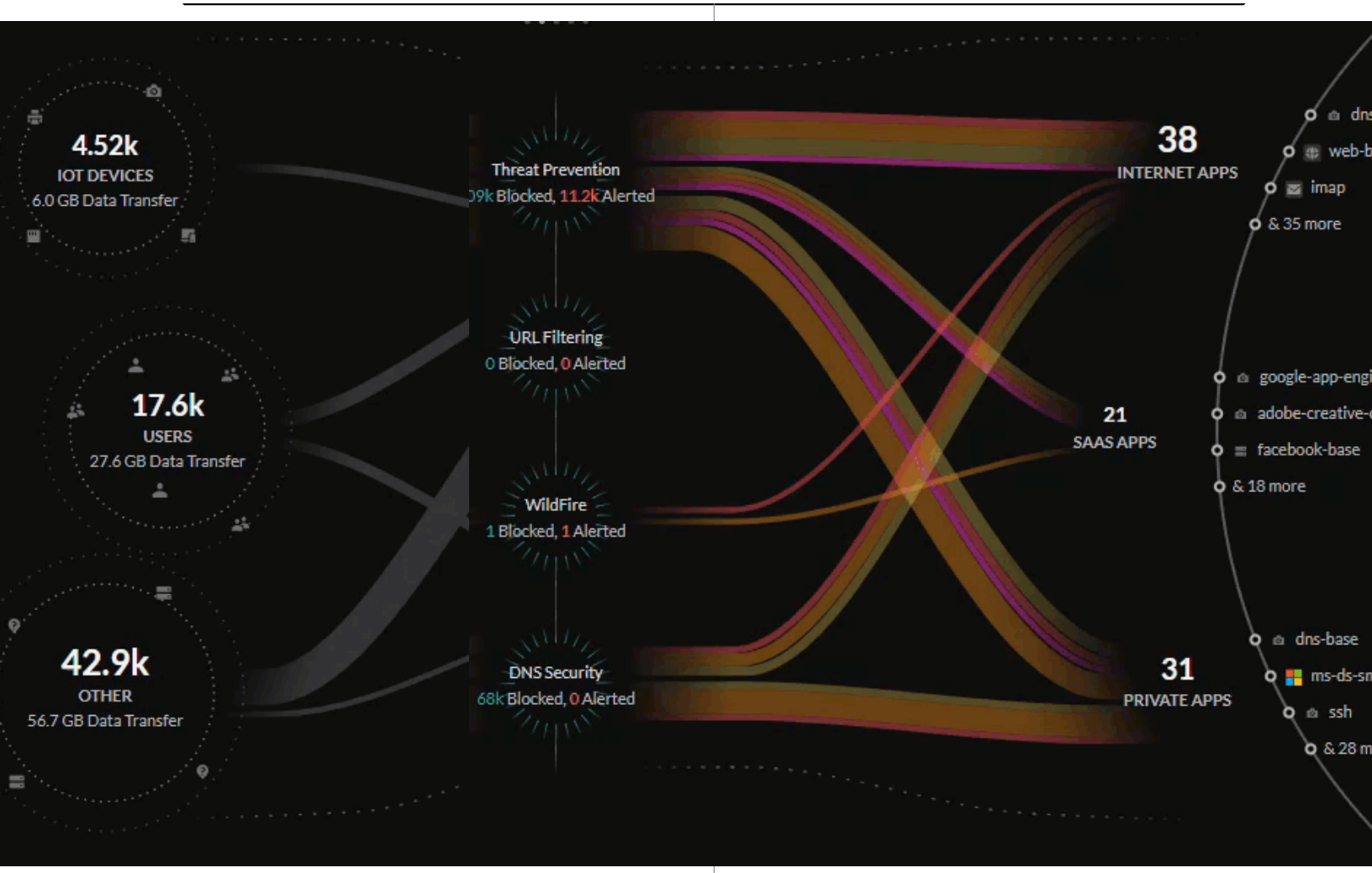
Avec une licence AI Access, vous pouvez filtrer le trafic dans toutes les vues du centre de commande par **GenAI Apps (Applis GenAI) uniquement** pour mieux évaluer comment les applis GenAI utilisées par les utilisateurs sur votre réseau pourraient affecter la sécurité de vos données.

Pour plus d'informations sur AI Access Security et les licences AI Access Security, cliquez ici.

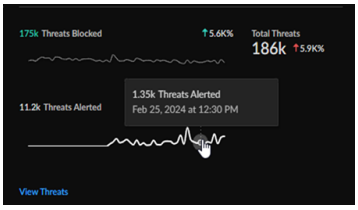




Lorsque vous regardez l'une des vues, vous pouvez passer la souris sur les lignes pour plus d'informations sur votre réseau, telles que le trafic ou les menaces bloquées ou autorisées sur votre réseau.



Sous le résumé visuel central se trouvent plusieurs indicateurs clés suivis par vos abonnements activés. Ceux-ci fournissent des informations exploitables sur votre réseau. Ces indicateurs clés permettent de naviguer vers l'une des pages contextuelles détaillées où vous pouvez trouver plus d'informations sur les indicateurs qui ont fait surface, puis explorer les solutions possibles.



Vues du centre de commande de Strata Cloud Manager

Le centre de commande vous fournit quatre vues différentes, chacune avec ses propres données et mesures suivies à examiner et à interagir avec.

- Résumé
- Menaces
- Santé opérationnelle
- Sécurité des données

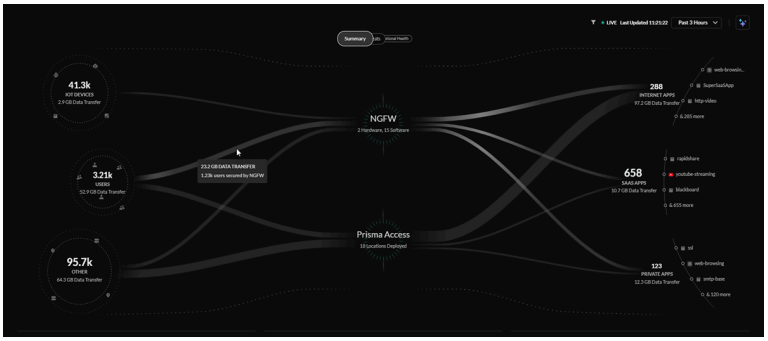
Centre de commande (Résumé)

La vue **Summary (Résumé)** vous présente un aperçu général de tout le trafic de vos utilisateurs, hôtes externes, périphériques IoT et applications. Elle vous donne également un aperçu des problèmes et anomalies sur votre réseau qui sont mis en évidence par les autres vues. Vous pouvez utiliser cette vue comme premier aperçu de la performance de votre réseau chaque jour.

Résumé des licences	• Vous devez disposer d'au moins une de ces licences qui est fournie avec une licence Strata Logging Service qui vous permettra d'utiliser le Centre de commande Strata :
	  ❑ Licence Prisma Access
	  ❑ AIOps pour licence NGFW Premium
	• Ou une licence AIOPs pour NGFW gratuit à côté d'une licence Strata Logging Service
	• Licences nécessaires pour des métriques supplémentaires dans la vue Résumé :
	  ❑ Abonnements CDSS (Cloud-Delivered Security Services)
	  ❑ Abonnements Data Security
	  ❑ Licence ADEM
	  ❑ Licence AI Access

La vue Résumé centrale

La vue Résumé centrale fournit un aperçu des données transférées entre les périphériques IoT, les utilisateurs, les hôtes externes accédant aux ressources à partir d'Internet, les applis Internet, les applis SaaS et les applis privées de votre réseau.



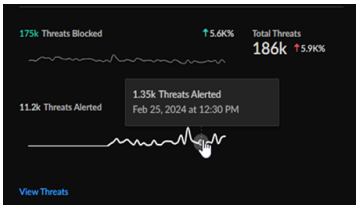
Les lignes de la vue Résumé centrale représentent les transferts de données et le trafic sur votre réseau. L'épaisseur des lignes représente le volume de données transférées à partir des sources et des applications.

Vous pouvez voir comment ces sources sont sécurisées par votre infrastructure réseau :

- Déploiements Prisma Access
- Pare-feu nouvelle génération depuis votre inventaire Strata Logging Service

Nombre total de menaces

Le widget **Total Threats Count (Nombre total de menaces)** vous donne un aperçu du nombre total de menaces détectées dans votre réseau, combien de menaces ont été bloquées, combien de menaces ont fait l'objet d'une alerte et l'évolution des menaces à partir d'une plage de temps sélectionnée.



Cliquez sur Aperçu des activités **(Insights (Aperçu) > Activity Insights (Aperçu des activités) > Threats (Menaces))** pour obtenir une analyse plus détaillée des menaces qui pèsent sur votre réseau.

Incidents ouverts et expérience utilisateur

Le widget **Open Incidents and User Experience (Incidents ouverts et expérience utilisateur)** vous donne une vue sur le nombre total d'incidents ouverts, la ventilation de l'expérience utilisateur bonne et potentiellement dégradée de segments individuels de la chaîne de prestation de services d'un périphérique utilisateur à une application, et la modification des incidents ouverts à partir d'une plage de temps sélectionnée.

Cliquez sur le tableau de bord Expérience d'application **(Dashboards (Tableaux de bord) > Application Experience (Expérience d'application))** pour une analyse plus détaillée de la qualité et de l'expérience de l'utilisateur sur votre réseau ainsi que des mesures de performance.

Profils de données majeurs par action

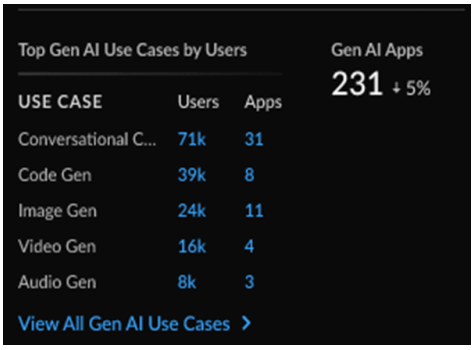
Les widgets **Top Data Profiles (Profils de données majeurs)** vous donnent un aperçu des meilleurs profils de filtrage des données prédéfinis, du nombre de correspondances trouvées dans le trafic réseau et des mesures prises pour les données sensibles en fonction de ces profils de données.

Cliquez sur la vue Sécurité des données **(Command Center (Centre de commande) > Data Security (Sécurité des données) ()** pour une analyse plus détaillée des données sensibles sur votre réseau.

Exemples d'utilisation de la GenAI par les utilisateurs et les applis de la GenAI

Le widget **Top GenAI Use Cases by User (Principaux cas d'utilisation des GenAI par utilisateur)** vous donne un aperçu des principaux cas d'utilisation des applis GenAI par les utilisateurs de vos réseaux, du nombre d'utilisateurs pour chaque cas d'utilisation et du nombre d'applications GenAI qui correspondent à chaque cas d'utilisation.

Vous pouvez aussi consulter le nombre total d'applis GenAI sur vos réseaux, ainsi que le pourcentage d'évolution des applications en fonction du filtre temporel.



Cliquez sur le tableau de bord AI Access Security **(Insights (Informations) > AI Access)** dans Aperçu des activités pour une analyse plus détaillée de l'adoption des applis GenAI sur votre réseau et des recommandations sur la façon de mieux sécuriser vos données.

Pour plus d'informations sur AI Access Security et sur la façon dont votre organisation peut adopter en toute sécurité des applications GenAI tout en atténuant les risques pour la sécurité de vos données, commencez ici.

Menaces

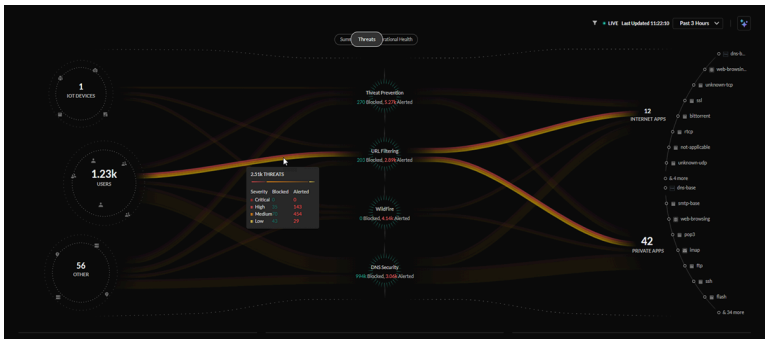
La vue **Threats (Menaces)** indique le trafic inspecté sur votre réseau et les menaces détectées par vos abonnements CDSS. Vous pouvez utiliser cette vue pour surveiller les menaces bloquées et alertées sur votre réseau ou enquêter sur les zones de votre réseau qui nécessitent des stratégies mises à jour pour mieux bloquer les menaces alertées.

Licences de menaces	• Licences de menaces, notamment : ❑ Licence de prévention de menaces ❑ Licence de filtrage des URL ❑ Licence WildFire ❑ Licence DNS Security

La vue Menaces centrales

La vue Menaces centrales fournit un aperçu de toutes les menaces sur votre réseau qui ont été identifiées par vos abonnements actifs aux services de sécurité fournis dans le cloud.

La vue Menaces indique comment vos abonnements CDSS Palo Alto Networks protègent votre trafic en surveillant les menaces potentielles sur votre réseau. Le Centre de commande vous donne un aperçu du pourcentage de trafic inspecté pour vos périphériques IoT, utilisateurs et applications, et du nombre total de menaces autorisées ou alertées.

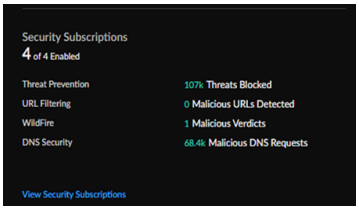


Les lignes de la vue Menaces centrales représentent le trafic surveillé par vos abonnements de sécurité, l'épaisseur représentant le volume de menaces détectées et la couleur si les menaces sont de gravité critique, élevée, moyenne ou faible.

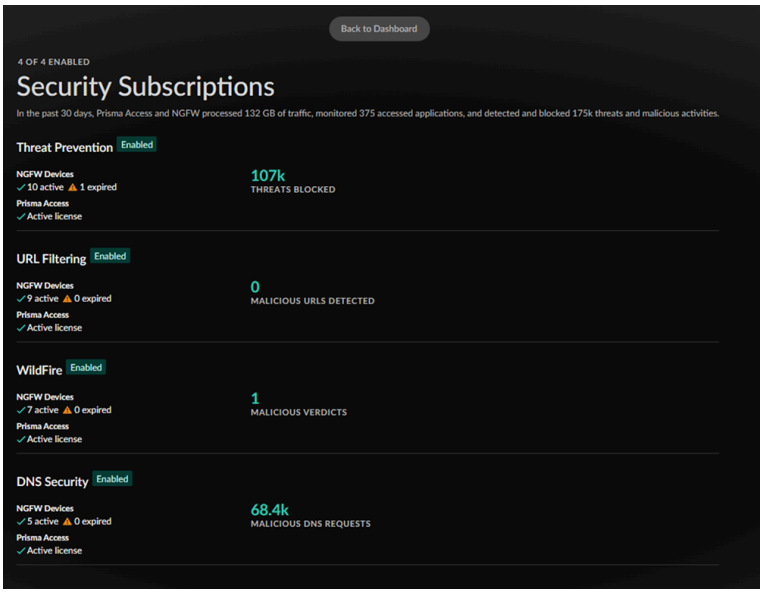
Abonnements de sécurité

Le widget **Security Subscriptions (Abonnements de sécurité)** vous donne un aperçu de vos abonnements de sécurité fournis dans le Cloud. Il vous indique ceux qui sont actifs et vous donne un aperçu de la façon dont ils sécurisent votre réseau.

Abonnement	Description
Prévention des menaces	La prévention des menaces protège votre réseau à la fois contre les menaces liées aux produits de base (qui sont omniprésentes, mais non sophistiquées) et contre les menaces ciblées et avancées perpétuées par des cybercriminels organisés.
Filtrage des URL	Le Filtrage avancé des URL est notre solution complète de filtrage d'URL qui protège votre réseau et les utilisateurs contre les menaces basées sur le Web.
WildFire	Le service d'analyse des logiciels malveillants WildFire, fourni dans le cloud, utilise des données et des renseignements sur les menaces provenant de la plus grande communauté mondiale du secteur. Il utilise une analyse avancée pour identifier automatiquement les menaces inconnues et stopper les hackers dans leur élan.
Sécurité DNS	Sécurisez automatiquement votre trafic DNS en utilisant le service de sécurité DNS de Palo Alto Networks.

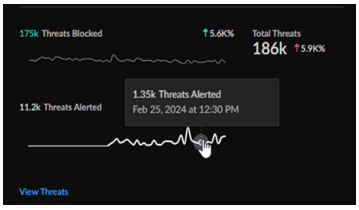


En cliquant sur le widget **Security Subscriptions (Abonnements de sécurité) (Command Center (Centre de commandes) > View Security Subscriptions (Afficher les abonnements de sécurité))** vous fournit un rapport détaillé de l'état de vos abonnements par rapport à vos déploiements NGFW et Prisma Access. Cliquez sur **Back to the Dashboard (Retour au tableau de bord)** pour revenir à la vue **Threats (Menaces)**.



Nombre total de menaces

Le widget **Total Threats Count (Nombre total de menaces)** vous donne un aperçu du nombre total de menaces détectées dans votre réseau, combien de menaces ont été bloquées, combien de menaces ont fait l'objet d'une alerte et l'évolution des menaces à partir d'une plage de temps sélectionnée.



Cliquez sur Informations sur l'activité **(Insights (Informations) > Activity Insights (Informations sur l'activité) > Threats (Menaces))** pour une analyse plus détaillée des menaces qui pèsent sur votre réseau.

Menaces bloquées et alertées

Le widget **Blocked and Alerted Threats (Menaces bloquées et alertées)** vous donne une vue d'ensemble des menaces détectées sur votre réseau, en les classant par catégorie, niveau de menace (critique, élevé, moyen et faible), et si les menaces ont été bloquées ou alertées.

Cliquez ici afin d'obtenir un tableau plus détaillé de toutes les menaces qui affectent votre réseau **(Insights (Informations) > Activity Insights (Informations sur l'activité) > Threats (Menaces))**.

Santé opérationnelle

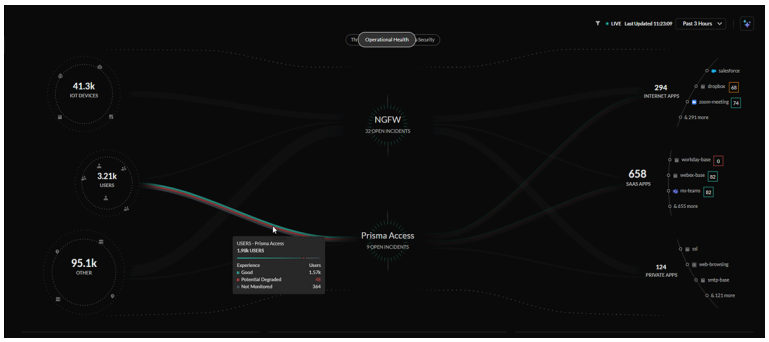
La vue **Operational Health (Santé opérationnelle)** montre l'état de l'infrastructure et l'expérience utilisateur sur votre réseau. Vous pouvez utiliser cette vue pour surveiller l'état de vos déploiements NGFW et Prisma Access ainsi que l'expérience utilisateur sur votre réseau et examiner la gravité des incidents ouverts dans chaque zone.

Licences de santé opérationnelle	• Suivi des abonnements, notamment : ❑ Observabilité ADEM ❑ ADEM alimenté par l'IA ❑ AIOps pour NGFW premium

Vue centrale de la santé opérationnelle

La vue centrale sur la santé opérationnelle fournit un aperçu de la santé de l'infrastructure et de l'expérience utilisateur sur votre réseau. Si les utilisateurs possèdent une licence ADEM (Gestion de l'expérience numérique autonome), ils recevront des données améliorées dans cette vue.

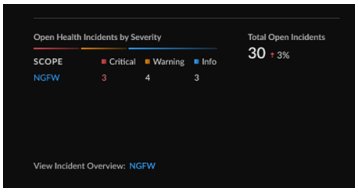
La vue Santé opérationnelle montrera comment votre abonnement ADEM Palo Alto Networks surveille l'expérience numérique de tous les utilisateurs et applications dans votre environnement SASE.



Les lignes de la vue Santé opérationnelle centrale représentent tous les utilisateurs de votre réseau. Les utilisateurs sont organisés par score d'expérience utilisateur, les couleurs des lignes représentant une note considérée comme bonne, médiocre ou non surveillée.

Total des incidents ouverts et des incidents par gravité

Le widget **Open Health Incidents by Severity (Incidents de santé ouverts triés par gravité)** vous donne une vue sur tous les incidents ouverts sur votre réseau, répartis par étendue (NGFW, Prisma Access et Prisma SD-WAN), gravité et quantité d'incidents.



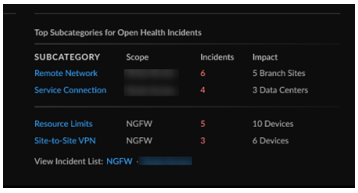
Le widget suit le pourcentage de variation des incidents ouverts en fonction de la période sélectionnée.

Cliquez sur le tableau de bord **Incidents and Alerts (Incidents et alertes)** pour chaque portée disponible **(Incidents and Alerts (Incidents et alertes) > Prisma Access / NGFW > All Incidents (Tous les incidents))**.

Meilleures sous-catégories pour Incidents de santé ouverts

Le widget **Top Subcategories for Open Health Incidents (Meilleures sous-catégories pour Incidents de santé ouverts)** vous donne un aperçu des meilleures sous-catégories d'incidents de santé ouverts sur votre réseau, organisées par portée, sous-catégorie, quantité d'incidents, et ce qui est touché (centres de données, sites, appareils, etc.).

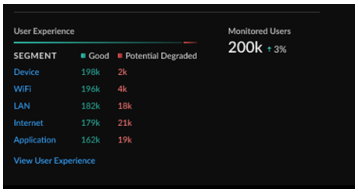
Le widget affichera les cinq premières sous-catégories pour une portée unique, ou les deux premières sous-catégories pour plusieurs portées lorsqu'elles sont disponibles.



Cliquez sur le tableau de bord **Incidents and Alerts (Incidents et alertes) (Incidents and Alerts (Incidents et alertes) > Prisma Access / NGFW / Prisma SD-WAN)** pour plus de détails sur les incidents.

Utilisateurs surveillés et expérience utilisateur

Le widget **Open Incidents and User Experience (Incidents ouverts et expérience utilisateur)** vous donne une vue sur le nombre total d'incidents ouverts, la ventilation de l'expérience utilisateur bonne et potentiellement dégradée de segments individuels de la chaîne de prestation de services d'un périphérique utilisateur à une application, et la modification des incidents ouverts à partir d'une plage de temps sélectionnée.



Cliquez sur le tableau de bord **Application Experience (Expérience de l'application) (Dashboards (Tableaux de bords) > Application Experience (Expérience de l'application))** pour une ventilation plus détaillée de l'expérience sur votre réseau et des mesures de performance.

Meilleures pratiques

Sécurité des données

La vue **Data Security (Sécurité des données)** affiche toutes les données sensibles détectées sur votre réseau et diverses applications SaaS connectées. Vous pouvez l'utiliser pour surveiller et identifier les flux de données sensibles à haut risque dans votre entreprise.

Licences de sécurité des données	• Licences de sécurité des données, notamment : ❑ Licence SaaS Security ❑ Licences de sécurité des données ❑ Licence Enterprise DLP

Vue centrale de la sécurité des données

La vue centrale de la sécurité des données fournit la carte des données sensibles et à haut risque sur votre réseau et les applications SaaS connectées. Le centre de commande vous donne un aperçu des utilisateurs de données sensibles dans l'organisation, des applications spécifiques sanctionnées, non sanctionnées, tolérées ou non marquées où une activité de données sensibles a été détectée (chargement, téléchargement ou exposition de ressources) ainsi que le nombre de ressources autorisées, bloquées, mises en quarantaine, révoquées, partagées ou exposées.

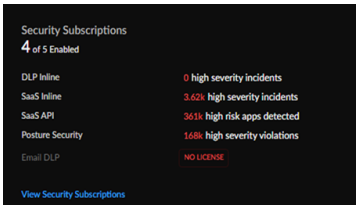
Les lignes de la vue centrale Sécurité des données représentent les données sensibles détectées grâce à des solutions de sécurité des données au repos et des données en mouvement, l'épaisseur des lignes représentant la quantité de données et la couleur indiquant si ces données ont été signalées ou classées comme critiques, à risque élevé, moyen ou faible.

Abonnements de sécurité

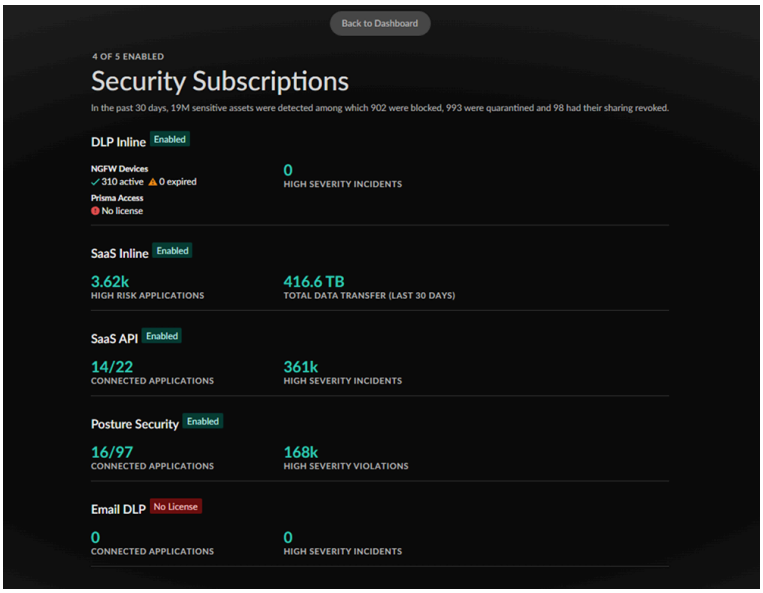
Le widget **Security Subscriptions (Abonnements de sécurité)** vous donne une vue sur vos abonnements de sécurité des données, lesquels sont actifs, et un instantané de la façon dont ils sécurisent votre réseau.

Abonnement	Description
DLP Inline	Enterprise DLP est un service cloud qui utilise des algorithmes d'apprentissage automatique supervisé pour

Abonnement	Description
	trier les documents sensibles en catégories afin de se prémunir contre les expositions, les pertes de données et l'exfiltration de données.
SaaS Inline	La solution SaaS Inline permetStrata Logging Service de découvrir toutes les applications SaaS utilisées sur votre réseau.
API SaaS	SaaS API est un service cloud que vous pouvez connecter directement à vos applications SaaS sanctionnées à l'aide de l'API de l'appli cloud et fournir la classification des données, le partage ou la visibilité des autorisations, ainsi que la détection des menaces au sein de l'application.
Sécurité des postures	La gestion de la posture de sécurité des données (SSPM, SaaS Security Posture Management) permet de détecter et de corriger les paramètres mal configurés dans les applications SaaS sanctionnées grâce à une surveillance continue.
Email DLP	Email DLP est un module supplémentaire de Enterprise DLP qui empêche l'exfiltration des e-mails contenant des informations sensibles avec des détections de données alimentées par IA/ML.

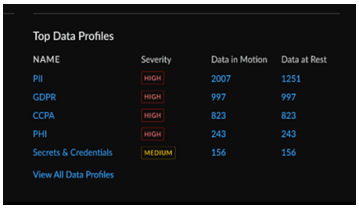


En cliquant sur le widget **Security Subscriptions (Abonnements de sécurité) (Command Center (Centre de commandes) > View Security Subscriptions (Afficher les abonnements de sécurité)**, vous obtenez un rapport détaillé sur l'état de vos abonnements par rapport à vos déploiements NGFW et Prisma Access. Cliquez sur **Back to the Dashboard (Retour au tableau de bord)** pour revenir à la vue **Data Security (Sécurité des données)**.



Profils de données majeurs

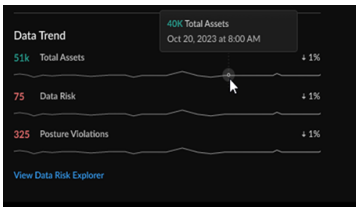
Le widget **Top Data Profiles (Profils de données majeurs)** affiche les profils de données les plus détectés pour toutes les données sensibles inspectées, la gravité du profil de données ainsi que le nombre de correspondances détectées en ligne avec les données en mouvement par rapport aux données au repos.



Cliquez sur le tableau de bord **Data Loss Prevention (Prévention des pertes de données) (Gérer > Configuration (Configuration) > Data Loss Prevention (Prévention des pertes de données - DLP))** pour examiner tous les profils de données prédéfinis et ajouter des profils de données personnalisés.

Tendance des données

Le widget **Data Trend (Tendance des données)** montre la tendance des données sensibles surveillées par vos abonnements de sécurité de données, organisée en fonction de la variation en pourcentage du total des actifs, des risques liés aux données et des violations de posture.



Cliquez sur le tableau de bord du **Data Risk (Risque de données) (Manage (Gérer) > Configuration (Configuration) > Data Loss Prevention (Prévention des pertes de données - DLP) > Data Risk**

(Risque de données)) pour comprendre votre score global de risque de données et passer en revue les recommandations concrètes en vue d'améliorer la posture de sécurité des données de votre organisation.

Informations : Informations sur l'activité

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels • Prisma SD-WAN	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Prisma SD-WAN ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Les autres licences et prérequis nécessaires pour accéder à certaines vues Informations sur les activités sont : ☐ Strata Logging Service ☐ Services de sécurité fournis par le cloud (CDSS) ☐ Observabilité ADEM ☐ Rapport WAN Clarity ☐ Un rôle qui a l'autorisation d'afficher le tableau de bord → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

L'outil Informations sur l'activité vous offre une vue détaillée des activités de votre réseau Prisma Access et les déploiements NGFW. Cette vue rassemble vos données réseau telles que le trafic réseau, l'utilisation des applications, les menaces et les activités des utilisateurs en un seul endroit. L'outil Informations sur l'activité fournit des fonctionnalités de visualisation, de surveillance et de création de rapports pour vous permettre d'effectuer vos tâches en toute simplicité. Une fois que vous avez identifié les domaines qui nécessitent votre attention avec le centre de commande Strata Cloud Manager, utilisez les liens contextuels pour accéder à l'outil Informations sur l'activité ou à d'autres tableaux de bord pour une analyse plus approfondie.

L'outil Informations sur l'activité dispose de filtres avancés pour vous aider à vous concentrer sur les aspects de la sécurité qui comptent pour votre déploiement. La fonctionnalité de création de rapports avancée dans l'outil Informations sur l'activité vous permet de télécharger, de partager

et de planifier des rapports à partir des données de l'onglet Présentation. Le rapport présente les données séparément pour chaque filtre appliqué dans le tableau de bord. Vous pouvez également planifier des rapports pour l'outil Informations sur l'activité et des tableaux de bord à partir du **Strata Cloud Manager** > **menu** des rapports.

Lancez Strata Cloud Manager et cliquez sur **Informations** () pour commencer.

Que vous montre l'outil Informations sur l'activité ?

L'outil Informations sur l'activité affiche des données agrégées par Strata Logging Service locataire déployé dans Prisma Access et les environnements NGFW. Vous pouvez filtrer les données pour un déploiement spécifique. L'outil Informations sur l'activité comporte différents onglets. Chacun de ces onglets fournit une vue unifiée des données réseau par rapport aux applications, aux utilisateurs, aux menaces, aux URL et à l'utilisation du réseau.

- **Présentation** : affiche les données relatives aux applications, aux menaces, aux utilisateurs, aux URL et aux sessions avec le nombre maximal d'activités impliquées dans la plage de temps sélectionnée. Parcourez cette vue pour identifier rapidement toute irrégularité au sein de votre réseau, puis approfondissez pour examiner les activités qui nécessitent une enquête.
- **Applications** : aperçu de toutes les utilisations des applications sur le réseau, notamment le transfert de données, les risques liés aux applications et les capacités ADEM pour surveiller l'expérience des applications.
- **Applications SD-WAN** : affichez les performances des applications Prisma SD-WAN avec des détails sur le score de santé pendant une période donnée, les statistiques de transaction et les mesures d'utilisation de la bande passante.
- **Menaces** : fournit une vue d'ensemble de toutes les menaces que les services de sécurité de Palo Alto Networks ont détectées et bloquées sur votre réseau.
- **Utilisateurs** : fournit des informations plus approfondies sur le trafic et les activités d'un utilisateur, y compris les capacités d'ADEM à surveiller l'expérience utilisateur.
- **URL** : affiche les URL consultées sur votre réseau, combien d'entre elles sont malveillantes, les utilisateurs et les applications accédant aux URL, les règles autorisant les URL sur votre réseau et l'application par vos services de sécurité.
- **Règles** : donne des informations sur les règles de politique de sécurité autorisant le trafic généré par les utilisateurs et les applications, les menaces détectées dans les sessions de trafic et les URL impactant la règle.
- **Régions** : affiche les détails du trafic réseau par rapport aux applications, aux utilisateurs, aux menaces et aux URL.

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

Les informations suivantes peuvent vous aider :

- Identifiez les applications que vous souhaitez surveiller, améliorez l'expérience utilisateur des applications ayant des scores faibles et contrôlez les applications non autorisées et risquées.
- Affichez les menaces les plus pertinentes pour votre déploiement et obtenez un aperçu des menaces à enquêter.
- Affinez vos règles de politique de sécurité et vos règles de trafic en fonction de vos conclusions tirées des journaux pour combler les failles de sécurité.

- Surveillez l'activité des utilisateurs pour détecter et arrêter les menaces potentielles et protéger l'utilisation abusive d'informations sensibles.

Informations sur l'activité : Vue d'ensemble

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels • Prisma SD-WAN	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Les autres licences et prérequis nécessaires pour accéder à certaines vues Informations sur les activités sont : ❑ Strata Logging Service ❑ Services de sécurité fournis par le cloud (CDSS) ❑ Observabilité ADEM ❑ Rapport WAN Clarity ❑ Un rôle qui a l'autorisation d'afficher le tableau de bord → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Afficher le résumé des applications, menaces, utilisateurs, URL et règles les plus observées dans votre réseau pour la période sélectionnée. Cette vue permet d'identifier rapidement toute irrégularité au sein de votre réseau, puis d'approfondir l'examen de l'activité qui nécessite une enquête. La vue d'ensemble comprend :

- Les 5 applications et catégories d'applications les plus actives de votre réseau en termes de nombre de sessions, de transfert de données, de menaces détectées, d'URL accessibles et d'utilisateurs ayant accédé aux applications. Cliquer sur **Afficher toutes les applications** pour se référer aux détails de l'application.

- Les 5 principales menaces et catégories de menaces qui affectent le plus les sessions, les utilisateurs et les applications. Afficher les détails des sessions, des utilisateurs et

des applications dans les onglets Visionneuse de journaux, Utilisateurs et Applications respectivement.

- Tendance du trafic réseau des sessions bloquées, autorisées et alertées, quantité de données transférées et utilisateurs générant le plus de trafic.

- Top 5 des utilisateurs ayant le plus de sessions de trafic, de données transférées, de menaces détectées dans le trafic, d'URL accédées et de scores d'expérience utilisateur pour les applications surveillées.
- Les URL les plus consultées avec des détails sur la session, les utilisateurs et les applications accédant aux URL.

- Les 5 règles de sécurité les plus impactantes configurées dans votre déploiement avec des filtres afin de connaître les sessions, les utilisateurs, les URL, les menaces, les données transférées, les applications impliquées dans le trafic correspondant aux règles.

Vous pouvez utiliser les filtres pour afficher les points de données sur lesquels vous souhaitez vous concentrer et qui sont pertinents au regard de votre déploiement. Ces filtres sont disponibles dans tous les onglets du tableau de bord.

Filtres

L'outil Informations sur l'activité dispose de filtres avancés pour vous aider à vous concentrer sur les aspects de la sécurité qui comptent pour votre déploiement. Les filtres disponibles sont les suivants :

- **Plage horaire** : afficher les données pour une période de temps spécifiée
- **Sélection de la portée** : données spécifiques à un déploiement : Prisma Access, NGFW
- **Sous-locataire** : instance Prisma Access pour laquelle les données sont affichées
- **Nom d'utilisateur** : afficher les activités impliquant un utilisateur individuel
- **Application** : événements réseau concernant une application spécifique
- **Type d'application** : type d'application ; SaaS, Internet, privé
- **Catégorie de menace** : les données relatives à une catégorie particulière de menaces
- **Activité de la menace** : vue spécifique des menaces autorisées ou bloquées
- **Niveau de risque de l'URL** : les données concernant les URL avec un niveau de risque spécifique ; élevée, moyenne ou faible
- **Catégorie d'URL** : filtrer les données en fonction de la catégories d'URL
- **Emplacement de la source** : afficher l'activité provenant d'un emplacement spécifique
- **Lieu de destination** : afficher l'activité ciblée sur une région spécifique
- **URL** : activité liée à une URL spécifique consultée.

- **Application SaaS** : données relatives à une application SaaS spécifique
- **Demande sanctionnée** : afficher les données des applications approuvées ou non approuvées uniquement
- **Type de port** : trier le trafic des applications traversant des ports standard ou non standard.
- **Protocole** : afficher le trafic qui utilise des ports TCP, UDP ou HTTP spécifiques
- **Type de source** : afficher l'activité générée par un appareil, des utilisateurs ou d'autres personnes en particulier.

Rapports

Cliquez sur l'une des icônes,  dans l'**Aperçu** pour télécharger, partager et planifier des rapports à partir des données de l'ongletAperçu Vous pouvez également planifier des rapports à partir des menus**Strata Cloud Manager** > **Rapports**; cliquez sur l'icône et sélectionnez Informations sur l'activité – Résumé dans la liste déroulante **Type**.

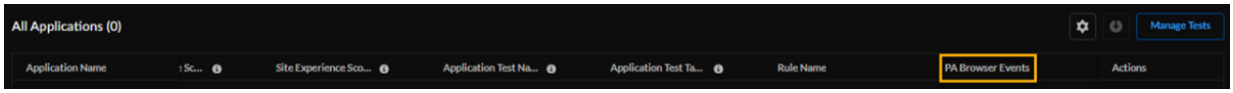
Informations sur l'activité : Applications

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	Vous devez disposer d'au moins une de ces licences pour utiliser l'onglet Informations sur l'activité : ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) ou AIOps for NGFW Premium license (use the Strata Cloud Manager app) Les autres licences nécessaires pour afficher l'onglet Informations sur l'activité : Applications sont les suivantes : ❑ Strata Logging Service ❑ ADEM Observability débloqueront des fonctionnalités Prisma supplémentaires

Surveiller les applications dans vos configurations Prisma Access et NGFW, les utilisateurs utilisant l'application. Les scores de risque, l'expérience utilisateur pour chaque application, et comprenez l'impact sur la sécurité posé par les applications à risque. Les résultats concernant l'utilisation des applications peuvent vous aider à affiner votre politique de sécurité afin de contrôler les applications non autorisées et à risque. Cliquez sur **Informations sur l'activité > Applications** en vue d'afficher les informations suivantes :

- **Applications par scores de risque** : le nombre total d'applications en cours d'exécution dans votre organisation et le nombre d'applications qui réussissent bien, passable et médiocre. Les applications sont classées en trois catégories : bonnes, moyennes et médiocres, sur la base de leur scores d'expérience.
- **Transfert de données d'application** : total des données téléchargées et téléchargées à travers les pare-feu NGFW et Prisma Access pendant l'intervalle de temps sélectionné. Vous pouvez filtrer pour afficher le transfert de données provenant de la catégorie d'application et transitant par la destination depuis l'appareil (centre de données ou pare-feu).
- **Toutes les applications** : utilisez ce widget pour voir quelles applications Prisma Access sont surveillées avec des tests synthétiques exécutés sur elles et des applications exécutées sur vos environnements NGFW. Le tableau affiche également leur score d'expérience, qui vous donne l'état de chaque application. Si vous disposez d'un abonnement au navigateur Prisma Access,

une colonne pour **PA Browser Events** s'affiche. Sélectionner le nombre d'événements et il vous redirigera vers les pages de gestion du navigateur Prisma Access.



Vous pouvez télécharger les données du tableau au format csv (applications Prisma Access uniquement). Cliquez sur le bouton **Gérer les tests** afin d'afficher tous les tests synthétiques mis en place pour toutes vos applications Prisma Access dans la table Tests d'application. Si vous souhaitez créer un test pour surveiller une application, cliquez sur **Contrôler l'application pour afficher son état** sous la colonne Expérience utilisateur.

- **Les informations sur l'application** : voir les détails généraux de l'application ainsi que les détails concernant l'activité de l'application et l'expérience de l'application.
  - L'onglet **Activité** indique le nombre total de menaces observées dans l'application, le nombre total d'utilisateurs accédant à l'application, les données transférées via l'application, les événements liés aux données du navigateur PA et les événements liés à l'accès au navigateur PA.

    L'image suivante montre les informations de l'application sur les **événements de données du navigateur PA** et les **événements d'accès au navigateur PA**. L'affichage par défaut présente un **agrégat** de tous les événements et des événements bloqués, ou vous pouvez choisir d'afficher une **ventilation** par **type d'événement** et **nombre**.

  - L'onglet **Expérience** affiche le score d'expérience de l'application, la tendance du score pendant la plage de temps sélectionnée et les indicateurs de performance réseau.

Si une application est une appli conteneur, les statistiques affichées sont une synthèse de toutes les applications du conteneur. Par exemple, gmail est une application conteneur (il est impossible d'obtenir un App-ID pour gmail). Il regroupe des applications telles que gmail-posting, gmail-downloading, gmail-uploading, et autres. Le score de risque défini pour cette application conteneur est le score de risque le plus élevé trouvé pour les applications contenues. Toutes les autres mesures sont calculées en additionnant les valeurs trouvées pour les applications contenues.

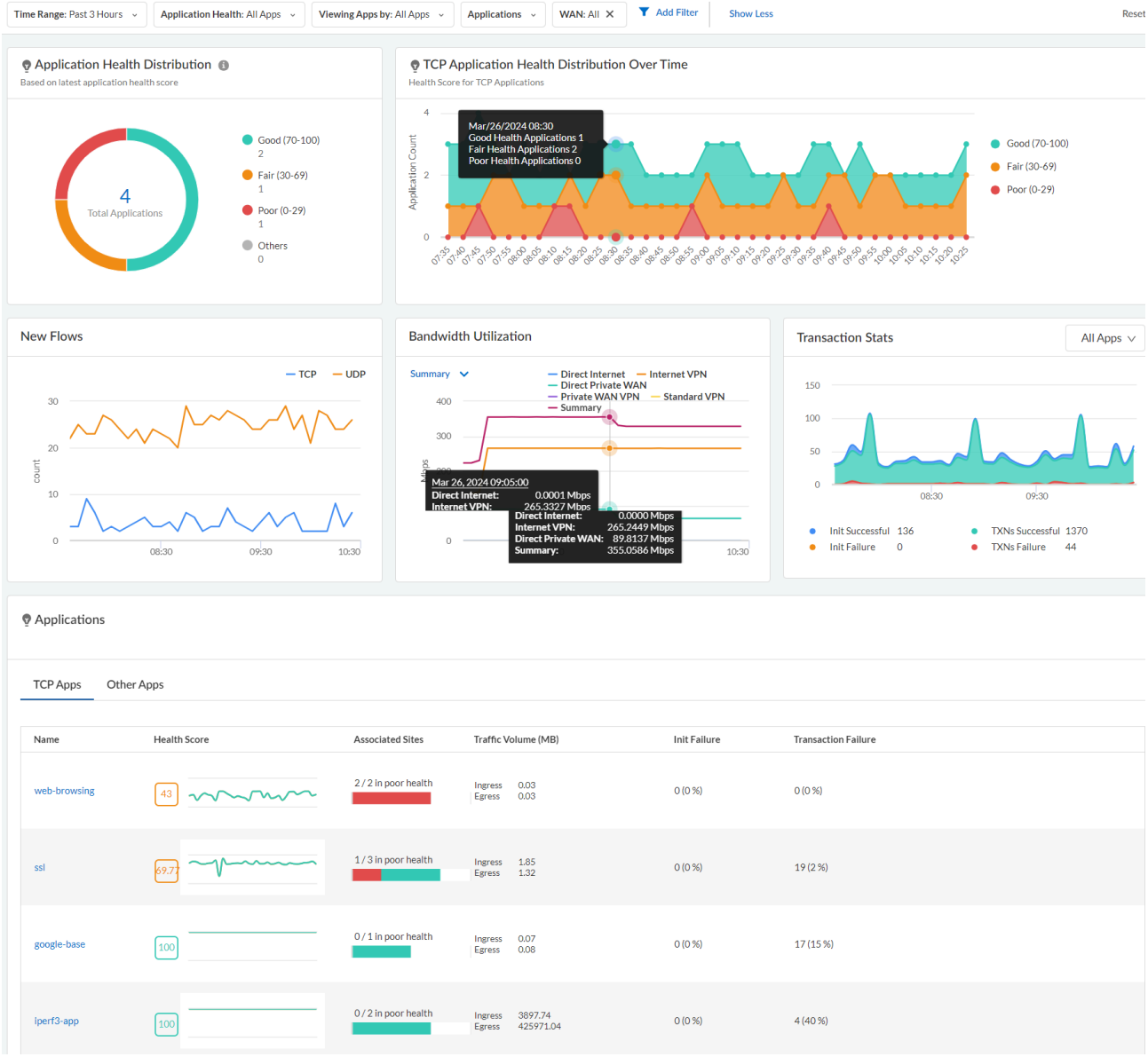
Rapports : vous ne pouvez pas générer un rapport couvrant les données de cette vue. Toutefois, vous pouvez utiliser le rapport **Utilisation des applications** pour afficher les données d'utilisation

des applications dans votre réseau. Pour planifier un rapport, dans le menu **Strata Cloud Manager** > **Rapports**, cliquez sur l'icône et sélectionnez Utilisation de l'application dans la liste déroulante **Type**.

Informations sur l'activité : Applications SD-WAN

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma SD-WAN	❑ Licence Prisma SD-WAN ❑ Licence WAN Clarity Reporting pour afficher certains widgets

Afficher les principales applications qui ne fonctionnent pas bien dans Prisma SD-WAN. Afficher le score de santé déterminé pour toutes les mauvaises applications, la liste des mauvaises applications pour un locataire en fonction du score de santé, et le score de santé moyen des mauvaises applications pour les 3 dernières heures par intervalles de 5 minutes.



- **Distribution de l'état des applications** (nécessite une licence WAN Clarity) : La répartition des demandes bonnes, moyennes et médiocres pour un locataire donné.
- **Distribution de l'état de l'application TCP au fil du temps** (nécessite une licence WAN Clarity) : La distribution des applications TCP de bonne, moyenne et mauvaise qualité sur une période donnée. Le graphique de la série temporelle doit être calculé et actualisé en fonction de la durée sélectionnée. Par exemple, les durées prises en charge sont de 1 heure, 3 heures, un jour, sept jours, 30 jours et 90 jours, et l'intervalle est de 1 minute, 5 minutes, 1 heure et un jour, respectivement.
- **Nouveaux flux** : Affiche les nouveaux flux TCP et UDP pour une application, un ensemble spécifique d'applications ou toutes les applications pour une période donnée. Un flux TCP est considéré comme nouveau lorsqu'il voit le premier paquet SYN. Un flux UDP est considéré comme un nouveau flux lorsqu'il voit le premier paquet UDP dans l'une ou l'autre direction. Un flux est une séquence de paquets dans les deux directions, identifiée par l'IP de la source et de la destination, le port de la source et de la destination, et le protocole.
- **Utilisation de la bande passante** : Le graphique de l'utilisation de la bande passante affiche la quantité de bande passante utilisée sur un sentier dans un réseau. Utiliser le tableau pour identifier la congestion du réseau WAN dans un réseau qui peut entraver les performances de l'application. Il s'agit d'une représentation visuelle du pic de bande passante, de la bande passante totale consommée par un site particulier, et de l'application ; si le téléchargement se fait dans la direction d'entrée ou de sortie. Déplacez votre curseur dans le graphique de l'utilisation de la bande passante pour obtenir une vue plus granulaire de l'utilisation de la bande passante avec une application ou un horodatage. En règle générale, les applications sont classées par ordre d'utilisation de la bande passante.
- **Statistiques de transaction** : Fournit des statistiques de transaction sur les flux TCP, y compris les succès et les échecs d'initiation/transaction pour une application spécifique ou toutes les applications, un chemin particulier ou tous les chemins, et tous les événements de santé.
- **Applications** : Répertorie tous les détails de l'application, tels que le nom, le profil d'application, le score d'intégrité, les sites impactés, le volume de trafic, l'initialisation/l'échec et la transaction/l'échec. Lorsque vous cliquez sur le nom de l'application, vous pouvez voir les détails de l'application individuelle sur une nouvelle page.

Informations sur l'activité : Menaces

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	Vous devez disposer d'au moins une de ces licences pour utiliser l'outil Informations sur l'activité : ☐ Prisma Access ☐ AIOps for NGFW Free (use the AIOps for NGFW Free app)AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Les autres licences nécessaires pour afficher l'onglet Informations sur l'activité : menaces sont les suivantes : ☐ Strata Logging Service ☐ Les licences CDSS ☐ ADEM Observability débloqueront des fonctionnalités supplémentaires de Prisma Access

Obtenez une vue d'ensemble de l'activité des menaces et des différents types de menaces observées sur votre réseau. L'onglet montre le nombre total de sessions de menaces observées dans vos déploiements Prisma Access et NGFW, la répartition des chiffres en fonction de la catégorie et de la gravité de la menace pour la période sélectionnée. Vous pouvez effectuer une recherche sur un artefact de sécurité (hachage de fichier, URL, domaine ou adresse IP (IPv4 ou IPv6)) associé à une menace pour connaître l'analyse des renseignements sur les menaces de Palo Alto Networks et les conclusions des analyses de tiers.

Examinez les détails suivants concernant les menaces propres à votre réseau :

- **Nom de menace** – Nom de signature de menace. Utilisez ceci pour trouver les dernières informations de l'archivage sécurisé des menaces sur la menace, y compris toutes les sessions de menaces pendant une plage de temps.
- **ID de la menace** – ID de signature de menace unique. Utilisez l'ID de la menace pour rechercher les dernières informations relatives à cette signature dans la base de données des menaces de Palo Alto Networks.
- **Catégorie et sous-catégorie** de menaces : le type de menaces sur la base des signatures de menaces (antivirus, logiciels espions (C2) et vulnérabilité).
- **Licences** : services de sécurité de Palo Alto Networks ayant détecté la menace.

- **Sévérité** : la gravité de la menace est déterminée en fonction de la facilité d'exploitation de la vulnérabilité, de l'impact sur la vulnérabilité, de l'omniprésence du produit vulnérable, de l'impact de la vulnérabilité, etc. La gravité est classée comme suit :
  - Critique : cette vulnérabilité affecte les installations par défaut de logiciels très largement déployés et les exploits peuvent compromettre l'accès à la racine. Le code d'exploitation (informations sur la manière d'exploiter le code du système, méthodes, preuve de concept (POC)) est largement disponible et facile à exploiter. Le pirate n'a pas besoin d'informations d'authentification particulières, ni de connaissances sur les victimes individuelles.
  - Élevée : menaces pouvant devenir critiques, mais ayant des facteurs atténuants; par exemple, elles peuvent être difficiles à exploiter, ne mènent pas à des privilèges élevés ou ne ciblent pas un grand nombre de victimes.
  - Moyenne : menaces mineures dont l'impact est minimisée, telles que les attaques DoS qui ne compromettent pas la cible ou les exploitations nécessitant qu'un pirate soit hébergé sur le même réseau local que la victime, affectent uniquement les configurations non standard ou les applications obscures, ou fournissent un accès très limité.
  - Faible : menaces à surveiller ayant très peu d'incidence sur l'infrastructure de l'entreprise. Celles-ci requièrent généralement un accès au système physique ou local et peuvent entraîner des problèmes DoS ou de confidentialité de la victime, ainsi qu'une fuite des informations.
  - Informationnel : événements suspects qui ne constituent pas une menace immédiate, mais qui sont signalés pour attirer l'attention sur l'existence possible de problèmes plus graves.
- **Sessions totales** : le nombre de sessions où la menace a été détectée. Cliquez sur le nom de la menace pour afficher toutes les sessions de menaces associées dans la période spécifiée. Le tableau des sessions de menaces fournit le contexte de la menace, comme l'heure à laquelle les services de sécurité de Palo Alto Network ont détecté les menaces, les utilisateurs, les règles, les applications, les appareils touchés par la menace et la mesure prise (autorisée ou bloquée) face à la menace.
- **Nombre total d'utilisateurs** : nombre d'utilisateurs exposés à la menace.
- **Menaces autorisées et menaces bloquées** : examinez la mesure prise face à la menace pour vous assurer que les mesures ne déclenchent pas de faux positifs sur votre réseau.
- **Actions** : enquêtez sur l'historique des journaux de la menace dans la Visionneuse de journaux.

Rapports : vous ne pouvez pas générer de rapport couvrant les données de cette vue.

Informations sur l'activité : Utilisateurs

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	Vous devez disposer d'au moins l'une de ces licences pour utiliser l'outil Informations sur l'activité : ❑ Prisma Access ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) ou AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Les autres licences nécessaires pour consulter les informations sur l'activité : Les onglets utilisateurs sont : ❑ Strata Logging Service ❑ Advanced URL Filtering licences ❑ Cloud Identity Engine licences ❑ Advanced Threat Prevention licence ❑ ADEM Observability débloquera des fonctionnalités supplémentaires de Prisma Access

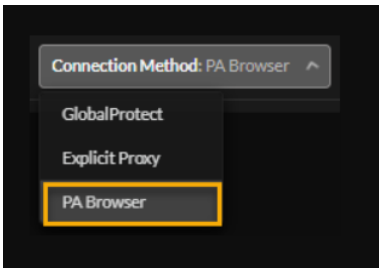
Surveillez l'activité des utilisateurs dans vos environnements Prisma Access et NGFW. Vous pouvez afficher les données des utilisateurs qui se connectent aux services de sécurité Prisma Access et NGFW soit via l'application GlobalProtect sur leurs périphériques, soit via Explicit Proxy à l'aide d'un navigateur Web sur leurs périphériques. La surveillance de l'activité des utilisateurs permet de détecter et d'arrêter les menaces potentielles, de protéger l'utilisation abusive d'informations sensibles et d'ajuster les règles de la politique de sécurité pour combler les lacunes.

Vous pouvez filtrer les données utilisateur en fonction de :

- Déploiement ; Prisma Access, NGFW
- Méthodes et versions de connexion ; GlobalProtect, Explicit Proxy, Prisma Access Browser
- Nom d'utilisateur
- Nom du périphérique
- Emplacement d'origine du trafic et emplacements Prisma Access
- Applications auxquelles les utilisateurs accèdent et filtres de score d'expérience utilisateur

Consultez les informations suivantes ici :

- **Utilisateurs connectés/actifs** : surveiller les données agrégées sur vos utilisateurs actuellement connectés à GlobalProtect, Utilisateurs mobiles de proxy explicite et leNavigateur Prisma Access.



  Afficher le nombre d'utilisateurs connectés à votre réseau au moment où les données ont été récupérées ou comme indiqué dans l'horodatage. Il est possible **d'afficher les tendances par utilisateurs** ou par **périphérique utilisateur**. Sélectionner le numéro pour afficher le tableau **Utilisateurs connectés | périphériques utilisateurs connectés** pour plus d'informations sur tous les utilisateurs connectés et tous leurs périphériques.

  Afficher les données d'accès aux privilèges dynamiques dans **afficher la tendance par utilisateurs** ou par **périphérique utilisateur**, **Utilisateurs connectés | Périphériques utilisateur connectés**et **Distribution du projet par théâtre**.

- **Utilisateurs surveillés** : afficher le nombre total d'utilisateurs ou de périphérique utilisateur surveillés par ADEM et leur expérience utilisateur moyenne, qui est le score d'expérience agrégé pour tous les utilisateurs surveillés sur ADEM. Cliquez sur le numéro pour afficher les détails de l'activité de l'utilisateur par rapport à l'expérience utilisateur.
- **Utilisateurs à risque** : afficher le nombre d'utilisateurs impactés par les menaces. La flèche vers le haut ou vers le bas compare cette plage de temps avec une plage de temps précédente pour déterminer la différence, en pourcentage, du nombre de périphériques connectés. Sélectionner Afficher plus de détails pour les versions de GlobalProtect ou l'utilisation du pool d'adresses IP pour voir les détails sur les utilisateurs à risque dans votre environnement.
- **Les détails de la version de GlobalProtect** affichent les versions de GlobalProtect installées sur vos périphériques. Vous pouvez voir combien d'utilisateurs se connectent à chaque version. Utilisez les données pour assurer la conformité avec la dernière version de l'application GlobalProtect. Passer la souris sur les lignes de tendance de distribution pour voir les adresses IP des utilisateurs connectés à ce moment-là.
- **Consulter l'utilisation du pool IP** par différents théâtres d'allocation de pool IP en fonction du nombre d'utilisateurs connectés à ce moment-là. Le pourcentage d'utilisation du pool IP sur le graphique correspond au nombre de blocs de pool IP utilisés parmi tous les blocs de pool IP disponibles sur tous les sous-réseaux. Vous pouvez prendre des mesures proactives en ajoutant des sous-réseaux lorsque vous voyez une barre de pool IP approchant la capacité maximale pour une région.
- Le tableau **Utilisateurs** affiche des informations sur les utilisateurs connectés pendant la période. Cliquez sur le nom d'utilisateur pour obtenir une visibilité sur les habitudes de

navigation d'un utilisateur individuel : ses sites les plus fréquemment visités, les sites avec lesquels il transfère des données et les tentatives d'accès à des sites à haut risque.

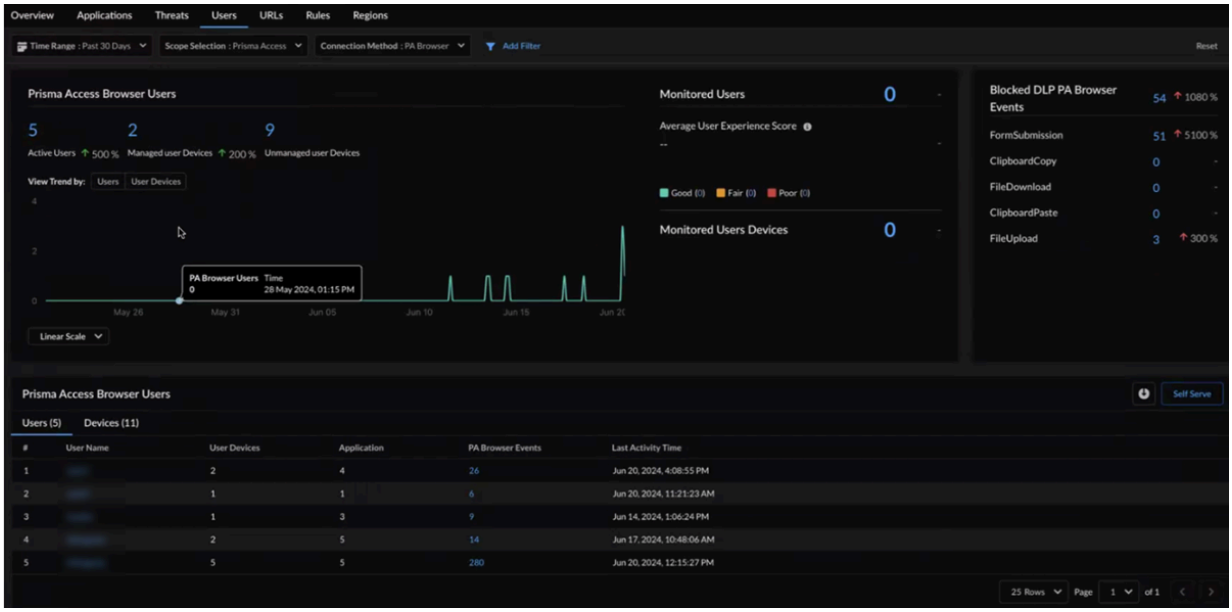
- **Menaces**
  - **Résumé de navigation** : consultez les chiffres relatifs aux types de sites avec lesquels l'utilisateur a effectué le plus de transfert de données et le nombre de visites sur le site par l'utilisateur.
  - **Top 10 des catégories d'URL les plus visitées** : afficher les principales catégories d'URL pour l'utilisateur en fonction du transfert de données. Vous pouvez également voir le nombre d'URL uniques consultées qui relèvent de chaque catégorie d'URL.
  - **Résumé de la navigation par URL** : parmi les URL uniques visitées par l'utilisateur, faites attention aux visites vers des URL malveillantes et à haut risque : ces sites peuvent exposer votre réseau à des menaces, à des pertes de données et à des violations de conformité. Si le nombre de visites sur ces sites est plus élevé que prévu, modifiez la règle de votre politique de sécurité afin de combler les lacunes.
  - **Top 10 des URL** : examiner le niveau de risque des sites les plus fréquemment visités par l'utilisateur. Les URL à haut risque doivent être surveillées, car elles sont susceptibles d'exposer votre réseau à des menaces.
  - **URL bloquées par risque** : il s'agit des URL bloquées auxquels l'utilisateur a le plus souvent tenté d'accéder. Consultez les journaux de filtrage des URL et voyez si vous devez ajuster la règle de politique de sécurité pour modifier l'action.
  - **Menaces graves** : afficher le nombre total de menaces détectées pour l'utilisateur et les chiffres basés sur la gravité des menaces. Comparer le nombre avec d'autres utilisateurs. Ajuster la règle de politique de sécurité si les chiffres sont inhabituellement élevés.
  - **Menaces les plus graves** : il s'agit des menaces les plus fréquemment détectées pour l'utilisateur.
- **Connectivité** : affiche la tendance des périphériques sur lesquels l'utilisateur est connecté pendant une période donnée et les détails de connexion de l'appareil pour chaque événement de connexion et de déconnexion de l'utilisateur.
- **Expérience** : fournit les données d'expérience utilisateur pour le périphérique, le score d'expérience et la tendance pour chacune des applications surveillées, ainsi que les mesures de performance pour l'utilisateur surveillé et les applications pour les appareils individuels.

- Navigateur Prisma Access : sélectionnez la **méthode de connexion du navigateur Prisma Access** pour afficher des informations sur vos utilisateurs du navigateur Prisma Access.

  Le graphique de tendance de l'activité **des utilisateurs du navigateur Prisma Access** indique le nombre d'utilisateurs qui ont été actifs à un moment donné dans le filtre de plage de temps sélectionné. Le graphique indique la répartition des périphériques de ces utilisateurs actifs installés avec un agent de connectivité Prisma Access (appareils gérés) et sans aucun agent (utilisateurs non gérés)

  . Le navigateur Prisma Access offre une visibilité inégalée sur les actions d'un utilisateur de navigateur, indiquant si les actions de l'utilisateur sur son appareil en ce qui concerne les actifs de données de l'entreprise sont autorisées ou bloquées par la politique DLP de l'entreprise.

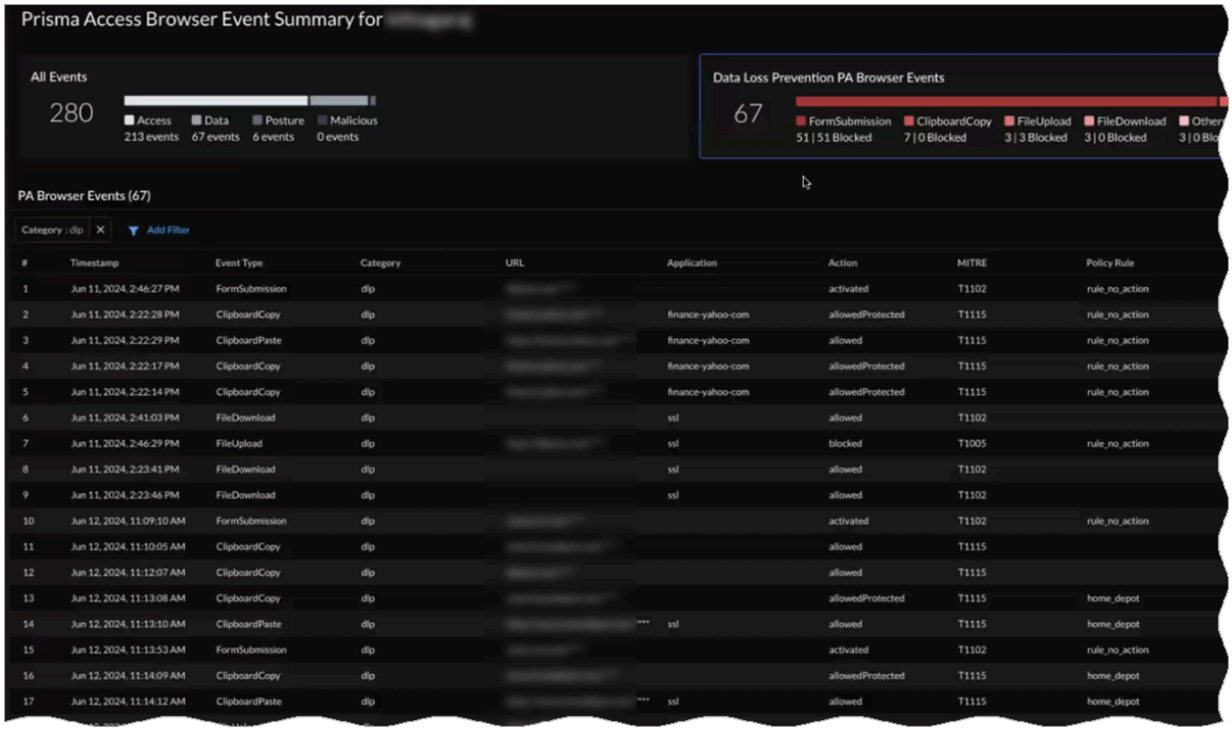
Le widget Événements de navigateur DLP PA bloqués affiche les événements indiquant les actions de l'utilisateur effectuées sur le navigateur qui sont bloquées par la politique.



Le tableau **Utilisateurs du navigateur Prisma Access** affiche la liste des utilisateurs actifs accédant aux applications via le navigateur Prisma Access. Cliquez sur n'importe quel **nom d'utilisateur** pour voir **l'activité** de cet utilisateur dans la page **Activités** > **des détails de l'utilisateur** .

La page **Résumés des événements du navigateur Prisma Access** répertorie toutes les actions du navigateur effectuées par l'utilisateur via le navigateur dans l'intervalle de temps sélectionné. La vue par défaut du tableau **des événements du navigateur PA** affiche la liste de tous **les événements du navigateur** DLP, qu'ils soient autorisés ou bloqués par la politique. Vous pouvez basculer les vues vers d'autres catégories d'événements, telles que **les événements d'accès**, **les événements de posture**ou **les événements malveillants** en sélectionnant la catégorie d'événement appropriée. Dans chaque catégorie **d'événement**, vous pouvez afficher la répartition des types d'événements, ainsi que l'horodatage indiquant le moment où l'événement du navigateur a été exécuté, des informations sur l'URL de

l'application consultée, le nom de l'application et toute note d'attaque MITRE associée pertinente.

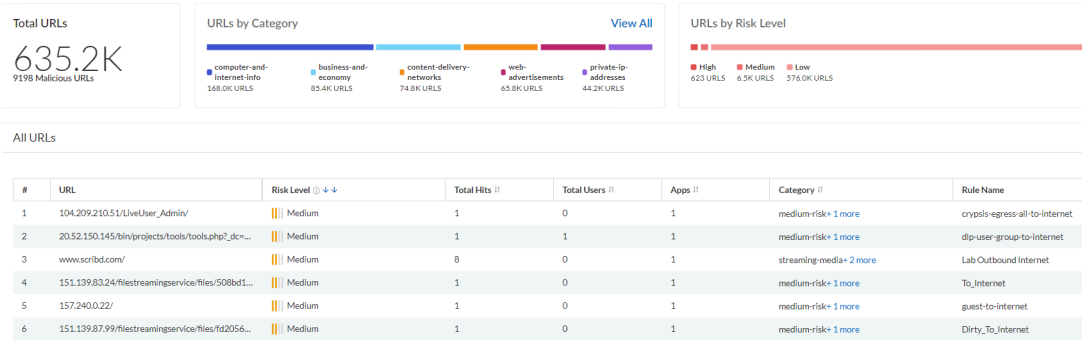


Rapports : vous ne pouvez pas générer un rapport couvrant les données de cette vue. Cependant, vous pouvez utiliser le rapport d'activité utilisateur pour afficher l'activité spécifique à un utilisateur de votre réseau. Afin de planifier un rapport à partir du menu **Strata Cloud Manager** > **Rapports**, cliquez sur l'icône et sélectionnez Utilisateurs dans la liste déroulante **Type**.

Informations sur l'activité : URL

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	Vous devez disposer d'au moins l'une de ces licences pour utiliser l'outil Informations sur l'activité : ☐ Prisma Access ☐ AIOps for NGFW Free (use the AIOps for NGFW Free app) ou AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Les autres licences nécessaires pour consulter les informations sur l'activité : Les onglets des URL sont les suivants : ☐ Strata Logging Service ☐ Advanced URL Filtering licence

Cette vue résume l'activité des URL dans vos déploiements Prisma Access et NGFW que le service de filtrage avancé des URL a détecté. Vous pouvez connaître le nombre total d'URL détectés dans votre réseau pendant la période spécifiée, la répartition de ces URL par catégorie d'URL et le niveau de risque. Utiliser les options de filtrage pour filtrer la vue dans le tableau de bord.



Utiliser les données ici pour

- Identifier les catégories d'URL les plus consultées, les URL uniques avec la catégorie d'URL, l'historique des URL dans votre réseau ainsi que les résultats de l'analyse globale. Sur la base des URL malveillantes filtrées par le service de filtrage des URL, ces catégories d'URL sont susceptibles d'exposer votre réseau à des contenus malveillants et exploitants. C'est une bonne pratique de bloquer ces catégories d'URL.

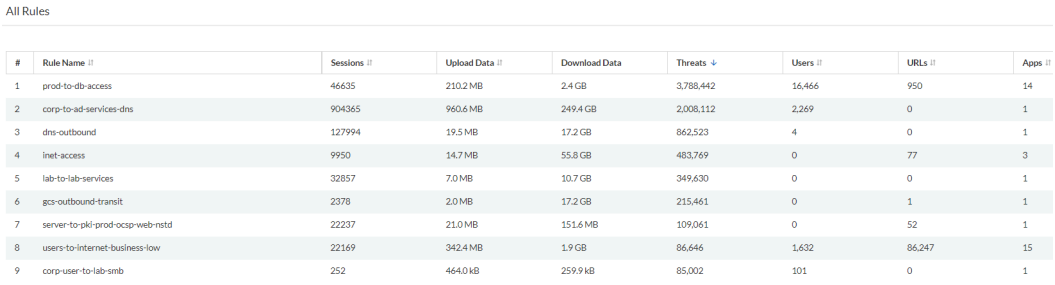
- Examiner les URL à haut risque et leur impact sur les utilisateurs, les applications et les règles. Les sites d'URL à haut risque ne sont pas confirmés comme malveillants. Cependant, ils peuvent toujours exposer votre réseau à des menaces (un site qui n'est pas malveillant, mais qui est hébergé par un FAI à toute épreuve, est un exemple de site à haut risque). Envisagez de cibler ces sites grâce à des règles de décryptage et de politique de sécurité strictes.

Rapports : vous ne pouvez pas générer de rapport couvrant les données de cette vue.

Informations sur l'activité : Règles

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	Vous devez disposer d'au moins l'une de ces licences pour utiliser l'outil Informations sur l'activité : ☐ Prisma Access ☐ AIOps for NGFW Free (use the AIOps for NGFW Free app) ou AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Les autres licences nécessaires pour consulter les informations sur l'activité : L'onglet Règles est le suivant : ☐ Strata Logging Service

Affichez les règles de politique de sécurité qui sont appliquées à l'ensemble du trafic de votre réseau. Les règles de politique de sécurité déterminent la nécessité de bloquer ou d'autoriser une session en fonction des attributs du trafic, tels que l'adresse IP source et de destination, l'application, l'utilisateur et le service. Tout le trafic passant par votre réseau est comparé à une session et chaque session est comparée à une règle de politique de sécurité. Lorsqu'une session correspond, la règle de politique de sécurité est appliquée.


All Rules

#	Rule Name	Sessions	Upload Data	Download Data	Threats	Users	URLs	Apps
1	prod-to-db-access	46635	210.2 MB	2.4 GB	3,788,442	16,466	950	14
2	corp-to-ad-services-dns	904365	960.6 MB	249.4 GB	2,008,112	2,269	0	1
3	dns-outbound	127994	19.5 MB	17.2 GB	862,523	4	0	1
4	inet-access	9950	14.7 MB	55.8 GB	483,769	0	77	3
5	lab-to-lab-services	32857	7.0 MB	10.7 GB	349,630	0	0	1
6	gcs-outbound-transit	2378	2.0 MB	17.2 GB	215,461	0	1	1
7	server-to-pki-prod-ocsp-web-nstd	22237	21.0 MB	151.6 MB	109,061	0	52	1
8	users-to-internet-business-low	22169	342.4 MB	1.9 GB	86,646	1,632	86,247	15
9	corp-user-to-lab-smb	252	464.0 kB	259.9 kB	85,002	101	0	1

Le tableau de bord affiche les informations suivantes sur l'événement réseau correspondant à la règle de politique de sécurité :

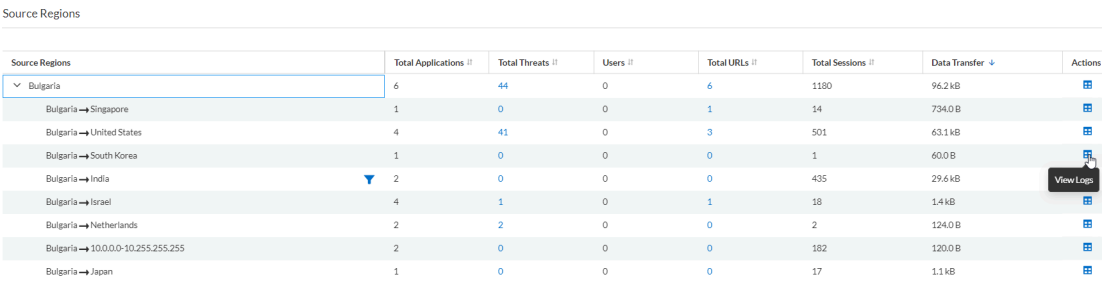
Sessions de trafic, données transférées, menaces détectées au cours des sessions, utilisateurs touchés, URL parcourues et applications consultées. Examinez les règles qui correspondent le mieux aux sessions de trafic, analysez ces sessions pour comprendre si la règle est trop permissive et si elle n'est pas trop restrictive etOptimiser la règle si nécessaire.

Rapports : vous ne pouvez pas générer de rapport couvrant les données de cette vue.

Informations sur l'activité : Régions

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	Vous devez disposer d'au moins l'une de ces licences pour utiliser l'outil Informations sur l'activité : ☐ Prisma Access ☐ AIOps for NGFW Free (use the AIOps for NGFW Free app) ou AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Les autres licences nécessaires pour consulter les informations sur l'activité : L'onglet Régions est le suivant : ☐ Strata Logging Service

Il s'agit des régions à partir desquelles provient le trafic sur votre réseau. Cette vue fournit des informations sur les menaces, les utilisateurs, les URL, les sessions réseau et les transferts de données provenant de ces emplacements. Vous pouvez également approfondir la question pour connaître l'emplacement ciblé du trafic. Cliquez sur Actions pour afficher les Journaux de trafic de la séance. Vous pouvez utiliser les données pour identifier et réduire les régions qui sont des cibles pour les menaces qui tentent d'infiltrer votre réseau. Optimiser la règle qui s'applique aux régions ciblées.



Des options de filtrage permettent de réduire le trafic à destination et en provenance d'une source et d'une destination spécifiques. Les autres options de filtrage sont les suivantes :

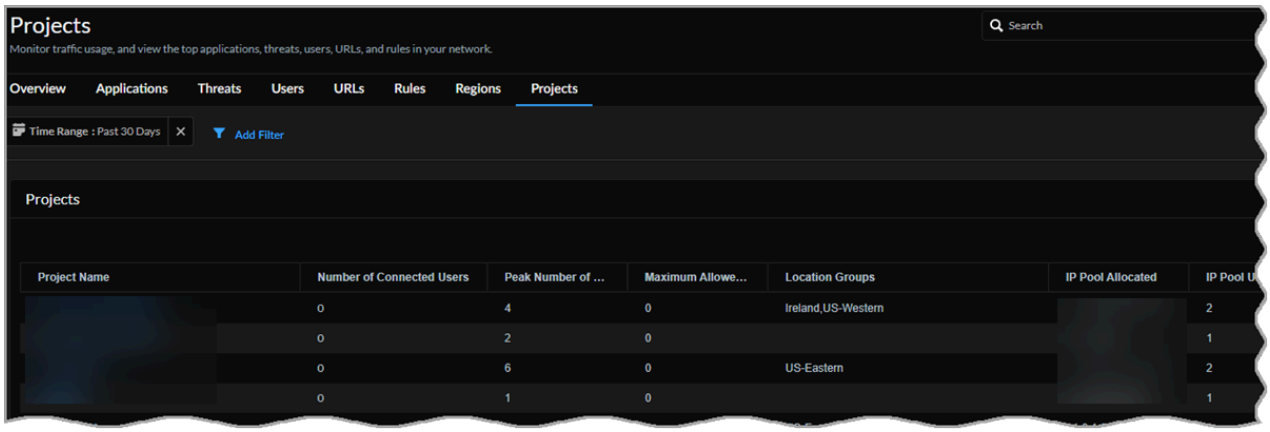
- le trafic observé dans un déploiement spécifique ; Prisma Access, NGFW
- le trafic à destination et en provenance d'applications sanctionnées ou non sanctionnées
- le trafic utilisant des ports et des protocoles spécifiques
- le trafic impliquant des types de menaces, des catégories de menaces, des URL et des catégories d'URL spécifiques

Rapports : vous ne pouvez pas générer de rapport couvrant les données de cette vue. Cependant, vous pouvez consulter le rapport sur l'utilisation du réseau afin d'obtenir des informations détaillées sur le trafic de votre réseau. Pour planifier un rapport, dans le menu **Strata Cloud Manager** > **Rapports**, cliquez sur l'icône et sélectionnez Utilisation du réseau dans la liste déroulante **Type**.

Informations sur l'activité : Projets

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	Vous devez posséder au moins l'une de ces licences pour utiliser l'outil Informations sur les activités : ☐ Prisma Access ☐ AIOps for NGFW Free (use the AIOps for NGFW Free app) ou AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro

Obtenez une visibilité sur votre déploiement de Prisma Access Agent en utilisant Strata Cloud Manager pour surveiller l'activité de votre projet Dynamic Privilege Access.



- Le tableau **Projets** offre un aperçu des projets auxquels les utilisateurs de Dynamic Privilege Access accèdent à l'aide de Prisma Access. Sélectionnez le nom d'un projet pour afficher sa page de détails.
- La page de détails du projet montre :
  - **Aperçu** : voir le nombre maximal d'utilisateurs autorisés et le nombre maximal d'utilisateurs pendant la plage de temps sélectionnée pour ce projet.
  - **Utilisation de pools d'adresse IP** : afficher le nombre d'IP utilisées et le nombre d'IP encore disponibles pour les pools de ce projet.
  - **Utilisateurs connectés** : afficher un graphique des utilisateurs connectés pendant la plage de temps sélectionnée.
  - **Utilisateurs connectés par groupe** de localisation – Consultez le nombre d'utilisateurs par groupe de localisation Prisma Access dans lequel ils se trouvent.

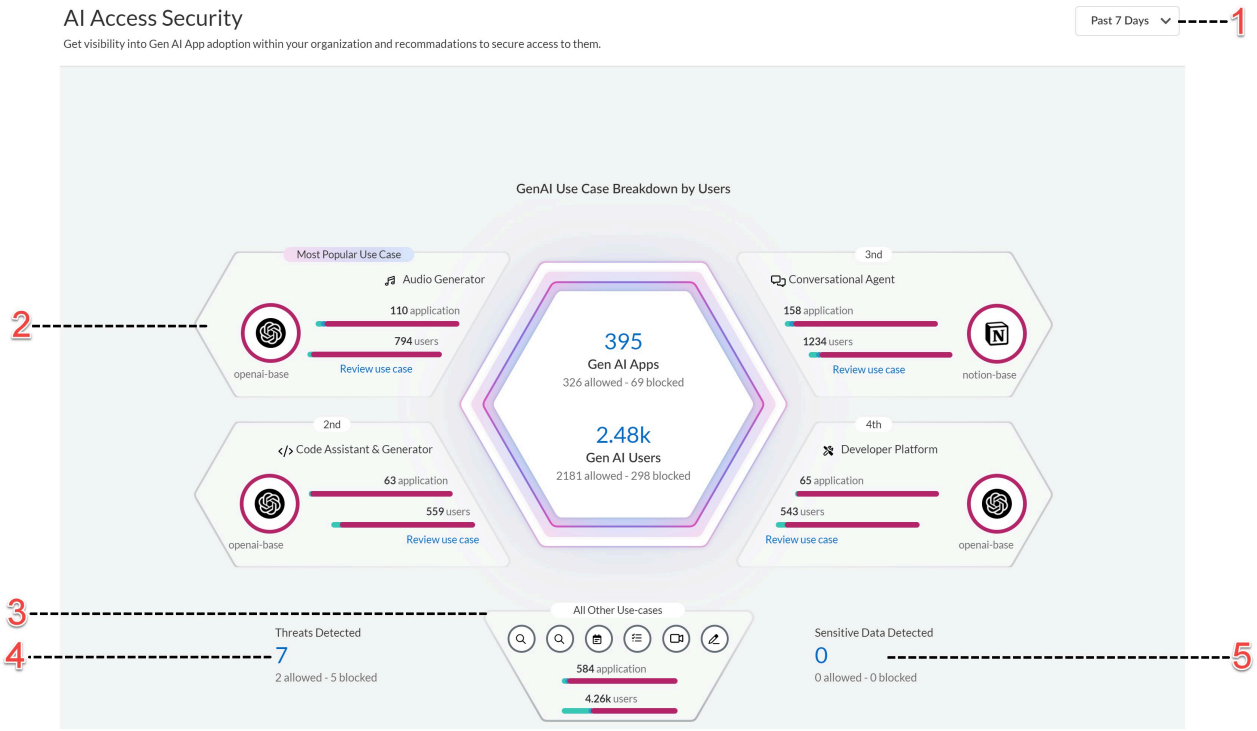
Informations : IA Access

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	L'une des licences suivantes : ❑ AI Access Security ❑ Licence CASB-PA ❑ Licence CASB-X Pour plus d'informations sur les licences qui prennent en charge AI Access Security, cliquez ici.

Les applications d'intelligence artificielle générative (GenAI) sont des applications d'intelligence artificielle capables de générer du texte, des images, des vidéos et d'autres formes de données en réponse à des invites de l'utilisateur et d'apprendre en permanence sur la base des entrées de données de l'utilisateur. Ils sont adoptés à une vitesse remarquable et présentent des possibilités infinies pour les entreprises. Cependant, la nature de l'amélioration contentieuse des applications d'intelligence artificielle générative présente un nouveau danger pour les entreprises et les administrateurs de sécurité : comment pouvez-vous vous assurer que vos employés n'exposent pas de données sensibles ou propriétaires aux applis d'intelligence artificielle générative ?

Palo Alto Networks présente AI Access Security, dont le but est de favoriser l'adoption sécurisée des applications d'intelligence artificielle générative dans votre organisation.

Utilisez le tableau de bord AI Access Security Insights pour filtrer l'utilisation d'applications d'intelligence artificielle générative sur votre réseau. Le tableau de bord AI Access Security Insights fournit des détails approfondis pour vous aider à comprendre quelles applis d'intelligence artificielle générative sont utilisées et leurs utilisateurs.



Pour en savoir plus sur la façon de sécuriser vos données sensibles à partir des applications GenAI, cliquez ici.

Informations : AI Runtime Security

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ Activez votre licence AI Runtime Security ❑ Prérequis pour la configuration d'AI Runtime Security ❑ Intégrer et activer un compte cloud dans SCM

Palo Alto Networks AI Runtime Security est une solution de sécurité centralisée spécialement conçue pour protéger l'architecture du réseau cloud de votre entreprise contre les attaques réseau classiques et spécifiques à l'IA en tirant parti d'une sécurité en temps réel alimentée par l'IA. Il permet de sécuriser vos modèles d'IA de nouvelle génération, vos applications d'IA et vos ensembles de données d'IA contre les menaces réseau telles que les injections de commandes, les fuites de données sensibles, les sorties non sécurisées (par exemple, les logiciels malveillants et les URL) et les attaques DoS de modèle.

Utilisez le tableau de bord AI Runtime Security Insights pour comprendre la surface d'attaque de votre réseau cloud et défendre vos actifs cloud contre les menaces malveillantes.

Pour en savoir plus sur la façon de sécuriser votre flux de trafic réseau IA et non IA contre les attaques potentielles, cliquez ici.

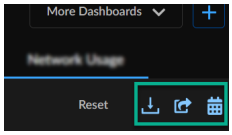
Tableaux de bord : Strata Cloud Manager

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels • Prisma SD-WAN	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro ☐ Prisma SD-WAN Les autres licences et prérequis nécessaires pour accéder à certains tableaux de bord sont : ☐ Services de sécurité fournis par le cloud (CDSS) ☐ Observabilité ADEM ☐ Un rôle qui a l'autorisation d'afficher le tableau de bord → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Strata Cloud Manager fournit un ensemble de tableaux de bord interactifs qui vous présente une vue complète des applications, des périphériques ION, des menaces, des utilisateurs et des abonnements de sécurité à l'œuvre dans votre réseau. Les tableaux de bord fournissent une visibilité sur la santé, la posture de sécurité et l'activité de votre déploiement qui vous aide à prévenir ou à combler les lacunes en matière de performance et de sécurité dans votre réseau. La prise en charge du tableau de bord s'étend aux produits et abonnements Palo Alto Networks pris en charge pour la gestion du cloud, ainsi qu'à d'autres sources, notamment Traps, Cortex XDR, Prisma SaaS et Proofpoint. Les données que vous voyez dépendent souvent de votre abonnement. Vous pouvez passer en revue chaque rubrique du tableau de bord pour voir quelles sont les exigences de licence pour ce tableau de bord, si les autorisations de rôle peuvent avoir un impact sur les données visibles et pour en savoir plus sur les différents types de données que chaque abonnement débloque.

Vous pouvez accéder aux tableaux de bord à partir du menu **Dashboards (Tableaux de bord)** dans le volet de navigation de gauche. Le tableau de bord Santé SASE est épinglé par défaut

sur la page de destination. Cliquez sur **More Dashboards (Plus de tableaux de bord)** et cochez ou décochez la case située à côté du nom d'un tableau de bord pour épingler ou désépingler le tableau de bord sur la page de destination des tableaux de bord. Vous pouvez également créer votre propre tableau de bord à l'aide de l'option **Construire mon tableau de bord**. Certains tableaux de bord ont également la possibilité de télécharger et de partager des rapports Rapports : Strata Cloud Manager que vous pouvez partager hors ligne et planifier des mises à jour régulières. Pour voir si les rapports sont pris en charge dans un tableau de bord, vérifiez si les icônes suivantes sont disponibles :



Intégrer avec le Moteur d’identité sur le cloud

Nous vous recommandons de configurer le Moteur d’identité sur le cloud (Directory Sync) pour tirer le meilleur parti des tableaux de bord. Cloud Identity Engine (Moteur d’identité cloud) est une application gratuite de Palo Alto Networks qui donne aux autres applications un accès en lecture seule à vos informations Active Directory, et vous permet de :

- **Obtenir des données de l’activité de l’utilisateur** : Cloud Identity Engine vous permet de spécifier l’utilisateur pour lequel vous souhaitez exécuter un rapport.
- **Partagez facilement et en toute sécurité des rapports avec d’autres membres de votre organisation** avec Cloud Identity Engine configuré, vous pouvez facilement ajouter des destinataires à un rapport planifié. Les destinataires de votre rapport sont contrôlés par Cloud Identity Engine, et s’il ne trouve pas de correspondance, il effectue une étape de validation supplémentaire en vérifiant le domaine d’adresse e-mail par rapport aux domaines d’adresse e-mail associés à votre compte de support. Ces contrôles permettent de s’assurer que les rapports ne sont pas envoyés en dehors de votre organisation.

Les applis intégrées doivent être déployées dans la même région. À tout moment, vous pouvez vous rendre au concentrateur pour intégrer Cloud Identity Engine à Prisma Access ou Directory Sync. # Intégrer les applis Palo Alto Networks

Prise en charge des tableaux de bord

Certains supports du tableau de bord dans le produit sont en attente de la migration de Lancement de Strata Cloud Manager vers Strata Cloud Manager.

Fonctionnalité	Pris en charge sur				Licences et autres exigences	Portée des données agrégées
	Prisma Access (gestion du cloud)	Prisma Acce (Géré par Panorama)*	AIOps for N	Plateforme multilocatair Prisma SASE		
	• Docs pour Prisma Access (Managed by Strata Cloud Manager) et Prisma Access (Managed by Panorama)		• Docs pour AIOps for NGFW	• Docs pour la plateforme multilocataire Prisma SASE		
Santé SASE	Oui	Oui	Oui		• Observabilité ADEM • ADEM alimenté par l'IA	
Meilleures pratiques	Oui	Non	Versions PAN-OS : 10.0 ou version ultérieure	Oui	[Uniquement pour AIOps for NGFW] Activer le partage de télémétrie dans les périphériques	• Prisma Access (Manage par locataire • AIOps for NGFW : par NGFW/ Panorama associé à l'instance AIOps for NGFW
Résumé de la conformité	Non	Non	Oui	Non	[Uniquement pour les AIOps pour NGFW] Activer le partage de télémétrie dans les périphériques	AIOps pour NGFW : par NGFW/ Panorama associé à AIOps pour instance NGFW

Fonctionnalité	Pris en charge sur				Licences et autres exigences	Portée des données agrégées
	Prisma Access (gestion du cloud)	Prisma Acce (Géré par Panorama)*	AIOps for N	Plateforme multilocatair Prisma SASE		
BPA à la demande	Non	Non	Oui	Non	TSF	AIOps pour NGFW : par NGFW/ Panorama associé à AIOps pour instance NGFW
Récapitulatif	Oui	Oui	Oui	Oui	• Licence Strata Logging Service • Licence de prévention des menaces • Licence de filtrage des URL • Licence WildFire • Licence Enterprise DLP	Locataire par Strata Logging Service
WildFire	Oui	Non	Oui	Oui**	Licence WildFire	Par groupe de services aux locataires(TSG)
Sécurité DNS	Oui	Oui	Oui	Oui**	Licence Security DNS.	Par groupe de services aux locataires(TSG)
Visionneuse de journaux	Oui	Oui	Oui	Oui	Licence Strata	Locataire par Strata

Fonctionnalité	Pris en charge sur				Licences et autres exigences	Portée des données agrégées
	Prisma Access (gestion du cloud)	Prisma Acce (Géré par Panorama)*	AIOps for N	Plateforme multilocatair Prisma SASE		
					Logging Service	Logging Service
Recherche de l'IOC	Oui	Non	Oui	Oui**	Conditions requises pour afficher le graphique de tendance dans la recherche : • Licence DNS • Licence WildFire • Strata Logging Service Licence • Filtrage des URL	
Télécharger/ Partager/ Planifier	Oui	Oui	Oui	Oui		Reportez-vous à la colonne fonctionnalité respective dans ce tableau
Sécurité SaaS :	Oui	Non	Non	Non	• Licence de sécurité Saas Security • Strata Logging Service	Locataire par Prisma Access

Fonctionnalité	Pris en charge sur				Licences et autres exigences	Portée des données agrégées
	Prisma Access (gestion du cloud)	Prisma Acce (Géré par Panorama)*	AIOps for N	Plateforme multilocatair Prisma SASE		
Incidents DLP	Oui	Non	Non	Non	Licence Enterprise DLP	Locataire par Prisma Access
Santé du périphérique	Non	Non	Oui	Non	• [Uniquement pour AIOps for NGFW] Activer le partage de télémétrie dans les périphériques	AIOps for NGFW : par NGFW/ Panorama associé à une instance AIOps for NGFW
Informations sur la posture de sécurité	Non	Non	Oui	Non		AIOps for NGFW : par NGFW/ Panorama associé à une instance AIOps for NGFW
Prévention avancée des menaces	Non	Non	Oui	Non	• Licence de Prévention des menaces ou Prévention avancée des menaces • Strata Logging Service	Locataire par Strata Logging Service
IoT Security	Oui	Oui	Oui	Non	Licence IoT Security	Locataire par IoT Security
Prisma SD-WAN	Non	Non	Non	Oui	Licence Prisma SD-WAN	Locataire par Prisma SD-WAN

Fonctionnalité	Pris en charge sur				Licences et autres exigences	Portée des données agrégées
	Prisma Access (gestion du cloud)	Prisma Acce (Géré par Panorama)*	AIOps for N	Plateforme multilocatair Prisma SASE		
CVE PAN-OS	Non	Oui	Oui		[Uniquement pour les AIOps pour NGFW] Activer le partage de télémétrie dans les périphériques	• AIOps pour NGFW : par NGFW/ Panorama associé à AIOps pour instance NGFW • PSIRT Base de données des CVE utilisant l'accès API
Adoption de CDSS	Oui	Oui	Oui		[Uniquement pour les AIOps pour NGFW] Activer le partage de télémétrie dans les périphériques	AIOps pour NGFW : par NGFW/ Panorama associé à AIOps pour instance NGFW
Adoptions de fonctionnalité	Non	Oui	Oui		[Uniquement pour les AIOps pour NGFW] Activer le partage de télémétrie dans les périphériques	AIOps pour NGFW : par NGFW/ Panorama associé à AIOps pour instance NGFW

Prisma Access (Géré par Panorama)* -

- Pour les utilisateurs de Prisma Access (gérés par Panorama) dont les Strata Logging Service sont hébergés dans la région hors Amérique. Vous devez donner votre consentement pour

permettre à Prisma Access de lire et de traiter les données de Strata Logging Service dans la région hors Amérique. Relisez et acceptez l'avis de confidentialité sur la page d'accueil du tableau de bord pour donner votre consentement et consulter d'autres tableaux de bord et journaux. Seuls les administrateurs d'applis, d'instances et de comptes peuvent voir et accepter la déclaration de confidentialité.

- Les tableaux de bord ne sont pas pris en charge dans les environnements multilocataires Prisma Access (gérés par Panorama).

Oui* : oui signifie que toutes les versions de Prisma Access et PAN-OS sont prises en charge.

Oui** : dans la plate-forme multilocataire, les locataires sont identifiés comme groupes de services aux locataires (GST) et reçoivent un identifiant GST. Un seul ou plusieurs locataires peuvent être associés par portail de soutien à la clientèle (CSP). Les données présentées dans le tableau de bord dépendent des scénarios suivants:

- Votre application à partir de laquelle vous accédez au tableau de bord doit être prise en charge par TSG et accessible via la plateforme SASE ou la vue locataire sur le concentrateur https://docs.paloaltonetworks.com/hub/hub-getting-started.
- Vous avez associé des périphériques à votre locataire en utilisant les Services communs dans le concentrateur.
- Vérifiez si vos locataires ont un mappage un-à-un ou plusieurs-à-un avec CSP.
  - Si vos locataires disposent d'un mappage un-à-un avec CSP, vous pouvez afficher les données du tableau de bord sur toutes les sources (par exemple, dans le tableau de bord WildFire, les données sur les échantillons des pare-feux Palo Alto Networks, Prisma Access, Traps, Cortex XDR, Prisma SaaS, Proofpoint et les téléchargements manuels sont affichés).
  - Si plusieurs locataires sont associés par CSP, le tableau de bord affiche les données provenant uniquement de Prisma Access, des pare-feu Palo Alto Networks et des appliances Panorama associées à des locataires spécifiques et non d'autres sources.

AIOps for NGFW* - Les tableaux de bord disponibles dans AIOps for NGFW dépendent du niveau de licence Free ou Premium.

Tableau de bord : Créer un tableau de bord personnalisé

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels • Prisma SD-WAN	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN Les autres licences et prérequis nécessaires à la visibilité sont : ❑ https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/dashboards pour déverrouiller certains widgets dans le tableau de bord ❑ Un rôle qui a l'autorisation d'afficher le tableau de bord → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

En dehors des tableaux de bord par défaut, vous pouvez créer des tableaux de bord personnalisés pour obtenir une visibilité sur les domaines qui vous intéressent dans votre réseau à l'aide de widgets. Les widgets sont des éléments utilisés pour créer un tableau de bord. Les widgets sont classés et stockés dans la bibliothèque à widgets. Cliquez sur **Dashboards (Tableaux de bord)** > **+** et sélectionnez une catégorie dans la liste déroulante pour afficher les widgets. Les widgets disponibles dans la bibliothèque de widgets varient en fonction de vos abonnements aux services de sécurité. Par exemple, si vous disposez des licencesAIOps for NGFW Premium et Advanced WildFire, vous pouvez afficher et utiliser tous les widgets sous la catégorie WildFire pour créer un tableau de bord.

Il s'agit des catégories de widgets disponibles pour créer un tableau de bord. Vous pouvez vous reporter aux liens ci-dessous pour connaître les licences requises pour accéder aux widgets de ces catégories et en savoir plus.

- Tableau de bord : Prévention avancée des menaces
- Tableau de bord : Sécurité DNS
- Tableau de bord : WildFire

Créez un tableau de bord

Vous pouvez ajouter jusqu'à 10 widgets dans un tableau de bord personnalisé et créer 10 tableaux de bord personnalisés par utilisateur. Le tableau de bord et les widgets peuvent être personnalisés à tout moment. Vous pouvez modifier la tuile du widget, sa description, afficher ou masquer les filtres, les paramètres du tableau de bord tels que la mise en page, le nom du tableau de bord et les descriptions, et également inclure des filtres dans le tableau de bord.

STEP 1 | Cliquez sur **Dashboards (Tableaux de bord)** > **+**.

STEP 2 | Entrez le nom du tableau de bord.

STEP 3 | Sélectionnez une catégorie de widgets dans la section déroulante (liste) Bibliothèque de widgets.

STEP 4 | Ajoutez le widget au tableau de bord : passez la souris sur le widget pour en savoir plus sur le widget. Faites glisser et déposer le widget sur le canevas du tableau de bord.

Vous pouvez ajouter d'autres widgets de types identiques ou différents d'une autre catégorie de widgets au canevas du tableau de bord.

STEP 5 | Passez de l'affichage des **données échantillons** à **celui des données réelles** pour savoir à quoi ressemble votre widget de tableau de bord. Des exemples de données vous aident à visualiser l'apparence de votre tableau de bord et le type d'informations que vous pouvez voir. Utilisez les **Données réelles** pour afficher les données réelles de votre déploiement.

STEP 6 | (Facultatif) Vous pouvez personnaliser le tableau de bord dans la vue de l'éditeur :

- Réorganisez les widgets dans le tableau de bord : sélectionnez-le et faites-le glisser et déposez-le si nécessaire dans le canevas.
- Modifier un widget : cliquez sur l'icône de modification située dans le coin supérieur droit de chaque widget pour en modifier les paramètres. Les paramètres disponibles varient en fonction du widget et ne sont pas les mêmes pour tous les widgets. Par exemple, le nom du widget, sa description et les options de filtrage et de tri des données dans le widget, telles que le verdict, l'action, peuvent être modifiés.

  Vous pouvez modifier les paramètres du widget dans la vue de l'éditeur ou après avoir enregistré le tableau de bord.

STEP 7 | Enregistrez le tableau de bord et cliquez sur **Go to see dashboard (Aller à voir le tableau de bord)** en haut de la page pour ouvrir le tableau de bord.

STEP 8 | (Facultatif) Après avoir enregistré le tableau de bord, vous pouvez :

- Modifiez la plage horaire pour laquelle vous souhaitez afficher les données du tableau de bord.

  Vous ne pouvez modifier l'heure qu'après avoir enregistré le tableau de bord. Dans la vue de l'éditeur, la plage horaire est définie par défaut sur 24 heures.

- Utilisez l'icône Modifier ou Supprimer pour modifier ou supprimer le tableau de bord personnalisé.

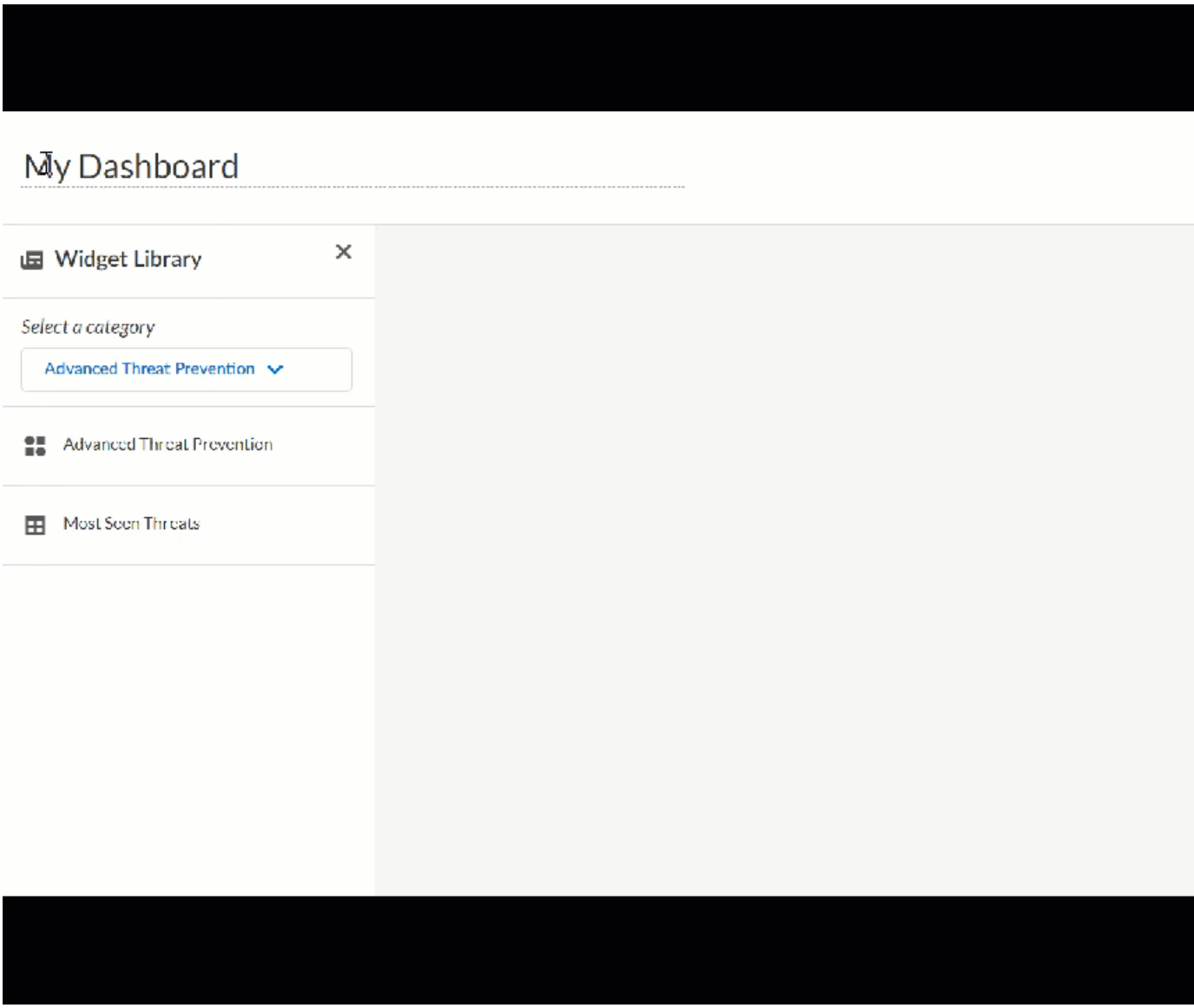


Tableau de bord : Santé du périphérique

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium ou Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Dashboards (Tableaux de bord)** > **Device Health (Santé du périphérique)** pour commencer.

Que vous indique ce tableau de bord ?

Le tableau de bord affiche les données agrégées de tous les pare-feux intégrés à votre locataire et envoie également des données de télémétrie.

Le tableau de bord de l'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.

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

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 ; et
- répertorier les périphériques qui nécessitent une attention particulière dans votre déploiement et prioriser les problèmes en vue de les résoudre.

La fonctionnalité de rapport (télécharger, partager et planifier le rapport) n'est pas prise en charge pour ce tableau de bord.

Tableau de bord de la santé du périphérique : Scores de santé du périphérique

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium ou Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Dashboards (Tableaux de bord)** > **Device Health (Santé du périphérique)** pour afficher le tableau de bord.

Le widget du tableau de bord affiche :

- 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 gravité du score de santé des périphériques intégrés à votre déploiement. Cliquez sur le lien du numéro pour connaître les détails du périphérique, les statistiques sur la santé du périphérique et les alertes relatives au périphérique qui nécessite une attention particulière.

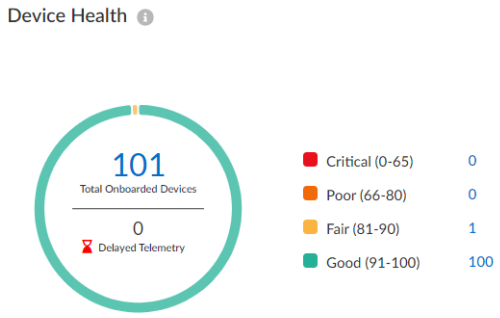
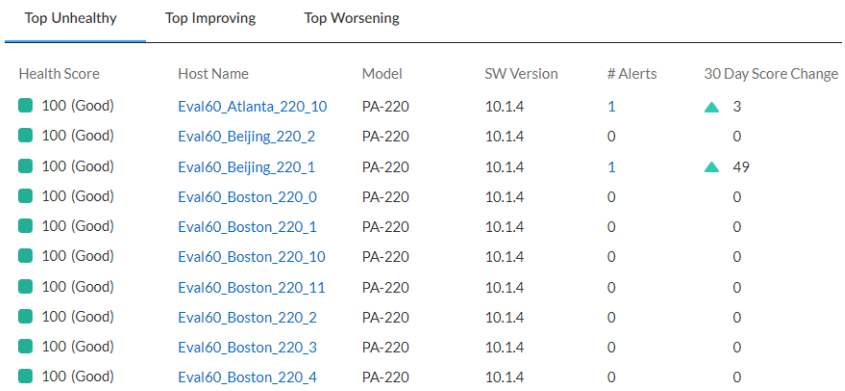


Tableau de bord de la santé du périphérique : Statistiques du périphérique

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium ou Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Dashboards (Tableaux de bord)** > **Device Health (Santé du périphérique)** pour afficher le tableau de bord.



Principaux éléments en mauvaise santé

Il s'agit des périphériques présentant le plus de problèmes de santé et de performances dans votre déploiement. Vous pouvez également effectuer un zoom avant pour afficher les détails du périphérique et les alertes sur ce dernier. Corrigez les alertes critiques pour améliorer le score de santé et la santé du déploiement.

Principale amélioration

Consultez les 10 meilleurs périphériques au cours de la période de 30 jours avec des scores de santé améliorés par rapport aux scores de santé actuels des périphériques.

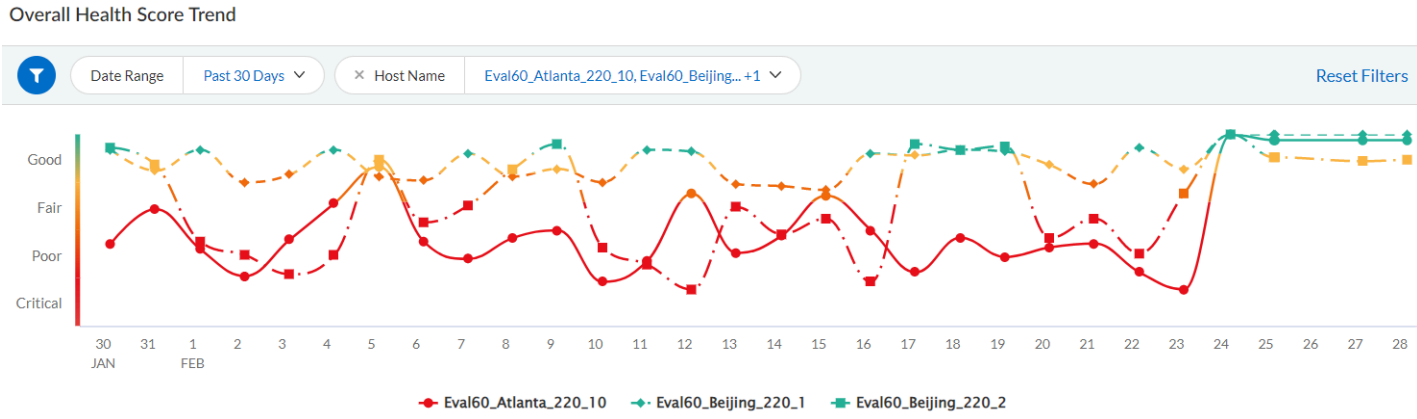
Principale aggravation

Vérifiez la santé du périphérique sur une période de 30 jours. Voici les 10 principaux périphériques dont les scores de santé ont diminué par rapport aux scores d'états actuels des périphériques.

Tableau de bord de la santé du périphérique : Tendance du score

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium ou Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Dashboards (Tableaux de bord)** > **Device Health (Santé du périphérique)** pour afficher le tableau de bord.



Ce tableau indique l'évolution de l'état de santé de votre déploiement au cours de la période sélectionnée. Survolez le point de déclenchement pour connaître les périphériques qui contribuent à la gravité du score de santé. Vous pouvez afficher les tendances d'un ou de plusieurs périphériques filtrés par le nom d'hôte, le modèle ou la version du logiciel.

Tableau de bord : Récapitulatif

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels • Prisma SD-WAN	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro ☐ Prisma SD-WAN Les autres licences et prérequis nécessaires à la visibilité sont : ☐ https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/dashboards pour déverrouiller certains widgets dans le tableau de bord ☐ Un rôle qui a l'autorisation d'afficher le tableau de bord → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Strata Cloud Manager** > **Dashboards (Tableaux de bord)** > **More Dashboards (Plus de tableaux de bord)** > **Executive Summary (Récapitulatif)** pour commencer.

Que vous indique ce tableau de bord ?

Le tableau de bord affiche des données agrégées par locataire Strata Logging Service.

Le tableau de bord du Récapitulatif vous montre comment vos abonnements de sécurité Palo Alto Networks vous protègent. Ce rapport détaille les activités malveillantes détectées par ces abonnements sur votre réseau : **WildFire**, **Advanced Threat Prevention (Prévention des menaces avancée)**, **Advanced URL Filtering (Filtrage des URL avancé)**et **Enterprise DLP (entreprise DLP**. Le tableau de bord présente des données pour chacun de ces services, avec des liens vers les tableaux de bord des services de sécurité, qui permettent d'approfondir les recherches.

Ce tableau de bord prend en charge les rapports. Ces icônes,  en haut à droite d'un tableau de bord, indiquent que les rapports sont pris en charge pour ce tableau de bord. Vous pouvez

partager, télécharger et planifier des rapports qui couvrent les données affichées par ce tableau de bord.

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

- Examinez toutes les activités malveillantes détectées par les abonnements actifs de Palo Alto Networks. Vérifiez si vous devez affiner les paramètres d'abonnement ou les paramètres des règles de sécurité pour combler les failles de sécurité.
- Vous présente des données sectorielles pour vous donner une perspective sur le paysage des menaces auxquelles vous êtes confronté et sur la façon dont vous vous situez par rapport à vos pairs.

Le tableau de bord fournit les données suivantes.

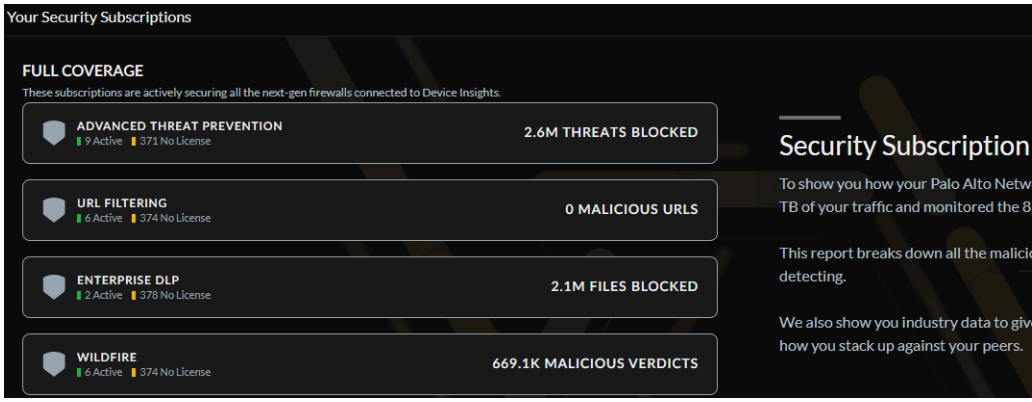
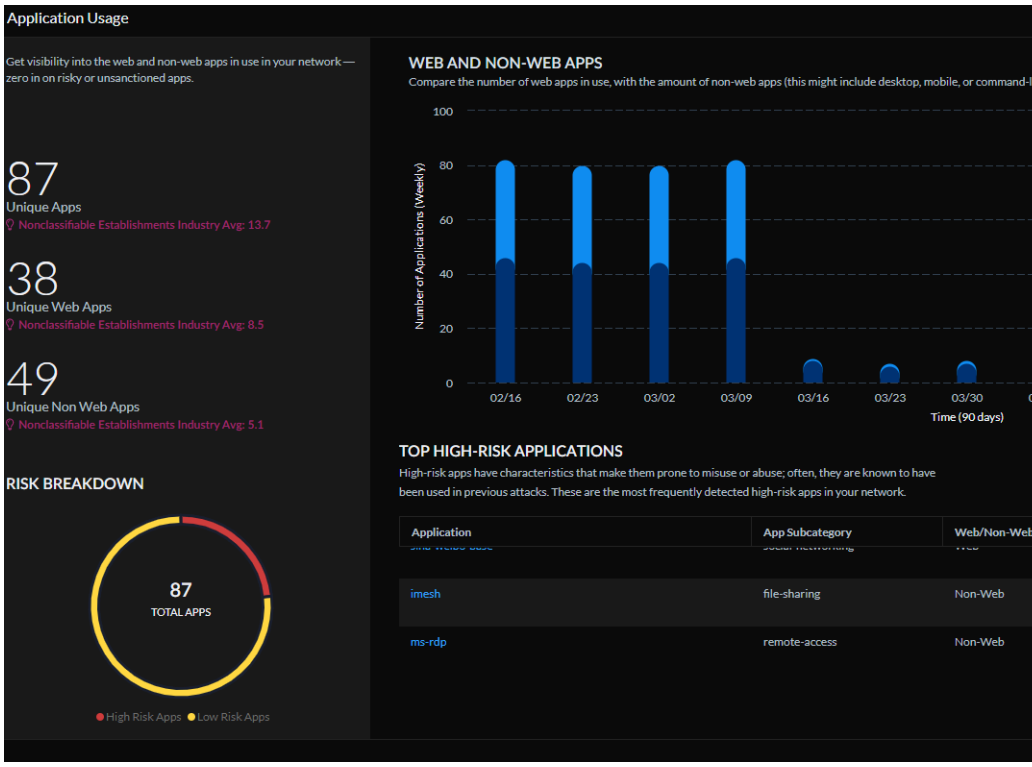
Tableau de bord du résumé exécutif : Vos abonnements de sécurité	Ce rapport vous donne des chiffres sur les activités malveillantes que vos abonnements détectent et préviennent : • applications à haut risque • menaces graves (exploits, logiciel malveillant et C2) • activité Web malveillante • Menaces basées sur des fichiers (y compris des menaces inédites) • perte de données 

Tableau de bord du résumé exécutif : Utilisation de l'application	Examinez les journaux de trafic pour les applications à haut risque et voyez comment vous pouvez renforcer la posture de sécurité. 
Tableau de bord récapitulatif : Prévention avancée des menaces *Nécessite une licence de prévention des menaces avancée.*	Examinez les règles de politique de sécurité qui autorisent la plupart des menaces. Examinez ces règles pour voir où vous pouvez activer une application plus stricte des menaces. En savoir plus.
Tableau de bord récapitulatif : Filtrage d'URL *Nécessite une licence de filtrage des URL avancé.*	Passez en revue l'activité des sites Web malveillants sur votre réseau, en particulier le nombre de sites Web

malveillants auxquels vos utilisateurs tentent d'accéder.

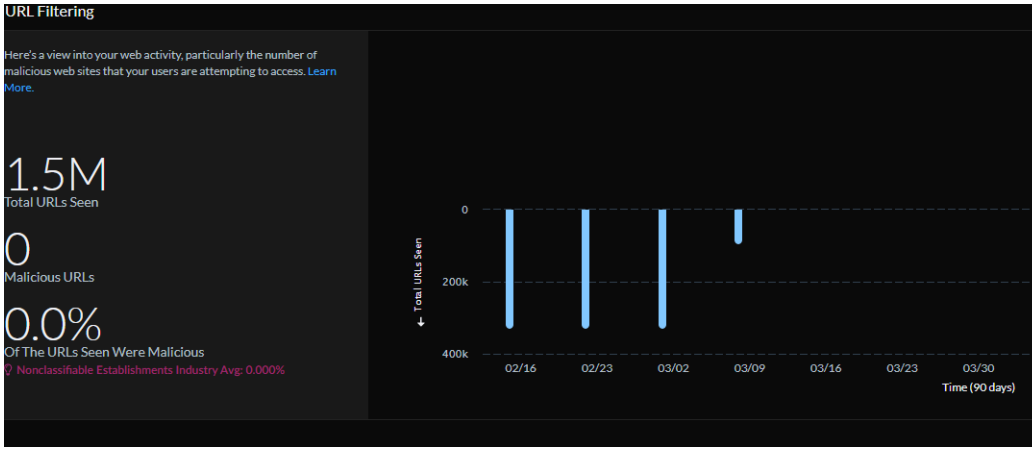


Tableau de bord récapitulatif : WildFire

Nécessite une licence Advanced WildFire.

Les données de ce tableau de bord vous donnent un aperçu du paysage des menaces dans votre secteur et de la façon dont votre couverture de sécurité se compare à celle d'organisations similaires. Ces données sectorielles sont également affichées pour les abonnements que vous n'utilisez pas ; cela vous aide à voir s'il existe des endroits où vous pouvez augmenter la couverture pour combler les failles de sécurité.

Voici un gros plan du type de données fournit par ce tableau de bord : ici, vous pouvez voir le travail effectué par WildFire pour protéger votre réseau et votre secteur. En savoir plus. #

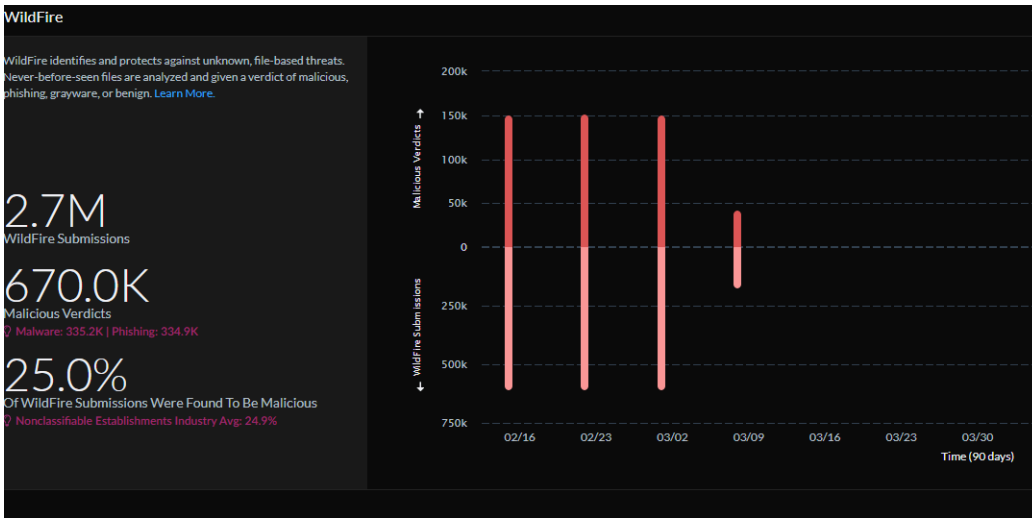


Tableau de bord récapitulatif : Enterprise DLP

Nécessite une licence Entreprise DLP.

Découvrez comment votre service Palo Alto Networks Entreprise DLP protège vos données en appliquant des normes de sécurité des données. Ce tableau de bord donne un aperçu des applications vers lesquelles la plupart des téléchargements sont empêchés par la DLP et du nombre total de fichiers bloqués par la DLP dans votre réseau. Ces données peuvent également vous permettre de vous comparer à vos homologues du secteur et d'évaluer les normes de votre posture de sécurité.

Passez en revue les applications et les noms d'utilisateur sources pour mieux comprendre l'origine des incidents DLP et les gérer.

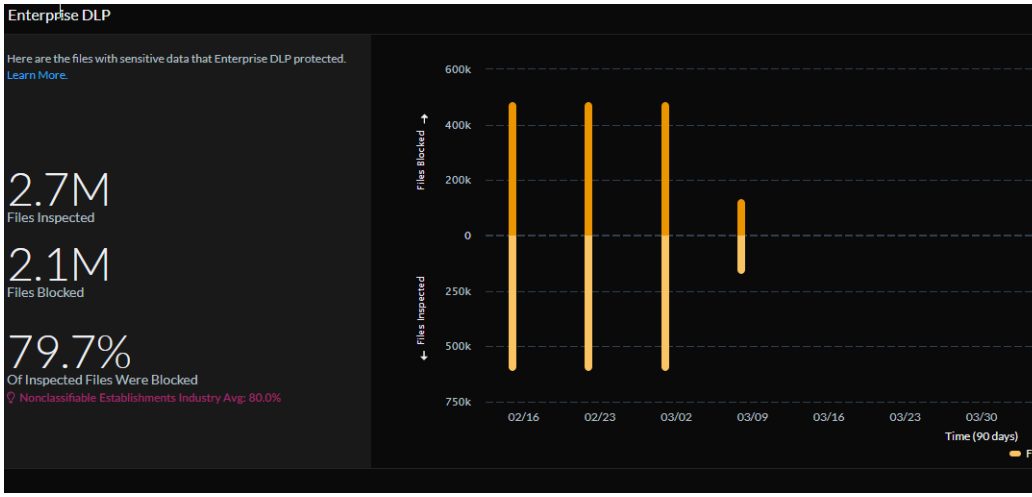
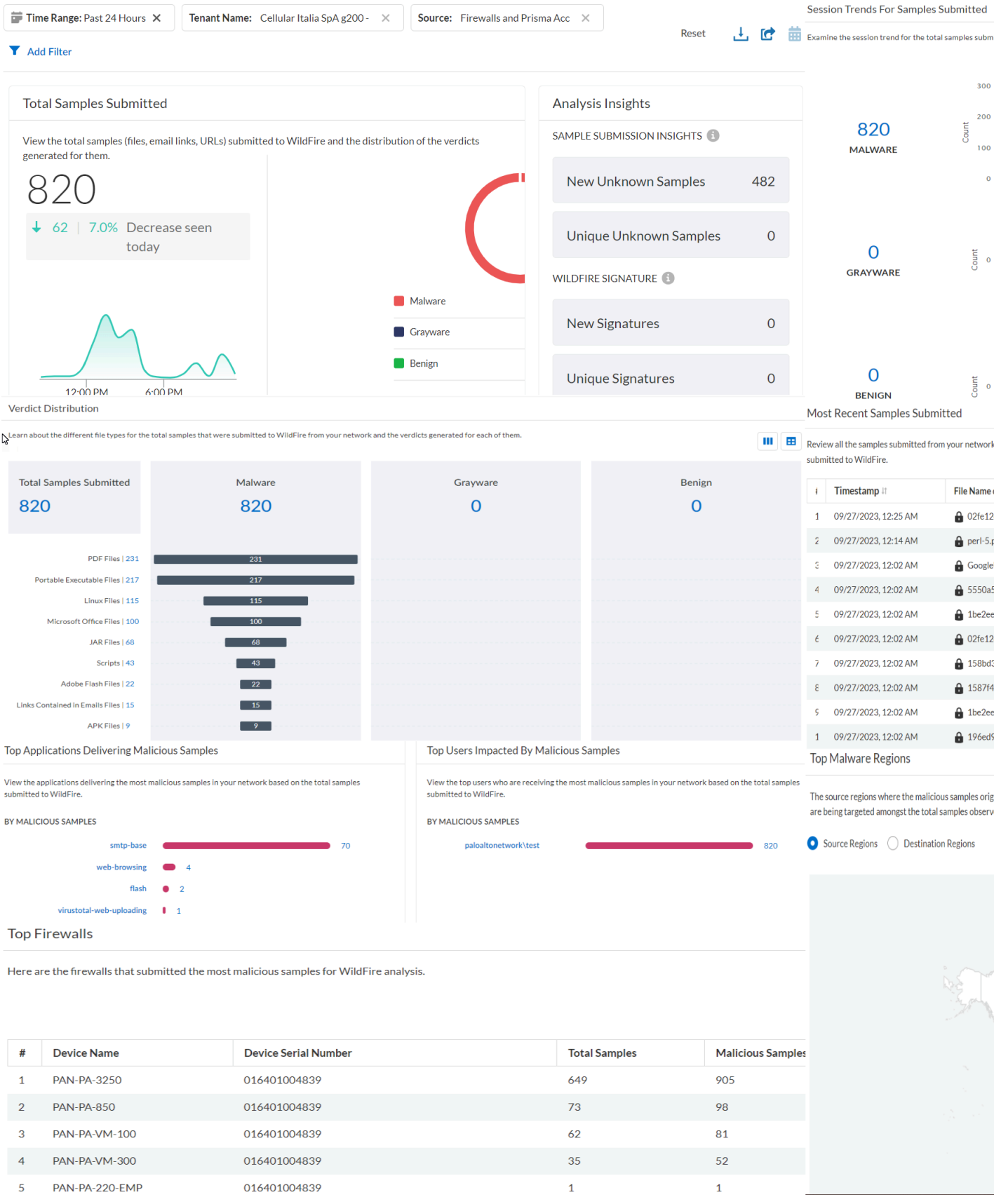


Tableau de bord : WildFire

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Les autres licences et prérequis nécessaires à la visibilité sont : ☐ Un rôle qui a la permission d'afficher le tableau de bord ☐ Advanced WildFire → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Strata Cloud Manager** > **Dashboards (Tableaux de bord)** > **More Dashboards (Plus de tableaux de bord)** > **WildFire** pour commencer.



#	Device Name	Device Serial Number	Total Samples	Malicious Samples
1	PAN-PA-3250	016401004839	649	905
2	PAN-PA-850	016401004839	73	98
3	PAN-PA-VM-100	016401004839	62	81
4	PAN-PA-VM-300	016401004839	35	52
5	PAN-PA-220-EMP	016401004839	1	1

Que vous indique ce tableau de bord ?

Le tableau de bord affiche des données agrégées par groupe de services locataire (TSG). Le tableau de bord montre les données sur Prisma Access, les pare-feu Palo Alto Networks et les appliances Panorama associées à votre locataire, à condition que vos locataires aient un mappage un-à-un avec votre compte portail de support client. Le tableau de bord n'affiche pas les données provenant d'autres sources si plusieurs locataires sont associés par portail de support client.

Découvrez comment WildFire vous protège contre les nouveaux logiciels malveillants qui se cachent dans les fichiers et les exécutables. Ce tableau de bord prend en charge les rapports. Ces icônes,  en haut à droite d'un tableau de bord, indiquent que les rapports sont pris en charge pour ce tableau de bord. Vous pouvez partager, télécharger et planifier des rapports qui couvrent les données affichées par ce tableau de bord.

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

Utilisez ce tableau de bord pour

- (requiert une licence AIOps for NGFW Premium) surveiller les soumissions WildFire et obtenir les détails des échantillons WildFire soumis au cloud WildFire pour analyse.
- afficher les détails des utilisateurs ciblés, les applications qui ont fourni les fichiers, les pare-feu qui ont soumis les échantillons pour analyse et toutes les URL impliquées dans l'activité de commande et de contrôle des fichiers.
- (Nécessite une licence AIOps for NGFW Premium)consultez les journaux WildFire et le rapport d'analyse et affinez les paramètres WildFire pour votre déploiement en fonction du rapport.

Tableau de bord WildFire : Filtres

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Les autres licences et prérequis nécessaires à la visibilité sont : ☐ Un rôle qui a la permission d'afficher le tableau de bord ☐ Advanced WildFire → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	dépendent de la ou des licences que vous utilisez.

Le tableau de bord WildFire fournit ces options de filtrage pour affiner l'accès à des données spécifiques du tableau de bord.

- **Plage horaire** – Sélectionnez dans l'icône **Dernières 24 heures**, **7 derniers jours**, **30 derniers jours**ou **Plage horaire personnalisée** pour afficher les données d'une période spécifique.
- **Nom du locataire** – le locataire dont les données du tableau s'affichent.
- **Source** – la portée des données du tableau de bord provient des pare-feu de Prisma Access et de Palo Alto Networks.
- **Échantillons** – Sélectionnez dans l'icône **Public** ou **Privé** pour afficher les données soumises à partir d'un environnement de cloud public ou de cloud privé Wildfire.
- **Verdict** – Afficher les échantillons identifiés comme **Bénin**, **Logiciel malveillant** ou **Logiciel indésirable** dans l'analyse de WildFire.
- **Action** – Sélectionnez l'option **Autoriser** ou **Bloquer** pour afficher les échantillons WildFire autorisés ou bloqués par votre règle de politique.
- **Type de fichier** – Affichez les données en fonction du type de fichier de l'échantillon analysé par WildFire. En savoir plus sur le Types de fichiers pris en charge pour l'analyse de WildFire.
- **Hachage de fichier** – Affichez les données d'un hachage de fichier analysé par WildFire. Voici une liste des versions de hachage générées par WildFire pour chaque fichier analysé :
  - **SHA-1** – Affiche la valeur SHA-1 du fichier.
  - **SHA-256** – Affiche la valeur SHA-256 du fichier.
  - **MD5** – Affiche les informations MD5 du fichier.
- **Nom de l'appli** – Filtrez les données en fonction des échantillons fournis par une application.
- **Région source** – Filtrez pour afficher les échantillons envoyés à partir d'un emplacement spécifique.
- **Région de destination** – Filtrez pour afficher les échantillons reçus à un endroit spécifique.
- **Nom d'utilisateur** – Entrez le nom d'utilisateur pour filtrer les données de l'utilisateur ciblé pour diffuser l'échantillon dans votre réseau.
- **Numéro de série de l'appareil** – Filtrez les données du périphérique qui a soumis l'échantillon à WildFire pour analyse.

Tableau de bord WildFire : Nombre total d'échantillons soumis

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Les autres licences et prérequis nécessaires à la visibilité sont : ❑ Un rôle qui a la permission d'afficher le tableau de bord ❑ Advanced WildFire → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Dashboards (Tableaux de bord)** > **More Dashboards (Plus de tableaux de bord)** > **WildFire** pour afficher le tableau de bord.

Le nombre total d'échantillons soumis à WildFire pour analyse au cours de la période sélectionnée. Le widget indique le nombre d'échantillons soumis à partir de chaque source et le verdict généré pour les échantillons. Le widget montre également le pic des échantillons soumis à WildFire pour analyse. Examinez les pics d'échantillons de logiciels malveillants et prenez des mesures pour atténuer les impacts des menaces sur votre réseau.

Tableau de bord WildFire : Informations sur l'analyse

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Les autres licences et prérequis nécessaires à la visibilité sont : ❑ Un rôle qui a la permission d'afficher le tableau de bord ❑ Advanced WildFire

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	→ Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Dashboards (Tableaux de bord)** > **More Dashboards (Plus de tableaux de bord)** > **WildFire** pour afficher le tableau de bord.

Obtenez des informations sur les échantillons WildFire uniques soumis à partir de votre réseau et les signatures générées. Utilisez les données pour comprendre les nouvelles menaces qui ont été observées uniquement dans votre réseau dans le délai sélectionné et le nombre de fois que votre réseau a été protégé par les signatures générées.

- **Échantillons uniques inconnus** : nombre d'échantillons soumis à WildFire à partir de votre réseau qui ne sont vus que dans votre réseau, auparavant inconnus de WildFire et non disponibles dans d'autres flux publics ou privés.
- **Nouveaux échantillons inconnus** : nombre de nouveaux échantillons soumis à WildFire à partir de votre réseau qui sont auparavant inconnus de WildFire (avec sha256 distinct).
- **Signatures uniques** : nombre de signatures générées à partir d'échantillons uniques à votre environnement.
- **Nouvelles signatures** : nombre de nouvelles signatures créées par WildFire à partir de tous vos échantillons téléchargés.

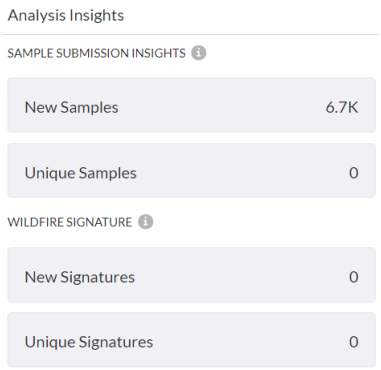


Tableau de bord WildFire : Tendances de la session pour les échantillons soumis

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	❑ Strata Cloud Manager Pro Les autres licences et prérequis nécessaires à la visibilité sont : ❑ Un rôle qui a la permission d'afficher le tableau de bord ❑ Advanced WildFire → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Dashboards (Tableaux de bord)** > **More Dashboards (Plus de tableaux de bord)** > **WildFire** pour afficher le tableau de bord.

Examinez les tendances pour tous les échantillons soumis à WildFire depuis votre réseau et le verdict pour ces échantillons. Vous pouvez effectuer une recherche du CIO sur ces échantillons pour connaître l'historique de l'échantillon dans votre réseau et les résultats de l'analyse globale dudit l'échantillon.

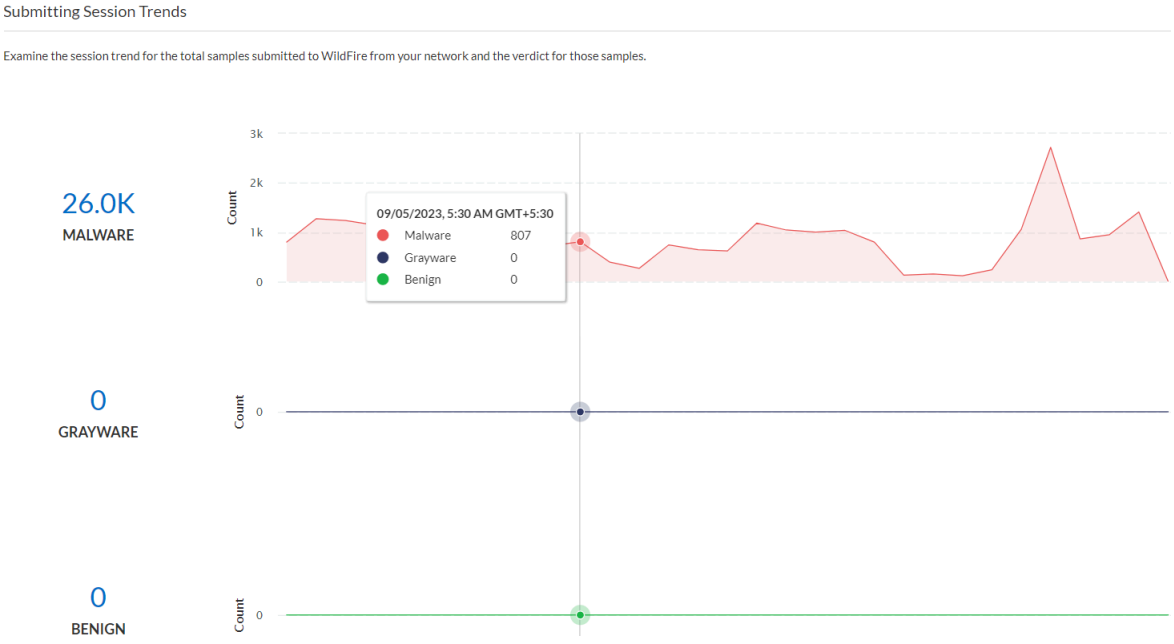


Tableau de bord WildFire : Répartition des verdicts

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Les autres licences et prérequis nécessaires à la visibilité sont : ❑ Un rôle qui a la permission d'afficher le tableau de bord ❑ Advanced WildFire → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Dashboards (Tableaux de bord)** > **More Dashboards (Plus de tableaux de bord)** > **WildFire** pour afficher le tableau de bord.

Obtenez plus d'informations sur les verdicts pour les nouveaux échantillons que WildFire a détectés pour la première fois dans votre réseau. Concentrez-vous sur les types d'échantillons qui dissimulent le plus souvent des logiciels malveillants. Cliquez sur le lien pour en savoir plus sur l'échantillon.

Tableau de bord WildFire : Principales applications fournissant des échantillons malveillants

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Les autres licences et prérequis nécessaires à la visibilité sont : ☐ Un rôle qui a la permission d'afficher le tableau de bord ☐ Advanced WildFire → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Dashboards (Tableaux de bord)** > **More Dashboards (Plus de tableaux de bord)** > **WildFire** pour afficher le tableau de bord.

Passez en revue les détails des applications qui ont fourni les échantillons les plus malveillants sur votre réseau. Cliquez sur le nombre d'échantillons malveillants pour en savoir plus sur les échantillons.

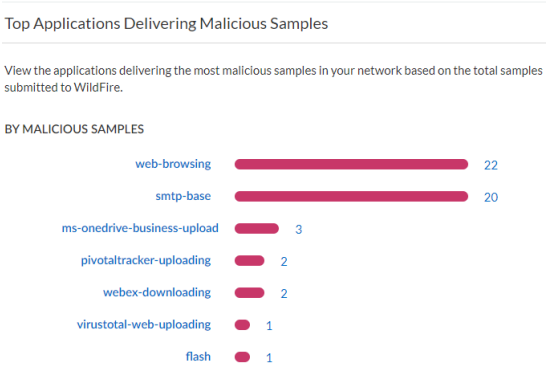


Tableau de bord WildFire : Principaux utilisateurs touchés par les échantillons malveillants

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Les autres licences et prérequis nécessaires à la visibilité sont : ☐ Un rôle qui a la permission d'afficher le tableau de bord ☐ Advanced WildFire → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Dashboards (Tableaux de bord)** > **More Dashboards (Plus de tableaux de bord)** > **WildFire** pour afficher le tableau de bord.

Cela montre les comptes d'utilisateur qui sont le plus fréquemment utilisés pour fournir des échantillons malveillants dans votre réseau. Cliquez sur le nom d'utilisateur pour analyser les modèles d'activité de l'utilisateur.

Tableau de bord WildFire : Principales régions de logiciels malveillants

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Les autres licences et prérequis nécessaires à la visibilité sont : ❑ Un rôle qui a la permission d'afficher le tableau de bord ❑ Advanced WildFire → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Dashboards (Tableaux de bord)** > **More Dashboards (Plus de tableaux de bord)** > **WildFire** pour afficher le tableau de bord.

Examinez les emplacements d'origine des échantillons malveillants ou qui ont été livrés sur votre réseau. Vous pouvez afficher le nombre d'échantillons pour les régions source et de destination sous forme de carte ou de tableau. Utilisez cette méthode pour affiner les régions ciblées par les logiciels malveillants et le type d'attaque de logiciels malveillants.

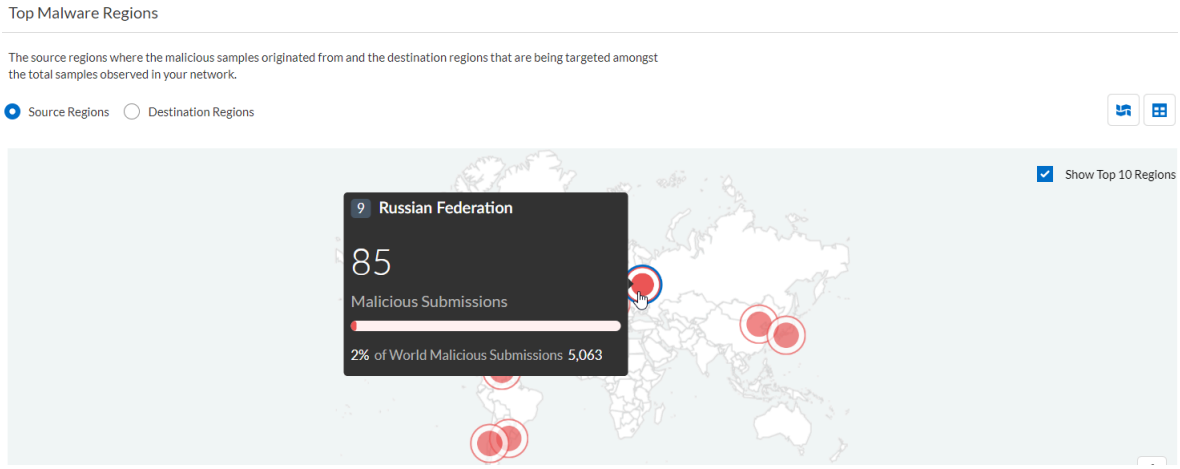


Tableau de bord WildFire : Principaux pare-feu

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Les autres licences et prérequis nécessaires à la visibilité sont : ❑ Un rôle qui a la permission d'afficher le tableau de bord ❑ Advanced WildFire → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Dashboards (Tableaux de bord)** > **More Dashboards (Plus de tableaux de bord)** > **WildFire** pour afficher le tableau de bord.

Affichez les pare-feu qui soumettent les échantillons les plus malveillants à WildFire pour analyse. Examinez ces pare-feu pour localiser les points de terminaison impactés et reconfigurer les règles de politique pour atténuer les menaces et contenir les fichiers malveillants à la source.

Top Firewalls

Here are the firewalls that submitted the most malicious samples for WildFire analysis.

#	Device Name	Device Serial Number	Total Samples	Malicious Samples
1	PAN-PA-3250	016401004839	4866	6947
2	PAN-PA-5220-AC	016401004839	1168	1715
3	PAN-PA-VM-300	016401004839	619	1054
4	PAN-PA-VM-100	016401004839	673	1017
5	PAN-PA-850	016401004839	39	56
6	PAN-PA-VM-500-E60	016401004839	5	6
7	PAN-PA-220-EMP	016401004839	3	5
8	PAN-PA-5260-AC	016401004839	1	1

Tableau de bord : Sécurité DNS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Les autres licences et prérequis nécessaires à la visibilité sont : ☐ Un rôle qui a l'autorisation d'afficher le tableau de bord ☐ Sécurité DNS ou Sécurité DNS avancée → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Strata Cloud Manager** > **Dashboards (Tableaux de bord)** > **More Dashboards (Plus de tableaux de bord)** > **DNS Security (Sécurité DNS)** pour commencer.

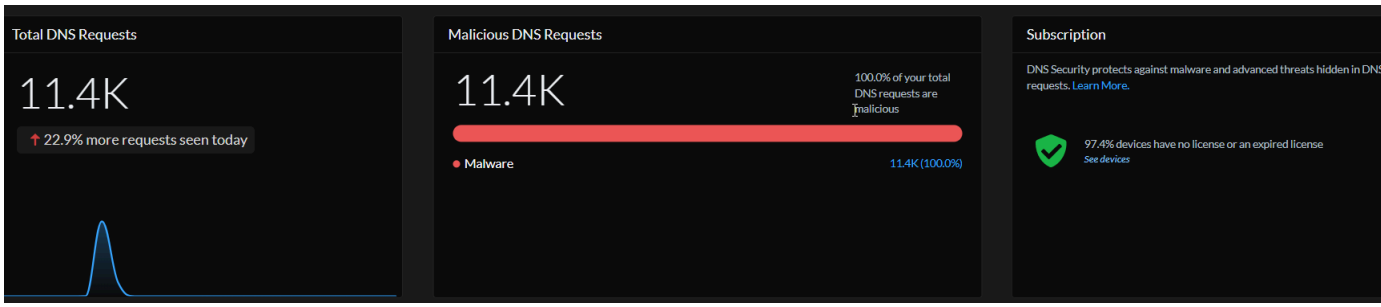
Que vous indique ce tableau de bord ?

Le tableau de bord affiche des données agrégées par groupe de services locataire (TSG).
Le tableau de bord affiche les données sur Prisma Access, les pare-feu Palo Alto Networks et les périphériques Panorama associés à votre locataire.

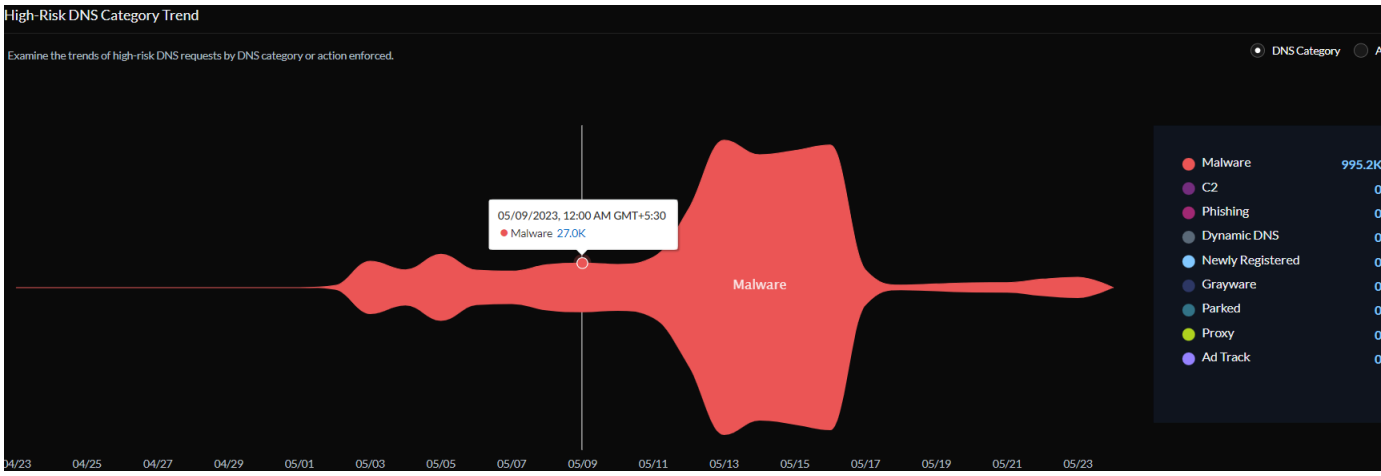
Le nouveau tableau de bord Sécurité DNS vous montre comment votre abonnement de sécurité DNS vous protège contre les menaces avancées et les logiciels malveillants qui utilisent DNS. Vous pouvez également filtrer les informations affichées sur le tableau de bord par plage horaire, action entreprise, domaine, adresse IP de résolution et catégorie DNS. Les filtres source et nom du locataire indiquent la source et le nom du locataire pour lesquels les données sont affichées dans le tableau de bord. Vous pouvez afficher : statistiques et tendances des requêtes DNS

- **Nombre total de requêtes DNS** : affiche le nombre total de requêtes DNS traitées par la sécurité DNS. Le graphique linéaire illustre le nombre de requêtes DNS en fonction de la plage de temps définie par l'utilisateur. La spécification d'une plage de temps personnalisée met à jour le graphique linéaire en conséquence.

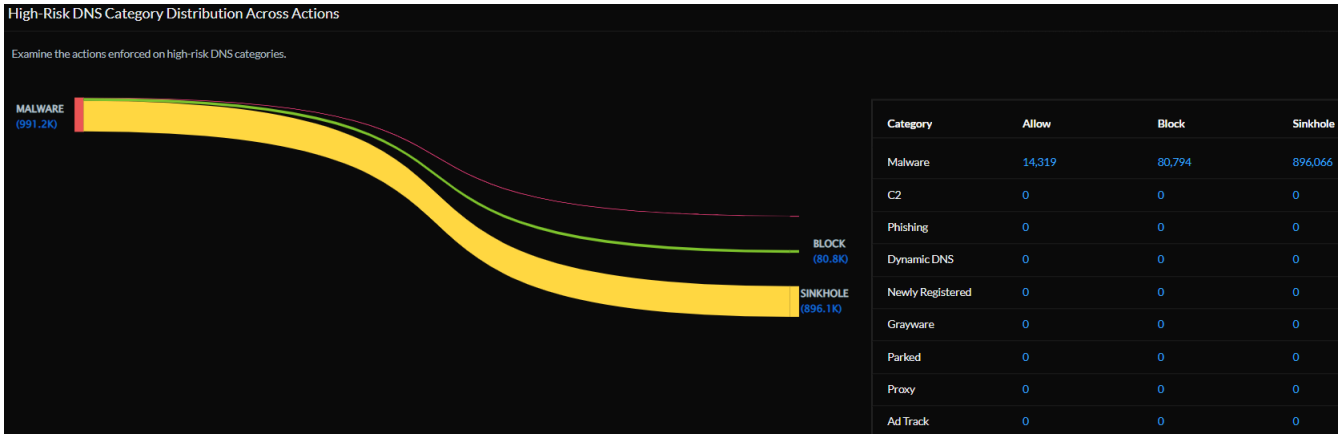
- **Requêtes DNS malveillantes** : affiche un graphique à barres empilées indiquant les requêtes DNS classées comme malveillantes. Cliquez sur le lien numérique afin d'afficher les détails des requêtes DNS.
- **Abonnement** : affiche le nombre de périphériques de votre réseau avec un abonnement de Sécurité DNS. Un pourcentage de périphériques qui ne disposent pas de la sécurité DNS ou dont l'abonnement a expiré est également affiché avec un lien vers une liste complète.



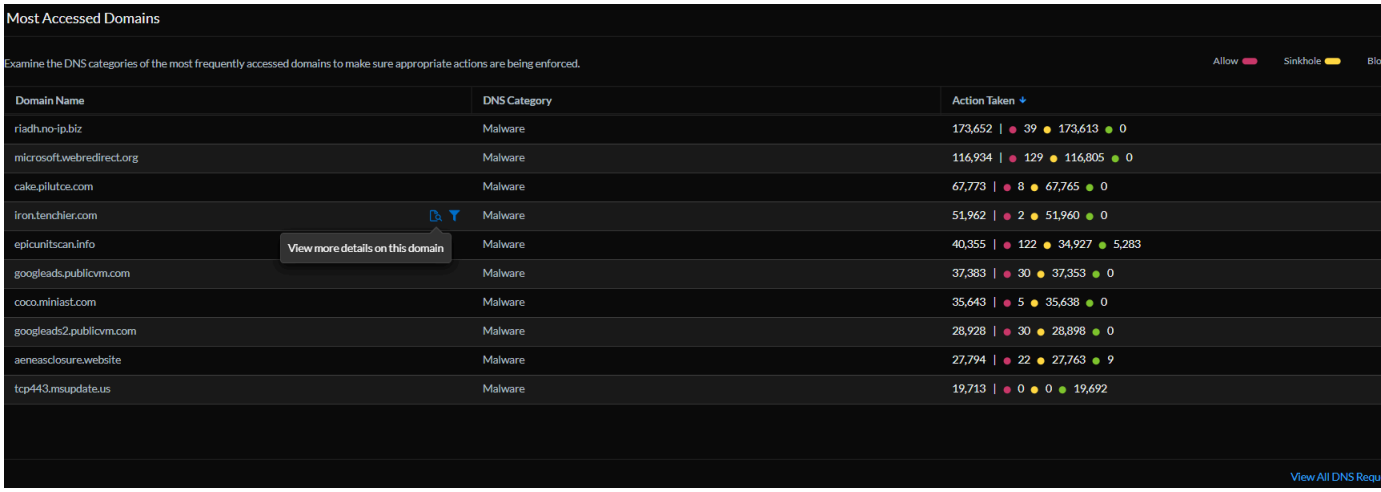
- **Tendances des catégories DNS à haut risque** : examinez la tendance des requêtes DNS à haut risque en fonction de la catégorie DNS ou en fonction des mesures prises à leur encontre. Survoler un flux spécifique pour ouvrir une fenêtre contextuelle indiquant le nombre de requêtes ou le type d'action appliquée.



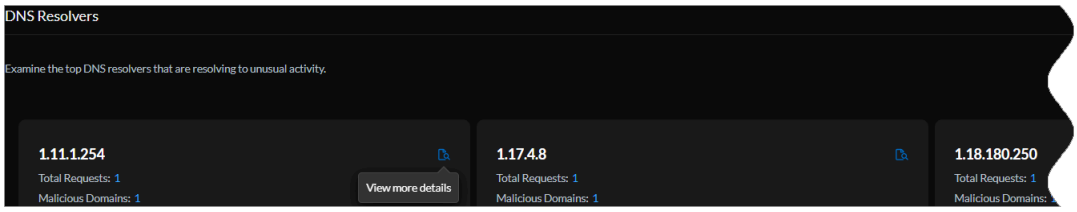
- **Répartition des catégories DNS à haut risque entre les actions** : examinez les actions entreprises par le pare-feu contre des catégories DNS à haut risque particulières.



- **Domaines d'accès les plus consultés** : fournit une liste des 10 domaines les plus fréquemment demandés sur votre réseau ainsi que la catégorie DNS et l'action entreprise. Vous pouvez afficher plus de détails et les journaux pertinents pour un domaine. Sélectionnez **Afficher toutes les requêtes DNS** afin d'obtenir la liste complète des domaines auxquels vous avez accédé.

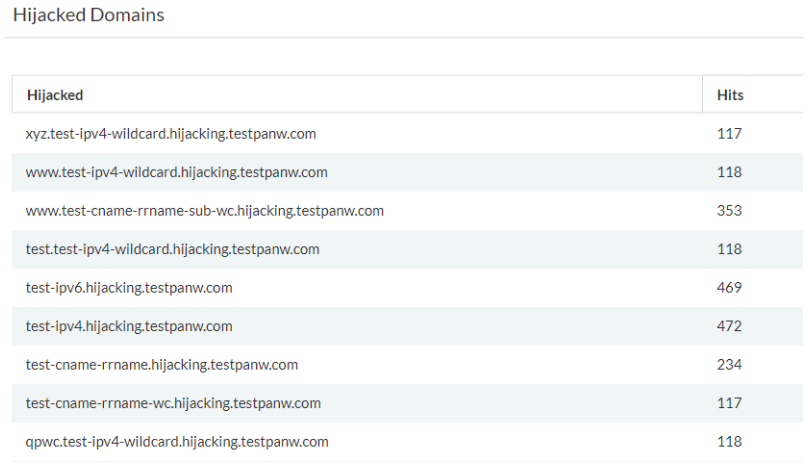


- **Résolveurs DNS** : surveille les activités de résolution des DNS malveillantes et suspectes dans votre réseau. Affichez les principaux résolveurs DNS qui résolvent des domaines malveillants et ceux qui résolvent un nombre anormalement bas de requêtes DNS. Cliquez sur l'icône de recherche pour afficher plus de détails sur l'artefact (adresse IP). Vous pouvez afficher l'historique de l'artefact dans votre réseau et les résultats de l'analyse globale.



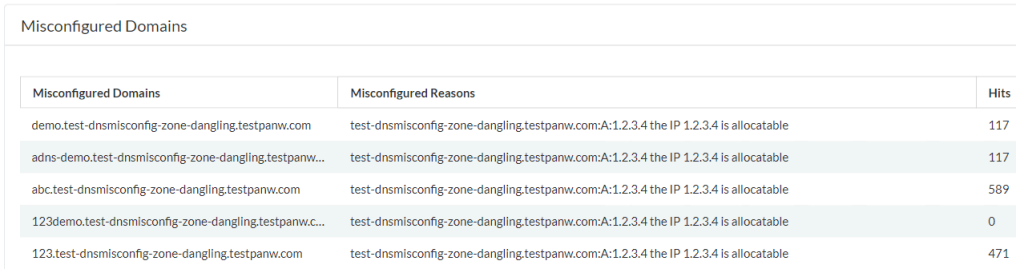
- **Utilisateurs visitant des domaines malveillants** : examinez les hôtes de votre réseau qui tentent de résoudre le nom d'hôte ou le domaine d'une URL malveillante.

- **(Nécessite une licence de Sécurité DNS avancée) Domaines piratés** : fournit une liste des domaines piratés tels que déterminés par Sécurité DNS avancée. Pour chaque entrée, il existe une raison de catégorisation et un nombre de trafics atteint en fonction de l'adresse IP source.


Hijacked Domains

Hijacked	Hits
xyz.test-ipv4-wildcard.hijacking.testpanw.com	117
www.test-ipv4-wildcard.hijacking.testpanw.com	118
www.test-cname-rrname-sub-wc.hijacking.testpanw.com	353
test.test-ipv4-wildcard.hijacking.testpanw.com	118
test-ipv6.hijacking.testpanw.com	469
test-ipv4.hijacking.testpanw.com	472
test-cname-rrname.hijacking.testpanw.com	234
test-cname-rrname-wc.hijacking.testpanw.com	117
qpwc.test-ipv4-wildcard.hijacking.testpanw.com	118

- **(Nécessite une licence de sécurité DNS avancée) Domaines mal configurés** : fournit une liste de domaines non résolvables associés aux domaines parents publics spécifiés par l'utilisateur. Pour chaque entrée, il existe une raison de mauvaise configuration et un nombre de trafics atteint basé sur l'adresse IP source.


Misconfigured Domains

Misconfigured Domains	Misconfigured Reasons	Hits
demo.test-dnsmisconfig-zone-dangling.testpanw.com	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	117
adns-demo.test-dnsmisconfig-zone-dangling.testpanw...	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	117
abc.test-dnsmisconfig-zone-dangling.testpanw.com	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	589
123demo.test-dnsmisconfig-zone-dangling.testpanw.c...	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	0
123.test-dnsmisconfig-zone-dangling.testpanw.com	test-dnsmisconfig-zone-dangling.testpanw.com:A:1.2.3.4 the IP 1.2.3.4 is allocatable	471

Ce tableau de bord prend en charge les rapports. Ces icônes,  en haut à droite d'un tableau de bord, indiquent que les rapports sont pris en charge pour ce tableau de bord. Vous pouvez partager, télécharger et planifier des rapports qui couvrent les données affichées par ce tableau de bord.

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

Ce tableau de bord vous permet de :

- examiner comment les requêtes DNS sont traitées et catégorisées
- obtenir un aperçu des menaces basées sur le DNS
- détecter les requêtes DNS provenant de domaines piratés et mal configurés avec la sécurité DNS avancée

Tableau de bord : AI Runtime Security

Le tableau de bord du centre de commande Strata Cloud Manager (SCM) fournit une vue consolidée des charges de travail cloud déployées dans les clusters et les machines virtuelles, telles que les pods, les modèles, les applis, les machines virtuelles et les espaces de noms.

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• AI Runtime Security	☐ Activez votre licence AI Runtime Security ☐ Conditions préalables à la configuration du AI Runtime Security ☐ Intégrez et activez un compte Cloud dans SCM

Découvrir les ressources du Cloud

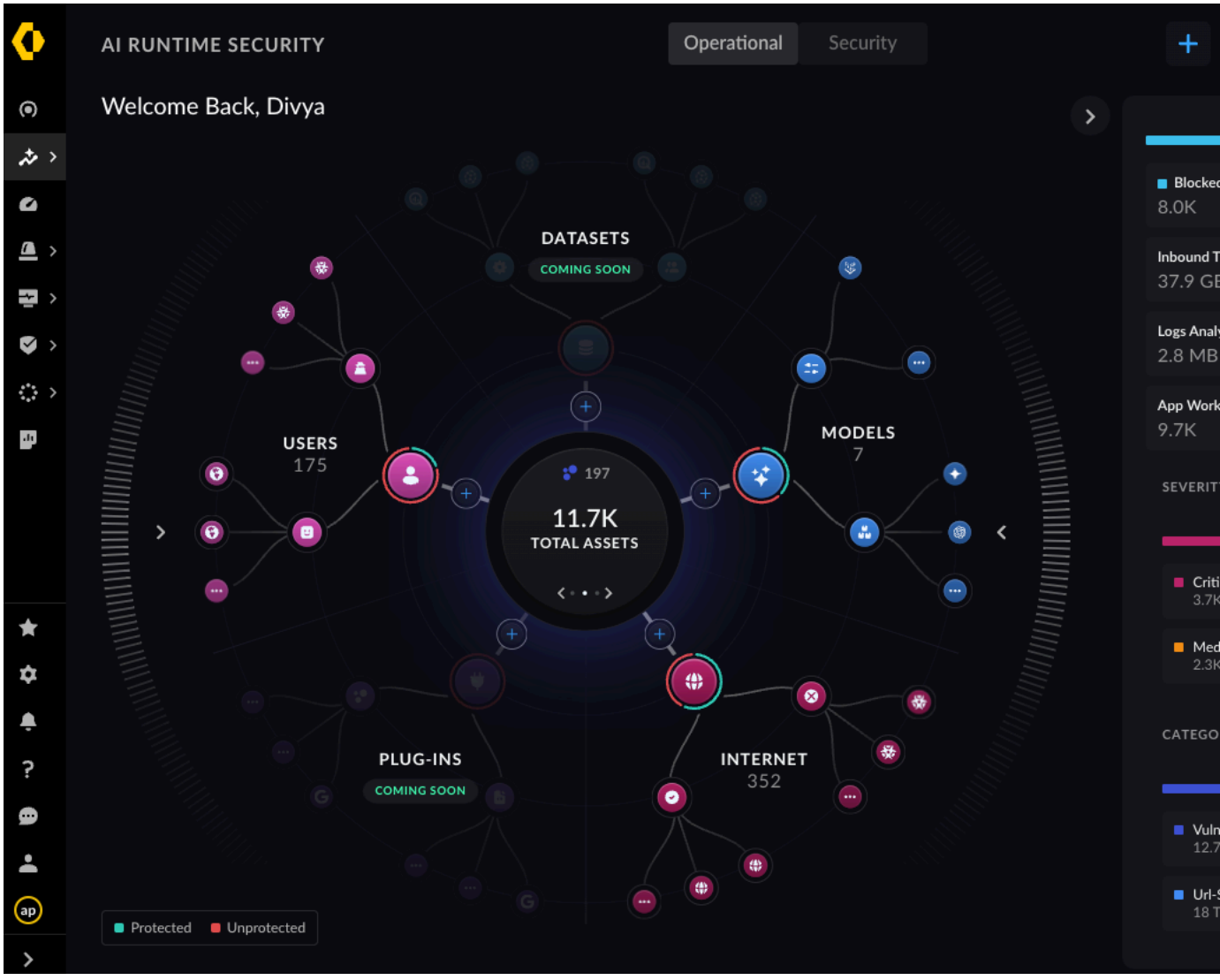
Une fois votre compte cloud intégré dans SCM et votre compte de service activé, le tableau de bord SCM fournit une découverte unifiée en temps réel des ressources de vos charges de travail cloud.

Le **centre de commande des applications cloud** dans SCM sous **Insights (Informations)** → **AI Runtime Security** fournit des informations exploitables sur la découverte de toutes les ressources cloud de votre compte cloud intégré.

La découverte des ressources sur le tableau de bord SCM est classée dans la vue opérationnelle et la vue de sécurité.

La découverte montre la répartition des menaces en fonction de l'urgence des menaces et des catégories de risques telles que la détection des vulnérabilités, la sécurité des URL et l'injection rapide.

1. La **vue opérationnelle** est une vue agrégée de :
    1. Le nombre total et répartition des actifs découverts dans vos environnements cloud intégrés
    2. Flux de trafic : protégés et non protégés par l'instance AI Runtime Security
    3. Charges de travail des applications (conteneurs, fonctions sans serveur et machines virtuelles)
    4. Modèles d'IA interrogés
    5. Applications utilisateur accédant aux destinations Internet
    6. Applications des utilisateurs d'applications accessibles à partir d'applications externes
    7. Statistiques du trafic entrant et sortant



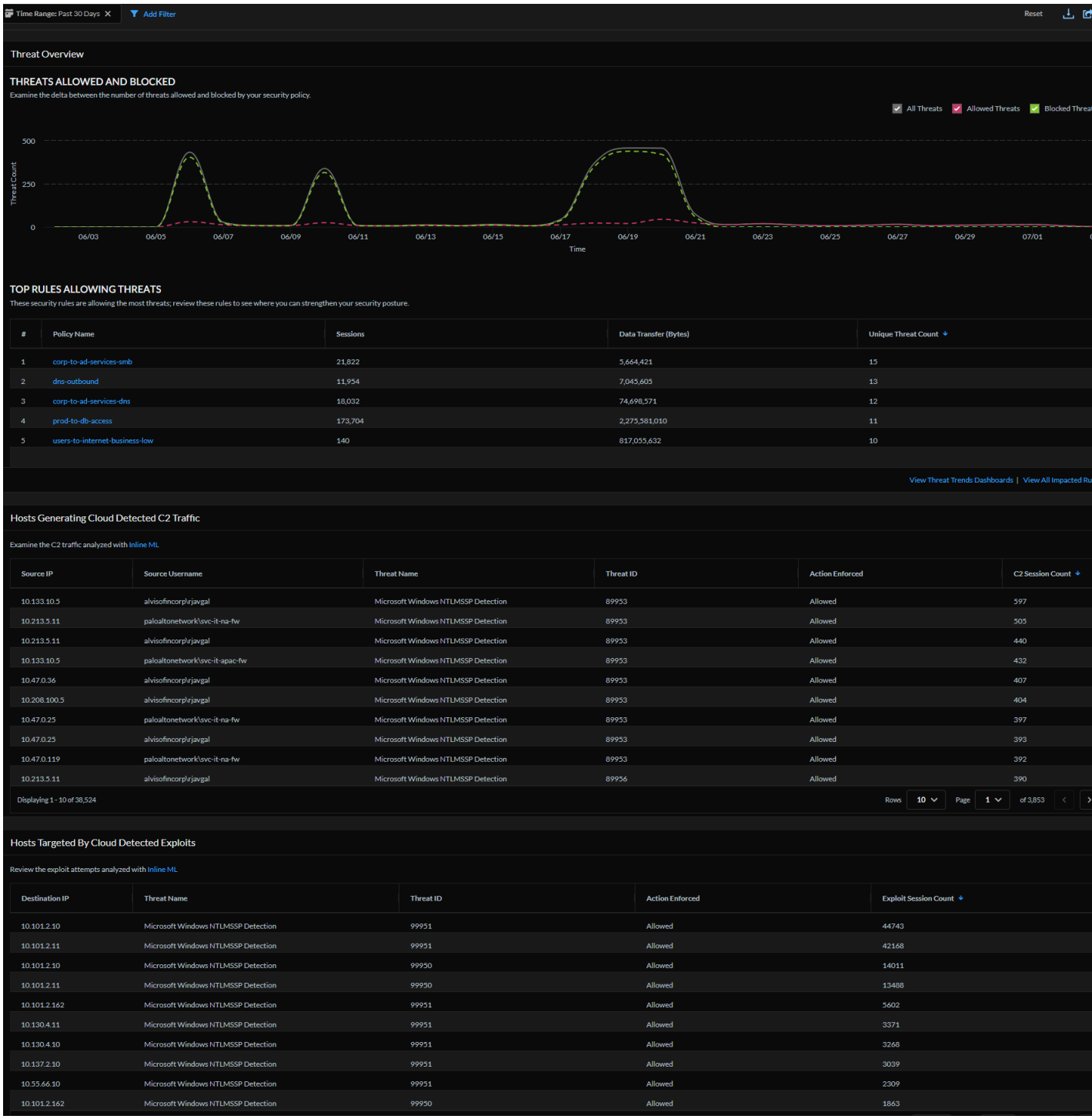
2. Dans la **Vue de sécurité** :
    1. Vous pouvez ajouter une instance AI Runtime Security (icône « + ») afin de protéger le trafic réseau non protégé tel qu'identifié dans la vue opérationnelle.
    2. Si la protection de l'instance AI Runtime Security existe déjà, redirigez le trafic non protégé via l'instance AI Runtime Security disponible.

Ensuite, il faut détecter les flux réseau à risque entre les appli utilisateur, les modèles d'IA et Internet. Consultez AI Traffic Network Risk Analysis et Deploy an AI Runtime Security instance pour surveiller et défendre votre architecture réseau cloud.

Tableau de bord : Prévention avancée des menaces

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Les autres licences et prérequis nécessaires à la visibilité sont : ☐ Un rôle https://docs.paloaltonetworks.com/common-services/identity-and-access-access-management/manage-identity-and-access/about-roles-and-permissions qui a l'autorisation d'afficher le tableau de bord ☐ Prévention des menaces ou Prévention des menaces avancée → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Strata Cloud Manager** > **Dashboards (Tableaux de bord)** > **More Dashboards (Plus de tableaux de bord)** > **Advanced Threat Prevention (Prévention avancée des menaces)** pour commencer.



Que vous indique ce tableau de bord ?

Le tableau de bord affiche des données agrégées par locataire Strata Logging Service.

Le tableau de bord de la prévention avancée des menaces donne un aperçu des menaces détectées dans votre réseau et identifie les possibilités de renforcer votre posture de sécurité.

Les menaces sont détectées à l'aide de modèles d'analyse cloud en ligne et de signatures de menaces générées à partir de données de trafic malveillant collectées à partir de divers services Palo Alto Networks. Ce tableau de bord fournit une vue chronologique des menaces autorisées et bloquées ainsi qu'une liste des hôtes générant du trafic C2 détecté dans le cloud et des hôtes ciblés par des exploits détectés dans le cloud.

Ce tableau de bord prend en charge les rapports. Ces icônes,  en haut à droite d'un tableau de bord, indiquent que les rapports sont pris en charge pour ce tableau de bord. Vous pouvez partager, télécharger et planifier des rapports qui couvrent les données affichées par ce tableau de bord.

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

Utilisez ce tableau de bord pour :

- obtenir une visibilité sur les menaces dans votre trafic réseau
- , analyser les sessions de menaces pour améliorer la précision de vos règles de politique,
- obtenir un aperçu de la menace en temps réel détectée par l'analyse cloud en ligne,
- obtenir un contexte autour de la menace à partir des journaux et des rapports cloud et utiliser ces données pour améliorer votre processus de réponse aux incidents.

Tableau de bord avancé de prévention des menaces : Vue d'ensemble des menaces

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro Les autres licences et prérequis nécessaires à la visibilité sont : ❑ Un rôle https://docs.paloaltonetworks.com/common-services/identity-and-access-access-management/manage-identity-and-access/about-roles-and-permissions qui a l'autorisation d'afficher le tableau de bord ❑ Prévention des menaces ou Prévention des menaces avancée → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Strata Cloud Manager** > **Dashboards (Tableaux de bord)** > **More Dashboards (Autres tableaux de bord)** > **Advanced Threat Prevention (Prévention des menaces avancées)** pour afficher le tableau de bord.

Comparer le delta entre les menaces autorisées et bloquées par vos règles de sécurité.

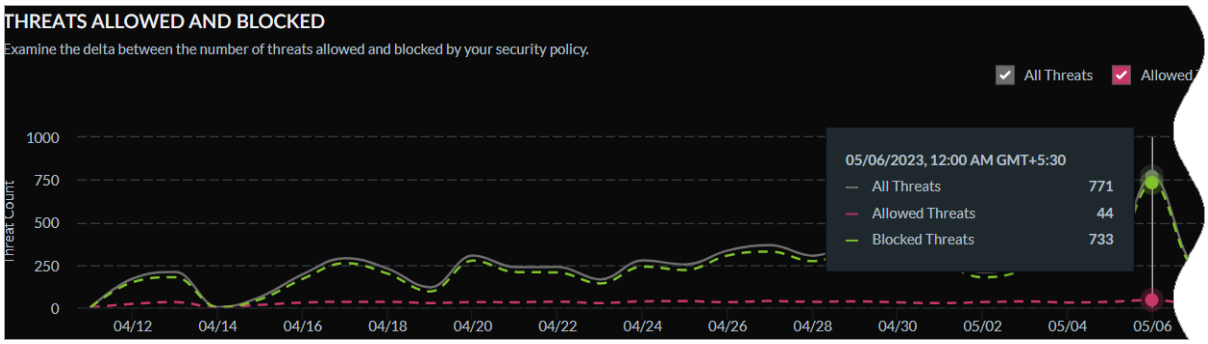


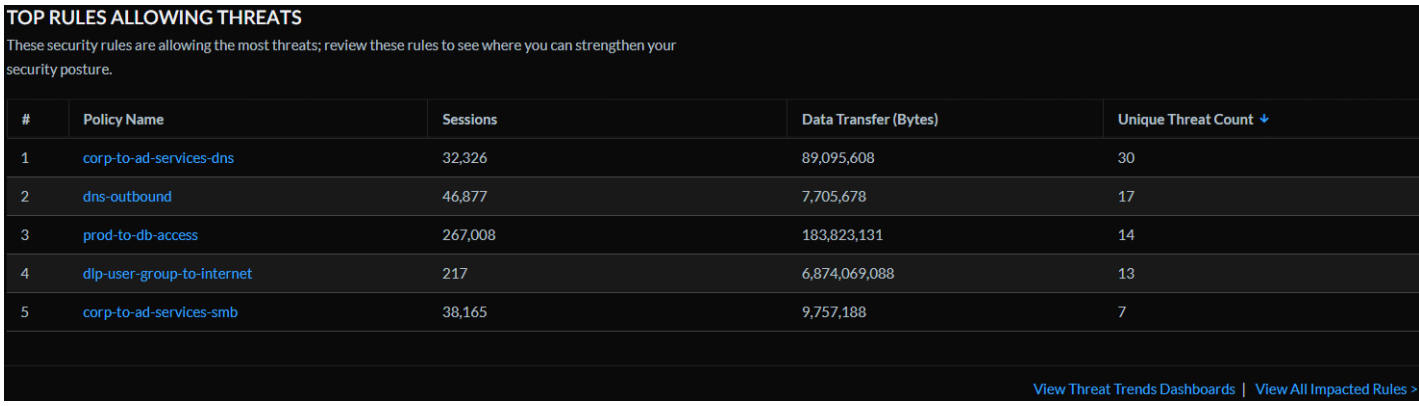
Tableau de bord avancé de prévention des menaces : Principales règles autorisant les menaces

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Les autres licences et prérequis nécessaires à la visibilité sont : ☐ Un rôle https://docs.paloaltonetworks.com/common-services/identity-and-access-access-management/manage-identity-and-access/about-roles-and-permissions qui a l'autorisation d'afficher le tableau de bord ☐ Prévention des menaces ou Prévention des menaces avancée → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Strata Cloud Manager** > **Dashboards (Tableaux de bord)** > **More Dashboards (Autres tableaux de bord)** > **Advanced Threat Prevention (Prévention des menaces avancées)** pour afficher le tableau de bord.

Examinez les sessions de menaces qui correspondaient à la règle de politique de sécurité et voyez si vous devez modifier la règle de politique pour renforcer votre posture de sécurité. Vous pouvez analyser plus en détail les menaces et les règles de correspondance dans Informations sur l'activité.



Colonne	Description
Nom de politique	Règle de politique de sécurité qui autorise les menaces correspondantes.
Sessions	Le nombre de sessions de menaces correspondant à la règle de politique de sécurité.
Transfert de données (octets)	Quantité de données circulant dans les sessions qui correspondait à la règle de politique de sécurité.
Nombre de menaces uniques	Le nombre de menaces correspondant à la règle de politique de sécurité.

Tableau de bord avancé de prévention des menaces : Hôtes générant du trafic C2 détecté dans le cloud

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Les autres licences et prérequis nécessaires à la visibilité sont : ☐ Un rôle https://docs.paloaltonetworks.com/common-services/identity-and-access-access-management/manage-identity-and-access/about-roles-and-permissions qui a l'autorisation d'afficher le tableau de bord ☐ Prévention des menaces ou Prévention des menaces avancée → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Strata Cloud Manager** > **Dashboards (Tableaux de bord)** > **More Dashboards (Autres tableaux de bord)** > **Advanced Threat Prevention (Prévention des menaces avancées)** pour afficher le tableau de bord.

Examiner les adresses IP source et les utilisateurs responsables de la génération de trafic de commande et de contrôle (C2). La prévention des menaces avancées utilise des moteurs basés sur le cloud et une analyse cloud en ligne pour détecter et analyser le trafic à la recherche de C2 inconnu et de vulnérabilités. Cliquez sur l'icône de recherche à côté de l'IP source pour examiner les modèles d'utilisation liés à l'IP source. Un lien contextuel vers la Visionneuse de journaux vous aide à analyser les sessions de menaces, télécharger la capture de paquets et le rapport cloud afin d'obtenir un contexte supplémentaire et exploiter les données analytiques de menaces Palo Alto Networks et améliorer vos processus de réponse aux incidents.

Tableau de bord avancé de prévention des menaces : Hôtes ciblés par des exploits détectés dans le cloud

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Les autres licences et prérequis nécessaires à la visibilité sont : ☐ Un rôle https://docs.paloaltonetworks.com/common-services/identity-and-access-access-management/manage-identity-and-access/about-roles-and-permissions qui a l'autorisation d'afficher le tableau de bord ☐ Prévention des menaces ou Prévention des menaces avancée → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Strata Cloud Manager** > **Dashboards (Tableaux de bord)** > **More Dashboards (Autres tableaux de bord)** > **Advanced Threat Prevention (Prévention des menaces avancées)** pour afficher le tableau de bord.

Ce sont les adresses IP visées par les exploits de vulnérabilité. La prévention des menaces avancées utilise des moteurs basés sur le cloud et une analyse cloud en ligne pour détecter et analyser ce trafic. Survolez l'adresse IP de destination et cliquez sur l'icône de recherche pour examiner les modèles d'utilisation liés à l'IP de destination. Affichez les journaux pour obtenir des informations concernant la menace. Télécharger les rapports cloud et la capture de paquets à partir des journaux afin d'obtenir des informations supplémentaires et utiliser les données analytiques des menaces ainsi que les renseignements sur les menaces de Palo Alto Networks pour améliorer vos processus de réponse aux incidents.

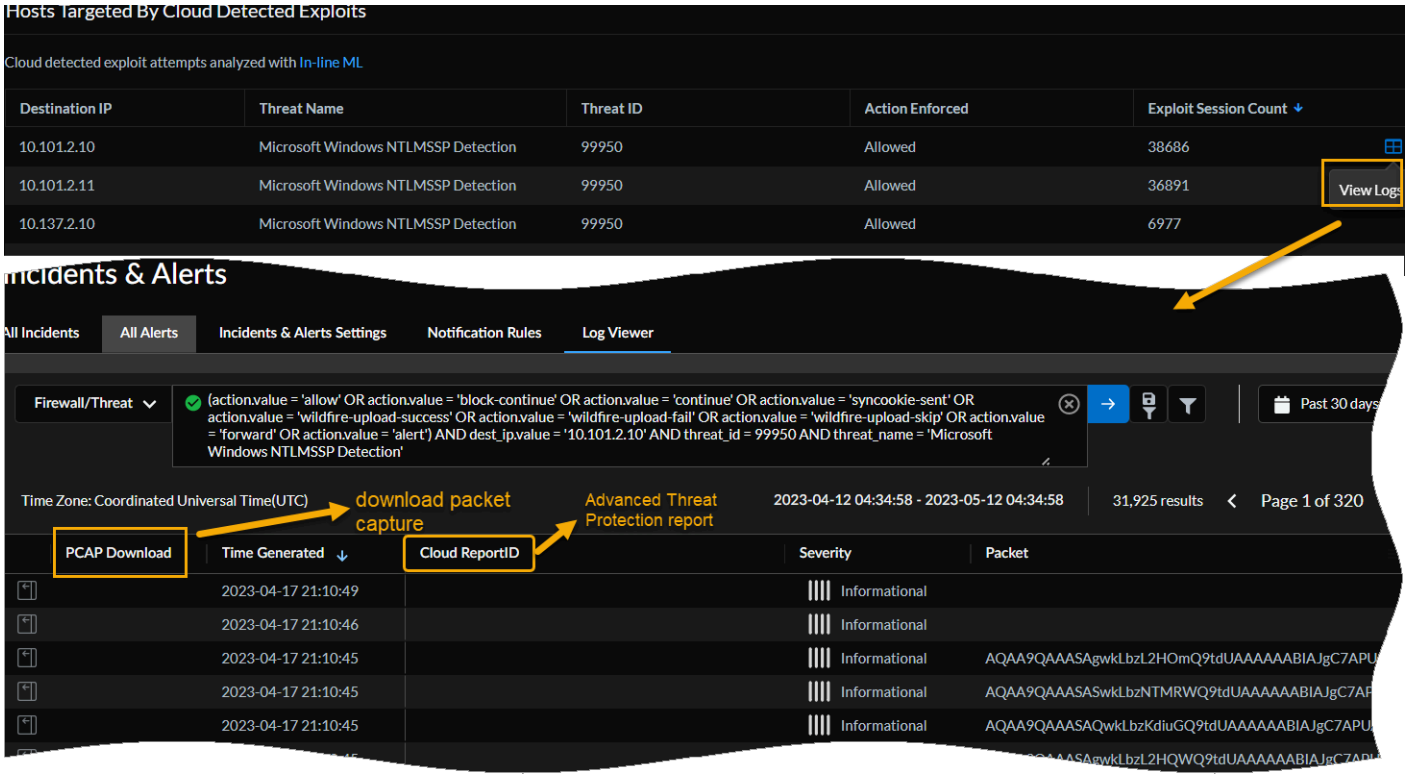
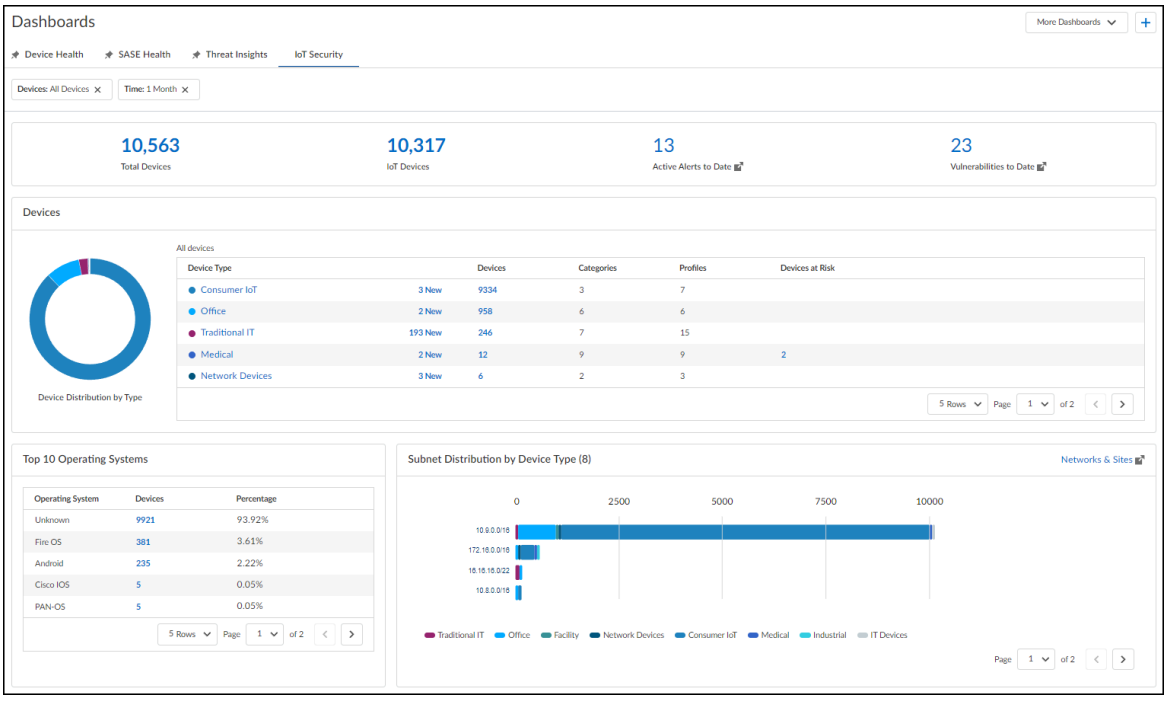


Tableau de bord : IoT Security

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Les autres licences et prérequis nécessaires à la visibilité sont : ☐ Un rôle qui a l'autorisation d'afficher le tableau de bord ☐ IoT Security → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Pour commencer, sélectionnez **Dashboards (Tableaux de bord)** > **More Dashboards (Plus de tableaux de bord)** > **IoT Security (Sécurité IoT)**.



Que vous indique ce tableau de bord ?

Le tableau de bord IoT Security fournit des informations sur les périphériques présents sur le réseau, leurs profils de périphérique et leurs systèmes d'exploitation, ainsi que la façon dont ils sont répartis par type de périphérique dans les sous-réseaux. Pour les produits de sécurité IoT avancés (Entreprise IoT Security plus, Industriel IoT Security, ou Médical IoT Security), le tableau de bord IoT Security affiche en outre le nombre total d'alertes et de vulnérabilités actives à ce jour.

Le texte en bleu est interactif. Voici ce qui se passe lorsque vous cliquez dessus :

- Résumé (en haut) : **Total Devices (Nombre total de périphériques)** et **IoT Devices (Périphériques IoT)** lien vers la page **Monitor (Moniteur)** > **Assets (Actif)** avec des filtres appliqués pour afficher l'inventaire de tous les périphériques ou de tous les périphériques IoT. Le texte en bleu indiquant les alertes et les vulnérabilités actives à ce jour ouvre les pages correspondantes dans votre portail IoT Security. (Lorsqu'il n'y a pas d'alertes ou de vulnérabilités, le nombre est 0 et aucun lien n'est disponible).
- Périphériques : cliquez sur une section du graphique ou sur une entrée de la colonne Type de périphérique pour effectuer un zoom avant afin d'afficher les catégories de périphériques d'un type choisi, puis sur les profils de périphériques d'une catégorie choisie. En cliquant sur **back (retour)** sur le graphique ou le chemin de navigation au-dessus du tableau, vous pouvez revenir à un niveau plus large de classification des périphériques.

  Les numéros présents dans les colonnes Périphériques et Périphériques à risque sont liés à la page **Monitor (Moniteur)** > **Assets (Actif).**Strata Cloud Manager applique automatiquement un filtre pour afficher les périphériques correspondant à la colonne et à la ligne choisies, qui peuvent être Type de périphérique, Nom de la catégorie ou Nom du profil en fonction du niveau actuel affiché.

  > *Vous voyez parfois le nombre de nouveaux périphériques détectés par IoT Security sur le réseau. Ces numéros apparaissent à gauche des numéros dans la colonne Périphériques. IoT Security considère que les périphériques sont « nouveaux » s'il les détecte pour la première fois sur le réseau dans le filtre horaire défini en haut du tableau de bord.*
- Les 10 principaux systèmes d'exploitation : les chiffres de la colonne Périphériques renvoient à la page **Monitor (Moniteur)** > **Assets (Actif)** avec un filtre appliqué pour n'afficher que les périphériques dotés du système d'exploitation choisi.
- Distribution des sous-réseaux par type de périphérique : survolez la barre d'un sous-réseau pour afficher le nombre de périphériques regroupés par type de périphériques dans le sous-réseau. Ces informations vous permettent de déterminer si un trop grand nombre de types de périphériques sans rapport les uns avec les autres sont mélangés dans le même sous-réseau. Par exemple, si vous voyez des périphériques IoT d'installations, industriels et grand public dans un sous-réseau, vous pouvez segmenter les périphériques de chaque type dans leurs propres sous-réseaux distincts. Cliquer sur **Networks & Sites (Réseaux et sites)** ouvre une nouvelle fenêtre de navigateur et ouvre **Networks (Réseau)** > **Networks and Sites (Réseaux et sites)** > **Networks (Réseau)** dans le portail de sécurité IoT.

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

Utilisez les données de ce tableau de bord pour en savoir plus sur les périphériques de votre réseau :

Filters (Filtres) (en haut de la page)

- Filtrez les données affichées dans le tableau de bord par type de périphériques et par période (année, mois, semaine, jour ou heure écoulés) pour afficher les données sur les périphériques qui vous intéressent.

Summary (Résumé) (en haut du tableau de bord)

- Consultez le nombre total de périphériques qui ont été actifs sur votre réseau, déterminé par le type de périphérique et les filtres de temps.
- Sur le nombre total de périphériques actifs, voyez combien sont spécifiquement des périphériques IoT.
- Développez une idée du paysage de sécurité dans lequel les périphériques fonctionnent en voyant le nombre d'alertes actives et de vulnérabilités détectées à ce jour.

Périphériques

- Découvrez le nombre de périphériques parmi les différents types de périphériques et explorez le nombre de périphériques répartis entre différentes catégories de périphériques, puis entre différents profils de périphérique. Découvrez combien de périphériques à risque critique se trouvent à chaque niveau de classification de plus en plus granulaire et de quel type de périphériques il s'agit.

Les 10 principaux systèmes d'exploitation

- De tous les périphériques détectés par le système d'exploitation IoT Security, consultez les 10 systèmes d'exploitation les plus courants, le nombre de périphériques qui utilisent chacun d'eux et le pourcentage de détection.

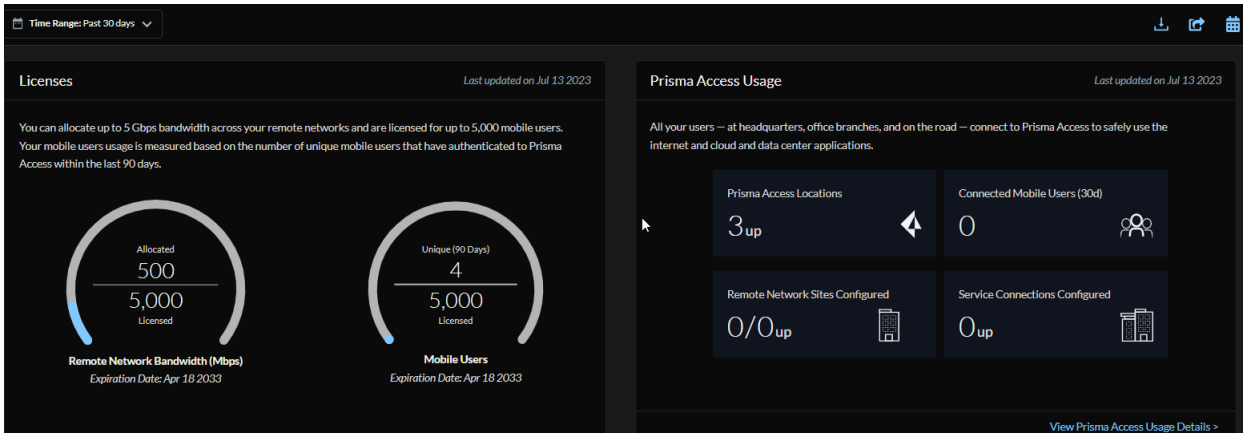
Distribution des sous-réseaux par type de périphérique

- Découvrez comment les différents types de périphériques sont répartis dans les sous-réseaux du réseau. Si un sous-réseau héberge une diversité de périphériques, il est recommandé de procéder à une segmentation en sous-réseaux distincts.

Tableau de bord : Prisma Access

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	L'une des options suivantes : ☐ Licence Prisma Access ☐ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Strata Cloud Manager** > **Dashboards (Tableaux de bord)** > **More Dashboards (Plus de Tableaux de bord)** > **Prisma Access** pour commencer.



Que vous indique ce tableau de bord ?

Assurez-vous de tirer profit de ce à quoi vous avez accès avec votre licence et bénéficiez d'une vision globale de l'état et des performances de votre environnement Prisma Access.

Les données d'utilisation de Prisma Access incluent :

- Un aperçu de votre utilisation de Prisma Access : vos licences, les emplacements Prisma Access et la capacité des utilisateurs mobiles et/ou l'utilisation de la bande passante
- Les meilleurs emplacements Prisma Access pour les utilisateurs mobiles et les réseaux distants
- La consommation globale de la bande passante pour les réseaux distants et les sites de connexion aux services, ainsi que les réseaux distants et les sites de connexion aux services qui consomment le plus
- Tendances de la déconnexion des tunnels, notamment les tunnels les plus impactés

Le tableau de bord présente les données agrégées par locataire Prisma Access.

Ce tableau de bord prend en charge les rapports. Ces icônes,  en haut à droite d'un tableau de bord, indiquent que les rapports sont pris en charge pour ce tableau de bord. Vous pouvez partager, télécharger et planifier des rapports qui couvrent les données affichées par ce tableau de bord.

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

Ce tableau de bord permet d'obtenir une visibilité sur l'utilisation de Prisma Access dans votre réseau et d'ajuster vos paramètres de configuration en fonction des données du tableau de bord.

Tableau de bord : Expérience d'application

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ Licence Prisma Access ❑ Licence ADEM Observability pour afficher les données relatives aux applications surveillées ❑ Licence pour les réseaux distants *(Nécessaire pour consulter les données relatives à l'expérience des sites distants)*

- Cliquez sur **Strata Cloud Manager** > **Dashboards (Tableaux de bord)** > **More Dashboards (Plus de tableaux de bord)** > **Expérience d'application** pour commencer.

Que vous indique ce tableau de bord ?

Les données affichées dans ce tableau de bord changeront et correspondront à la carte que vous aurez sélectionnée : expérience utilisateur mobile ou expérience sur site distant. Si vous êtes novice en ce qui concerne AI-Powered ADEM, vous pouvez commencer par recenser les applications utilisées dans votre entreprise et utiliser ces informations pour identifier les applications pour lesquelles vous souhaitez créer des tests d'appli. En outre, si des utilisateurs ou des sites distants signalent des problèmes d'application, ce tableau de bord est un bon point de départ pour identifier le problème. Les données d'utilisation de l'application sont extraites du trafic utilisateur réel transitant par Prisma Access. Elles incluent le trafic des Utilisateurs mobiles et des sites distants.

Vous pouvez ajouter un filtre pour réduire les résultats afin d'afficher les données pour des applications spécifiques, le type de déploiement, le score d'expérience, les utilisateurs mobiles, les groupes ou les emplacements Prisma Access. Consultez le score d'expérience individuel pour l'application et le nombre d'utilisateurs et de sites distants qui sont affectés par les problèmes de performance existants.

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

Après avoir examiné les applications en cours d'exécution sur votre réseau et déterminé celles que vous souhaitez surveiller, vous pouvez créer un test d'appli. Lorsque vous créez des tests d'appli, gardez à l'esprit la possibilité de créer des tests d'appli destinés à plusieurs utilisateurs ou sites. Le nombre de tests est basé sur le nombre de tests d'appli exécutés par chaque utilisateur ou périphérique ION (par exemple, si vous avez un test d'appli pour Slack et que vous le destinez à 1 000 utilisateurs, il sera comptabilisé dans votre licence comme étant 1 000 tests).

Tableau de bord de l'expérience d'application : Carte de l'expérience utilisateur mobile

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ Licence Prisma Access ❑ Licence ADEM Observability pour afficher les données relatives aux **Monitored Applications (Applications surveillées)**

Ce widget vous indique la moyenne du score par segment d'application pour tous les utilisateurs mobiles et pour toutes les applications surveillées. Il vous indique également la répartition des bonnes, moyennes et mauvaises expériences en fonction du nombre d'appareils de l'utilisateur. Vous avez la possibilité d'analyser les utilisateurs dont les performances sont moyennes ou médiocres afin de commencer à enquêter. Le score d'expérience de cette carte vous donnera une indication de l'expérience numérique globale de l'utilisateur. Pour chaque application surveillée par utilisateur mobile, l'ADEM calcule un score basé sur les 5 métriques critiques : la disponibilité de l'application, le temps de résolution DNS, le temps de connexion TCP, le temps de connexion SSL et la latence HTTP. Si l'application échoue au test de disponibilité (l'application est indisponible), le score d'expérience est de 0. Si l'application est accessibilité, alors seulement les quatre autres mesures seront calculées. Chacune des mesures ci-dessus (autres que l'accessibilité des applications) a une pondération différente et des seuils inférieurs et supérieurs définis, et leur pondération combinée est égale à 100. La somme de ces scores individuels détermine le score de l'expérience de l'application pour un utilisateur. La moyenne de tous les résultats de l'échantillon de test pour chaque application détermine le score d'expérience d'un utilisateur.

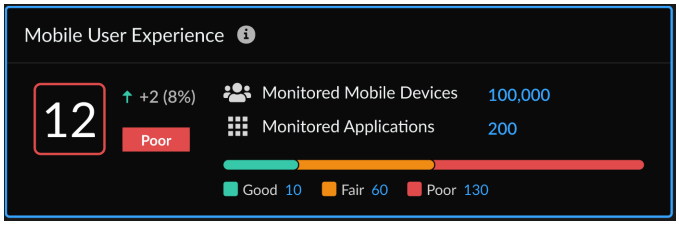


Tableau de bord de l'expérience d'application : Carte d'expérience du site distant

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ Licence Prisma Access ❑ Licence ADEM Observability pour afficher les données relatives aux **Monitored Applications (Applications surveillées)** ❑ Licence pour les réseaux distants

Le score d'expérience du site distant est un score moyen de toutes les applications surveillées sur tous les chemins WAN actifs. La moyenne de tous les résultats des échantillons de test collectés à partir des applications individuelles contrôlées pour ce site distant. Le score d'expérience global (entouré d'un carré de couleur) du site ou de l'agence distant. Il s'agit d'une moyenne des scores d'expérience de tous les échantillons de test collectés sur les chemins actifs de toutes les applications surveillées pour ce site. Bien que le score d'expérience de chaque chemin de sauvegarde soit calculé individuellement et disponible pour chaque site et application distants, le score d'expérience des chemins de sauvegarde ne sont pas pris en charge lors du calcul du score d'expérience d'un site distant. Vous pouvez creuser les sites qui connaissent des performances passables ou médiocres en cliquant sur le chiffre à côté de Passable ou Pauvre.

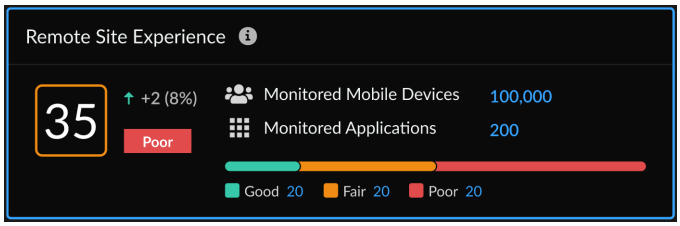


Tableau de bord de l'expérience d'application : Tendance du score de l'expérience

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ Licence Prisma Access ❑ Licence ADEM Observability pour afficher les données relatives aux **Monitored Applications (Applications surveillées)**

Ce widget affiche un graphique chronologique de l'expérience moyenne des utilisateurs de téléphones mobiles. Le score d'expérience est calculé et affiché à intervalles réguliers pendant la période sélectionnée. L'axe des ordonnées est codé par couleur en fonction de la fourchette de score pour vous indiquer la qualité de votre score d'expérience (rouge = médiocre, jaune = moyen, et vert = bon). À l'aide du curseur de votre souris, survolez la ligne de tendance pour voir le score d'expérience au moment où votre curseur est placé.

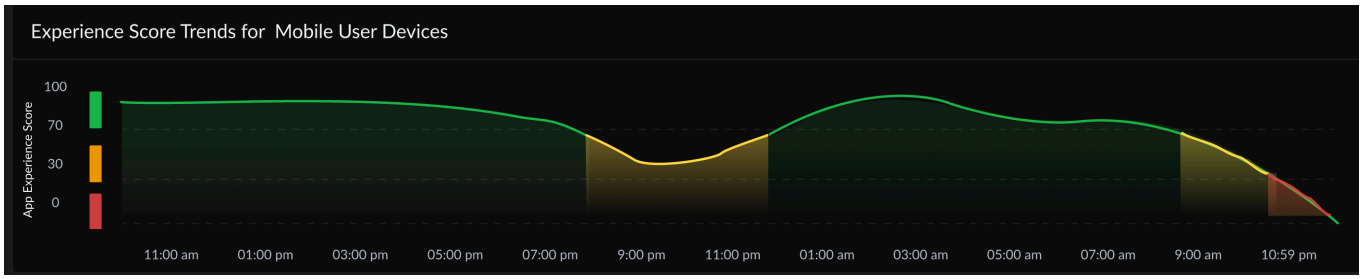
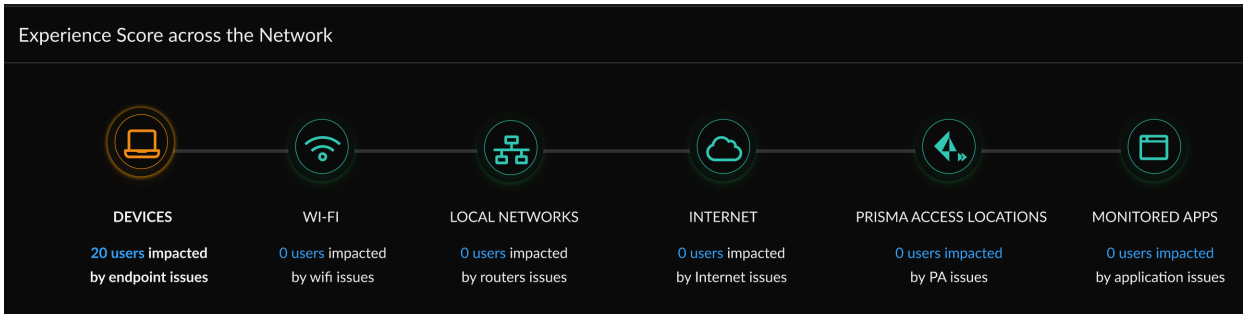


Tableau de bord de l'expérience d'application : Score d'expérience à travers le réseau

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ Licence Prisma Access ❑ Licence ADEM Observability pour afficher les données relatives aux **Monitored Applications (Applications surveillées)**

Identifier le segment du réseau qui pourrait causer des problèmes au sein de votre organisation, depuis les terminaux (pour les utilisateurs mobiles) ou les succursales (sites distants) jusqu'aux applications. Vous êtes en mesure de voir quel segment du réseau peut être à l'origine de problèmes au sein de votre organisation, depuis les terminaux et les sites distants Prisma SD-WAN jusqu'à l'application. Vous pouvez déterminer quel segment (par exemple, une interruption du service Internet ou une panne d'ordinateur, ou une panne d'appli SaaS) a un impact sur l'expérience numérique au sein de votre organisation, ainsi que le nombre précis d'utilisateurs ou de sites qui en subissent l'impact. Les icônes sont codées par couleur et sont basées sur la moyenne du score de segment de tous les utilisateurs mobiles. Une icône verte signifie Bon (le score est >= 70), le jaune signifie Moyen (le score est compris entre 30 et 70), le rouge signifie Mauvais (le score est < 30).



Périphériques : métriques de l'état de santé du dispositif (CPU/Mémoire/Espace disque/File d'attente du disque/Batterie)

Wi-Fi : métriques WIFI (qualité du signal, Tx, Rx, SSID, BSSID, canal)

Réseaux locaux : indicateurs de performance du réseau (latence/perte/gigue)

Internet : indicateurs de performance du réseau (latence/perte/gigue) si un périphérique n'est pas connecté à GlobalProtect, le segment Internet, les indicateurs de performance du réseau seront similaires à ceux du test TCP PING exécuté pour le segment d'application.

Emplacements de Prisma Access : indicateurs de performance du réseau (latence/perte/gigue) le test pour ce segment n'est pas exécuté si l'appareil n'est pas connecté à GlobalProtect.

Applications surveillées : indicateurs de performance du réseau (latence/perte/gigue) indicateurs de performance des applications (disponibilité, recherche DNS, connexion TCP, connexion SSL, latence HTTP, délai jusqu'au premier octet, délai jusqu'au dernier byte (octet), transfert de données)

Tableau de bord de l'expérience d'application : Distribution mondiale des scores d'expérience d'application

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ Licence Prisma Access ❑ Licence ADEM Observability pour afficher les données relatives aux **Monitored Applications (Applications surveillées)**

En fonction de la carte que vous sélectionnez, la vue cartographique de ce widget vous montre la situation des sites Prisma Access en fonction du nombre total d'utilisateurs mobiles et d'applications surveillées ou du nombre total de sites distants et d'applications en surveillance sur un site Prisma Access spécifique. Les sites Prisma Access sont marqués par des cercles dont le code couleur représente l'état des scores des segments d'application de tous les utilisateurs mobiles surveillés et des sites distants connectés au site Prisma Access spécifique où le cercle apparaît. À l'aide de votre souris, survolez un cercle pour voir les scores d'expérience pour l'emplacement, ainsi que le nombre total de périphériques d'utilisateurs mobiles ou de sites distants surveillés et le nombre total d'applis surveillées pour cet emplacement. Plusieurs emplacements géographiquement très proches les uns des autres sont représentés par un cercle contenant un chiffre. Le nombre indique le nombre d'emplacements regroupés dans cette zone. Dans le but de voir exactement quels lieux ont été regroupés, faites un zoom avant sur la carte.

Tableau de bord de l'expérience d'application : Score d'expérience pour les sites les plus surveillés

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ Licence Prisma Access ❑ Licence ADEM Observability pour afficher les données relatives aux **Monitored Applications (Applications surveillées)**

Ce widget présente une carte par application et affiche les sites ayant les scores les plus élevés. Ce widget montre l'évolution du score d'expérience des sites distants pendant la période sélectionnée. Faites passer le curseur de votre souris sur la ligne de tendance pour voir le score d'expérience pour ce point précis dans le temps.

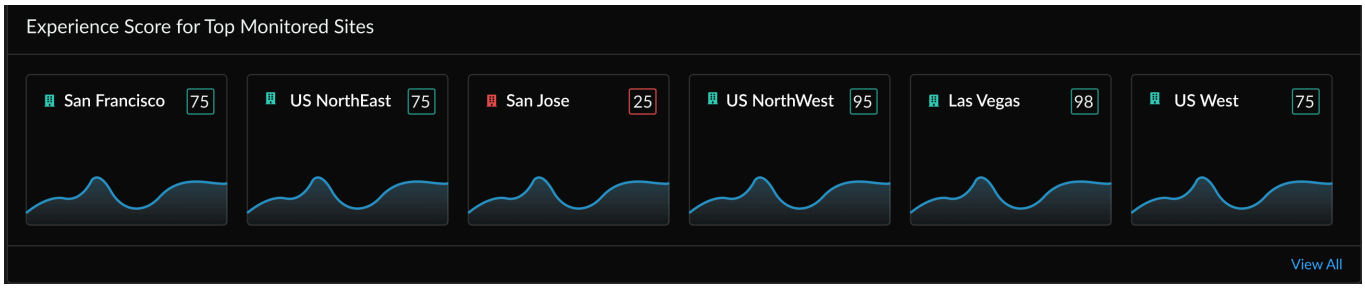


Tableau de bord de l'expérience d'application : Score d'expérience pour les meilleures applis surveillées

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ Licence Prisma Access ❑ Licence ADEM Observability pour afficher les données relatives aux **Monitored Applications (Applications surveillées)**

Chaque carte d'application vous indique le score moyen du segment d'application (le nombre compris dans le carré) pour tous les utilisateurs mobiles sous surveillance pour cette application particulière sur le site distant. Le score d'expérience est calculé comme une moyenne des scores d'expérience de toutes les applications sous surveillance. Le score d'expérience décrit l'expérience de bout en bout pour les chemins actifs de l'application. Il s'agit de la moyenne de tous les échantillons de test collectés sur les chemins actifs pour cette application spécifique uniquement. La ligne de tendance indique la moyenne de tous les échantillons de données APM de 5 minutes pour la période sélectionnée.

Vous pouvez voir le nombre d'applications que vous surveillez et le nombre de chemins d'accès actifs et de secours qui sont surveillés. Chaque carte d'application indique le nombre de chemins concernés. Cliquer sur une carte d'application pour voir les mesures de cette application spécifique.

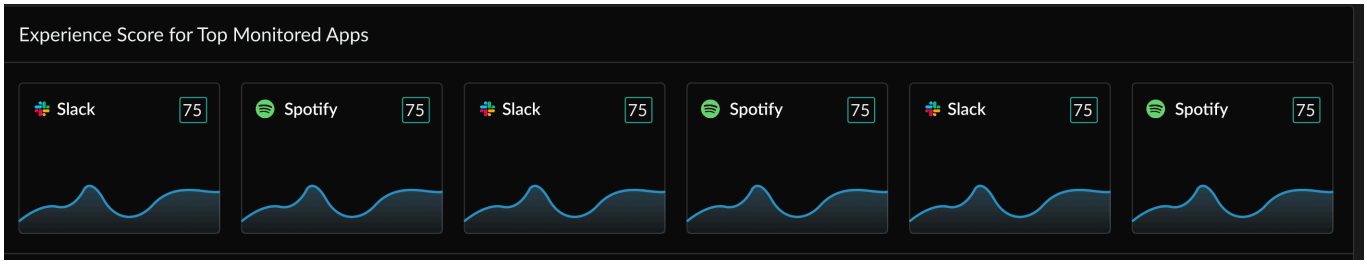


Tableau de bord de l'expérience d'application : Indicateurs de performance de l'application

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ Licence Prisma Access ❑ Licence ADEM Observability pour afficher les données relatives aux **Monitored Applications (Applications surveillées)**

Autonomous DEM utilise TCP ping et Curl pour déterminer les performances de l'application de bout en bout.

Mesure	Description
Disponibilité	Disponibilité de l'application (en pourcentage) pendant **l'intervalle de temps**.
Recherche DNS	Temps de résolution DNS.
Connexion TCP	Temps nécessaire pour établir une connexion TCP.
Connexion SSL	Temps nécessaire pour établir une connexion SSL.
Latence HTTP	Temps nécessaire pour établir une connexion HTTP.
Temps jusqu'au premier octet	La somme du temps de recherche DNS, de connexion TCP, de connexion SSL et de latence HTTP donne le temps du premier byte (octet).
Transfert de données	Durée totale du transfert de l'ensemble des données.
Temps jusqu'au dernier octet	Temps écoulé jusqu'au premier byte (octet) + temps de transfert des données.

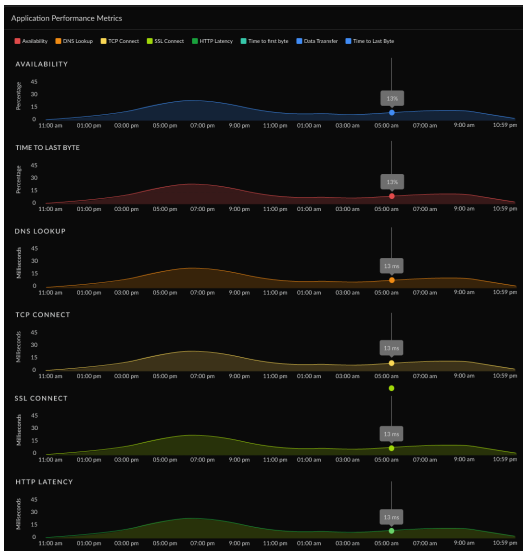


Tableau de bord de l'expérience d'application : Indicateurs de performance réseau

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ Licence Prisma Access ❑ Licence ADEM Observability pour afficher les données relatives aux **Monitored Applications (Applications surveillées)**

ADEM utilise des pings ICMP pour déterminer la performance du réseau sur chaque segment.

Mesure	Description
Disponibilité	Mesure de disponibilité du réseau pendant la **Time Range (Plage horaire)**.
Latence du réseau	Temps nécessaire pour transférer les données sur le réseau.
Perte de paquets	Perte de paquets lors de la transmission de données.
Jitter	Changement de latence pendant la **Time Range (Plage horaire)**.

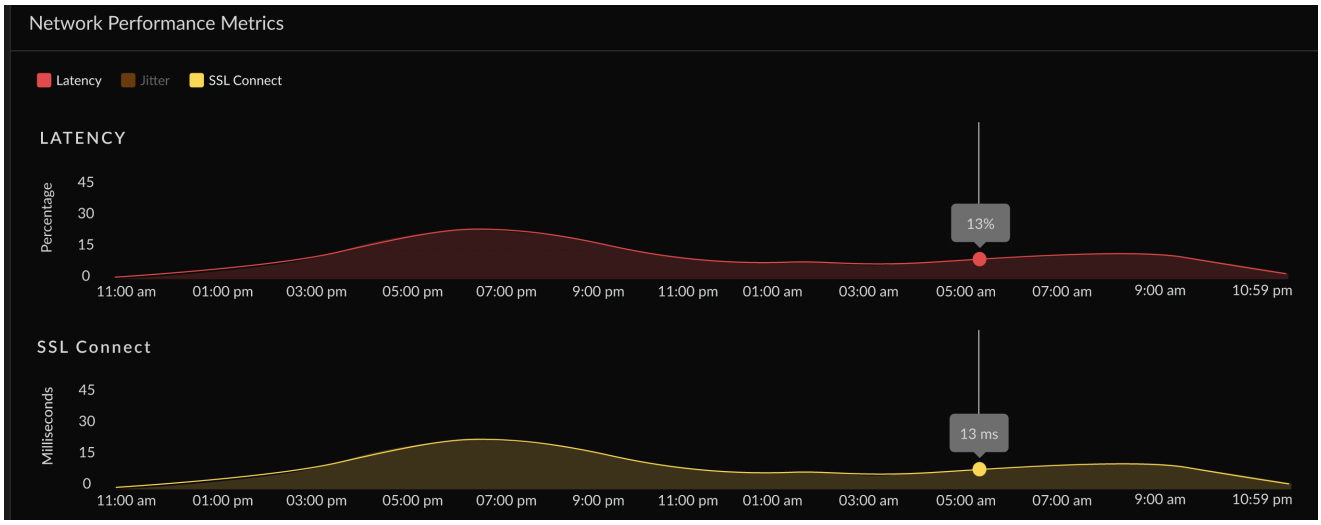
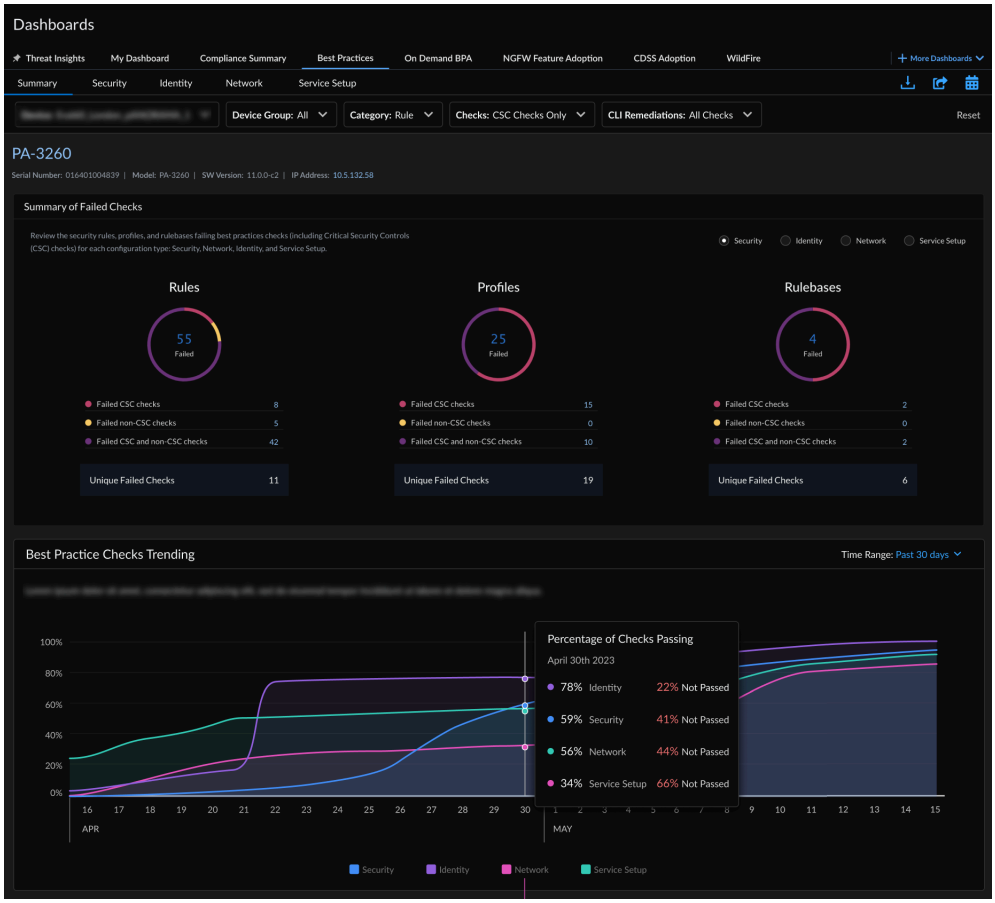


Tableau de bord : Meilleures pratiques

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Strata Cloud Manager** > **Dashboards (Tableaux de bord)** > **More Dashboards (Plus de tableaux de bord)** > **Best Practices (Meilleures pratiques)** pour commencer.



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.

Le tableau de bord des meilleures pratiques évalue 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.

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 stratégie 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 appareil 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.

Ce tableau de bord prend en charge les rapports. Ces icônes,  en haut à droite d'un tableau de bord, indiquent que les rapports sont pris en charge pour ce tableau de bord. Vous pouvez partager, télécharger et planifier des rapports qui couvrent les données affichées par ce tableau de bord.

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 secteurs nécessitant des changements pour une gestion plus efficace de votre environnement.

Tableau de bord : Résumé de la conformité

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ AIOps for NGFW Premium ou Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Vous pouvez consulter l'historique des modifications apportées à la vérification de sécurité effectués jusqu'à 12 mois auparavant, regroupés par le Center for Internet Security et le 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 contrôles des meilleures pratiques et le nombre de contrôles échoués pour chaque contrôle.

Interagissez avec le graphique et la liste afin de voir la relation entre les contrôles et leurs statistiques historiques. Consultez les détails des contrôles individuels et des vérifications qui leur sont associées, et sélectionnez une vérification des meilleures pratiques pour afficher la configuration du pare-feu qui échoue à la vérification.

Le cadre des contrôles de sécurité critiques du CIS est un ensemble prioritaire de mesures recommandées et de meilleurs pratiques qui aident à protéger les organisations et leurs données contre les vecteurs de cyberattaques connus. Vous pouvez consulter les résumés des contrôles pour 11 des 16 contrôles de base et fondamentaux du CIS :

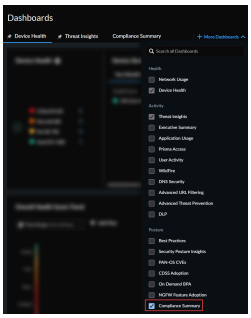
- CSC 3 : Gestion continue des vulnérabilités
- CSC 4 : Utilisation contrôlée des privilèges administratifs
- CSC 6 : Maintenance, surveillance et analyse des journaux d'audit.
- CSC 7 : Protection des messageries et des navigateurs Web
- CSC 8 : Défenses contre les logiciels malveillants
- CSC 9 : Limitation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

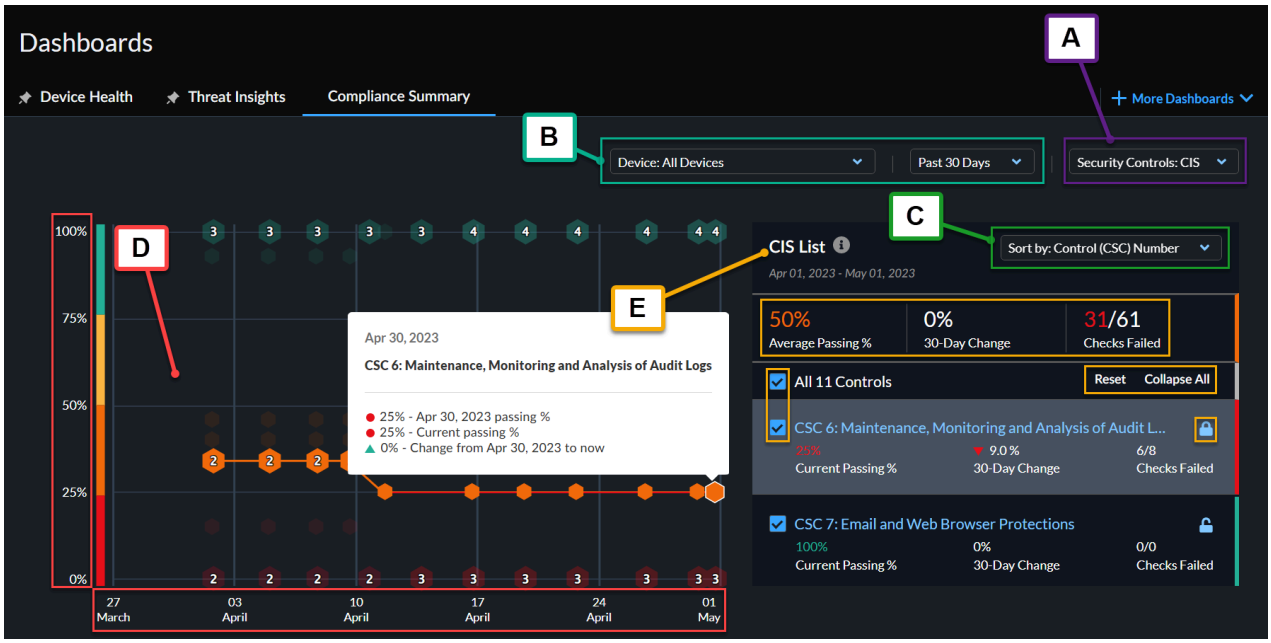
Le cadre de cybersécurité NIST SP 800-53 contrôle fournit des conseils aux organismes fédéraux et autres organisations pour mettre en œuvre et maintenir des contrôles de sécurité et de protection de la vie privée pour leurs systèmes d'information. Vous pouvez afficher les résumés des vérifications pour 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 accéder au tableau de bord récapitulatif de la conformité, accédez à **Dashboards (Tableaux de bord)**, puis sélectionnez l’onglet **Résumé de la conformité**.

*Si vous ne voyez pas de **Compliance Summary (Résumé de la conformité)** parmi les choix d’onglets, sélectionnez **More Dashboards (Plus de tableaux de bord)**, puis cochez la case **Compliance Summary (Résumé de la conformité)** dans les choix répertoriés sous **Posture**.*





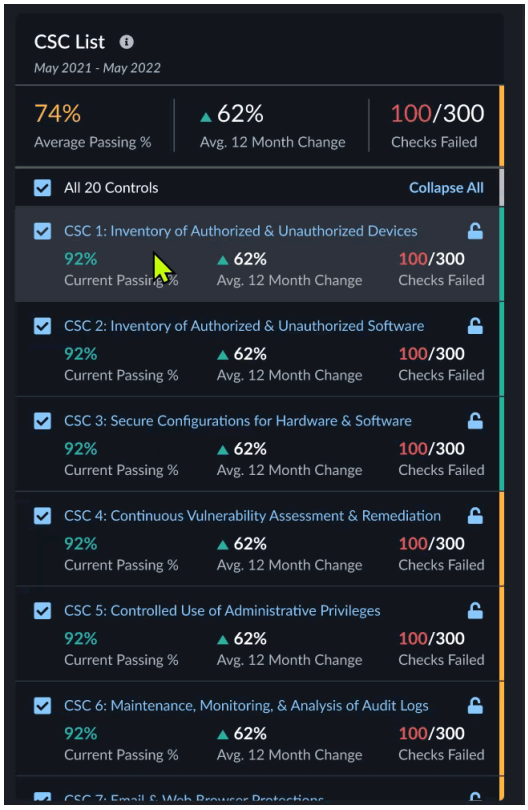
A) Commutateur des contrôles de sécurité	Sélectionnez les contrôles CIS ou NIST

B) Filtrer par	• Périphérique
	• Intervalle de temps
	  • 7 derniers jours
	  • 30 derniers jours
	  • 90 derniers jours
	  • 6 derniers mois
	  • 12 derniers mois

C) Classer par	• Numéro de contrôle CSC • % de réussite actuelle • % changement • Nombre de contrôles échoués
D) Graphique linéaire	• Passage % : affiche le pourcentage de passage pour un type de contrôle donné. • Chronologie : montre quand le pourcentage a été mesuré pour un type de contrôle donné.

E) Liste de vérification	• Statistiques
	  • % moyen de réussite : indique le pourcentage moyen de réussite des contrôles.
	  • Variation de 12 mois : montre la variation sur une période de 12 mois.
	  • Vérifications échouées : affiche le nombre de vérifications échouées.
	• Contrôles sélectionnés : une coche permet de visualiser un contrôle sur le graphique linéaire.
	• Réinitialiser : supprime tous les verrous.
	• Réduire tout/Agrandir tout : affiche/ Masque les statistiques dans la liste.
	• Verrouiller le graphique linéaire : garde les contrôles verrouillés en vue sur le graphique linéaire.

- *Sélectionnez un contrôle sur la liste pour voir les vérifications des meilleures pratiques qu'il inclut.*



- *Sélectionnez une vérification des meilleures pratiques pour afficher la configuration du pare-feu qui échoue au contrôle.*

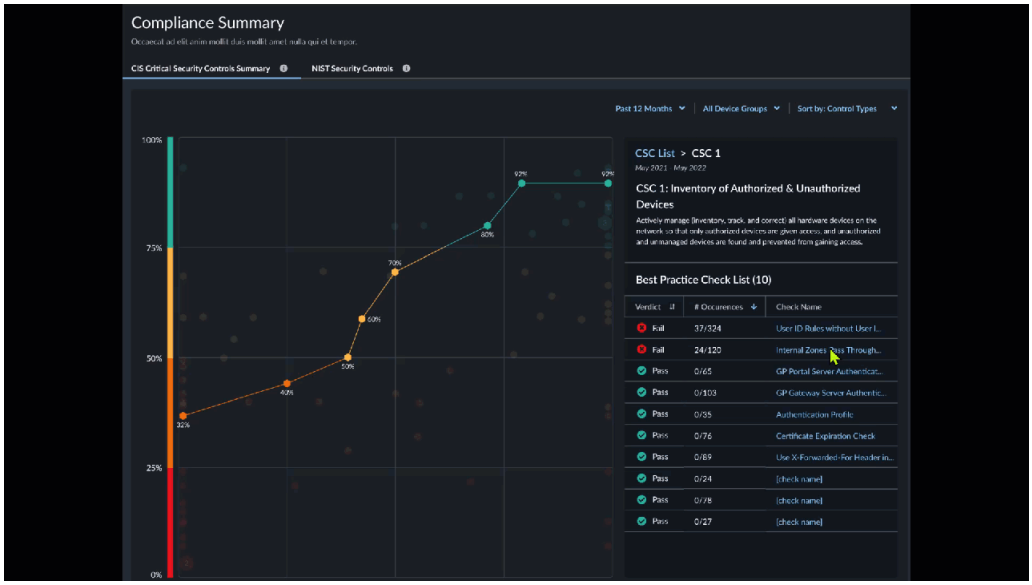
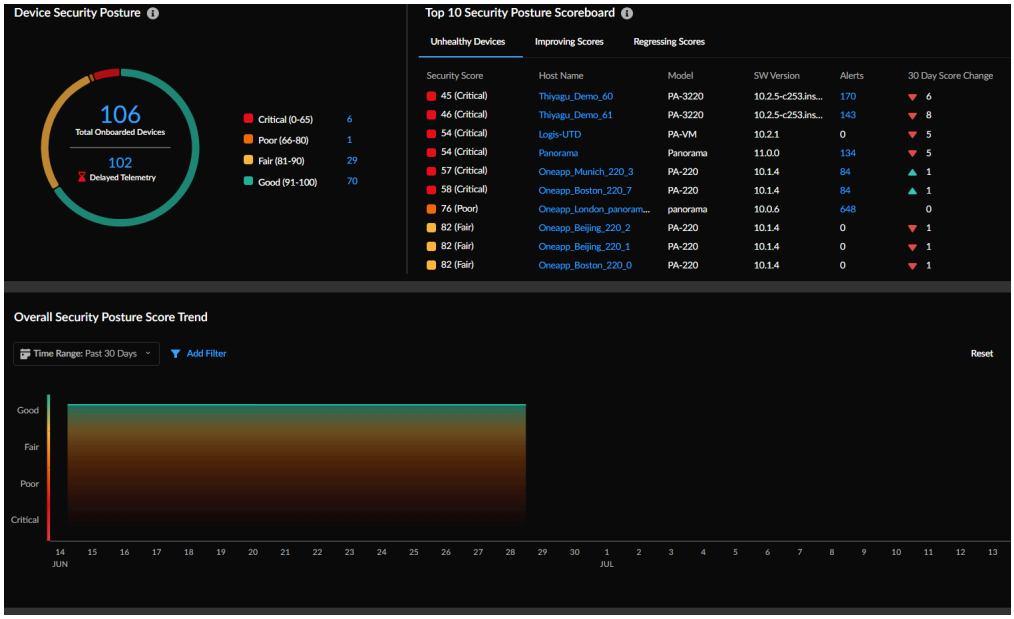


Tableau de bord : Informations sur la posture de sécurité

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium ou Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Strata Cloud Manager** > **Dashboards (Tableaux de bord)** > **More Dashboards (Plus de tableaux de bord)** > **Security Posture Insights (Informations sur la posture de sécurité)** pour commencer.



Que vous indique ce tableau de bord ?

Le tableau de bord affiche des données agrégées pour tous les pare-feu associés à votre locataire dans lesquels des données de télémétrie sont également envoyées.

Obtenez une visibilité sur l'état et les tendances 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.

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

Utilisez ce tableau de bord pour :

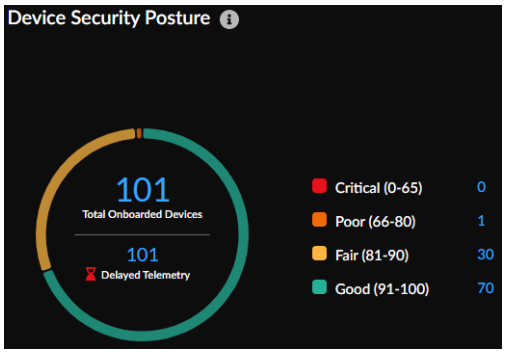
- Découvrez la tendance des problèmes qui ont un impact sur la sécurité de votre déploiement.
- Découvrez les améliorations que vous avez apportées à votre déploiement en matière de sécurité en examinant l'historique des scores de sécurité.
- Limitez les périphériques où il est possible d'améliorer la posture de sécurité et hiérarchisez les problèmes pour les résoudre.

La fonctionnalité de rapport (télécharger, partager et planifier le rapport) n'est pas prise en charge pour ce tableau de bord.

Tableau de bord des informations sur la posture de sécurité : Posture de sécurité du périphérique

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium ou Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Strata Cloud Manager** > **Dashboards (Tableaux de bord)** > **More Dashboards (Plus de tableaux de bord)** > **Security Posture Insights (Informations sur la posture de sécurité)** pour afficher le tableau de bord.



Le widget du tableau de bord affiche :

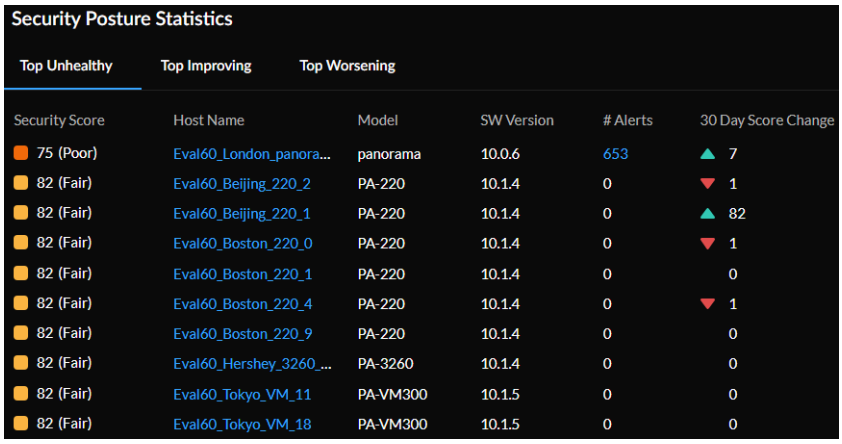
- Le nombre total de NGFW intégrés.
- Le nombre de périphériques qui n'ont pas envoyé de données de télémétrie pendant plus de 12 heures.

- 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.

Tableau de bord des informations sur la posture de sécurité : Statistiques sur les postures de sécurité

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium ou Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Strata Cloud Manager** > **Dashboards (Tableaux de bord)** > **More Dashboards (Plus de tableaux de bord)** > **Security Posture Insights (Informations sur la posture de sécurité)** pour afficher le tableau de bord.



Principaux éléments en mauvaise santé

Nous avons sélectionné les 10 périphériques qui ont le plus d'impact sur la sécurité de votre déploiement. Vous pouvez également consulter les détails du périphérique et les alertes qui s'y rapportent. Effectuez les étapes de correction pour les alertes critiques sur les périphériques afin d'améliorer l'état de sécurité.

Principale amélioration

Consultez les 10 principaux périphériques présentant des scores de sécurité améliorés sur une période de 30 jours, par rapport aux scores de sécurité actuels des périphériques.

Principale aggravation

Il s'agit des périphériques dont les scores de sécurité ont diminué par rapport aux scores de sécurité actuels des périphériques. Consultez les alertes sur ces périphériques et établissez des priorités pour les réparer.

Tableau de bord des informations sur la posture de sécurité : Tendance du score

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium ou Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Strata Cloud Manager** > **Dashboards (Tableaux de bord)** > **More Dashboards (Plus de tableaux de bord)** > **Security Posture Insights (Informations sur la posture de sécurité)** pour afficher le tableau de bord.

Le graphique présente l'évolution 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 la posture de sécurité. Vous pouvez afficher les tendances d'un ou de plusieurs périphériques filtrés par le nom d'hôte, le modèle ou la version du logiciel.

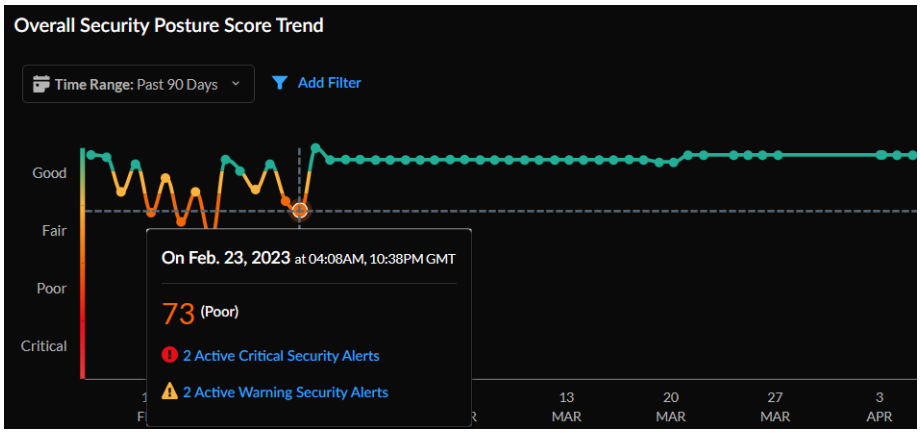
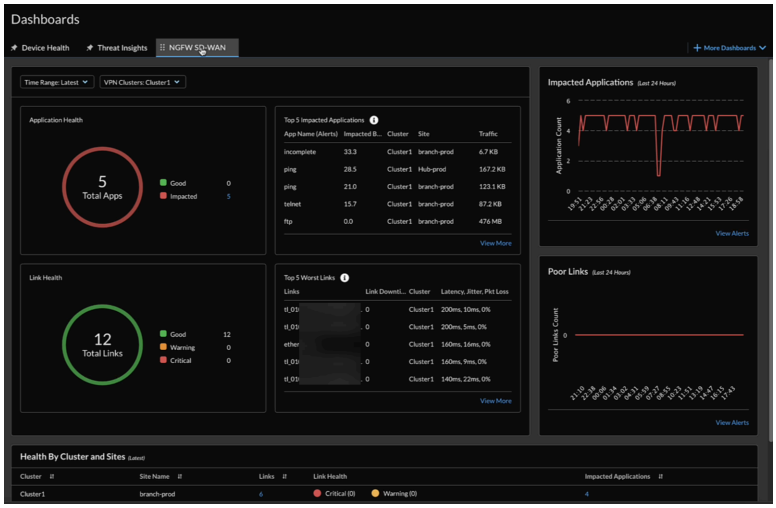


Tableau de bord : NGFW SD-WAN

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ AIOps for NGFW Premium ou Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Dashboards > More Dashboards > NGFW SD-WAN (Tableaux de bord > Plus de tableaux de bord > NGFW SD-WAN)** pour commencer.



Afin d'utiliser ce tableau de bord, vous pouvez configurer un réseau étendu défini par logiciel (SD-WAN) pour Strata Cloud Manager vos pare-feu nouvelle génération Palo Alto Networks.

Que vous indique ce tableau de bord ?

Le tableau de bord **NGFW SD-WAN** vous indique les mesures de performances des liens et du trafic d'application pour les pare-feu gérés dans le cloud avec SD-WAN.

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

Ce tableau de bord vous permet de :

- Avoir de la visibilité des mesures de performance des applications et des liens dans vos clusters VPN permet de résoudre les problèmes en affichant des informations récapitulatives dans tous les clusters VPN.
- Faire une analyse approfondie des problèmes pour isoler les sites, les applications et les liens concernés.

- Déclencher des alertes exploitables pour enquêter et restaurer les liens défaillants et les applications. Grâce à la détection d'anomalies, à la bande de normalité et aux prévisions optimisées par ML, les alertes exploitables sont basées sur des seuils fondés sur des données, et vous obtiendrez des informations sur les tendances.

Découvrez dans cette vidéo comment surveiller le tableau de bord NGFW SD-WAN.

Tableau de bord NGFW SD-WAN : Santé de l'application

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	☐ AIOps for NGFW Premium ou Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Le tableau de bord affiche :

- Le nombre total d'applications pour la durée et le cluster VPN sélectionnés.
- Le nombre d'applications affectées, c'est-à-dire une ou plusieurs applications du le cluster VPN pour lesquelles aucun des chemins n'a de performances gigue, de latence ou de perte de paquets répondant aux seuils spécifiés dans le profil de qualité du chemin dans la liste des chemins d'accès parmi lesquels le pare-feu peut choisir.
- Le nombre d'applications de bonne qualité, c'est-à-dire les applications du cluster VPN qui ne rencontrent pas de problèmes de gigue, de latence ou de performances de perte de paquets.

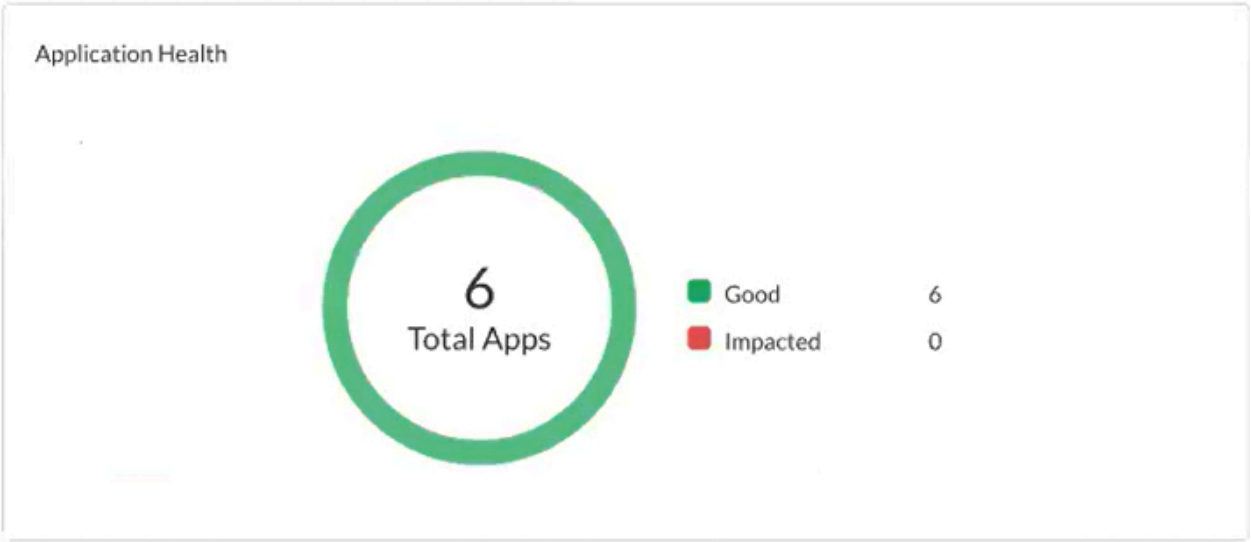
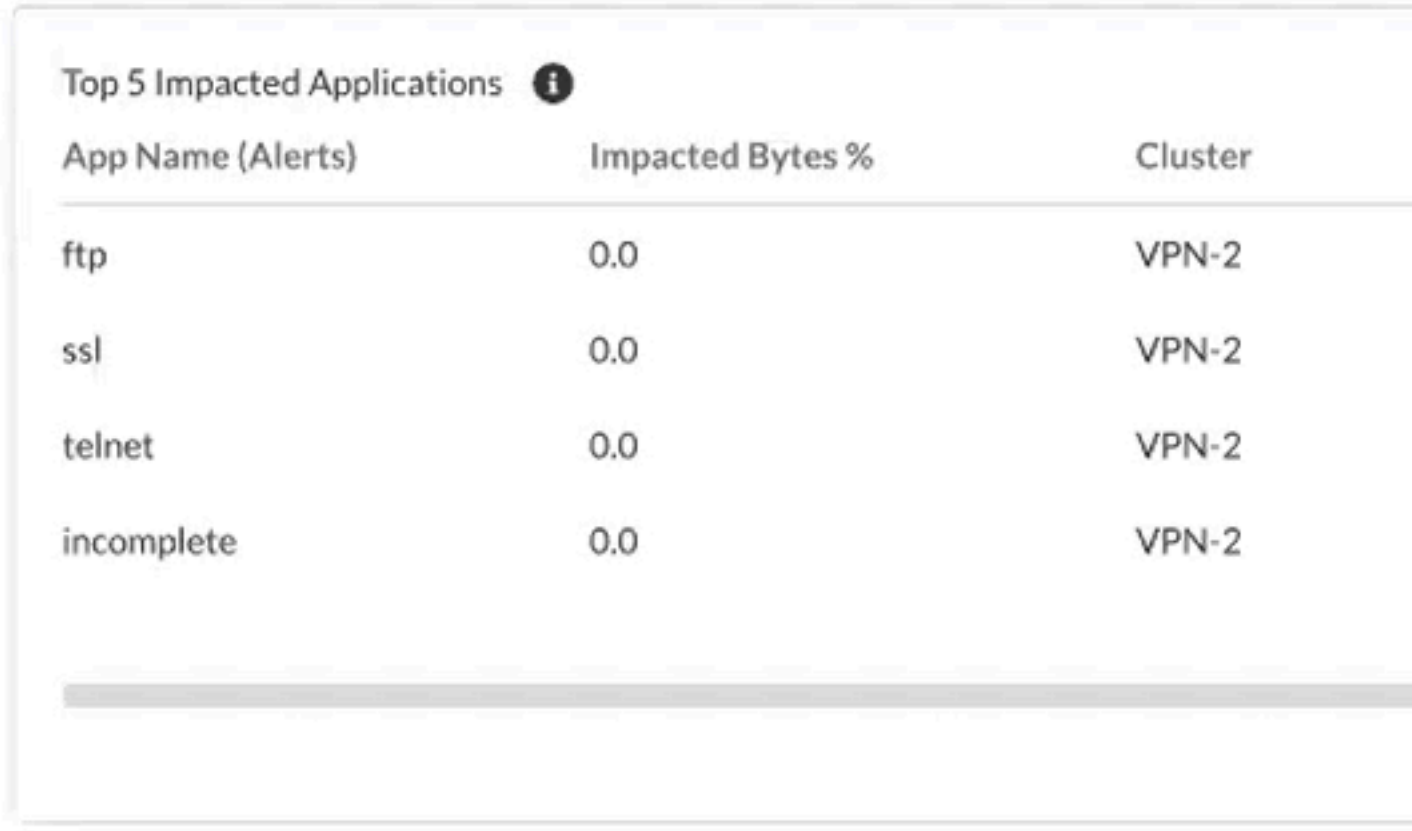


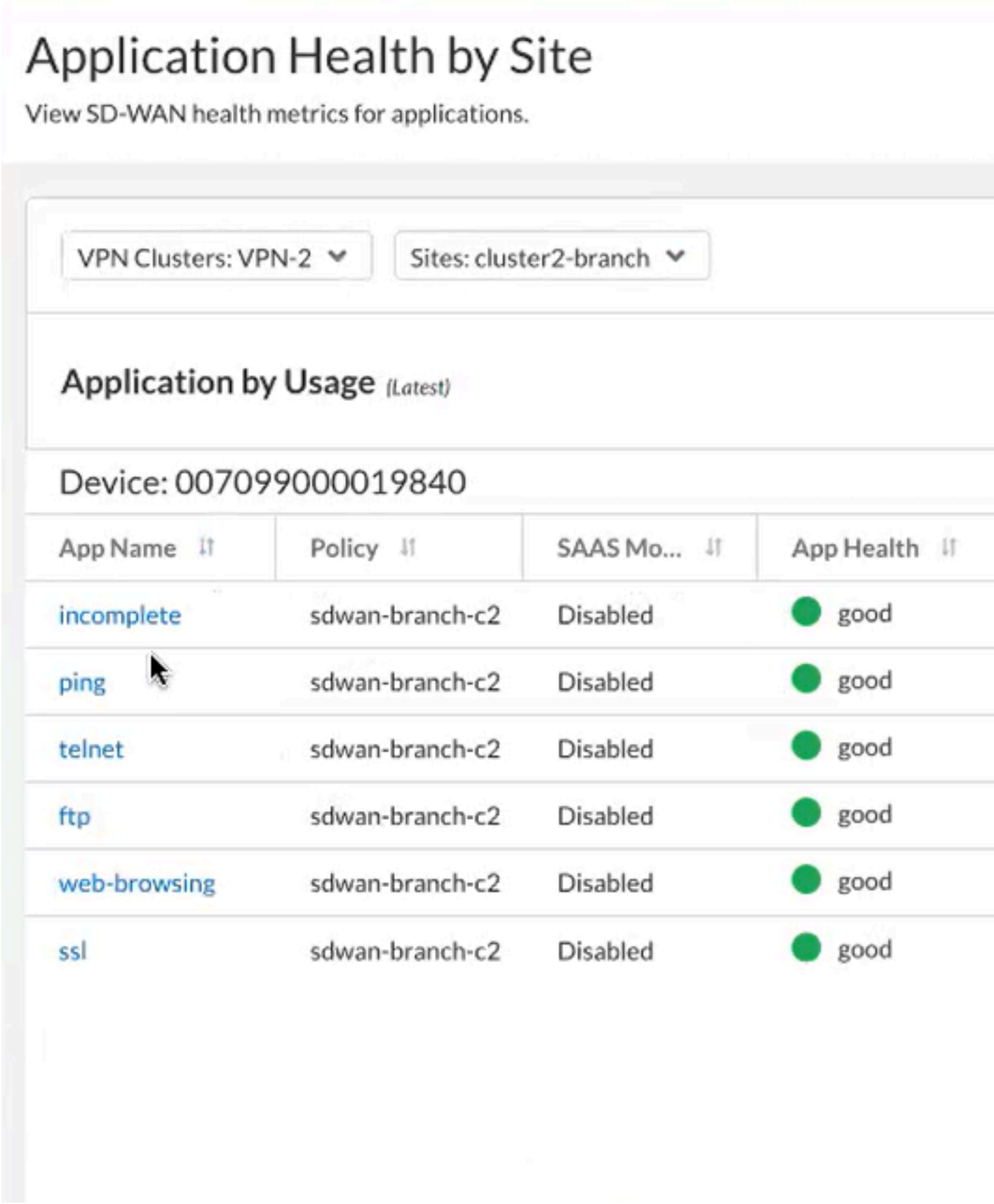
Tableau de bord NGFW SD-WAN : Principales applications impactées

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	☐ AIOps for NGFW Premium ou Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Pour la durée et le cluster VPN sélectionnés, Strata Cloud Manager affiche les 5 principales applications impactées en fonction du calcul du pourcentage de trafic touché sur le total des bytes (octets). Plus le pourcentage calculé est élevé, plus l'impact sur l'application est important.



Cliquez sur **Afficher davantage** pour vérifier toutes les applications concernées.



De plus, cliquez sur une application pour afficher ses détails, notamment sur le trafic et les liens utilisés. Vous pouvez également cliquer sur un lien utilisé pour afficher ses détails.

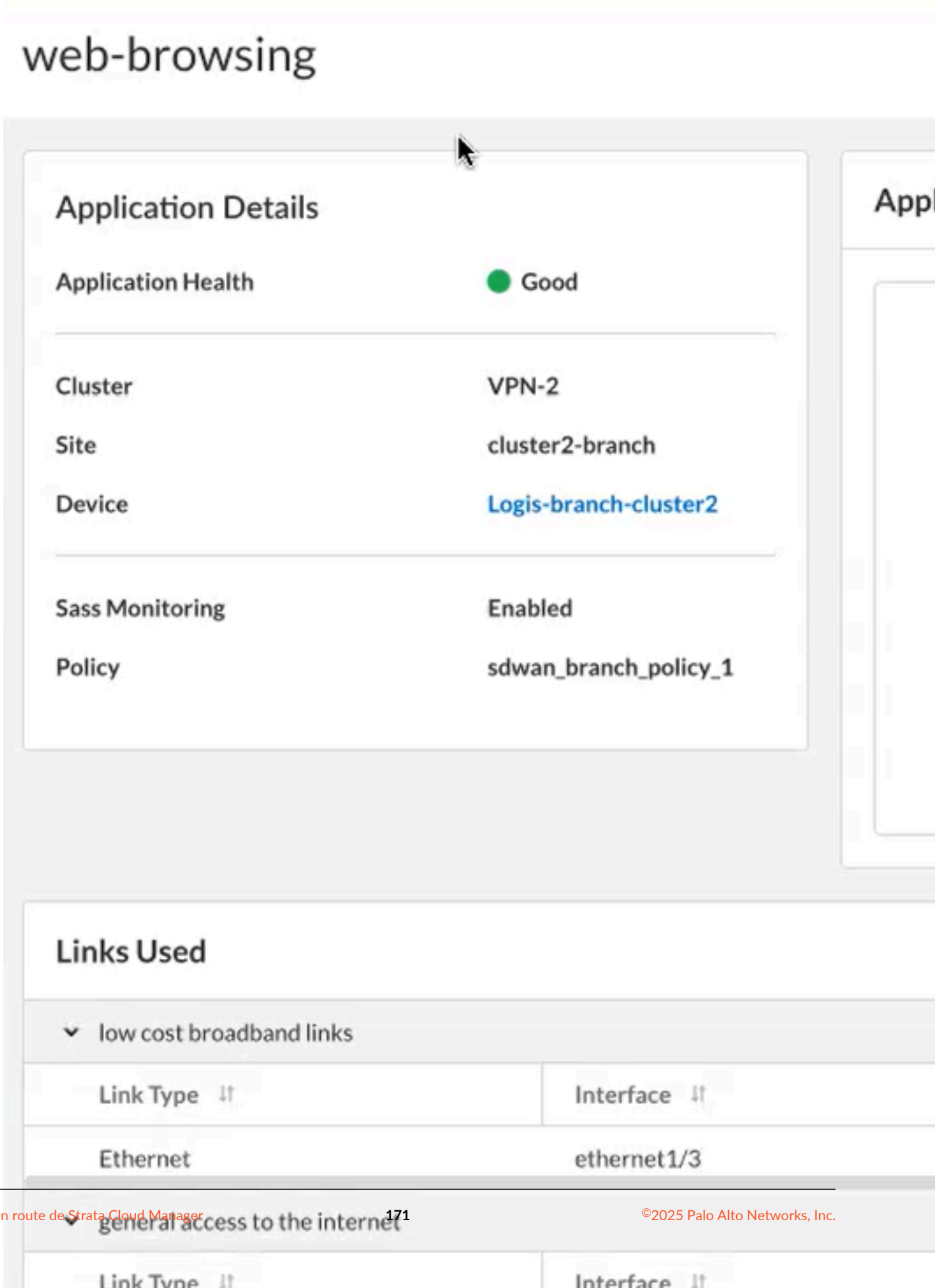


Tableau de bord NGFW SD-WAN : Applications touchées

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	☐ AIOps for NGFW Premium ou Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Le graphique indique une tendance montrant les applications impactées au cours des dernières 24 heures. Passez votre curseur sur la ligne de tendance pour voir les applications impactées à un moment précis.
- Cliquez sur **Voir les alertes** pour afficher les alertes associées qui sont déclenchées en raison des applications impactées.

Tableau de bord NGFW SD-WAN : État du lien

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	☐ AIOps for NGFW Premium ou Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Le nombre total de liens pour la durée et le cluster VPN sélectionnés.
- Le nombre de liens classés comme Critiques, Avertisseurs et Bons.
- Cliquez sur le lien numérique correspondant à **Critique** pour afficher les alertes déclenchées en raison des performances de la liaison SD-WAN.

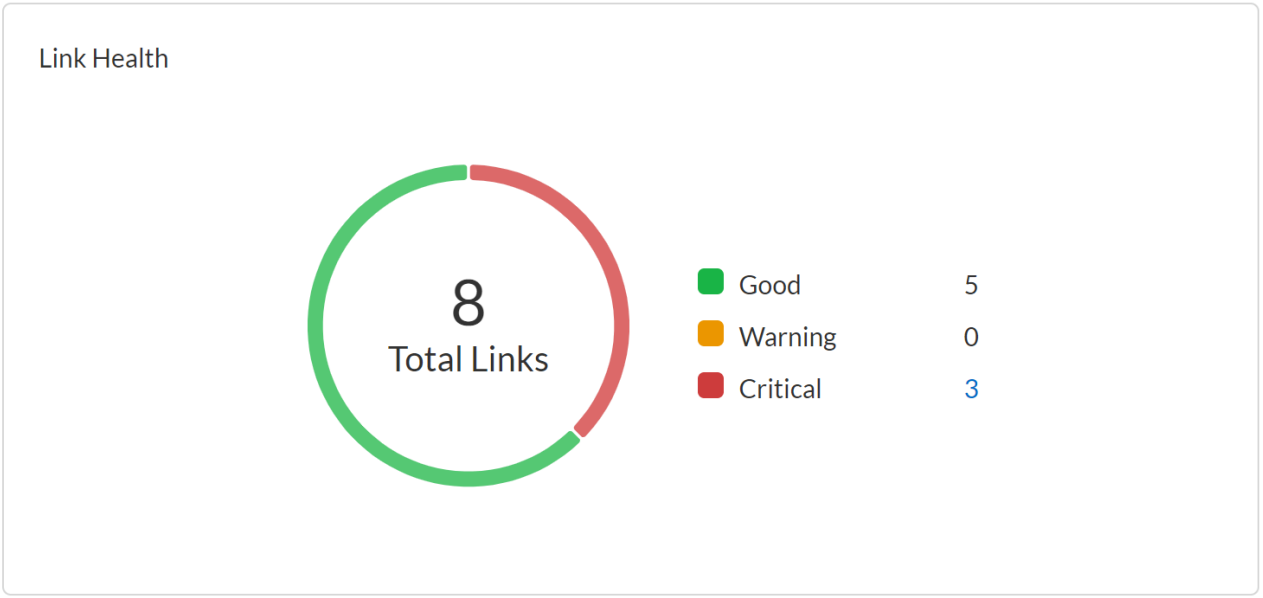
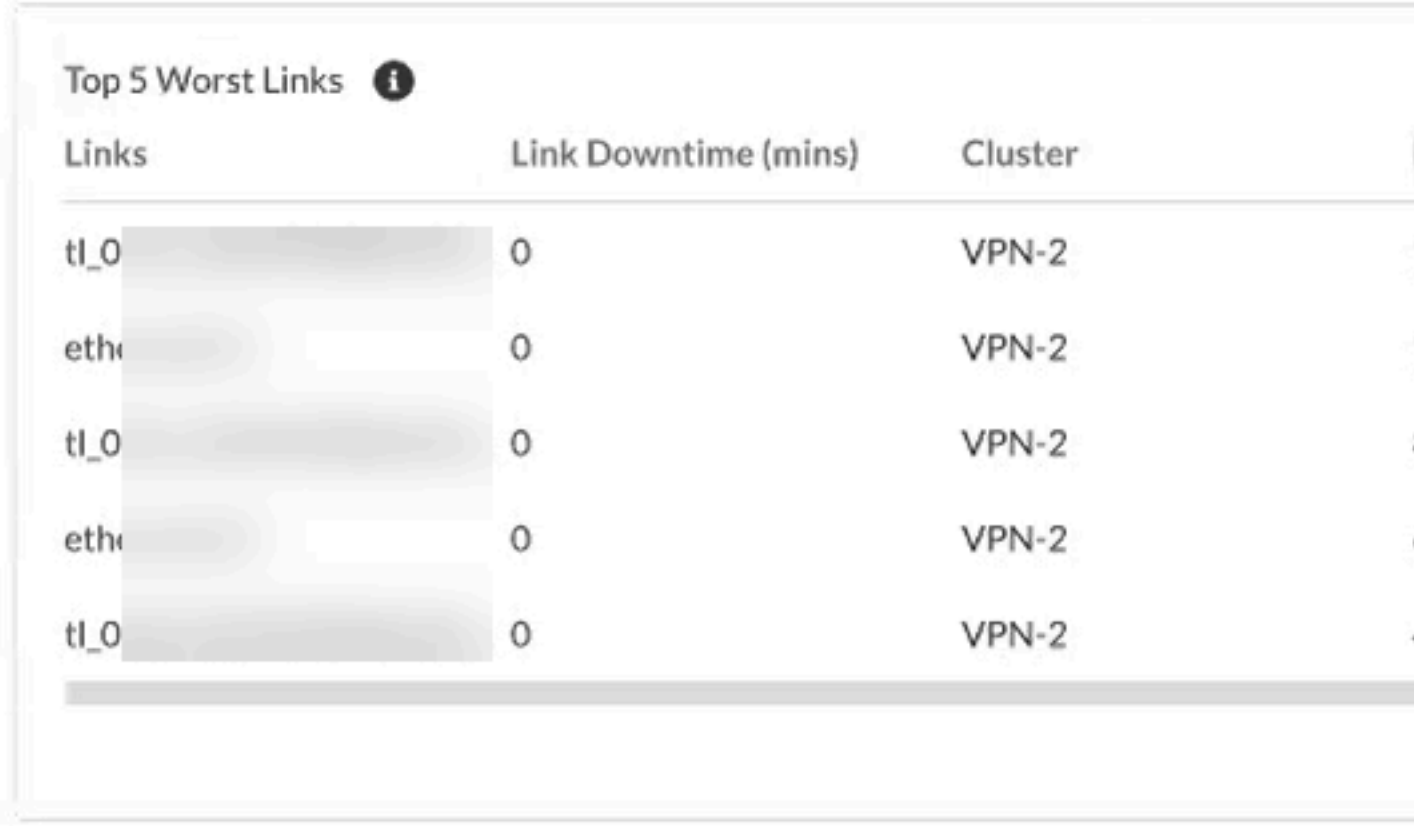


Tableau de bord NGFW SD-WAN : Principaux liens défectueux

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ AIOps for NGFW Premium ou Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Pour la durée et le cluster VPN sélectionnés, Strata Cloud Manager affiche les 5 liens les plus défectueux en fonction du calcul de la moyenne des métriques de l'interface (Interruption du tunnel, Latence, Gigue et Perte de paquets). Les liens sont classés en fonction de la priorité de l'interruption du tunnel, de la latence, de la perte de paquets et de la gigue. Plus la moyenne calculée est élevée, moins la qualité des liens est bonne.



Vous pouvez cliquer sur **Afficher davantage**pour vérifier tous les liens concernés.

En outre, cliquez sur un lien pour afficher ses détails, notamment les graphiques basés sur la performance des liens.

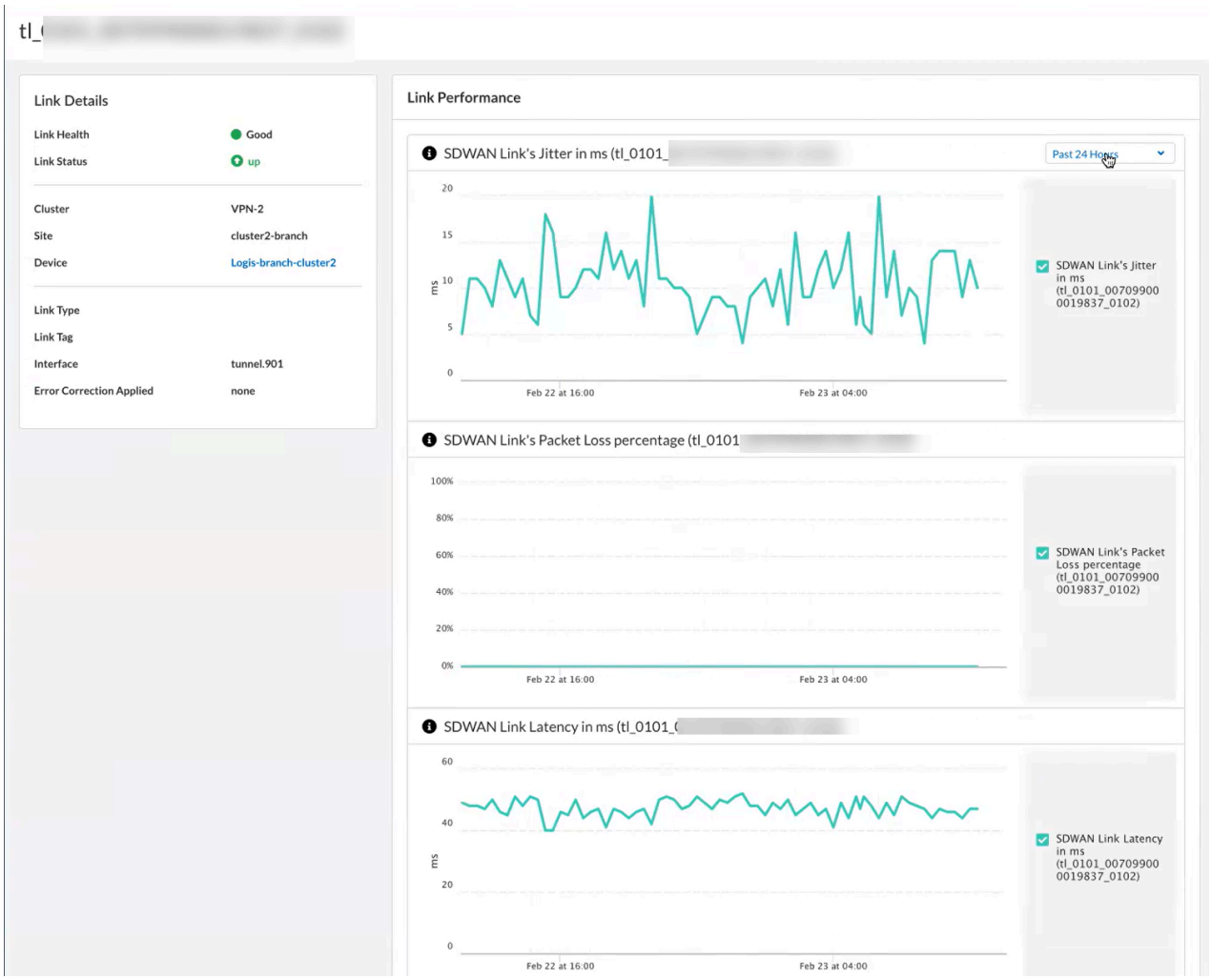


Tableau de bord NGFW SD-WAN : Mauvais liens

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ AIOps for NGFW Premium ou Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Le graphique indique la tendance des liens défectueux détectés au cours des dernières 24 heures. Passez votre curseur sur la ligne de tendance pour visualiser les liens défectueux à un moment précis.
- Cliquez sur **Voir les alertes** pour afficher les alertes associées qui sont déclenchées en raison des liens défectueux.

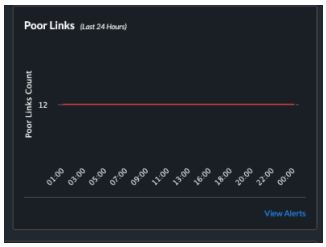
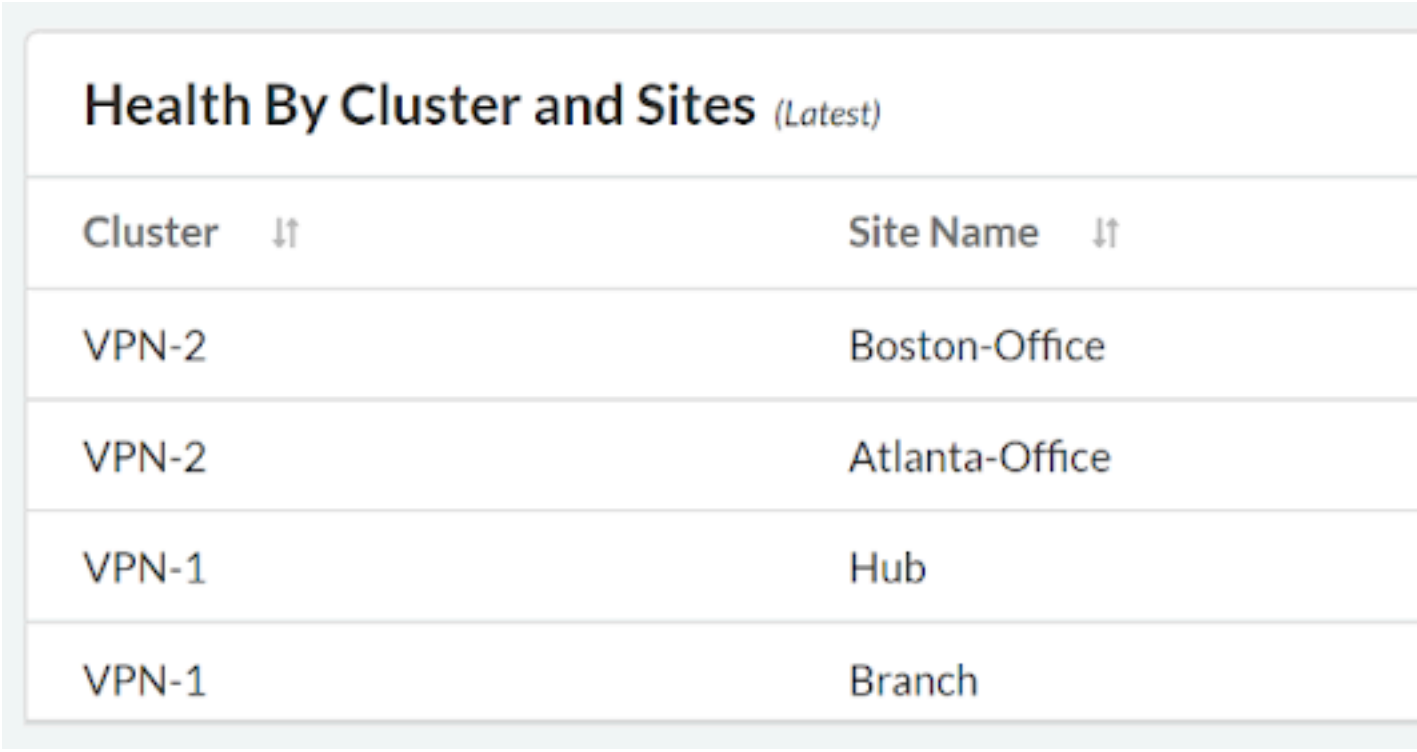


Tableau de bord NGFW SD-WAN : Santé par cluster et par site

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ AIOps for NGFW Premium ou Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Consultez le nombre de liens, leur état et les applications impactées pour chaque site.



Cliquez sur les liens numériques sous ces colonnes pour afficher des détails à leur sujet.

Tableau de bord : Prisma SD-WAN

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma SD-WAN	❑ Licence Prisma SD-WAN Les autres licences et prérequis nécessaires à la visibilité sont : ❑ https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/dashboards pour déverrouiller certains widgets dans le tableau de bord ❑ WAN Clarity pour l'analyse prédictive ❑ rôle qui a l'autorisation d'afficher le tableau de bord → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Que vous indique ce tableau de bord ?

Le Tableau de bord vous présente une vue graphique de haut niveau des métriques du réseau, des périphériques et des applications de Prisma SD-WAN. De plus, il vous indique :

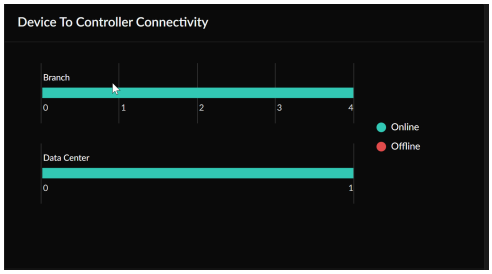
- L'état de la connectivité des périphériques de vos succursales et centres de données vers le contrôleur.
- Les données d'applications des périphériques pour votre trafic entrant et sortant.
- Informations et rapports de base sur le réseau pour tous les sites de succursales d'un locataire au cours de la semaine écoulée.
- Informations sur les principaux sites de succursales et de centres de données en fonction du nombre d'incidents générés.
- Les mesures de la qualité des liens sur l'ensemble de vos sites, comme le score MOS, la perte de paquets, la gigue et la latence.
- S'appuyer sur la capacité à prévoir au niveau d'un site en fonction des informations recueillies au cours des trois à six mois précédents.

Tableau de bord Prisma SD-WAN : Connectivité entre le périphérique et le contrôleur

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma SD-WAN	❑ Licence Prisma SD-WAN

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	Les autres licences et prérequis nécessaires à la visibilité sont : ☐ https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/dashboards pour déverrouiller certains widgets dans le tableau de bord ☐ WAN Clarity pour l'analyse prédictive ☐ rôle qui a l'autorisation d'afficher le tableau de bord → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Le widget de connectivité du périphérique au contrôleur représente le nombre de périphériques ION en ligne et hors ligne connectés au contrôleur Prisma SD-WAN pour une succursale et un centre de données. À l'aide de ce graphique interactif, vous pouvez afficher l'état en ligne ou hors ligne d'un périphérique réclamé pour la succursale et le centre de données correspondants.



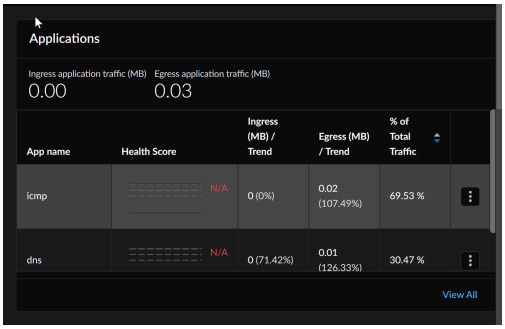
En cliquant sur **Branch (Succursale)** ou **Data Center (Centre de données)** dans le graphique interactif, vous pouvez voir le nom, l'état, la version du logiciel installé, la dernière activité et l'état de redondance des périphériques réclamés et non réclamés.

Tableau de bord Prisma SD-WAN : Applications

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma SD-WAN	☐ Licence Prisma SD-WAN Les autres licences et prérequis nécessaires à la visibilité sont : ☐ https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/dashboards pour déverrouiller certains widgets dans le tableau de bord ☐ WAN Clarity pour l'analyse prédictive

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	❑ rôle qui a l'autorisation d'afficher le tableau de bord → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Le widget Applications affiche des informations sur l'utilisation des applications sur le site pendant la plage de temps sélectionnée. Le trafic total d'entrée et de sortie de l'application pour l'intervalle de temps s'affiche. Les 10 applications les plus importantes en termes de volume de trafic sont affichées avec les autres trafics. Cliquez sur **View All (Afficher tout)**pour voir la distribution de l'état de l'application, la distribution de l'état de l'application TCP dans le temps, les nouveaux flux, l'utilisation de la bande passante, les stats de transaction pour la plage de temps sélectionnée ainsi que les applications supérieures. Le tableau de bord permet d'analyser les performances d'une application et les mesures par site pour la période sélectionnée.



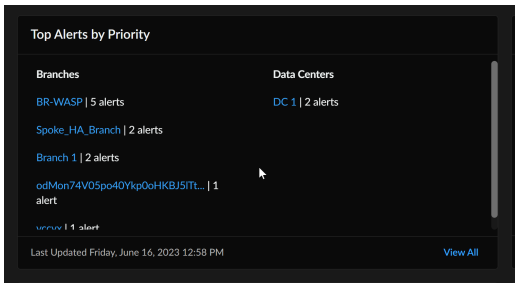
Les mesures de toutes les applications TCP sont initialement affichées, mais il est possible de sélectionner l'une des 10 principales applications TCP pour se concentrer plus précisément sur une application spécifique.

Tableau de bord Prisma SD-WAN : Les principales alertes par priorité

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma SD-WAN	❑ Licence Prisma SD-WAN Les autres licences et prérequis nécessaires à la visibilité sont : ❑ https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/dashboards pour déverrouiller certains widgets dans le tableau de bord ❑ WAN Clarity pour l'analyse prédictive ❑ rôle qui a l'autorisation d'afficher le tableau de bord

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	→ Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Le widget **Principales alertes par priorité** affiche les 5 principales alertes par priorité. Vous pouvez obtenir des informations sur les principaux sites des succursales et des centres de données en fonction du nombre d'alertes générées dans la période sélectionnée. Vous pouvez explorer les informations d'alerte par site pour la plage horaire sélectionnée.



Cliquer sur **View All (Afficher tout)** pour afficher les informations suivantes sur les alertes :

- Lorsque l'alerte a été créée.
- Nom de l'incident.
- L'objet principal visé.
- La sensibilité de l'alerte.
- La qualité de l'alerte.

Cliquez sur les points de suspension pour résoudre l'alerte.

Tableau de bord Prisma SD-WAN : Qualité globale des liens

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma SD-WAN	❑ Licence Prisma SD-WAN Les autres licences et prérequis nécessaires à la visibilité sont : ❑ https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/dashboards pour déverrouiller certains widgets dans le tableau de bord ❑ WAN Clarity pour l'analyse prédictive ❑ rôle qui a l'autorisation d'afficher le tableau de bord → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	dépendent de la ou des licences que vous utilisez.

Le widget **Qualité globale des liens** fournit un aperçu global de l'état actuel des liens pour tous vos sites et en ce qui la plage horaire sélectionnée. Vous pouvez explorer pour consulter les performances des liens, la perte de flux des liens, la gigue des liens et la latence des liens, ce qui permet d'analyser les informations que vous souhaitez afficher plus en détail dans les Mesures de qualité des liens du tableau de bord.

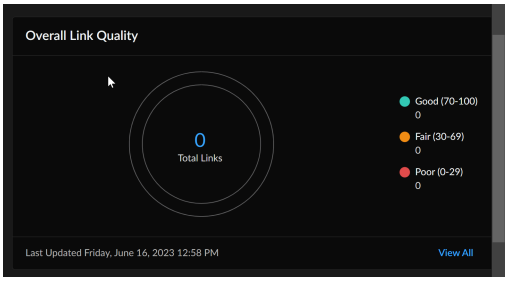
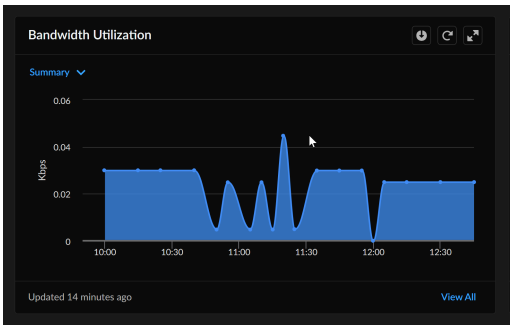


Tableau de bord Prisma SD-WAN : Utilisation de la bande passante

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma SD-WAN	☐ Licence Prisma SD-WAN Les autres licences et prérequis nécessaires à la visibilité sont : ☐ https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/dashboards pour déverrouiller certains widgets dans le tableau de bord ☐ WAN Clarity pour l'analyse prédictive ☐ rôle qui a l'autorisation d'afficher le tableau de bord → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Le widget Utilisation de la bande passante affiche la quantité de bande passante utilisée sur un circuit dans un réseau. Cette représentation visuelle indique les pointes de bande passante, la bande passante totale consommée par un site spécifique et l'application. Elle indique si le téléchargement se fait dans la direction de l'entrée, de la sortie ou dans les deux directions.



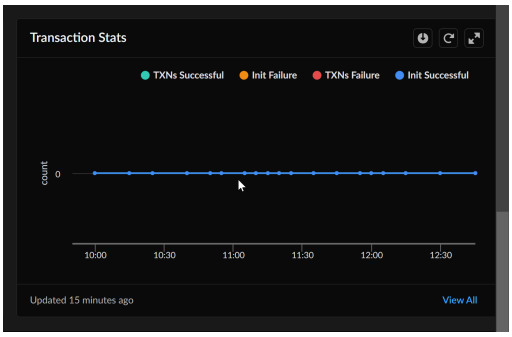
Déplacez votre curseur dans le graphique **Bandwidth Utilization (Utilisation de la bande passante)** pour obtenir une vue plus détaillée de l'utilisation de la bande passante avec une application ou un horodatage. En règle générale, les applis sont répertoriées par ordre d'utilisation de leur bande passante. Le graphique affiche la bande passante utilisée au fil du temps. La vue de 1 h fournit des données granulaires par minute, et l'image 1D présente des données toutes les 5 minutes. Les données du graphique 1D sont en moyenne supérieures à 5 minutes pour chaque échantillon. Si l'utilisation se maintient au-delà de 5 minutes, vous pouvez voir le pic d'utilisation correspondant sur les deux graphiques.

Vous pouvez utiliser l'option de téléchargement à partir du widget pour télécharger le graphique d'utilisation de la bande passante au format PDF, CSV, XLS ou PNG.

Tableau de bord Prisma SD-WAN : Statistiques de transaction

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma SD-WAN	❑ Licence Prisma SD-WAN Les autres licences et prérequis nécessaires à la visibilité sont : ❑ https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/dashboards pour déverrouiller certains widgets dans le tableau de bord ❑ WAN Clarity pour l'analyse prédictive ❑ rôle qui a l'autorisation d'afficher le tableau de bord → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Le widget Statistiques de transaction fournit des statistiques de transaction sur les flux TCP, y compris les succès et échecs d'initiation/transaction pour une application spécifique ou toutes les applications, un chemin particulier ou tous les chemins, et tous les événements relatifs à l'état. Il mesure la performance et la disponibilité des réseaux et des applications qui s'exécutent sur les circuits du réseau. En ce qui concerne chaque requête sur un chemin donné, Prisma SD-WAN surveille, en temps réel, les taux d'erreur des transactions d'initiation et de transfert de données.



À partir du graphique Statistiques de transaction, affichez la liste des applis par leur utilisation de la bande passante ou par chemin. Vous pouvez filtrer les transactions réussies pour obtenir une vue précise des statistiques d'échec des transactions. Le graphique affiche le nombre de transactions réussies ou échouées pour les catégories suivantes :

- **Init Sucessful (Initialisation réussie)** : Réussite de la connexion en trois étapes.
- **TXNs Sucessful (TXNs réussi)** : Transfert de données réussi après l'achèvement de l'établissement de la connexion en trois étapes.
- **Init Failure (Défaillance initiale)** : Échec de la connexion en trois étapes. Les raisons de l'échec peuvent inclure une mauvaise configuration du pare-feu, un problème au niveau du serveur d'application, une mauvaise configuration de la liste de Network Access Control (contrôle d'accès au réseau - NAC) ou un problème au niveau du fournisseur du réseau WAN.
- **TXNs Failure (Échec du TXN)** : Échec du transfert de données après l'achèvement de la connexion en trois étapes. Les raisons de l'échec peuvent être un pare-feu mal configuré, un problème de serveur d'application, une liste de Network Access Control (contrôle d'accès au réseau - NAC) mal configurée ou un problème de fournisseur de réseau WAN.

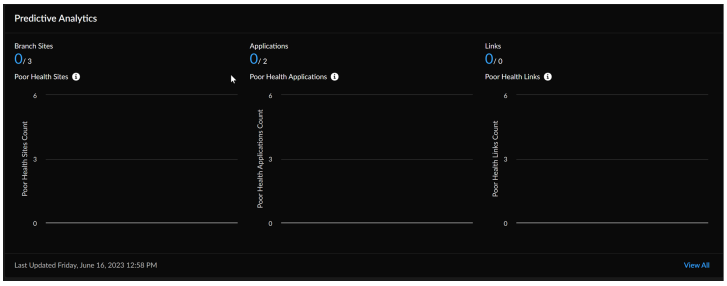
Vous pouvez utiliser l'option de téléchargement à partir du widget pour télécharger le graphique d'utilisation de la bande passante au format PDF, CSV, XLS ou PNG.

Tableau de bord Prisma SD-WAN : Analyse prévisionnelle

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma SD-WAN	❑ Licence Prisma SD-WAN Les autres licences et prérequis nécessaires à la visibilité sont : ❑ https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/dashboards pour déverrouiller certains widgets dans le tableau de bord ❑ WAN Clarity pour l'analyse prédictive ❑ rôle qui a l'autorisation d'afficher le tableau de bord → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	dépendent de la ou des licences que vous utilisez.

Le widget de l'Analyse prévisionnelle fournit des informations sur l'état des sites et des applications et une surveillance proactive pour identifier les problèmes critiques et les résoudre plus rapidement, améliorant ainsi les niveaux de service. Il identifie les sites, les liens et les applications critiques et les classe dans la catégorie : **Good (Bon)**, **Fair (Satisfaisant)**et **Poor (Médiocre)** au niveau du locataire, en fonction des scores d'intégrité de l'IA/ML. Le widget consiste à prévoir l'utilisation des ressources au niveau du site de la succursale sur la base des informations recueillies au cours des trois à six mois précédents.



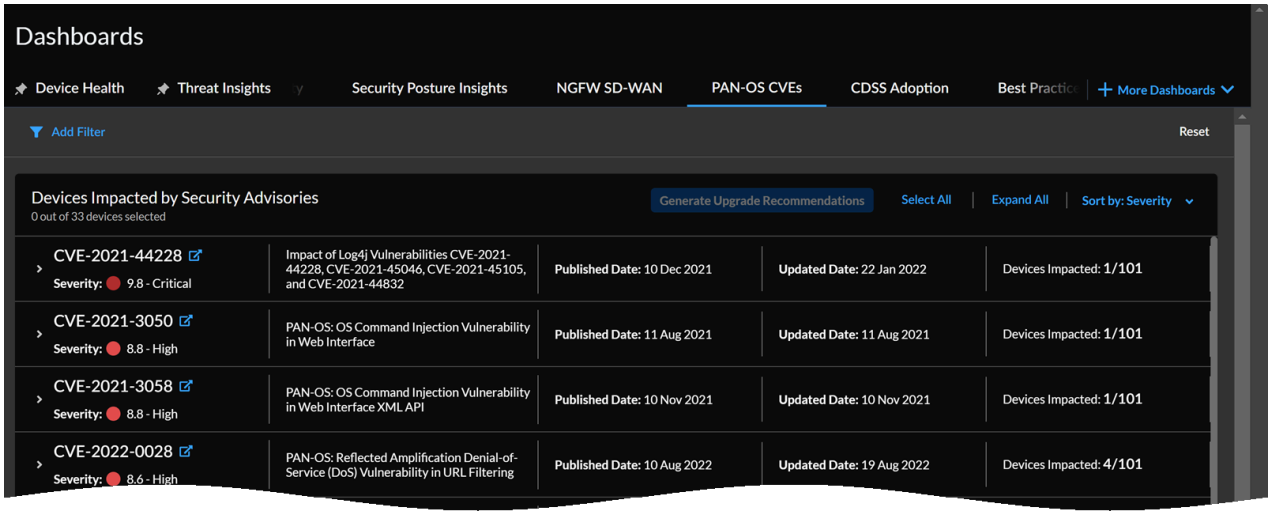
L'intervalle de temps par défaut pour consulter les mesures est de trois heures ; toutefois, vous pouvez l'ajuster à des périodes plus courtes ou plus longues en fonction de l'étendue des informations souhaitées. Découvrez les 10 principaux sites dont l'utilisation de la bande passante a augmenté au cours des 28 jours précédents ; vous pouvez afficher les prévisions à sept jours lorsque les prévisions à 28 jours ne sont pas disponibles et prédire l'utilisation future de la capacité de la succursale.

Cliquer sur **View All (Afficher tout)** pour obtenir des informations sur les sites des succursales, les applications, les liens, le réseau, les principaux sites dont le volume de trafic a augmenté au cours des 30 derniers jours, ainsi que sur les prévisions de capacité et les défaillances des sites.

Tableau de bord : CVE PAN-OS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium ou Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Dashboards > More Dashboards > PAN-OS CVEs (Tableaux de bord > Plus de tableaux de bord > CVE PAN-OS)** pour commencer.



Que vous indique ce tableau de bord ?

Le tableau de bord affiche les données agrégées pour tous les pare-feu et Panorama intégrés à votre locataire et qui envoient également des données de télémétrie. En outre, il affiche les données de télémétrie de la base de données NGFW PSIRT relatives aux CVE.

Le tableau de bord **PAN-OS CVE** vous indique le nombre de périphériques impactés par une vulnérabilité spécifique en fonction des fonctionnalités qui ont été activées sur les périphériques. Strata Cloud Manager analyse les fonctionnalités qui ont été activées pour déterminer les périphériques impactés par le CVE.

Une fois que vous avez compris les vulnérabilités des périphériques concernés, vous pouvez planifier votre mise à niveau à l'aide de la fonctionnalité Recommandations de mise à niveau. Développez les CVE et sélectionnez les pare-feu que vous souhaitez mettre à niveau pour corriger les vulnérabilités, puis cliquez sur **Generate Upgrade Recommendations (Générer des**

recommandations de mise à niveau). Vous êtes redirigé vers NGFW - Recommandations de mise à niveau pour afficher le rapport généré.

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

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

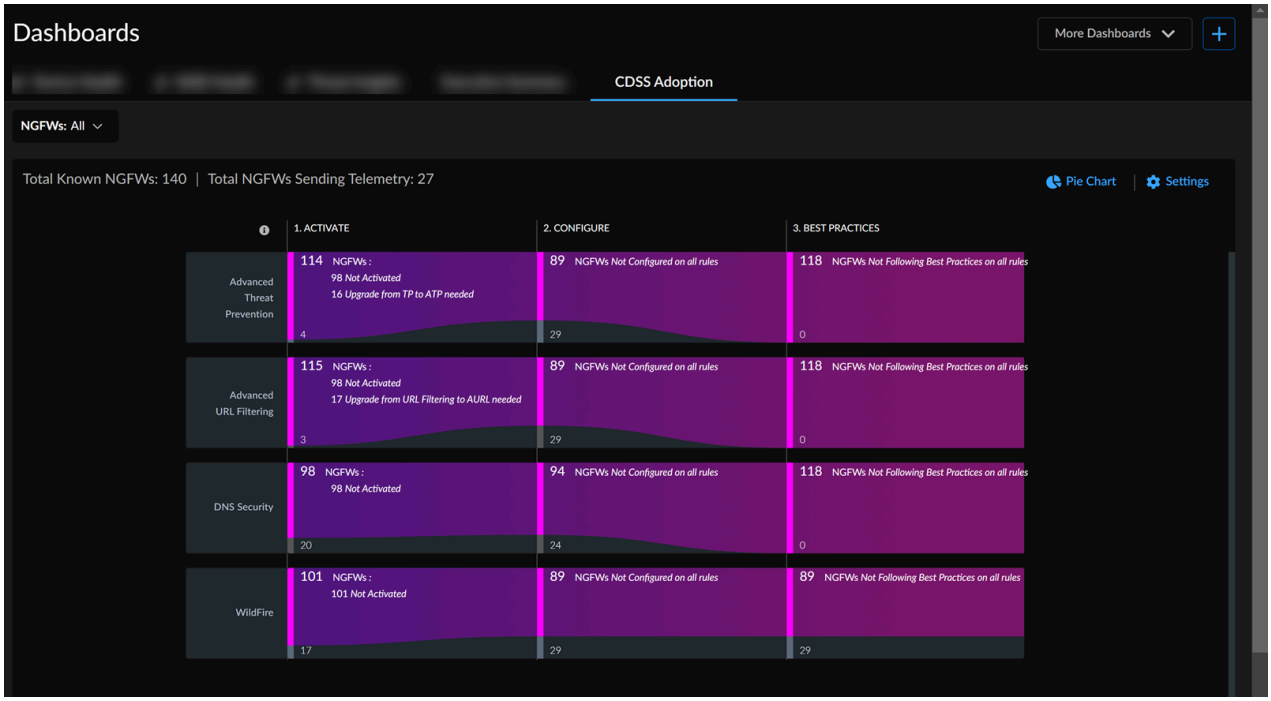
Ce tableau de bord vous permet de :

- Décider quels périphériques mettre à niveau pour atténuer une vulnérabilité.
- Afficher les détails sur un périphérique impacté, tels que le nom de l'hôte, le modèle, le numéro de série, la version du logiciel et la dernière mise à jour de télémétrie en développant un CVE.
- Filtrer les CVE et les trier davantage par **Severity (Gravité)** ou **Devices Impacted (Appareils impactés)**.
- Consultez l'avis associé à un CVE en cliquant dessus.

Tableau de bord : Adoption de CDSS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium ou Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Dashboards (Tableaux de bord)** > **Posture (Posture)** > **CDSS Adoption (Adoption de CDSS)** pour commencer.



Que vous indique ce tableau de bord ?

- *Le tableau de bord affiche les données agrégées de tous les pare-feux intégrés à votre locataire et envoie également des données de télémétrie.*
- *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.*

Le tableau de bord **CDSS Adoption (Adoption de CDSS)** affiche les abonnements recommandés aux services de sécurité fournis par le cloud (CDSS) 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.

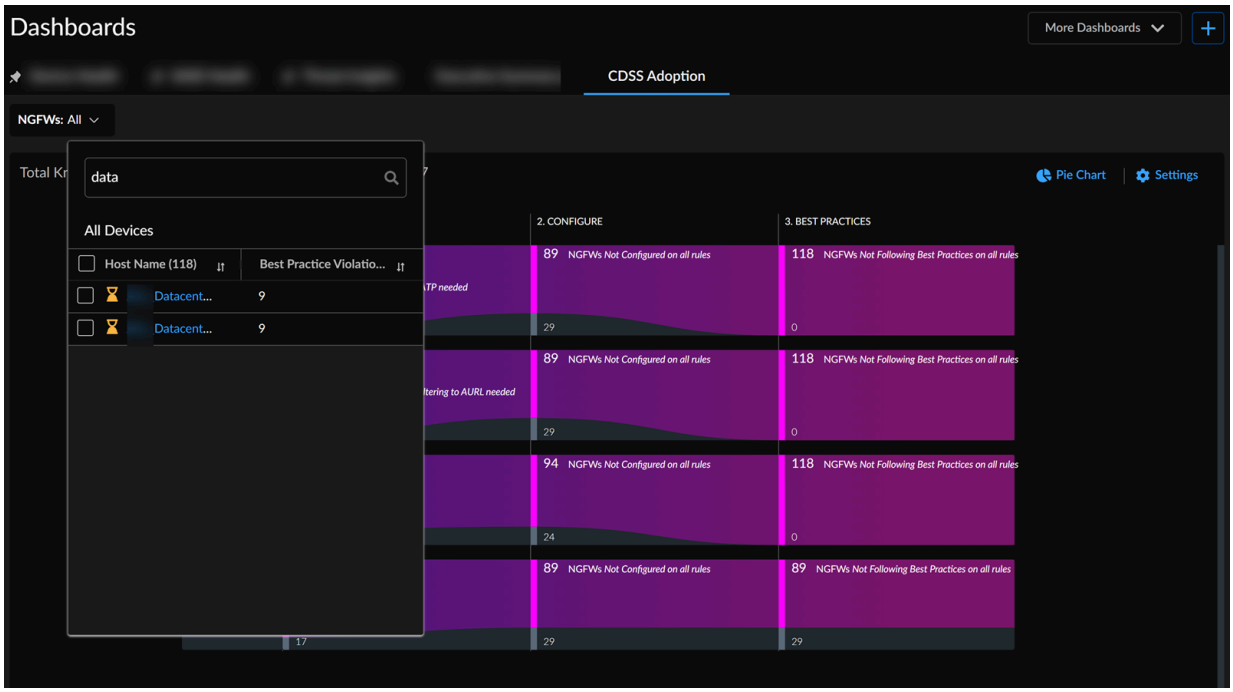
La vidéo suivante montre comment surveiller les abonnements de sécurité à l'aide du tableau de bord **CDSS Adoption (Adoption de CDSS)** :

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

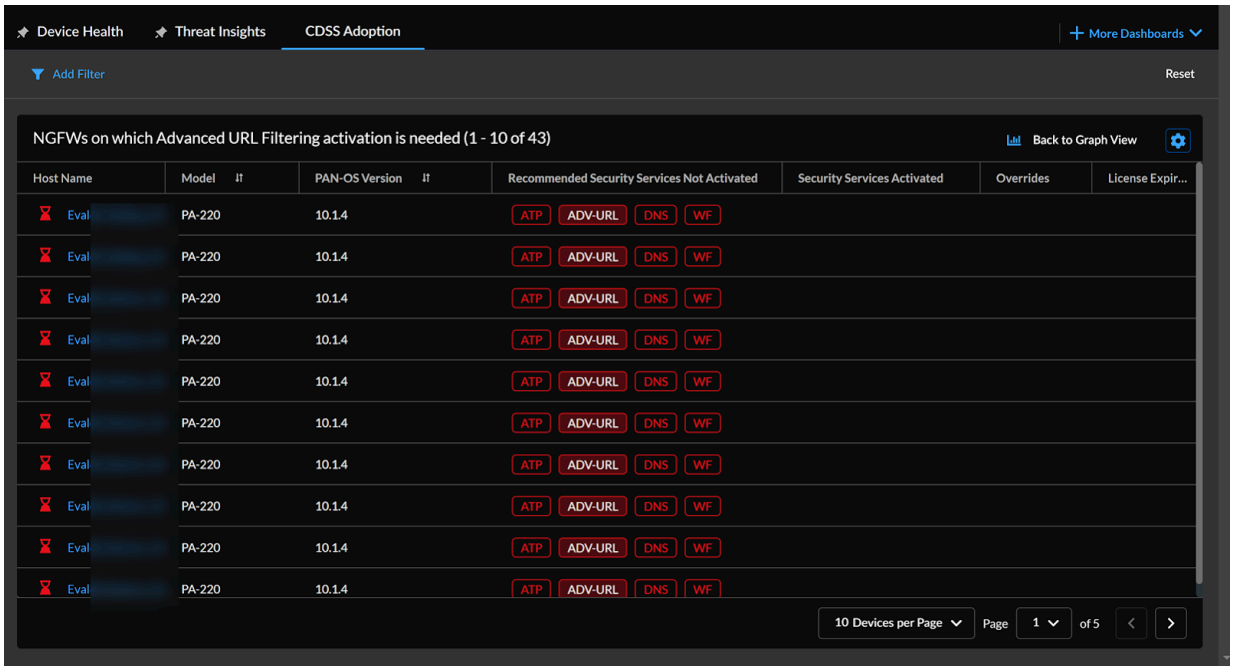
Ce tableau de bord vous aide dans les domaines suivants :

- En haut de la page Vue d'ensemble, vous pouvez afficher le nombre total de NGFW connus et le nombre de NGFW envoyant des données de télémétrie dans votre instance AIOps pour NGFW. L'adoption de la CDSS implique de progresser 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. Pour utiliser une licence d'abonnement de sécurité dans un périphérique, vous devez l'activer, puis configurer le service ou la fonctionnalité en conséquence.

  Pour se concentrer sur les données relatives aux services de sécurité d'un NGFW spécifique, filtrez le graphique en fonction de ce dernier. Vous pouvez également afficher les violations des meilleures pratiques pour un périphérique dans cette liste déroulante.

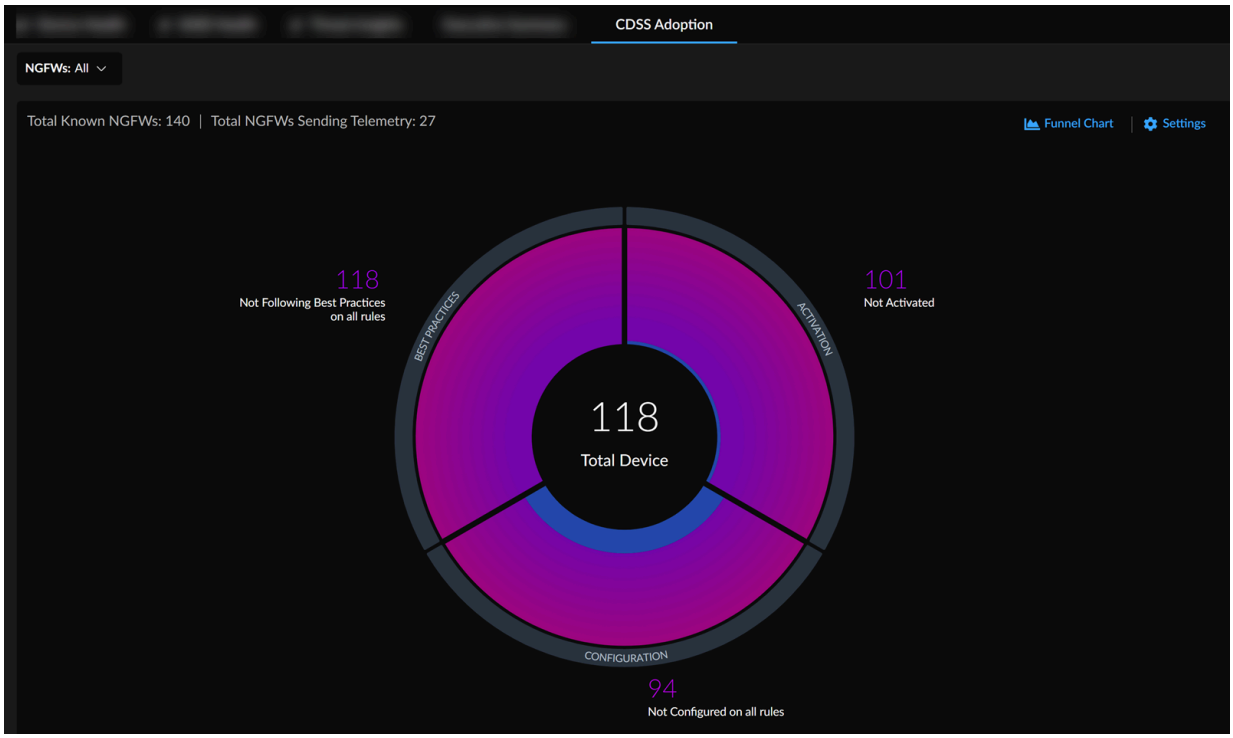


- Vous pouvez cliquer sur l'une des valeurs sous **ACTIVATE (ACTIVER)**, **CONFIGURE (CONFIGURER)**ou **BEST PRACTICES (MEILLEURES PRATIQUES)** pour afficher les détails sous forme de tableau.

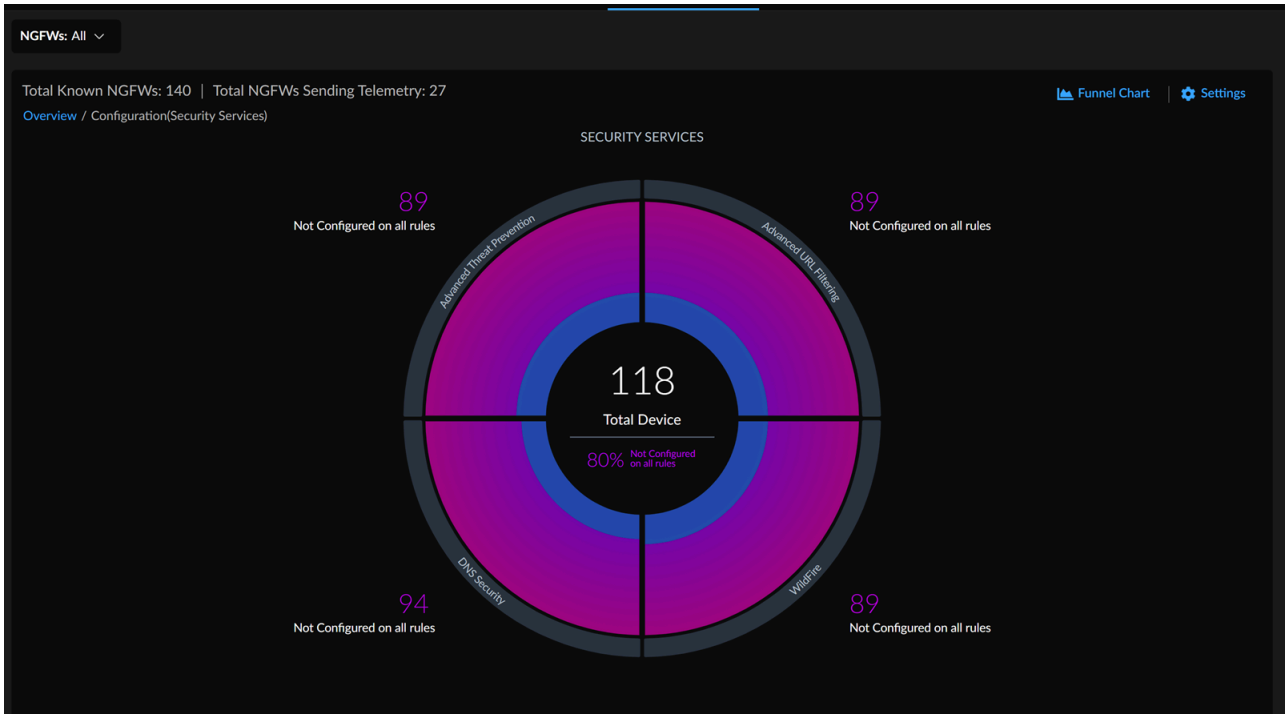


Dans cet exemple, AIOps pour NGFW recommande l'activation du filtrage avancé d'URL (ADV-URL) ainsi que des services de sécurité de Protection contre les menaces avancées (ATP), DNS (Domain Name System) et WildFire (WF) pour les NGFW. Vous pouvez cliquer sur **Back to Graph View (Retour à la vue graphique)** pour accéder à la page Vue d'ensemble.

- Vous pouvez également afficher les mêmes données de posture de sécurité dans un format de graphique à secteurs. Cliquez sur l'icône du graphique circulaire pour afficher les informations sur les services de sécurité recommandés dans un format de graphique circulaire.



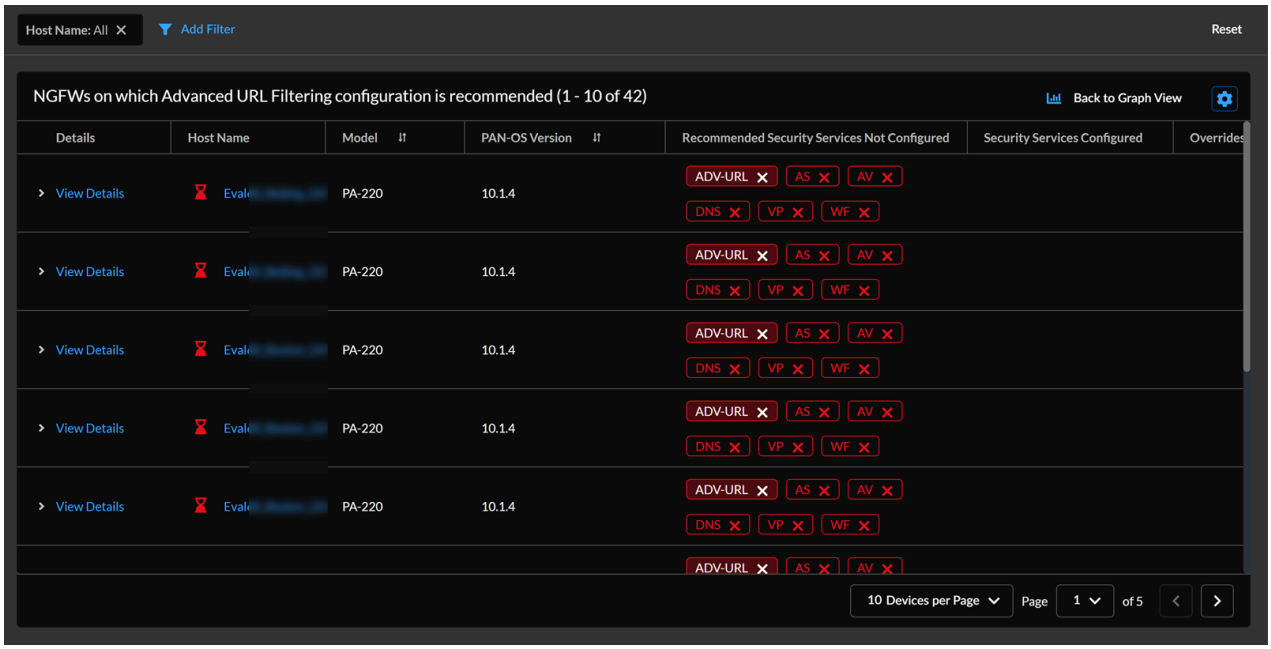
- Vous pouvez cliquer sur les sections du graphique circulaire pour afficher les informations sur le service de sécurité individuel.



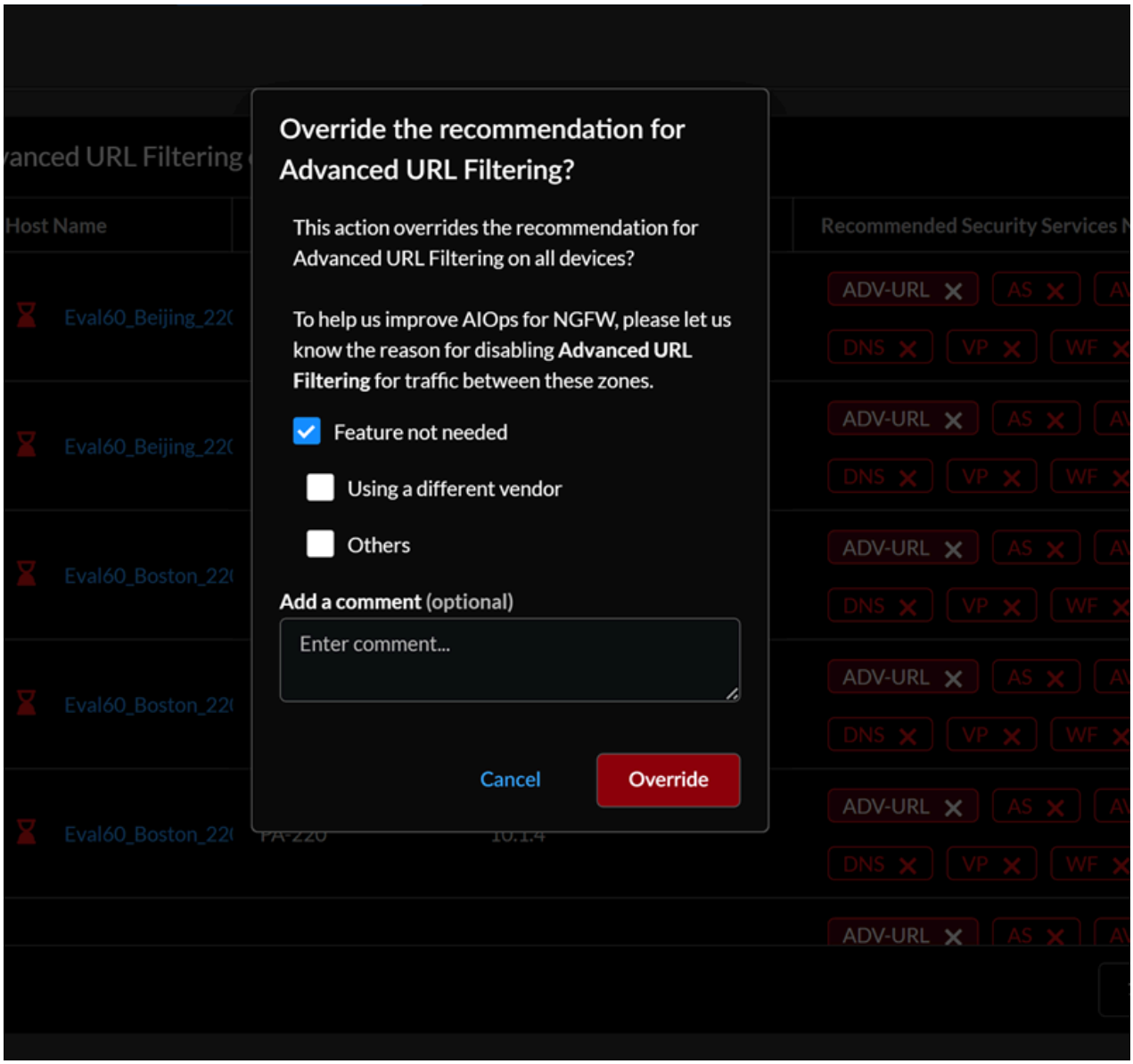
Dans cet exemple, pour afficher le NGFW où la sécurité DNS n'est pas configurée, vous pouvez soit cliquer sur la valeur au-dessus de l'icône **Sécurité DNS** d'un graphique circulaire ou cliquez sur l'icône **Sécurité DNS** d'un graphique circulaire.

Remplacer le service de sécurité recommandé

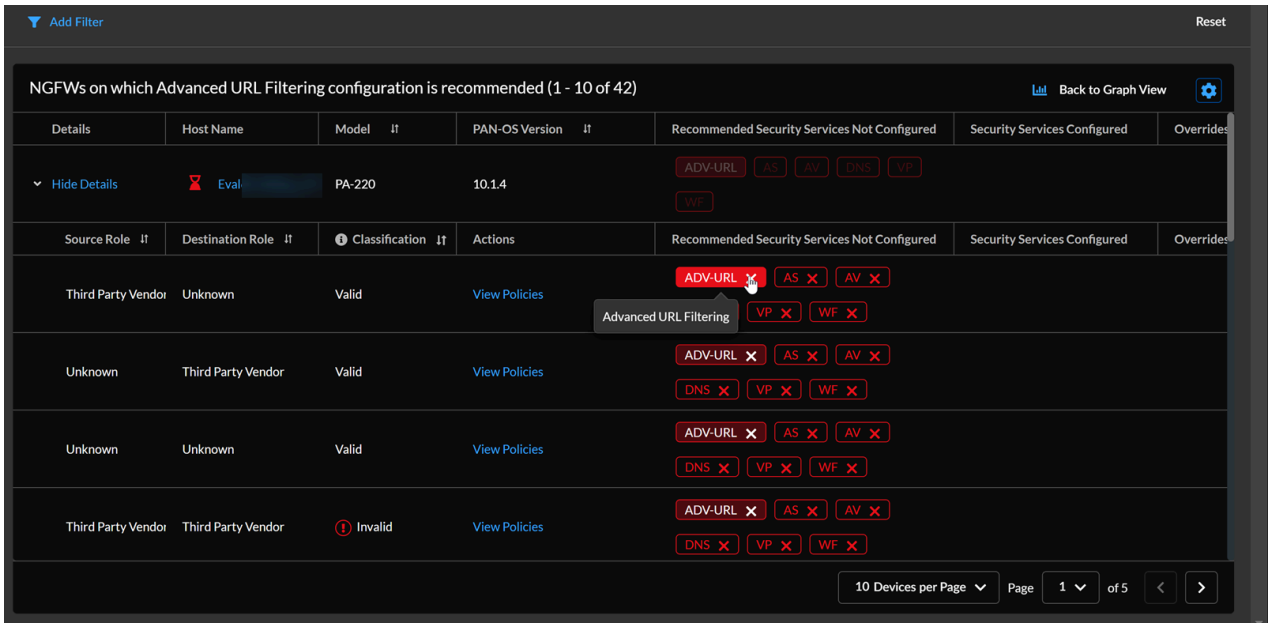
Si vous n'avez pas besoin d'un service de sécurité recommandé pour une raison quelconque, vous pouvez le remplacer. Cliquez sur une valeur sous **CONFIGURE (CONFIGURER)** Pour afficher les détails sous forme de tableau, vous pouvez remplacer le service de sécurité recommandé.



Dans cet exemple, AIOps pour NGFW recommande la configuration du filtrage avancé d'URL (ADV-URL) ainsi que d'autres services de sécurité pour un appareil. Vous pouvez annuler le service de sécurité ADV-URL pour le périphérique NGFW et toutes les zones qui s'y trouvent.

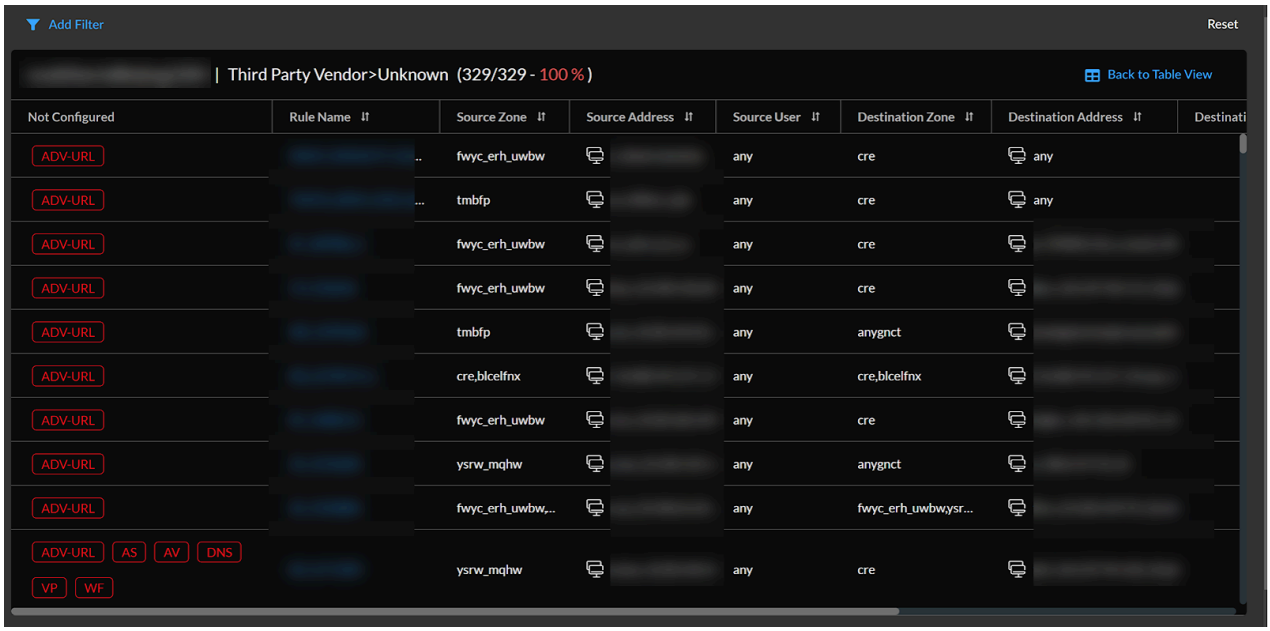


Vous pouvez également remplacer le service de sécurité recommandé au niveau de la zone. **View Details (Afficher les détails)** pour qu'un pare-feu de nouvelle génération affiche les rôles source et de destination, les stratégies et les services de sécurité recommandés.



Dans cet exemple, vous pouvez remplacer l'icône **ADV-URL (URL de l'ADV)** pour le rôle source en tant que **Third Party Vendor (Fournisseur tiers)** et le rôle de destination en tant que **Unknown (Inconnu)**. Vous pouvez également restaurer la recommandation remplacée en cliquant sur le service de sécurité sous la colonne **Overrides (Remplacer)**.

Vous pouvez **View Policies (Afficher les politiques** associées à des rôles. Sélectionnez une règle pour afficher ses détails sans avoir à quitter l'appli.



Cliquez sur **Back to Table View (Retour à la vue tableau)** pour afficher les services de sécurité sous forme de tableau.

Tableau de bord : Adoptions de fonctionnalité

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium ou Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Cliquez sur **Dashboards (Tableaux de bord)** > **Feature Adoption (Adoption des fonctionnalités)** pour commencer.

Que vous indique ce tableau de bord ?

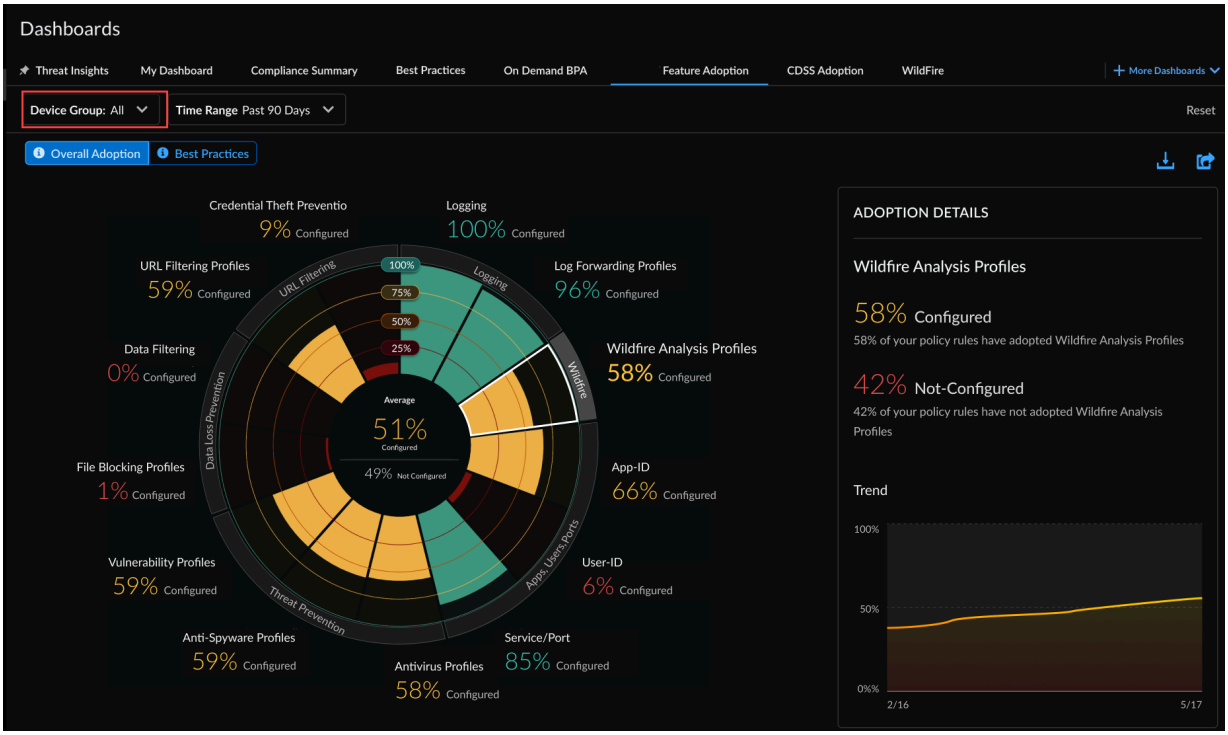
Le tableau de bord affiche les données agrégées de tous les pare-feux intégrés à votre locataire et envoie également des données de télémétrie.

Le tableau de bord **Feature Adoption (Adoption des fonctionnalités)** vous indique les fonctionnalités de sécurité que vous utilisez dans votre déploiement et vous pouvez l'utiliser pour identifier les lacunes en matière d'adoption. 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.

Comment utiliser ce tableau de bord

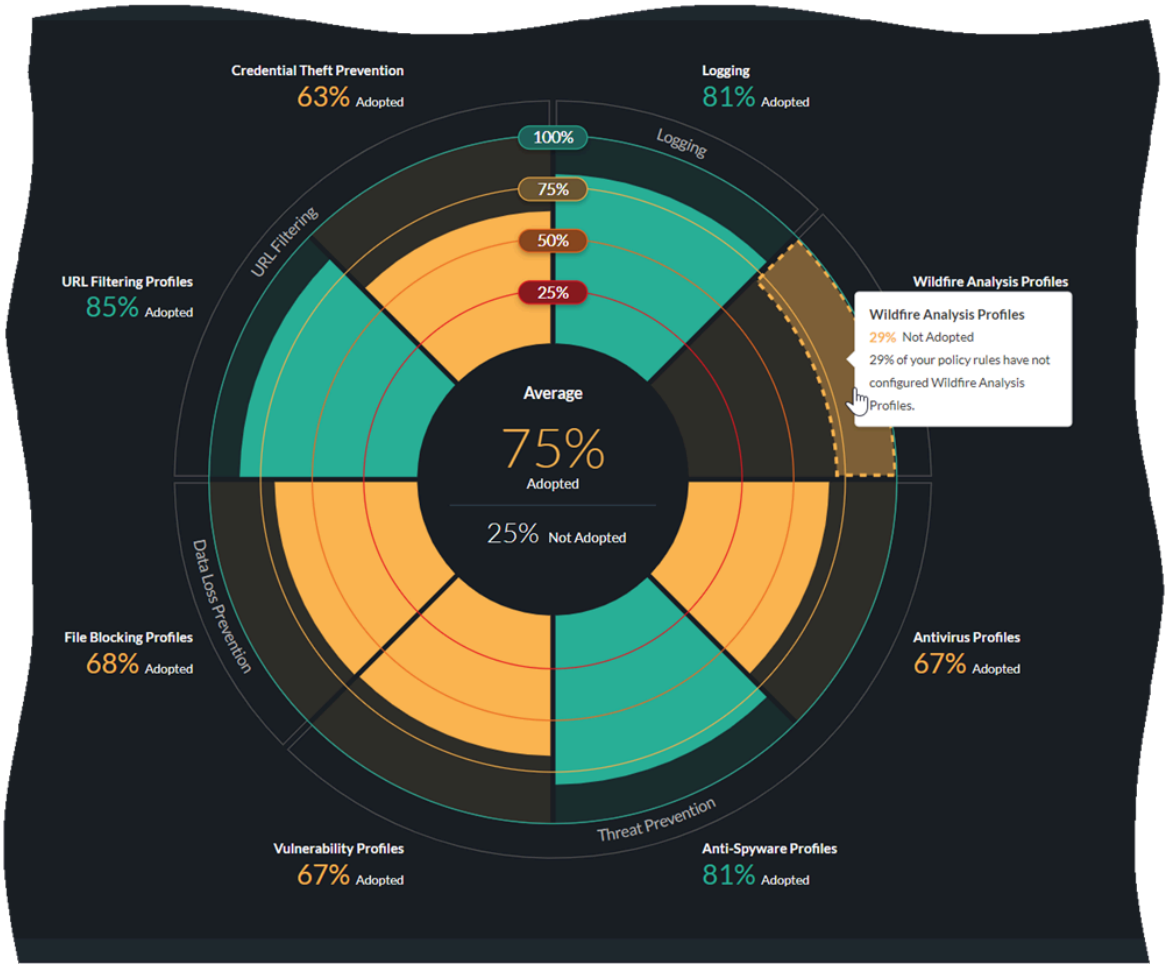
- Afin de vous concentrer sur l'adoption de fonctionnalités pour un ensemble spécifique de pare-feu, vous pouvez filtrer le graphique en fonction du groupe de périphériques, y compris

les périphériques gérés par Panorama. Vous pouvez également consulter des tableaux de tendances historiques en matière d'adoption.

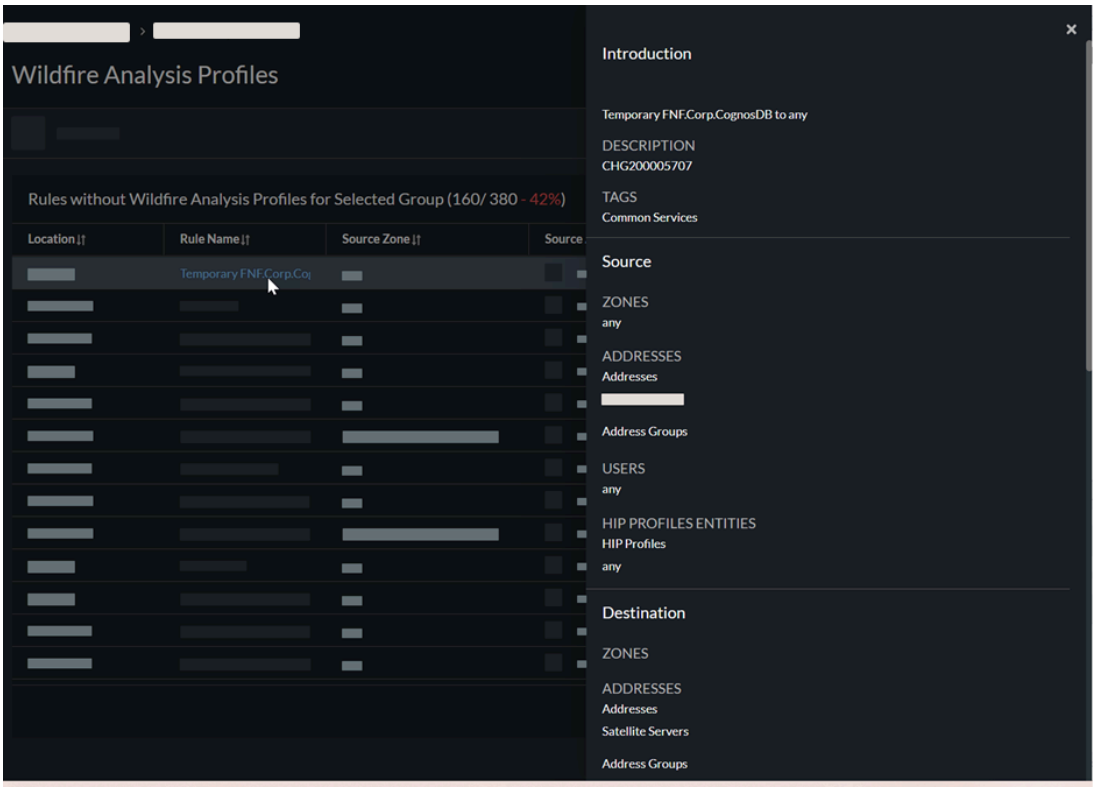


- *Lorsque vous générez un rapport BPA à la demande à l'aide d'une TSF, les informations relatives à l'adoption de votre TSF sont reflétées dans le tableau de bord Adoption des fonctionnalités. (PAN-OS 9.1 et plus TSFs)*
- *Vous pouvez exporter les données d'adoption au format .csv pour les utiliser dans des applications tierces telles que Microsoft Excel*

- Sélectionnez la section correspondant à une fonctionnalité dans le tableau pour afficher les règles de politique qui ne disposent pas de cette fonctionnalité.



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

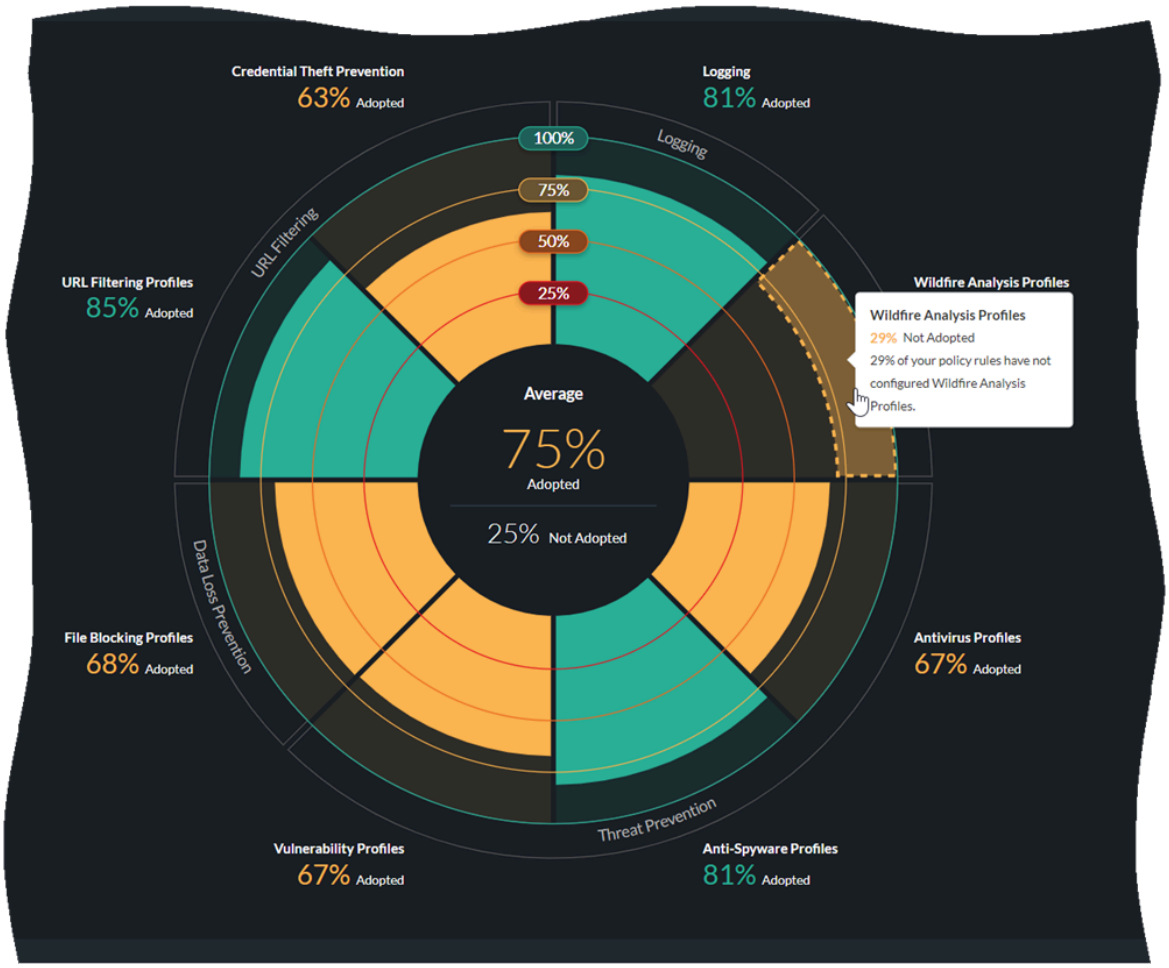


Identifiez les failles en matière d'adoption

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 situation de base afin d'identifier les failles dans l'adoption des fonctionnalités de la politique de sécurité.

Le résumé d'adoption permet d'identifier les périphériques, les zones et les domaines dans lesquels vous pouvez améliorer 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 sur le Groupe d'appareils afin de réduire le champ d'application et d'identifier les failles.

Dans **Dashboard (Tableau de bord)** > **Feature Adoption (Adoption des fonctionnalités)**choisir **Overall Adoption (Adoption globale)** pour vérifier les taux d'adoption des fonctionnalités suivantes. Sélectionnez **Best Practices (Meilleures pratiques)** pour voir les taux d'adoption de ces fonctionnalités qui respectent les meilleures pratiques de Palo Alto Networks. Utilisez ces informations comme critères d'identification des écarts : si le taux d'adoption réel ne correspond pas aux recommandations, prévoyez de combler l'écart :



- Appliquez les profils d'analyse WildFire, d'antivirus, d'antispyware, de vulnérabilité et de blocage de fichiers à toutes les règles qui autorisent le trafic, avec un objectif d'adoption de 100 % ou presque de 100 %. Si vous n'appliquez aucun profil à une règle d'autorisation, vérifiez qu'il existe une bonne raison professionnelle de ne pas appliquer le profil.

  La configuration de profils de sécurité sur toutes les règles d'autorisation permet au pare-feu d'inspecter le trafic décrypté à la recherche de menaces, quels que soient l'application ou le service/port. Après avoir mis à jour la configuration, vous pouvez exécuter le BPA pour les périphériques non liés à la télémétrie afin de mesurer la progression et d'intercepter les nouvelles règles qui n'ont pas de profils de sécurité attachés.

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

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

Dans le résumé des applis, des utilisateurs et des ports du résumé de l'adoption, vérifiez les taux d'adoption des capacités suivantes. Utilisez les recommandations comme critères d'identification des failles. Si le taux d'adoption réel ne correspond pas aux recommandations, envisagez de remédier à la faille en procédant comme suit :

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

Dans le résumé de l'enregistrement du résumé de l'adoption, vérifiez les taux d'adoption des capacités suivantes. Utilisez les recommandations comme critères d'identification des failles. Si le taux d'adoption réel ne correspond pas aux recommandations, envisagez de remédier à la faille en procédant comme suit :

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

En résumé :

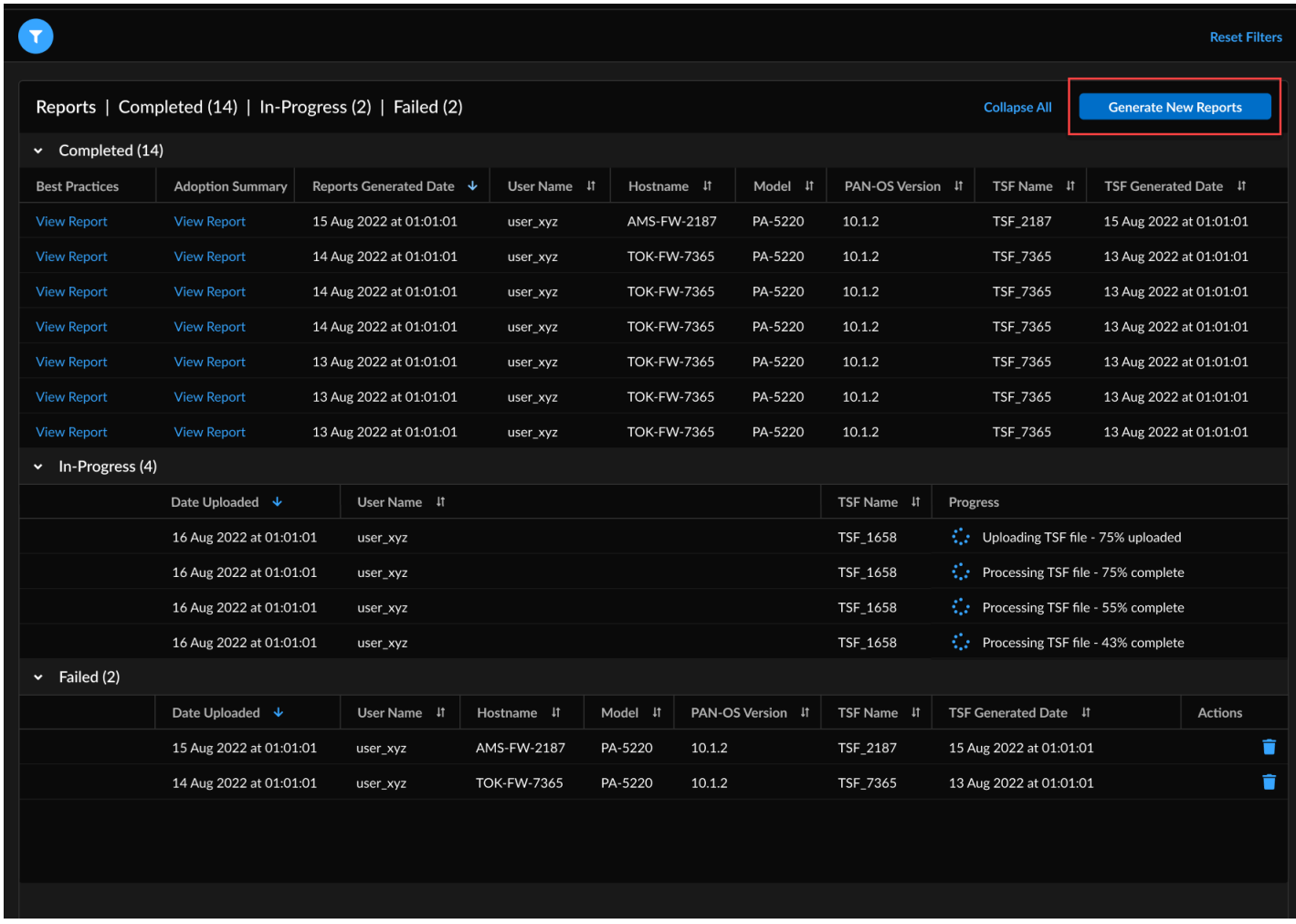
Fonctionnalité	Objectif d'adoption
WildFire	Le plus près possible de 100 % des règles de la politique de sécurité
Antivirus	Le plus près possible de 100 % des règles de la politique de sécurité
Antispyware	Le plus près possible de 100 % des règles de la politique de sécurité
Vulnérabilité	Le plus près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

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

Tableau de bord : BPA à la demande

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	☐ Strata Cloud Manager Essentials ☐ AIOps for NGFW Premium ou Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

- Allez à **Dashboards (Tableaux de bord)** > **On Demand BPA (BPA à la demande)** pour commencer.



Que vous indique ce tableau de bord ?

Le tableau de bord présente le rapport d'évaluation des meilleures pratiques (BPA) basé sur les fichiers TSF téléchargés des périphériques.

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 d'assistance 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.

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

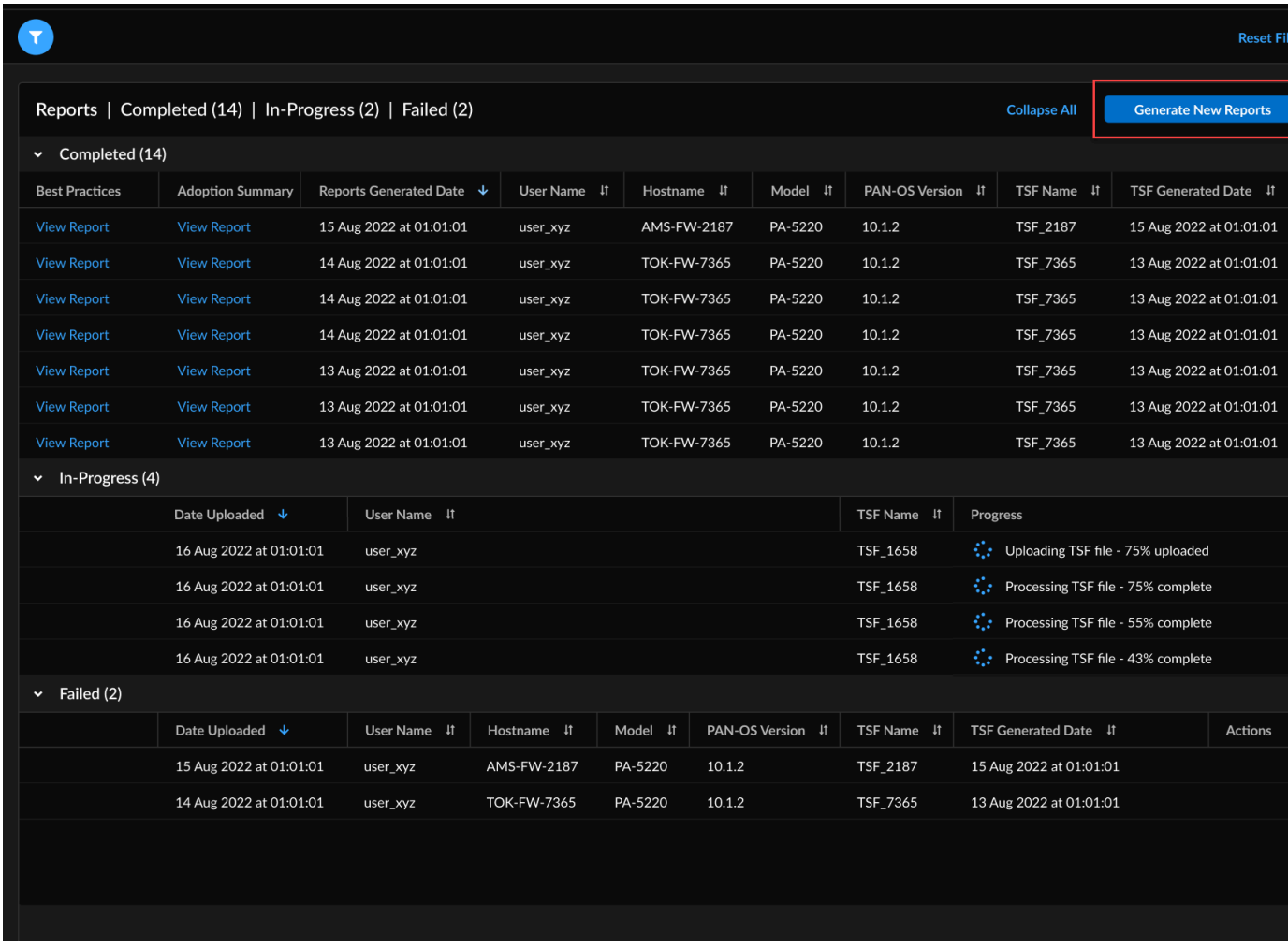
Le BPA évalue votre posture de sécurité par rapport aux meilleures pratiques de Palo Alto Networks et priorise les améliorations à apporter aux périphériques. Les meilleures pratiques en matière de sécurité permettent de prévenir les menaces connues et inconnues, de réduire la surface d'attaque et de fournir une visibilité sur le trafic, afin que vous puissiez savoir 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 Centre pour la sécurité Internet. Consultez le guide des meilleures pratiques pour renforcer la posture de sécurité et mettre en œuvre des améliorations.

Générer un rapport BPA à la demande

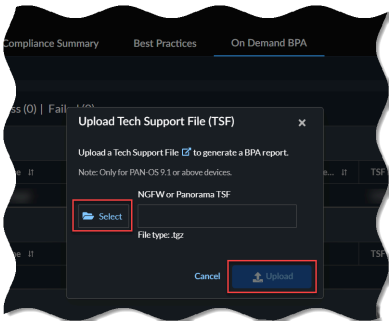
Suivez ces étapes pour générer le rapport BPA à la demande.

STEP 1 | Accédez à **Dashboards (Tableaux de bord)** > **On Demand BPA (BPA à la demande)**.

STEP 2 | **Générer un nouveau rapport BPA.**



STEP 3 | **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 débit 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.*
- *Pour plus d'informations sur la capture, le traitement et le stockage des données de Palo Alto Networks, consultez AIOps pour la confidentialité NGFW dans le Centre de confiance.*

STEP 4 | **View Report (Consultez le rapport)** ci-dessous**Completed (Terminé)** pour voir les résultats.

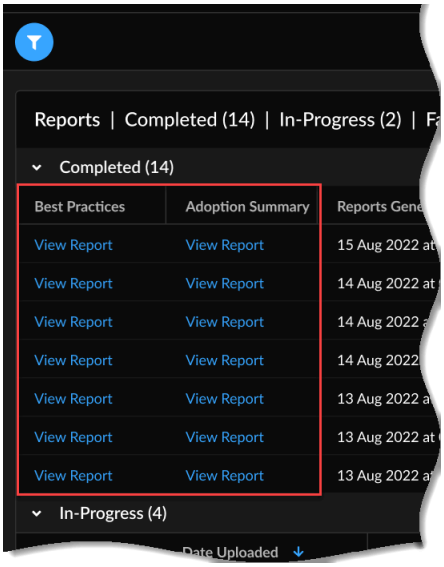


Tableau de bord : Santé SASE

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	• L'une des options suivantes : ❑ Observabilité Prisma Access et ADEM ❑ Strata Cloud Manager Pro • Un rôle qui a l'autorisation d'afficher le tableau de bord → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Que vous indique ce tableau de bord ?

Ce tableau de bord vous présente l'état général de vos utilisateurs mobiles, de vos sites distants et de vos applications (si vous avez acheté une AI-Powered ADEM licence) qui sont actuellement connectés à Prisma Access. Les chiffres dans les cercles représentent le nombre d'utilisateurs ou de sites qui sont actuellement connectés à partir de l'emplacement Prisma Access où ils apparaissent. Un point représente un seul utilisateur ou site. Les zones de la carte sur fond bleu indiquent que les chiffres affichés dans cette région constituent une prédiction ou une prévision.

Filtrez les données affichées dans ce tableau de bord avec un ou plusieurs des filtres suivants

- la plage horaire
- Emplacement Prisma Access
- Emplacement de la source

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

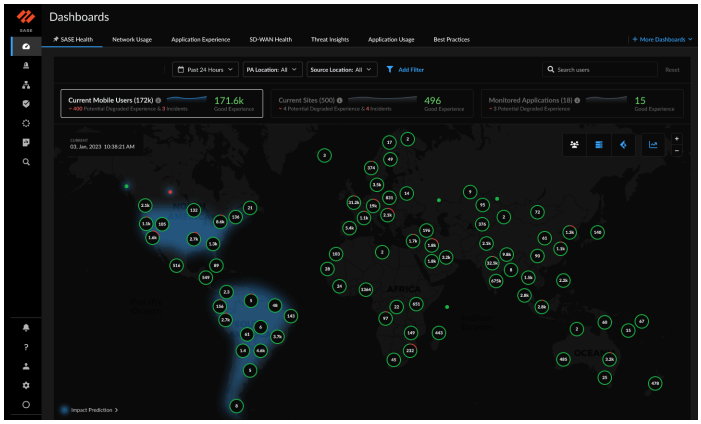
Utilisez le tableau de bord pour obtenir une vue d'ensemble et un état général du nombre d'utilisateurs mobiles et de sites distants connectés à Prisma Access, classés en fonction de leur emplacement sur la carte. Vous pouvez également consulter leur état général dans ce tableau de bord.

Tableau de bord de l'état SASE : Utilisateurs mobiles actuels : vue cartographique

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	• L'une des options suivantes : ❑ Observabilité Prisma Access et ADEM ❑ Strata Cloud Manager Pro

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	• Un rôle qui a l'autorisation d'afficher le tableau de bord → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Le **Current Mobile Users (Utilisateurs mobiles actuels)** dans l'onglet **SASE Health (État SASE)** le tableau de bord vous montre une vue d'ensemble de la répartition de l'expérience de l'utilisateur mobile sur tous les sites. Le nombre dans les cercles correspond au nombre d'utilisateurs mobiles qui sont actuellement connectés à Prisma Access en utilisant GlobalProtect. Un point représente un seul utilisateur mobile. Un cercle ou un point vert indique une bonne note pour l'expérience utilisateur. De même, un rouge indique un score d'expérience dégradé. Les notes d'expérience dégradées comprennent les notes Passable et Médiocre combinées. Le graphique linéaire à droite des **Current Mobile Users (Utilisateurs mobiles actuels)** vous indique une tendance des scores d'expérience moyens pour tous les utilisateurs mobiles au cours de la **Time Range (Plage horaire)**.



Cliquez sur le nombre (représentant le nombre d'utilisateurs de l'expérience potentiellement dégradée) en regard de l'icône **Potential Degraded Experience (Expérience potentiellement dégradée)** ou **Incidents (Incidents)** pour afficher les détails de l'expérience utilisateur dégradée dans un volet qui s'ouvre sur la gauche.

Tableau de bord de l'état SASE : Sites actuels - Vue cartographique

Où puis-je l'utiliser ?	De quoi ai-je besoin ?

• Prisma Access (Managed by Panorama or Strata Cloud Manager)	• L'une des options suivantes :
	  ☐ Observabilité Prisma Access et ADEM
	  ☐ Strata Cloud Manager Pro
	• Un rôle qui a l'autorisation d'afficher le tableau de bord

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	→ Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Ce tableau de bord vous indique le nombre de sites configurés se connectant aux emplacements Prisma Access dans le monde. Le nombre entre parenthèses est le nombre total de sites connectés et le nombre à droite de la carte est le nombre de sites qui ont obtenu une bonne note d'expérience. Les sites dont les scores d'expérience ne peuvent être obtenus pour quelque raison que ce soit ne sont pas exclus du calcul du nombre de sites connectés. La ligne bleue indique la tendance de la note d'expérience moyenne pour tous les sites au fil du temps. En dessous des sites actuels, vous voyez le nombre de sites dont l'expérience est dégradée (mauvaise) ainsi que le nombre d'incidents pour l'ensemble des sites. Les incidents peuvent relever d'une ou de plusieurs des catégories suivantes : Infrastructure, services réseau, centres de données et sites tiers (les centres de données sont en panne).

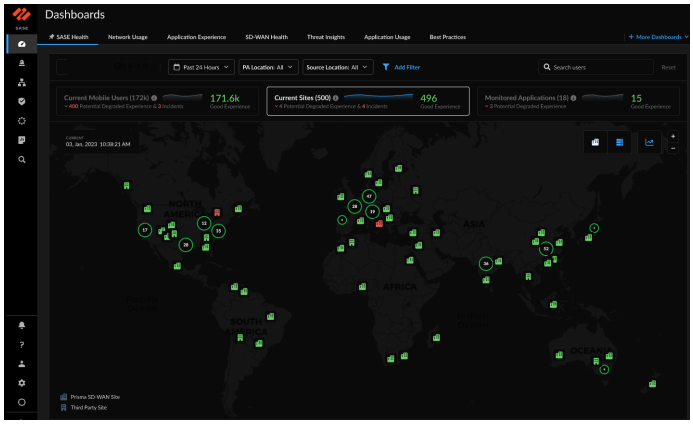


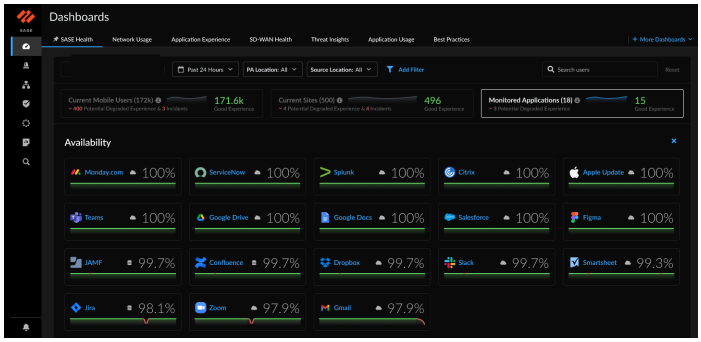
Tableau de bord de l'état SASE : Applications surveillées

Où puis-je l'utiliser ?	De quoi ai-je besoin ?

• Prisma Access (Managed by Panorama or Strata Cloud Manager)	• L'une des options suivantes :
	  ❑ Observabilité Prisma Access et ADEM
	  ❑ Strata Cloud Manager Pro
	• Un rôle qui a l'autorisation d'afficher le tableau de bord
	→ Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Consultez les mesures de disponibilité des applications dans l'onglet **Monitored Applications (Applications surveillées)** du tableau de bord **SASE Health (État SASE)**. Ce tableau de bord

vous indique combien d'applications sont surveillées par ADEM et combien d'entre elles ont un score dégradé. Ce chiffre tient compte de l'expérience de l'application pour les utilisateurs mobiles et les sites distants. Les applications ayant obtenu une note médiocre ou moyenne sont considérées comme ayant une expérience dégradée. Vous pouvez également voir la disponibilité de l'application pendant la période sélectionnée à l'aide du filtre.



Le nombre à droite du nom de l'application indique le pourcentage de temps pendant lequel l'application était disponible au cours de **Time range (Plage horaire)**.

Surveiller : Strata Cloud Manager

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels • Prisma SD-WAN	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro ☐ Prisma SD-WAN Les autres licences et prérequis nécessaires à la visibilité sont : ☐ Observabilité ADEM ☐ DEM autonome pour réseaux distants ☐ ADEM alimenté sur l'IA ☐ Rapport de WAN Clarity ☐ Un rôle qui a l'autorisation d'afficher le tableau de bord → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Bénéficiez d'une visibilité complète sur le trafic de votre réseau et sur les produits et abonnements que vous gérez avec Strata Cloud Manager. Dans Prisma Access, vous pouvez surveiller de façon protectrice l'état de santé et de connectivité de vos réseaux distants, de vos applications, de vos périphériques NGFW et de vos utilisateurs mobiles. Strata Cloud Manager fournit également des fonctionnalités pour surveiller les performances des services réseau communs, les détails de consommation de vos licences d'abonnement et gérer l'outil utilisé pour analyser les problèmes de connectivité. Les utilisateurs Prisma SD-WAN peuvent également surveiller la qualité et la connectivité des applications Prisma SD-WAN, des périphériques ION, des centres de données ici réunis en un seul endroit.

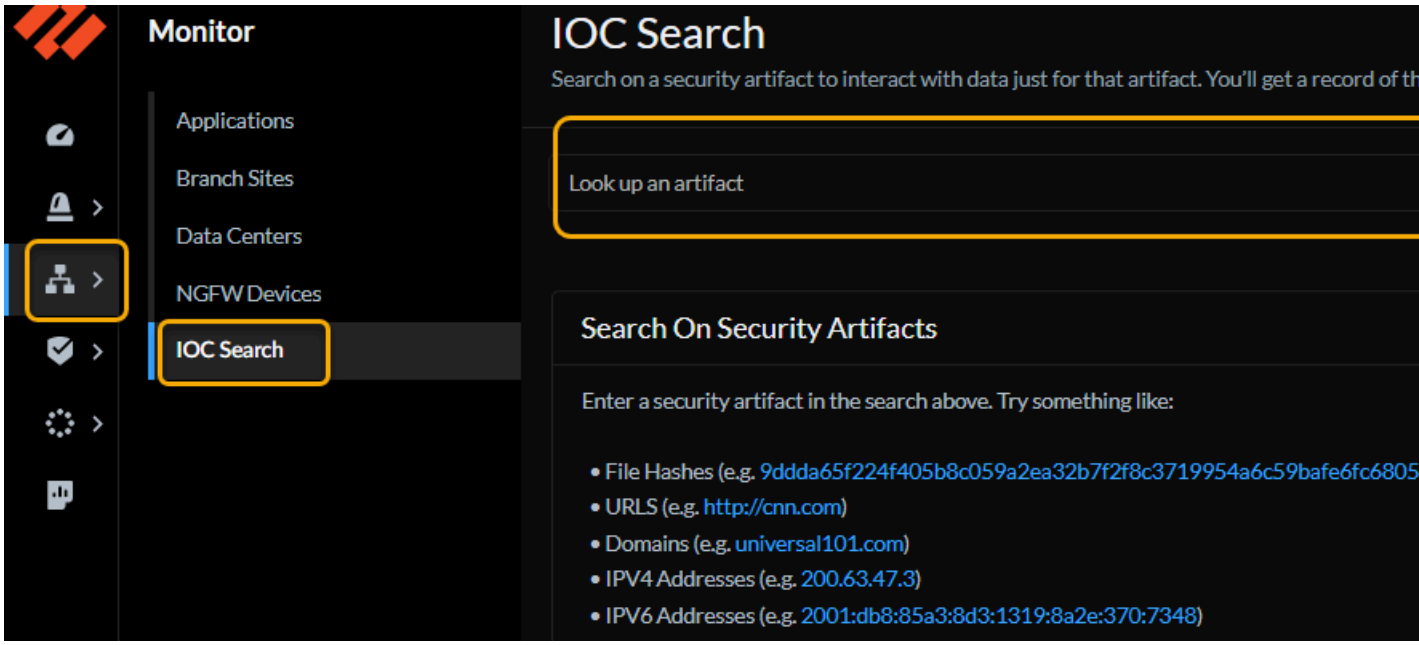
Surveiller : Recherche de l'IOC

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels • Prisma SD-WAN	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro ☐ Prisma SD-WAN Les autres licences et prérequis nécessaires à la visibilité sont : ☐ Observabilité ADEM ☐ DEM autonome pour réseaux distants ☐ ADEM alimenté sur l'IA ☐ Rapport de WAN Clarity ☐ Un rôle qui a l'autorisation d'afficher le tableau de bord → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Vous pouvez effectuer une recherche sur un artefact de sécurité pour interagir avec les données relatives à cet artefact. Les résultats de la recherche incluent :

- L'historique et l'activité de l'artefact dans votre réseau. *Évaluez la prévalence de l'artefact dans votre réseau et comparez-le à ceux de l'industrie.*
- Les renseignements sur les menaces de Palo Alto Networks concernant l'artefact, sont basés sur l'analyse de l'ensemble du trafic traité et analysé par Palo Alto Networks.
- Consolidation des résultats de l'analyse des tiers pour l'artefact.

Cliquez sur **Monitor (Surveiller)** > **IOC Search (Rechercher l'IOC)** pour commencer.

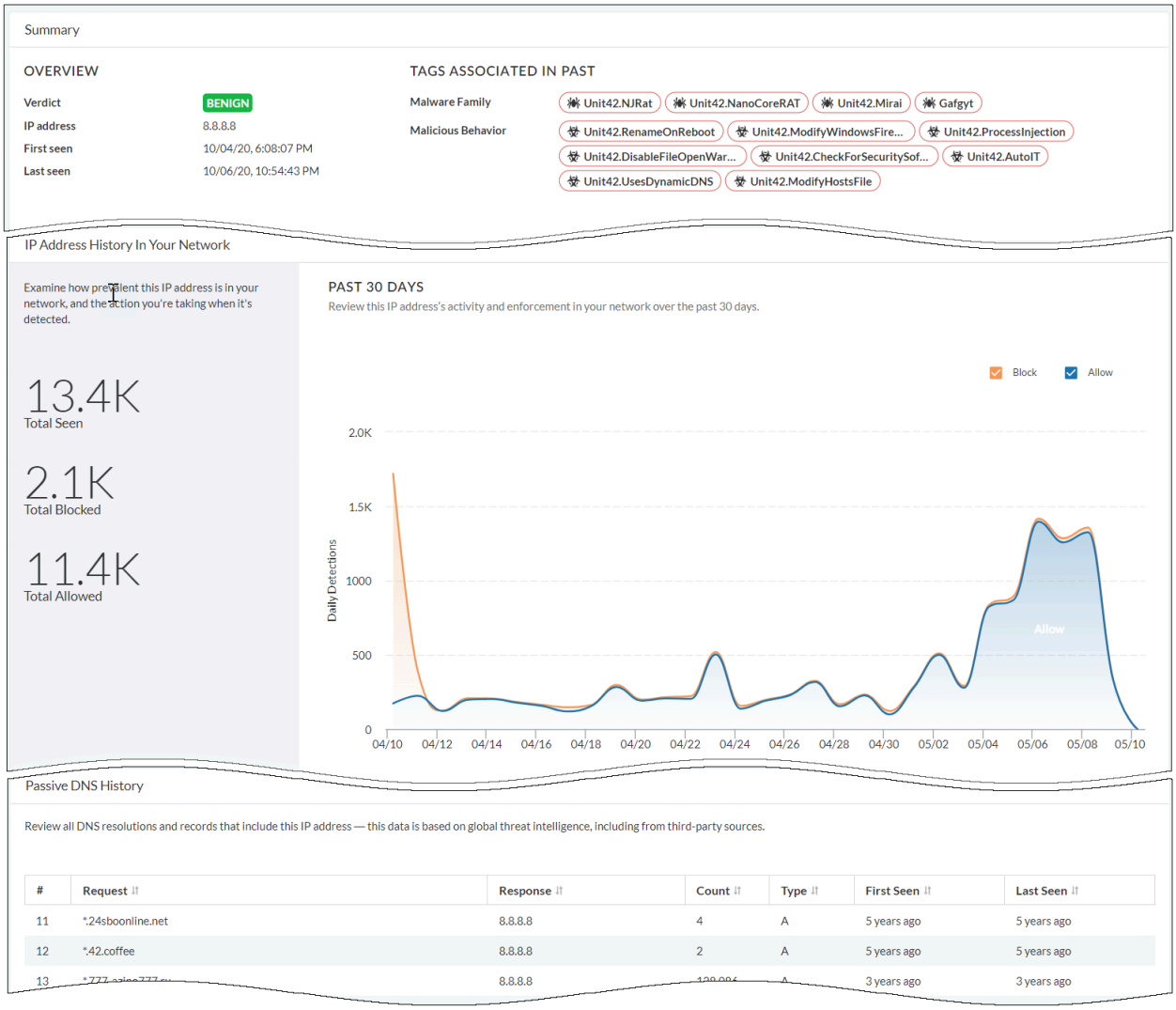


Pour commencer, recherchez l'un de ces types d'artefacts : un **hachage de fichier**, une **URL**, un **domaine** ou une **adresse IP** (IPv4 ou IPv6).

Adresse IP

Vous pouvez rechercher une adresse IP pour analyser les informations sur les menaces liées aux activités d'adresse IP dans votre réseau. Les données suivantes sont affichées dans le résultat de la recherche :

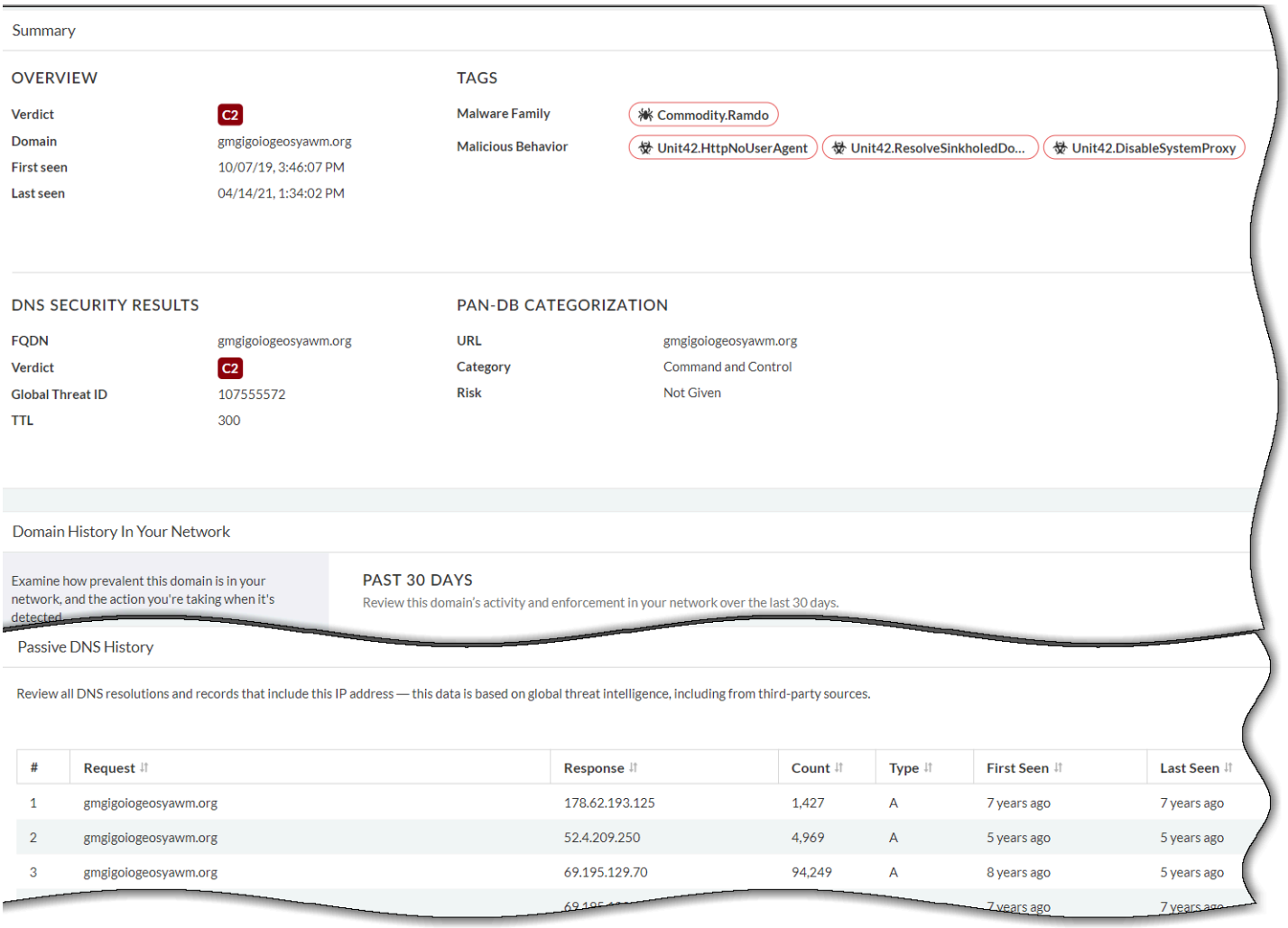
- Nombre total de fois où une adresse IP a été détectée dans votre réseau au cours des 30 derniers jours.
- Représentation graphique de l'action entreprise (autorisation ou blocage) sur l'adresse IP.
- Liste des requêtes DNS contenant l'adresse IP en fonction des renseignements sur les menaces de Palo Alto Networks et de sources tierces.



Domaine

Affichez un résumé des activités associées au domaine dans votre réseau. Les résultats de la recherche incluent :

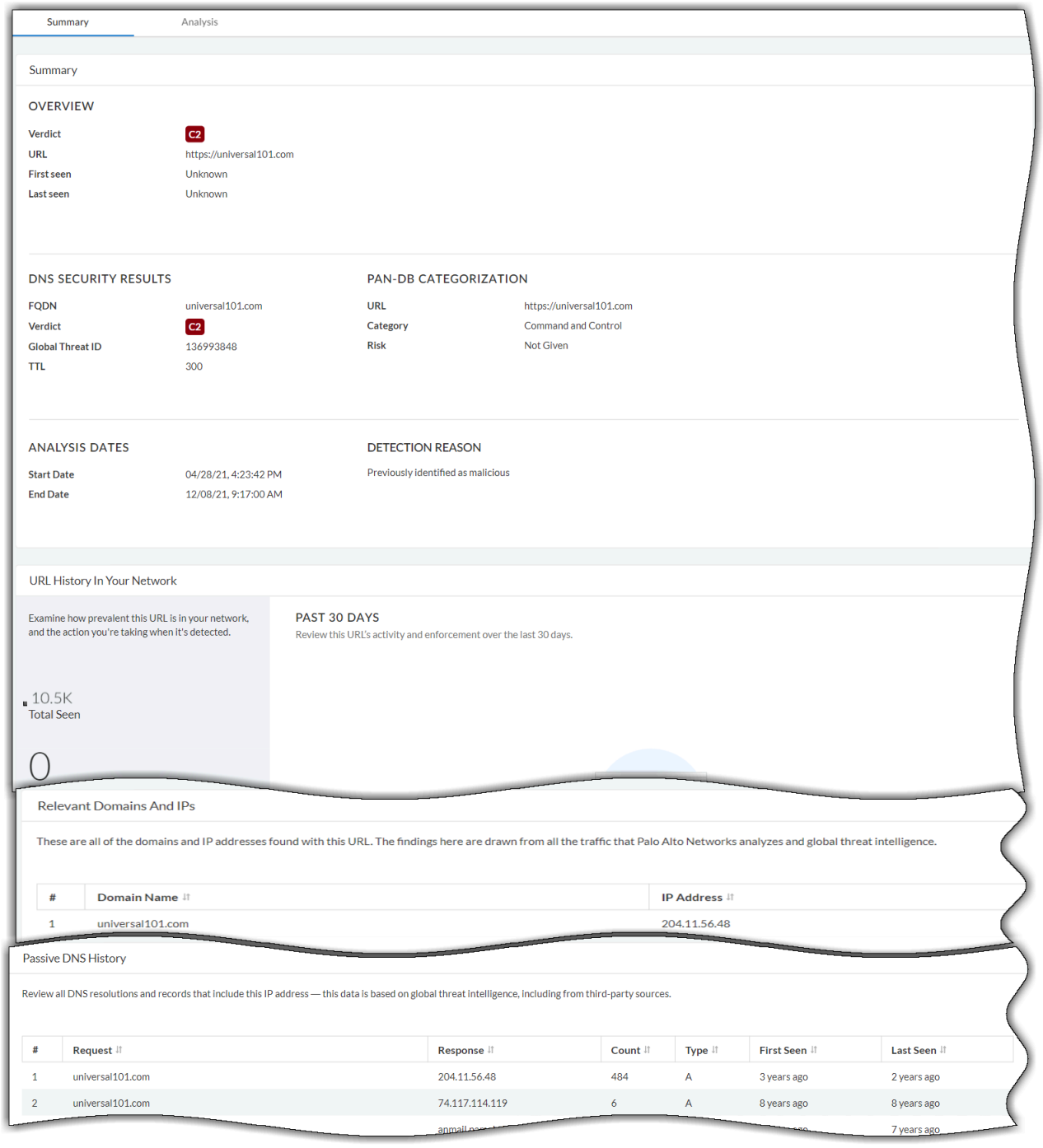
- Classification du domaine dans votre réseau sur la base de l'analyse de l'échantillon WildFire.
- Nombre total d'activités associées au domaine au cours des 30 derniers jours.
- Mise en œuvre appliquée à chaque activité sous forme de graphique.
- Les informations issues de l'analyse de WildFire qui appuient les données utilisées dans l'attribution du verdict pour le domaine.
- Activité DNS collectée à partir de toutes les soumissions WildFire qui contiennent des instances de ce domaine.



URL

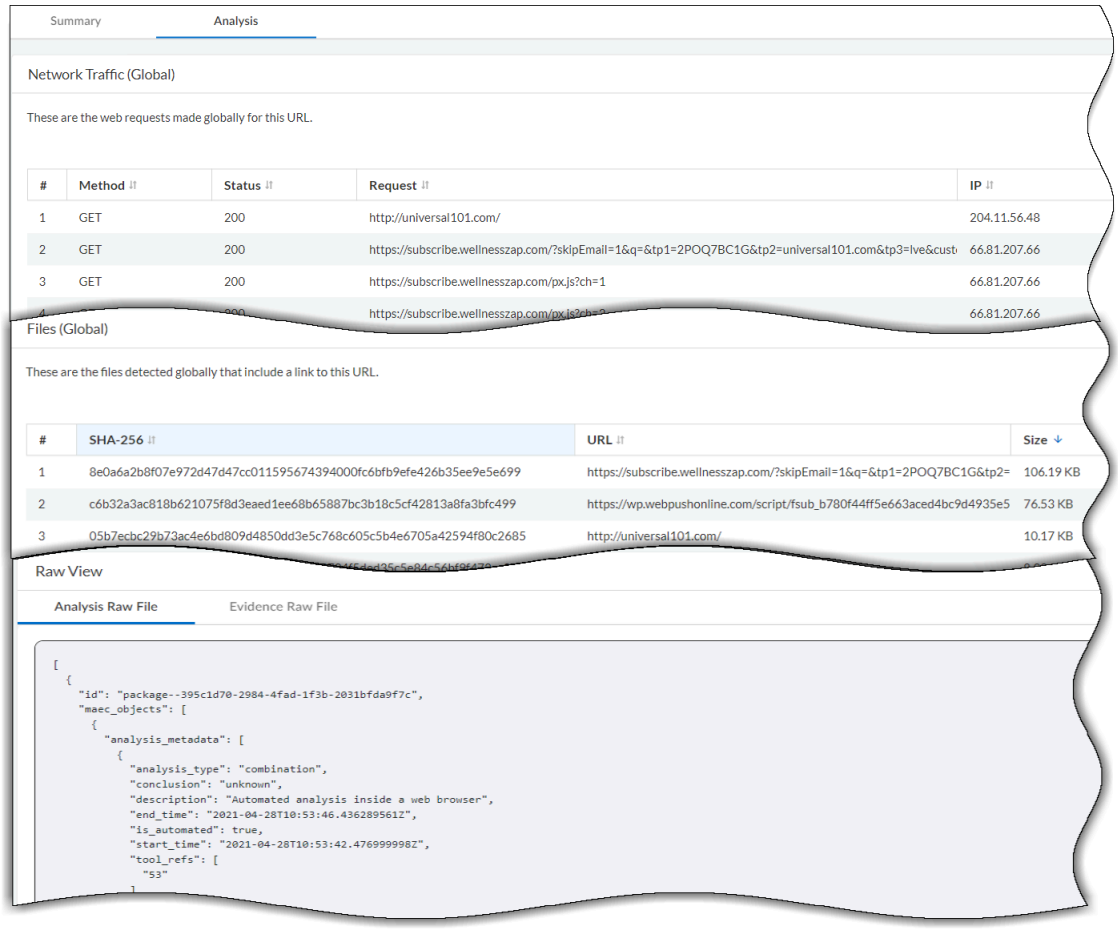
Découvrez l'activité de l'URL dans l'ensemble du trafic analysé par Palo Alto Networks. Les résultats de la recherche incluent :

Résumé : examinez un résumé de l'activité de l'URL dans votre réseau. Les données incluent : Résultats de la sécurité DNS pour l'URL et la catégorisation PAN-DB.



Capture d'écran : affiche une capture d'écran du site Web lorsque vous effectuez une recherche sur un artefact URL.

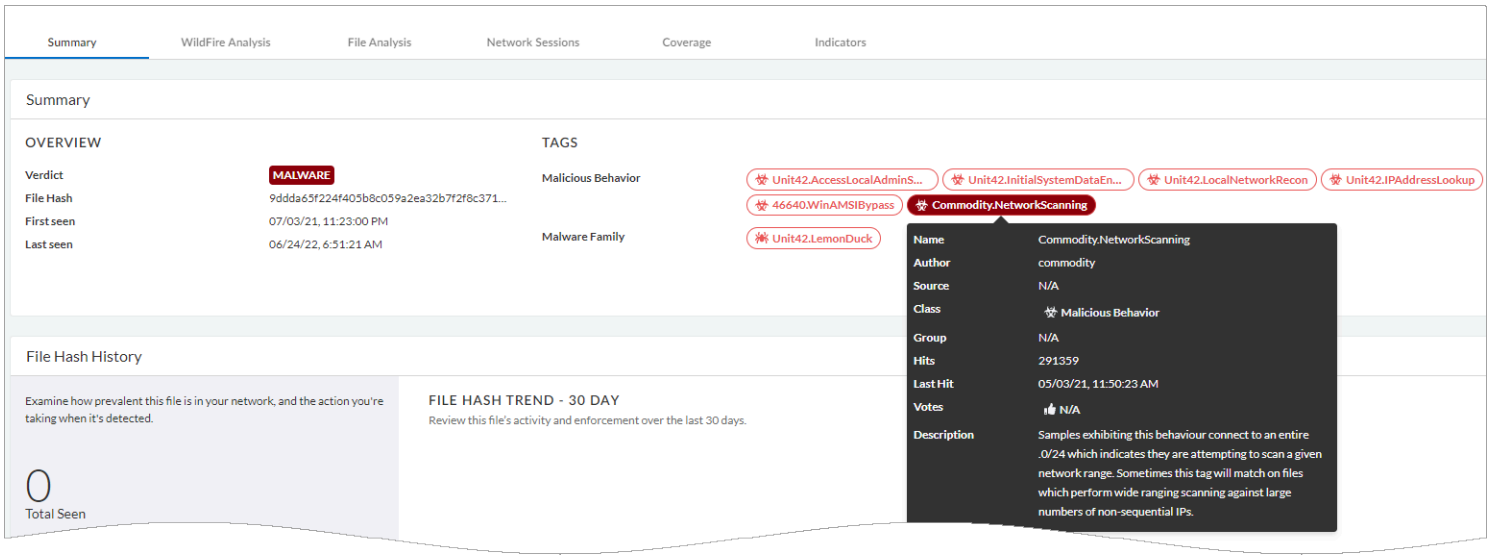
Analyse : consultez les données d'analyse de fichiers qui incluent les requêtes faites globalement pour cette URL, et les fichiers détectés avec cette URL. Pour en savoir plus, vous pouvez utiliser la valeur de hachage du fichier ou la vue du fichier.



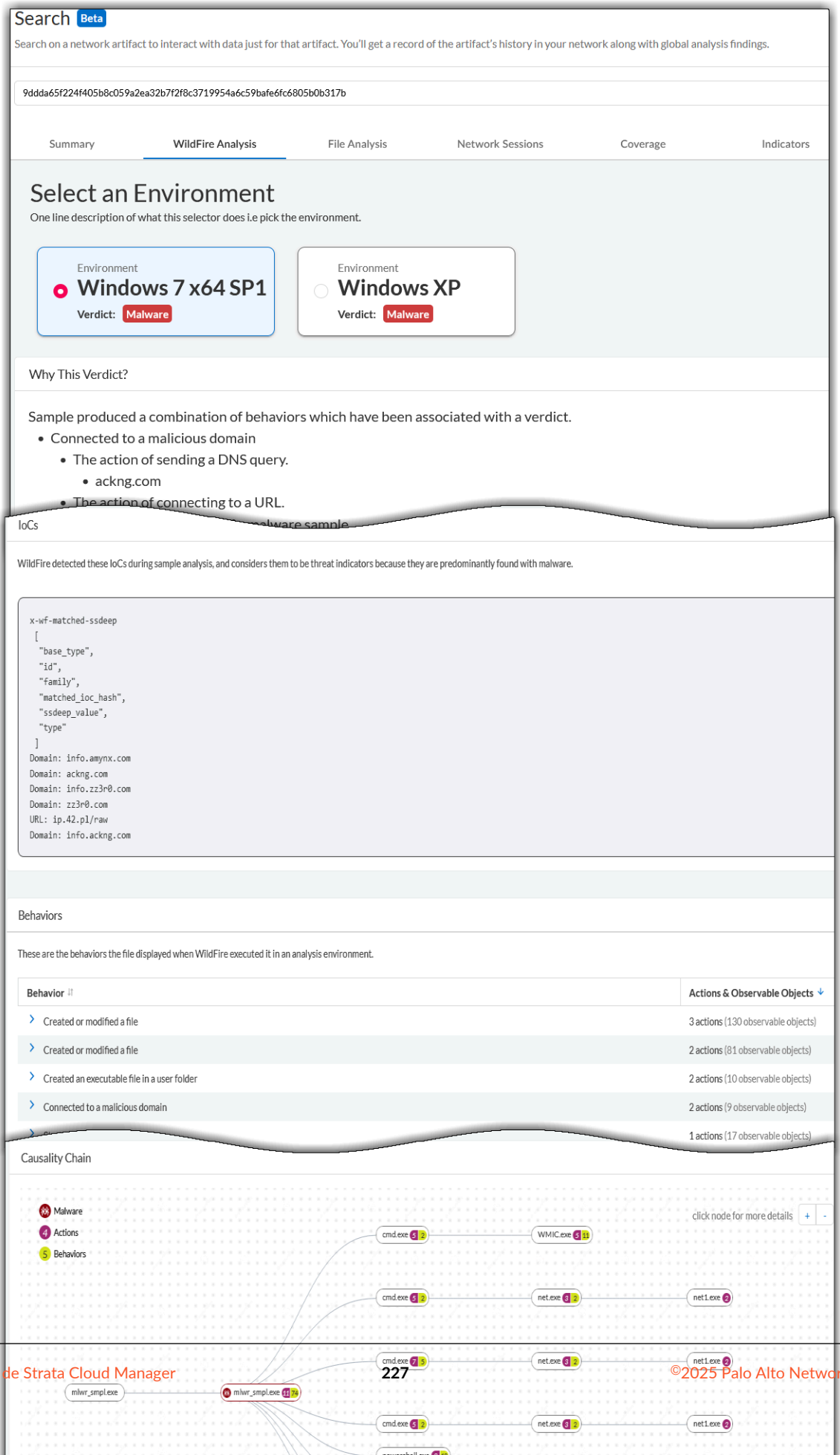
Hachage de fichier

La recherche de hachage de fichier résume l'activité du fichier, l'analyse des propriétés du fichier et les détails de l'analyse d'échantillon WildFire. Vous pouvez approfondir le résultat de la recherche pour examiner les données suivantes :

Résumé : affichez le verdict de hachage du fichier et l'historique de l'activité du fichier dans votre réseau. Cliquez sur le nom de l'étiquette pour en afficher les détails. Les étiquettes peuvent vous aider à comprendre si le fichier fait partie du groupe de menaces, de campagnes ou d'acteurs.



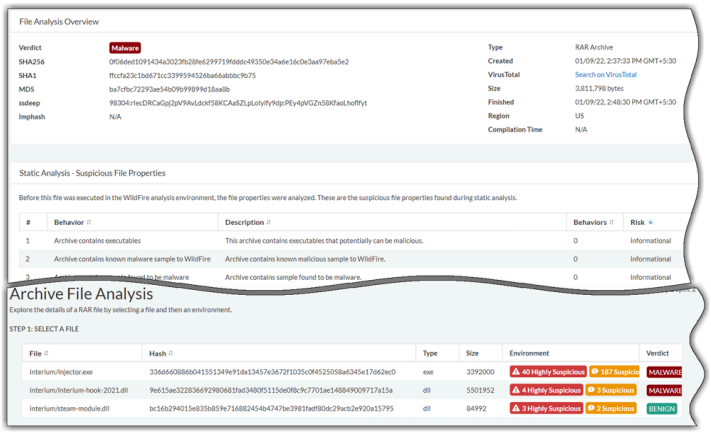
Analyse WildFire : évaluez le fonctionnement de l'échantillon (fichier) pendant l'analyse WildFire. Vous pouvez consulter les informations sur le verdict de l'échantillon, les indicateurs de menace détectés lors de l'analyse de l'échantillon et le fonctionnement lors du traitement de l'échantillon dans l'environnement d'analyse. Vous pouvez également consulter les captures d'écran des différentes étapes du processus capturées lors de l'analyse de l'échantillon WildFire.



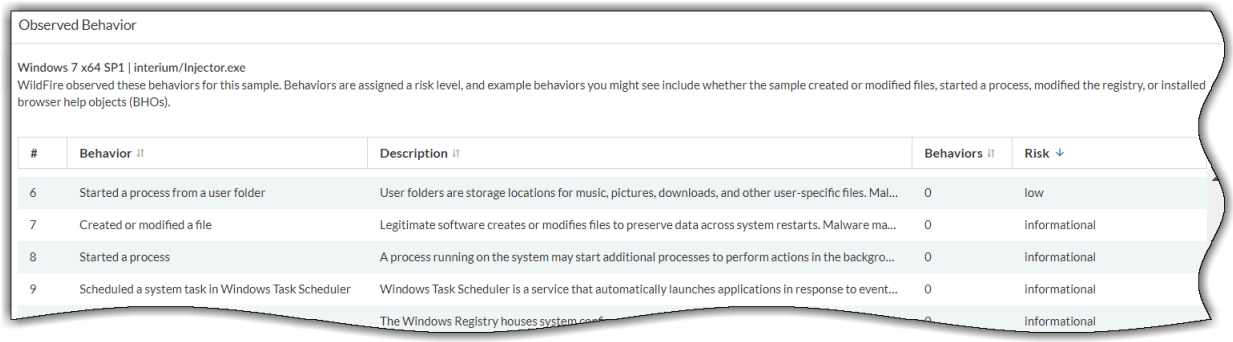
Analyse de fichiers : comparez l'analyse avant et après l'exécution de l'échantillon (fichier) dans l'environnement d'analyse WildFire.

Aperçu :vérifiez le verdict de l'échantillon ici. Si le verdict est mal classé, demander une modification du verdict. L'équipe de lutte contre les menaces de Palo Alto Networks examine de plus près l'échantillon et met à jour le verdict s'il s'avère incorrect.

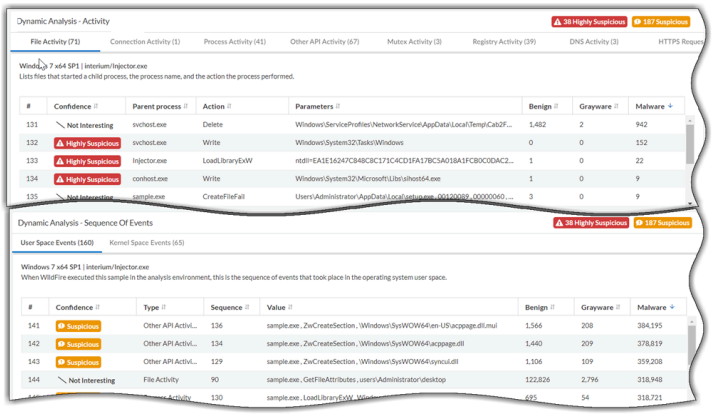
Analyse statique : l'analyse statique examine le contenu d'un fichier spécifique avant que le fichier ne soit exécuté dans l'environnement d'analyse WildFire. La recherche montre également les propriétés des fichiers suspects trouvés lors de l'analyse statique. Le résultat de la recherche varie selon le type de fichier. La capture d'écran présente ici une analyse statique pour un fichier d'archive.



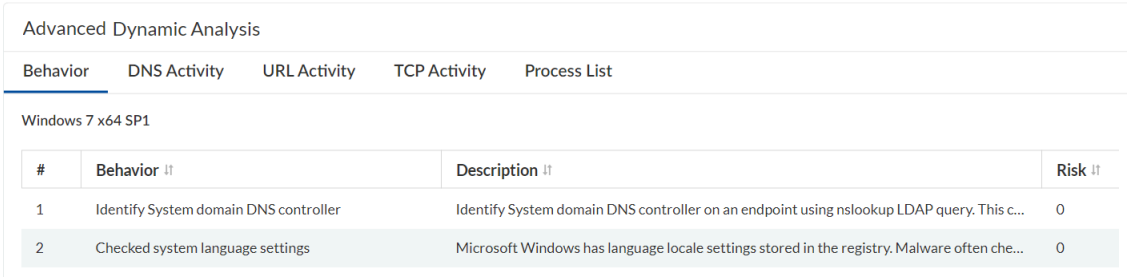
Type de fonctionnement observé : examinez l'analyse du fonctionnement de WildFire concernant l'échantillon dans un environnement particulier.



Analyse dynamique : vérifie le fichier en détail en extrayant des informations et des indicateurs supplémentaires pour un réseau compromis. Vous pouvez vérifier les activités du processus impliqué et la séquence des événements qui se sont déroulés dans votre système lors de l'exécution du fichier.

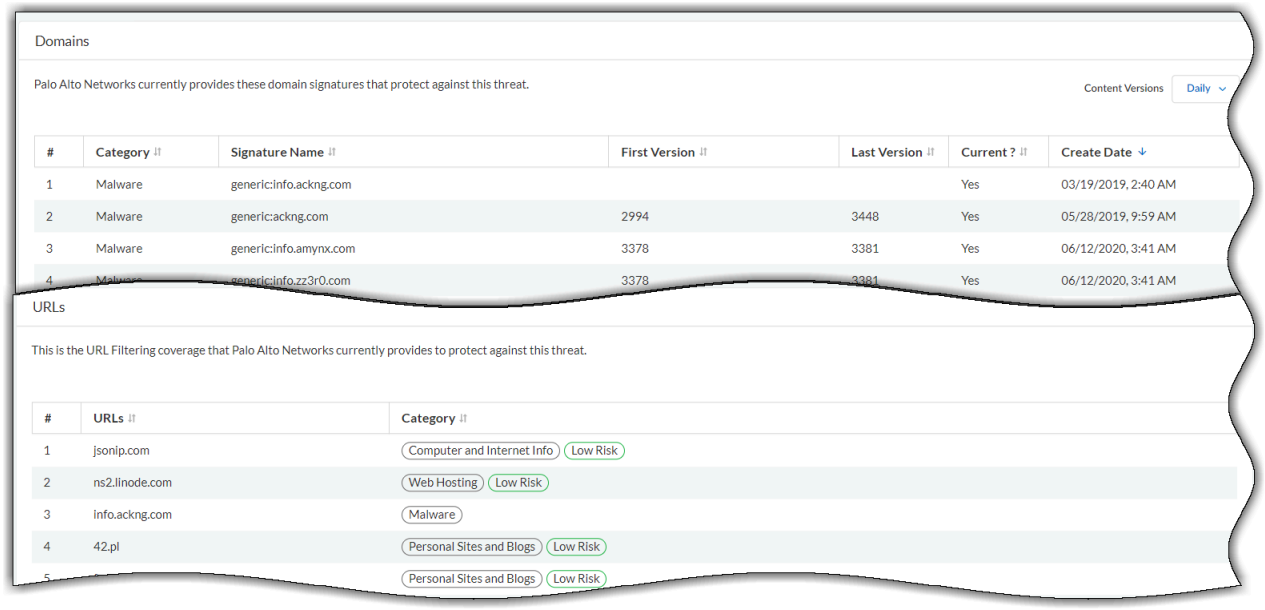


Analyse dynamique avancée : consultez les résultats d'analyse d'échantillons analysés par les techniques avancées de WildFire (analyse intelligente de la mémoire d'exécution, analyse dynamique de l'hyperviseur, émulation de dépendance, etc.), un moteur basé sur le cloud qui détecte et prévient les menaces de logiciels malveillants très évasifs. Vous pouvez afficher les fonctionnements observés et utiliser ces informations pour l'analyse post-exécution.



Sessions réseau : découvrez la session réseau pour un échantillon. Utilisez ces données pour en savoir plus sur le contexte de la menace, connaître les hôtes et les clients affectés, ainsi que les applications utilisées pour diffuser le logiciel malveillant.

Protection : vérifiez la protection de signature pour un échantillon afin d'évaluer le niveau de protection contre les menaces. Vous pouvez visualiser les signatures associées aux domaines à partir desquels l'échantillon a été téléchargé et les URL auxquelles l'échantillon a accédé.



Indicateurs : voir les artefacts qui sont des indicateurs pour un réseau intégré. Les indicateurs sont catégorisés en fonction des types d'artefacts; domaine, adresse IP, URL, en-têtes d'agent utilisateur et objets d'exclusion mutuelle. Les artefacts à haut risque sont étiquetés comme suspects ou hautement suspects.

Domain

2 Highly Suspicious 4 Suspicious 4 Interesting

These domains - seen when this sample was executed in the WildFire analysis environment - are predominantly found with malware, and can indicate a compromised network.

#	Confidence	Indicator	Matching Indicators	Benign	Grayware	Malware
1	Highly Suspicious	info.ackng.com		0	0	234
2	Highly Suspicious	42.pl		97	5	499
3	Suspicious	ns3.epik.com		555	43	28,611
					44	28,595

IPv4

1 Highly Suspicious 2 Suspicious

These IP addresses - seen when this sample was executed in the WildFire analysis environment - are predominantly found with malware, and can indicate a compromised network.

#	Confidence	Indicator	Matching Indicators	Benign	Grayware	Malware
1	Highly Suspicious	88.214.207.96		30	1	277
2	Suspicious	127.0.0.1		273,674	891,030	7,528,431
					8	562

URL

1 Highly Suspicious 4 Interesting

These URLs - seen when this sample was executed in the WildFire analysis environment - are predominantly found with malware, and can indicate a compromised network.

#	Confidence	Indicator	Matching Indicators	Benign	Grayware	Malware
1	Highly Suspicious	/e.png?id=		0	0	233
2	Suspicious	ip.42.pl/raw		104	7	507
3	Interesting	zz3r0.com/e.png?id=GVZ823834177364.GVZ823834177364.local&ma...		--	--	--
					--	--

User Agent

1 Suspicious

These user agent headers - seen for HTTP requests that were sent when this sample was executed in the WildFire analysis environment - are predominantly found with malware, and can indicate a compromised network.

#	Confidence	Indicator	Matching Indicators	Benign	Grayware	Malware
1	Suspicious	Python-urllib/2.7		5,162	26,246	54,432

Mutex

5 Interesting

A mutex (mutual exclusion object) allows programs to share the same resource, though the resource cannot be used by more than one program simultaneously. These mutexes are predominantly found with malware, and can indicate a compromised network.

#	Confidence	Indicator	Matching Indicators	Benign	Grayware	Malware
1	Interesting	testmutex_{D0E858DF-985E-4907-B7FB-8D732C3FC3B9}		1	0	0
2	Interesting	Local\c:!users!jgs9ctxe4sno!appdata!roaming!microsoft!windows!cookies!		--	--	--
					--	--

Surveiller : Sites des succursales

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels • Prisma SD-WAN	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro ☐ Prisma SD-WAN Les autres licences et prérequis nécessaires à la visibilité sont : ☐ Observabilité ADEM ☐ DEM autonome pour réseaux distants ☐ ADEM alimenté sur l'IA ☐ Rapport de WAN Clarity ☐ Un rôle qui a l'autorisation d'afficher le tableau de bord → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Sites des succursales : Prisma Access

Sélectionnez**Monitor (Surveiller)** > **Branch Sites (Sites des succursales)** > **Prisma Access** pour afficher l'état et la connectivité de vos réseaux distants et l'utilisation de tous vos réseaux distants déployés dans différents Prisma Access lieux. Il indique en temps réel l'état de la connectivité et les détails de la consommation de la bande passante, ainsi que d'autres détails du déploiement. Les utilisateurs mobiles, les succursales et les points de vente se connectent à des réseaux distants. Vous pouvez également consulter l'état des tunnels configurés dans vos réseaux distants et chez vos utilisateurs mobiles.

En plus des widgets qui s'affichent avec la Prisma Access licence, ce tableau de bord affiche le score d'expérience du site et Prisma SD-WAN les détails du site de succursale uniquement si vous disposez de ADEM Observability ou de la AI-Powered ADEM licence.

Sites des succursales : Prisma SD-WAN

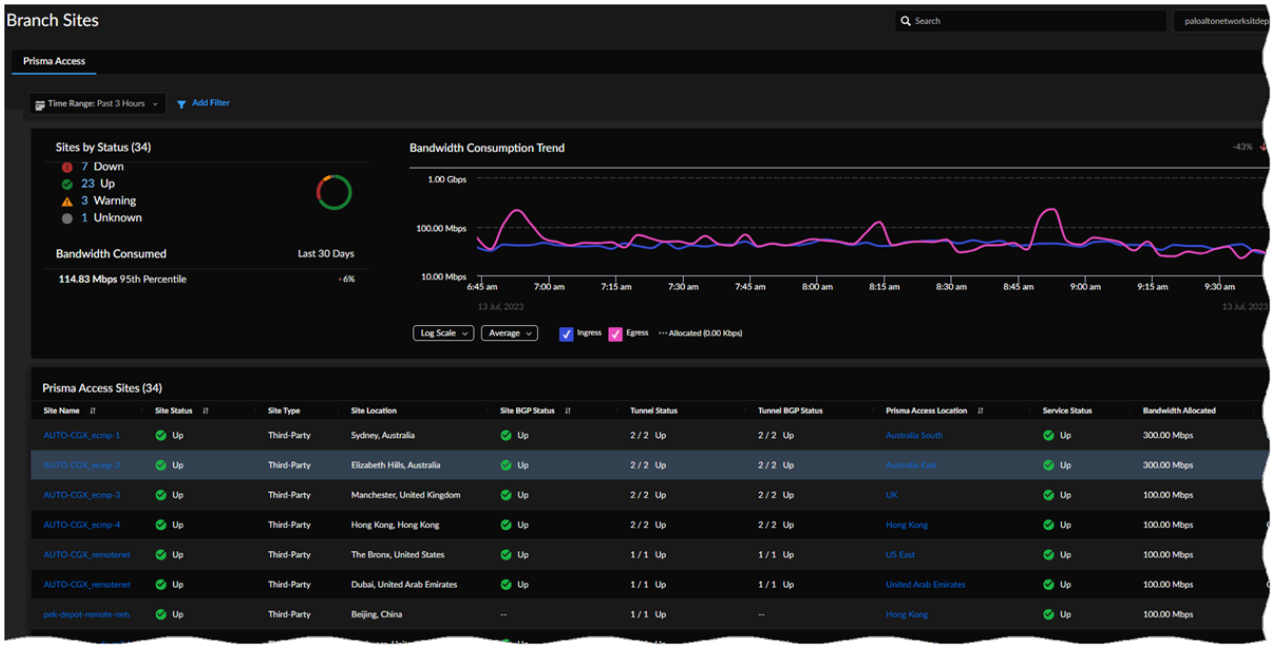
Choisir **Monitor (Surveiller)** > **Branch Sites (Sites des succursales)** > **Prisma SD-WAN** Pour configurer un site de succursale dans Prisma SD-WAN. Les sites de succursale comprennent les succursales que vous avez dans votre réseau étendu à Prisma SD-WAN. Vous pouvez configurer

un site de succursale avant ou après l'arrivée des périphériques ION sur un site donné. Le site de succursale de Prisma SD-WAN fournit les vues suivantes :

- La vue **cartographique** du site de succursale communique l'état de connectivité des périphériques de votre site de succursale au contrôleur et l'état de l'alarme pour le site.
- La vue**Liste** vous indique le nombre de sites actifs au cours du **Time Range (Plage horaire)** sélectionnés et les indicateurs de qualité globale des sites de la succursale.
- La vue **Activité** présente les principales analyses d'application, le dernier score d'intégrité du site et la répartition de l'état du site au fil du temps.
- Prisma Access
- Prisma SD-WAN

Sites des succursales (Prisma Access)

Sélectionnez **Branch Sites (Sites des succursales)** > **Prisma Access** pour consulter l'état et la connectivité de vos réseaux distants et l'utilisation de tous vos réseaux distants déployés à différents Prisma Access endroits.



Il indique en temps réel l'état de la connectivité et les détails de la consommation de la bande passante, ainsi que d'autres détails du déploiement. Les utilisateurs mobiles, les succursales et les points de vente se connectent à des réseaux distants. Vous pouvez également consulter l'état des tunnels configurés dans vos réseaux distants et chez vos utilisateurs mobiles. Pour une description détaillée de ces widgets, consultez Afficher et surveiller les sites des succursales.

Vous pouvez :

- Consultez les sites de vos réseaux distants en fonction de leur état.
- Consultez les tendances de la consommation de bande passante des réseaux distants.
- Consultez vos sites Prisma Access, et sélectionnez n'importe quel site pour afficher plus de détails.

- Ouvrez **IPSec Termination Node Utilization Details (Détails de l'utilisation du nœud de terminaison IPSec)**pour afficher les détails de consommation de bande passante de chaque SPN dans le site.
- Visualisez les données et les tendances du tunnel pour un site.
- Consultez l'état, la qualité, la connectivité et les informations sur la consommation du site.

Sites des succursales (Prisma SD-WAN)

Vous pouvez configurer un site de succursale avant ou après l'arrivée des périphériques ION sur un site donné. Le site de succursale de Prisma SD-WAN fournit les vues suivantes :

- La vue **Map (Carte)** du site de succursale communique l'état de connectivité des périphériques de votre site de succursale au contrôleur et l'état de l'alarme pour le site. Lorsqu'un site de succursale est sélectionné, les informations suivantes s'affichent :
  - Résumé du site : est utilisé pour l'analyse et le dépannage.
  - Configurations : est utilisé pour la configuration du site et de l'appareil.
  - Connexions de superposition : est utilisé pour afficher l'état de toutes les connexions VPN superposées.
- La **List (Liste)** vous indique le nombre de sites actifs au cours du **Time Range (Plage horaire)** sélectionné et les indicateurs de qualité globale des sites de la succursale. Le score moyen d'un site médiocre est la moyenne de tous les échantillons médiocres des sites identifiés comme médiocres. Le graphique de la série temporelle est calculé et actualisé en fonction de la durée sélectionnée. Par exemple, les durées prises en charge sont d'une heure, trois heures, 24 heures, sept jours, 30 jours et 90 jours. L'intervalle est d'une minute, de cinq minutes, d'une heure et d'un jour, respectivement.
  - **Site Connectivity Health Distribution (Connectivité du site de distribution de l'intégrité)** : Le graphique de répartition des sites bons, passables et médiocres pour un locataire donné en fonction de la distribution la plus récente de l'intégrité et de la connectivité du site.
  - **Site Connectivity Health Distribution Over Time (Distribution de la qualité de la connectivité des sites au fil du temps)** : Le graphique de la série temporelle du score de qualité des périphériques fonctionnant avec le logiciel 5.6.1 ou une version plus récente.
  - **Site Application Experience Score (Score d'expérience des applications du site)** : Le score d'expérience des applications du site
  - **Prisma SD-WAN Branch Sites (Sites de la succursale Prisma SD-WAN)** : Voir la qualité du site, la qualité de la connectivité du site, la qualité du circuit, la qualité du réseau de distribution, et l' approche du seuil de la capacité d'un site de succursale. Vous pouvez explorer et filtrer davantage un site de succursale par prédiction de site, état d'alarme et état ADEM.

- La vue **Activité** présente les principales analyses d'application, le dernier score d'intégrité du site et la répartition de l'état du site au fil du temps. Il s'agit notamment de :
  - Distribution de l'intégrité du site : affiche le graphique de distribution des sites bons, passables et médiocres pour un locataire donné en fonction du dernier score d'intégrité du site.
  - Distribution de l'intégrité du site au fil du temps : affiche le graphique de série chronologique de la distribution de l'intégrité du site au fil du temps pour un locataire donné en fonction du score d'intégrité d'un site de succursale.
  - Utilisation de la bande passante : affiche l'utilisation de la bande passante de chaque application sur un site et un chemin WAN, avec des données sur les dix applis qui consomment le plus de bande passante sur le réseau.
  - Statistiques de transaction : affiche les statistiques de transaction sur les flux TCP, y compris les réussites et les échecs d'initiation/transaction pour une application spécifique ou toutes les applications, un chemin particulier ou tous les chemins d'accès et tous les événements d'intégrité.
  - Nouveaux flux : affiche les nouveaux flux TCP et UDP d'une application, d'un ensemble spécifique d'applications ou de l'ensemble des applications d'une période donnée.
  - Flux simultanés : vous aide à comprendre combien de connexions sont actives sur votre réseau par application.

Surveiller : Centres de données

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels • Prisma SD-WAN	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro ☐ Prisma SD-WAN Les autres licences et prérequis nécessaires à la visibilité sont : ☐ Observabilité ADEM ☐ DEM autonome pour réseaux distants ☐ ADEM alimenté sur l'IA ☐ Rapport de WAN Clarity ☐ Un rôle qui a l'autorisation d'afficher le tableau de bord → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

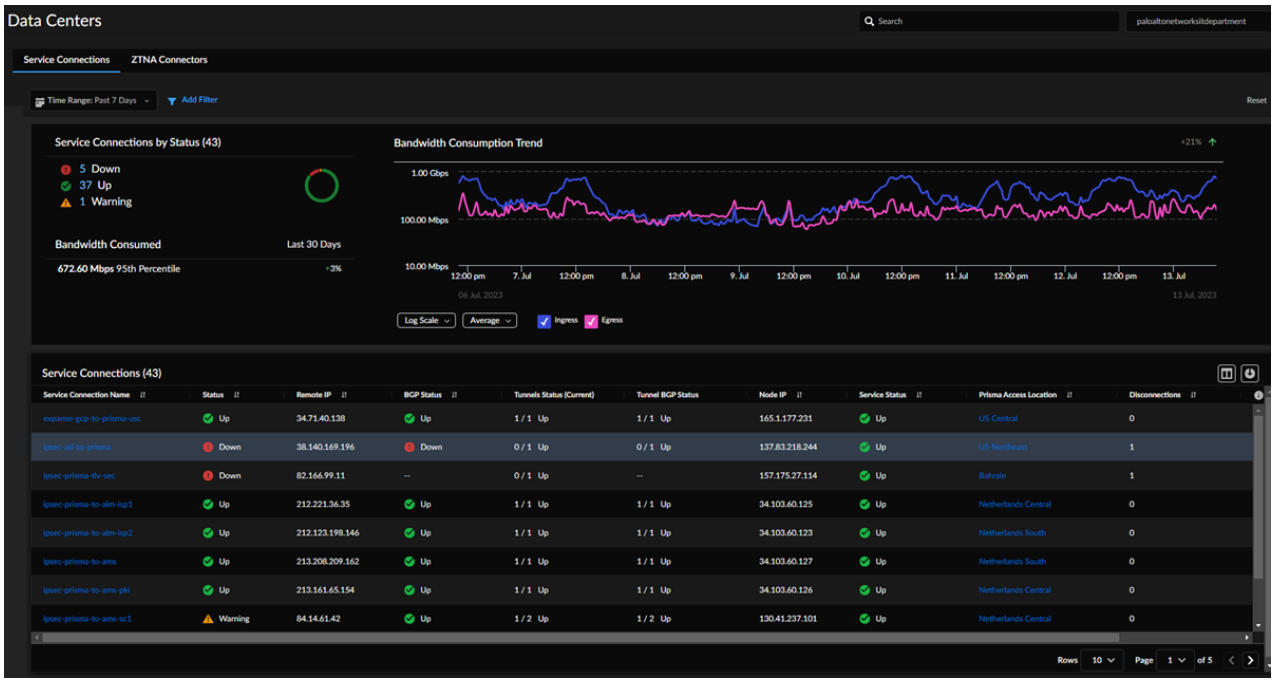
Surveiller les performances des connexions de service, des connecteurs ZTNA et de la connectivité des sites dans les Prisma SD-WAN centres de données. Sélectionnez **Monitor (surveiller)** > **Prisma Access** > **Data Centers (Centres de données)** > **Service de connections (Connexions de service)** ou **ZTNA Connectors (Connecteurs ZTNA)** pour afficher la qualité et l'état des connexions de service et des connecteurs ZTNA dans Prisma Access.

Pour chaque Prisma SD-WAN centre de données, sélectionnez **Monitor (Surveiller)** > **Data Centers (Centres de données)** > **Prisma SD-WAN** pour afficher les informations de connectivité du site et l'état des connexions de superposition VPN.

- Connexions aux services
- Connecteurs ZTNA
- Prisma SD-WAN

Connexions aux services

Sélectionnez **Monitor (Surveiller)** > **Data Centers (Centres de données)** > **Service Connections (Connexions aux services)** pour commencer.



Consultez les données agrégées sur les connexions de service ainsi que les informations sur les connexions de service individuelles. Les connexions aux services sont utilisées à la fois par les utilisateurs mobiles et les réseaux distants. Outre l'accès aux ressources de l'entreprise, les connexions de service permettent à vos utilisateurs mobiles de se rendre dans les succursales. Pour une description détaillée de ces widgets, voir Afficher et surveiller les centres de données dans le *Guide d'administration Prisma Access*.

- Sélectionnez un intervalle de temps pour visualiser les connexions de service par état et leur tendance de consommation de bande passante.
- Affichez la qualité de toutes vos connexions de service.
- Visualisez la tendance de la consommation de bande passante pour toutes vos connexions de service.
- Affichez les données relatives à vos connexions de service, telles que l'état, l'adresse IP distante, l'état BGP, l'état actuel du tunnel et d'autres données. Sélectionnez n'importe quelle connexion de service pour afficher ses détails.

Connecteurs ZTNA

Sélectionnez **Monitor (Surveiller)** > **Data Centers (Centres de données)** > **ZTNA Connectors (Connecteurs ZTNA)** pour commencer.

Le connecteur ZTNA (Zero Trust Network Access) simplifie l'accès aux applications privées pour toutes vos applications. La VM du connecteur ZTNA de votre environnement forme automatiquement des tunnels entre vos applications privées et Prisma Access. Affichez un résumé de tous les connecteurs ZTNA configurés, y compris **Application Targets (Cibles de l'application)** associé au connecteur, sa bande passante moyenne et médiane, et le **Status (État)** (vers le haut, partiellement vers le haut ou vers le bas). Pour une description détaillée de ces widgets, consultez Afficher et surveiller les centres de données dans le *Guide d'administration de Prisma Access*.

Vous pouvez :

- Afficher la qualité et l'état d'un groupe de connecteurs ZTNA.
- Afficher la qualité et l'état de chaque connecteur ZTNA.

Centres de données (Prisma SD-WAN)

Les sites Prisma SD-WAN comprennent les centres de données que vous souhaitez avoir dans votre réseau étendu. Vous avez la possibilité d'héberger des applications et des services d'entreprise dans un centre de données. Dans le cadre de la création d'un centre de données, vous pouvez sélectionner un domaine et un ensemble de politiques par défaut, configurer des réseaux WAN, des catégories de circuits, des étiquettes de circuits et des spécifications de circuit. Le centre de données**Prisma SD-WAN** affiche la liste des centres de données avec le nom du centre de données, le périphérique ION et les alarmes ouvertes pour le site.

Pour un centre de données, vous voyez :

- L'onglet de **Configuration (Configuration)** qui vous indique les informations de connectivité du site, les modes de déploiement, les profils des groupes de référence pour le multicast WAN, l'Internet et les circuits WAN privéset les préfixes IP. Vous pouvez également configurer un agent d'utilisateur et voir les détails de la Configuration du cluster pour le centre de données.
- L'onglet **Overlay Connections (Connexions superposées)** affiche l'état de toutes les connexions superposées VPN. La connectivité de chaque site est calculée en fonction de l'état de ses connexions VPN superposées.

Surveiller : Services du réseau

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels • Prisma SD-WAN	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro ☐ Prisma SD-WAN Les autres licences et prérequis nécessaires à la visibilité sont : ☐ Observabilité ADEM ☐ DEM autonome pour réseaux distants ☐ ADEM alimenté sur l'IA ☐ Rapport de WAN Clarity ☐ Un rôle qui a l'autorisation d'afficher le tableau de bord → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

La page **Monitor (Surveiller)** > **Network Services (services réseau)** , vous permet d'afficher les performances des services réseau courants qui influent sur l'accès aux applications par l'utilisateur. Sélectionnez l'onglet **Authentification GlobalProtect (Authentification de GlobalProtect)** afin d'afficher le nombre de réussites ou d'échecs d'authentification de GlobalProtect à différents niveaux. Sélectionnez **Network Services (Services réseau) : DNS** to see DNS Proxy requests and responses received across tenants with respect to (pour voir les requêtes et les réponses de proxy DNS reçues par les locataires en ce qui concerne) Prisma Access Proxy DNS.

- Authentification GlobalProtect
- DNS

Authentification GlobalProtect

Sélectionnez **Monitor (Surveiller)** > **Network Services (Services réseau)** > **Authentification GlobalProtect (Authentification GlobalProtect)** pour commencer.

Vous pouvez consulter les performances des services réseau courants qui affectent votre expérience utilisateur pour l'accès aux applications dans Insights. Les services réseau incluent la notification pour le nombre de succès et d'échecs liés à l'authentification GlobalProtect. Cette mesure permet d'évaluer la capacité des utilisateurs mobiles à se connecter à Prisma Access. Vous pouvez consulter :

- des précisions relatives au nombre de succès d'authentification pour GlobalProtect pour différents sites.
- le nombre d'échecs d'authentification pour GlobalProtect pour différents sites.
- les échecs du délai d'authentification pour GlobalProtect pour différents sites.

Pour une description détaillée de ces widgets, consultez Afficher et surveiller les services réseau.

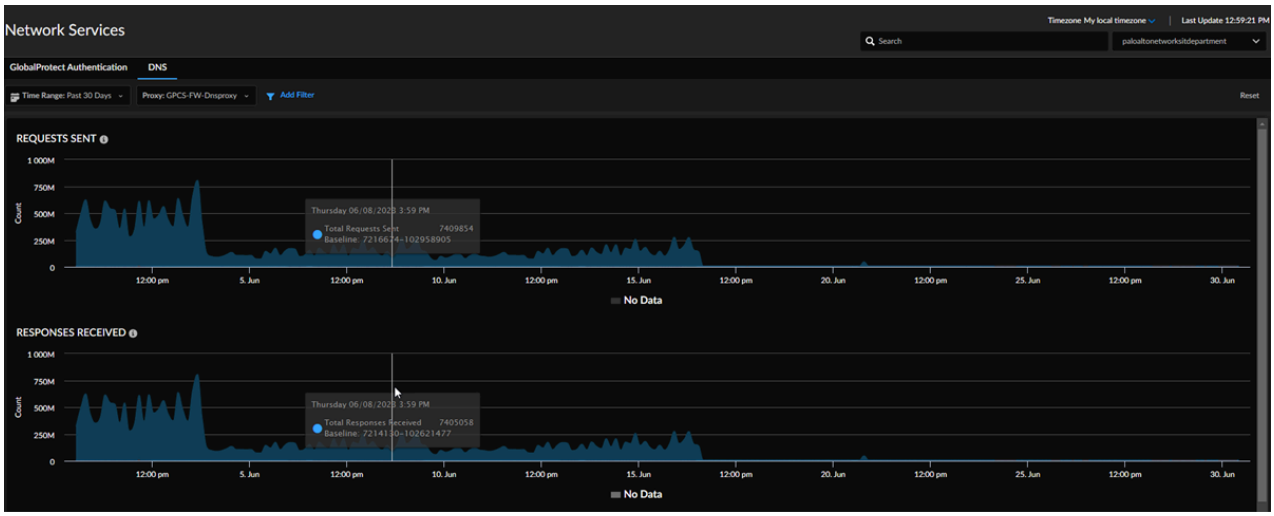
DNS

Sélectionnez **Monitor (Surveiller)** > **Network Services (Services réseau** > **DNS** pour commencer.

Services de réseau : DNS displays DNS Proxy requests and responses (affiche les requêtes et réponses du proxy DNS). Les filtres suivants sont disponibles :

- **Plage horaire**
- **Noms de proxy DNS**

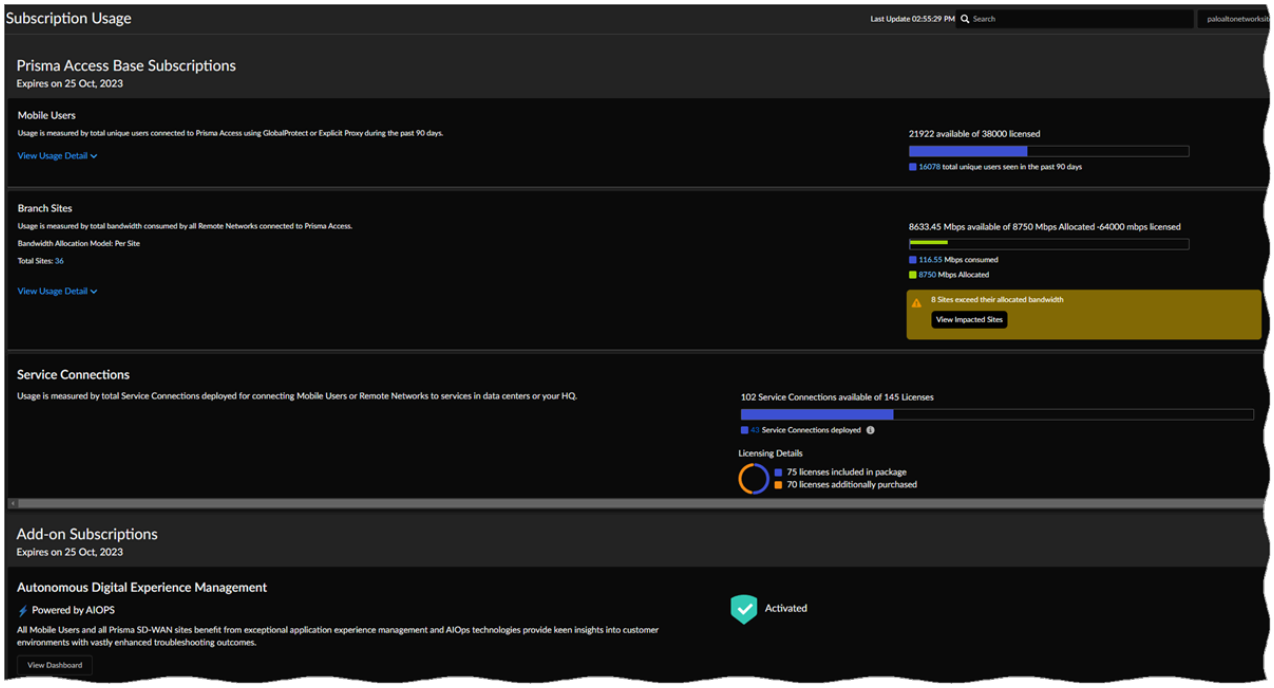
Les valeurs du filtre DNS Proxy sont liées aux 30 derniers jours et sont automatiquement sélectionnées lors du chargement (c'est-à-dire que s'il n'y a pas de données Proxy explicites, les filtres Proxy explicites n'existent pas). Pour des informations plus détaillées, consultez Afficher et surveiller les services réseau.



Surveiller : Utilisation de l’abonnement

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ Licence Prisma Access ❑ AI-Powered ADEM pour débloquer certaines fonctionnalités.

Sélectionnez **Monitor (Surveiller)** > **Subscription Usage (Utilisation des abonnements)** pour afficher les détails de l’utilisation de vos **Prisma Access Base Subscriptions (Abonnements Prisma Access de base)**, notamment le nombre total d’utilisateurs uniques connectés, la bande passante utilisée par les utilisateurs du réseau distant, le nombre total de connexions de service déployées et les détails sur les abonnements complémentaires.



- **Mobile Users (Utilisateurs mobiles)** : Affichez le nombre de licences **Mobile Users (Utilisateurs mobiles)** uniques que vous avez utilisées jusqu’à présent. Le widget affiche le nombre total de licences utilisées par les utilisateurs mobiles uniques connectés auPrisma Access cours des 90 derniers jours, car les licences sont basées sur les données de connexion Prisma Accessdes 90 derniers jours. Un utilisateur qui s’est connecté à Prisma Access au moins une fois au cours des 90 derniers jours contribue à l’utilisation d’une licence d’Utilisateur mobile.
- **Branch Sites (Sites des succursales)** : Consultez l’utilisation totale de la bande passante consommée par tous les réseaux distants connectés à Prisma Access. Affichez la quantité de bande passante que vous avez allouée et celle que vous avez utilisée, en Mbits/s. Vous voyez l’utilisation de la bande passante totale utilisée par tous les réseaux distants connectés à Prisma Access.

- **Subscriptions Usage (Utilisation des abonnements)** : Découvrez combien de licences **Service Connections (Connexions aux service)** vous avez utilisées jusqu'à présent.

Consultez la section **Add-on Subscriptions (Abonnements complémentaires)** sur cette page pour voir les licences supplémentaires que vous avez achetées, telles que les licences **Autonomous Digital Experience Management (Gestion de l'expérience numérique autonome)** pour les Utilisateurs mobiles et les Réseaux distants. Vous pouvez voir le nombre total de licences achetées ainsi que le nombre de licences non utilisées jusqu'à présent. Affichez **Application Tests for Mobile User Monitoring (Tests d'application pour la surveillance des Utilisateurs mobiles)** : le nombre de tests d'application restants que vous pouvez créer pour vos Utilisateurs mobiles. Les tests d'application sont déterminés par le nombre d'utilisateurs mobiles surveillés, avec un maximum de 10 tests d'application autorisés par Utilisateur mobile.

Pour plus d'informations, consultez Afficher et surveiller l'utilisation de l'abonnement.

Surveiller : Périphériques ION

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma SD-WAN	❑ Licence Prisma SD-WAN

Les périphériques ION de Prisma SD-WAN vous permettent de combiner des réseaux WAN disparates, tels que MPLS, LTE et des liaisons Internet, en un seul réseau étendu (WAN) hybride et haute performance.

L'écran **Device List (Liste des périphériques)** fournit des informations sur la liste des périphériques Prisma SD-WAN, y compris la version logicielle et l'état du périphérique ION, où vous pouvez mettre à niveau la version logicielle du périphérique ou configurer un périphérique.

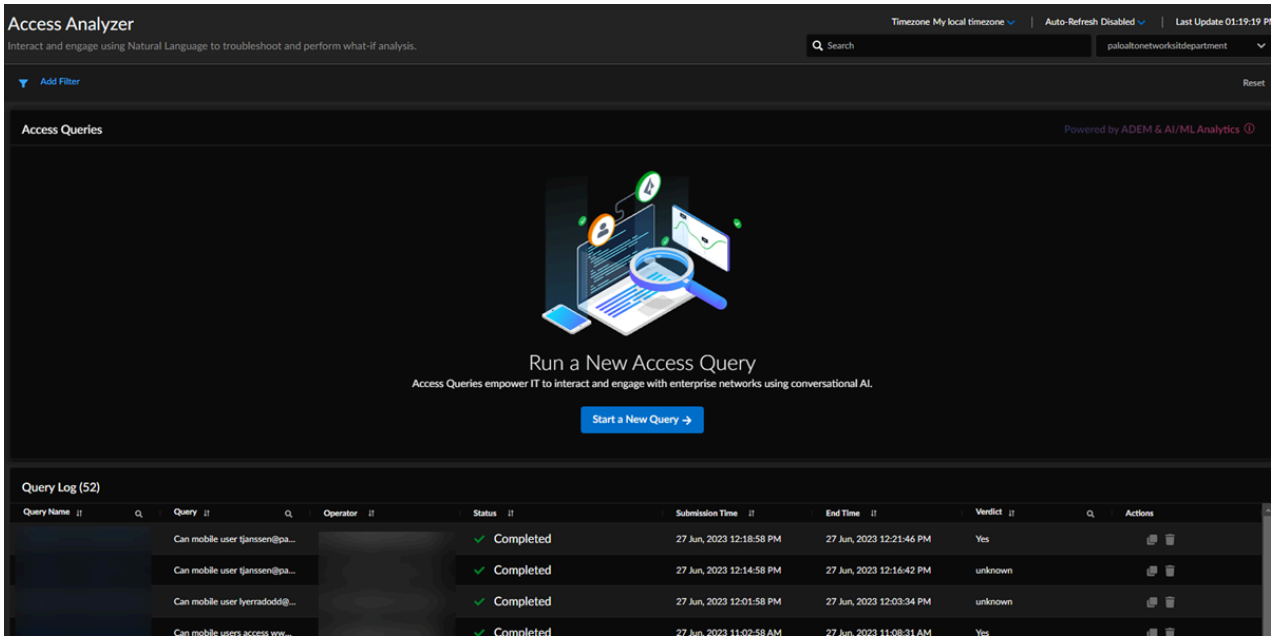
Entité	Description
Nom du périphérique	Affiche le nom configuré pour le périphérique ION.
Informations sur le périphérique	Affiche le type et le numéro de série du périphérique ION.
Logiciels	Affiche la version actuelle du logiciel du périphérique. Cliquez sur **Upgrade (Mettre à niveau)** pour modifier la version du logiciel du périphérique.
Dernière activité	Affiche des informations sur la date de la dernière configuration et de la dernière mise à niveau du périphérique ION.
État	Affiche l'état actuel du périphérique ION.
Redondance	S'affiche si le périphérique ION fait partie d'une configuration High Availability (haute disponibilité - HA).
Actions	Vous pouvez choisir de configurer le périphérique ION à partir du menu ellipse.

L'écran **Device Activity (Activité du périphérique)** affiche divers rapports d'activité du périphérique pour un site au cours des dernières 24 heures.

Surveiller : Analyseur d’accès

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ Licence Prisma Access ❑ Licence AI-Powered ADEM

Sélectionnez **Monitor (Surveiller)** > **Access Analyzer (Analyseur d’accès)** pour démarrer une nouvelle requête Analyseur d’accès et afficher un tableau des requêtes existantes.



L’analyseur d’accès fournit une surveillance automatique de votre environnement SASE. Cette solution offre un outil d’IA conversationnel pour le dépannage contextuel et l’analyse des hypothèses afin d’analyser les problèmes d’accès et de connectivité dans votre environnement SASE.

Vous pouvez :

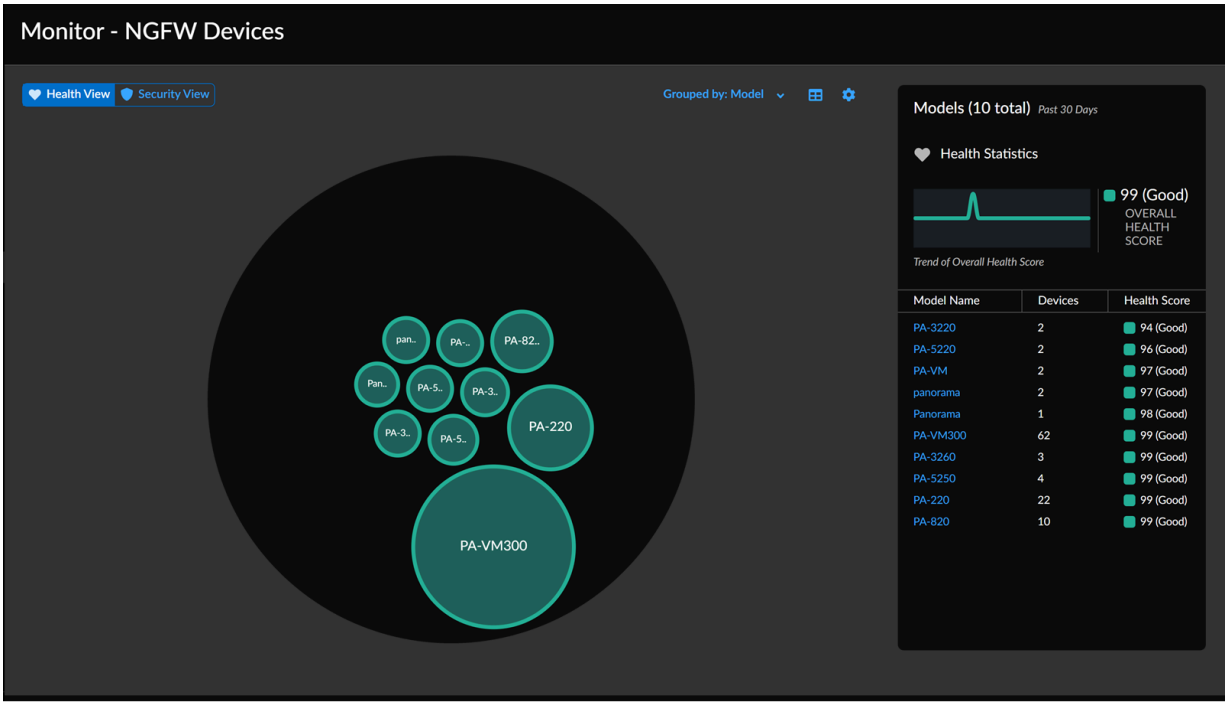
- Apprendre à créer une requête en langage naturel dans Analyseur d’accès.
- Démarrer une nouvelle requête Access Analyzer.
- Consultez la liste des requêtes existantes et sélectionnez l’une d’entre elles dans le tableau pour obtenir plus de détails.

Surveiller : Périphériques NGFW

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ AIOps for NGFW Free (use the AIOps for NGFW Free ap ou AIOps for NGFW Premium license (use the Strata Cloud ❑ Crédits NGFW logiciels *(pour les logiciels VM-Series NGFW)*

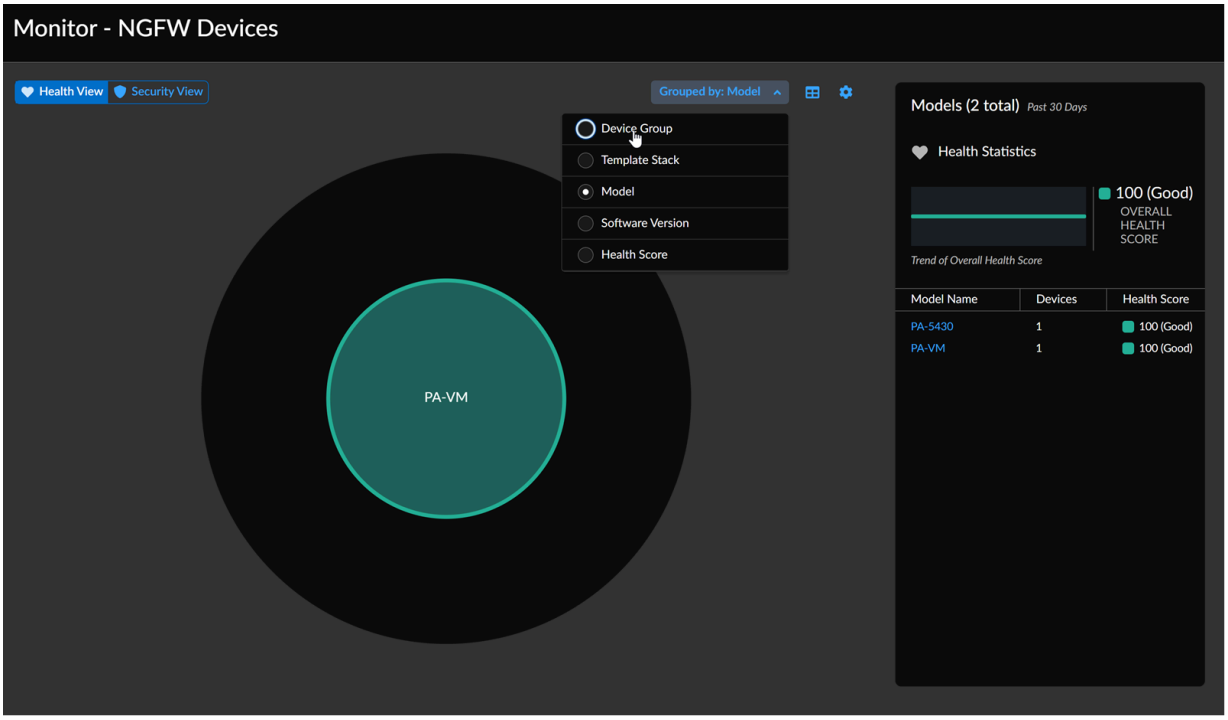
Dans **Monitor (Surveiller)** > **NGFW Devices (Périphériques NGFW)**, vous pouvez obtenir une représentation interactive à code couleur des périphériques de votre déploiement pour une gestion et une enquête faciles et intuitives.

STEP 1 | Sélectionnez **Monitor (Surveiller)** > **NGFW Devices (Périphériques NGFW**.



STEP 2 | Sélectionnez **Health (Santé)** ou **Security (Sécurité)**.

STEP 3 | Sélectionnez l'attribut par lequel vous souhaitez que la visualisation soit **Grouped by (Groupée)**.



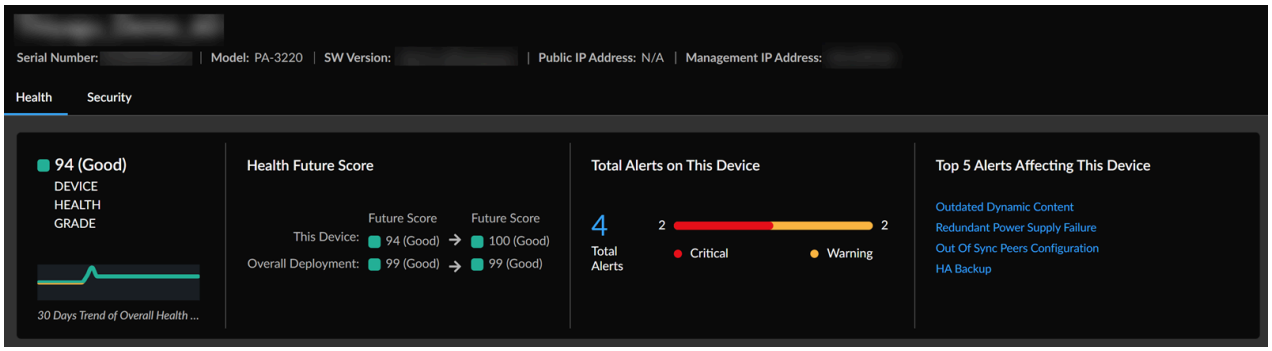
*Les options de regroupement **Device Group (Groupe de périphériques)** et **Template Stack (Pile de modèles)** ne sont disponibles que dans les déploiements gérés par Panorama où Panorama envoie la télémétrie des périphériques.*

STEP 4 | Sélectionnez un groupe pour afficher les périphériques qu'il contient et sélectionnez un périphérique pour afficher des informations générales le concernant.

Si vous souhaitez en savoir plus sur un périphérique, sélectionnez-le.

Afficher les détails du périphérique

En sélectionnant un périphérique dans la visualisation **NGFW Devices (Appareils NGFW)** ou en suivant un lien ailleurs dans l'appli, vous pouvez afficher des détails spécifiques sur un pare-feu ou un appareil Panorama, tels que le niveau de qualité, les métriques, les connexions, etc.



Niveau de santé du périphérique

L’état actuel du périphérique et un graphique montrant son historique au cours des 30 derniers<x> jours. Les niveaux de qualité possibles sont Bon, Moyen, Mauvais et Critique.

Classe de santé après correction

L’état du périphérique après avoir répondu aux alertes ouvertes. Cette mosaïque vous indique également l’état de votre déploiement global après la fermeture des alertes.

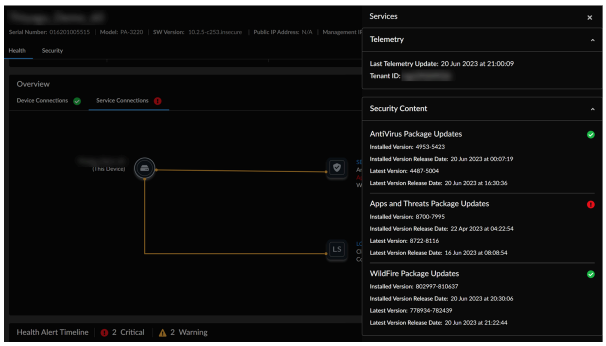
Nombre total d’alertes

Le nombre total d’alertes ouvertes sur le périphérique.

Les 5 principales alertes

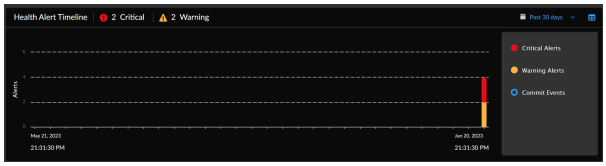
Les cinq alertes les plus courantes sur ce périphérique au cours des 30 derniers jours.

Présentation > Connexions des périphériques Les autres périphériques connectés à celui que vous regardez actuellement. Sélectionnez un périphérique pour afficher ses détails.	
Aperçu > Connexions de service Un aperçu de tous les services de sécurité et de journalisation intégrés à ce périphérique. Sélectionnez un service pour accéder à ses détails.	



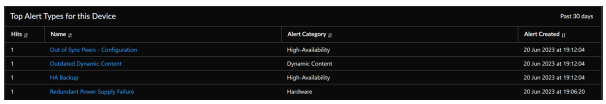
Chronologie des alertes

Une chronologie des alertes de périphérique et des événements de validation. Les alertes sont classées en tant qu'événements critiques, d'avertissement ou de validation. Basculer pour afficher les données d'alerte au format tableau.



Les principaux types d'alertes pour ce périphérique

Les alertes les plus courantes au cours des 30 derniers jours. Sélectionnez une alerte pour en afficher les détails.



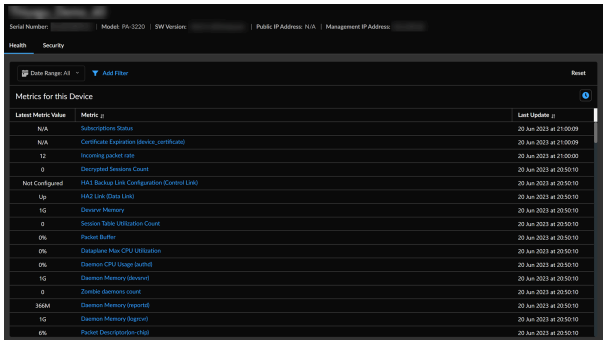
Les 10 principales applications à utiliser

Les dix applications utilisant le plus de données sur le pare-feu.

Mesures pour ce périphérique

Une liste de toutes les mesures de qualité collectées pour les contrôles de sécurité exécutés sur le périphérique, y compris les données de liaison HA.

Sélectionnez une métrique pour afficher ses détails.



Surveiller : Analyseur de capacité

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW	☐ AIOps for NGFW Premium ou Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

L'Analyseur de capacité vous permet d'analyser et de surveiller la capacité des ressources de vos appareils en suivant l'utilisation de leurs métriques en fonction de leurs types de modèles. L'analyseur de capacité offre les avantages suivants :

- Une compréhension complète de l'utilisation des métriques existantes et de la capacité de métrique inutilisée jusqu'à la limite maximale.
- Une visualisation de carte thermique qui présente l'utilisation des mesures par rapport aux plateformes matérielles dans une vue unique et permet d'approfondir les détails.
- La possibilité de planifier la mise à niveau vers des pare-feux de plus grande capacité en fonction de vos besoins spécifiques.

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

Voici une vidéo qui montre comment utiliser la fonctionnalité Analyseur de capacité :

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 notifications en temps opportun. Les alertes de l'analyseur de capacité sont générées 3 mois à l'avance et identifient les goulets d'étranglement potentiels. Cela vous permet de planifier le nettoyage de la configuration ou d'augmenter les capacités NGFW avant qu'elles n'atteignent leur utilisation maximale et de maintenir la stabilité du système. Voir Alertes de santé premium pour la liste des alertes de capacité prises en charge.

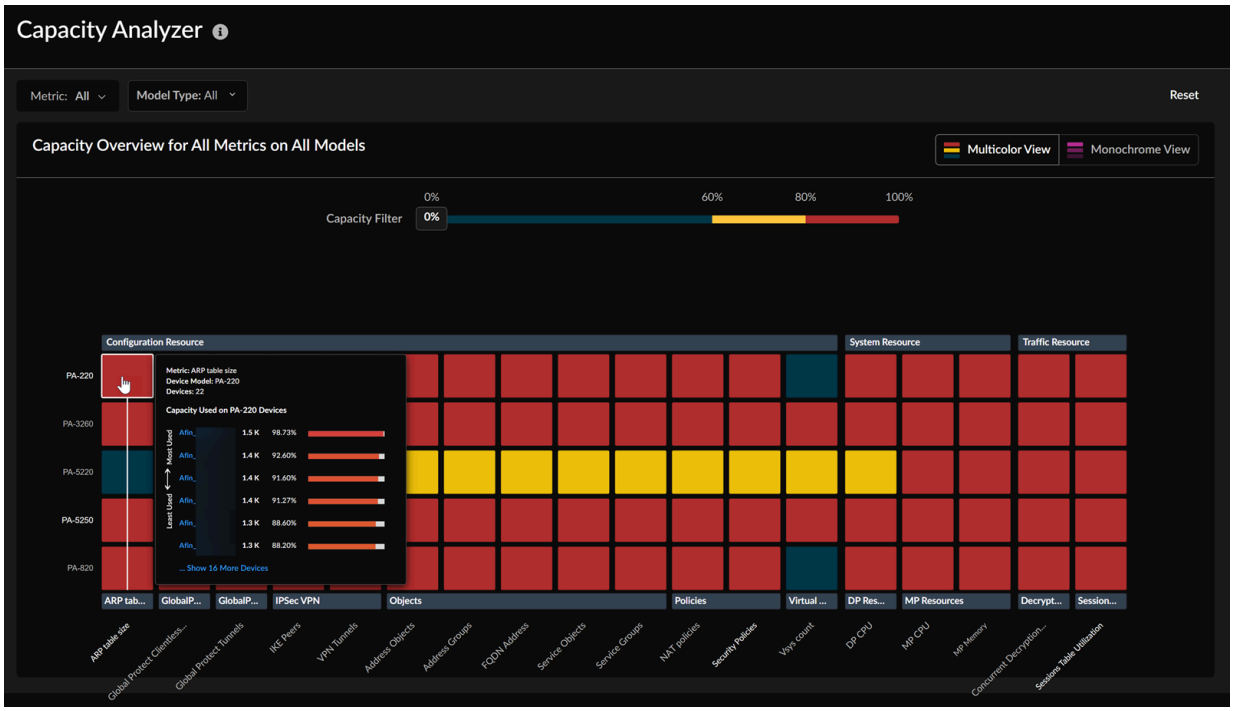
L'analyseur de capacité regroupe les métriques en fonction des types suivants :

- Métriques de ressources de configuration telles que les stratégies NAT et les objets d'adresse.
- Métriques de ressources opérationnelles du système telles que le processeur, la mémoire, les disques et les journaux.
- Métriques de ressources de trafic telles que l'utilisation du décryptage et l'utilisation de la table de session.

La carte thermique affiche l'utilisation des métriques pour chaque périphérique. La couleur la plus foncée représente une utilisation plus élevée et la couleur plus claire indique une utilisation plus faible. Par défaut, **Multicolor View (Vue multicolore)** est sélectionnée. Vous pouvez aussi passer à l'icône **Monochrome View (Vue monochrome)**.

Ci-après, sont énumérées les différentes façons d'utiliser la carte thermique de l'analyseur de capacité pour obtenir des informations sur l'utilisation des métriques :

- Passez votre curseur sur un bloc de métrique d'un appareil pour afficher une info-bulle qui fournit les détails suivants :
  - Nom de la métrique
  - Modèle du périphérique et liste des périphériques
  - Plage de capacité de l'appareil



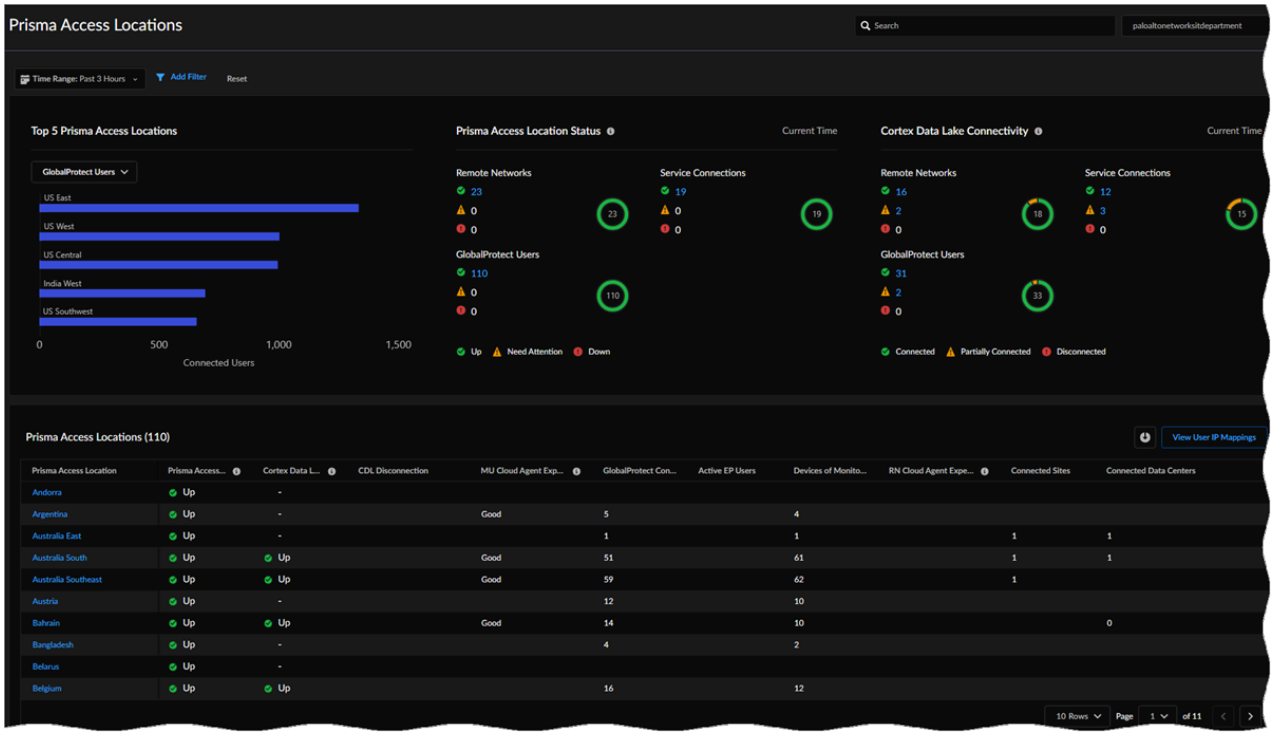
- Filtrez les données à l'aide des attributs suivants :
  - **Metric (Métrique)** : sélectionnez une ou plusieurs métriques que vous souhaitez afficher ou rechercher à l'aide du nom de la métrique.
  - **Model (Modèle)** : sélectionnez un ou plusieurs modèles d'appareils ou effectuez une recherche à l'aide du nom du modèle.
  - **Capacity (Capacité)** : sélectionnez la capacité sur le **Capacity Filter (Filtre de capacité)** écaille.

Pour en savoir plus sur l'utilisation de la carte thermique de l'analyseur de capacité, consultez la section Analyser la capacité des métriques.

Surveiller : Emplacements Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ Licence Prisma Access Il s'agit d'une fonctionnalité Prisma Access Insights.

Sélectionnez **Monitor (Surveiller)** > **Prisma Access Locations (Emplacements Prisma Access)** pour commencer. À partir de là, vous pouvez voir l'état de tous vos sites Prisma Access pour vos réseaux distants et vos utilisateurs mobiles. Pour une description détaillée de ces widgets, consultez Afficher et surveiller les emplacements Prisma Access dans le *Guide d'administration Prisma Access*.

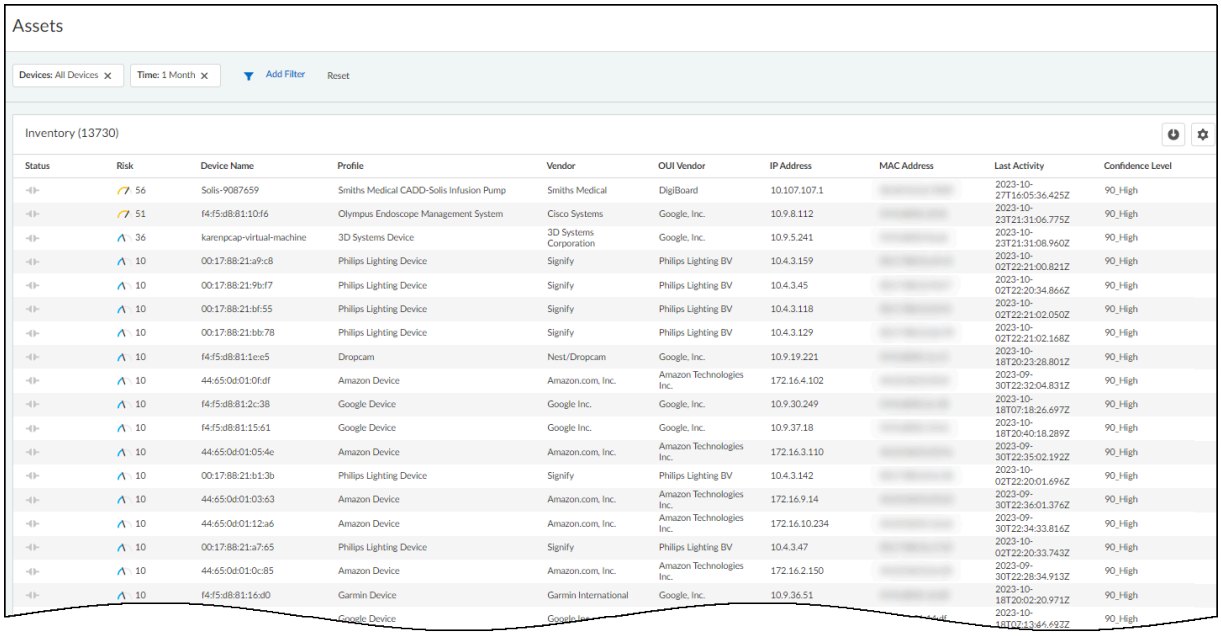


- Consultez les 5 principaux emplacements de Prisma Access pour les réseaux distants, les connexions de service, les utilisateurs mobiles GlobalProtect ou les utilisateurs mobiles de Proxy explicite en fonction de la bande passante totale consommée.
- Consultez l'état de vos emplacements Prisma Access.
- Consultez la Strata Logging Service connectivité.
- Affichez le tableau d'emplacements Prisma Access, qui répertorie tous les emplacements Prisma Access, et sélectionnez un Emplacement Prisma Access individuel par son nom pour afficher ses détails.

Surveiller : Ressources

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ Abonnement IoT Security ❑ Crédits NGFW logiciels *(pour les logiciels VM-Series NGFW)*

Pour commencer, sélectionnez **Surveiller > actifs**. À partir de là, vous pouvez voir un inventaire géré de manière dynamique des périphériques IoT, OT et IT sur votre réseau avec de nombreux attributs pour chacun d'entre eux, tels que ses adresses IP et MAC ; profil, fournisseur, modèle et système d'exploitation ; et (pour les produits de sécurité IoT avancés) son score de risque au niveau du périphérique.



Utilisez les données de cet inventaire pour connaître les actifs de votre réseau :

- Affichez un inventaire généré de dynamiquement et à jour des périphériques détectés sur votre réseau, y compris les périphériques IoT, OT et IT.
- Alors que le tableau de bord IoT affiche les types de périphériques que vous avez à un niveau élevé, l'inventaire des ressources vous permet d'explorer des périphériques individuels pour voir plus de détails et évaluer leur posture de sécurité.
- Filtrez les données affichées dans le tableau de bord par site, type de périphérique, période et un ou plusieurs attributs de périphériques pour afficher les données sur les périphériques qui vous intéressent.
- Affichez et masquez les colonnes pour afficher les attributs des périphériques qui sont importants pour vous. Il y a plus de 100 colonnes d'attributs parmi lesquelles choisir.

- Téléchargez les données affichées sur la page actuellement active sous forme de fichier au format CSV pour les inclure dans les rapports ou pour référence future. Le fichier contient les périphériques et les attributs de périphériques que vous avez affichés au moment du téléchargement.

Incidents et alertes : Strata Cloud Manager

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels • Prisma SD-WAN	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ☐ Prisma SD-WAN ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro Les autres licences et prérequis nécessaires à la visibilité sont : ☐ Un rôle qui a l'autorisation d'afficher le tableau de bord → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

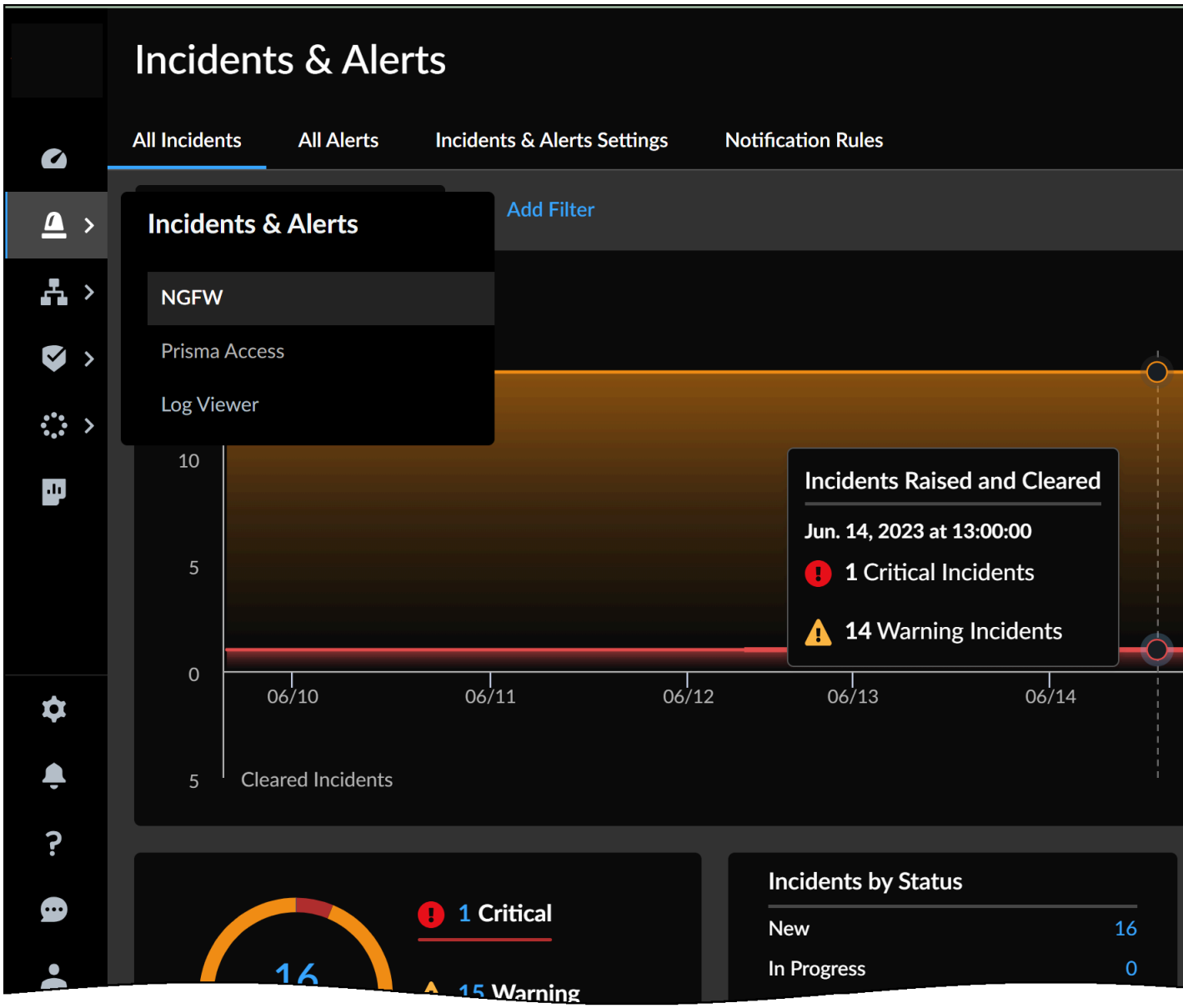
Strata Cloud Manager vous offre un cadre commun permettant d'interagir et d'enquêter sur les incidents et les alertes des Produits et abonnements Palo Alto Networks détectés dans votre entreprise :

- Incidents et alertes : NGFW
- Incidents et alertes : Prisma Access
- Incidents et alertes : Prisma SD-WAN

Afin de vous aider à maintenir l'état actuel de vos périphériques et déploiements, et pour éviter toute interruption de votre activité, explorez chacune des pages réservées aux incidents et aux alertes pour :

- visualiser les incidents et les alertes sur l'ensemble de votre réseau et effectuer des recherches approfondies ; et
- créer et réviser les règles qui déclenchent les notifications des incidents et des alertes.

Vous pouvez passer de vos incidents et alertes et le Incidents et alertes : Visionneuse de journaux pour examiner l'activité sur votre réseau qui se déclenche ou qui est associée à des incidents et des alertes.



Incidents et alertes : NGFW

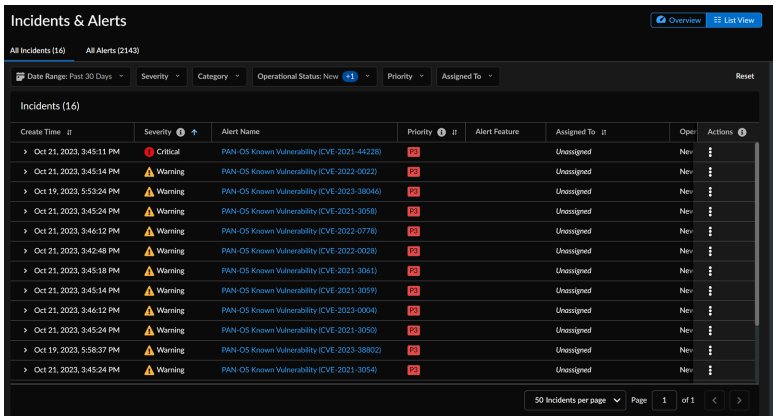
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ L'une des licences suivantes : ❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) ou AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro

Pour vous aider à maintenir l'état de vos périphériques et à éviter les incidents qui perturbent votre activité, vos applications génèrent des incidents et des alertes en fonction d'un ou plusieurs problèmes qu'elles ont détectés lors du déploiement de votre pare-feu. Avec **Incidents & Alerts (Incidents et alertes)** > **NGFW**, vous obtenez une vue unique de vos incidents et alertes sur les NGFW.

Voici comment être opérationnel avec **NGFW Incidents & Alerts (Incidents et alertes NGFW)** :

- Les incidents vous signalent les vulnérabilités. Vous pouvez les examiner et prendre des mesures préventives si nécessaire.

  Accédez à **Incidents & Alerts (Incidents et alertes)** > **NGFW (Pare-feu de nouvelle génération)** > **Tous les incidents** pour visualiser les incidents sur l'ensemble de votre réseau et interagir avec eux.



- Une alerte indique un problème particulier (dégradation ou perte de fonctionnalité du pare-feu) qui doit être résolu. Des alertes peuvent également être générées sur la base d'une corrélation ou d'une agrégation de plusieurs événements. Cette agrégation des événements en une seule

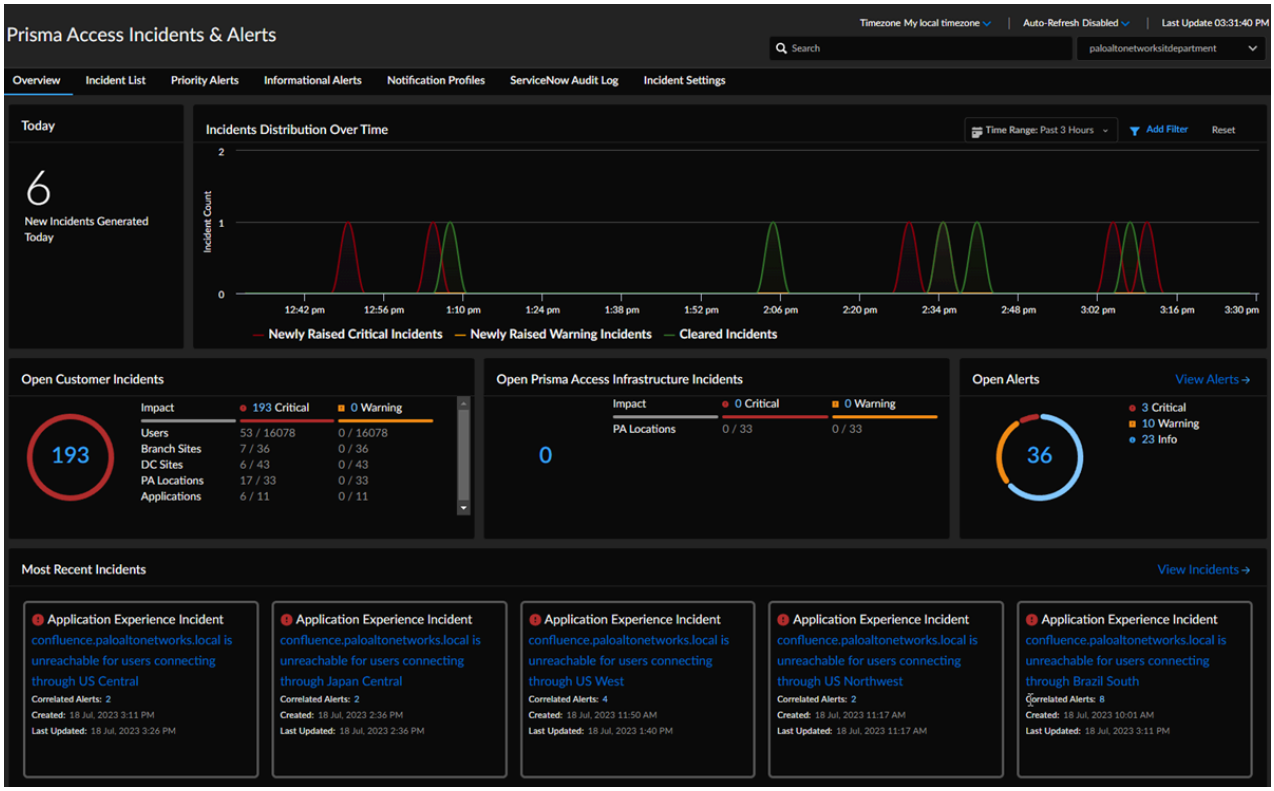
alerte facilite le triage, rationalise le transfert des alertes entre les équipes, centralise les informations critiques et réduit la fatigue liée aux notifications.

Accédez à **Incidents & Alerts (Incidents et alertes)** > **NGFW (Pare-feu de nouvelle génération)** > **Toutes les alertes** pour afficher les alertes sur votre réseau et interagir avec elles.

Incidents et alertes : Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ Licence AI-Powered ADEM ❑ Licence ADEM Observability ❑ Licence Prisma Access

Sélectionnez **Incidents & Alerts (Incidents et alertes)** > **Prisma Access Incidents & Alerts (Incidents et alertes Prisma Access)** pour commencer. Les incidents et les alertes accessibles dans votre environnement dépendent de vos licences.



Obtenir un aperçu

Consultez un Aperçu des informations sur les incidents et les alertes liés à votre environnement Prisma Access. Les incidents et les alertes accessibles dans votre environnement dépendent de vos licences.

Voir tous les incidents

Affichez la liste des incidents, qui indiquent tous les incidents dans votre environnement. Utilisez le menu déroulant **Add Filter (Ajouter un filtre)** drop-down pour sélectionner Incidents par les colonnes du tableau (vous pouvez filtrer sur plusieurs). Dans le tableau, sélectionnez un **Incident (incident)** pour afficher ses informations détaillées.

Visualisez les alertes prioritaires

Consultez Alertes prioritaires, qui décrivent l'état de votre environnement Prisma Access.

Visualisez les alertes d'information

Consultez les alertes d'informations, qui vous informent des mises à jour logicielles en cours et de l'état d'avancement des mises à jour en cours ou terminées.

Profils de notification

À partir des Profils de notification, vous pouvez afficher des informations sur les **Notification Subscriptions (Abonnements de notification)** et créer un nouveau **Notification Profile (Profil de notification)** ou le modifier.

Journal d'audit ServiceNow

Si vous utilisez ServiceNow, vous pouvez consulter le journal d'audit ServiceNow, qui affiche chaque **Incident ID (ID d'incident)** ServiceNow. Il indique également les opérations ServiceNow effectuées sur chaque incident, telles que la création, la mise à jour et la suppression.

Paramètres d'incident

À partir des Paramètres d'incident, vous pouvez personnaliser les incidents que vous recevez par catégorie d'incident et par code d'incident.

Incidents et alertes par code

Consultez les incidents et les alertes en fonction de leur code d'identification, comprenez les problèmes et les questions qu'ils décrivent et découvrez comment y remédier. Les incidents et les alertes sont classés par licence :

- Incidents ADEM alimentés par l'IA
- Incidents ADEM
- Incidents Prisma Access
- Alertes prioritaires
- Alertes d'information

Afin d'obtenir des renseignements sur les incidents et les alertes, consultez le Guide de référence sur les incidents et les alertes.

Pour plus d'informations sur l'intégration de ServiceNow, voir Intégrer ServiceNow à Prisma Access dans le *Guide d'intégration*.

Incidents et alertes : Prisma SD-WAN

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma SD-WAN	❑ Licence Prisma SD-WAN

Prisma SD-WAN génère des incidents et des alertes lorsque le système atteint des seuils définis par le système ou par le client ou lorsque le système présente des défaillances. Utilisez ces incidents et alertes pour assurer le dépannage du système.

Sélectionnez **Incidents and Alerts (Incidents et alertes)** > **Prisma SD-WAN** pour afficher les incidents et alertes dans Strata Cloud Manager.

Utilisez les onglets suivants pour parcourir les incidents et les alertes dans Prisma SD-WAN.

- Vue d'ensemble
- Incidents
- Alertes
- Paramètres

Vue d'ensemble

Consultez les incidents et alertes et leurs catégories dans Prisma SD-WAN. L'onglet **Overview (Aperçu)** est votre vue par défaut.

Consultez les principaux incidents et alertes qui affichent les informations suivantes.

Type d'incident	Affiche la catégorie de l'incident.
Description	Affiche la description de l'incident.
Sévérité	Affiche le niveau de gravité de l'incident.
Priorité	Affiche la priorité de l'incident.
Alertes corrélées	Affiche le nombre d'incidents agrégés dans cet incident.
État	Affiche l'état de l'incident.
Créé	Affiche la date à laquelle l'incident a été signalé par le système.
Dernière mise à jour	Affiche la date de la dernière mise à jour de l'incident par le système.

Incidents

Un incident indique une défaillance dans le système. Les incidents sont signalés et neutralisés et leur gravité varie :

- Critique : tout ou une partie d'un réseau est en panne et nécessite une action rapide.
- Avertissement : impacte le réseau et nécessite une attention rapide.
- Informationnel : le réseau est dégradé et nécessite une attention rapide.

Alertes

Une alerte peut être ou non l'indication d'une défaillance dans le réseau. Une alerte est déclenchée lorsqu'un seuil défini par le système ou par le client est atteint.

Paramètres

Utilisez l'onglet **Settings (Paramètres)** pour créer des stratégies d'incident afin de gérer la suppression de code d'événement en fonction des classifications et des attributs d'action spécifiés configurés. Des règles de politique d'incident permettent de supprimer ou d'intensifier les incidents qui surviennent au cours d'une période programmée. En outre, vous pouvez également modifier la priorité par défaut des incidents générés par le système pour un niveau de priorité qui correspond mieux aux besoins de votre entreprise.

Incidents et alertes : Visionneuse de journaux

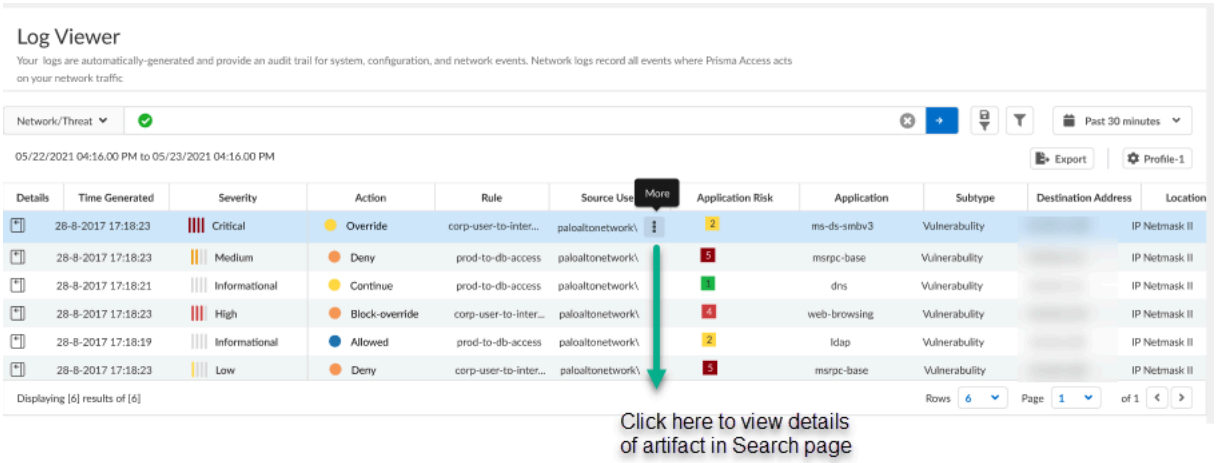
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ou AIOps for NGFW Free (use the AIOps for NGFW Free app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Un rôle qui a l'autorisation d'afficher le tableau de bord

Log Viewer (Visionneuse de journaux) offre les capacités d'explorer : où vous pouvez afficher et interagir avec vos journaux stockés dans Strata Logging Service.

Log Viewer (Visionneuse de journaux) fournit une piste d'audit pour les événements système, de configuration et de réseau. Passez d'un tableau de bord à vos journaux afin d'obtenir des détails et examiner les résultats. Un champ d'interrogation et des préférences en matière d'intervalle de temps vous permettent d'affiner les journaux spécifiques qui vous intéressent.

- En savoir plus sur la façon de construire vos requêtes
- Découvrez les nouvelles fonctionnalités de Log Viewer dans les Strata Logging ServiceNotes de mise à jour.

Log Viewer (Visionneuse de journaux) met en évidence les actions et la gravité des journaux pour vous aider à comprendre comment les sessions sont appliquées. Vous pouvez également afficher les détails des artefacts de sécurité des journaux dans la page Rechercher.



* Vous pouvez afficher les détails dans la recherche pour les types de journaux et les champs de journaux suivants :

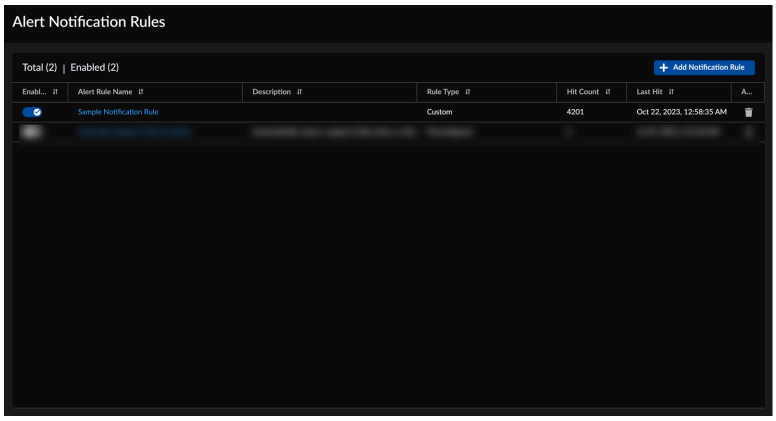
Type de journal	Nom de colonne
Trafic, Menace, URL, Fichier	• Adresse source • Adresse de destination • Source NAT • Destination NAT
Menace, Fichier	Hachage de fichier
URL	• URL • Domaine d'URL
Sécurité DNS	• Adresse source • Adresse de destination • Domaine • Nom de domaine complet

Paramètres des incidents et des alertes

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ AIOps for NGFW Free (use the AIOps for NGFW Free app) ou AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro

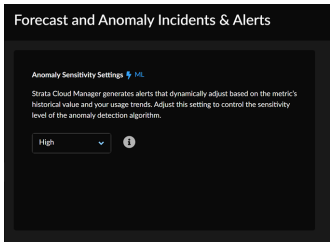
- Les préférences de notification, telles que les alertes susceptibles de déclencher des notifications, la manière dont vous recevez les notifications et la fréquence à laquelle vous les recevez, sont définies dans une règle de notification.

  Accédez à **Incidents & Alerts (Incidents et alertes)** > **Incident & Alert Settings (Paramètres des incidents et des alertes)** > **Règles de notification** pour afficher et ajouter des règles permettant de déclencher des notifications.



- Strata Cloud Manager génère des alertes et des incidents adaptés de manière dynamique en fonction de la valeur historique de la mesure et de vos tendances d'utilisation. Cette option permet de contrôler le niveau de sensibilité de l'algorithme de détection des anomalies.

  Accédez à **Incidents & Alerts (Incidents et alertes)** > **Incident & Alert Settings (Paramètres des incidents et des alertes)** > **Anomaly Sensitivity (Sensibilité aux anomalies)** pour configurer le niveau de sensibilité de l'algorithme de détection des anomalies.

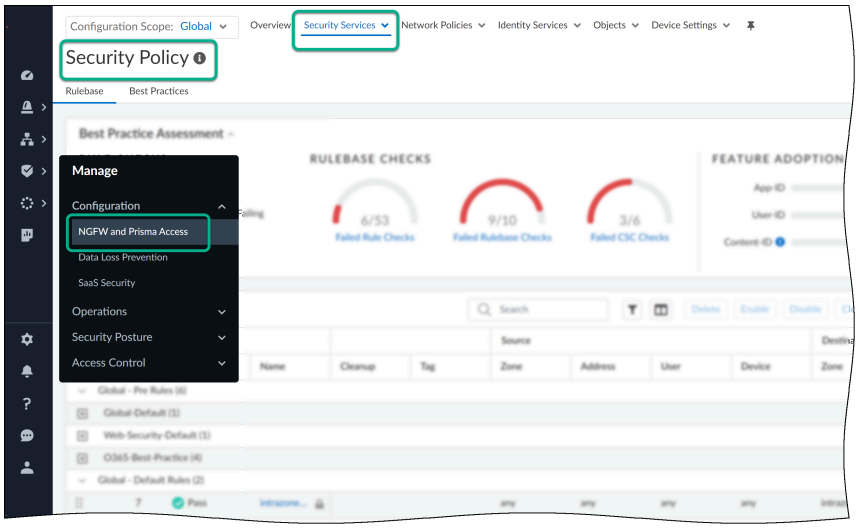


Gestion : NGFW et Prisma Access

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Strata Cloud Manager vous permet de configurer une politique de sécurité partagée entre vos pare-feu de nouvelle génération et Prisma Access. pour commencer :

- ❑ Configurez Prisma Access, vos NGFW, ou les deux avec Strata Cloud Manager
- ❑ Configurez des dossiers pour regrouper les pare-feu de nouvelle génération (NGFW) qui nécessitent des paramètres similaires. Les dossiers Prisma Access sont prédéfinis, et vous permettent de cibler la configuration en fonction du type de déploiement : utilisateurs mobiles, réseaux distants, connexions de service.
- ❑ Réglez l'icône Gestion : Portée de la configuration dans lequel vous voulez travailler. Vous pouvez configurer des paramètres qui s'appliqueront à l'échelle mondiale, à la fois à vos NGFW et à votre environnement Prisma Access, et vous pouvez également cibler la configuration sur des NGFW spécifiques ou des déploiements Prisma Access en fonction des dossiers Flux de travail : Gestion des dossiers.
- ❑ Utilisez Gestion : Extraits pour normaliser une configuration de base commune pour un ensemble de NGFW ou de déploiements. Les extraits de code vous permettent d'intégrer rapidement de nouveaux périphériques, utilisateurs ou emplacements avec une configuration dont la configuration a été vérifiée et de réduire le temps nécessaire à l'intégration d'un nouveau périphérique.
- ❑ Atteindre **Manage (Gérer)** > **Configuration (Configuration)** > **NGFW and Prisma Access (Accès NGFW et Prisma)** pour commencer à créer votre politique de sécurité et à la partager entre vos NGFW et Prisma Access à l'aide des fonctionnalités de gestion décrites ci-dessus.



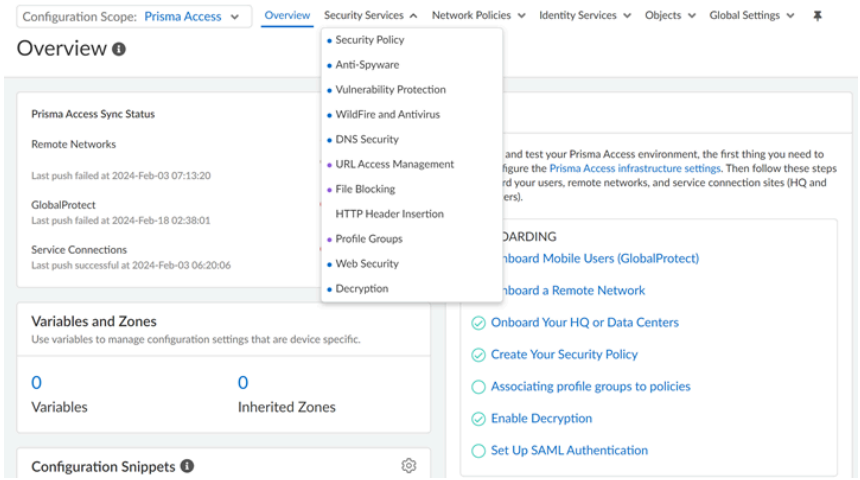
Gestion : Portée de la configuration

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Avec Strata Cloud Manager, vous pouvez appliquer des paramètres de configuration et appliquer une politique à l'échelle globale à l'ensemble de votre environnement, ou cibler les paramètres et la politique à certaines parties de votre organisation. Lorsque vous travaillez dans votre gestion de la configuration Strata Cloud Manager, **Configuration Scope (Étendue de la configuration)** en cours est toujours visible pour vous, et vous pouvez basculer votre vue pour gérer une configuration plus large ou plus granulaire.

Vous pouvez obtenir des précisions sur les éléments de configuration applicables à un champ de configuration particulier et savoir s'ils sont hérités d'un champ de configuration commun ou s'ils sont générés par le système. Les indicateurs de configuration codés par couleur vous aident à comprendre d'où les configurations sont héritées et distinguent visuellement les types d'objets pour faciliter la lecture.

- Le point gris montre la configuration héritée
- Le point violet indique une configuration prédéfinie
- Le point bleu indique que l'objet est présent dans la zone de configuration actuelle



Les paramètres de configuration **globaux** vous permettent de gérer et d'appliquer facilement les exigences de politiques qui s'appliquent à l'ensemble de votre trafic réseau. Vous pouvez également cibler les paramètres de politique et de configuration en fonction des types de déploiements pour lesquels ils sont utiles.

- **Prisma Access**
  - **Conteneur d'utilisateurs mobiles** : les paramètres s'appliquent à tous les types de connexion des utilisateurs mobiles : GlobalProtect et Explicit Proxy, ou individuellement à chaque type de connexion.
  - **Réseaux distants** : les paramètres s'appliquent aux sites réseau distants (filiales, points de vente, etc.).
  - **Connexions de service** ; les paramètres s'appliquent aux sites de connexion de service (siège et centres de données).
- **Tous les pare-feu** : les paramètres s'appliquent à tous vos NGFW, ou à des dossiers spécifiques qui regroupent les NGFW qui nécessitent des paramètres de configuration partagés ou spécifiques ou l'application de politiques.

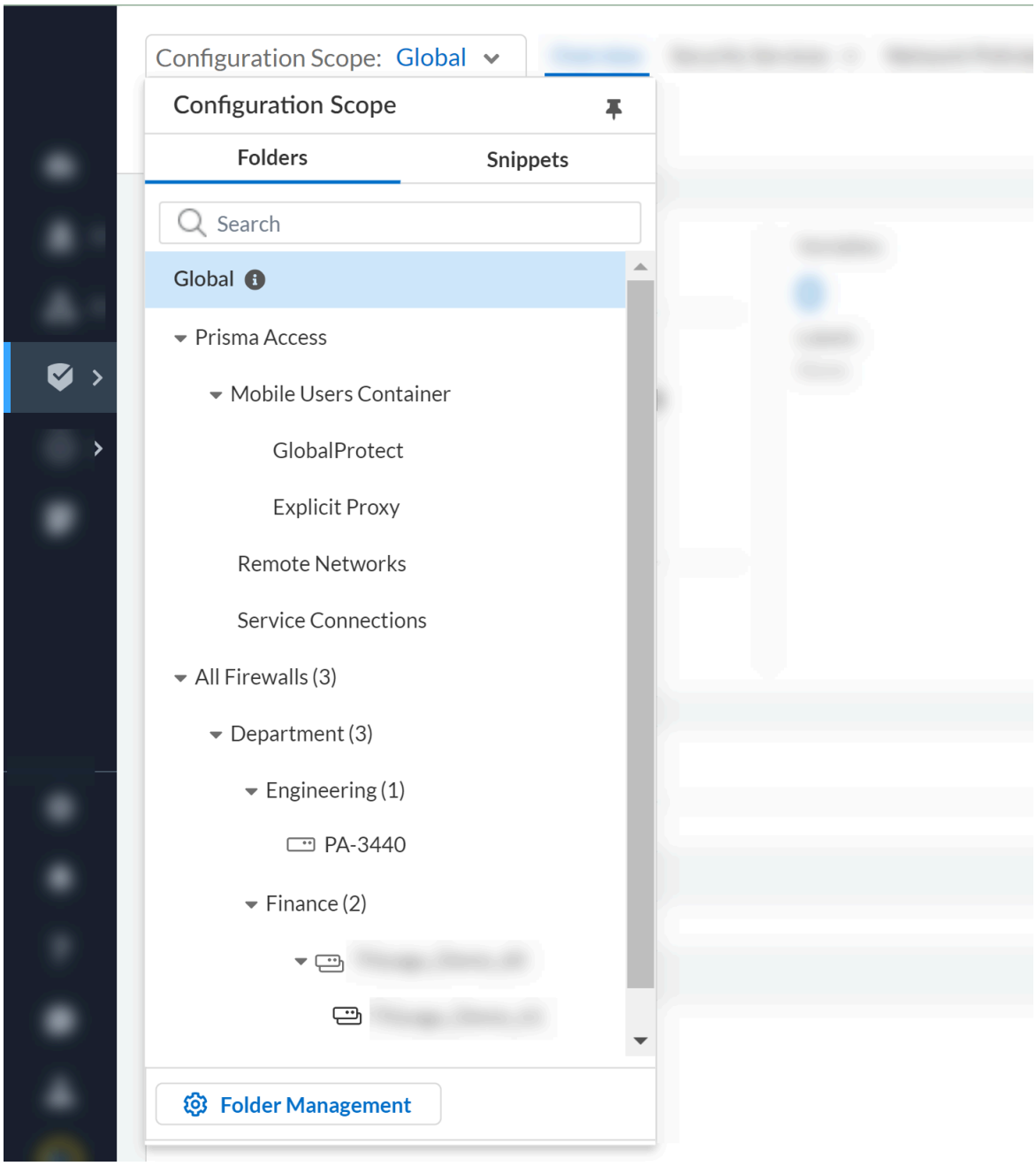
En savoir plus sur :

- **Flux de travail : Gestion des dossiers**

  Utilisez des dossiers pour regrouper logiquement vos périphériques et vos types de déploiement afin de simplifier la gestion de la configuration.
- **Gestion : Extraits**

  Utilisez des extraits de code pour regrouper les configurations que vous pouvez rapidement envoyer à vos pare-feu ou déploiements.
- **Gestion : Variables**

  Utilisez des variables dans vos configurations pour prendre en charge les objets de configuration spécifiques au périphérique ou au déploiement.



Gestion : Extraits

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium ☐ Strata Cloud Manager Essentials

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

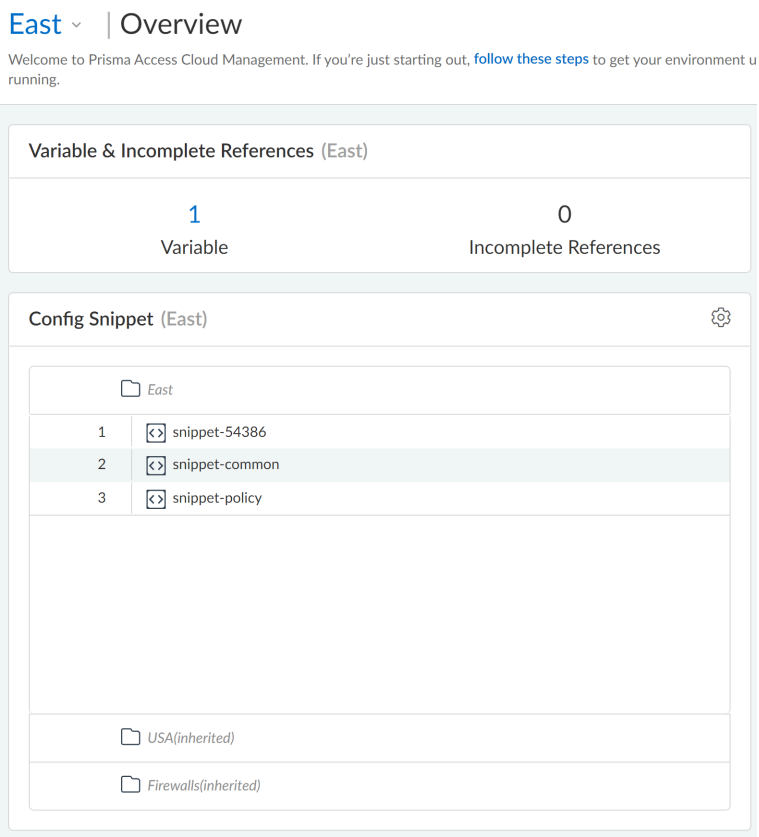
Utilisez les extraits pour regrouper les configurations que vous pouvez rapidement intégrer à vos pare-feux ou à vos déploiements.

Un extrait est un objet de configuration qui ne peut s'inscrire dans une hiérarchie ou un groupement d'objets de configuration que vous pouvez associer à un dossier, à un déploiement ou à un périphérique. Les extraits sont utilisés pour normaliser une configuration de base commune pour un ensemble de pare-feux ou de déploiements, ce qui permet d'intégrer rapidement de nouveaux périphériques avec une bonne configuration connue et de réduire le temps nécessaire à l'intégration d'un nouveau périphérique. Par exemple, vous pouvez installer un nouveau pare-feu dans une succursale distante. Vous pouvez associer un ensemble d'extraits contenant toutes les configurations de règles de réseau et de politique nécessaires au dossier auquel appartient le nouveau pare-feu. Cela permet de réduire le temps nécessaire à la configuration du pare-feu pour protéger la succursale distante.

Les associations d'extraits ont une priorité descendante en cas de conflit de valeurs d'objets. Les règles avec des noms en double ne sont pas autorisées et la validation échoue lors de la création d'un extrait portant le même nom dans n'importe quel dossier ou lors de l'association d'un extrait à un dossier si l'extrait portant le même nom est déjà associé.

Cela signifie que si le premier et le dernier extrait associé ont des valeurs différentes pour le même objet, la valeur du premier extrait est héritée par le périphérique ou le déploiement. De plus, toutes les configurations héritées d'un extrait peuvent être remplacées au niveau du sous-dossier, du déploiement ou du périphérique.

Au sein d'une hiérarchie de dossiers, un extrait peut n'être associé qu'une seule fois dans une hiérarchie de dossiers. Cela signifie qu'un extrait ne peut pas être associé à la fois à un dossier et au dossier qui lui est rattaché. Toutefois, vous pouvez associer le même extrait à différents dossiers ou à des dossiers imbriqués dans d'autres dossiers. Les extraits qui sont déjà associés à un dossier dans la hiérarchie des dossiers sont grisés de sorte qu'il ne puissent pas être utilisés plus d'une fois, le cas échéant.



Référencement de la configuration transversale dans les extraits

Cette fonctionnalité vous permet de référencer toutes les configurations ou objets communs attachés à une portée globale et de les pousser vers Prisma Access et les pare-feux NGFW. Ces objets et configurations partagés dans le cadre global sont disponibles pour tous les extraits. Un extrait associé à la portée globale est considéré comme un extrait global. Les objets définis dans ces extraits attachés à la portée globale peuvent être référencés dans tous les extraits de la configuration.

Par exemple, vous pouvez créer un extrait nommé Variable globale pour consolider les variables et l'attacher à une portée globale. Cela permet de faciliter le référencement et la disponibilité de tous les autres extraits de la configuration. De même, vous pouvez gérer efficacement les catégories d'URL personnalisées pour les règles de politique d'accès, les profils de prévention des menaces, les zones, les adresses et d'autres objets représentant des segments de réseau standard.

Créer un extrait

Créez et associez un extrait à un dossier, un déploiement ou un périphérique pour appliquer une configuration de base commune à un groupe de périphériques. Vous pouvez associer autant d'extraits que nécessaire à un dossier, un déploiement ou un périphérique.

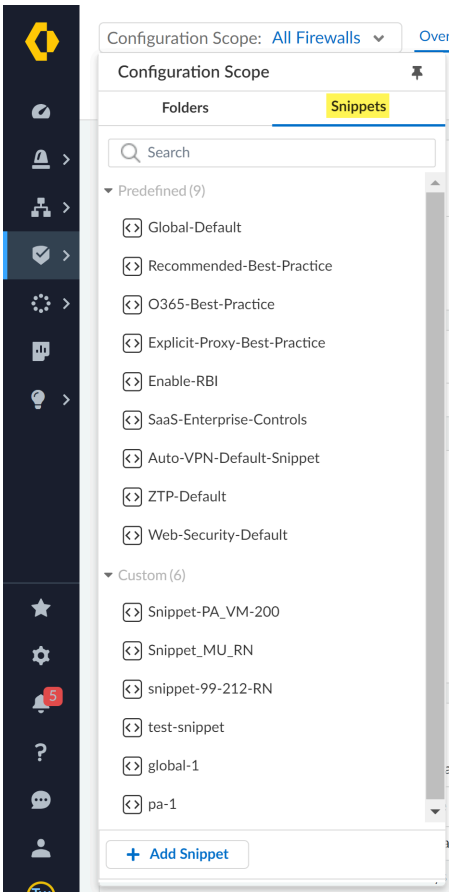
Les extraits peuvent être modifiés et réassociés à n'importe quel dossier, déploiement ou périphérique à tout moment après leur création.

Les extraits personnalisés qui ne sont plus utilisés peuvent être supprimés.

STEP 1 | Se connecter à Strata Cloud Manager.

STEP 2 | Sélectionnez **Manage (Gestion)** > **Configuration (Configuration)** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Overview (Aperçu)** et développez l'étendue de configuration pour afficher les **Snippets (Extraits)**.

STEP 3 | **Add Snippet (Ajouter un extrait).**

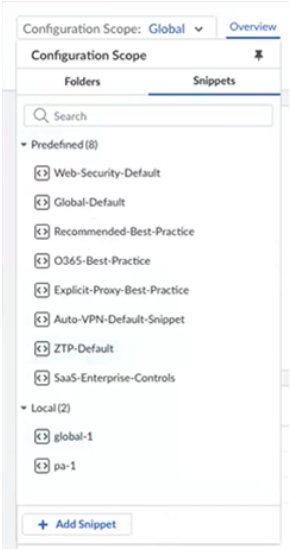


STEP 4 | Créez les extraits.

1. Donnez à l'extrait un **Name (Nom)** descriptif.
2. (Facultatif) Saisissez une **Description** pour l'extrait.
3. (Facultatif) Attribuer une ou plusieurs **Labels (Étiquettes)**.

   Vous pouvez sélectionner une étiquette existante ou en créer une nouvelle en saisissant l'étiquette que vous souhaitez créer.
4. **Créer**.

   Les extraits nouvellement créés sont classés dans la catégorie Extraits **Local (Locaux)**. Une fois les extraits publiés, ils sont déplacés sous extraits publiés.



STEP 5 | Créez votre configuration d'extrait.

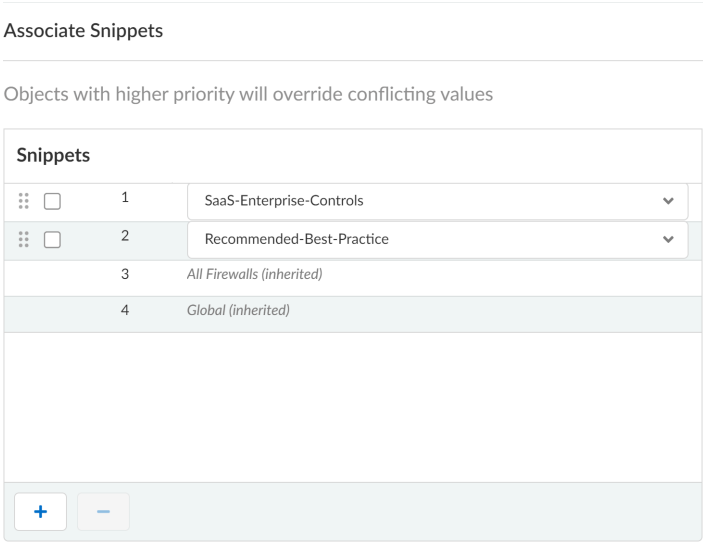
Vous vous trouvez à présent dans le champ de configuration de l'extrait. Toutes les configurations que vous créez dans le champ d'application de l'extrait ne s'appliquent qu'à cet extrait.

Lorsque vous êtes dans le champ d'application de l'extrait, vous pouvez consulter **Overview (Aperçu)** de l'extrait pour obtenir des informations détaillées sur l'extrait. Cela inclut des informations telles que le nombre de variables, des informations sur la création et la dernière mise à jour de l'extrait, ainsi que la liste de tous les dossiers, déploiements et périphériques auxquels l'extrait est associé.

STEP 6 | Associez un extrait.

1. Sélectionnez **Manage (Gestion)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Overview (Aperçu)** et développez la portée de configuration pour afficher l'**Config Tree (Arborescence de configuration)**.
2. Sélectionnez le dossier, le déploiement ou le périphérique auquel vous souhaitez associer l'extrait.
3. Modifiez l'**Config Snippet (Extrait de configuration)**.
4. Ajoutez les extraits que vous souhaitez associer et classez-les selon vos besoins.

   Si vous associez un extrait à la portée globale, il devient référençable et disponible pour tous les autres extraits de la configuration. Tous les extraits pourront faire référence aux objets que vous avez dans l'extrait attaché au dossier global.
5. **Close (Fermer)**.



STEP 7 | **Push Config (Transmettre la configuration)** pour transmettre vos modifications de configuration sur votre réseau.

Modifier un extrait

Modifiez les configurations, les détails et les associations de vos extraits.

Les extraits personnalisés qui ne sont plus associés à un dossier, un déploiement ou un périphérique peuvent être supprimés.

STEP 1 | Se connecter à Strata Cloud Manager.

STEP 2 | Sélectionnez **Manage (Gestion)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Overview (Aperçu)** et développez la portée de configuration pour afficher les **Snippets (Extraits)**.

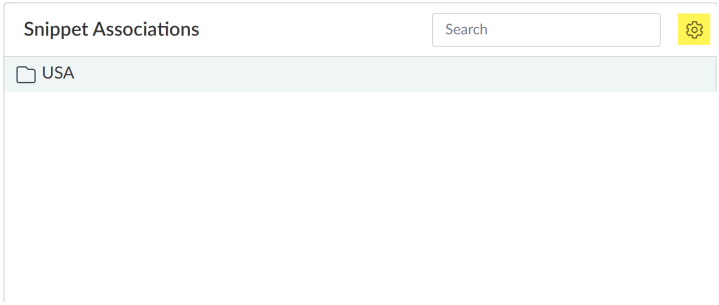
STEP 3 | Sélectionnez l'extrait que vous souhaitez modifier.

Après avoir sélectionné un extrait, vous êtes redirigé vers **Overview (Aperçu)** de l'extrait.

STEP 4 | (Facultatif) Modifiez l'extrait pour modifier le **Name (Nom)**, **Description**, ou pour changer ou assigner des **Labels (Étiquettes)** supplémentaires. Activez ou désactivez **Pause Update (Mettre en pause)** pour voir les différences de configuration et décider d'accepter la modification.

STEP 5 | Modifiez les **Snippet Associations (Associations d'extrait)** pour réassocier l'extrait à un dossier, déploiement ou périphérique différent ou pour associer l'extrait à des dossiers, déploiements ou périphériques supplémentaires.

Quittez la fenêtre de réintégration des extraits pour appliquer les modifications.



STEP 6 | Apportez les modifications nécessaires à la configuration des extraits.

STEP 7 | **Push Config (Transmettre la configuration)**.

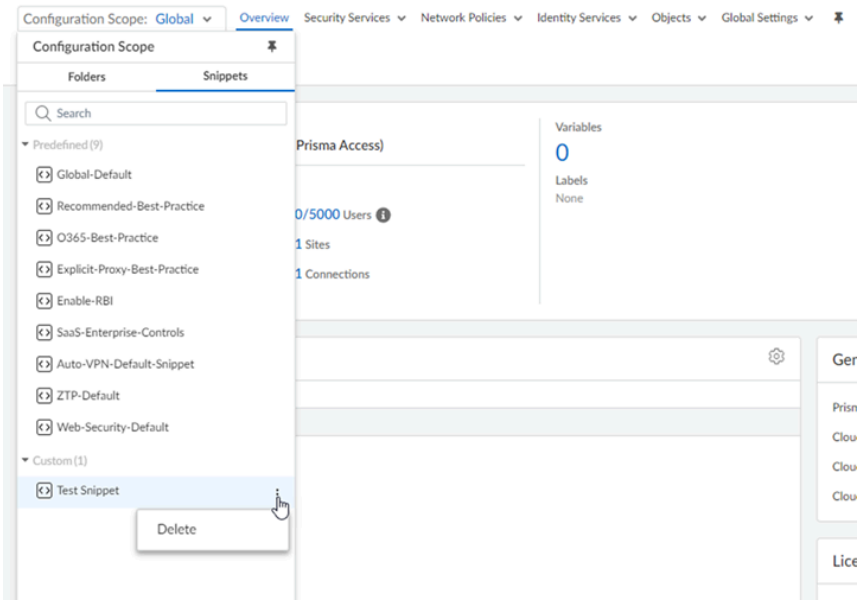
Supprimer un extrait

Supprimez vos extraits personnalisés pour garder vos configurations organisées. Les extraits doivent être dissociés de tout pare-feu, dossier ou déploiement avant de pouvoir être supprimés. La suppression des extraits prédéfinis n'est pas possible.

STEP 1 | Se connecter à Strata Cloud Manager.

STEP 2 | Sélectionnez **Manage (Gestion)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Overview (Aperçu)** et développez la**Configuration Scope (Portée de configuration)** pour afficher les extraits.

STEP 3 | Cliquez sur les trois points verticaux de l'extrait personnalisé que vous souhaitez supprimer.



STEP 4 | **Delete (Supprimer)** l'extrait.

> *Les extraits actuellement associés à des dossiers, déploiements ou périphériques ne peuvent pas être supprimés. Modifiez d'abord les **Snippet Associations (Associations d'extrait)** pour supprimer toutes les associations existantes avant qu'il puisse être supprimé.*

Cloner un extrait

Si vous souhaitez utiliser un extrait existant comme modèle pour un nouvel extrait, vous pouvez facilement le cloner afin de ne pas avoir à configurer un nouvel objet.

Les extraits clonés ne sont associés à aucun périphérique, dossier ou déploiement, ce qui vous permet de les personnaliser librement sans avoir à les dissocier avant de commencer vos configurations.

STEP 1 | Se connecter à Strata Cloud Manager.

STEP 2 | Sélectionnez **Manage (Gestion)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Overview (Aperçu)** et développez la**Configuration Scope (Portée de configuration)** pour afficher les extraits.

STEP 3 | Cliquez sur les trois points verticaux de l'extrait personnalisé que vous souhaitez cloner.

STEP 4 | **Clone (cloner)** l'extrait.

1. (Facultatif) Donnez un nouveau nom à l'extrait cloné.

Partager une configuration d'extrait

Cette fonctionnalité offre une méthode unique et flexible pour partager des configurations communes entre tous les locataires, y compris dans un environnement multilocataire. Vous pouvez enregistrer et gérer diverses configurations sous forme d'extraits, et les partager

facilement entre les locataires d'un même compte client. Cette capacité offre une flexibilité et un contrôle considérables dans la gestion des configurations partagées entre les différents environnements des locataires.

En outre, cette fonctionnalité prend en charge la gestion centralisée de la configuration pour les scénarios courants parmi les locataires et la supervision des configurations globales au sein d'une configuration d'unité multi-métier.

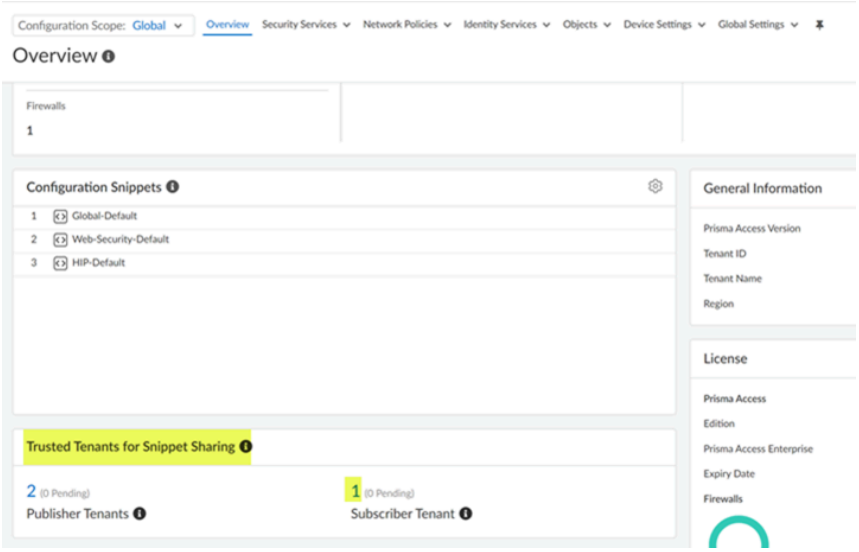
Dans ce cadre, le locataire éditeur partage des extraits avec le locataire abonné, tandis que le locataire abonné reçoit des extraits du locataire éditeur.

STEP 1 | Se connecter à Strata Cloud Manager.

STEP 2 | Sur le locataire de l'éditeur, sélectionnez **Manage (Gestion)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Overview (Aperçu)**, sélectionnez la portée de configuration **Global (globale)**.

STEP 3 | **Établir la confiance entre les locataires** : Établir une connexion entre les locataires abonnés et éditeurs afin de permettre le partage des extraits.

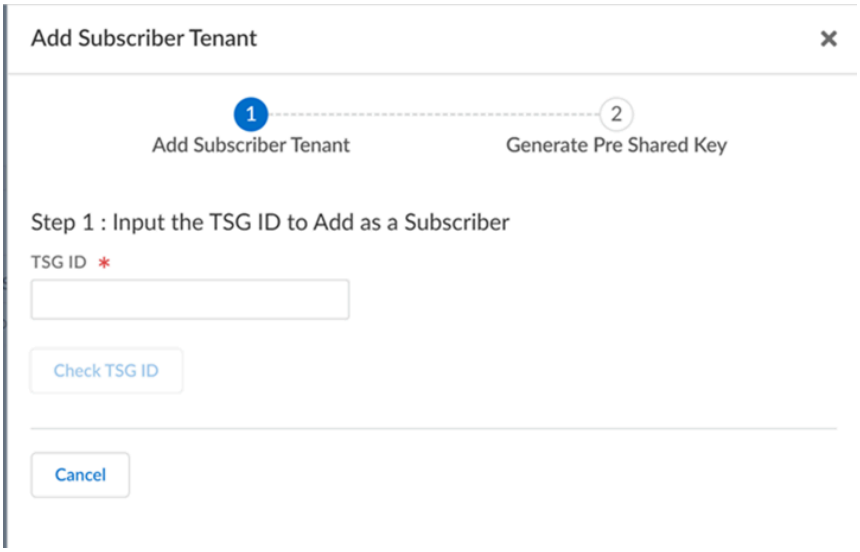
1. Cliquez sur **Subscriber Tenant (Locataire abonné)** sous **Locataires de confiance pour le partage des extraits (Trusted Tenants for Snippet Sharing)**.



2. **Add Subscriber Tenant (Ajouter un locataire abonné)**

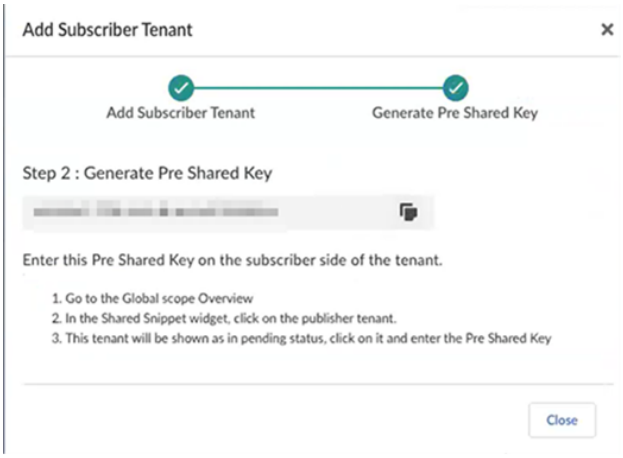
3. Entrez l'**TSG ID (ID TSG)** à ajouter en tant que locataire abonné, et **Check TSG ID (Vérifier l'ID TSG)**. Cela permet d'éviter les attaques basées sur des STG générées de manière aléatoire ou sérialisées.

   Une fois la validation réussie, un message de confirmation indique que l'ID TSG a été vérifié.



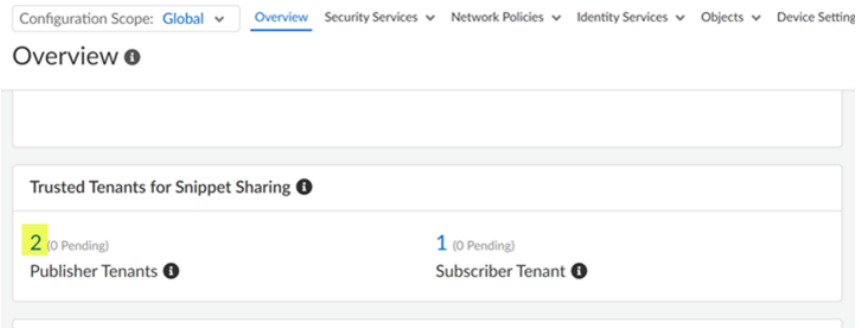
4. **Ensuite : Générer la clé pré partagée**.

   Copier le PSK généré. Vous saisirez ce PSK lors de la validation du locataire de l'éditeur à l'étape 4.



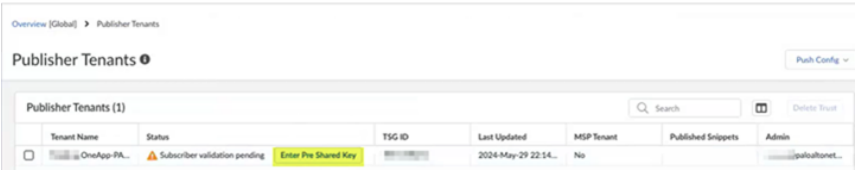
STEP 4 | Allez dans locataire abonné, sélectionnez **Manage (Gestion)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Overview (Aperçu)** et définissez l'étendue de configuration sur **Global (Global)**.

1. L'état **Publisher Tenants (Locataires éditeurs)** sous **Trusted Tenants for Snippet Sharing (Locataires de confiance)** pour le partage d'extraits s'affiche comme **Pending (En attente)**.



2. Cliquez sur **Publisher Tenants (Locataires éditeurs)** et **Enter Pre Shared Key (Entrez la clé prépartagée)**générée à l'étape précédente, puis **Validate (Validez)** le locataire abonné.

   Après validation réussie, un message confirme que le locataire est digne de confiance, établissant ainsi la confiance entre l'abonné et les locataires éditeurs.



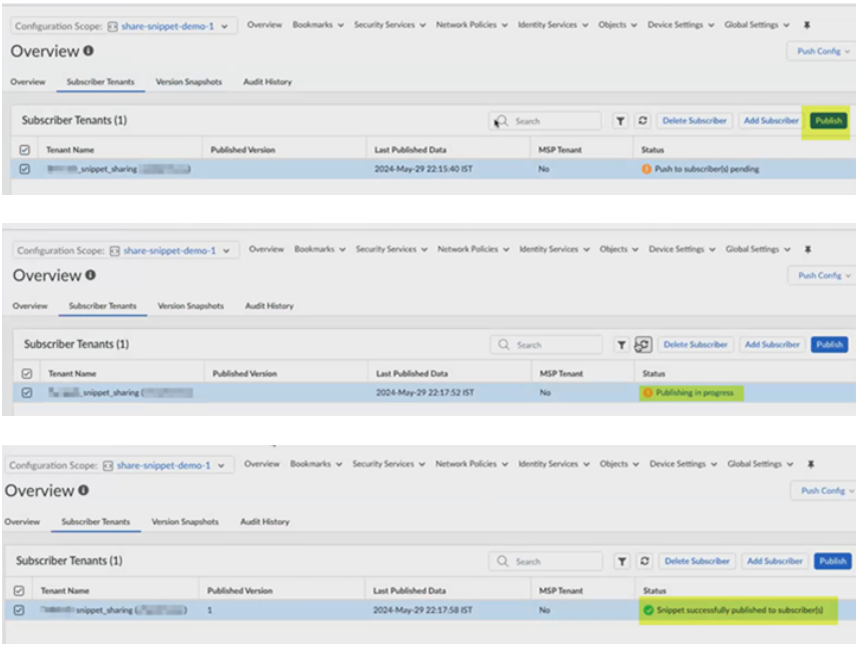
STEP 5 | Publier un extrait à un abonné locataire.

1. Créez et associez l'extrait à un dossier.Les

   extraits nouvellement créés sont disponibles sous extraits **Local (Locaux)**.

   - L'onglet **Overview (Aperçu)** affiche les détails de l'extrait tels que le nom, la description, l'heure de création (lorsque l'extrait a été chargé côté abonné), l'heure de dernière mise à jour et les détails des étiquettes.
   - L'onglet **Subscriber Tenants (Locataires abonnés)** affiche le nom du locataire, la version publiée sur le locataire, la dernière date de publication et l'état de la publication.
     - Cliquez sur **Published Version (Version publiée)** pour examiner les modifications de configuration.
     - Avant de publier un extrait à un locataire, **Add Subscriber (Ajoutez un abonné)** et **Save (Enregistrez)**.
   - La **Version Snapshots (Rubrique Instantanés)** donne un historique de la configuration de votre extrait. Sur cet écran, vous pouvez comparer les instantanés de configuration avec votre configuration candidate, et **Save Version Snapshot (Enregistrer l'instantané de version)** ou **Load (Charger)** un instantané de configuration antérieur comme candidat. Cliquez sur le numéro de **Version (version)** pour afficher les différences de configuration.
   - L' **Audit History (Historique d'audit)** fournit une piste de vérification de toutes les actions lancées par l'administrateur. Il enregistre des détails tels que le numéro de version publié, les modifications apportées, le propriétaire de la modification, la date et l'heure de la modification, et les spécificités de la modification.
2. Sous l'onglet **Subscriber Tenant (Locataire abonné)**, sélectionnez le nom du locataire et **Publish (Publier)**.

   Cela envoie la requête de publication au locataire abonné. Dans la colonne **Status (État)** indique que l'extrait a été publié avec succès pour l'abonné et l'extrait sera disponible sous extraits publiés.



STEP 6 | Vérifier sur le locataire de l'abonné.

1. Accédez à **Overview (Aperçu)** > **Configuration Scope (Extraits de Configuration)** > **Snippets (Extraits)**, et sélectionnez l'extrait sous **Snippets (extraits).** Vous

   êtes redirigé vers **Overview (Aperçu)** de l'extrait qui affiche des détails tels que le nom du locataire de l'éditeur, la description, l'ID TSG, l'heure de création de l'extrait, l'heure de dernière mise à jour, les étiquettes et les détails de la configuration de pause.

STEP 7 | Supprimez la confiance.

Les extraits abonnés associés à des dossiers ou des pare-feux ne peuvent être clonés et ne peuvent pas être supprimés.

1. Allez à locataire abonné ou éditeur.
2. Cliquez sur **Subscriber Tenant (Locataire abonné)** sous **Tenants for Snippet Sharing (Locataires de confiance pour le partage des extraits.)**.
3. Sélectionnez le **Tenant Name (Nom du locataire)**, et **Delete Trust (Supprimer la confiance)**.

Après avoir supprimé la protection, l'extrait ne sera plus associé au pare-feu ou au dossier et deviendra un extrait local.

Classification des extraits

- Prédéfini : Tous les utilisateurs de Strata Cloud Manager peuvent accéder à ces extraits pour configurer rapidement de nouveaux pare-feux et déploiements avec des configurations de meilleures pratiques.
- Local : Ces extraits modifiables sont créés au sein du locataire et ne peuvent pas être partagés avec d'autres locataires abonnés.
- Publié : Les abonnés locataires de confiance ont accès à ces extraits partagés, qui ne peuvent être ni clonés ni modifiés.

- Abonné : Ces extraits, partagés par le locataire de l'éditeur, peuvent être clonés par les utilisateurs, mais ne peuvent pas être modifiés.

Gestion : Variables

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Faites appel à des variables pour vos configurations afin de prendre en compte les objets de configuration spécifiques à un périphérique ou à un déploiement.

Les variables sont un outil avancé qui vous permet de standardiser vos configurations tout en vous donnant la possibilité de prendre en charge des valeurs de configuration uniques spécifiques à l'appareil ou au déploiement. Les variables vous permettent de réduire le nombre d'extraits de code que vous devez gérer, tout en conservant les valeurs de configuration spécifiques au pare-feu ou au déploiement, selon les besoins.

Par exemple, vous disposez d'un extrait de code pour la configuration que vous souhaitez associer à plusieurs dossiers imbriqués où chaque dossier imbriqué contient un ensemble de pare-feu spécifiques à un emplacement géographique. Dans l'extrait de code, vous avez configuré des règles de politique pour restreindre l'accès aux systèmes critiques de l'entreprise pour des plages d'adresses IP spécifiques uniquement. Dans ce scénario, vous pouvez créer une variable pour chaque plage d'adresses IP spécifique à chaque dossier imbriqué et utiliser cette variable dans la configuration de l'extrait de code hérité. Cela vous permet de gérer et d'envoyer les modifications de configuration tout en utilisant moins d'extraits de code pour prendre en charge les valeurs de configuration spécifiques à l'appareil ou au déploiement.

Les variables peuvent être créées au niveau du dossier, du déploiement ou du pare-feu. Lorsque vous créez une variable pour un dossier, celle-ci est héritée par tous les dossiers imbriqués sous le dossier. En cas de conflit avec les variables dans la portée de configuration d'un dossier, le pare-feu ou le déploiement hérite de la valeur de la variable du dossier contenant les dossiers imbriqués. Toutefois, vous pouvez remplacer une variable héritée au niveau du dossier, du déploiement ou du pare-feu imbriqué.

Les types de variables suivants sont pris en charge :

Type de variable	Description
Numéro AS	Numéro de système autonome à utiliser dans votre configuration BGP.
Nombre	Nombre d'événements qui doivent se produire afin de déclencher une action.
ID du périphérique	Device-ID à utiliser pour attribuer un évaluateur de priorité de périphérique dans une High Availability (haute disponibilité - HA) active/active.
Priorité du périphérique	Priorité du périphérique pour indiquer une préférence pour le pare-feu qui doit assumer le rôle actif High Availability (haute disponibilité - HA) active/passive.
Trafic sortant max.	Valeur maximale de sortie à utiliser dans la configuration du profil Quality of Service (qualité de service - QoS).
Nom de domaine complet	Fully Qualified Domain Name (nom de domaine complet - FQDN)
ID du groupe	ID de groupe High Availability (haute disponibilité - HA).
IP du masque réseau	IP statique ou adresse réseau.

Type de variable	Description
Plage d'IP	Une plage d'adresses IP. Par exemple, **`192.168.1.10-192.168.1.20`**.
Caractère générique IP	Masque générique d'IP pour autoriser ou refuser des adresses IP similaires. Par exemple, `10.0.0.5/255.255.0.255`.
Étiquette de liens	Étiquette de lien à utiliser dans votre configuration SD-WAN.
Pour cent	Pourcentage entre **`0`** et **`99`**.
Port	Port source ou de destination.
Profil QoS	Profil QoS à utiliser dans les configurations QoS.
Taux	Rate pour spécifier un seuil qui déclenche une action. Par exemple, le `Taux d'alarme` pour un profil de protection DoS.
ID de routeur	ID de routeur lorsque vous configurez le protocole BGP (Border Gateway Protocol) pour un routeur logique.
Minuteur	Minuterie en secondes pour configurer un seuil qui déclenche une action.
Employé	Une zone de sécurité.

Création d'une variable

Vous pouvez également créer une variable en ligne où une variable est prise en charge.

STEP 1 | Connectez-vous à Strata Cloud Manager.

STEP 2 | Choisissez **Manage (Gestion)** > **Configuration** > **NGFW and Prisma Access (Accès NGFW et Prisma)** > **Overview (Aperçu)** et sélectionnez la portée de configuration dans laquelle vous souhaitez créer la variable.

Dans **Folders (Dossiers)**, sélectionnez le dossier ou le périphérique pour lequel vous souhaitez créer une variable.

Dans le **Snippets (Extraits)**, sélectionnez l'extrait de code spécifique pour lequel vous souhaitez créer une variable.

STEP 3 | Dans la section Variables, cliquez sur le nombre de variables affiché.

STEP 4 | **Ajouter une variable**.

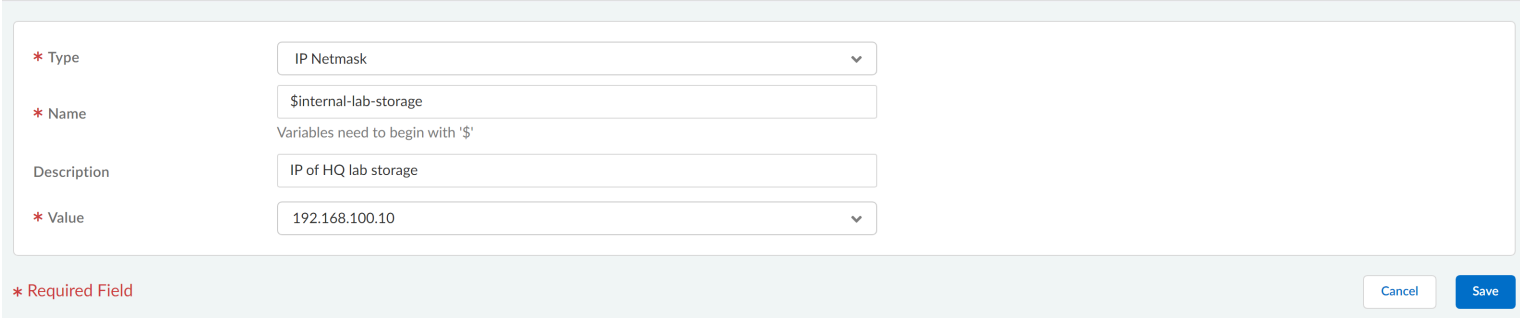
STEP 5 | Créez la variable.

Dans cet exemple, un `Masque de réseau IP` est créée pour être utilisée comme objet d'adresse pour une ressource interne critique.

1. Sélectionnez la variable **Type**.
2. Donnez à la variable un **Nom** descriptif.

   Tous les noms de variables doivent commencer par **$**.
3. (Facultatif) Saisissez une **Description** de la variable.
4. Entrez la **Value (Valeur)** de la variable.
5. **Save (Enregistrer)**.

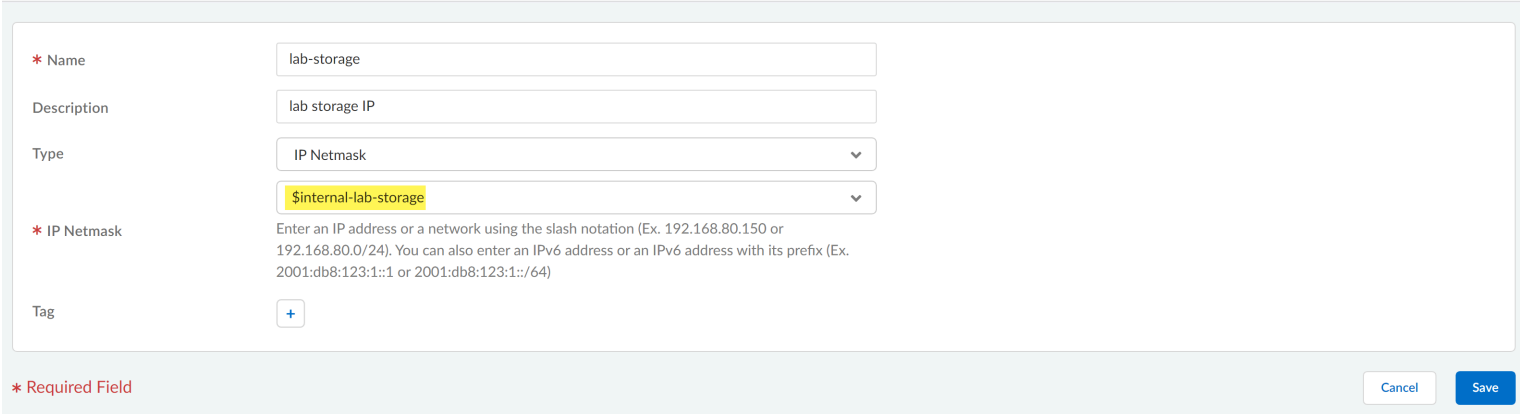
Variables



STEP 6 | Ajoutez la variable à votre configuration.

Dans cet exemple, le `$internal-laboratoire-stockage` créée à l'étape précédente est ajouté à la configuration de l'objet d'adresse.

Addresses



STEP 7 | Transmettre la configuration.

Importer une variable

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Strata Cloud Manager	❑ Licence AIOps for NGFW Premium

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
	❑ Licence Prisma Access

Importer des variables dans Strata Cloud Manager à l'aide d'un fichier CSV. Les importations de variables sont conçues pour remplacer plusieurs variables héritées de la hiérarchie de dossiers par le pare-feu, ou déjà configurées dans l'étendue de configuration du pare-feu, avec de nouvelles valeurs spécifiques au pare-feu.

La variable doit déjà être héritée de la hiérarchie de dossiers ou configurée dans l'étendue de configuration du pare-feu pour être remplacée à l'aide d'importations de variables. L'importation de variables pour créer des variables entièrement nouvelles n'est pas prise en charge.

STEP 1 | Connectez-vous à Strata Cloud Manager.

STEP 2 | Choisissez **Manage (Gestion)** > **Configuration** > **NGFW and Prisma Access (Accès NGFW et Prisma)** > **Overview (Aperçu)**.

STEP 3 | Dans la section Variables, cliquez sur le nombre de variables affiché.

STEP 4 | Choisissez **CSV Export/Import (Exportation/importation CSV)** > **Export (Exportation)** pour exporter les variables que vous souhaitez remplacer.

Palo Alto Networks vous recommande d'exporter d'abord les variables que vous souhaitez écraser. Cela garantit que le fichier CSV dans lequel vous téléchargez Strata Cloud Manager est correctement formaté. Cela accélère également le processus d'importation en garantissant que le dossier cible et les variables de pare-feu sont correctement attribués.

STEP 5 | Modifiez les variables dans le fichier CSV exporté.

Tenez compte des points suivants lorsque vous modifiez votre fichier CSV pour l'importation.

- Seuls les éditeurs de texte simples, tels que le Bloc-notes, peuvent modifier un fichier CSV exporté.
- # Signifie que la variable est créée dans la hiérarchie des dossiers et héritée par le pare-feu.

  Retirez le # pour remplacer la valeur de la variable héritée par une valeur spécifique au pare-feu.

  Une valeur de variable ajoutée avec # est ignorée par Strata Cloud Manager lors de l'importation, car seules les valeurs de variable de remplacement dans la zone de configuration du pare-feu sont prises en charge.
- `-S/O-` Signifie que la variable n'existe pas dans la configuration du pare-feu. Cela signifie que la variable a été créée en dehors de la hiérarchie de dossiers à laquelle appartient le pare-feu.

  Modification de la valeur d'une variable en `-S/O-` n'est pas pris en charge. Strata Cloud Manager ignore toute valeur de variable modifiée en `-S/O-`.

  Attribution d'une valeur spécifique au pare-feu à une variable avec la valeur `-S/O-` n'est pas prise en charge, car la variable n'existe pas dans l'étendue de configuration du pare-feu. La variable doit être héritée par le pare-feu à partir de la hiérarchie des dossiers,

ou configurée dans la portée de configuration du pare-feu, afin d'être remplacée par l'importation de variables.

- Une valeur variable de `Aucun#` ou `Aucun` signifie que la variable a été créée avec la variable **Value (Valeur)** comme **None (Aucun)**.

  Vous pouvez modifier n'importe quelle valeur de variable comme suit : `Aucun` pour supprimer la valeur, mais pas la variable.

- Pour une variable créée dans la portée de configuration du pare-feu, la suppression d'une valeur de variable et son maintien vide entraînent la suppression de la variable.

  Pour une variable créée dans la hiérarchie des dossiers et héritée par le pare-feu, la suppression d'une valeur de variable et son maintien vide rétablissent la valeur de la variable à celle héritée de la hiérarchie des dossiers.

1. Localisez et ouvrez le fichier CSV que vous avez exporté. Le format du fichier CSV exporté, le nom est le suivant :

   ```
   <cloud-management-tenant-name> - Prisma Access_<export-date>_Variables
   ```

2. Modifiez les variables si nécessaire.

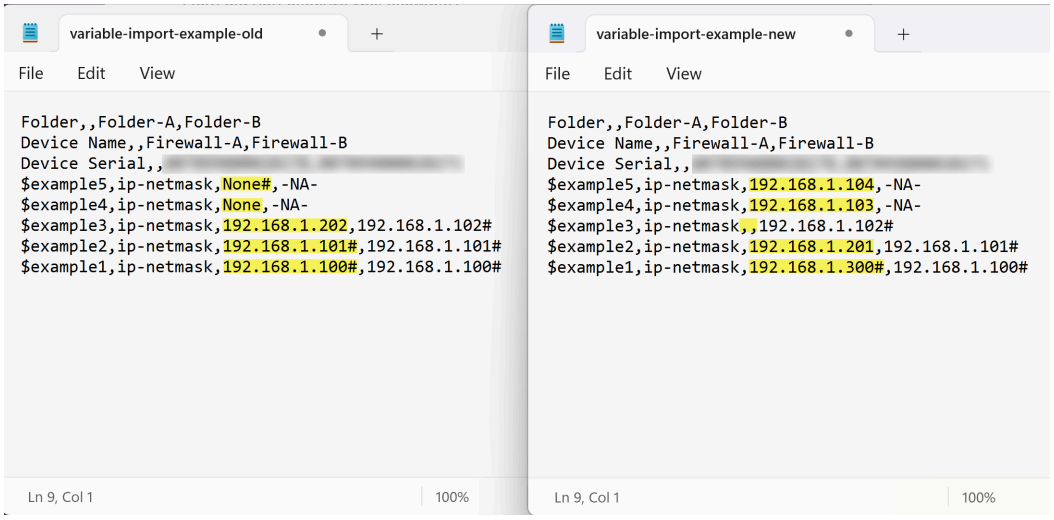
   Palo Alto Networks ne recommande pas de modifier les noms de dossiers, les noms de périphériques ou les numéros de série des périphériques. Cela peut entraîner des échecs d'importation.

   Dans l'exemple ci-dessous, les modifications suivantes ont été apportées aux valeurs des variables dans le `Pare-feu-A` Portée de configuration pour illustrer comment

l'importation de variables peut être utilisée pour modifier plusieurs variables en une seule opération.

- `$example 1` : écraser la valeur `Aucun#` héritée par une valeur spécifique au pare-feu.
- `$example2` : écrase la valeur `Aucun` propre au pare-feu par une valeur spécifique au pare-feu.
- `$example3` : si la variable a été créée dans la portée de configuration du pare-feu, une valeur vide supprime la variable.

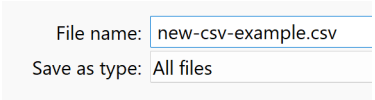
  Si la variable a été héritée de la hiérarchie des dossiers et a été remplacée dans la portée de configuration du pare-feu, une valeur vide restaure la valeur de la variable héritée de la hiérarchie des dossiers.
- `$example4` : écrase la valeur héritée `192.168.1.101` par une valeur spécifique au pare-feu.
- `$example5`—Exemple de changement de variable Strata Cloud Manager ignore parce que # est toujours ajouté.



STEP 6 | Cliquez sur Save (Enregistrer) pour enregistrer vos modifications.

Choisissez **File (Fichier)** > **Save (Sauvegarder)** pour enregistrer les modifications que vous avez apportées au fichier CSV.

Vous pouvez également sélectionner **File (Fichier)** > **Save As (Enregistrer sous)** pour enregistrer vos modifications dans un nouveau fichier CSV. Pour créer un fichier CSV, vous devez inclure **`.csv`** comme l'extension de fichier.



STEP 7 | Importez le fichier CSV dans Strata Cloud Manager.

1. Sélectionnez **Manage (Gestion)** > **Configuration** > **Overview (Aperçu)**.
2. Dans la section Variables, cliquez sur le nombre de variables affiché.
3. Sélectionnez **CSV Export/Import (Exportation/importation CSV)** > **Import (Importation)**.
4. **Choose File (Choisissez Fichier)** et sélectionnez le fichier CSV contenant les variables que vous avez modifiées.
5. **Import (Importer)**.

Exporter des variables

Exportez vos variables de configuration de dossier et de pare-feu au format CSV vers votre appareil local. L'exportation de vos variables est utile lorsque vous écrasez un grand nombre de variables sur plusieurs pare-feu.

L'exportation de variables d'interface créées lorsque vous configurez une interface au niveau du dossier n'est pas prise en charge.

STEP 1 | Connectez-vous à Strata Cloud Manager.

STEP 2 | Sélectionnez **Manage (Gestion)** > **NGFW and Prisma Access (Accès NGFW et Prisma)** > **Configuration** > **Overview (Aperçu)**.

STEP 3 | Dans la section Variables, cliquez sur le nombre de variables affiché.

STEP 4 | Sélectionnez **CSV Export/Import (Exportation/importation CSV)** > **Export (Exportation)**.

STEP 5 | Sélectionnez le dossier et les pare-feu contenant les variables que vous souhaitez exporter et cliquez sur **Next (Suivant)**.

*Si vous souhaitez exporter toutes les variables créées sur Strata Cloud Managersélectionnez **Tous les pare-feu**.*

STEP 6 | Sélectionnez une ou plusieurs variables à exporter.

STEP 7 | (Facultatif) **Preview (Aperçu)** les variables sélectionnées pour afficher des détails supplémentaires.

À partir de l'aperçu des variables, vous pouvez afficher des informations telles que le nom de la variable, la portée de configuration où la variable a été créée et la valeur de la variable.

Cliquez sur **Cancel (Annuler)** et passez à l'étape suivante ou **Download CSV (Télécharger CSV)** sur votre appareil local.

STEP 8 | **Export (Exporter)** les variables sélectionnées au format CSV.

Le fichier CSV est exporté et téléchargé localement sur votre appareil. Le format du fichier CSV exporté, le nom est le suivant :

```
<cloud-management-tenant-name> - Prisma Access_<export-
date>_Variables
```


Gestion : Vue d’ensemble

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l’accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Considérez la page Vue d’ensemble comme votre point de départ vers NGFW et Prisma Access, à la fois pour la première configuration et pour la gestion quotidienne de la configuration (**Manage (Gérer)** > **Configuration (Configuration)** > **NGFW et Prisma Access** > **Overview (Vue d’ensemble)**.

- Global
- Prisma Access
- Strata Cloud Manager

Global

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Licence Prisma Access

Si vous sélectionnez le cadre de configuration **Global (Global)**, vous pouvez afficher les détails suivants :

- Dossiers globaux que vous avez créés et leurs variables
- Pare-feu avec conflits de configuration
- État de la synchronisation du pare-feu et état de la connectivité du pare-feu

- Renseignements généraux
- Séquences de configuration
- Licence
- Des locataires de confiance pour le partage de séquences
- Instantanés des versions de la configuration

Vue d'ensemble de la configuration (Prisma Access)

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licence Prisma Access

Si vous commencez à utiliser Prisma Access :

- La liste de contrôle **Basics (Bases)** vous montre comment être opérationnel avec Prisma Access. Terminez les tâches et les étapes pas à pas ici pour commencer avec une configuration de base ; puis, testez votre environnement et développez votre déploiement.
- Voici comment fonctionnent les dossiers de politique et de configuration.
- Voici comment pousser les modifications de configuration à Prisma Access.

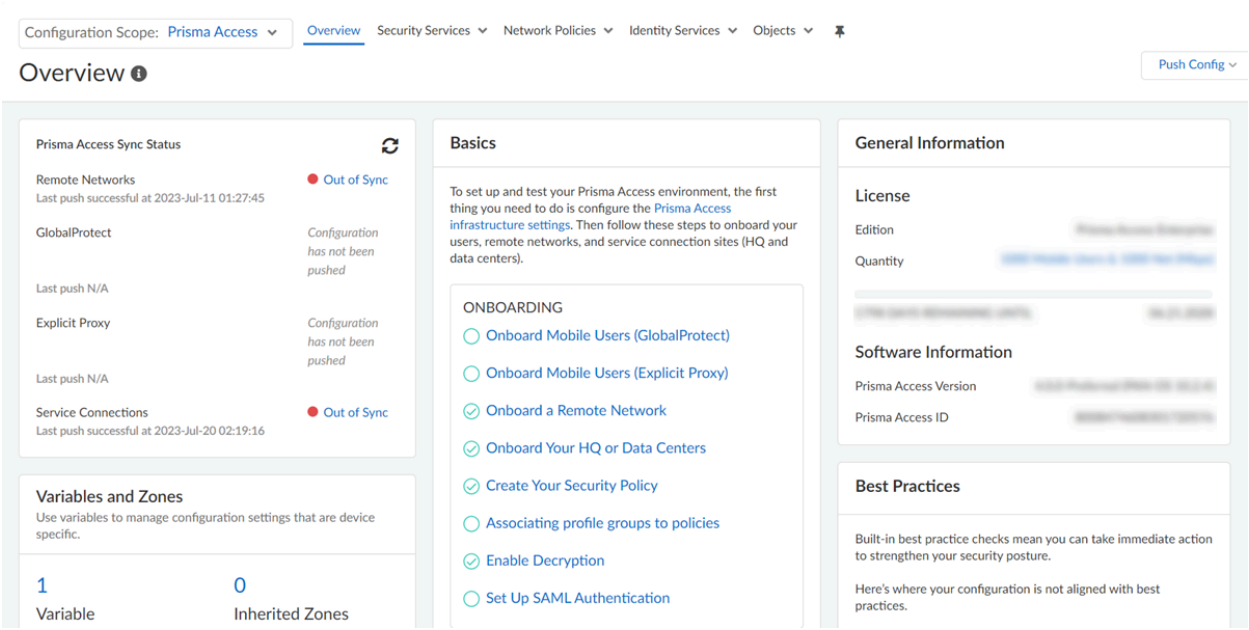
Pour plus d'informations sur votre environnement Prisma Access :

- Consultez les informations sur la licence pour afficher les offres qui accompagnent votre abonnement Prisma Access.
- Le panneau **À propos** affiche les **informations logicielles et locataires** de votre environnement Prisma Access.

Pour la gestion quotidienne de la configuration :

- Obtenir un aperçu de l'état de la configuration
- Standardiser une configuration de base commune pour des déploiements Prisma Access à l'aide des extraits de configuration
- Recherchez des instantanés de configuration : comparez les versions de configuration et restaurez (ou chargez) une version antérieure pour récupérer d'une configuration poussée ayant un impact involontaire sur le flux de trafic ou la sécurité
- Optimisez votre configuration en nettoyant les objets et les règles inutilisés et en renforçant les règles qui introduisent des failles de sécurité en autorisant les applications non utilisées
- Identifiez les zones où vous pouvez apporter des modifications de configuration qui renforceraient votre posture de sécurité

- Vous pouvez également trouver des informations sur votre licence Prisma Access et les éléments que celle-ci contient

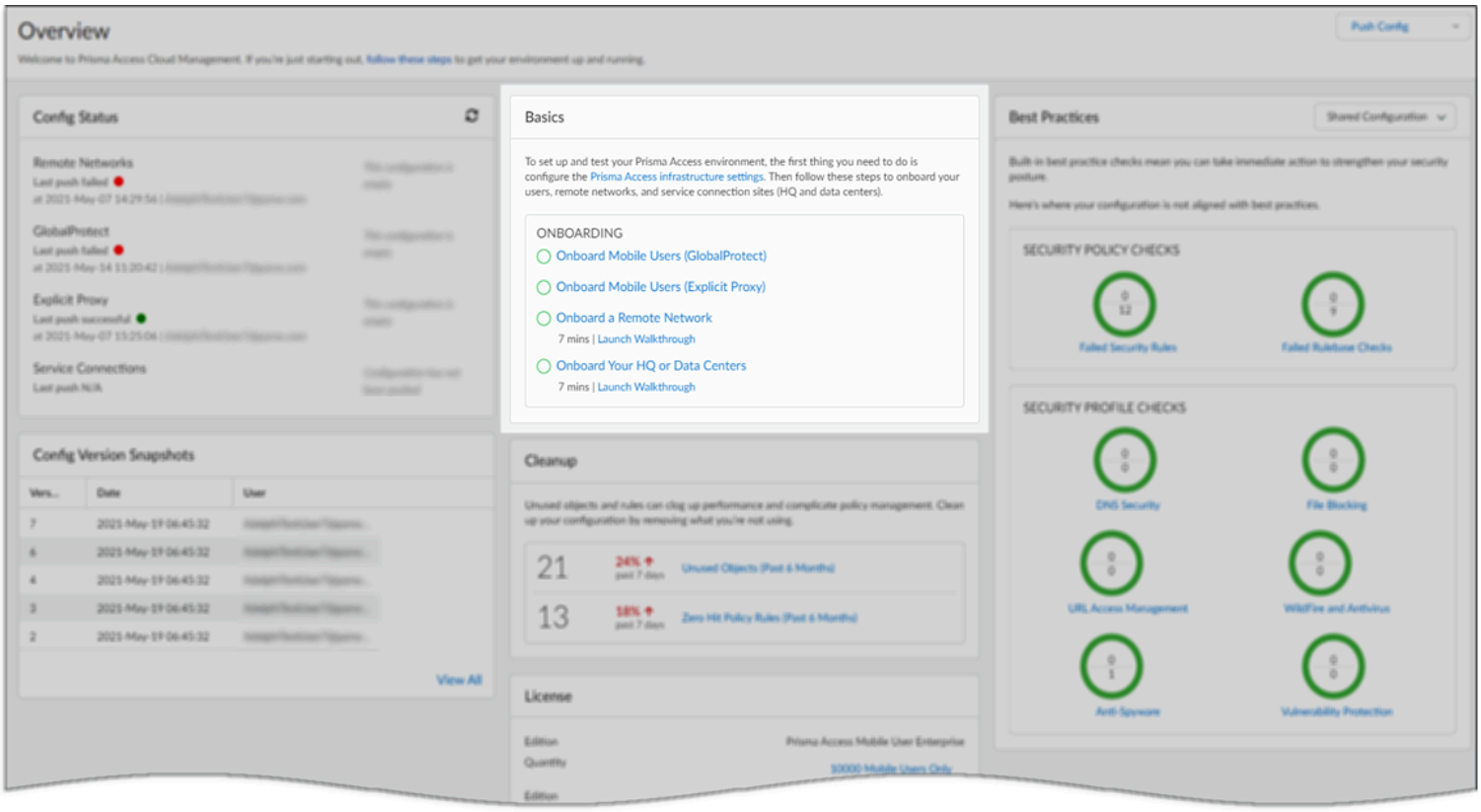


Une fois la configuration de base terminée, vous pouvez commencer à tester votre environnement et à élaborer votre déploiement.

De Base

Les **Bases** de la configuration Prisma Access vous permettent d'être opérationnel avec Prisma Access. Terminez les tâches ici pour commencer avec une configuration de base, que vous pouvez ensuite utiliser pour tester votre environnement et construire votre déploiement.

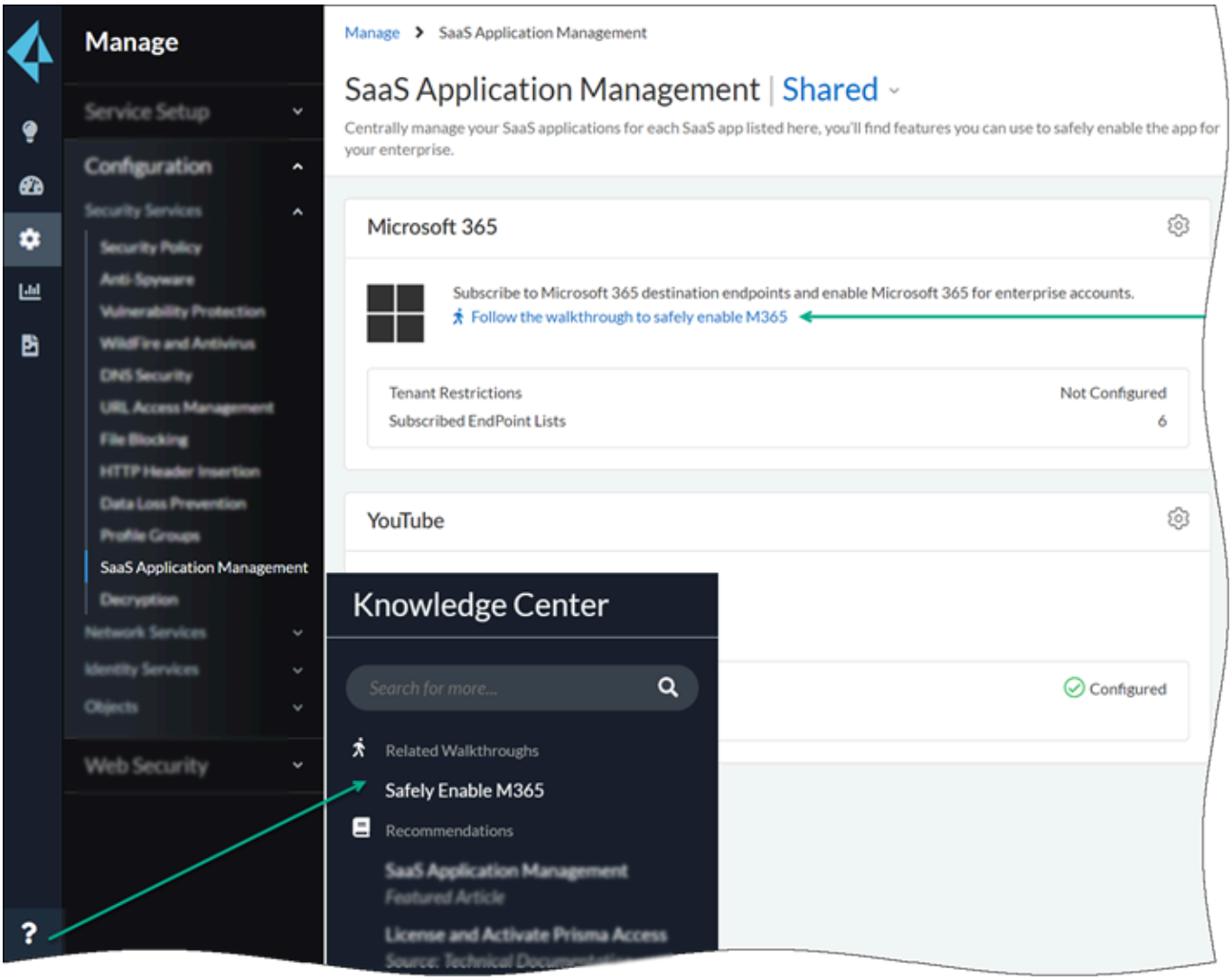
Chaque tâche vous renvoie à la page où vous pouvez mettre en place la configuration associée ; lorsque vous avez terminé, les tâches de cette liste s'affichent comme étant terminées. Vous pouvez ainsi suivre vos progrès en un coup d'œil, ce qui est particulièrement utile si vous êtes en phase d'intégration.

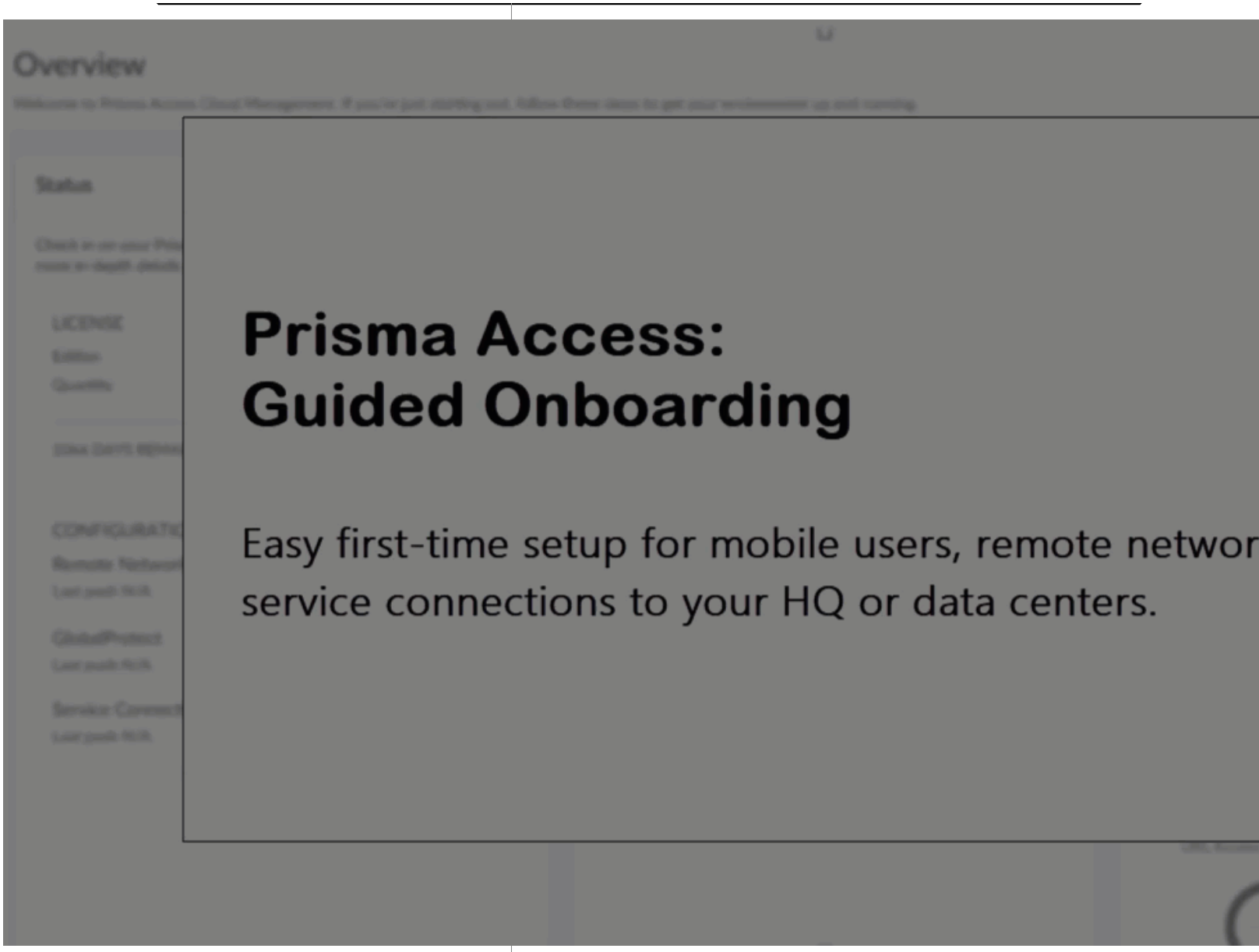


Cheminements

Certaines tâches comprennent également des cheminements qui vous guident à travers les étapes de base requises pour mettre votre environnement en marche.

Des cheminements d'intégration sont disponibles sur le tableau de bord **Overview (Vue d'ensemble)**. Vous pouvez cliquer sur l'aide pour voir si des cheminements sont fournis pour la page sur laquelle vous vous trouvez, et garder un œil sur les cheminements que vous pouvez lancer directement sur la page :





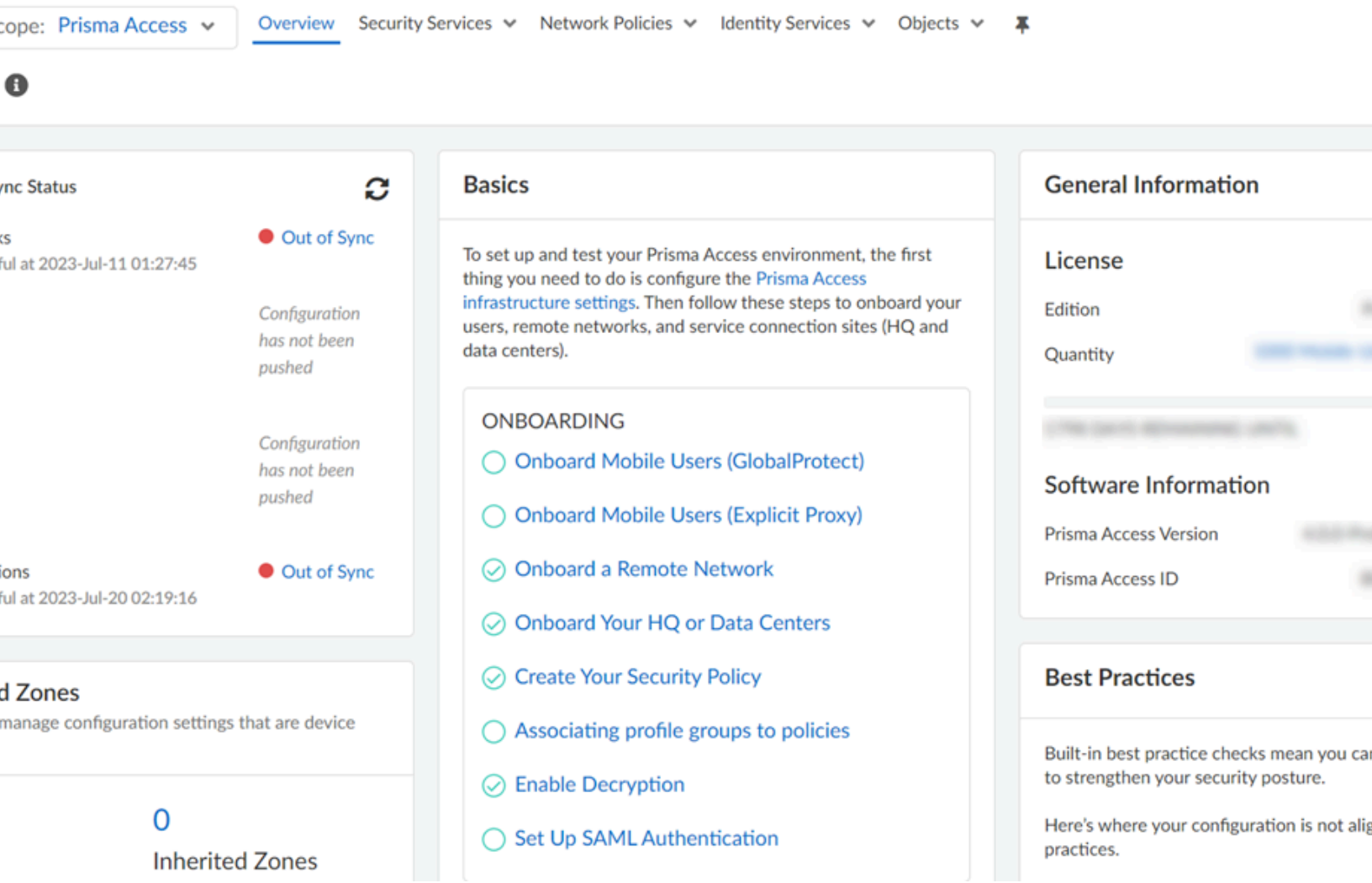
Statut de synchronisation de Prisma Access

Sur la page **Overview (Vue d'ensemble)**, vous pouvez vérifier rapidement l'état de vos configurations Prisma Access. Si vous constatez quelque chose d'inattendu, approfondissez la question pour identifier la configuration concernée. Voici les états susceptibles d'être vus :

- **La configuration n'a pas été** transmise : jusqu'à présent, aucune configuration n'a été poussée vers Prisma Access.
- **Cette configuration est vide** : un utilisateur a poussé une configuration vierge vers Prisma Access. Une configuration avait été mise en place auparavant, de sorte que la poussée vers Prisma Access aurait pu consister à supprimer la configuration. Accédez à **Push Config (Transmettre la configuration)** > **Jobs (Tâches)** pour examiner les modifications récentes.

- **Désynchronisé** : un utilisateur a poussé une configuration vers Prisma Access, mais la poussée est accompagnée d'une erreur ou d'un avertissement. Cela peut être un problème de configuration ou un problème lié au transfert vers Prisma Access.
- **Synchronisation** : la dernière configuration poussée vers Prisma Access a réussi, et aucune erreur ne s'est produite.

Si vous voyez un phénomène inattendu, cliquez sur l'état pour ouvrir une carte qui montre les endroits où vous avez des utilisateurs mobiles (GlobalProtect ou connexions proxy explicites), des réseaux distants ou des connexions de service. Ainsi, vous pouvez alors repérer la configuration qui nécessite une révision ou une mise à jour.



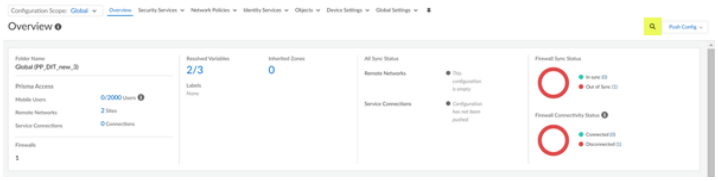
Recherche globale à l'aide de la recherche de configuration

La recherche de configuration vous permet de trouver des objets de configuration et des paramètres spécifiques pour une chaîne de caractères particulière, tels que les adresses IP, le nom d'objet, les objets référencés, les objets en double, les noms de politiques, les règles de politiques, les politiques couvertes pour des CVE spécifiques, l'UUID de règle, les extraits prédéfinis ou le nom d'application et d'obtenir la liste de toutes les références où l'objet est utilisé.

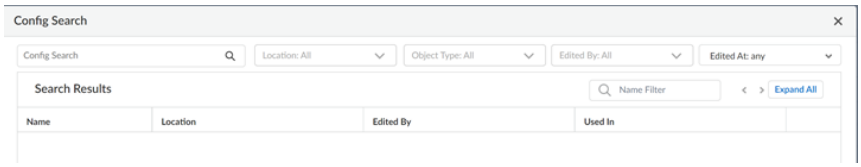
1. En vue de lancer **Config Search (Recherche de configuration)**, cliquez sur l'icône

   à côté de **Push Config (Transmettre la configuration)** sur le côté supérieur droit de l'interface Web. **Config Search (Recherche de configuration)** est disponible à partir de toutes les pages sous **Manage (Gérer)**.

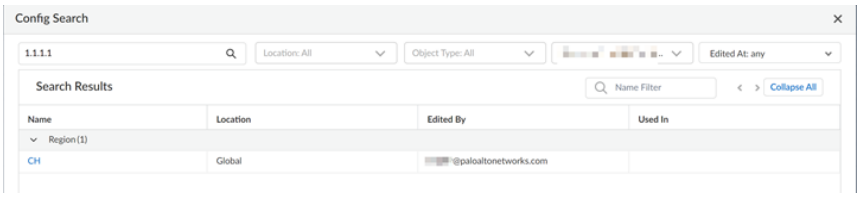
2. Dans l'écran **Config Search (Recherche de configuration)**, vous pouvez effectuer une recherche à l'aide des champs **Config String (Chaîne de configuration)**, **Location (Emplacement)**, **Object Type (Type d'objet)**, **Edited By (Édité par)** ou **Edited At (Édité à)**.

   Conseils de recherche :

   - Vous pouvez rechercher une expression exacte en la plaçant entre guillemets.
   - Les espaces entre les termes de la recherche sont traités comme des opérations ET. Par exemple, si vous faites porter la recherche sur une politique d'entreprise, les résultats de la recherche incluent les instances où les termes entreprise et politique existent dans la configuration
   - Pour relancer une recherche précédente, cliquez sur l'icône **Config Search (Recherche de configuration)**, qui affiche les 50 dernières recherches. Cliquez sur un élément de la liste pour relancer la recherche. La liste d'historique de recherche est différente pour chaque compte administrateur.
   - La recherche de configuration est disponible pour chaque champ consultable. Par exemple, vous pouvez rechercher une politique de sécurité sur les types d'objets suivants : Étiquettes, Zone, Adresse, Utilisateur, Profil HIP, Application, UUID et Service.
   - L'emplacement est regroupé par Dossiers et Extraits. Il est possible de sélectionner plusieurs lieux de recherche. Si vous ne sélectionnez aucun emplacement, **All (Tous)** les emplacements seront sélectionnés par défaut.
   - Si le type d'objet n'est pas sélectionné, **All (Tout)** sera sélectionné.

3. Les résultats de la recherche sont classés par catégories et fournissent des liens vers l'emplacement de configuration dans Strata Cloud Manager. Ceci vous permet de trouver facilement toutes les occurrences et références de la chaîne recherchée.

Aperçu de la configuration (Strata Cloud Manager)

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series, funded with Software NGFW Credits	❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app)

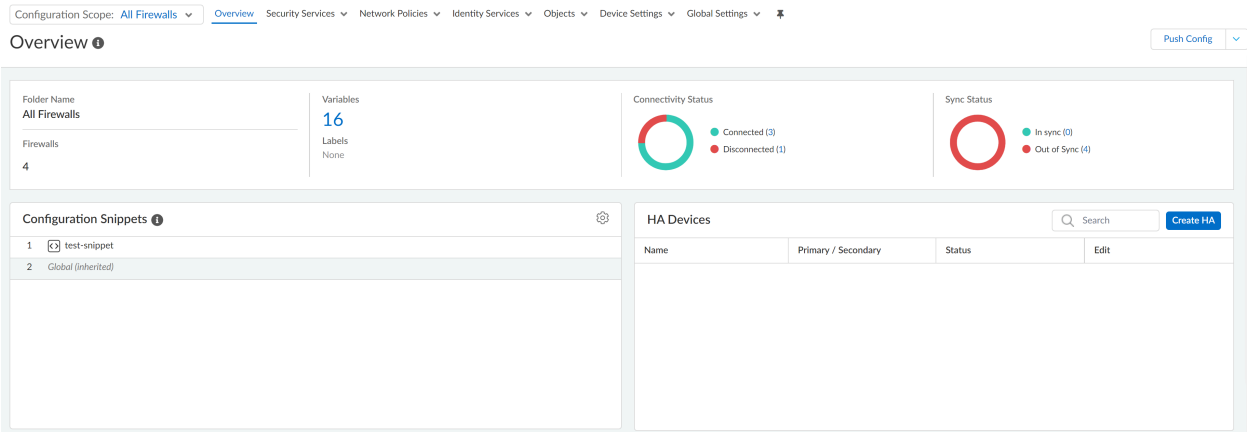
Si vous commencez à peine à gérer la gestion du cloud de NGFW :

- Voici comment fonctionnent les dossiers de politique et de configuration.
- Voici comment pousser les changements de configuration sur les pare-feux.

Pour la gestion quotidienne de la configuration :

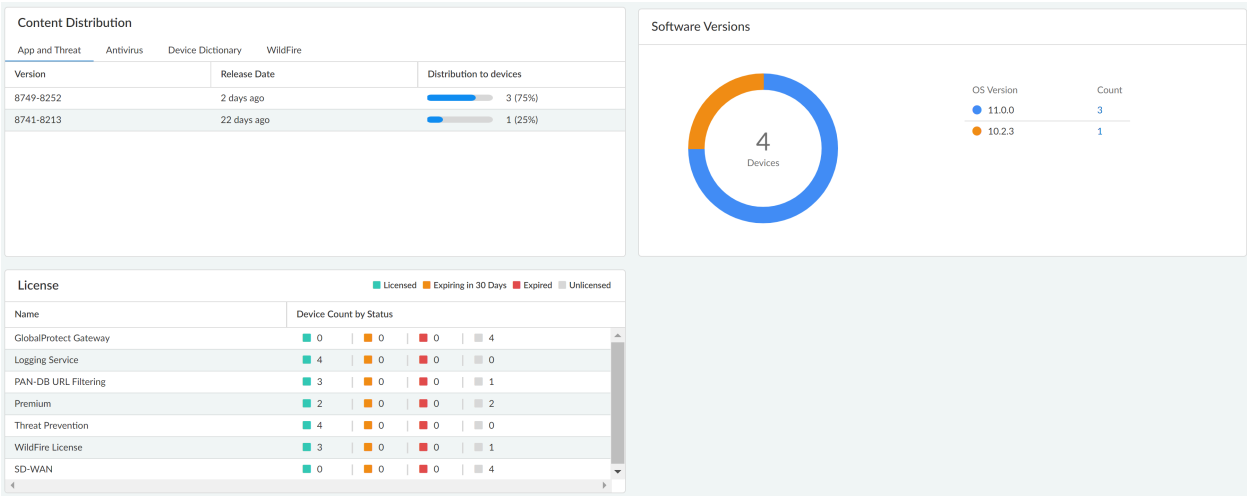
- Obtenez un résumé du nom du dossier actuel, du nombre de pare-feux ajoutés au dossier, du nombre de variables Gestion : Variables créées pour le dossier.
- Bénéficiez d'une visibilité et d'un contrôle accrus sur les configurations de pare-feu locales sans avoir besoin de basculer entre la gestion centralisée et les pare-feux individuels pour la gestion des configurations locales.
  - **Firewalls with config conflict (Pare-feu avec conflits de configuration)** indique le nombre de pare-feux avec des conflits. Cliquez sur le numéro pour afficher les conflits pour les pare-feux avec leur emplacement. Cliquez sur n'importe quel pare-feu pour voir les conflits au niveau du périphérique.
  - **Objects with config conflicts (Objets avec conflits de configuration)** affiche le nombre de conflits par pare-feu. Cliquez sur le numéro pour afficher les objets en conflit et leurs types pour un pare-feu spécifique. Un clic sur l'objet permet d'obtenir des informations détaillées sur le conflit.
- Normaliser une configuration de base commune pour un ensemble de pare-feux gérés à l'aide d'extraits de configuration Gestion : Extraits.
- Configurez les pare-feux gérés en configuration High Availability (haute disponibilité - HA) pour assurer la redondance et la continuité des entreprises.
- Examiner l'état de **Connectivité** des pare-feux gérés à Strata Cloud Manager

- Examinez **l'état de synchronisation** de configuration entre Strata Cloud Manager et la configuration en cours d'exécution sur vos pare-feux gérés.



Pour plus d'informations sur les pare-feu gérés :

- Examinez les détails de la **distribution de contenu** et des **Software Versions (versions logicielles)** pour voir quelles mises à jour du contenu dynamique et quelles versions logicielles PAN-OS sont exécutées sur vos pare-feux gérés.
- Examinez les détails des **License (Licences)** pour voir quelles licences sont activées sur vos pare-feux gérés.



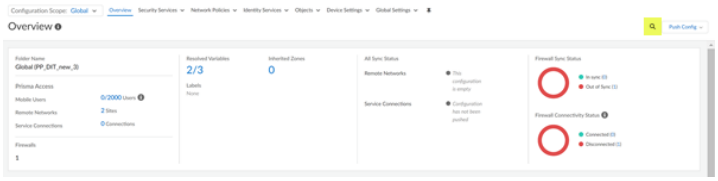
Recherche globale à l'aide de la recherche de configuration

La recherche de configuration vous permet de rechercher des objets de configuration et des paramètres pour une chaîne particulière, tels que les adresses IP, le nom d'objet, les objets référencés, les objets en double, les noms de politiques, les règles de politiques, les politiques couvertes pour des CVE spécifiques, l'UUID de règle, les extraits prédéfinis ou le nom d'application et d'obtenir la liste de toutes les références où l'objet est utilisé.

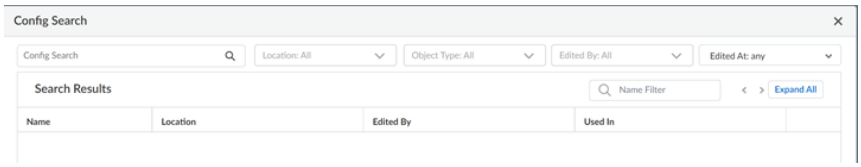
1. En vue de lancer **Config Search (Recherche de configuration)**, cliquez sur l'icône

   à côté de **Push Config (Transmettre la configuration)** sur le côté supérieur droit de l'interface Web. **Config Search (Recherche de configuration)** est disponible à partir de toutes les pages sous **Manage (Gérer)**.

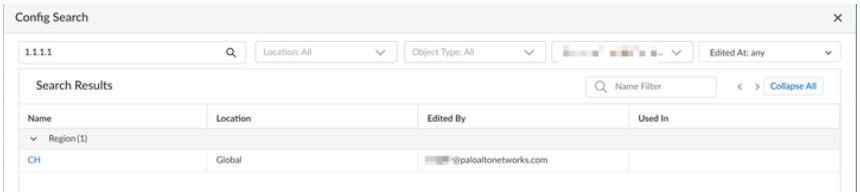
2. Dans l'écran **Config Search (Recherche de configuration)**, vous pouvez effectuer une recherche à l'aide des champs **Config String (Chaîne de configuration)**, **Location (Emplacement)**, **Object Type (Type d'objet)**, **Edited By (Édité par)** ou **Edited At (Édité à)**.

   Conseils de recherche :

   - Vous pouvez rechercher une expression exacte en la plaçant entre guillemets.
   - Les espaces entre les termes de la recherche sont traités comme des opérations ET. Par exemple, si vous faites porter la recherche sur une politique d'entreprise, les résultats de la recherche incluent les instances où les termes entreprise et politique existent dans la configuration
   - Afin de relancer une recherche précédente, cliquez sur l'icône Recherche de configuration, qui affiche les 50 dernières recherches. Cliquez sur un élément de la liste pour relancer la recherche. La liste d'historique de recherche est unique pour chaque compte administrateur.
   - La recherche de configuration est disponible pour chaque champ consultable. Par exemple, vous pouvez rechercher une politique de sécurité sur les types d'objets suivants : Étiquettes, Zone, Adresse, Utilisateur, Profil HIP, Application, UUID et Service.
   - L'emplacement est regroupé par dossiers et extraits. Il est possible de sélectionner plusieurs lieux de recherche. Si vous ne sélectionnez aucun emplacement, **All (Tous)** les emplacements seront sélectionnés par défaut.
   - Si le type d'objet n'est pas sélectionné, **All (Tout)** sera sélectionné.

3. Les résultats de la recherche sont classés par catégories et fournissent des liens vers l'emplacement de configuration dans Strata Cloud Manager. Ceci vous permet de trouver facilement toutes les occurrences et références de la chaîne recherchée.

Gestion : Services de sécurité

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Gérez vos services de sécurité et protégez votre réseau, vos systèmes et vos utilisateurs.

Accédez à **Manage (Gérer)** > **Configuration (la configuration)** > **NGFW and Prisma Access(NGFW et Prisma Access)** > **Security Services (Services de sécurité)**.

Avec les services de sécurité, vous avez la possibilité de :

- Définissez comment vous souhaitez appliquer le trafic Prisma Access avec Gestion : Politique de Sécurité.
- Arrêtez les menaces cryptées dans le trafic chiffré Gestion : Déchiffrement.

Gestion : Politique de Sécurité

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Votre politique de sécurité vous permet de définir la manière dont vous souhaitez appliquer le trafic dans vos déploiements Prisma Access et NGFW. Le trafic qui transite par votre

environnement Strata Cloud Manager est évalué selon vos règles de sécurité et les règles sont appliquées de haut en bas.

Pour configurer votre politique de sécurité, accédez à **Manage (Gestion)** > **Configuration (Configuration)** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Security Policy (Politique de sécurité)**.

Démarrer avec la politique de sécurité

Voici quelques mesures que vous pouvez prendre dès à présent pour mettre la politique de sécurité à votre service.

- Créer une règle de politique de sécurité : les politiques de sécurité vous permettent d'appliquer des règles et de prendre des mesures, et peuvent être aussi générales ou spécifiques que nécessaire.
- Suivre les règles au sein d'une base de règles : chaque règle au sein d'une base de règles est automatiquement numérotée ; lorsque vous déplacez ou réorganisez des règles, les numéros changent en fonction du nouvel ordre.
- Appliquer les meilleures pratiques en matière de règles de politique : lors de la création ou de la modification de règles, vous pouvez exiger une description de règle, une étiquette, un commentaire d'audit, etc. pour garantir que votre base de règles de politique est correctement organisée et regroupée, et pour conserver l'historique des règles importantes à des fins d'audit.
- Règles de politique de test : utilisez l'analyseur de politique pour vérifier les règles de politique.
- Activer un profil de sécurité : un profil de sécurité est appliqué pour analyser le trafic une fois que l'application ou la catégorie est autorisée par la politique de sécurité.
- Créer un groupe de profils de sécurité : un groupe de profils de sécurité est un ensemble de profils de sécurité qui peuvent être traités comme une unité, puis facilement ajoutés aux politiques de sécurité.
- Configurer le blocage de fichiers : identifiez les types de fichiers spécifiques que vous souhaitez bloquer ou surveiller.
- Créez un profil de filtrage des données : empêchez les informations sensibles de quitter votre réseau.
- Gérer la sécurité Web : contrôlez l'accès (navigation générale) à Internet et aux applications SaaS.

Gestion : Déchiffrement

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : Prisma Access AIOps for NGFW Premium Strata Cloud Manager Essentials Strata Cloud Manager Pro

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	→ Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Activez le décryptage pour arrêter les menaces cachées dans le trafic crypté. Il vous suffit d'importer vos certificats de déchiffrement. Pour tout le reste, nous avons prévu des paramètres de meilleures pratiques que vous pouvez utiliser pour vous lancer.

Apprenez-en plus sur le décryptage du trafic ici.

Accédez à **Manage (Gérer)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Decryption (Décryptage)**.

Présentation du décryptage

Les protocoles de chiffrement Secure Sockets Layer (SSL) et Secure Shell (SSH) sont utilisés pour sécuriser le trafic entre deux entités, telles qu'un serveur Web et un client. SSL et SSH encapsulent le trafic, en cryptant les données de manière à ce qu'elles soient insignifiantes pour des entités autres que le client et le serveur avec les certificats pour affirmer la confiance entre les périphériques et les clés pour décoder les données. Déchiffrez le trafic SSL et SSH pour :

- Empêcher les logiciels malveillants dissimulés dans le trafic crypté de s'introduire à l'intérieur de votre réseau. Par exemple, un pirate compromet un site Web qui utilise le chiffrement SSL. Les employés visitent ce site Web et, sans le savoir, télécharge une exploitation ou un fichier malveillant. Le fichier malveillant utilise ensuite le terminal infecté de l'employé pour se déplacer latéralement à l'intérieur du réseau et compromettre d'autres systèmes.
- Empêcher les informations sensibles de transiter à l'extérieur du réseau.
- Garantir que les applications appropriées fonctionnent sur un réseau sécurisé.
- Décrypter le trafic de manière sélective. Par exemple, créez une politique et un profil de décryptage pour exclure le trafic des sites financiers ou relatifs à la santé du décryptage.

Le décryptage du proxy SSH n'est pas pris en charge dans Strata Cloud Manager.

Politiques de décryptage

Strata Cloud Manager fournit deux types de règles de politique de décryptage : Proxy de transfert SSL pour contrôler le trafic SSL sortant et inspection entrante SSL pour contrôler le trafic SSL entrant.

Proxy de transfert SSL

Lorsque vous configurez le pare-feu pour qu'il déchiffre le trafic SSL destiné à des sites externes, il fonctionne comme un serveur de proxy de transfert SSL. Utilisez une politique de décryptage de proxy de transfert SSL pour décrypter et inspecter le trafic SSL/TLS des utilisateurs internes vers le Web. Le déchiffrement de proxy de transfert SSL empêche le fichier malveillant dissimulé en tant que trafic chiffré SSL d'entrer dans votre réseau d'entreprise en le déchiffrant de sorte que le pare-feu puisse appliquer des profils de décryptage, des stratégies de sécurité et des profils au trafic.

Inspection SSL entrante

Utilisez l'inspection SSL entrant pour déchiffrer et inspecter le trafic entrant SSL/TLS d'un client vers un serveur réseau ciblé (tout serveur pour lequel vous avez le certificat et que vous pouvez importer sur le pare-feu) et bloquer les sessions suspectes. Par exemple, supposons qu'un acteur malveillant souhaite exploiter une vulnérabilité connue de votre serveur Web. Le décryptage SSL/TLS entrant offre une visibilité sur le trafic, permettant au pare-feu de répondre à la menace de manière proactive.

Profils de décryptage

Vous pouvez associer un profil de déchiffrement à une règle de politique pour appliquer des paramètres d'accès granulaires au trafic, comme les vérifications des certificats du serveur, les modes non pris en charge et les échecs.

Profils de proxy de transfert SSL

Le profil de décryptage du proxy de transfert SSL contrôle la vérification du serveur, les contrôles du mode de session et les contrôles d'échec pour le trafic SSL/TLS sortant défini dans les stratégies de décryptage du proxy de transfert auxquelles vous attachez le profil.

Profils d'inspection SSL entrante

Le profil de décryptage d'inspection entrante SSL contrôle les vérifications du mode de session et les vérifications d'échec pour le trafic SSL/TLS entrant défini dans les stratégies de décryptage d'inspection entrante auxquelles vous attachez le profil.

Profil pour l'absence de déchiffrement

Aucun profil de décryptage n'effectue de vérification du serveur pour le trafic que vous choisissez de ne pas déchiffrer. Vous joignez un profil Aucun décryptage à une politique de décryptage Aucun décryptage qui définit le trafic à exclure du décryptage. (N'utilisez pas la politique pour exclure le trafic que vous ne pouvez pas décrypter parce qu'un site interrompt le décryptage pour des raisons techniques, comme un certificat épinglé ou une authentification mutuelle. Ajoutez plutôt le nom d'hôte à la liste d'exclusion du décryptage.)

Conseils de décryptage

- **Utilisez les règles de politique relatives aux bonnes pratiques comme point de départ pour élaborer votre politique de décryptage**

  Ces règles, l'une qui décrypte le trafic et l'autre qui exclut le contenu sensible du décryptage, sont construites sur la base de catégories d'URL.

- **Exclure le contenu sensible du décryptage**

  Excluez le contenu sensible du décryptage pour des raisons commerciales, juridiques ou réglementaires.

  - Exclusions de décryptage prédéfinies : Palo Alto Networks conserve cette liste d'exclusions et la met à jour régulièrement. Cette liste s'applique globalement et par défaut à tout le trafic auxquels vous spécifiez pour le décryptage. Vous pouvez désactiver les entrées de la liste si cela correspond aux besoins de votre entreprise.
  - Exclusions personnalisées : excluez globalement les sites ou les applications du décryptage.
  - Exclusions basées sur des politiques : utilisez des catégories d'URL et des listes dynamiques externes pour créer des règles de décryptage ciblées et basées sur des politiques. Définissez

une action de règle de politique de décryptage sur **no-decrypt (aucun décryptage)** pour exclure le trafic correspondant du décryptage.

Placez toujours les exclusions de décryptages en haut de vos règles de politique, afin qu'elles soient appliquées en premier.

- **Considérez que vous pouvez appliquer certains paramètres de décryptage à l'échelle mondiale et en cibler d'autres à des emplacements spécifiques**
  - Votre politique de décryptage Strata Cloud Manager est appliquée globalement à tous les NGFW et emplacements Prisma Access.

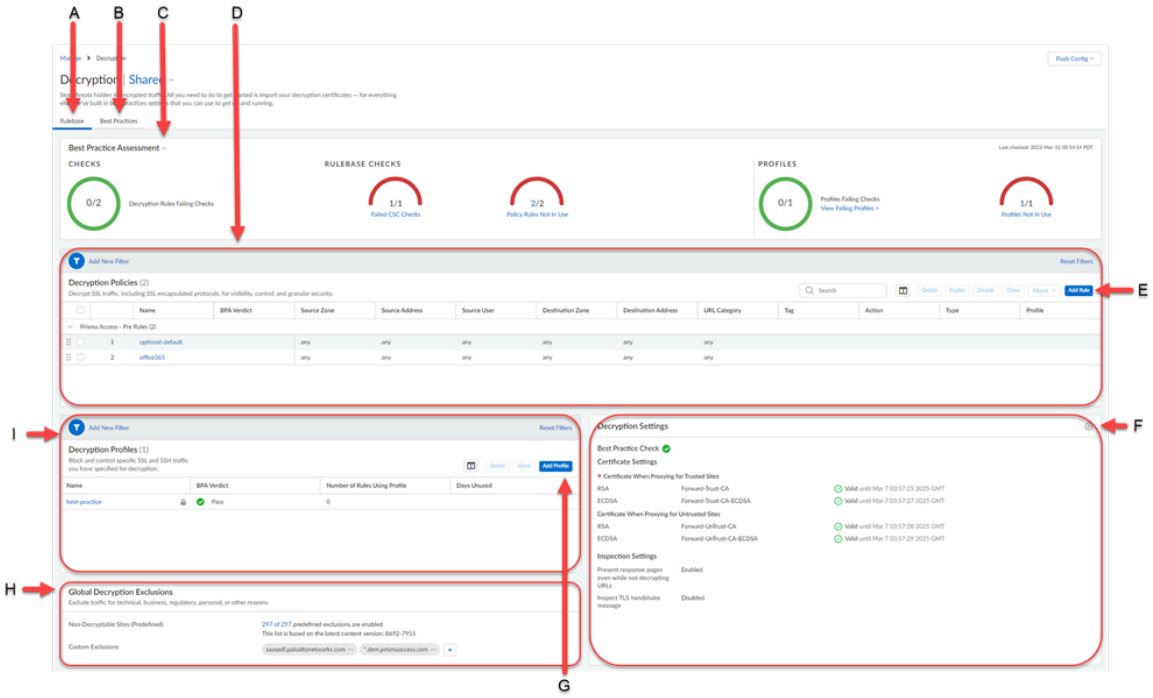
    Gestion > **Configuration** > **NGFW et Prisma Access** > **Services de sécurité** > **Déchiffrement**
  - Accédez à la politique de décryptage pour chaque type afin de créer des règles de politique ciblant des pare-feu spécifiques, des emplacements d'utilisateurs mobiles, des sites réseau distants ou des connexions de service

    Gestion > **Configuration** > **NGFW et Prisma Access** > **Portée de la configuration** > **Global / Pare-feu / Utilisateurs mobiles / Réseaux distants / Connexions de service**
- **L'ordre des règles est important**

  Les règles de la politique de décryptage sont appliquées de haut en bas. Placez les règles que vous souhaitez appliquer en premier en haut de votre liste de règles de politique de décryptage. Les règles globales (règle « avant ») sont appliquées en premier et sont toujours répertoriées avant les règles spécifiques aux utilisateurs mobiles, aux réseaux distants et aux connexions de service.

Le décryptage en bref

L'écran Décryptage est l'endroit où vous pouvez configurer les politiques et les profils de décryptage et afficher vos évaluations des meilleures pratiques.



A) Base de règles : les vérifications de la base de règles examinent la manière dont la politique de sécurité est organisée et gérée, y compris les paramètres de configuration qui s'appliquent à de nombreuses règles.

B) Meilleures pratiques : ici, vous pouvez obtenir une vue complète de la manière dont votre implémentation de fonctionnalité s'aligne sur les meilleures pratiques. Examinez les vérifications ayant échoué pour voir où vous pouvez apporter des améliorations (vous pouvez également examiner les vérifications réussies).

C) Évaluation des meilleures pratiques : les scores des meilleures pratiques sont affichés sur le tableau de bord de décryptage. Ces scores vous donnent un aperçu de vos progrès réalisés à ce qui concerne les meilleures pratiques. En un coup d'œil, vous pouvez identifier les domaines nécessitant une enquête plus approfondie ou les domaines dans lesquels vous souhaitez prendre des mesures pour améliorer votre posture de sécurité.

D) Politiques de décryptage : liste des politiques de décryptage intégrées. Vérifiez la configuration de la politique, le type de politique (*proxy de transfert SSL*, *inspection SSL entrante*ou *proxy SSH*), l'action de la politique (*décryptage* ou *aucun décryptage*) et le verdict BPA.

E) Ajouter une règle : ajoutez et configurez de nouvelles stratégies de décryptage.

F) Paramètres de déchiffrement : accédez aux paramètres du certificat et du décryptage. Certificats d'importation et d'exportation.

G) Ajouter un profil : ajoutez et configurez de nouveaux profils de décryptage.

H) Exclusions de décryptage globales : applications exclues du décryptage.

I) Profils de décryptage : liste des profils de décryptage intégrés. Consultez la configuration du profil, les politiques qui utilisent le profil et le verdict BPA.

Gestion : Politiques réseau

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Vous avez la possibilité de créer différents types de politiques réseau pour protéger votre réseau contre les menaces et les perturbations. Ceci vous permet d'optimiser l'allocation des ressources réseau et de gérer vos politiques réseau afin de hiérarchiser le trafic et de configurer les classifications des applications.

Les règles sont évaluées du haut vers le bas et lorsque le trafic correspond aux critères de la règle définie, les règles suivantes ne sont pas évaluées. Vous devez ordonner des règles de politique plus spécifiques au-dessus des règles plus génériques afin d'appliquer les meilleurs critères de correspondance possibles. Un journal est généré pour le trafic qui correspond à une règle de politique lorsque la journalisation est activée pour la règle. Les options de journalisation sont configurables pour chaque règle.

Les règles de politique de meilleures pratiques sont disponibles pour la plupart des types de politiques et vous aident à démarrer rapidement et en toute sécurité. Bien que ces règles ne puissent pas être modifiées pour garantir que vous disposez toujours d'un niveau minimum de sécurité, vous pouvez les cloner si vous souhaitez les utiliser comme base pour personnaliser votre politique.

Accédez à **Manage (Gestion)** > **Configuration (Configuration)** > **Network Policies (Politiques de réseau)** > **NGFW and Prisma Access (NGFW et Prisma Access)**.

Avec les politiques réseau, vous pouvez :

- Donnez la priorité au trafic le plus important pour vos opérations avec Gestion : QoS.
- Gérez comment Prisma Access classe vos applications avec Gestion : Contrôle prioritaire sur l'application.

Gestion : QoS

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	L'une des options suivantes : ☐ Licence Prisma Access ☐ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Grâce à Quality of Service (qualité de service - QoS), vous pouvez prioriser le trafic critique de l'entreprise et les applications nécessitant une faible latence (comme la VoIP et les applications vidéo).Pour ajouter ou modifier une règle de politique QoS, accédez à **Manage (Gestion)** > **Configuration (Configuration)** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Network Policies (Politiques de réseaux)** > **QoS**.

Règle de politique QoS

Règles de politique de Quality of Service (qualité de service - QoS) pour identifier le trafic nécessitant un traitement préférentiel ou une limitation de la bande passante. Les règles QoS vous permettent d'exécuter de manière fiable les applications et le trafic à priorité élevée avec une capacité réseau limitée. Vous pouvez configurer le traitement QoS du trafic à l'aide des points de code de services différenciés (DSCP). Ces points de code sont des valeurs d'en-tête de paquet qui peuvent être utilisées pour demander (par exemple) une haute priorité ou une livraison au mieux pour le trafic. Prisma Access applique les valeurs DSCP pour le trafic entrant et marque une session avec une valeur DSCP lorsque le trafic de session quitte le pare-feu. Cela signifie que tout le trafic entrant et sortant d'une session bénéficie d'un traitement QoS continu. Vous pouvez configurer le traitement de la QoS du trafic en utilisant les points de code suivants :

- **Expédition rapide (EF)**—Permet de demander une bande passante garantie à faible perte et faible latence pour le trafic.

  Les paquets avec des valeurs de point de code EF sont généralement garantis avec la plus haute priorité

  .
- **Expédition assurée (AF)**—Utilisée pour fournir une livraison fiable pour les applications.

  Les paquets avec points de code AF indiquent une requête pour que le trafic reçoive un traitement plus prioritaire que le meilleur effort fourni. Les paquets avec points de code EF ont priorité sur les paquets avec code de point AF.
- **Sélecteur de classe (CS)**—Permet d'assurer la compatibilité ascendante avec les adresses IP du réseau utilisant le champ de préséance IP pour marquer le trafic prioritaire.
- **Priorité IP (ToS)**—Utilisée par les adresses IP réseau héritées pour marquer le trafic prioritaire.

- **Point de code personnalisé**—Permet de créer un point de code personnalisé à mettre en correspondance avec le trafic en saisissant un Codepoint Name (Nom de point de code) et une Binary Value (Valeur binaire).

  Par exemple, vous pouvez créer une règle de politique QoS pour prioriser les communications vocales, telles que la Voice over IP (voix sur IP - VoIP), afin de garantir une transmission cohérente des paquets. Cela garantit une communication vocale cohérente.

Gestion : Contrôle prioritaire sur l'application

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Créer une politique de contrôle prioritaire sur l'application afin de désigner les applications à traiter en utilisant le chemin rapide de l'inspection de la couche 4 au lieu d'utiliser l'App-ID pour l'inspection de la couche 7. Cette mesure oblige le nœud d'application de la sécurité à traiter la session comme une vérification régulière avec état. Elle permet d'économiser les temps de traitement de l'application. Vous pouvez créer une règle de politique de contrôle prioritaire sur l'application lorsque vous ne souhaitez pas contrôler le trafic des applications propre à l'entreprise entre des adresses IP connues. Par exemple, si vous avez une application propre à l'entreprise sur un port non standard, sachant que les utilisateurs accédant à l'application sont sanctionnés et que les deux se trouvent dans la zone approuvée, vous pouvez remplacer les exigences d'inspection de l'application pour les utilisateurs de confiance accédant à l'application propre à l'entreprise.

Afin de modifier la façon dont Prisma Access classe les applications, rendez-vous sur **Manage (Gérer)** > **Configuration (Configuration)** > **NGFW et Prisma Access** > **Network Policies (Politiques réseau)** > **Application Override (Contrôle prioritaire sur l'application)** pour ensuite créer votre règle de politique de contrôle prioritaire sur l'application.

Conseils relatifs au contrôle prioritaire sur l'application.

Lorsque vous créez une règle de politique de contrôle prioritaire sur l'application, vous empêchez App-ID de classer le trafic de votre déploiement et d'effectuer une inspection des menaces sur la base de l'identification de l'application. Afin de prendre en charge les applications propriétaires internes, il est utile de penser à créer une application propre à l'entreprise (au lieu d'une règle de contrôle prioritaire sur l'application) qui inclut la signature de l'application afin que Strata Cloud Manager effectue une vérification de couche 7 et analyse le trafic de l'application afin d'identifier

des menaces. Afin de créer une application propre à l'entreprise, accédez à **Gérer** > **Configuration** > **NGFW et Prisma Access** > **Objets** > **Applications**.

Politiques de règles de contrôle prioritaire sur l'application

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

- **Source**
  - **Zones**—**Ajouter** des zones sources.
  - **Adresses**—**Ajouter** adresses sources, groupes d'adresses ou régions et spécifiez les paramètres.
- **Destination**
  - **Zones**—**Ajouter** pour choisir les zones de destination.
  - **Adresses**—**Ajouter** adresses sources, groupes d'adresses ou régions et spécifiez les paramètres.
- **Application**
  - **Application** : sélectionnez le contrôle prioritaire sur l'application pour les flux de trafic qui correspondent aux critères de règle ci-dessus. Lors du contrôle prioritaire d'une application personnalisée, aucune inspection des menaces n'est effectuée, La seule exception à cette règle est le remplacement par une application prédéfinie qui prend en charge la vérification des menaces.

    Afin de définir de nouvelles applications, accédez à **Manage (Gérer)** > **Configuration (Configuration)** > **NGFW et Prisma Access** > **Objects (Objets)** > **Applications (Applications)**.
- **Protocole**
  - **Protocole** : sélectionnez le protocole (**TCP** ou **UDP**) pour laquelle autoriser un contrôle prioritaire sur l'application.
  - **Port** : saisir le numéro de port (de 0 à 65535) ou la plage de numéros de ports (port1-port2) pour les adresses de destination définies. Utiliser des virgules pour séparer les ports ou les plages.

Gestion : Transfert basé sur une politique

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	dépendent de la ou des licences que vous utilisez.

Les règles de transfert basé sur une politique permettent au trafic d'emprunter un autre chemin que le prochain saut spécifié dans la table de routage. Elles sont généralement utilisées pour spécifier une interface de sortie pour des raisons de sécurité ou de performance.

Accédez à **Manage (Gestion)** > **Configuration (Configuration)** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Network Policies (Politiques de réseaux)** > **Policy Based Forwarding (Transfert basé sur une politique)**.

Utilisez une règle de transfert basé sur une politique pour diriger le trafic vers une interface de sortie spécifique et remplacer le chemin par défaut du trafic. Avant de créer une règle de transfert basé sur une politique, assurez-vous de comprendre que l'ensemble d'adresses IPv4 est traité comme un sous-ensemble de l'ensemble d'adresses IPv6.

Utilisez les sections suivantes pour configurer une règle de transfert basée sur une politique :

- **Source**
  - **Zones**—**Ajouter** des zones sources.
  - **Interface**—**Ajoutez** l'interface source.
  - **Adresses**—**Ajoutez** des adresses de source, des groupes d'adresses ou des régions et spécifiez les paramètres.
  - **Utilisateurs**—**Ajoutez** les utilisateurs et les groupes d'utilisateurs auxquels la politique s'applique.
- **Destination**
  - **Adresses**—**Ajoutez** des adresses sources, des groupes d'adresses ou des régions et spécifiez les paramètres.
- **Applications et services**
  - **Entités d'application** — Sélectionnez les applications que vous souhaitez acheminer par d'autres chemins.

    Ainsi, une règle de transfert basé sur une politique peut être appliquée avant que le pare-feu dispose de suffisamment d'informations pour déterminer l'application. Par conséquent, les règles propres à une application ne sont pas recommandées pour être utilisées avec le transfert basé sur une politique. Dans la mesure du possible, utilisez un objet de service.

    Vous ne pouvez pas utiliser d'applications propres à l'entreprise, de filtres d'applications ou de groupes d'applications dans les règles de transfert basé sur des stratégies.
  - **Entités de service**—Sélectionnez les services et les groupes de services que vous souhaitez acheminer par des canaux alternatifs.

- **Transfert**
  - **Action**—Vous pouvez définir l'Action à effectuer lorsque vous faites correspondre un paquet en choisissant parmi :
    - **Transférer**—Dirige le paquet vers **l'interface de sortie spécifiée**.
    - **Supprimer**—abandonne le paquet.
    - **No PBF**—Exclut les paquets qui correspondent aux critères de source, de destination, d'application ou de service définis dans la règle. Les paquets correspondants utilisent la table des routes au lieu de PBF.
  - **Interface de sortie**—Sélectionnez les informations réseau à l'endroit où vous souhaitez transférer le trafic correspondant à votre règle de transfert basé sur une politique.
  - **Prochaine étape**
    - **IP Address IP**—saisissez une adresse IP, ou sélectionnez un objet d'adresse de type masque réseau IP, à laquelle le pare-feu transfère les paquets mis en correspondance.
    - **FQDN**—saisissez un FQDN (ou sélectionnez ou créez un objet d'adresse de type FQDN) auquel le pare-feu transfère les paquets mis en correspondance.
    - **Aucun**—en l'absence d'un saut suivant, l'adresse IP de destination du paquet est utilisée comme saut suivant. Le transfert échoue si l'adresse IP de destination n'est pas dans le même sous-réseau que l'interface de sortie.
  - **Surveiller**—Activez la surveillance pour vérifier la connexion à une adresse IP cible ou à l'adresse IP de saut suivant si aucune adresse IP n'est spécifiée

Gestion : NAT

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

NAT vous permet de traduire les adresses IPv4 privées non routables en une ou plusieurs adresses IPv4 globalement routables, conservant ainsi les adresses IP routables d'une entreprise. NAT vous permet également de ne pas divulguer les adresses IP réelles des hôtes qui nécessitent un accès à des adresses publiques. Il vous permet également de gérer le trafic en effectuant une redirection de port. Vous pouvez utiliser NAT pour résoudre des problèmes de conception réseau

et permettre ainsi aux réseaux disposant de sous-réseaux IP identiques de communiquer entre eux.

Vous pouvez configurer une règle de politique NAT pour qu'elle corresponde au moins à la zone source et à la zone de destination d'un paquet. Outre les zones, vous pouvez configurer des critères de correspondance en fonction du service, de l'adresse source et de destination, et de l'interface de destination du paquet. Vous pouvez configurer plusieurs règles NAT.

Accédez à **Manage (Gestion)** > **Configuration (Configuration)** > **Network Services (Services de réseau)** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **NAT**.

Troubleshoot (Résolvez) *les problèmes de connectivité : obtenez une vue globale de vos états de routage et de tunnel, et explorez les détails pour trouver les anomalies et les configurations problématiques.*

Gestion : SD-WAN

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• SD-WAN	❑ licence SD-WAN

Une règle de politique SD-WAN spécifie les applications et/ou les services et un profil de distribution de trafic pour déterminer comment le pare-feu sélectionne le chemin préféré pour un paquet entrant qui n'appartient pas à une session existante et qui correspond à tous les autres critères comme les zones de source et destination, les adresses IP source et destination et l'utilisateur source. La règle de politique SD-WAN spécifie aussi un profil de qualité de chemin pour les seuils de latence, instabilité et perte de paquets. Lorsque l'un des seuils est dépassé, le pare-feu sélectionne un nouveau chemin pour les applications et/ou les services.

Pour configurer une politique SD-WAN, sélectionnez**Manage (Gestion)** > **Configuration (Configuration)** > **Network Policies (Politiques réseau)** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **SD-WAN**.

Règles

Vous pouvez définir les Règles avant et les Règles après dans un contexte partagé, comme politiques partagées pour tous les pare-feu gérés ou dans un contexte de groupe de périphériques pour que les règles soient spécifiques à un groupe de périphériques :

- **Pré-règles**—Règles ajoutées au début de la liste des règles et évaluées en premier. Vous pouvez utiliser les pré-règles pour faire respecter la Politique d'utilisation acceptable d'une organisation. Par exemple, vous pouvez bloquer l'accès à des catégories d'URL spécifiques ou permettre du trafic DNS pour tous les utilisateurs.
- **Post-règles après**—Les règles ajoutées en fin de liste des règles et évaluées après les règles avant, et les règles définies localement sur le pare-feu. Les pré-règles comprennent généralement des règles visant à refuser l'accès au trafic sur la base de l'**App-ID™**, **User-ID™** ou d'un **Service**.

Profils

Créez des profils à appliquer à des ensembles d'applications et services indiqués dans les règles de politique SD-WAN.

Qualité du chemin

SD-WAN vous permet de créer un profil de qualité de chemin pour chaque ensemble d'applications, de filtres d'application, de groupes d'applications, de services, d'objets de service et d'objets de groupe de service qui ont des exigences uniques en matière de qualité de réseau et de référencer le profil dans une règle de politique SD-WAN. Dans le profil, vous définissez le seuil maximum de trois paramètres : la latence, la gigue et la perte de paquets. Lorsqu'un lien SD-WAN dépasse un de ces seuils, le pare-feu sélectionne un meilleur chemin d'accès pour les paquets qui correspond à la règle SD-WAN où vous appliquez ce profil.

Qualité SaaS

SD-WAN vous permet de créer des profils de qualité SaaS (Software-as-a-Service) pour mesurer la qualité du chemin entre votre pare-feu de concentrateur ou de succursale et les applications SaaS côté serveur afin de surveiller avec précision la fiabilité de l'application SaaS et de changer de chemin en cas de dégradation de la qualité du chemin. Cela permet au pare-feu de déterminer avec précision quand basculer vers un lien d'Accès Internet Direct (DIA) différent.

Le profil de qualité SaaS vous permet d'indiquer l'application SaaS à surveiller en utilisant un algorithme d'apprentissage adaptatif qui surveille l'activité de l'application ou en indiquant l'application SaaS qui utilise l'adresse IP, le FQDN ou l'URL de l'application.

Répartition du trafic

Pour ce profil de distribution du trafic, sélectionnez la méthode utilisée par le pare-feu pour distribuer les sessions et basculer vers un meilleur chemin lorsque la qualité du chemin se détériore. Ajoutez les étiquettes de liens que le pare-feu doit considérer lorsqu'il détermine le lien par lequel il transfère le trafic SD-WAN. Vous appliquez un profil de distribution du trafic à chaque règle de politique SD-WAN que vous créez.

Correction d'erreur

Si votre trafic SD-WAN inclut une application qui est sensible à la perte de paquets ou à la corruption, comme de l'audio, VoIP ou vidéo-conférence, vous pouvez appliquer soit la Forward Error Correction (FEC) ou la duplication de paquets en tant que moyen de correction de l'erreur. Avec FEC, le pare-feu récepteur (décodeur) peut récupérer des paquets perdus ou corrompus en utilisant des bits de parité que l'encodeur intègre dans un flux d'application. La duplication de paquet est une autre méthode de correction d'erreur dans laquelle une session d'application est dupliquée depuis un tunnel vers un second tunnel. Pour utiliser une de ces méthodes, créez un Profil de correction des erreurs et référencez-le dans une règle de politique SD-WAN pour des applications spécifiques.

(Vous devez également spécifier les interfaces accessibles au pare-feu pour la correction d'erreurs en indiquant dans un profil d'interface SD-WAN les interfaces éligibles pour la sélection d'interface du profil de correction d'erreurs.)

Interface SD-WAN

Créez un profil d'interface SD-WAN pour définir les caractéristiques des connexions ISP et spécifier la vitesse des liens et la fréquence selon laquelle le pare-feu surveille le lien, et spécifier une Étiquette de liens pour le lien. Lorsque vous spécifiez la même Étiquette de liens pour

plusieurs liens, vous regroupez ces liens physiques dans un lot de liens ou dans un fat pipe. Vous devez configurer un profil d'interface SD-WAN et le spécifier pour une interface Ethernet activée avec SD-WAN avant de pouvoir sauvegarder l'interface Ethernet.

Étiquettes de liens

Créez une étiquette de liens afin d'identifier un ou plusieurs liens physiques que vous souhaitez que les applications et les services utilisent dans un ordre spécifique au cours d'une distribution de trafic SD-WAN et d'une protection par basculement. Le regroupement de plusieurs liens physiques vous permet de maximiser la qualité des applications et des services si l'état du lien physique se détériore.

Lorsque vous planifiez comment regrouper vos liens, tenez compte de l'utilisation ou de l'objectif des liens et regroupez les en conséquence. Par exemple, si vous configurez des liens prévus pour un trafic à faible coût ou non crucial pour l'entreprise, créez une étiquette de liens et groupez ces interfaces ensemble afin de vous assurer que le trafic prévu passe principalement sur ces liens et pas sur des liens plus onéreux qui peuvent avoir un impact sur des applications ou des services critiques pour l'entreprise.

Gestion : Services d’identité

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l’accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Apprenez à gérer vos services d’identité et confirmez que seuls certains utilisateurs peuvent accéder aux bonnes données sur votre réseau.

Accédez à **Manage (Gestion)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identity Services (Services d’identité)**.

Grâce aux services d’identité, vous avez la possibilité de :

- Autoriser uniquement les utilisateurs légitimes à accéder à votre réseau en connectant Prisma Access à votre fournisseur d’identité (IdP) et en choisissant la méthode d’authentification que vous souhaitez utiliser, dans Gestion : Authentification.
- Donner à Prisma Access un accès en lecture seule à vos informations Active Directory avec leGestion : Moteur d'identité sur le cloud.
- Renforcer votre politique de sécurité de manière cohérente et partager les données d’identité avec les périphériques locaux sur des sites réseau distants ou des sites de connexion de service (siège social et centres de données) avec Gestion : Redistribution d’identité.

Gestion : Authentification

Où puis-je l’utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l’accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	→ Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Afin de s'assurer que seuls les utilisateurs légitimes ont accès à vos ressources les plus protégées, Prisma Access prend en charge plusieurs types d'authentification, notamment SAML, TACACS+, RADIUS, LDAP, Kerberos, MFA, l'authentification de base de données locale et SSO.

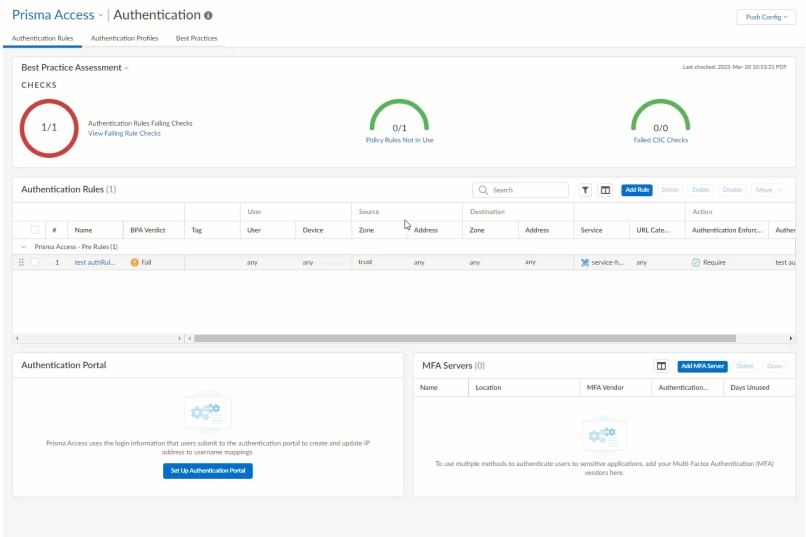
Afin de configurer vos stratégies d'authentification, accédez à **Manage (Gérer)** > **Configuration (Configuration)** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identity Services (Services d'identité)** > **Authentication (authentification)**.

Les services qui s'intègrent avec Prisma Access afin de fournir l'authentification, et les fonctionnalités à prendre en compte lorsque vous planifiez votre configuration d'authentification sont énumérés ci-après :

Appui à l'authentification

SAML	Si vos utilisateurs accèdent à des services et applications externes à votre réseau, vous pouvez utiliser SAML pour intégrer Prisma Access à un fournisseur d'identité (IdP) chargé de contrôler l'accès aux services et applications internes et externes. Single Sign-On (ouverture de session unique - SSO) SAML permet à un seul utilisateur d'accéder à plusieurs applications. Elle est utile dans les environnements où chaque utilisateur accède à de nombreuses applications et où l'authentification pour chacune d'entre elles entraverait la productivité de l'utilisateur. Dans ce cas, Single Sign-On (ouverture de session unique - SSO) SAML permet à une connexion d'accéder à plusieurs applications. Dans le même ordre idée, le service de déconnexion unique (SLO) en SAML permet de fermer une session accédant à plusieurs applications en se déconnectant d'une seule session. SSO fonctionne pour les utilisateurs mobiles qui accèdent aux applications via l'application GlobalProtect. De même que les utilisateurs des réseaux distants qui accèdent aux applications via le portail d'authentification. SLO est disponible pour les utilisateurs de l'application GlobalProtect. *Vous ne pouvez pas utiliser les profils d'authentification SAML pour des séquences d'authentification.*
TACACS+	Terminal Access Controller Access-Control System Plus (TACACS+) est une famille de protocoles permettant une authentification et une autorisation à partir d'un serveur centralisé. TACACS+ crypte les noms d'utilisateurs et mots de

	passe, assurant ainsi une meilleure sécurité que RADIUS, qui crypte uniquement les mots de passe. TACACS+ est aussi plus fiable car il utilise le protocole TCP, alors que RADIUS utilise le protocole UDP.
RADIUS	Radius (Remote Authentication Dial-In User Service) est un protocole réseau bénéficiant d'un large support et fournissant une authentification et une autorisation centralisées. Vous pouvez également ajouter un serveur RADIUS à Prisma Access en vue d'implémenter une authentification multi-facteurs.
LDAP	LDAP (Lightweight Directory Access Protocol) est un protocole standard d'accès aux répertoires d'informations. Vous pouvez utiliser LDAP pour authentifier les utilisateurs qui accèdent à des applications ou des services via le portail d'authentification.
Kerberos	Kerberos est un protocole d'authentification qui permet un échange sécurisé d'informations entre les parties en utilisant des clés uniques (appelées tickets) pour identifier les parties. Avec Kerberos, vous pouvez authentifier les utilisateurs qui accèdent aux applications via le portail d'authentification. Lorsque la SSO Kerberos est activée, l'utilisateur doit se connecter uniquement pour un premier accès au réseau (par exemple, une connexion à Microsoft Windows). À l'issue de cette première connexion, l'utilisateur peut accéder à n'importe quel service basé sur un navigateur dans le réseau sans avoir à se connecter à nouveau jusqu'à l'expiration de la session SSO. Pour utiliser Kerberos, vous devez d'abord avoir un compte Kerberos pour Prisma Access qui authentifiera les utilisateurs. Un compte permet de créer un keytab Kerberos qui est un fichier contenant le nom principal et le mot de passe haché du pare-feu ou de Panorama. Un keytab est indispensable au processus SSO. Kerberos SSO est disponible uniquement pour les services et les applications internes à votre environnement Kerberos. Lorsque la SSO est activée pour des services et applications externes, il est possible d'utiliser SAML.
Moteur d'identité sur le cloud	Le moteur d'identité cloud (CIE) fournit à la fois l'identification et l'authentification des utilisateurs mobiles dans le cadre d'un déploiement Prisma Access-Proxy explicite. Le moteur d'identité cloud s'intègre au service de cache d'authentification par proxy explicite (ACS). Il utilise des fournisseurs d'identité SAML (IdP) pour fournir une authentification aux utilisateurs mobiles de proxy explicite.

MFA	L'authentification multi-facteurs (MFA) vous permet de mettre en œuvre plusieurs défis d'authentification de différents types (appelés *facteurs*) pour protéger vos services et applications les plus sensibles. Par exemple, vous pourriez souhaiter disposer d'une authentification plus forte pour les documents financiers clés que pour les moteurs de recherche. Prisma Access dispose d'une liste intégrée des fournisseurs MFA pris en charge. Cette liste est automatiquement mise à jour au fur et à mesure que de nouveaux fournisseurs sont ajoutés : 
Authentification de base de données locale	Créez une base de données qui s'exécute localement sur Prisma Access et contient des comptes d'utilisateurs (noms d'utilisateur et mots de passe ou mots de passe hachés). Ce type d'authentification est utile pour créer des comptes d'utilisateurs qui réutilisent les informations d'identification des comptes Unix existants dans les cas où vous connaissez uniquement les mots de passe hachés, pas les mots de passe en texte brut. Pour les comptes utilisant des mots de passe en clair, vous pouvez également définir la complexité du mot de passe et les paramètres d'expiration. Cette méthode d'authentification est disponible pour les utilisateurs qui accèdent aux services et applications via le portail d'authentification ou l'application GlobalProtect.

Caractéristiques de la fonctionnalité d'authentification

SSO	Si vous utilisez SAML ou Kerberos, vous pouvez mettre en œuvre une Single Sign-On (ouverture de session unique - SSO), qui permet aux utilisateurs de ne s'authentifier qu'une seule fois pour accéder à plusieurs

	services et applications. SAML et Kerberos prennent en charge la SSO.
Portail d'authentification	Rediriger les requêtes Web qui correspondent à une règle d'authentification vers une page de connexion Prisma Access où elles sont invitées à s'authentifier. Prisma Access utilise les informations que l'utilisateur soumet à ce portail d'authentification pour créer ou mettre à jour des correspondances d'adresse IP avec les noms d'utilisateur. Ceci est particulièrement utile pour les réseaux distants, afin que vous continuiez à surveiller et à appliquer le trafic en fonction d'un utilisateur (ou d'un groupe). Lorsqu'un utilisateur initie le trafic Web (HTTP ou HTTPS) correspondant à une règle, Prisma Access invite l'utilisateur à s'authentifier via le portail d'authentification. Prisma Access crée ou met à jour la correspondance entre l'adresse IP et le nom d'utilisateur en fonction des informations que l'utilisateur soumet au portail. Cela vous permet de savoir exactement qui accède à vos applications et données les plus sensibles à partir d'un site réseau distant.
Séquence d'authentification	Si vous utilisez plusieurs types d'authentification à différentes fins, vous pouvez définir une séquence d'authentification pour classer vos profils. Prisma Access recherche chaque profil sur la base de votre classement, jusqu'à ce que l'un d'entre eux authentifie l'utilisateur.

Fonctionnement de l'authentification

Après avoir ajouté les services d'authentification de votre organisation à Prisma Access (voici comment), Prisma Access authentifie les utilisateurs à plusieurs points :

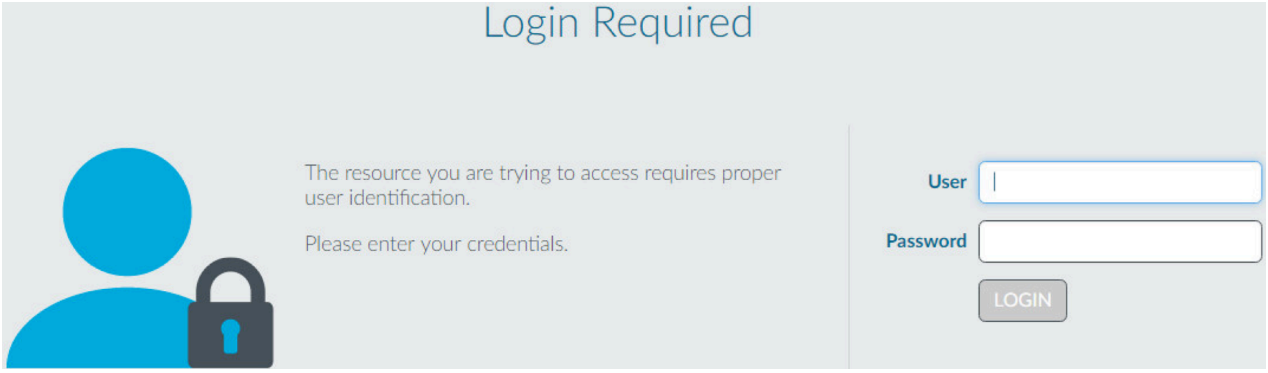
- **Lorsqu'ils se connectent à Prisma Access**

  Voici comment définir la manière dont vous souhaitez que les utilisateurs mobiles s'authentifient sur Prisma Access. Vous n'avez pas besoin de définir des paramètres d'authentification pour les utilisateurs de réseaux distants qui se connectent à Prisma Access, car le trafic du réseau distant est acheminé par des tunnels VPN sécurisés.

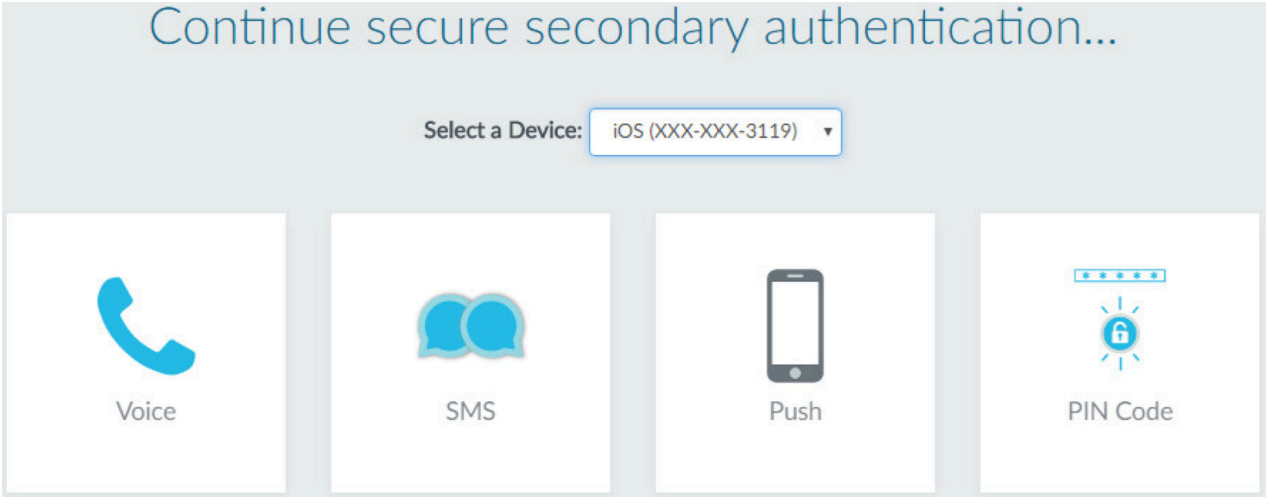
- **Lorsque le trafic des utilisateurs répond à vos exigences en matière d'authentification supplémentaire**

  Voici comment exiger que les utilisateurs s'authentifient (à l'aide d'une ou de plusieurs méthodes) pour accéder aux applications d'entreprise et aux ressources réseau protégées.

Lorsque les utilisateurs génèrent un trafic Web correspondant à vos exigences d'authentification, Prisma Access vérifie que les utilisateurs sont légitimes en les invitant à s'authentifier à l'aide d'une ou plusieurs méthodes (facteurs), telles que l'authentification par connexion et mot de passe, vocale, SMS, push ou One-Time Password (mot de passe à usage unique - OTP) : les facteurs utilisés par Prisma Access sont tous basés sur le service d'authentification et les paramètres que vous spécifiez dans vos *profils d'authentification*. Pour le premier facteur (connexion et mot de passe), les utilisateurs s'authentifient via le portail d'authentification.



Pour les autres facteurs, les utilisateurs s'authentifient ensuite via une page de connexion d'authentification multi-facteurs.



Après avoir authentifié les utilisateurs, Prisma Access évalue vos règles de sécurité pour déterminer s'il faut autoriser l'accès à l'application. Prisma Access enregistre toutes les activités où les utilisateurs tentent d'accéder à des applications, services ou ressources que vous avez désignés pour un accès sécurisé.

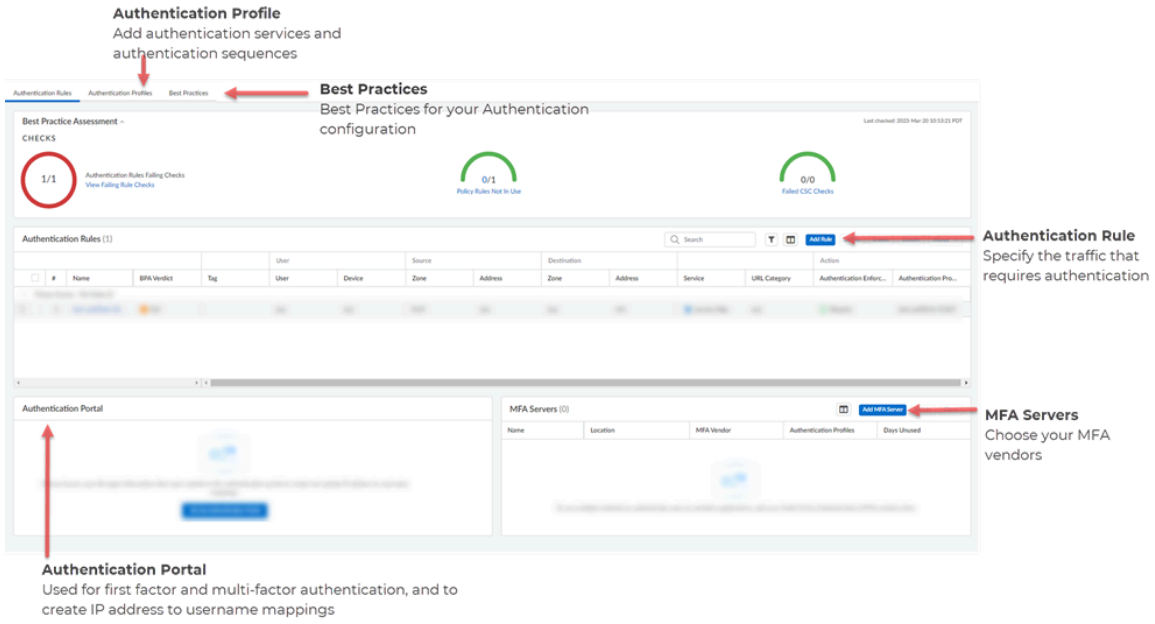
Gestion : Configuration de l'authentification

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	L'une des options suivantes : ☐ Licence Prisma Access ☐ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Pour configurer l'authentification avec Prisma Access dans Strata Cloud Manager, ajoutez d'abord votre/vos service(s) d'authentification à Prisma Access. Spécifiez ensuite le trafic

pour lequel vous souhaitez exiger une authentification. Ces paramètres permettent d'ajouter d'autres fonctionnalités d'authentification, telles que MFA, des séquences d'authentification, ou d'activer Prisma Access pour créer et mettre à jour les correspondances entre les mappages noms d'utilisateurs/adresses IP.

Voici comment commencer : tous les paramètres dont vous avez besoin pour activer l'authentification avec Prisma Access se trouvent au même endroit : **Manage (Gérer)** > **Identity Services (Services d'identité)** > **Authentification**.

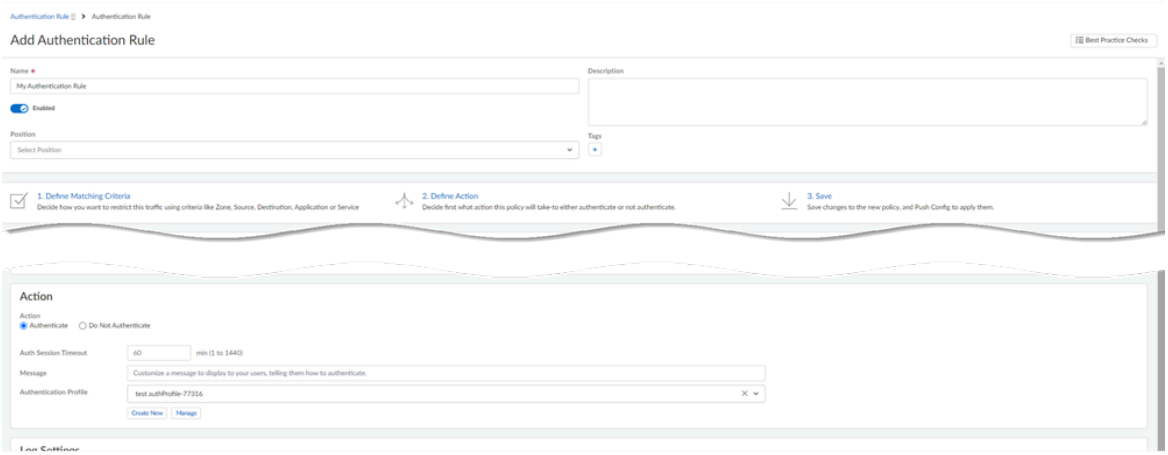


- **Règles d'authentification** C'est ici que vous spécifiez le trafic pour lequel vous souhaitez exiger une authentification

  La configuration d'une règle d'authentification inclut l'ajout d'un profil d'authentification à la règle. Lorsque Prisma Access détecte un trafic correspondant à une règle d'authentification, il applique les méthodes et paramètres d'authentification définis dans le profil d'authentification au trafic correspondant. Le profil est l'élément qui définit la manière dont les utilisateurs devront s'authentifier.

  1. Accédez à **Manage (Gérer)** > **Identity and Access Services (Services d'identité et d'accès)** > **Authentication (Authentification)** > **Authentication Rule (Règle d'authentification)** et **Add Authentication Rule (Ajouter une règle d'authentification)**.
  2. Définissez les utilisateurs, les services et les catégories d'URL qui nécessitent une authentification.

3. Attribuez la valeur **Authenticate (Authentifier)** à l'action de la règle et choisissez le **Profile (Profil)** qui définit la méthode d'authentification que vous souhaitez utiliser pour le trafic correspondant à cette règle.



- **Profil d'authentification** Ajoutez vos services d'authentification ici et définissez les paramètres d'authentification

  Connectez Prisma Access aux services que vous souhaitez utiliser pour authentifier les utilisateurs (SAML, TACACS+, RADIUS, LDAP ou Kerberos) et définissez les paramètres d'authentification (par exemple, définissez une limite pour les tentatives de connexion infructueuses).

  Si vous utilisez un service d'authentification sur site, vous devez d'abord créer une connexion de service pour connecter le service d'authentification sur site à Prisma Access. Revenez ici par la suite pour configurer votre profil d'authentification.

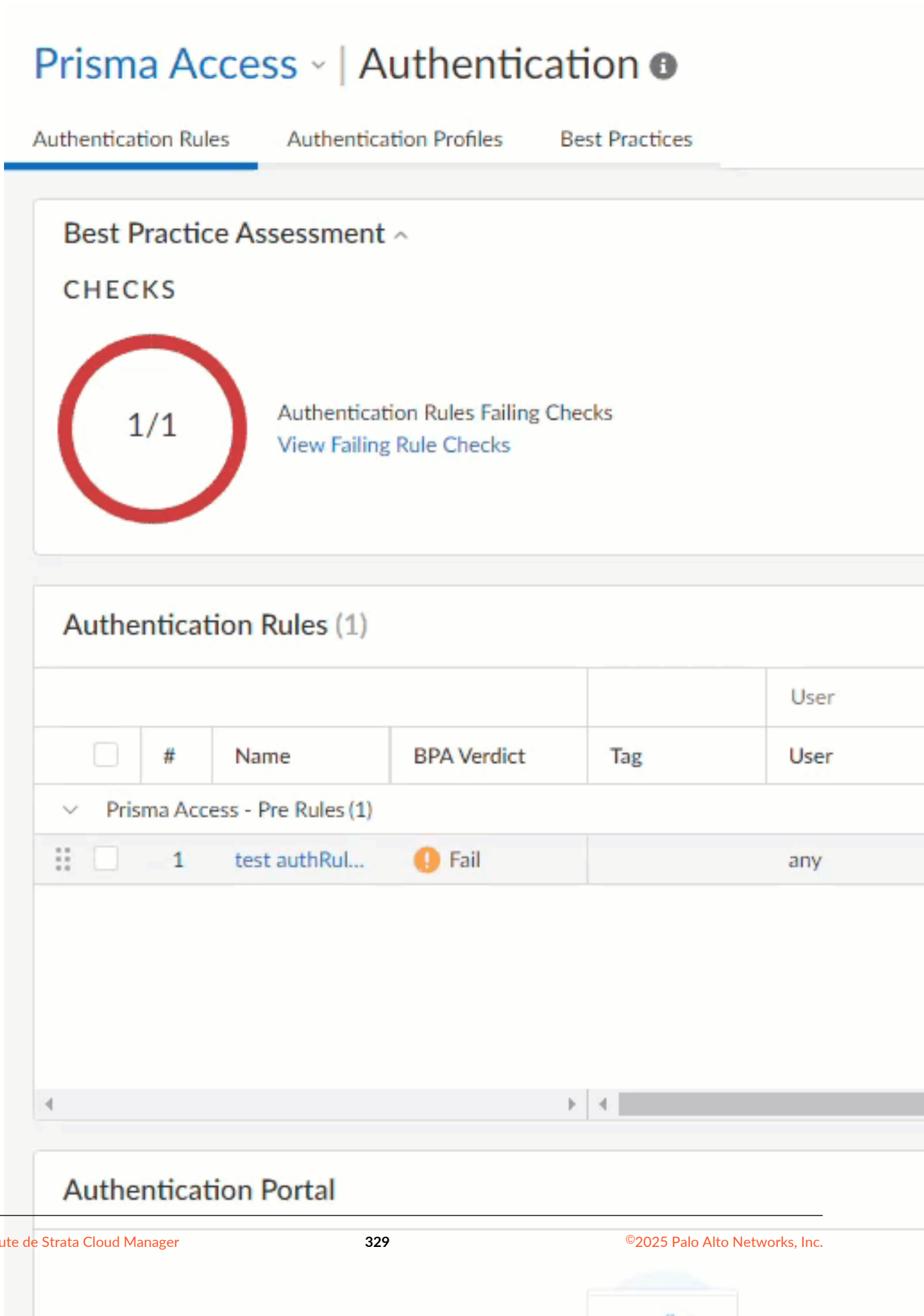
  Accédez à **Manage (Gérer)** > **Identity and Access Services (Services d'identité et d'accès)** > **Authentication (Authentification)** > **Authentication Profile (Profil d'authentification)** > **Add Profile (Ajouter un profil)** et commencez par définir le **Auth Type (Type d'authentification** du profil :

  Vous serez invité à ajouter des détails sur le service d'authentification que vous avez choisi qui permettront à Prisma Access de se connecter au service et de lire les informations d'identification de l'utilisateur et les autorisations de rôle. Des paramètres supplémentaires pour personnaliser l'authentification sont fournis dans le profil et peuvent varier en fonction du type d'authentification que vous configurez.

- **Serveurs MFA** Spécifiez le fournisseur MFA que vous utilisez

  Afin d'utiliser plusieurs méthodes pour authentifier les utilisateurs auprès d'applications sensibles, commencez par ajouter les fournisseurs MFA que vous souhaitez utiliser (**Add MFA**

Server (Ajouter un serveur MFA)). Prisma Access fournit une liste de fournisseurs MFA parmi lesquels vous pouvez choisir.



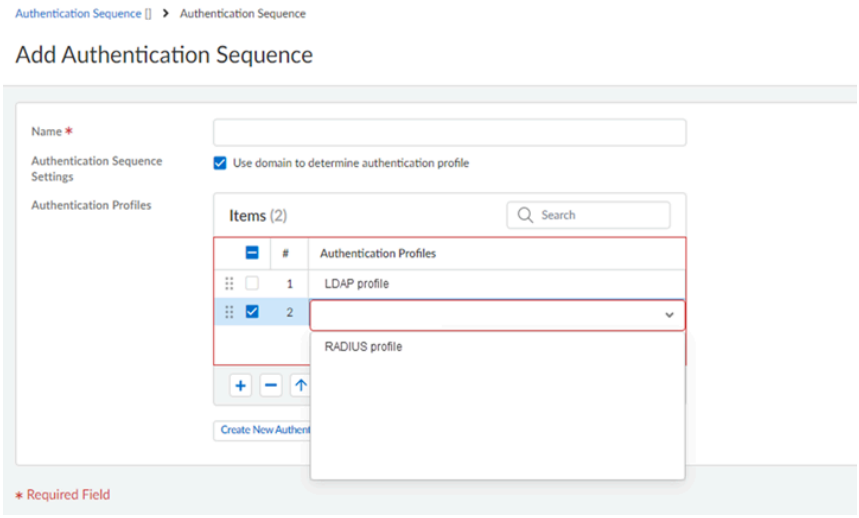
- **Portail d'authentification** Configurez le portail d'authentification (également appelé *Portail captif*) pour les utilisateurs des sites réseau distants et activez Prisma Access pour créer des mappages noms d'utilisateurs/adresses IP

  Pour l'authentification à premier facteur (identifiant et mot de passe), les utilisateurs des sites réseau distants doivent s'authentifier via le portail d'authentification. Si l'authentification réussit, Prisma Access affiche une page de connexion MFA pour chaque facteur d'authentification supplémentaire requis. Prisma Access utilise les informations d'identification soumises par les utilisateurs pour créer et mettre à jour les mappages noms d'utilisateurs/adresses IP. Cela signifie que vous saurez toujours qui, sur un site distant du réseau, accède au contenu Web et aux applications d'entreprise.

-

- **Séquence d'authentification** Classez les profils d'authentification dans l'ordre dans lequel vous souhaitez que Prisma Access les essaie

  Sélectionnez **Manage (Gérer)** > **Identity and Access Services (Services d'identité et d'accès)** > **Authentication (Authentification)** > **Authentication Profile (Profil d'authentification)** et **Add Authentication Sequence (Ajouter une séquence d'authentification)** pour classer vos profils d'authentification. Prisma Access vérifie chacun d'eux dans l'ordre jusqu'à ce que l'utilisateur soit authentifié avec succès.



Gestion : Profiles d'authentification

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	L'une des options suivantes : ☐ Licence Prisma Access ☐ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
	dépendent de la ou des licences que vous utilisez.

Un profil d'authentification définit le service d'authentification qui valide les informations d'identification des administrateurs qui accèdent à l'interface Web du pare-feu et des utilisateurs finaux qui accèdent aux applications via le portail captif ou GlobalProtect. Le profil d'authentification définit également des options comme la Single Sign-On (ouverture de session unique - SSO).

- Kerberos
- Moteur d'identité sur le cloud

Moteur d'identité sur le cloud

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licence Prisma Access

Le moteur d'identité cloud (CIE) fournit à la fois l'identification et l'authentification des utilisateurs mobiles dans le cadre d'un déploiement Prisma Access-Proxy explicite. Le moteur d'identité cloud s'intègre au service de cache d'authentification par proxy explicite (ACS). Il utilise des fournisseurs d'identité SAML (IdP) pour fournir une authentification aux utilisateurs mobiles de proxy explicite.

Configurer un profil d'authentification afin d'authentifier les utilisateurs à l'aide du moteur d'identité cloud.

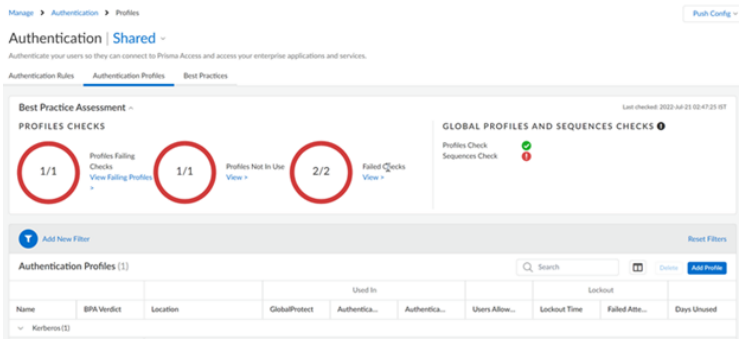
La méthode d'authentification SAML/CIE s'affiche uniquement si le service d'authentification cloud (CAS) est activé. Si l'authentification CIE ou CAS n'est pas prise en charge sur votre locataire Prisma Access. Il affiche uniquement la méthode d'authentification SAML.

Avant de commencer :

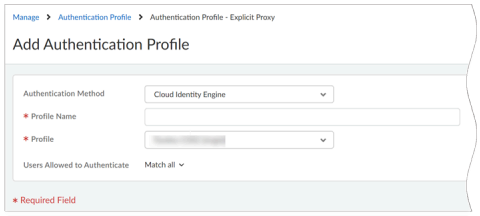
- Examiner les Instructions explicites pour les proxys.
- Configurer un profil d'authentification dans le Moteur d'identité cloud.

STEP 1 | Accédez à **Manage (Gestion)** > **Configuration (Configuration)** > **Identity Services (Services d'identité)** > **Authentication (Authentification)**, définissez la portée de la configuration

sur **Explicit Proxy (Proxy explicite)** et **Add Profile (Ajouter un profil)** sous **Authentication Profiles (Profils d'authentification)**.



STEP 2 | Sélectionnez **Authentication Method (Méthode d'authentification)** : **Cloud Identity Engine (Moteur d'identité cloud)**.



STEP 3 | Entrez un **Profile Name (Nom du profil)**.

STEP 4 | Sélectionner l'authentification du moteur d'identité cloud **Profile (Profil)** que vous avez configuré dans le Moteur d'identité cloud.

STEP 5 | Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.

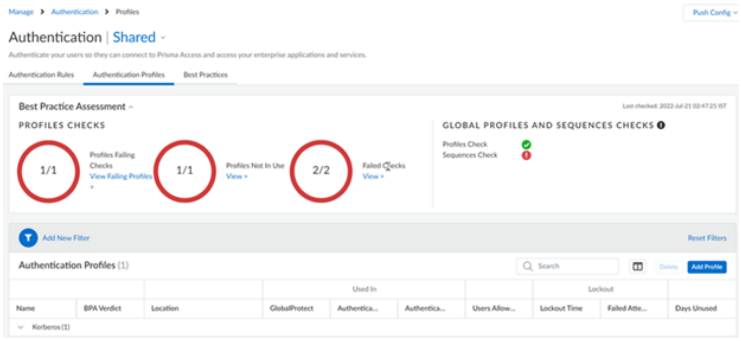
Kerberos

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licence Prisma Access

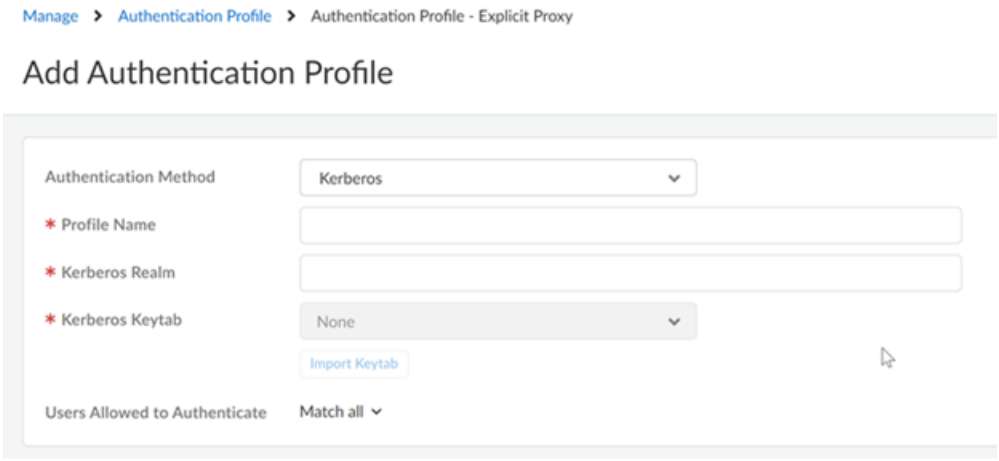
Kerberos est un protocole d'authentification de réseau informatique qui utilise des tickets pour permettre aux nœuds communiquant sur un réseau non sécurisé de prouver leur identité les uns aux autres de manière sécurisée.

Le profil d'authentification spécifie le profil du serveur pour le portail ou les passerelles à utiliser lorsqu'ils authentifient les utilisateurs. Procédez de la manière suivante pour configurer le profil d'authentification Kerberos permettant aux utilisateurs mobiles Explicit Proxy de se connecter à Prisma Access.

STEP 1 | Accédez à **Manage (Gérer)** > **Configuration (Configuration)** > **Identity Services (Services d'identité)** > **Authentication (Authentification)** > **Authentication Profiles (Profils d'authentification)** et **Add Profile (Ajouter un profil)**.



STEP 2 | Sélectionnez **Authentication Method (Méthode d'authentification)** : **Kerberos**.



STEP 3 | Entrez le **Nom du profil** pour identifier le profil du serveur. Le profil d'authentification spécifie le profil du serveur pour le portail ou les passerelles à utiliser lorsqu'ils authentifient les utilisateurs.

STEP 4 | Saisissez la **Kerberos Realm (Partition Kerberos)** (maximum de 127 caractères) afin de spécifier la portion nom d'hôte du nom de connexion de l'utilisateur. Par exemple, le nom de compte utilisateur utilisateur@EXEMPLE.LOCAL comporte la partition EXEMPLE.LOCAL.

STEP 5 | **Importation** un **Touche Kerberos** qui contient les informations de compte Kerberos. Lorsque vous y êtes invité, recherchez le fichier keytab, puis cliquez sur **Enregistrer**. Lors de l'authentification, le point de terminaison cherche d'abord à établir une ouverture de session unique en utilisant le keytab.

STEP 6 | Sélectionnez l'icône **Touche Kerberos**.

STEP 7 | Cliquez sur **Save (Enregistrer)**.

Gestion : Moteur d'identité sur le cloud

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Le Moteur d'identité sur le cloud (Directory Sync) donne à Prisma Access un accès en lecture seule à vos informations Active Directory, afin que vous puissiez facilement configurer et gérer des stratégies de sécurité et de décryptage pour les utilisateurs et les groupes.

Le Moteur d'identité sur le cloud fonctionne avec Active Directory et Azure Active Directory sur site.

Pour configurer le Moteur d'identité sur le cloud avec Prisma Access, commencez par vous rendre sur le concentrateur pour activer le Moteur d'identité sur le cloud et l'ajouter à Prisma Access. Allez ensuite dans Prisma Access pour valider la capacité de Prisma Access à accéder aux données de l'annuaire.

STEP 1 | Activer le Moteur d'identité sur le cloud

Le Moteur d'identité sur le cloud peut partager des informations Active Directory avec n'importe quelle application prise en charge sur le concentrateur. Il est gratuit et ne nécessite pas de code d'authentification pour commencer. La configuration du Moteur d'identité sur le cloud comprend l'activation de l'appli Moteur d'identité sur le cloud sur le concentrateur, la configuration de l'agent Moteur d'identité sur le cloud pour rassembler les mappages Active Directory et la configuration de l'authentification mutuelle entre l'identité et l'agent.

Assurez-vous de déployer l'instance Moteur d'identité sur le cloud dans la région où vous avez déployé Prisma Access et Strata Logging Service.

STEP 2 | Activer le Moteur d'identité sur le cloud pour Prisma Access.

Vous pouvez associer Prisma Access au Moteur d'identité sur le cloud lors de la première activation de Prisma Access ou à tout moment après :

- **Pendant que vous activez Prisma Access :** Lorsque vous activez Prisma Access géré dans le cloud pour la première fois, vous pouvez choisir une instance de Moteur d'identité sur le cloud pour Prisma Access. Assurez-vous de sélectionner une instance déployée dans la même région que Prisma Access.
- **Après avoir activé Prisma Access :** Pour activer le Moteur d'identité sur le cloud pour une instance Prisma Access existante, connectez-vous au concentrateur. Dans le menu

déroulant Paramètres du concentrateur (voir l'engrenage dans la barre de menu supérieure), sélectionnez **Manage Apps (Gérer les applis)**. Recherchez l'instance Prisma Access que vous souhaitez mettre à jour et sélectionnez l'instance Moteur d'identité sur le cloud que vous souhaitez utiliser.

STEP 3 | Vérifiez que Prisma Access est connecté au Moteur d'identité sur le cloud et que le Moteur d'identité sur le cloud partage des informations de répertoire avec Prisma Access.

- Vérifiez que vous pouvez afficher vos répertoires dans Prisma Access.

  Accédez à **Manage (Gérer)** > **Configuration (Configuration** > **Identity Services (Services d'identité)** > **Cloud Identity Engine (Moteur d'identité sur le cloud)** :

- Vérifiez que vous pouvez ajouter des utilisateurs et des groupes à une règle de politique.

  Sélectionnez **Manage (Gérer)** > **Security Services (Services de sécurité)** > **Security (Sécurité)** ou **Décryptage**. Dans une règle de politique de sécurité ou de décryptage, vérifiez que la liste déroulante **Users (Utilisateurs)** affiche vos entrées d'utilisateur et de groupe Active Directory. Vous pouvez maintenant commencer à ajouter ces utilisateurs et groupes à vos règles de politique de sécurité et de décryptage.

  Troubleshoot (Dépanner) *les problèmes liés au trafic qui n'est pas appliqué comme prévu : vérifiez l'état des pare-feux spécifiques pour comprendre s'il existe une inadéquation entre les stratégies attendues (telles que configurées) et les politiques appliquées.*

Gestion : Redistribution d'identité

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Utiliser Strata Cloud Manager pour configurer et gérer la redistribution des identités pour les NGFW et Prisma Access.

- Prisma Access
- NGFW

Redistribution d'identité (Prisma Access)

Afin que vous puissiez appliquer votre politique de sécurité de manière cohérente, Prisma Access partage les données d'identité que GlobalProtect découvre localement dans l'ensemble de votre environnement Prisma Access. Prisma Access peut également partager des données d'identité avec des périphériques locaux sur des sites réseau distants ou des sites de connexion de service (siège social et centres de données).

Pour Prisma Access Cloud Management, nous avons activé certaines redistributions de données d'identité par défaut, et pour ce qui reste, nous avons permis à la configuration d'activer la redistribution très simple (sélectionnez simplement une case à cocher pour sélectionner les données que vous souhaitez partager).

Depuis le tableau de bord Distribution d'identité, vous pouvez voir comment les données d'identité sont partagées et gérer la redistribution des données (**Manage (Gestion)** > **Configuration** > **Identity Services (Services d'identité)** > **Identity Redistribution (Redistribution d'identité)**.

Les données d'identité que vous pouvez redistribuer incluent :

- données HIP
- mappages d'adresses IP vers les étiquettes
- mappages d'utilisateurs vers les adresses IP
- mappages utilisateur vers étiquette
- Périphériques en quarantaine

Commencez à redistribuer les identités :

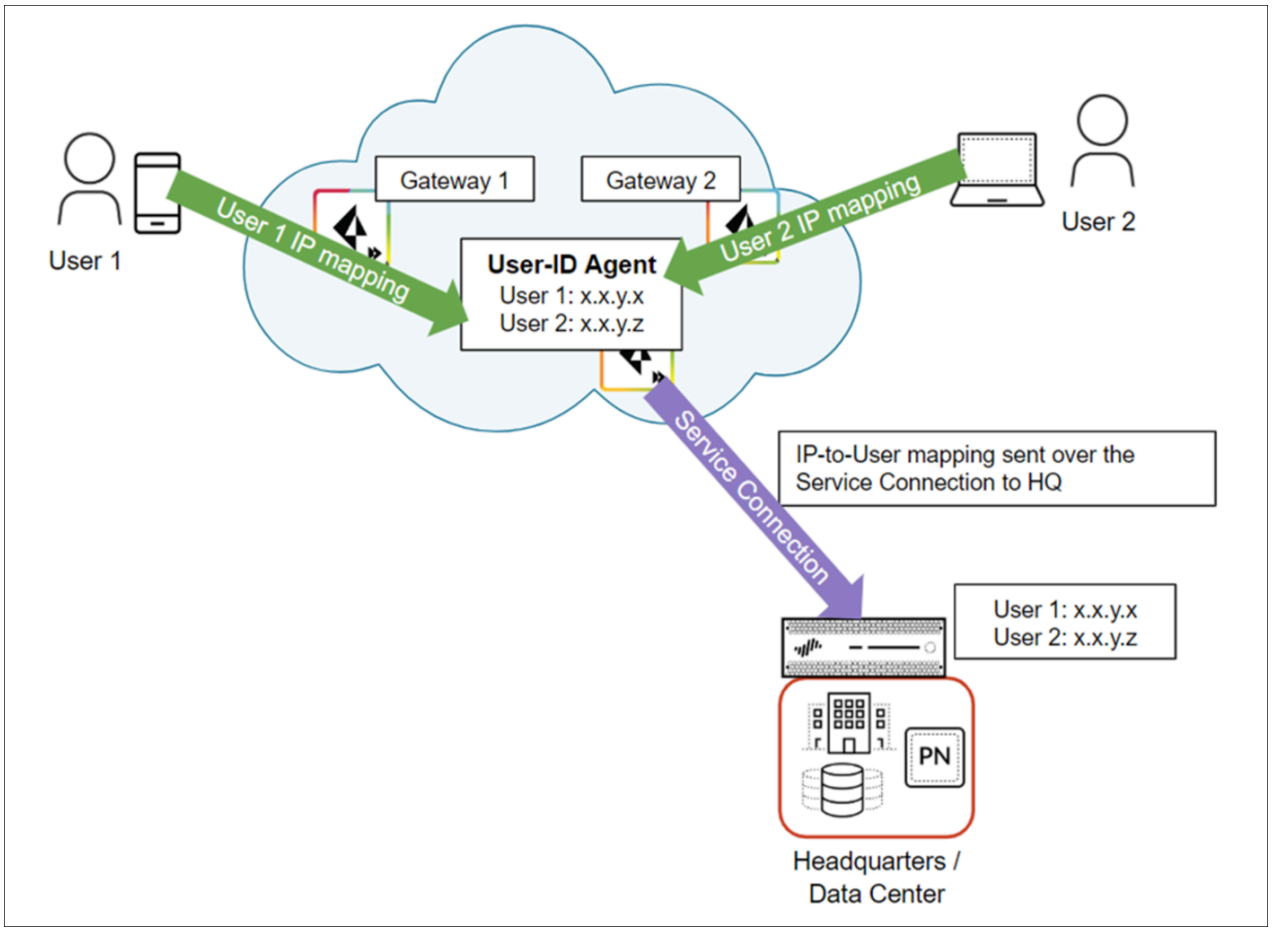
Comment fonctionne la redistribution d'identité

Lorsque les utilisateurs mobiles accèdent à une ressource sur un réseau distant ou au siège/centre de données sécurisé par un périphérique avec des politiques basées sur l'utilisateur, vous devez redistribuer les données d'identité des utilisateurs mobiles Prisma Access et des utilisateurs sur les réseaux distants vers ce périphérique sur site.

Lors de la connexion des utilisateurs à Prisma Access, Prisma Access recueille les données d'identité de l'utilisateur et les stocke.

Cet exemple montre deux utilisateurs mobiles qui ont un mappage nom d'utilisateur/adresse IP existant dans Prisma Access. Prisma Access rediffuse ensuite ce mappage par le biais d'une connexion de service aux périphériques sur site qui sécurisent le siège/centre de données.

Prisma Access Cloud Management permet automatiquement aux connexions de service de fonctionner comme des agents de redistribution d'identité (également appelés User-ID agent).



Configurer la redistribution d'identité

- Confirmez la configuration de votre connexion au service

  Si vous n'avez pas encore configuré de connexion de service pour votre siège social ou vos centres de données, vous pouvez commencer par configurer une connexion de service. Une connexion de service est nécessaire pour que Prisma Access partage les données d'identité dans votre environnement ; Prisma Access active automatiquement les connexions de service pour qu'elles fonctionnent comme des agents de redistribution. Le site de connexion de service nouvellement créé sera prêt à être utilisé comme agent de redistribution lorsque vous verrez qu'une adresse d'agent User-ID lui a été attribuée (Prisma Access le fait automatiquement, et cela ne prendra que quelques minutes). Accédez à **Manage (Gestion)** > **Configuration** > **Identity Services (Services d'identité)** > **Identity Redistribution (Redistribution d'identité)** et définissez la Portée de la configuration sur **Service Connections (Connexions de service)** pour vérifier les détails d'agent User-ID de connexion de service.

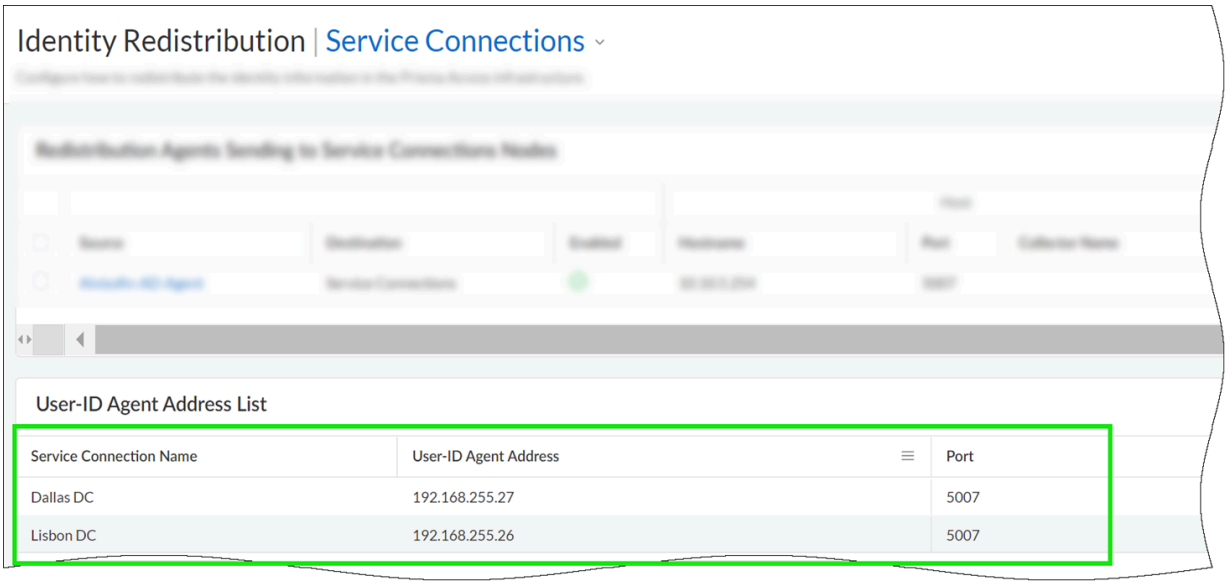
- Envoyer des données d'identité depuis Prisma Access vers Périphériques sur site

  Les informations de l'agent User-ID de la connexion de service sont tout ce dont vous avez besoin pour configurer Prisma Access afin de distribuer les données d'identité aux périphériques locaux.

  Accédez à **Manage (Gestion)** > **Configuration** > **Identity Services (Services d'identité)** > **Identity Redistribution (Redistribution d'identité)** et définissez la portée de la configuration

sur **Service Connections (Connexions de service)** pour obtenir les détails de l'agent User-ID de connexion de service.

Utilisez ces informations pour configurer Prisma Access en tant qu'agent de redistribution de données sur Panorama ou sur un pare-feu de nouvelle génération.

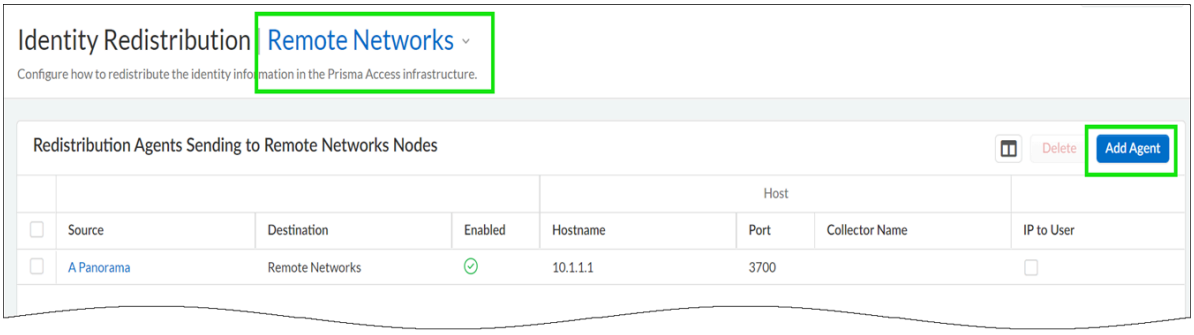


- Envoyez des données d'identité à partir des périphériques sur site vers Prisma Access

  Ajoutez des périphériques sur site à Prisma Access en tant qu'agents de redistribution ; les périphériques que vous ajoutez pourront distribuer des données d'identité à Prisma Access.

  - **À partir des périphériques situés sur des sites réseau distants :**

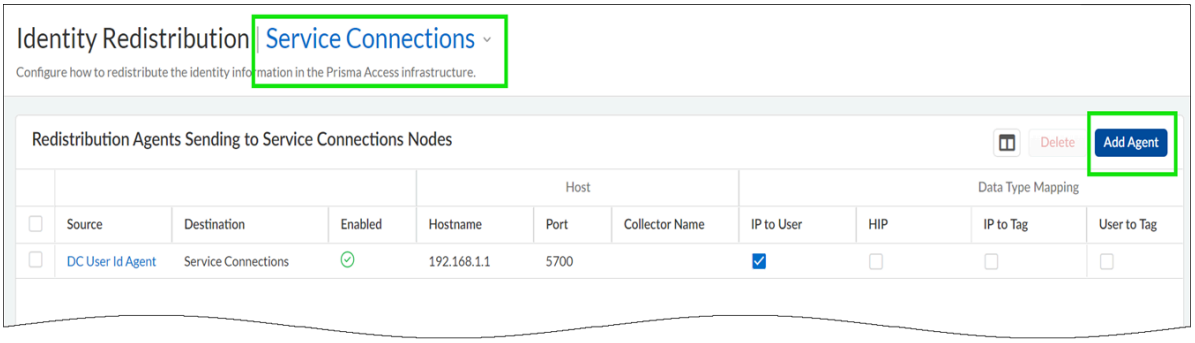
    Accédez au tableau de bord **Identity Redistribution (Redistribution des identités)**, définissez la porté de la configuration sur des **Remote Networks (Réseaux distants)** et **Add Agent (Ajouter un agent)**. En plus de spécifier les détails de l'hôte, sélectionnez le type de données que le périphérique partage avec Prisma Access. Les paramètres facultatifs incluent le nom et une clé pré-partagée pour le périphérique.



  - **À partir des périphériques situés sur les sites de raccordement au service :**

    Accédez au tableau de bord de **Identity Redistribution (Redistribution d'identité)**, définissez la portée de la configuration sur **Service Connections (Connexions de service)** et **Add Agent (Ajouter un agent)**. En plus de spécifier les détails de l'hôte, sélectionnez le type de données

que le périphérique partage avec Prisma Access. Les paramètres facultatifs incluent le nom et une clé pré-partagée pour le périphérique.



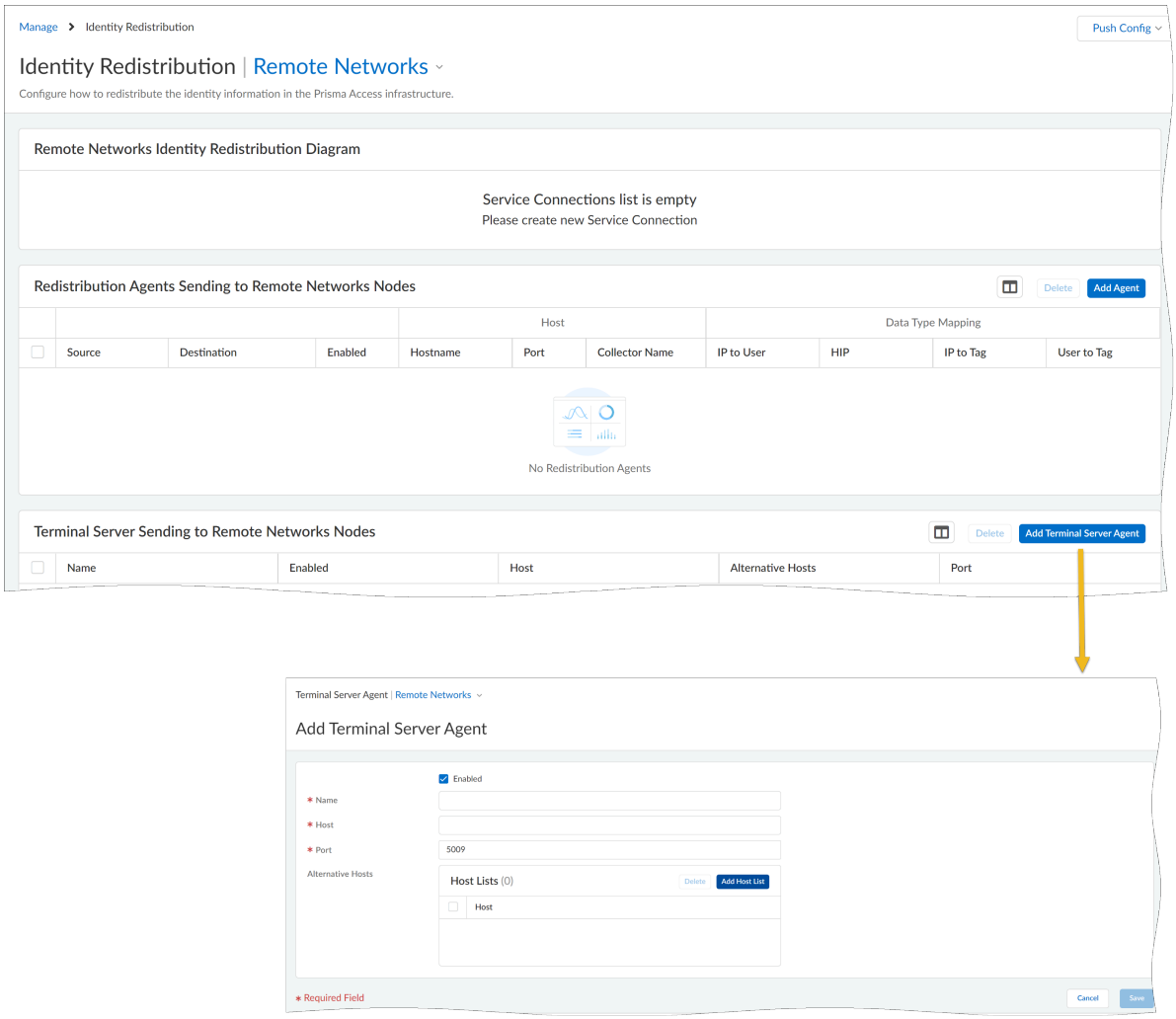
- Configurer l'agent Terminal Server pour le mappage d'utilisateurs

  L'agent Terminal Server (TS) alloue une plage de ports à chaque utilisateur pour identifier des utilisateurs spécifiques sur les serveurs de terminaux Windows. L'agent TS informe Prisma Access des plages de ports allouées, afin que Prisma Access puisse appliquer la politique en fonction des utilisateurs et des groupes d'utilisateurs.

  Dans le tableau de bord **Identity Redistribution (Redistribution d'identité)**, définissez la portée de la configuration sur **Remote Networks (Réseaux distants)**et **Ajoutez l'agent Terminal Server**

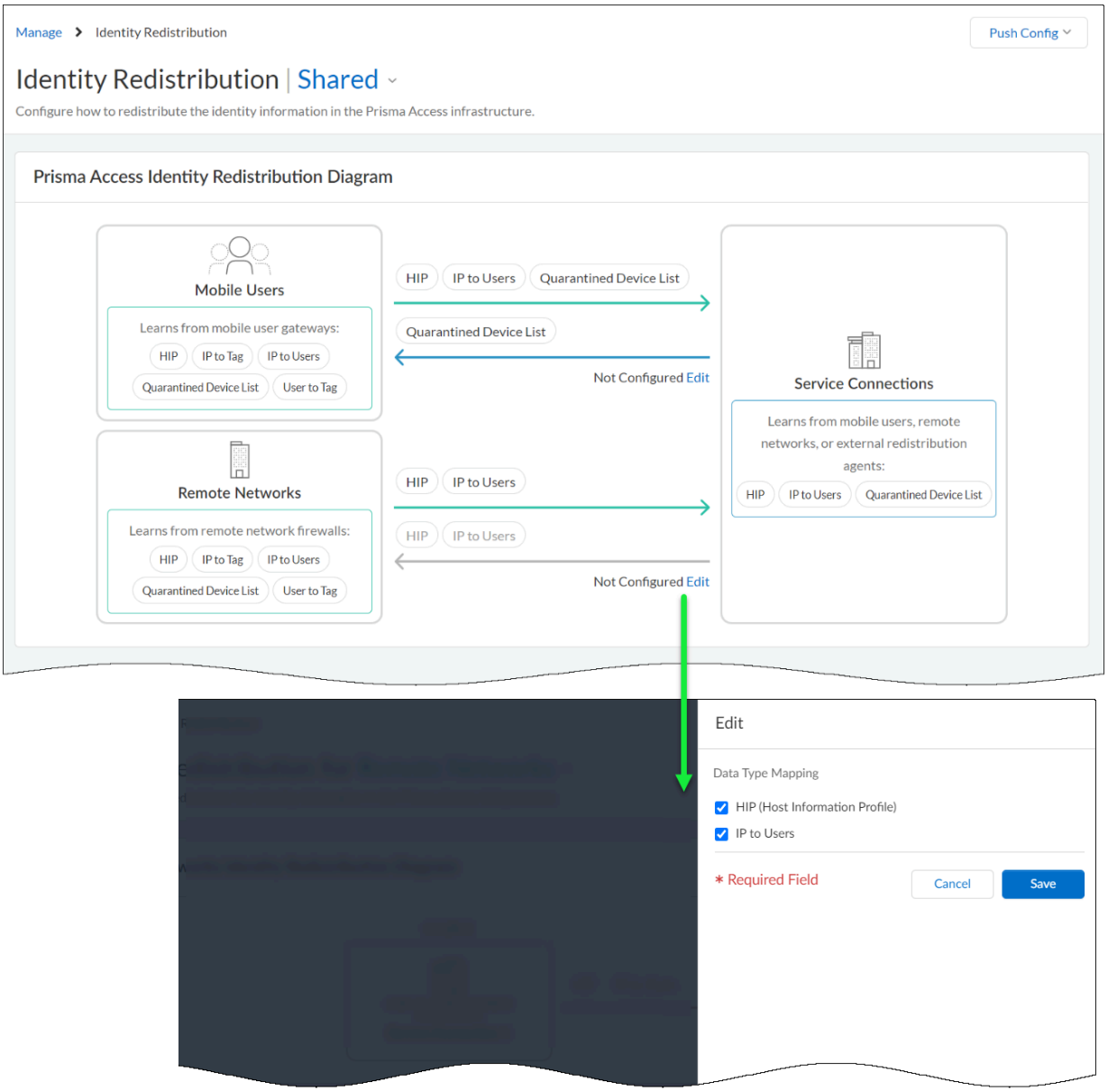
(Add Terminal Server Agent) sous **Terminal Server Sending to Remote Networks Nodes (Envoi du serveur Terminal Server aux nœuds de réseaux distants).**

- Par défaut, la configuration est **Enabled (Activée)**.
- Entrez un **Name (nom)** pour l'agent TS.
- Saisissez l'adresse IP de **Host (l'hôte)** Windows sur lequel l'agent TS est installé.
- Saisissez le numéro de **Port (Port)** sur lequel l'agent écoutera les requêtes de mappage d'utilisateur. Le port est défini sur 5009 par défaut.
- Cliquez sur **Save (Enregistrer)** pour enregistrer vos modifications.



- Distribuez les données d'identité dans votre environnement Prisma Access

  Dans le tableau de bord **Identity Redistribution (Redistribution d'identité)**, **modifiez** le diagramme pour spécifier les données d'identité que vous souhaitez collecter à partir de chaque source et partager sur Prisma Access.



- Pour activer vos modifications, envoyez la configuration à Prisma Access.

Redistribution d'identité (NGFW)

Si vous disposez d'un réseau à grande échelle, au lieu de configurer tous vos pare-feu pour qu'ils interrogent directement les sources d'informations de mappage, vous pouvez rationaliser l'utilisation des ressources en configurant certains pare-feu pour qu'ils collectent les informations de mappage par le biais de la redistribution. La redistribution des données offre également une granularité, vous permettant de redistribuer uniquement les types d'informations que vous

spécifiez aux seuls périphériques que vous sélectionnez. Vous pouvez également filtrer les mappages d'utilisateurs par IP ou les mappages de balises IP à l'aide de sous-réseaux et de plages afin de garantir que les pare-feu ne collectent que les mappages dont ils ont besoin pour appliquer les règles de politique.

Pour redistribuer les données, vous pouvez utiliser les types d'architecture suivants :

- **Architecture en étoile pour une seule région :**

  Pour redistribuer les données entre les pare-feu, la meilleure pratique consiste à utiliser une architecture en étoile. Dans cette configuration, un pare-feu de concentrateur collecte les données à partir de sources telles que les agents Windows User-ID, les serveurs syslog, les contrôleurs de domaine ou d'autres pare-feu. Configurez les pare-feu clients de redistribution pour qu'ils collectent les données du pare-feu concentrateur.
- **Architecture en étoile à plusieurs concentrateurs pour plusieurs régions :**

  Si vous avez déployé des pare-feu dans plusieurs régions et que vous souhaitez distribuer les données aux pare-feu de toutes ces régions afin d'appliquer les règles de politique de manière cohérente, quel que soit l'endroit où l'utilisateur se connecte, vous pouvez utiliser une architecture multihub et spoke pour plusieurs régions.
- **Architecture hiérarchique :**

  Pour redistribuer les données, vous pouvez également utiliser une architecture hiérarchique. Par exemple, pour redistribuer des données telles que les informations d'identification de l'utilisateur, organiser la séquence de redistribution en couches, où chaque couche a un ou plusieurs pare-feu. Dans la couche du bas, les agents User-ID intégrés à PAN-OS s'exécutant sur les pare-feu et les agents User-ID Windows s'exécutant sur les serveurs Windows mappent les adresses IP et les noms d'utilisateur. Dans chacune des couches supérieures se trouvent les pare-feu qui reçoivent les informations de mappage et les horodatages d'authentification d'un maximum de 100 points de redistribution situés dans la couche inférieure. Les pare-feu de la couche supérieure regroupent les informations et les horodatages de toutes les couches. Ce déploiement permet de configurer des règles de politique pour tous les utilisateurs dans les pare-feu de la couche supérieure et des règles de politique à une région ou à une fonction pour un sous-ensemble d'utilisateurs dans les domaines correspondants desservis par les pare-feu de la couche inférieure.

Lorsque le trafic n'est pas appliqué comme prévu, utilisez **Troubleshooting (Dépannage)** *pour vérifier l'état du plan de données de pare-feu spécifiques afin de comprendre s'il existe une inadéquation entre les politiques attendues (telles que configurées) et les politiques appliquées.*

STEP 1 | Se connecter à Strata Cloud Manager.

STEP 2 | Assurez-vous que votre déploiement Strata Cloud Manager remplit les conditions requises pour configurer la redistribution des identités.

1. Configurer et activer le moteur d'identité sur le cloud (CIE) pour votre locataire Strata Cloud Manager.

   Cette mesure est nécessaire pour utiliser la redistribution d'identité.

   1. Activez le moteur d'identité sur le cloud
   2. Pour configurer moteur d'identité sur le cloud.

2. Sélectionnez **Manage (Gestion)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Address Groups (Groupe d'adresses)** et **Add (Ajouter)** un Dynamic Address Group (groupe d'adresses dynamiques) avec les mappages d'adresse IP à balise requis.

   Pour le groupe d'adresses Type, sélectionnez **Dynamic (Dynamique)**. Configurez le Dynamic Address Group (groupe d'adresses dynamiques) au besoin et **Save (Enregistrer)**.

3. Sélectionnez **Manage (Gestion)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Objects (Objets)** > **Dynamic User Groups (Groupes d'utilisateurs dynamiques)** et **Add (Ajouter)** un groupe d'utilisateurs dynamiques avec les mappages nom d'utilisateur-étiquette requis.

   Configurez le groupe d'utilisateurs dynamiques au besoin et **Save (Enregistrer)**.

STEP 3 | Sélectionnez **Manage (Gestion)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identity Redistribution (Redistribution de l'identité)** > **Identity Redistribution** et sélectionnez l'étendue de configuration dans laquelle vous souhaitez configurer la redistribution des identités.

Vous pouvez sélectionner un dossier ou un pare-feu dans vos **Folders (Dossiers)** ou sélectionner **Snippets (Extraits)** pour configurer la redistribution d'identité dans un extrait.

STEP 4 | **Add Agent (Ajouter l'agent)**.

STEP 5 | Saisissez un **Name (Nom)** descriptif pour l'agent.

STEP 6 | Entrez l'adresse IP de l'**Host (hôte)**.

STEP 7 | Entrez dans le **Port (Port)** (la plage est de 1 à 65535).

STEP 8 | Sélectionnez le **Data Type Mapping (mappage de type de données)**.

- **IP de l'utilisateur** (Mappages d'utilisateur IP) : mappages nom d'utilisateur/adresse IP pour User-ID.
- **Host Information Profile (profil d'informations sur l'hôte - HIP)** : mappages adresse-étiquette IP pour les Dynamic Address Group (groupe d'adresses dynamiques).
- **IP à l'étiquette** : mappages étiquette/nom d'utilisateur pour les groupes d'utilisateurs dynamiques.
- **Utilisateurs vers l'étiquette** : données du profil d'informations sur l'hôte (HIP) de GlobalProtect, qui comprennent les objets et les profils HIP.
- **Liste des périphériques en quarantaine** : appareils que GlobalProtect identifie comme étant en quarantaine.

STEP 9 | **Save (Enregistrer)**.

STEP 10 | (Gestion Cloud de NGFW uniquement) Activer la redistribution des identités pour les pare-feu.

1. Sélectionnez **Manage (Gestion)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device Settings (Paramètres des périphériques)** > **Device Setup (Configuration de l'appareil)** > **Management (Gestion)** et sélectionnez **Customize (Personnaliser)** pour configurer une itinéraire de service pour le service **uid-agent**.

   Sélectionnez l'étendue de configuration où vous souhaitez créer l'itinéraire de service. Vous pouvez sélectionner un dossier ou un pare-feu dans vos **Folders (Dossiers)** ou sélectionner **Snippets (Extraits)** pour configurer l'itinéraire de service dans un extrait.
2. Activez le pare-feu pour qu'il réponde lorsque les autres pare-feu l'interrogent à propos des données à redistribuer.

   1. Sélectionnez **Manage (Gestion)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Paramètres du périphérique** > **Configuration du périphérique** > **Gestion** et activez le service réseau **User-ID (ID d'utilisateur)**.
   2. Sélectionnez **Manage (Gestion)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device Settings (Paramètres du périphérique)** > **Interfaces** pour créer ou sélectionner une interface de couche 3.

      Développez les **Advanced Settings (Paramètres avancés)**. Dans **Other (Autre)**, créez ou modifiez le profil de gestion pour activer **User-ID (l'identifiant utilisateur)**.

   - Sélectionnez

STEP 11 | Push Config (Transmettre la configuration).

Gestion : Utilisateurs et groupes locaux

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager) • NGFW, notamment ceux financés par les crédits NGFW logiciels	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ☐ Prisma Access ☐ AIOps for NGFW Premium ☐ Strata Cloud Manager Essentials ☐ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Stockez localement les informations d'authentification pour les administrateurs et les utilisateurs finaux. Vous avez la possibilité de stocker les informations d'authentification des administrateurs et des utilisateurs finaux qui s'authentifient à l'aide de GlobalProtect ou du portail d'authentification.

Pour configurer l'authentification de la base de données locale, vous créez une base de données qui s'exécute localement sur le pare-feu et qui contient des comptes d'utilisateurs (noms d'utilisateurs et mots de passe ou mots de passe hachés). Vous pouvez configurer une base de données d'utilisateurs qui se trouve localement sur le pare-feu pour authentifier les administrateurs qui accèdent à l'interface Web du pare-feu et pour authentifier les utilisateurs finaux qui accèdent aux applications via le portail d'authentification ou GlobalProtect.

L'authentification par base de données locale peut être associée à un profil d'authentification, de sorte qu'elle peut s'adapter à des déploiements où différents groupes d'utilisateurs nécessitent des paramètres d'authentification différents, tels que le Single Sign-On (ouverture de session unique - SSO) Kerberos ou l'authentification multifactorielle (MFA). Pour les comptes d'administrateur qui utilisent un profil d'authentification, les paramètres de complexité et d'expiration du mot de passe ne sont pas appliqués. Cette méthode d'authentification est disponible pour les administrateurs qui accèdent au pare-feu et aux utilisateurs finaux qui accèdent aux services et applications via le portail d'authentification ou GlobalProtect.

Accédez à **Manage (Gestion)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identity Services (Services d'identité)** > **Local Users & Groups (Utilisateurs et groupes locaux)** pour commencer à collecter des données d'authentification.

Créer un utilisateur local

STEP 1 | Se connecter à Strata Cloud Manager.

STEP 2 | Sélectionnez **Manage (Gestion)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identity Services (Services d'identité)** > **Local Users & Groups (Utilisateurs locaux et groupes)** > **Local Users (Utilisateurs locaux)** et sélectionnez la portée de la configuration dans laquelle vous souhaitez créer un utilisateur local.

Vous pouvez sélectionner un dossier ou un pare-feu dans vos **Folders (Dossiers)** ou sélectionner **Snippets (Extraits)** pour configurer un utilisateur local dans un extrait.

STEP 3 | **Add Local User (Ajouter un utilisateur local)**.

STEP 4 | Entrez le **Name (nom)** d'utilisateur.

STEP 5 | Vérifiez si l'utilisateur local est **Enabled (Activé)**.

Pour éviter de supprimer un utilisateur local de la base de données du pare-feu local pour l'authentification, vous pouvez décocher (désactiver) afin que l'utilisateur ne soit plus autorisé à s'authentifier.

STEP 6 | Saisissez un **Password (Mot de passe)** et **Confirm Password (Confirmez le mot de passe)**.

STEP 7 | **Save (Enregistrer)**.

STEP 8 | **Push Config (Transmettre la configuration)**.

Créer un groupe d'utilisateurs locaux

Regrouper plusieurs utilisateurs locaux en un seul groupe local afin d'ajouter des informations sur le groupe à la base de données du pare-feu local. Des groupes d'utilisateurs locaux peuvent

être créés pour gérer plusieurs utilisateurs locaux ayant les mêmes exigences en matière d'authentification.

STEP 1 | Se connecter à Strata Cloud Manager.

STEP 2 | Sélectionnez **Manage (Gestion)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Identity Services (Services d'identité)** > **Local Users & Groups (Utilisateurs locaux et groupes)** > **Local User Groups (Groupe d'utilisateurs locaux)** et sélectionnez la portée de la configuration dans laquelle vous souhaitez créer un utilisateur local.

Vous pouvez sélectionner un dossier ou un pare-feu dans vos **Folders (Dossiers)** ou sélectionner **Snippets (Extraits)** pour configurer un groupe d'utilisateurs locaux dans un extrait.

STEP 3 | **Add Local User Group (Ajouter un groupe d'utilisateurs locaux)**.

STEP 4 | Entrez un **Name (nom)** de groupe d'utilisateurs locaux.

STEP 5 | Ajoutez les **Local Users (Utilisateurs locaux)** que vous avez créés à l'étape précédente.

STEP 6 | **Save (Enregistrer)**.

STEP 7 | **Push Config (Transmettre la configuration)**.

Gestion : Paramètres du périphérique

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ Strata Cloud Manager Essentials ❑ AIOps for NGFW Premium ou Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

À partir de **Device Settings (Paramètres de périphérique)**, vous pouvez configurer les paramètres suivants pour vos pare-feu gérés dans le cloud :

Paramètre	Description
Interfaces	Configurez les interfaces pour permettre à votre pare-feu de fonctionner en plusieurs déploiements à la fois. Sous l'onglet **Ethernet**, utilisez l'onglet **Show local device configs (Afficher les configurations des périphériques locaux)** pour afficher les différentes configurations présentes sur le pare-feu local et Strata Cloud Manager.
Routage	Configurez des profils de routage, un routeur logique et un itinéraire statique pour vos pare-feu.
Tunnels IPSec	Configurez les tunnels IPSec pour authentifier et crypter les paquets d'adresses IP lorsqu'ils traversent le tunnel.
DHCP	Configurer DHCP pour fournir des paramètres de configuration TCP/IP et de la couche de liaison et pour fournir des adresses réseau à des utilisateurs configurés de manière dynamique
Zones	Configurez les zones pour segmenter votre réseau en zones fonctionnelles et organisationnelles afin de réduire votre surface d'attaque.
Proxy DNS	Configurer un proxy DNS pour configurer le pare-feu comme intermédiaire entre les clients et les serveurs DNS.
Configuration du périphérique	Configurez vos périphériques pour configurer les itinéraires de service, les paramètres de connexion, les services autorisés et les paramètres d'accès administratif

Paramètre	Description
	pour les interfaces de gestion et auxiliaires de vos pare-feux.
Proxy	Configurez un proxy Web pour consolider les fonctionnalités proxy et pare-feu en un seul périphérique. *Le proxy Web pour Strata Cloud Manager nécessite la pile routeur héritée. Si vous souhaitez que cela soit activé, veuillez contacter l'équipe de votre compte.*
Virtual Wire	Configurez un câble virtuel pour intégrer une interface de pare-feu dans un mappage afin que les deux interfaces connectées au pare-feu n'aient pas besoin de faire de commutation ou de routage.
GlobalProtect	Activez vos NGFW gérés dans le cloud en tant que passerelles et portails GlobalProtect, afin de fournir un accès distant flexible et sécurisé aux utilisateurs partout dans le monde.

Gestion : Paramètres généraux

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Panorama or Strata Cloud Manager)	L'une des options suivantes : ☐ Licence Prisma Access ☐ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Examinez et configurez les paramètres globaux dans Strata Cloud Manager **(Manage (Gestion) > Configuration (Configuration) > NGFW and Prisma Access (NGFW et Prisma Access) > Global Settings (Paramètres globaux))**

object	Description
Gestion des applications SaaS	Gestion centralisée de vos applications SaaS pour chacune de vos applis SaaS. La gestion des applis SaaS vous permet de trouver des fonctionnalités que vous pouvez utiliser pour activer en toute sécurité des applications pour votre entreprise.
Modèle de notification d'accompagnement des utilisateurs	Gérez de manière centralisée les modèles de notifications de l'utilisateur final pour avertir les utilisateurs par le biais de AI-Powered ADEM si l'utilisateur génère un incident de Enterprise Data Loss Prevention (E-DLP) lorsque le trafic contenant des données sensibles est inspecté et bloqué.
VPN automatique	La configuration manuelle des périphériques du réseau et l'établissement de tunnels VPN est un processus fastidieux et sujet à des erreurs de configuration. Auto VPN crée le tunnel VPN entre les périphériques réseau automatiquement. Auto VPN vous permet de créer un cluster VPN afin de connecter plusieurs réseaux locaux (LAN). SD-WAN avec Auto VPN facilite le déploiement et la gestion des déploiements SD-WAN.

Modèle de notification d'accompagnement des utilisateurs

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ GlobalProtect app version 6.3 ou ultérieure ❑ Licence Enterprise Data Loss Prevention (E-DLP) ❑ Licence pour utilisateurs mobiles Prisma Access ❑ Licence Prisma Access Ou l'une des licences suivantes qui incluent la licence Enterprise DLP ❑ Licence Prisma Access CASB ❑ Licence Next-Generation CASB for Prisma Access and NGFW (CASB-X)

Le modèle de notification d'accompagnement des utilisateurs finaux vous permet de configurer la notification affichée à vos utilisateurs dans l'interface utilisateur Access Experience (UI) lorsqu'ils génèrent un incident de Enterprise Data Loss Prevention (E-DLP). Un incident de Enterprise DLP est généré lorsqu'un fichier contenant des données sensibles est téléchargé ou chargé, ou si du trafic non basé sur un fichier contenant des données sensibles est publié dans un formulaire Web.

Pour déterminer ce qui est considéré comme des données sensibles, vous ajoutez une ou plusieurs **Inline DLP Rules (Règles DLP en ligne)**. Règles DLP contenant les critères de correspondance de trafic qui définit ce qui est considéré comme des données sensibles. La règle DLP est dérivée du profil de données Enterprise DLP du même nom. En outre, vous pouvez configurer des messages personnalisés pour lorsqu'un incident de Enterprise DLP **File Based (Basé sur des fichiers)** ou **Non-File Based non (Basés sur les non-fichiers)** est généré. Après la génération d'un incident de Enterprise DLP, l'utilisateur qui a généré l'incident peut consulter la notification Sécurité des données pour plus d'informations sur les données sensibles téléchargées, postées ou téléchargées.

Une seule notification est affichée par incident sur une période de 30 secondes, quel que soit le nombre de fois que l'utilisateur génère le même incident. Par exemple, un utilisateur tente de télécharger un fichier contenant des données sensibles vers l'application Box Web et Enterprise Data Loss Prevention (E-DLP) bloque le téléchargement. L'utilisateur tente alors immédiatement de télécharger le même fichier 5 fois de plus, mais est bloqué à chaque fois. Dans ce cas, une seule alerte Access Experience est générée, même si l'utilisateur a été bloqué 6 fois au total pour télécharger un fichier contenant une date sensible sur l'application Box Web.

STEP 1 | Contactez votre représentant Palo Alto Networks pour activer l'accompagnement de l'utilisateur final sur votre locataire.

STEP 2 | Installez la version6 6.3 ou ultérieure de GlobalProtect app sur Windows ou macOS.

STEP 3 | Connectez-vous à Strata Cloud Manager.

STEP 4 | Activer Autonomous DEM.

Sur Strata Cloud Manager, sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration Prisma Access)** > **GlobalProtect** > **GlobalProtect App (Application GlobalProtect)** et **Add App Settings (Ajouter les paramètres de l'application)**. Vous devez configurer ces paramètres requis pour afficher les notifications à vos utilisateurs dans l'interface utilisateur Access Experience lorsqu'ils génèrent un incident DLP.

- Activer **Autonomous DEM and GlobalProtect Log Collection for Troubleshooting (Collecte de journaux d'applications Autonomous DEM et GlobalProtect pour le dépannage)**
- **DEM for Prisma Access (Windows and Mac Only) (DEM pour Prisma Access (Windows et Mac uniquement))**—Sélectionnez **Install and User Cannot Enable or Disable DEM (Installer et l'utilisateur ne peut pas activer ou désactiver DEM)**
- **DEM for Prisma Access version 6.3 and above (Windows and Mac Only) (DEM pour Prisma Access version 6.3 et supérieure (Windows et Mac uniquement))**—Sélectionnez **Install the Agent (Installer l'agent)**

STEP 5 | (MacOS uniquement) Dans l'interface utilisateur Access Experience, sélectionnez **Settings (Paramètres)** > **Notifications** et activez **Allow notifications (Autoriser les notifications)**.

Ce paramètre doit être activé dans l'interface utilisateur Access Experience pour chaque utilisateur et est nécessaire pour afficher les notifications sur le bureau de l'utilisateur. Configurez le reste des paramètres de notifications Access Experience si nécessaire.

STEP 6 | Configurer Enterprise DLP.

1. Créez un profil de décryptage et une règle de politique.

   Ceci est nécessaire pour que les Enterprise DLP puissent décrypter et inspecter le trafic à la recherche de données sensibles.
2. Créez des modèles de données personnalisés pour définir vos critères de correspondance.

   Sinon, vous pouvez utiliser les modèles de données prédéfinis au lieu de créer des modèles de données personnalisés.
3. Créez un profil de données et ajoutez vos modèles de données.

   Seuls les profils de données personnalisés sont pris en charge. Par défaut, toutes les **Actions** prédéfinies des règles DLP sont définies sur **Alert (Alerte)**. Si vous devez cloner le profil de données prédéfini pour modifier **Action** de règle DLP.
4. Modifier la règle DLP.

   - Lorsque vous modifiez la règle DLP, vous devez définir **Action** sur **Block (Bloquer)**. Ceci est nécessaire pour générer des alertes dans l'interface utilisateur Access Experience. Aucune alerte ne s'affiche si **Action** est définie sur **Alert (Alerte)**.
   - Ajoutez la règle DLP à un groupe de profils et attachez le groupe de profils à une règle de politique de sécurité. Ceci est nécessaire pour que les Enterprise DLP génèrent un incident DLP qui génère ensuite une notification dans l'interface utilisateur Access Experience.

STEP 7 | Sélectionnez **Manage (Gestion)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Global Settings** > **User Coaching Notification Model (Modèle de notification d'accompagnement des utilisateurs)** et **Ajouter un modèle de notification**.

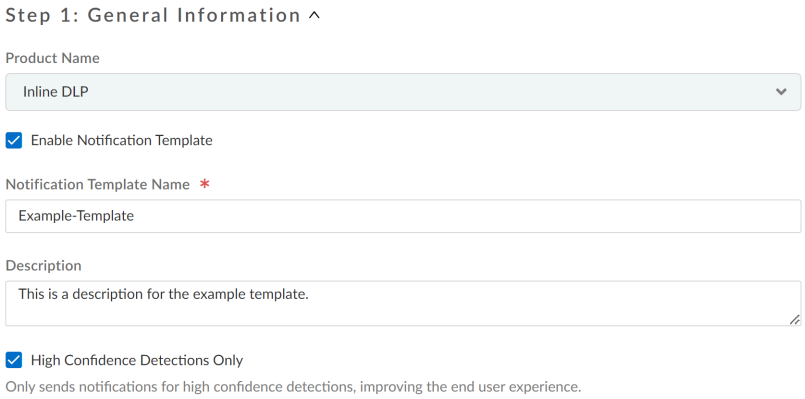
STEP 8 | Configurer les **General Information (Informations générales)**

1. Vérifiez que **Product Name (Nom du produit)** est **Inline DLP (DLP en ligne)**.

   C'est le paramètre par défaut et ne peut pas être modifié
2. Sélectionnez **Enable Notification Template (Activer le modèle de notification)** pour activer le modèle après l'enregistrement.

   Ce paramètre est activé par défaut.
3. Entrez un **Notification Template Name (Nom de modèle de notification)** descriptif.
4. (Facultatif) Saisissez une **Description** du modèle de notification.
5. (Facultatif) Sélectionnez **High Confidence Detections Only (Détections de haute confiance uniquement)** pour générer uniquement des alertes Access Experience pour les correspondances de trafic de haute confiance.

   Les correspondances de haute confiance reflètent la confiance des Enterprise DLP lors de la détection du trafic apparié. Pour les motifs d'expression régulière (regex), cela est basé sur la distance de caractère aux mots-clés de proximité configurés. Pour les modèles d'apprentissage automatique (ML), ce niveau de confiance est calculé par les modèles ML.

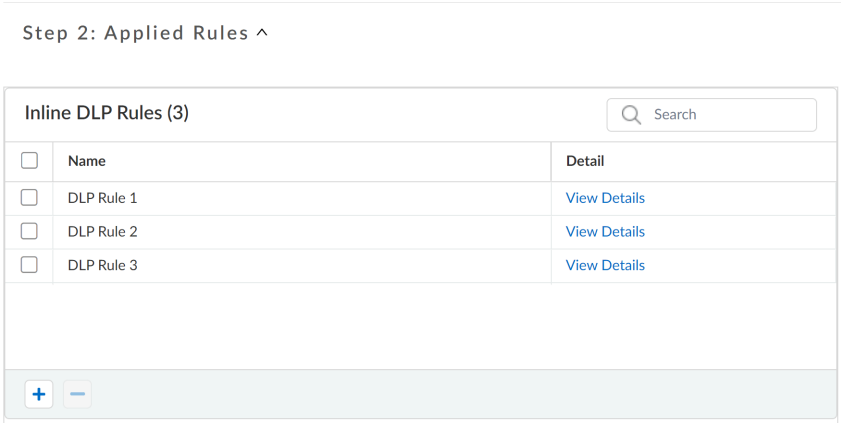


STEP 9 | Ajoutez une ou plusieurs **Applied Rules (Règles appliquées)** au modèle de notification.

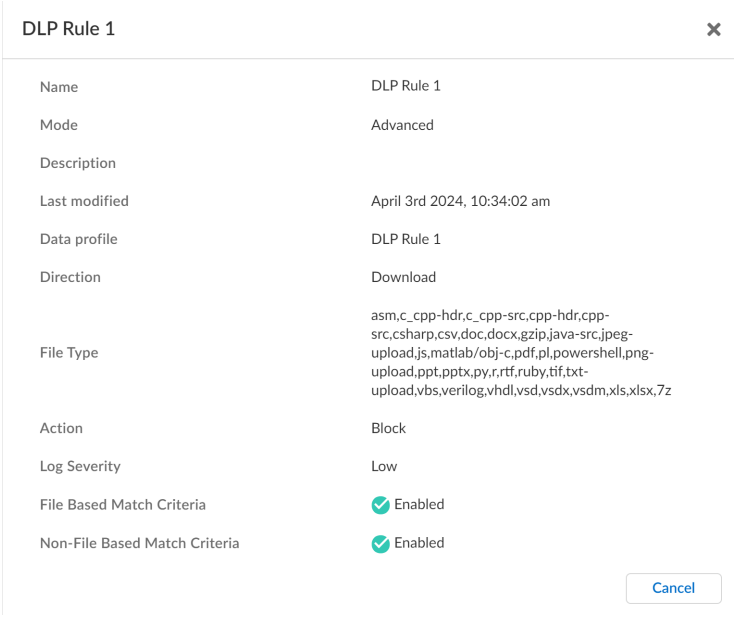
Les règles DLP doivent avoir la règle **Action** définie sur **Block (Bloquer)** et être ajoutées à un groupe de profils qui est attaché à une règle de politique de sécurité pour générer une notification Access Experience. Ajoutez uniquement des règles DLP ajoutées à un groupe de profils associé à une règle de politique de sécurité. Ceci est nécessaire pour que les Enterprise DLP génèrent un incident DLP qui génère ensuite une notification dans l'interface utilisateur

Access Experience. Une règle DLP unique peut être ajoutée à plusieurs modèles de notification d'accompagnement des utilisateurs.

Toutes les règles DLP ajoutées au modèle de notification génèrent le même **Notification Message (Message de notification)** lorsque Enterprise DLP bloque des données sensibles qui correspondent aux profils de données associés à la règle DLP.



Vous pouvez **View Details (Afficher les détails)** pour chaque règle DLP que vous ajoutez pour examiner les détails d'inspection spécifiques. Cela comprend la **Direction** d'inspection du trafic, **File Type (Type de fichier)** applicable, **Action** et la question de savoir si la règle DLP inspecte les **File Based Match Criteria (Critères de correspondance fondés sur les fichiers**, les **Non-File Based Match Criteria (Critères de correspondance non fondés sur les fichiers)** ou les deux.



STEP 10 | Définissez le **Notification Message (Message de notification)** que les utilisateurs reçoivent lorsque Enterprise DLP bloque des données sensibles qui correspondent aux profils de données associés à la règle DLP.

Les modèles de message sont les notifications toast Access Experience que les utilisateurs reçoivent lorsque Enterprise DLP bloque des données sensibles. Vous pouvez utiliser les variables suivantes dans vos modèles de messages. Vous devez inclure les chevrons pour chaque variable.

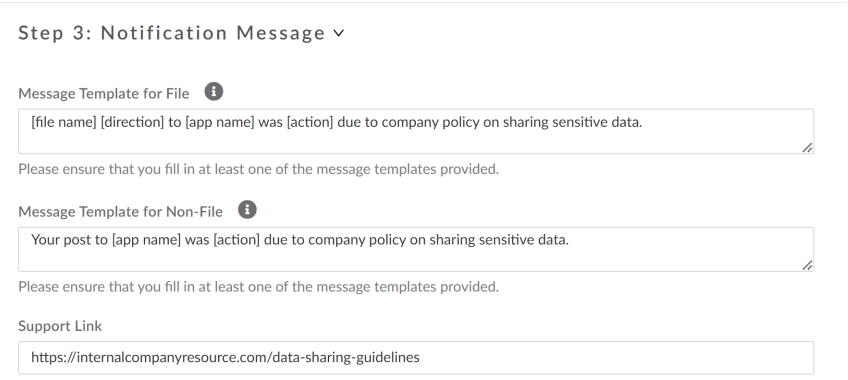
- **`[nom de fichier]`** — Nom et extension de fichier contenant des données sensibles bloquées par Enterprise DLP.
- (Basé uniquement sur les fichiers) **`[direction]`** — Spécifie si Enterprise DLP a bloqué un téléchargement ou un téléchargement de fichier.
- **`[nom de l'application]`** — L'utilisateur de l'application a tenté de télécharger ou de poster du contenu non basé sur un fichier.
- **`[action]`** — Enterprise DLP d'action prises lorsque des données sensibles ont été détectées. Cette valeur est toujours `Bloquée`.

1. Définissez le **Message Template for File (Modèle de message pour les détections)** basées sur les fichiers.

   Ignorez cette étape si la règle DLP n'est pas configurée pour les détections basées sur des fichiers.
2. Définissez **Message Template for Non-File (Le modèle de Message pour les détections basées sur des fichiers non-fichiers)**.

   Ignorez cette étape si la règle DLP n'est pas configurée pour les détections non basées sur les fichiers.
3. Ajouter un **Support Link (Lien de support)**.

   Vous pouvez ajouter des liens directement dans la notification toast Access Experience qui décrivent la politique de votre entreprise en matière de partage ou de téléchargement de données sensibles.



STEP 11 | **Save (Enregistrer)**.

STEP 12 | L'utilisateur qui a généré l'incident de Enterprise DLP peut afficher la notification de sécurité des données pour afficher un extrait des données sensibles qui ont été téléchargées, téléchargées ou publiées.

Gestion : de production

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (Managed by Panorama or Strata Cloud Manager) • Y compris VM-Series	❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licence(s) que vous utilisez.

Dépannage

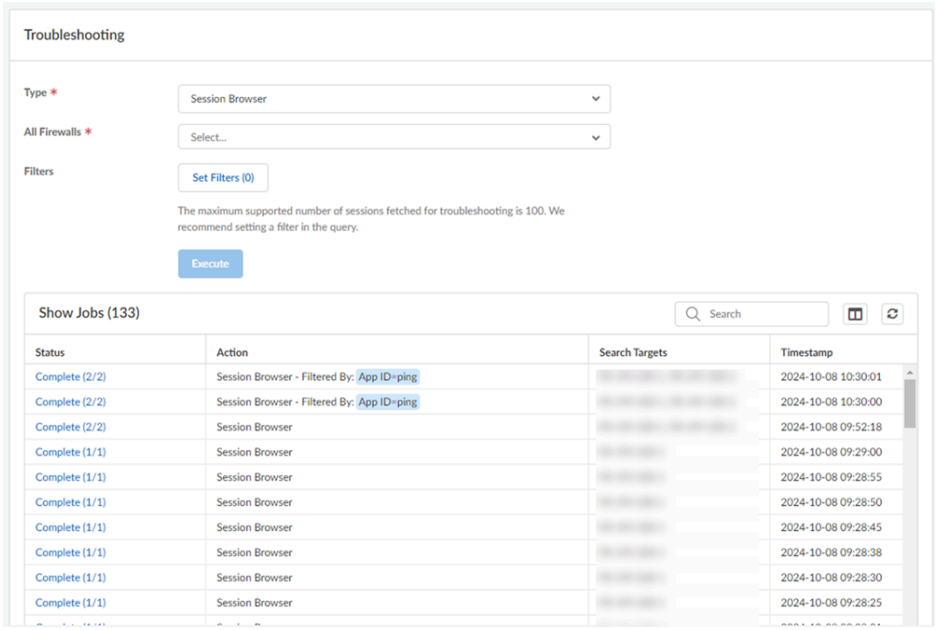
Dépannez vos NGFW à partir de Strata Cloud Manager sans avoir à passer d'une interface de pare-feu à l'autre.

Pour avoir plus d'informations sur le dépannage, cliquez sur ici.

Ce tableau de bord de dépannage vous permet de résoudre les problèmes liés au réseau, à l'identité et aux politiques pour vos NGFW par Strata Cloud Managed. À l'aide du tableau de bord de dépannage, vous pouvez localiser les anomalies et les configurations problématiques pour les domaines suivants :

- ❑ DNS Proxy
- ❑ NAT
- ❑ Groupes d'utilisateurs
- ❑ Dynamic Address Group (groupe d'adresses dynamiques)
- ❑ Groupes d'utilisateurs dynamiques
- ❑ ID de l'utilisateur
- ❑ Session de navigateur

Pour commencer, accédez à**Manage (Gestion)** > **Configuration (Configuration)** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Operations (Opérations)** > > **Troubleshooting (Dépannage)** > **Session Browser (Navigateur de la session)**.



Gestion : Recommandation en matière de politique IoT

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ Au moins une de ces licences est requise pour gérer votre configuration avec Strata Cloud Manager ; pour une gestion unifiée des NGFW et de Prisma Access, vous aurez besoin des deux : ❑ licences Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Abonnement IoT Security à un produit de sécurité IoT avancé (Enterprise IoT Security Plus, Industrial IoT Security ou Medical IoT Security)

La sécurité IoT fournit Strata Cloud Manager avec des recommandations de règles de politique de sécurité générées automatiquement et organisées par profil de périphérique. Le nombre de recommandations est limité à une par application et par profil. Choisissez un profil, sélectionnez les recommandations de règles que vous souhaitez utiliser, puis les pare-feu nouvelle génération ou Prisma Access les types de déploiement où vous souhaitez les appliquer.

Mise en route

Sélectionnez les recommandations de règles de politique de sécurité et appliquez-les aux pare-feu nouvelle génération ou à Prisma Access.

STEP 1 | Créez des dossiers ou des extraits pour les pare-feu nouvelle génération.

Vous pouvez ignorer cette étape si vous souhaitez utiliser des dossiers prédéfinis ou des dossiers ou extraits précédemment créés. Les dossiers Prisma Access sont prédéfinis.

Les dossiers sont essentiellement des conteneurs dans lesquels sont stockés différents types de règles, de configurations de sécurité et d'objets. Pour importer les recommandations de règles de politique générées par IoT SecurityIoT Security, les dossiers contiendraient des pare-feu nouvelle génération ou des déploiements Prisma Access.

Les extraits sont également des types de conteneurs qui peuvent être associé à plusieurs dossiers. Avec des dossiers et des extraits, vous pouvez importer des règles de politique dans les groupes de pare-feu ou de déploiements de votre choix.

Ainsi, vous pouvez créer un dossier appelé Californie et y placer 60 pare-feu, puis créer un autre dossier appelé Hawaï et y placer 15 pare-feu. Vous créez ensuite un extrait appelé CA-HI et le placez dans les dossiers Californie et Hawaï. Lorsque vous souhaitez importer des recommandations de règles uniquement vers des pare-feu en Californie, définissez la portée sur **Folder (Dossier)** et sélectionnez le dossier Californie. Si vous souhaitez importer les recommandations de règles en Californie et à Hawaï, définissez la portée sur **Snippet (Extrait)** et sélectionnez l'extrait CA-HI.

En fonction de la hiérarchie de la structure des dossiers, nous pourrions avoir un dossier parent comme US-West au-dessus de California et Hawaii. Ensuite, si vous importez des recommandations de règles alors que la portée est définie comme **Folder (Dossier)** et **US-West (Ouest États-Unis)** est sélectionné, les deux dossiers enfants Californie et Hawaï hériteront des règles importées. Cependant, cette solution ne fonctionnerait pas si vous vouliez uniquement importer des règles en Californie et à Hawaï et si ces pays avaient des dossiers apparentés tels que l'Oregon, l'Alaska, Washington et l'Arizona dans le dossier US-West. Vous pouvez alors utiliser l'extrait CA-HI.

STEP 2 | Créez des règles de politique de sécurité.

1. Sélectionnez **Manage (Gestion)** > **Configuration (Configuration)** > **IoT Policy Recommendation (Recommandation de politique IoT)**.
2. Sélectionnez un nom de profil.

   IoT Security utilise l'apprentissage machine pour générer automatiquement des recommandations de règles de politique de sécurité en fonction des comportements réseau normaux et acceptables des périphériques IoT dans le même profil de périphériques.

Strata Cloud Manager affiche une liste de ces recommandations organisées par application. Pour chaque comportement, vous pouvez observer ce qui suit :

Composante comportementale	Explication
Risque de l'appli	Elle représente le niveau de risque inhérent à une application déterminé par divers facteurs sur une échelle de risque croissant de 1 à 5.
Politique de sécurité créée	La présence d'un ou de plusieurs noms de dossiers ou d'extraits indique qu'une règle de politique de sécurité a été créée précédemment pour ce comportement. En cliquant sur l'un d'entre eux, un panneau latéral s'ouvre avec les noms du profil, de l'application et du dossier ou de l'extrait, ainsi que l'action de la règle de politique. Lorsque **No (Non)** s'affiche ici, cela indique qu'une règle n'a pas encore été créée.
Emplacement découvert	**Internal (Interne)** indique que la destination est sur le réseau local. **External (Externe)** indique que la destination est en dehors du réseau local.
Observé localement	**Yes (Oui)** indique que le comportement a été observé dans votre environnement locataire IoT Security. **No (Non)** indique qu'il a été observé dans plusieurs environnements locataires de sécurité IoT, mais pas dans le vôtre.
Utilisation de l'appli	**Common (Commun)** indique qu'une application a été détectée dans plusieurs environnements locataires de sécurité IoT. **Unique** indique qu'il a été observé dans votre environnement mais, pas dans ceux d'autres locataires qui ont également des périphériques dans le même profil.
Adresse de destination et FQDN	Cette destination est celle d'une règle de politique recommandée. Il peut s'agir de n'importe quel nom, d'une adresse IP ou d'un FQDN.
Profil de destination	Un profil est affiché lorsque la destination est interne et que le profil de périphérique de la destination est identifié.

Composante comportementale	Explication
Vu en dernier	En ce qui concerne les comportements observés localement, il s'agit de l'horodatage observé pour la dernière fois. Pour les comportements courants non observés localement, un tiret est affiché.

3. Sélectionnez un ou plusieurs comportements, puis **Create Security Policy (Créer une politique de sécurité)**.
4. Passez en revue les règles de politique de sécurité qui seront créées, puis sélectionnez la portée de configuration pour laquelle Strata Cloud Manager les appliquera.

   Pour appliquer les règles à un ou plusieurs pare-feu nouvelle génération ou aux déploiements Prisma Access dans un dossier, sélectionnez **Folders (Dossiers)**, puis choisissez le dossier dans Sélection de la portée.

   Pour appliquer les règles à un ou plusieurs pare-feu nouvelle génération ou les déploiements Prisma Access dans un extrait, sélectionnez **Snippets (Extraits)**, puis choisissez l'extrait dans Sélection de la portée.
5. **Créer une politique de sécurité**.

STEP 3 | Transférez la configuration vers les pare-feu nouvelle génération et les déploiements Prisma Access.

1. Sélectionnez **Manage (Gestion)** > **Operations (Opérations)** > **Push Config (Transmettre la configuration)**.
2. Sélectionnez les dossiers avec les modifications de configuration, **Push Config (Transmettre la configuration)**, **Push (Transmettre)**, puis **Push (Transmettre)** à nouveau.

   Strata Cloud Manager affiche un numéro d'identification dans la colonne ID de tâche pour les dossiers sélectionnés et l'état de la transmission de la configuration dans la colonne État de la transmission.

   Lorsque l'état de la transmission passe de **Pending (En attente)** à **Success (Réussite)**, vous savez que la configuration poussée a commencé à s'exécuter.
3. Pour voir l'état d'une tâche poussée, sélectionnez **Manage (Gestion)** > **Operations (Opérations)** > **Push Status (État de la transmission)**. Vous pouvez y voir l'état de la tâche principale ainsi que l'état des tâches secondaires, un pour chaque pare-feu ou déploiement.

Gestion : Enterprise DLP

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	• Licence Enterprise Data Loss Prevention (E-DLP) • **NGFW (Managed by Panorama)**—Soutien et licences de gestion des périphériques Panorama • Licence **Prisma Access (Managed by Strata Cloud Manager)**—Prisma Access • Licence **SaaS Security**—SaaS Security • **NGFW (Managed by Strata Cloud Manager)** : soutien et licencesAIOps for NGFW Premium Ou l'une des licences suivantes qui incluent la licence Enterprise DLP • Licence Prisma Access CASB • Licence Next-Generation CASB for Prisma Access and NGFW (CASB-X) • Licence Data Security

Enterprise Data Loss Prevention (E-DLP) protège les informations sensibles contre l'accès non autorisé, l'utilisation abusive, l'extraction ou le partage. Enterprise DLP sur Strata Cloud Manager vous permet d'appliquer les normes de sécurité des données de votre organisation et d'empêcher la perte de données sensibles dans vos NGFW, vos utilisateurs mobiles et vos réseaux distants Prisma Access.

Points forts des fonctionnalités

- **Tableau de bord Data Loss Prevention (Prévention des pertes de données - DLP) d'entreprise**

  Accédez à **Manage (Gestion)** > **Configuration** > **Data Loss Prevention (prévention des pertes de données - DLP)** pour configurer et gérer Enterprise DLP.

  Votre configuration Enterprise DLP est partagée entre les produits où vous utilisez Enterprise DLP. Vous pouvez donc afficher ici des paramètres qui ont été configurés ailleurs, et certains paramètres que vous pouvez configurer ici peuvent également être exploités dans d'autres produits.

- **Paramètres Enterprise DLP prédéfinis + personnalisés**

  Enterprise DLP inclut des paramètres intégrés que vous pouvez utiliser pour commencer rapidement à protéger vos contenus les plus sensibles :

  - Regex prédéfini et motif de données basé sur ML spécifiez les types courants d'informations sensibles (comme les cartes de crédit et les numéros de sécurité sociale) que vous voudrez peut-être analyser et protéger
  - Profils de données prédéfinis regroupent les modèles de données qui nécessitent généralement le même type d'application

  Vous pouvez également créer des modèles de données et des profils personnalisés directement sur Strata Cloud Manager.

- **Enquête sur les incidents DLP**

  Un incident DLP est généré lorsque le trafic correspond à un profil de données DLP attaché à une règle de politique de sécurité sur Strata Cloud Manager. Sur le Tableau de bord des incidents DLP, vous pouvez afficher les détails du trafic qui a déclenché l'incident, tels que les modèles de données correspondants, la source et la destination du trafic, le fichier et le type de fichier.

- **Recherche d'images dans les formats de fichiers pris en charge**

  Renforcez votre posture de sécurité pour prévenir l'utilisation abusive, la perte ou le vol accidentel de données grâce à la Reconnaissance optique de caractères (OCR). L'OCR permet au service cloud DLP d'analyser les types de fichiers pris en charge avec des images contenant des informations sensibles qui correspondent à vos profils de filtrage Enterprise DLP.

- **Correspondance exacte des données (EDM)**

  EDM est un outil de détection avancé visant à surveiller et protéger les données sensibles contre l'exfiltration. Utiliser la EDM pour détecter avec une grande précision les informations sensibles et personnellement identifiables (PII) telles que les numéros de sécurité sociale, les numéros de dossier médical, les numéros de compte bancaire et les numéros de carte de crédit, dans une source de données structurée telle que les bases de données, les serveurs d'annuaire ou les fichiers de données structurés (CSV et TSV).

- **Types de documents personnalisés**

  Téléchargez vos documents personnalisés contenant de la propriété intellectuelle ou des informations sensibles sur Enterprise Data Loss Prevention (E-DLP) afin de créer types de documents personnalisés. Vos types de documents personnalisés sont utilisés comme critères de correspondance dans le profil de données avancé pour détecter et restreindre l'exfiltration.

- **Email DLP**

  Email DLP empêche l'exfiltration d'e-mails contenant des informations sensibles grâce à des détections de données alimentées par l'IA/ML. En effet, Enterprise DLP peut empêcher l'exfiltration de données sensibles par le biais d'un courrier électronique sortant envoyé par un vendeur de votre entreprise vers son courrier électronique personnel.

- **Accès basé sur les rôles pour Enterprise DLP**

  Vous pouvez activer l'accès basé sur les rôles aux commandes Enterprise DLP dans Strata Cloud Manager. Cela vous permet de contrôler quels utilisateurs ont des privilèges d'accès en lecture et en écriture aux différentes parties de Enterprise DLP.

Mise en route

STEP 1 | Activer Enterprise DLP sur Strata Cloud Manager.

Pour configurer Enterprise DLP, vous devez créer un profil de décryptage pour permettre au service cloud DLP de vérifier le trafic. Sélectionnez **Manage (Gestion)** > **Configuration** > **Security Services (Services de sécurité)** > **Decryption (Décryptage)** et :

1. Sélectionnez **Manage (Gestion)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Decryption (Décryptage)** et **Add Rule (Ajouter une règle)**.

   Les paramètres de profil de décryptage prédéfinis permettent à Enterprise DLP de vérifier le traffic. La modification des paramètres prédéfinis du profil de décryptage n'est pas nécessaire, à moins que vous n'ayez besoin d'activer **Strip ALPN (Enlever l'ALPN)** (**Advanced Settings (Paramètres avancés)** > **SSL Forward Proxy (Proxy de transfert SSL)**).
2. Ajouter le profil de décryptage à une règle de décryptage **SSL Forward Proxy (Proxy de transfert SSL)**.

- Voici comment activer Enterprise DLP

STEP 2 | (Facultatif) Sélectionnez **Manage (Gérer)** > **Configuration (Configuration)** > **Data Loss Prevention (Prévention des pertes de données - DLP)** > **Detection Methods (Méthodes de détection)** et créez un Modèle de données

Vous pouvez créer des modèles de données personnalisés Enterprise DLP pour spécifier quel contenu est sensible et doit être protégé : il s'agit du contenu que vous filtrez. Vous pouvez créer un Modèle de données personnalisé basé sur des expressions régulières ou un modèle de données basé sur les propriétés du fichier.

- Comment créer un modèle de données ?

STEP 3 | Créez un profil de données

Regrouper les modèles de données qui doivent être appliqués de la même manière dans un profil de données. Vous pouvez également utiliser des profils de données pour spécifier des critères de correspondance et des niveaux de confiance supplémentaires pour la correspondance.

- Pour savoir comment créer un profil de données

STEP 4 | Créez une règle DLP

Spécifiez le trafic et les types de fichiers que vous Enterprise DLP souhaitez protéger. Définissez l'action que Enterprise DLP doit entreprendre lorsqu'un incident DLP est détecté.

- La méthode à suivre pour créer une règle DLP est la suivante

Gestion : Sécurité SaaS

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ Licence Prisma Access

Identifiez les menaces basées sur le cloud et les activités risquées des utilisateurs dans les applis autorisées et non autorisées avec SaaS Security Inline.

SaaS Security Inline (Sécurité SaaS en ligne) est intégré à Prisma Access géré dans le cloud pour vous offrir une vue centralisée de la sécurité réseau et CASB. Il offre une visibilité SaaS : qui inclut des analyses avancées et des rapports : afin que votre entreprise dispose des informations nécessaires pour comprendre les risques de sécurité des données liés à l'utilisation d'applications SaaS sanctionnées et non sanctionnées sur votre réseau.

L'offre Cloud Access Security Broker (CASB) comprend Saas Security Inline, Enterprise Data Loss Prevention (DLP) Inline, SaaS Security API, Data Loss Prevention (DLP) API et SaaS Security Posture Management (SSPM).

La licence de CASB-X (Next Generation Cloud Access Security Broker) contient tous les composants CASB tels que SaaS Security Inline, SaaS Security API, SaaS Security Posture Management (SSPM) et Enterprise DLP. Ce logiciel peut être appliqué aux périphériques Prisma Access gérés par le Cloud, Prisma Access gérés par Panorama et Next Generation Firewall (NGFW) gérés par Panorama dans un environnement à locataire unique.

Voici tout ce que vous devez savoir *pour utiliser SaaS Security sur Strata Cloud Manager.*

Mise en route

Voici comment démarrer avec SaaS Security Inline sur Prisma Access Cloud Management :

- Vérifiez que la licence SaaS Security est incluse dans votre abonnement Prisma Access.

  Accédez à **Gérer (Manage)** > **la Configuration (Configuration)** > **de la vue d'ensemble** pour vérifier ce qui est disponible avec votre licence.

- Si ce n'est pas déjà fait, activez l'appli SaaS Security Inline sur le hub.

  Une fois activé, SaaS Security Inline découvre automatiquement toutes les applications SaaS et tous les utilisateurs et analyse l'activité SaaS des utilisateurs et les données d'utilisation à partir de vos journaux Prisma Access qui sont stockés dans Strata Logging Service.

- Examiner et gérer les rôles et les accès des administrateurs.

  Accédez à **Settings (Paramètres)** > **Identity and Access (Identité et accès)** pour fournir un accès basé sur les rôles aux contrôles SaaS Security dans Prisma Access Cloud Management.

  > *Pour gérer de manière exhaustive SaaS Security, les utilisateurs doivent également être administrateur de l'appli SaaS Security Inline. Passez directement du tableau de bord Prisma Access Cloud Management à la **SaaS Security Console (Console de sécurité)** SaaS pour ajouter des administrateurs SaaS Security Inline.*

- Explorez le tableau de bord **SaaS Security** dans Prisma Access Cloud Management.

  Accédez à **Manage (Gérer)** > **Security (les services de)** > **configuration** > **SaaS Security**.

  Toutes les vues du tableau de bord sont prises en charge directement dans Prisma Access Cloud Management. Examinez ces vues pour identifier les applications et utilisateurs SaaS à risque et SaaS Security Posture Management. La gestion de la posture de sécurité des données (SSPM, SaaS Security Posture Management) permet de détecter et de corriger les paramètres mal configurés dans les applications SaaS sanctionnées grâce à une surveillance continue.

- Examiner et partager le rapport sur la sécurité du logiciel-service.

  SaaS Security Inline inclut un rapport SaaS Security qui fournit un aperçu de l'utilisation des applications avec des données et des vues agrégées avancées. Cette étude sert d'outil de communication entre l'équipe chargée de la sécurité du SaaS et la direction générale. Ces rapports PDF à la demande peuvent être partagés avec votre équipe de sécurité SaaS pour un contrôle périodique, ou envoyés par e-mail à vos cadres pour mettre en évidence les applications SaaS utilisées dans votre entreprise et les risques de sécurité qu'elles présentent.

  - En savoir plus sur le rapport SaaS Security
  - Voici comment générer le rapport SaaS Security dans l'appli SaaS Security Inline

- Découvrez ce que vous pouvez faire d'autre avec SaaS Security et Prisma Access Cloud Management.

Recommandations en matière de politique SaaS

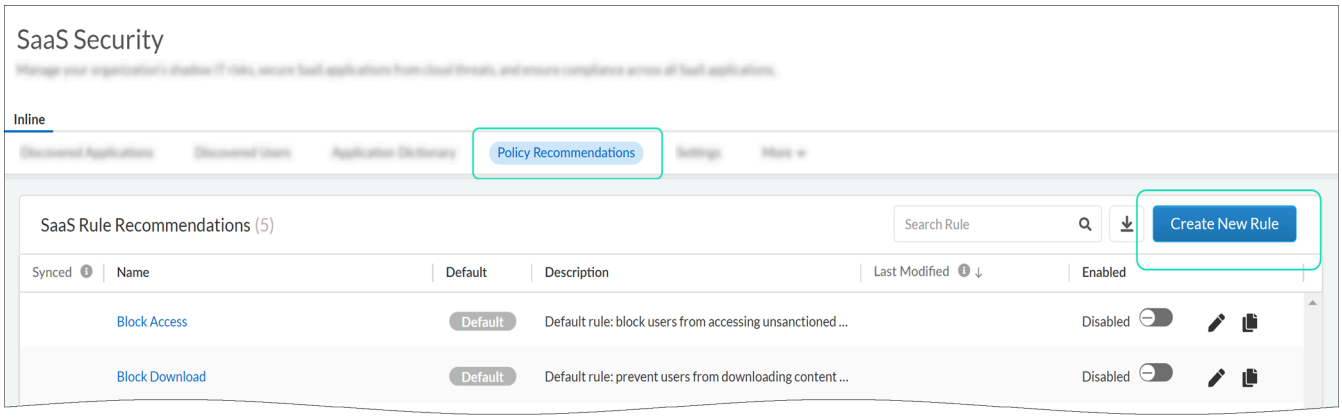
Afin d'obtenir une visibilité et un contrôle des applications SaaS, les administrateurs de sécurité SaaS créent des recommandations de règles SaaS avec des App-ID SaaS spécifiques fournis par l'App-ID Cloud Engine (ACE).

Dans Prisma Access Cloud Management, vous pouvez désormais consulter et choisir d'accepter les règles recommandées par les administrateurs SaaS Security. Les recommandations de règles SaaS sont ajoutées à votre politique d'accès Web. Vous devez avoir Web Security activé pour exploiter les recommandations de règles SaaS.

Voici comment vous pouvez commencer : consultez le flux de travail pour examiner et accepter les recommandations de politique SaaS ici :

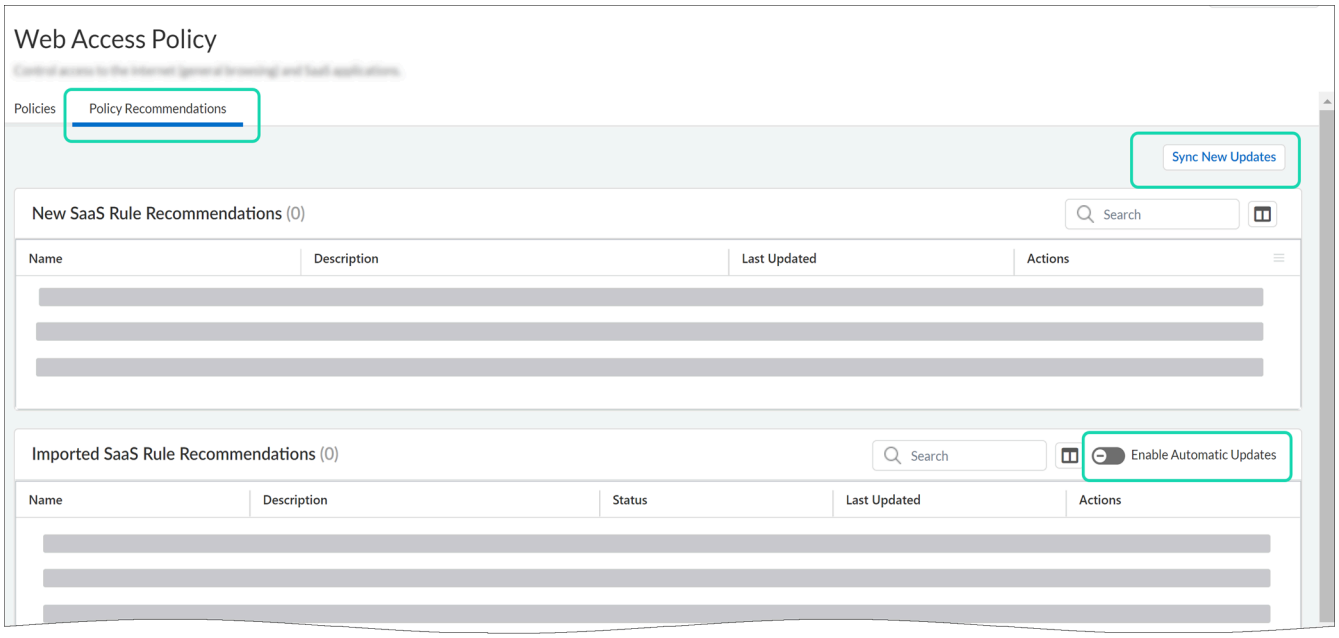
1. Les admins de SaaS Security créent des recommandations de règles SaaS dans l'application SaaS Security Inline ou directement dans Prisma Access Cloud Management.

   # Dans Prisma Access Cloud Management, accédez à **Manage (Gérer)** > **Configuration la configuration** > **Security Services (Services de sécurité)** > **Sécurité SaaS**

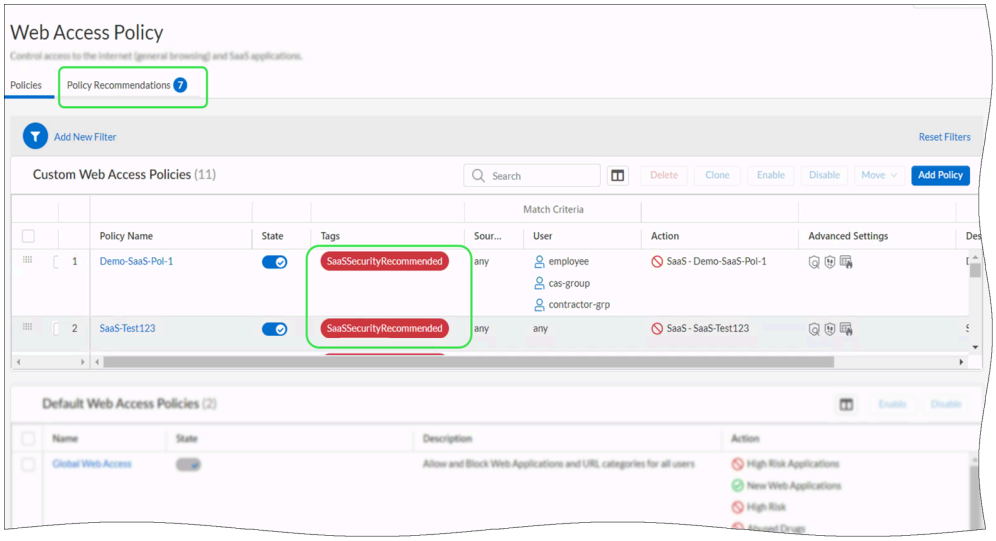


2. Vous pouvez examiner et importer des recommandations de règles SaaS.

   # Accédez à **Manage (Gérer)** > **Web Security (Sécurité Web)** > **Web Access Policy (Politique d'accès Web**



3. Vous pouvez facilement identifier les recommandations de règles SaaS que vous avez importées en les étiquetant.



Gestion : Prisma SD-WAN

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma SD-WAN	❑ Prisma SD-WAN licence

Prisma SD-WAN est une solution de réseau étendu défini par logiciel (SD-WAN) qui transforme les réseaux étendus (WAN) existants en une structure applicative (AppFabric) radicalement simplifiée et sécurisée, virtualisant les transports sous-jacents hétérogènes en un WAN hybride unifié. Le moteur de performance des applications se trouve au cœur du système.

Vous pouvez afficher des analyses granulaires axées sur les applications, élaborer une politique robuste et gérer le trafic du WAN en fonction des performances. Grâce aux périphériques ION (Instant-On Network), Prisma SD-WAN simplifie la conception, la construction et la gestion des réseaux étendus, en toute sécurité, à la périphérie du réseau.

Prisma SD-WAN prend en charge les politiques empilées pour les opérations de transfert de flux. À l'aide de stratégies définies de manière centralisée, chaque périphérique ION effectue des actions telles que la sélection automatique du chemin, la mise en forme du trafic ou l'équilibrage de charge actif-actif entre les liens, tandis que le contrôleur SD-WAN Prisma offre une visibilité complète sur les performances des applications et les temps de réponse sur tous les liens WAN.

Prisma SD-WAN contrôle les performances des applications réseau en fonction des accords de niveau de service (SLA) application-performance et des priorités professionnelles. Vous pouvez configurer les politiques, les ressources, les CloudBlades et les paramètres système pour les Prisma SD-WAN à l'aide de Strata Cloud Manager.

Sélectionnez **Gestion (Manage)** > **Prisma SD-WAN** pour gérer les configurations pour :

- Politiques
- Ressources
- Système

CloudBlades

Gestion : Politiques pour Prisma SD-WAN

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma SD-WAN	❑ Licence Prisma SD-WAN

Prisma SD-WAN prend en charge les politiques d'origine et empilées. À l'aide de politiques définies de manière centralisée, chaque périphérique ION effectue des actions telles que la sélection automatique du chemin, la mise en forme du trafic ou l'équilibrage de charge actif-actif entre les liens, tandis que le Prisma SD-WAN contrôleur offre une visibilité complète sur les performances des applications et les temps de réponse sur toutes les liaisons WAN.

Configurer les politiques dans Prisma SD-WAN à l'aide de Strata Cloud Manager.

STEP 1 | Choisir **Manage (Gestion)** > **Prisma SD-WAN** > **Policies (politiques)**.

Vous pouvez configurer les types de politiques suivants dans Prisma SD-WAN :

- Chemin

  Configurez des politiques de chemin empilées pour les opérations de transfert de flux et de mise en forme du trafic.
- Performance

  Configurez des politiques de performance pour mesurer les performances des applications et les SLA des applis.
- QoS

  Configurez des politiques QoS empilées pour spécifier les priorités de l'entreprise.
- Sécurité

  Configurez des politiques de sécurité empilées pour définir des règles qui déterminent l'accès aux applications au sein d'une branche.
- NAT

  Configurez des politiques NAT empilées pour garantir la confidentialité des réseaux internes connectés à des réseaux publics ou privés.
- Sécurité (Original)

  Il s'agit de politiques de sécurité héritées. Si vous êtes un nouvel utilisateur qui commence avec la version 6.0.1 du logiciel de périphérique ION, vous ne pouvez configurer que des politiques de sécurité empilées. Si vous avez configuré des politiques d'origine ou héritées, vous devez convertir ces politiques héritées en politiques empilées avant de pouvoir mettre à niveau votre périphérique vers la version 6.0.1.
- Réseau (Original)

  Il s'agit de politiques de réseau héritées. Si vous êtes un nouvel utilisateur qui commence avec la version 6.0.1 du logiciel de périphérique ION, vous ne pouvez configurer que des stratégies de réseau empilées. Si vous avez configuré des politiques d'origine ou héritées, vous devez convertir ces stratégies héritées en stratégies empilées avant de pouvoir mettre à niveau votre périphérique vers la version 6.0.1.

STEP 2 | Choisissez **Bindings (Liaisons)** pour lier des piles de politiques à un site.

Pour que les règles de politiques dans les piles Chemin, QoS, Sécurité et NAT soient efficaces, vous devez lier les piles de politiques à un site. Vous ne pouvez lier qu'une seule pile Chemin, QoS, Sécurité et NAT à un site à la fois.

Gestion : Types de ressources pour Prisma SD-WAN

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma SD-WAN	❑ Licence Prisma SD-WAN

Vous pouvez gérer différents types de ressources dans Prisma SD-WAN.

Gérer les ressources dans Prisma SD-WAN à l'aide de Strata Cloud Manager.

Sélectionnez **Manage (Gestion)** > **Prisma SD-WAN** > **Resources (Ressources)**.

Vous pouvez gérer les types de ressources suivants dans Prisma SD-WAN :

- Applications

  Les applications sont au cœur de la solution de Prisma SD-WAN. Les périphériques ION déployés sur le réseau analysent activement chaque flux d'application pour garantir que les politiques de performance, de conformité et de sécurité sont maintenues et que des connexions réseau optimales sont utilisées pour chaque flux. Le périphérique ION utilise des définitions d'application et des technologies d'empreintes digitales pour la sélection du chemin, Qos et les politiques de pare-feu.

  Les applications système sont disponibles par défaut, tandis que vous pouvez configurer des applications propres à l'entreprise en fonction des besoins de votre entreprise.

- Catégories de circuits

  Les catégories de circuits sont un regroupement logique de différents types de circuits et de connectivité qui peuvent être présents dans le réseau. Ce regroupement autorise des règles de politique réseau simplifiées et réutilisables pour l'ensemble du réseau. Par exemple, l'internet à large bande par câble, les liaisons internet LTE avec compteur, les liaisons internet par satellite, l'internet DSL ou les liaisons MPLS privées.

- Contextes de réseau

  Le contexte réseau segmente le trafic réseau dans le but d'appliquer différentes règles de politique réseau pour la même application. Une règle avec un contexte réseau est toujours prioritaire par rapport à une règle sans contexte réseau. Vous pouvez créer un ou plusieurs contextes réseau, mais un réseau LAN individuel ne peut appartenir qu'à un seul contexte réseau. Les contextes réseau doivent être attachés aux segments LAN appropriés pour être efficaces.

- Groupes de services et de DC

  Utilisez les groupes de services et de DC pour mapper des terminaux tiers à des groupes afin d'autoriser une certaine souplesse lors de la création de règles de politiques de réseau afin de garantir l'unicité entre les sites. Les règles de politique générale doivent rester les mêmes, quel que soit l'emplacement du site.

- Zones de sécurité

  Les zones de sécurité spécifient les limites d'application où le trafic est soumis à la vérification et au filtrage. Chaque zone de sécurité correspond à des réseaux connectés à des interfaces physiques, des interfaces logiques ou des sous-interfaces d'un périphérique.

Ces interfaces de niveau zone servent de proxy pour les circuits physiques et les circuits virtuels, tels que les circuits VLAN, VPN de couche 3 et VPN de couche 2.

- Modèles de sites

  Le modèle de configuration de site vous aide à créer des modèles de site personnalisés qui répondent à vos besoins de déploiement, vous autorisant à déployer efficacement des succursales et des centres de données à grande échelle en toute simplicité. En utilisant ce modèle, vous pouvez déployer plusieurs sites. Pour déployer plusieurs sites, vous pouvez utiliser un modèle existant, modifier un modèle existant ou créer un nouveau modèle.

- Filtres de préfixe

  Un préfixe est un groupe d'une ou plusieurs adresses IP individuelles ou sous-réseaux d'adresses IP. Les préfixes sont utilisés avec les politiques d'ensemble de chemins et les politiques prioritaires. Elles peuvent avoir une portée globale ou locale.

- **Configuration Profiles (Profils de configuration)**

  Utilisez des profils de configuration pour configurer les paramètres de différents types de ressources.

  - IPsec

    Créez un profil IPsec pour configurer les connexions VPN IPsec entre les périphériques de la succursale et les terminaux des services de sécurité cloud.

  - IPFIX

    Un profil IPFIX est un objet de configuration IPFIX global qui identifie la configuration du collecteur, la configuration du filtre, le modèle d'exportation des éléments d'information sur les flux et la configuration de l'échantillonneur de flux.

  - APN

    Créez un profil de nom de point d'accès (APN) pour définir le chemin réseau pour la connectivité des données cellulaires. Les informations APN sont nécessaires pour se connecter à un réseau cellulaire.

  - DNS

    Configurez un profil Domain Name System (système de noms de domaine - DNS) pour spécifier les paramètres de configuration du service DNS. Les paramètres généralement configurés comprennent les serveurs DNS, le mappage domaine/adresse,

la configuration du cache et la configuration DNSSEC. Une fois le profil de service DNS créé, il est lié à un périphérique.

- Modèles NTP

  Utilisez les modèles de configuration Network Time Protocol (protocole d'heure réseau - NTP) pour ajouter ou modifier des serveurs NTP.

- Multicast

  Créez un profil de configuration multicast WAN et associez-le à un site de succursale pour activer le routage multicast WAN pour le site de succursale.

- VRF

  Créez et associez le profil global (par défaut) des tables de routage et de transfert virtuels (VRF) et attribuez-le à tous les sites de succursales et de centres de données.

- Découverte IoT

  Utilisez la visibilité des périphériques IoT pour identifier les périphériques de votre réseau. Les périphériques Prisma SD-WAN branch ION inspectent les paquets, extraient des informations et génèrent des messages à envoyer à Strata Logging Service dans un format spécifique.

Gestion : CloudBlades pour Prisma SD-WAN

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma SD-WAN	❑ Licence Prisma SD-WAN ❑ Licence CloudBlade pour le CloudBlade correspondant

Utilisez la Prisma SD-WAN plateforme CloudBlades pour accéder en toute sécurité aux périphériques ION dans le but d'automatiser les flux de travail de l'interface Web avec des modèles personnalisés pour réduire la complexité opérationnelle.

Configurez CloudBlades dans Prisma SD-WAN en utilisant Strata Cloud Manager.

Sélectionnez **Manage (Gestion)** > **Prisma SD-WAN** > **CloudBlades**.

Vous pourrez visualiser les CloudBlades auxquels vous êtes abonné dans Prisma SD-WAN. Suivez les étapes du guide d'intégration au CloudBlade correspondant pour configurer votre CloudBlade.

Gestion : Les ressources du système destinées à Prisma SD-WAN

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma SD-WAN	❑ Licence Prisma SD-WAN

Gérer et surveiller les utilisateurs et les autorisations dans Prisma SD-WAN à l'aide des ressources disponibles sous l'onglet **System (Système)**.

Sélectionnez **Manage (Gestion)** > **Prisma SD-WAN** > **System (Système)**.

Vous pouvez configurer les types de ressources système suivants dans Prisma SD-WAN :

- Gestion des licences

  Utilisez la gestion des licences pour générer des jetons d'autorisation pour ION virtuel. Il s'agit d'un ensemble de contrôles visant à empêcher l'ajout non autorisé de périphériques virtuels dans un environnement.
- Journaux d'audit

  Utilisez Journaux d'audit pour afficher les enregistrements de modification de configuration dans un système. Vous pouvez utiliser ces journaux à des fins de conformité et de dépannage. Les registres d'audit fournissent des informations telles que les modifications apportées, le propriétaire de la modification, le moment de la modification et la portée de la modification sur un site, un système ou un sous-ensemble de sites.
- Préfixes d'entreprise

  Utilisez les préfixes d'entreprise pour permettre Prisma SD-WAN aux sites de centres de données d'annoncer facilement les routes et l'accessibilité aux sites de succursale.
- **Access Management (Gestion des accès)**
  - Accès de l'utilisateur
    - Gestion de l'utilisateur

      Ajoutez un nouvel utilisateur avec un rôle système selon les exigences de votre entreprise. Les rôles du système sont un ensemble prédéfini d'autorisations pour chaque rôle. Ces rôles incluent une collection d'une ou plusieurs autorisations système. Les rôles système disponibles sont les suivants : Root, Super administrateur, administrateur IAM, administrateur réseau, administrateur de sécurité et utilisateur avec vue unique.
    - Rôles personnalisés

      Vous pouvez créer des rôles personnalisés en combinant les rôles et autorisations système existants de différentes manières. Vous pouvez les créer en assemblant un ensemble d'autorisations système ou en ajoutant ou en supprimant des autorisations de rôle système.

- Exigences relatives au mot de passe

  Définissez le nombre de caractères et les conditions de sécurité des mots de passe. Vous pouvez également définir la fréquence de réutilisation des anciens mots de passe et d'actualisation des mots de passe.

- Accès au périphérique
  - Accès des utilisateurs à la boîte à outils
  - Politique d'accès hors ligne des périphériques
- Accès des locataires
  - Un jeton d'authentification

    Configurez un jeton d'authentification pour accéder Prisma SD-WAN APIs. Une fois le jeton généré pour un utilisateur, il peut être utilisé pour effectuer des appels répétés d'API, ce qui élimine les connexions inutiles pour accéder aux API.

    Un utilisateur ayant accès à un jeton d'authentification peut accéder à toutes les autorisations attribuées au jeton.

    Sélectionnez **Manage (Gestion)** > **System (Système)** > **Tenant Access (Accès locataire)** > **Auth Tokens (Jetons d'authentification)** > **Create Auth Token (Créer un jeton d'authentification)** pour créer un jeton d'authentification.
- Gestion des identités
  - Moteur d'identité Cloud

Gestion : Navigateur Prisma Access

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licence Prisma Access

À partir de Strata Cloud Manager, sélectionnez **Manage (Gestion)** > **Configuration** > **Prisma Access Browser (Navigateur Prisma Access)**.

Prisma Access Secure Enterprise Browser (Prisma Access Browser) est la seule solution qui sécurise à la fois les périphériques gérés et non gérés, grâce à un navigateur d'entreprise intégré en mode natif qui étend la protection aux périphériques non gérés. Reportez-vous à la section Qu'est-ce que le navigateur Prisma Access ?

Accueil

La page d'accueil est la page de destination lorsque vous accédez à Prisma Access Browser à partir de Strata Cloud Manager. Depuis la page d'accueil, vous pouvez utiliser les tableaux de bord du navigateur Prisma Access pour obtenir des informations utiles de l'analyse du comportement des utilisateurs et des données de navigation. Il existe une variété de tableaux de bord pour des cas d'utilisation spécifiques que vous souhaiterez peut-être surveiller, tels que le comportement des utilisateurs, la prévention des fuites de données, la sécurité Web et la politique. Les tableaux de bord contiennent une collection de widgets et certains d'entre eux apparaissent dans plusieurs tableaux de bord.

Analyse

Le Prisma Access Browser L'écran Événements est l'outil de visibilité clé pour analyser chaque activité au sein de votre déploiement du navigateur Enterprise afin de vérifier que les politiques et les règles fonctionnent comme elles le devraient. C'est ici que vous étudiez les événements du navigateur Prisma Access.

Répertoire

- Le répertoire des utilisateurs sert d'emplacement central pour les informations concernant les utilisateurs et leurs périphériques connectés au navigateur Prisma Access, l'appartenance à des groupes d'utilisateurs et les règles de politique associées. Gérer les utilisateurs du navigateur Prisma Access
- Le répertoire des périphériques fournit une liste de vos périphériques et groupes de périphériques du navigateur Prisma Access. Gérer les périphériques du navigateur Prisma Access
- Le navigateur Prisma Access est équipé d'une liste préexistante d'applications vérifiées. La liste des applications vérifiées fait référence au catalogue d'applications Palo Alto Networks App-ID™ et est régulièrement synchronisée avec la base de données cloud. Vous pouvez également créer des applications personnalisées et privées. Gérer les applications du navigateur Prisma Access
- Le navigateur Prisma Access garantit un répertoire d'extensions qui inclut les extensions installées par les utilisateurs finaux sur le navigateur. Ces informations vous permettent de maintenir une gestion appropriée des politiques d'entreprise, de gérer la visibilité et l'analyse des risques.Gérer les extensions de navigateur Prisma Access

Politique

- Vous pouvez utiliser des règles pour spécifier les utilisateurs, les groupes d'utilisateurs et les groupes d'appareils qui seront impactés par les différentes politiques. Ces règles régissent l'accès aux applications Web, les politiques de sécurité et les options de personnalisation. En utilisant des règles, vous pouvez contrôler avec précision l'accès des utilisateurs aux outils et composants de l'organisation.Gérer les règles de politique de navigateur Prisma Access
- Les commandes des règles Prisma Access Browser peuvent être configurées dans le corps de la règle individuelle. Les profils (contrôles externes) peuvent être utilisés lorsque vous souhaitez enregistrer des profils réutilisables (hérités) et les ajouter aux règles ultérieurement. Gérer les profils de politique du navigateur Prisma Access
- Utilisez des règles de connexion pour déterminer quels utilisateurs et quels périphériques ont accès à Prisma Access Browser. Gérer les règles de connexion du navigateur Prisma Access
- Une fois que vous avez défini les conditions de contournement dans les règles de politique, lorsque les utilisateurs tentent d'effectuer une action ou de visiter un site bloqué par la règle correspondante, ils peuvent soumettre une requête de contournement. Pour définir des conditions de contournement, configurez l'action d'invite pour activer les requêtes d'autorisation. Gérer les requêtes du navigateur Prisma Access pour contourner les règles de politique.

Administration

Gérez les intégrations pour des fonctionnalités supplémentaires avec les éléments suivants :

- Microsoft 365
- Protection des informations Microsoft
- Google Workspace
- Votiro
- Intelligence CrowdStrike Falcon
- OPSWAT MetaDefender
- YazamTech SelectorIT
- Symantec DLP

Gestion : de production

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ Au moins une de ces licences est nécessaire pour gérer votre configuration avec Strata Cloud Manager ; pour une gestion unifiée des NGFW et de Prisma Access, vous aurez besoin des deux : ❑ Prisma Access licence ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités à votre disposition dans Strata Cloud Manager dépendent des licences que vous utilisez.

Utilisez les opérations Strata Cloud Manager permettant de transmettre les modifications de configuration, de revoir les transmissions de configurations passées et de gérer les instantanés de vos versions de configuration pour les charger ou les rétablir vers une version de configuration précédente.

- Enregistrez les modifications de configuration
- Examinez l'état de la transmission de configuration
- Découvrez comment vous pouvez améliorer votre configuration

Gestion : Transmettre la configuration

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ Au moins une de ces licences est nécessaire pour gérer votre configuration avec Strata Cloud Manager ; pour une gestion unifiée des NGFW et de Prisma Access, vous aurez besoin des deux : ❑ Prisma Access licence ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités à votre disposition dans Strata Cloud Manager dépendent des licences que vous utilisez.

Une fois que vous avez apporté des modifications à la configuration et êtes prêt à l'activer, vous devez transmettre les modifications sur vos pare-feux. Vous avez la possibilité de transférer toutes les modifications de configuration ou de sélectionner des administrateurs spécifiques à inclure dans le transfert. Pour la première modification de la configuration, il est nécessaire que tous les administrateurs apportent des modifications à la configuration. Vous pouvez choisir les changements de configuration que vous souhaitez transférer à Prisma Access :

- **Sécurité Web**

  Transmettre les mises à jour de Sécurité Web vers Prisma Access.
- **Utilisateurs mobiles — GlobalProtect**

  Transmettre les mises à jour de Global Protect à Prisma Access.
- **Utilisateurs mobiles — Proxy explicite**

  Transmettre les mises à jour du Proxy explicite à Prisma Access.
- **Réseaux distants**

  Transmettre les mises à jour des Réseaux distants à Prisma Access.
- **Connexions aux services**

  Transmettre les mises à jour des Connexions aux services à Prisma Access.

Vous pouvez transférer une configuration pendant qu'un autre transfert de configuration est en cours. Prisma Access applique les modifications de configuration dans l'ordre où vous les soumettez.

Dans le cas où une configuration est transférée par erreur, ou qu'un changement provoque une perturbation du réseau ou de la sécurité, vous pouvez rétablir la configuration de Prisma Access à la configuration de Prisma Access la plus récente en cours d'exécution. Cela vous permet de

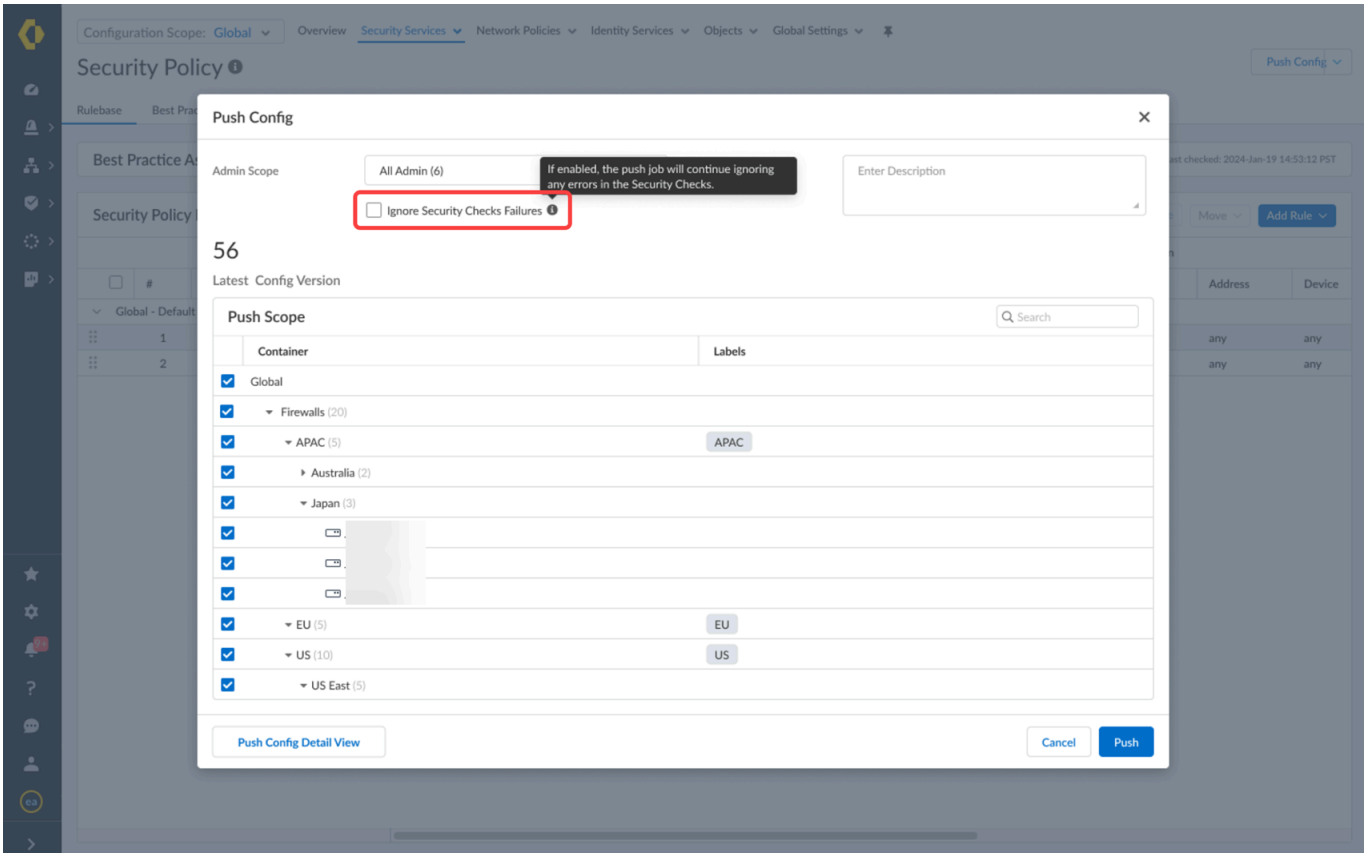
ramener la configuration de Prisma Access à une configuration en cours d'exécution fonctionnant de manière satisfaisante et qui ne compromet pas la sécurité de votre réseau. Vous n'avez pas la possibilité de sélectionner une configuration en cours d'exécution spécifique. Prisma Access sélectionne automatiquement la dernière configuration connue et revient à celle-ci.

STEP 1 | Se connecter à Strata Cloud Manager

STEP 2 | Modifier la configuration si nécessaire.

STEP 3 | **Push Config (Transmettre la configuration)** et **Push (Transmettre)** les modifications de votre configuration.

*Vous pouvez également sélectionner **Manage (Gestion)** > **Operations (Opérations)** > **Push Config To Devices (transmission des opérations vers les périphériques)**.*



Dans la boîte de dialogue de **Push Config (transmission de configuration)**, vous pouvez **ignorer les échecs des vérifications de sécurité**. Cette fonctionnalité vous permet de poursuivre les opérations de transfert même lorsque certains contrôles bloqueraient le processus. Si la case à cocher n'est pas sélectionnée (paramètre par défaut) et qu'un contrôle des meilleures pratiques avec une action de "blocage" échoue, Strata Cloud Manager interrompt la transmission.

STEP 4 | (Facultatif) **Add New Filter (Ajouter un nouveau filtre)**.

Vous pouvez filtrer les périphériques affichés dans l'étendue du transfert en appliquant des filtres. Appliquer des filtres n'a d'impact que sur les pare-feu ou les déploiements de Prisma

Access qui sont affichés dans l'étendue du transfert et n'a pas d'impact sur les périphériques vers lesquels vous effectuez le transfert.

STEP 5 | Modifiez l'étendue de la transmission

Modifier l'étendue du transfert vous permet de transférer des modifications de configuration ciblées à certains ou à tous vos pare-feu ou déploiements de Prisma Access.

La commande de transfert partiel de la configuration n'est pas prise en charge et vous devez transférer la totalité de la configuration Strata Cloud Manager si vous :

- Configurez un nouveau locataire *et c'est votre premier transfert de configuration.*
- Intégrez un pare-feu *à Strata Cloud Manager.*
- *Intégrez les utilisateurs mobiles et les utilisateurs distants de Prisma Access.*
- *Renommez ou déplacez un* dossier *de sorte qu'il soit imbriqué sous un autre dossier.*
- *Déplacez un pare-feu dans un autre dossier.*
- *Renommez, associez ou dissociez un* extrait.
- *Chargez une configuration.*
- *Renvoyez la configuration à la dernière configuration transférée ou à un instantané de la version précédente de la configuration.*

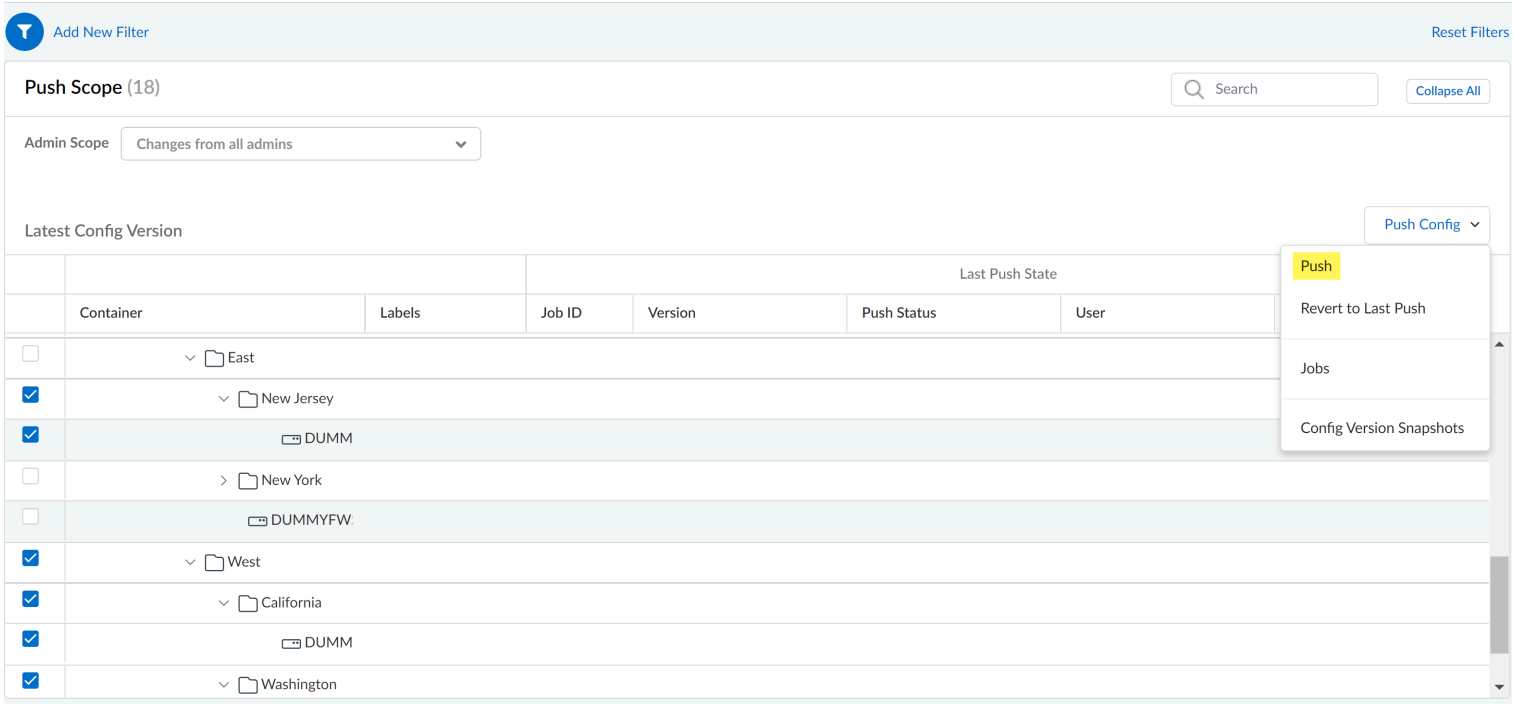
- **Admin Scope (Étendue d'administration)** : sélectionnez les modifications de configuration d'administrateur à inclure dans le transfert. Par défaut, l'étendue d'administrateur sélectionne l'utilisateur actuel, et les modifications apportées par cet utilisateur sont transmises aux pare-feu ou aux déploiements Prisma Access sélectionnés. La sélection des modifications **Changes from all admins (Modifications de tous les administrateurs)** inclut toutes les modifications de configuration effectuées par tous les administrateurs.

  Modifier l'étendue de l'administrateur pour sélectionner des administrateurs spécifiques inclut toutes les modifications de configuration effectuées par les administrateurs sélectionnés. Cette option ne peut pas être utilisée lors de la première transmission de la configuration. La sélection de modifications de configuration spécifiques à inclure dans la transmission n'est pas prise en charge.
- **Push Scope (Transmission de la configuration)** : sélectionnez les types de déploiement ou les dossiers vers lesquels vous souhaitez effectuer le transfert. Lorsque vous sélectionnez un déploiement ou un dossier, les modifications de configuration sont transmises vers tous les pare-feu ou déploiements.

  Lorsque vous sélectionnez un dossier contenant des sous-dossiers, tous les sous-dossiers et les pare-feu associés ou les déploiements Prisma Access sont inclus dans la transmission. La sélection d'un pare-feu spécifique ou d'un déploiement Prisma Access sélectionne automatiquement le dossier auquel il est associé.

STEP 6 | **Push Config (Transmettre la configuration)** et **Push (Transmettre)**.

Examinez les cibles de transmission et **Push (la transmission)**.



STEP 7 | Examinez l'état de la transmission de configuration.

Dans le cas où une configuration est transférée par erreur, ou qu'un changement provoque une perturbation du réseau ou de la sécurité, vous pouvez retourner à la configuration de Prisma Access.

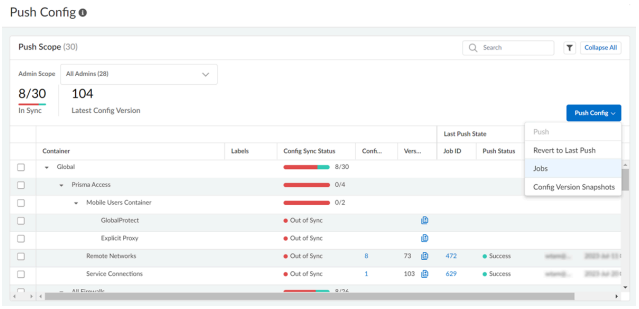
Restaurer, charger et comparer les versions de configuration

Afficher les tâches Prisma Access

Vous pouvez afficher l'historique **Jobs (Tâches)** sur Prisma Access pour afficher les détails des opérations lancées par les administrateurs, ainsi que les mises à jour automatiques du contenu et des licences. Cela inclut toutes les validations de configuration, les transferts et les inversions. Vous pouvez utiliser la vue Jobs (Tâches) pour dépanner les opérations qui ont échoué, examiner les avertissements associés aux validations terminées ou annuler les validations en attente.

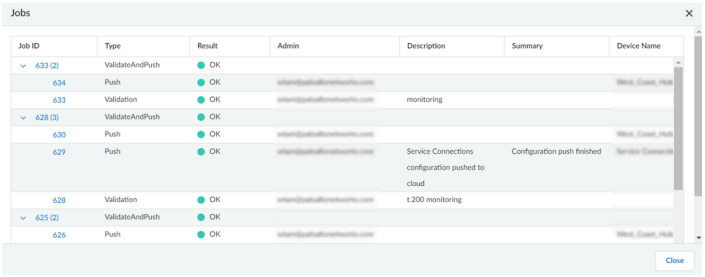
STEP 1 | Lancer Prisma Access.

STEP 2 | Dans la barre de menus supérieure, sélectionnez **Push Config (Transmettre la configuration)** et affichez les **Jobs (Tâches)** Prisma Access.



STEP 3 | Effectuez l'une des tâches suivantes :

- **Enquêtez sur les avertissements ou défaillances**—Lisez les commentaires de la rubrique Résumé pour obtenir des informations détaillées sur les avertissements ou les défaillances.
- **Affichez la description d'une validation**—Si un administrateur a saisi une description de validation, vous pouvez vous référer à la colonne Description pour comprendre l'objectif de la validation.
- **Vérifiez la position d'une opération dans la file d'attente**—Affichez la position et l'état de l'opération pour déterminer la position de l'opération.



Gestion : État de la transmission

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ Au moins une de ces licences est nécessaire pour gérer votre configuration avec Strata Cloud Manager ; pour une gestion unifiée des NGFW et de Prisma Access, vous aurez besoin des deux : ❑ Prisma Access licence ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités à votre disposition dans Strata Cloud Manager dépendent des licences que vous utilisez.

Examinez l'état du transfert de vos configurations précédentes vers vos pare-feu et vérifiez les détails tels que le résultat de l'opération de transfert, l'administrateur qui a initié le transfert et les pare-feux ciblés.

STEP 1 | Se connecter à Strata Cloud Manager

STEP 2 | Enregistrez les modifications de configuration.

STEP 3 | Sélectionnez **Manage (Gestion)** > **Operation (Opération)** > **Push Status (État du transfert)** et localisez l'opération de transfert de configuration que vous souhaitez examiner.

STEP 4 | Développez l'`ID du projet` pour le transfert de configuration que vous souhaitez évaluer.

Un travail `de validation de` la configuration est toujours effectué avant tout transfert de configuration. Lorsque vous effectuez un transfert vers plusieurs pare-feu, chaque transfert de configuration possède un `ID du projet` unique avec les détails du transfert.

STEP 5 | Examinez les détails de l'état de transmission de la configuration.

Par exemple, examinez le `Résultat` du transfert, l'`administrateur` ayant lancé le transfert de configuration, le `Résumé` du transfert de configuration, l'`heure de fin` et l'`heure de début` du transfert de configuration.

Le `Résultat` du transfert de configuration peut être soit `OK` si le transfert a été réussi, soit `ÉCHEC` si le transfert de configuration a échoué.

STEP 6 | Cliquez sur l'`ID du projet` unique pour une configuration de transfert vers un pare-feu en vue d'évaluer les détails du projet.

Les Détails du projet fournissent des informations détaillées sur les `Avertissements` et les`Erreurs` résultant de l'exécution du transfert de configuration. Par exemple, si un transfert vers un pare-feu a échoué, vous pouvez consulter les Détails du projet pour comprendre ce qui est à l'origine de l'échec du transfert de configuration.

Gestion : Instantanés de la version de la configuration

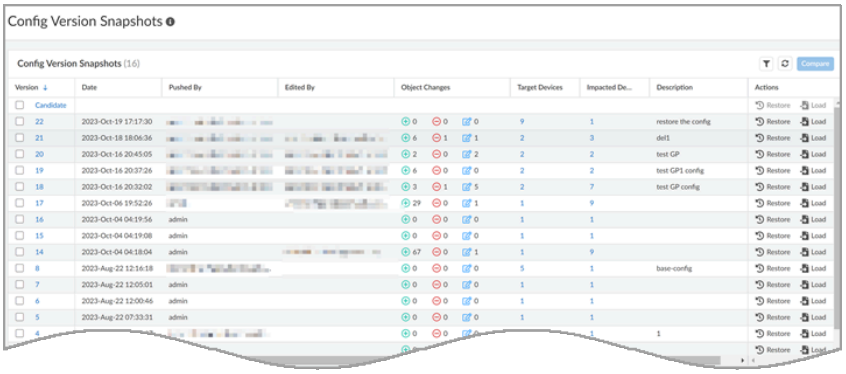
Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ Au moins une de ces licences est nécessaire pour gérer votre configuration avec Strata Cloud Manager ; pour une gestion unifiée des NGFW et de Prisma Access, vous aurez besoin des deux : ❑ Prisma Access licence ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités à votre disposition dans Strata Cloud Manager dépendent des licences que vous utilisez.

Les instantanés de configuration vous donnent un aperçu de l'historique de votre configuration Strata Cloud Manager. Lorsqu'une modification de la configuration poussée a des conséquences inattendues sur la sécurité ou un impact inattendu sur le trafic, vous pouvez revenir à une version antérieure. Vous pouvez également comparer les configurations pour déterminer ce qui a changé d'une version à l'autre.

Aperçu de l'instantané de la configuration

L'écran Version de l'instantané de configuration est l'endroit où vous pouvez examiner les configurations poussées, comparer les instantanés de configuration avec votre candidat de configuration et charger ou restaurer des configurations plus anciennes.

Sélectionnez **Manage (Gérer)** > **Operations (Opérations)** > **Config Version Snapshots (Instantanés de la version de configuration)** pour trouver des instantanés de configuration et restaurer, charger ou comparer des versions.



1. **Add New Filter (Ajouter un nouveau filtre)** : choisissez des filtres pour trier et filtrer les versions de configuration par colonne.
2. **Version** : le numéro de version de la configuration qui a été poussée.

   Le **candidat** vous permet de comparer les changements de configuration en cours effectués sur Strata Cloud Manager à une version antérieure de la configuration.

   Le numéro de la version de configuration est progressif. Par exemple, si vous avez 10 versions et que vous restaurez la version de configuration 2, la version de configuration passera de 10 à 11 (elle ne s'affichera pas comme 2).
3. **Date** : date et heure auxquelles la configuration a été envoyée.
4. **Pushed By (Poussé par)** : administrateur qui a poussé les modifications.
5. **Edited By (Modifié par)** : l'administrateur qui a effectué les modifications de configuration avant qu'elles ne soient poussées.
6. **Object Changes (Modifications d'objets)** : voyez combien d'objets ont été ajoutés, supprimés ou modifiés lorsque la configuration a été poussée.
7. **Target Devices (Périphériques cibles)** : périphériques ciblés dans le cadre de l'instantané de configuration poussée.

   Lorsque vous effectuez une action de **Restauration**, vous pouvez choisir sur quel périphérique effectuer l'opération.
8. **Impacted Devices (Périphériques concernés)** : périphériques qui ont été modifiés depuis la dernière configuration poussée. Les périphériques sont uniquement considérés comme impactés par rapport à l'instantané de configuration poussée précédent.

   Périphériques concernés et cibles

   Si vous avez deux périphériques, A et B, et que vous poussez uniquement vers le périphérique A, A devient le périphérique cible et impacté.

   Si vous envoyez ensuite à nouveau sur le périphérique A et B, A et B sont tous deux des périphériques ciblés, mais seul B est un périphérique impacté.

   Lors de l'exécution d'une action **de chargement** , les périphériques répertoriés seront impactés.
9. **Description** : passez en revue toutes les informations fournies au moment où la configuration a été poussée.
10. **Actualiser** : mettre à jour les informations dans la table d'instantanés.
11. **Réinitialiser les filtres** : effacez tous les filtres pour afficher toutes les versions de configuration.
12. **Comparer** : découvrez ce qui a changé d'une version à l'autre.

    Vous pouvez comparer uniquement deux versions à la fois.

13. **Actions** : vous pouvez **restaurer** ou **charger** une version de configuration.

- **Restaurer** : restaurer une version de configuration antérieure.

  La restauration d'une version de configuration met directement à jour la configuration en cours d'exécution sur les déploiements dans le cadre de l'envoi d'origine et ne nécessite pas de **transmettre la configuration**.

  Restaurez tous les périphériques ou déploiements dans la portée d'origine de la configuration poussée ou encore sélectionnez des périphériques ou déploiements spécifiques à restaurer. Vous ne pouvez pas étendre la configuration pour inclure des périphériques ou des déploiements en dehors de la portée d'origine.

  La restauration d'une version de la configuration ne supprime ni ne modifie la configuration candidate. La configuration en cours sera enregistrée. La restauration d'une configuration ne fait que mettre à jour la version de la configuration en cours d'exécution. Les déploiements peuvent sembler désynchronisés quand l'action de restauration est utilisée.
- **Load (Charger)** : chargez une version antérieure en tant que configuration candidate dans Strata Cloud Manager. Votre configuration candidate actuelle sera perdue lorsqu'une configuration plus récente sera chargée.

  Effectuez des mises à jour de la nouvelle configuration candidate ou appliquez la configuration à de nouveaux périphériques et déploiements en dehors de l'instantané de configuration d'origine et, lorsque vous êtes prêt, **Push Config (Transmettre la configuration)**.
- **Save (Enregistrer)** : enregistrez la configuration candidate en tant qu'instantané nommé à utiliser comme configuration connue. Disposer d'une configuration connue vous permet d'amener rapidement vos déploiements à un état connu et exploitable. Vous pouvez basculer entre vos **Named Snapshots (Instantanés nommés)** et les transferts de configuration enregistrés automatiquement dans **Version Snapshots (Instantanés de version)**.

Strata Cloud Manager enregistrera jusqu'à 6 mois d'instantanés ou 200 instantanés individuels.

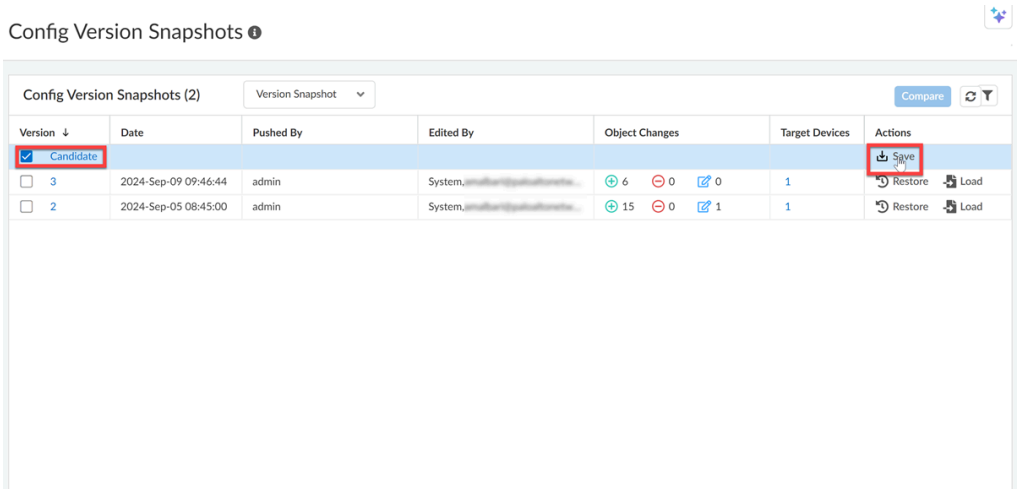
Enregistrer un Instantané nommé

Enregistrer le candidat de configuration actuel en tant qu'instantané nommé. Vous pouvez enregistrer une configuration partielle sous la forme d'un instantané nommé. L'enregistrement d'un instantané nommé vous permet de charger un état de configuration connu sans avoir à suivre les instantanés individuels qui seront finalement supprimés de la table d'instantanés des versions de configuration.

STEP 1 | Se connecter à Strata Cloud Manager.

STEP 2 | Sélectionnez **Manage (gérer)** > **Operations (Opérations)** > **Instantanés de la version de configuration**.

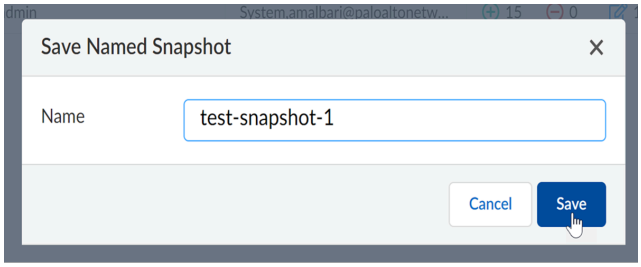
STEP 3 | Sélectionnez le **Candidate (Candidat)**.



STEP 4 | Cliquez sur **Save (Enregistrer)**.

STEP 5 | Entrez un **Name (nom)** jusqu'à 64 caractères.

Le nom de l'instantané sera par défaut **config_year-month-day-timestamp**.

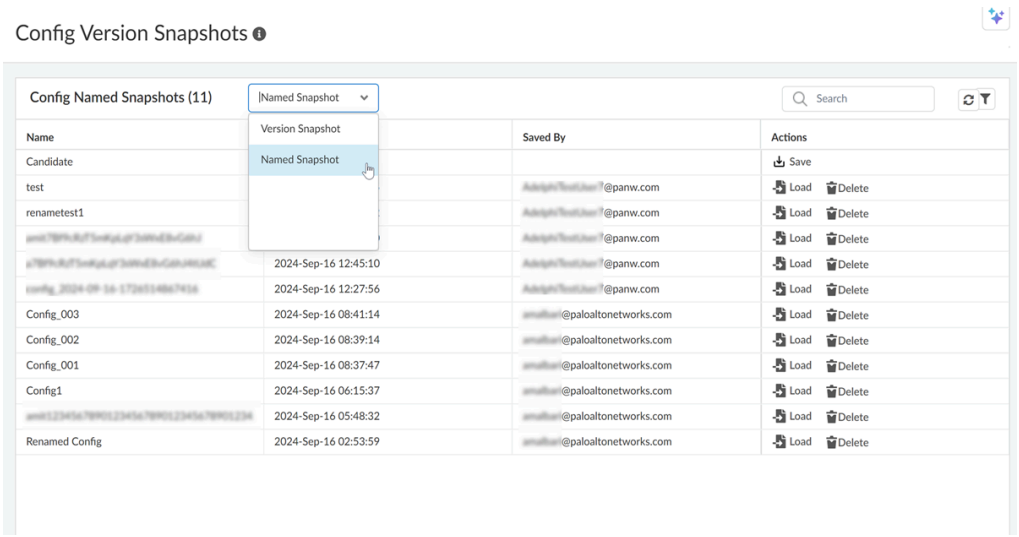


STEP 6 | **Save (Sauvegardez)** votre instantané.

STEP 7 | (Facultatif) Vérifiez que votre instantané a été enregistré en accédant aux **Named Snapshots** dans le tableau Instantanés de version de configuration.

Gestion des instantanés nommés

Les administrateurs ont la possibilité de supprimer leurs propres instantanés nommés. Les super utilisateurs peuvent supprimer tous les instantanés nommés.



Restaurer un instantané

Restaurer une configuration précédemment poussée. La restauration d'une ancienne configuration met à jour la configuration exécutée sur les déploiements et les périphériques. Ces changements ne sont pas reflétés dans la Strata Cloud Manager, les déploiements et les périphériques peuvent donc sembler désynchronisés.

Seuls les périphériques configurés qui étaient dans le champ d'application de la configuration poussée d'origine peuvent être restaurés vers une version sélectionnée.

STEP 1 | Se connecter à Strata Cloud Manager.

STEP 2 | Sélectionnez **Manage (gérer)** > **Operations (Opérations)** > **Instantanés de la version de configuration**.

STEP 3 | Sélectionnez la version de configuration que vous souhaitez restaurer.

1. (Facultatif) Sélectionnez le numéro de version pour consulter les modifications apportées par l'instantané de configuration.

STEP 4 | **Restaurer** la version.

1. (Facultatif) Sélectionnez les périphériques que vous souhaitez cibler avec l'action de restauration.
2. **Restore (Restaurer)**.

STEP 5 | (Facultatif) Sélectionnez **Manage (Gérer)** > **Configuration (Configuration)** > **Operations (Opérations)** > **Push Config (Transmettre la configuration)** pour valider la restauration de la configuration.

Charger un instantané

Charger un instantané de configuration antérieur à utiliser comme configuration candidate.

Une fois la configuration chargée, vous pouvez continuer à y apporter des modifications avant de la valider.

STEP 1 | Se connecter à Strata Cloud Manager.

STEP 2 | Sélectionnez **Manage (Gérer)** > **Operations (Opérations)** > **Config Version Snapshots (Instantanés de la version de configuration)**.

STEP 3 | Sélectionnez la version de configuration que vous souhaitez charger.

1. (Facultatif) Sélectionnez le numéro de version afin de consulter les modifications apportées par l'instantané de configuration.

STEP 4 | **Load (Charger)** la version.

STEP 5 | (Facultatif) Modifiez le candidat de configuration chargé selon vos besoins.

STEP 6 | **Push Config (Transmettre la configuration)**.

Gestion : Posture de sécurité

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ Au moins une de ces licences est nécessaire pour gérer votre configuration avec Strata Cloud Manager ; pour une gestion unifiée des NGFW et de Prisma Access, vous aurez besoin des deux : ❑ Prisma Access licence ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités à votre disposition dans Strata Cloud Manager dépendent des licences que vous utilisez.

Utilisez ces outils pour améliorer votre posture de sécurité et vérifier que vous êtes protégé contre les menaces en suivant les meilleures pratiques en matière de politique de sécurité.

- Personnalisez les contrôles liés à la posture de sécurité pour votre déploiement afin de maximiser les recommandations pertinentes dans Gestion : Paramètres de la posture de sécurité
- Utilisez Config Cleanup (Nettoyage de la configuration) pour identifier et supprimer les objets de configuration et les règles de politique inutilisées.
- Configurez les contrôles de conformité pour affiner et optimiser les règles de sécurité trop permissives afin qu'elles n'autorisent que les applications réellement utilisées sur votre réseau.
- Créez votre propre Gestion : Paramètres de la posture de sécurité : personnalisez les contrôles des meilleures pratiques existants ou créez et gérez des exemptions spéciales pour mieux répondre aux exigences professionnelles de votre organisation.
- Utilisez Policy Analyzer pour vous assurer rapidement que les mises à jour apportées à vos règles de politique de sécurité répondent à vos exigences et n'introduisent pas d'erreurs ou de mauvaises configurations (telles que des modifications entraînant des règles en double ou en conflit).

Gestion : Analyseur de politique

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• NGFW (Panorama géré) • VM-Series, funded with Software NGFW Credits (Panorama géré) • Prisma Access (Managed by Panorama)	❑ Au moins une de ces licences est nécessaire : ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro ❑ Module d'extension du Panorama CloudConnector pour les déploiements gérés par Panorama

Les mises à jour de vos règles de politique de sécurité sont souvent sensibles au temps et nécessitent une action rapide. Cependant, vous voulez-vous assurer que toute mise à jour que vous apportez 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).

Afin d'y parvenir, Policy Analyzer dans Strata Cloud Manager vous permet d'optimiser le temps et les ressources lors de la mise en œuvre d'une requête de modification. Policy Analyzer 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 défaillances, telles que les Zones d'ombre, les Redondances, les Généralisations, les Corrélations et les Consolidations dans votre base de règles.

Utilisez Policy Analyzer pour ajouter ou optimiser votre base de règles de politique de sécurité.

- **Avant d'ajouter une nouvelle règle**—Vérifiez si de nouvelles règles doivent être ajoutées. Policy Analyzer recommande la meilleure façon de modifier vos règles de politique de sécurité existantes pour répondre à vos exigences sans ajouter une autre règle, si possible.
- **Rationalisez et optimisez votre base de règles existante**—Voyez où vous pouvez mettre à jour vos règles pour réduire au minimum les prolifération 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 changements**—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 après le changement**—Permet de nettoyer la base de règles existante en identifiant les Zones d'ombres, les Redondances et autres défaillances accumulées au fil du temps.

Consultez Policy Analyzer pour en savoir plus.

Gestion : Optimiseur de politique

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ Au moins une de ces licences est nécessaire pour gérer votre configuration avec Strata Cloud Manager ; pour une gestion unifiée des NGFW et Prisma Access, vous aurez besoin des deux : ❑ licence Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités disponibles Strata Cloud Manager dépendent des types de licences que vous utilisez.

Essayez Policy Optimizer pendant qu'il est disponible en accès anticipé. Si vous souhaitez continuer à utiliser cette fonctionnalité au-delà de la période d'accès anticipé, contactez votre équipe chargée du compte.

Les règles trop permissives introduisent des failles de sécurité, car elles autorisent des applications qui ne sont pas utilisées sur votre réseau. Policy optimizer vous permet de convertir ces règles trop permissives en règles plus spécifiques et ciblées qui se limitent à autoriser uniquement les applications que vous utilisez réellement.

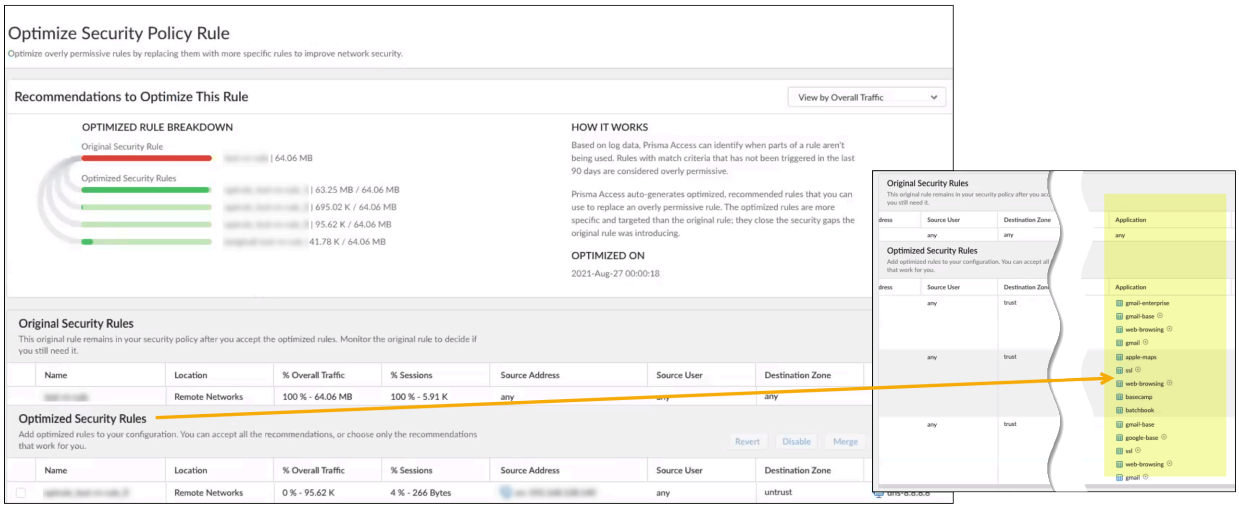
Seules les règles créées il y a plus de 90 jours sont prises en compte pour l'optimisation des politiques.

Comment cela fonctionne

Strata Cloud Manager analyse les données du journal et classe les règles comme trop permissives lorsqu'elles autorisent **tout** trafic d'application, et les règles doivent dater d'au moins 90 jours. Ces règles peuvent introduire des failles de sécurité, si elles autorisent un trafic qui n'est pas nécessaire pour une utilisation en entreprise.

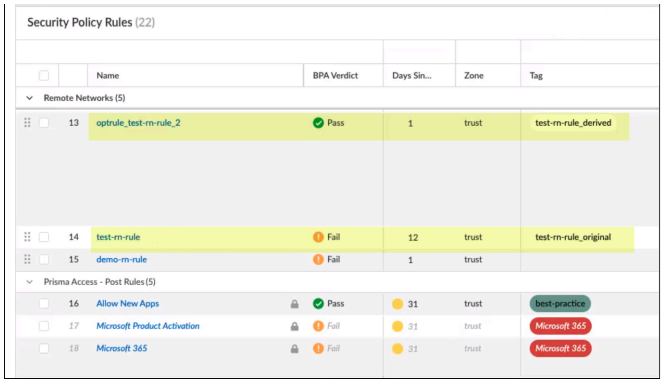
Pour les règles identifiées comme trop permissives, Strata Cloud Manager génère automatiquement des recommandations que vous pouvez accepter pour optimiser la règle. Strata Cloud Manager analyse les données du journal et classe les règles comme trop permissives lorsqu'elles autorisent tout trafic d'application, et les règles doivent dater d'au moins 90 jours.

Sélectionnez une règle trop permissive pour examiner, ajuster et accepter les recommandations d'optimisation. Le remplacement de ces règles par les règles recommandées plus spécifiques renforce votre posture de sécurité.



Accepter les recommandations d'optimisation d'une règle ne supprime pas la règle d'origine. La règle d'origine reste répertoriée sous les nouvelles règles de votre politique de sécurité ; cela vous permet de surveiller la règle et de la supprimer lorsque vous êtes sûr qu'elle n'est pas nécessaire.

La règle d'origine et les règles optimisées sont toutes deux marquées afin que vous puissiez les identifier facilement dans votre politique de sécurité :



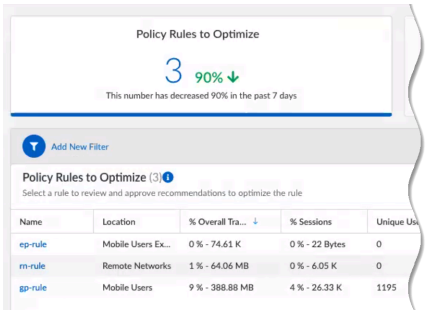
Optimiser une règle

STEP 1 | Visitez **Config Cleanup (Nettoyage de la configuration)** pour voir s'il existe des règles que vous pouvez optimiser.

Accédez à **Manage (Gestion)** > **Security Posture (Posture de sécurité)** > **Policy Optimizer (Optimisateur de politique)**.

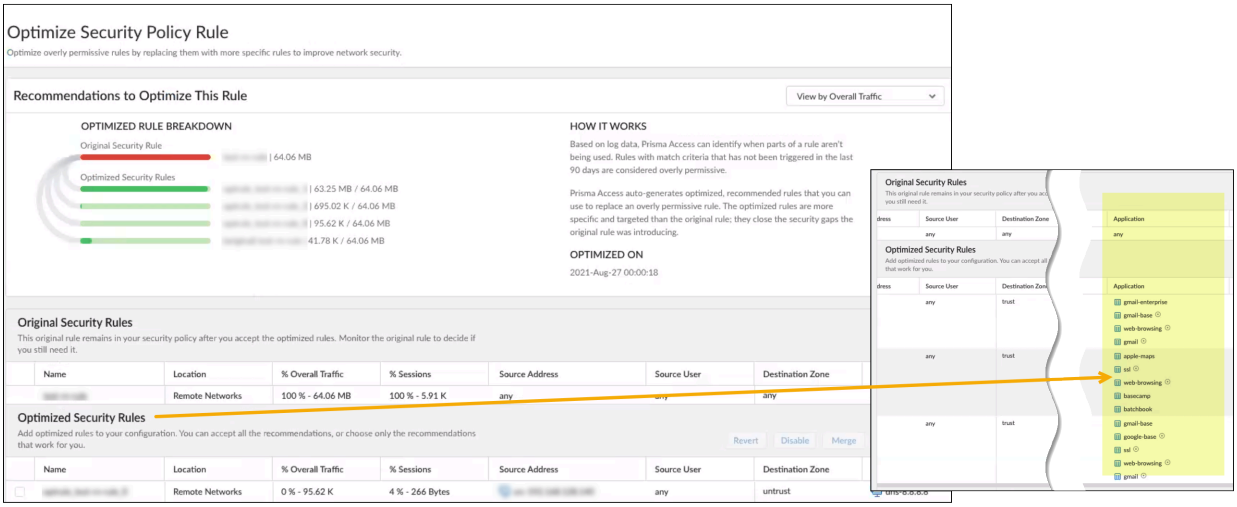
STEP 2 | Passez en revue les règles trop permissives et choisissez une règle pour voir les recommandations d'optimisation.

S'il existe plusieurs règles trop permissives, concentrez-vous sur l'optimisation des règles qui ont le plus d'impact sur le trafic ; cela vous permettra de réaliser les gains les plus significatifs en matière de renforcement de votre posture de sécurité.



STEP 3 | Examinez les règles recommandées et optimisées.

Vous pouvez voir quelle part du trafic de la règle d'origine sera couverte par chaque nouvelle règle. Notez les applications spécifiques que chaque nouvelle règle met en œuvre.



STEP 4 | Accepter tout ou une partie des recommandations de la règle.

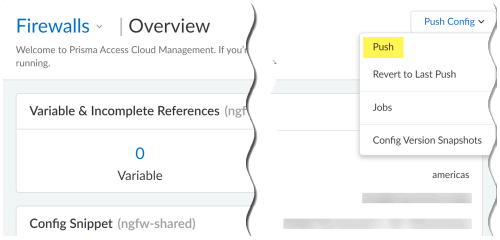
L'acceptation des nouvelles règles optimisées les ajoute à votre base de règles. Ils ne seront pas encore actifs ; cela se produira à l'étape suivante lorsque vous allez **Push Config (Transmettre la configuration)** vers Prisma Access.

Accept All (Accepter tout) accepte les règles recommandées telles qu'elles sont. Vous pouvez également apporter des modifications avant d'accepter les règles optimisées :

- Supprimer une règle d'optimisation. Ajoutez cette règle à une liste de règles que vous souhaitez exclure de l'optimisation (cette fois-ci et ultérieurement).
- Désactiver une règle optimisée. Cela signifie que vous n'acceptez pas cette règle et qu'elle ne sera pas ajoutée à la base de règles.
- Annulez toutes les modifications que vous avez apportées. Cette opération annule toutes les modifications que vous avez apportées et rétablit les règles telles qu'elles étaient recommandées.
- Fusionner les règles. Vous pouvez décider de le faire si vous trouvez que l'une des règles recommandées est similaire.

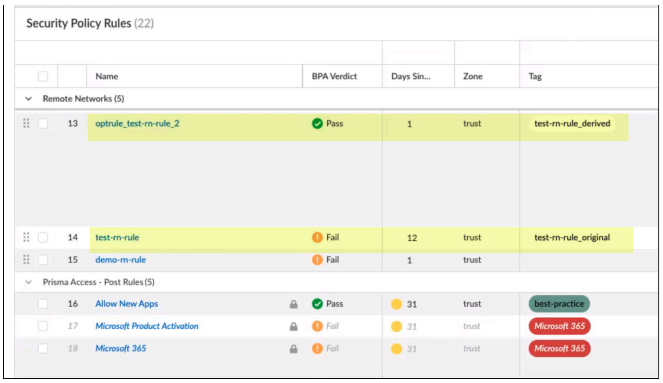
Après avoir accepté les règles optimisées, vous serez invité à **Update Rulebase (Mettre à jour la base de règles)**. Lorsque vous acceptez, les règles optimisées sont ajoutées à votre politique de sécurité. Toutefois, ils n'appliquent pas encore les règles de trafic.

STEP 5 | **Push Config (Transmettre la configuration)** pour envoyer les mises à jour de configuration à Prisma Access et commencer à appliquer les règles optimisées.



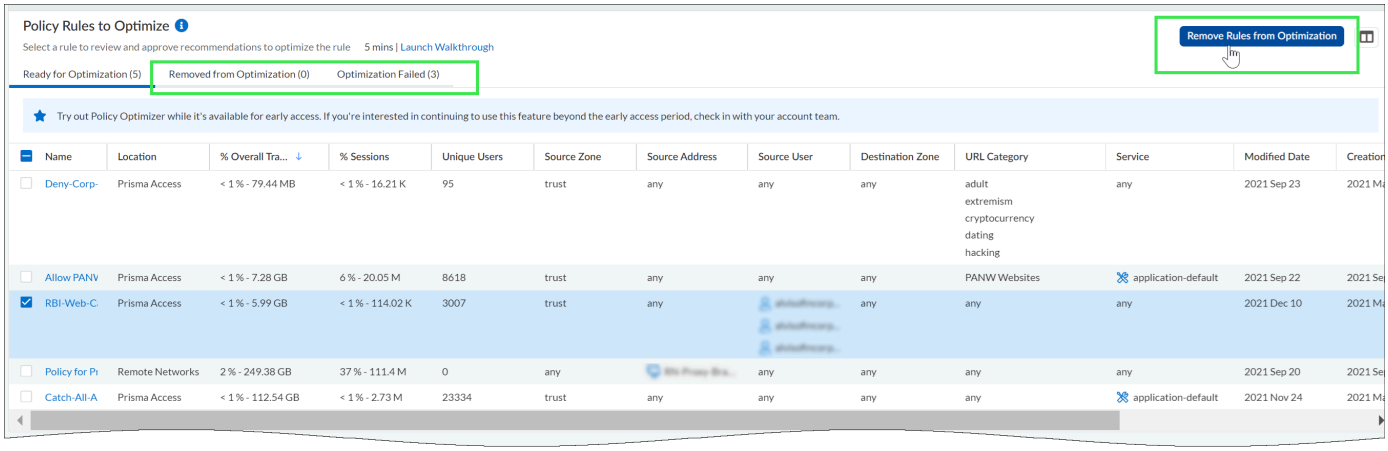
STEP 6 | Surveillez la règle initiale de manière à vous assurer que vous n'en avez pas besoin.

Les règles originales, trop permissives, restent dans votre politique de sécurité ; elles sont répertoriées sous les règles optimisées dans votre base de règles et sont étiquetées afin que vous puissiez les identifier facilement. Le nom de la balise ajoute _original au nom de la règle (par exemple, security-rule-name_original).



Exclure une règle de l'optimisation

Déplacez une règle vers la liste **Excluded from Optimization (Exclus de l'optimisation)** et Prisma Access ne l'optimisera pas. Les paramètres des règles restent tels quels.

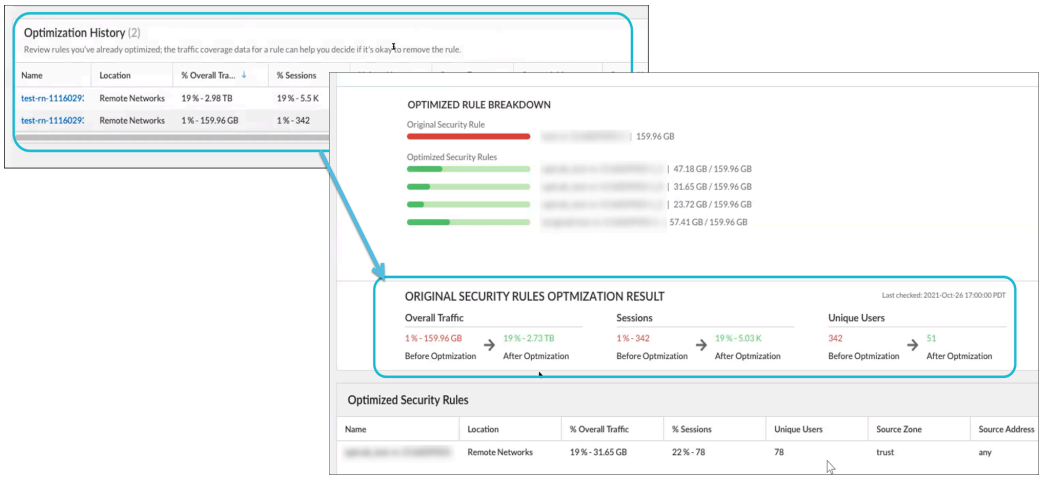


Assurez-vous de **Push Config (Transmettre la configuration)** après avoir déplacé une règle vers la liste d'exclusion ; après avoir exécuté la configuration, il peut falloir jusqu'à 24 heures pour que la règle s'affiche sur la liste. Vous pouvez toujours choisir d'ajouter à nouveau la règle à la liste d'optimisation ultérieurement.

Suivi des résultats de l'optimisation

Policy Optimizer affiche un historique des règles de sécurité que vous avez optimisées. Les données historiques incluent les résultats de l'optimisation : comparez la couverture du trafic de la règle d'origine avec les règles optimisées.

Les données que vous voyez pour **Policy Optimizer History (Historique de Policy Optimizer)** concernent les 30 derniers jours. Si une règle originale (une règle que vous avez optimisée) n'obtient aucun résultat pendant six mois, elle est supprimée de l'historique de Policy Optimizer et est classée à la place comme une règle de politique à zéro résultat.



Gestion : Nettoyage de la configuration

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ Au moins une de ces licences est nécessaire pour gérer votre configuration avec Strata Cloud Manager ; pour une gestion unifiée des NGFW et Prisma Access, vous aurez besoin des deux : ❑ licence Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités disponibles Strata Cloud Manager dépendent des types de licences que vous utilisez.

Utilisez Nettoyage de configuration pour identifier et supprimer les objets de configuration et les règles de politique inutilisés de votre configuration Strata Cloud Manager. La suppression des objets de configuration inutilisés permet de faciliter l'administration du pare-feu en éliminant l'encombrement et en ne conservant que les objets de configuration nécessaires à la mise en œuvre de la sécurité.

STEP 1 | Se connecter à Strata Cloud Manager.

STEP 2 | Sélectionnez **Manage (Gestion)** > **Security Posture (Posture de sécurité)** > **Config Cleanup (Nettoyage de la configuration)**.

STEP 3 | Sélectionnez les objets inutilisés et les règles de politique sur l'ensemble de votre configuration Strata Cloud Manager pour les 6 derniers mois.

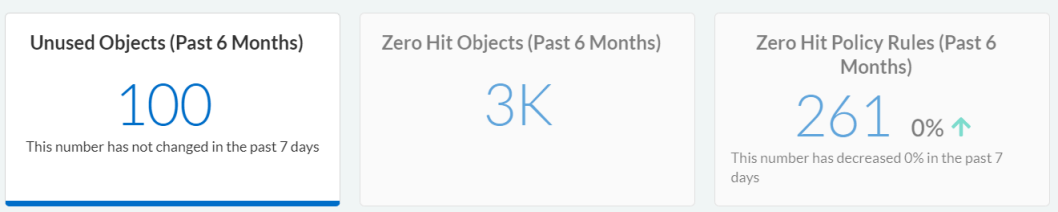
- **Policy Rules to Optimize (Règles de politique à optimiser)** : cliquez pour passer en revue les règles de politique qui sont trop permissives pour les convertir en règles plus spécifiques et ciblées qui n'autorisent que les applications que vous utilisez réellement.
- **Unused Objects (Past 6 Months) (Objets inutilisés (6 derniers mois))** : tous les objets de configuration qui sont restés inutilisés dans une règle de configuration ou de politique au cours des 6 derniers mois.
- **Règles zéro coup (6 derniers mois)** : Règles de politique avec objets de configuration dont l'objet de configuration dans la règle de politique ne reçoit aucun coup.

  Les objets de configuration répertoriés ont reçu zéro coup uniquement dans les règles de politique auxquelles ils sont associés. Leur utilisation peut être affectée par les autres règles de politique générale dans lesquelles elles sont utilisées.
- **Zero Hit Rules (Past 6 Months) (Règles zéro coup (au cours des 6 derniers mois))** : toutes les règles de politique qui ont eu zéro correspondance de trafic au cours des 6 derniers mois.

STEP 4 | Appliquer des filtres supplémentaires pour cibler des objets inutilisés spécifiques et des règles de politique.

Add New Filter (Ajouter un nouveau filtre) est pris en charge pour les **Unused Objects (Past 6 Months) (Objets inutilisés (6 derniers mois))** et **Zero Hit Policy Rules (Past 6 Months) (Règles de politique de zéro coup (6 derniers mois))**.

- **Objets inutilisés (6 derniers mois)** : vous pouvez filtrer et **Delete (Supprimer)** les objets inutilisés en fonction :
  - **Name (Nom)** : recherchez et sélectionnez un nom d'objet de configuration spécifique.
  - **Location (Emplacement)** : portée de configuration dans laquelle le nom de l'objet de configuration a été créé.
  - **Object Type (Type d'objet)** : type d'objet de configuration.
  - **Days Unused (Jours non utilisés** : nombre de jours d'utilisation de l'objet de configuration.
    - **< 50** : moins de 50 jours inutilisés.
    - **>= 50, <=100** : entre 50 et 100 jours inutilisés.
    - **< 50** : plus de 100 jours inutilisés.
- **Zero Hit Policy Rules (Past 6 Months) (Règles de stratégie zéro coup (6 derniers mois))** : vous pouvez filtrer et **Enable (Activer)**, **Disable (Désactiver)** ou **Delete (Supprimer)** les règles de politique zéro coup en fonction du **Name (Nom)**, des **Days with Zero Hits (Jours avec zéro coup)** ou de l'une des données `Source` et `Destination`.



Gestion : Paramètres de la posture de sécurité

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW, notamment ceux financés par les crédits NGFW logiciels • Prisma Access (Managed by Panorama or Strata Cloud Manager) • Prisma SD-WAN	Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Prisma SD-WAN ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités qui vous sont offertes dans Strata Cloud Manager dépendent de la ou des licences que vous utilisez.

Strata Cloud Manager exploite un ensemble de contrôles de meilleures pratiques prédéfinis qui s'alignent sur les contrôles standard de cybersécurité spécifiques au secteur, tels que CIS (Center for Internet Security) et NIST (National Institute of Standards and Technology) et les contrôles personnalisés que vous créez en fonction des besoins spécifiques de votre organisation. Ces contrôles évaluent les configurations et les paramètres au sein de l'infrastructure cloud, en identifiant les écarts par rapport aux meilleures pratiques ou aux exigences de conformité.

Les contrôles de l'état de la sécurité dans Strata Cloud Manager englobent une série de domaines de sécurité, notamment la sécurité du réseau, la protection des données et la gestion de l'identité et de l'accès. Ces contrôles évaluent les règles de pare-feu, le cryptage, les mécanismes d'authentification et l'intégrité générale des configurations.

Lorsque votre configuration détecte des écarts, Strata Cloud Manager fournit des informations exploitables et des recommandations de remédiation, et peut même automatiser certaines parties du processus de correction des mauvaises configurations et des paramètres non conformes pour vous aider à maintenir un environnement cloud sécurisé et conforme avec une intervention manuelle minimale.

Les paramètres de l'état de sécurité regroupent les fonctionnalités des pages de paramètres de contrôle de sécurité d'AIOps et de Strata Cloud Manager.

Sélectionnez **Manage (Gestion)** > **Settings (Paramètres)** > **Security Posture (État de sécurité)** pour afficher, gérer et personnaliser les contrôles de posture de sécurité pour votre déploiement afin de maximiser les recommandations pertinentes.

- **Security Checks (Vérifications de sécurité)** : liste des vérifications des meilleures pratiques utilisées pour évaluer votre configuration.

  Votre configuration est comparée à ces vérifications pour évaluer la posture de sécurité de vos périphériques et générer des alertes de sécurité. Vous pouvez effectuer les actions suivantes pour gérer ces vérifications en fonction de votre environnement :

  1. Définissez le niveau de complexité de vos contrôles personnalisés afin d'identifier les contrôles les plus critiques pour votre déploiement.

     Vous pouvez modifier le niveau de complexité de vos contrôles personnalisés, mais les niveaux de complexité des contrôles des meilleures pratiques de Palo Alto Networks sont fixes et ne peuvent pas être modifiés.

  2. Créez et supprimez vos propres vérifications personnalisées, clonez et modifiez les vérifications existantes pour en créer de nouvelles, et faites des exceptions spéciales

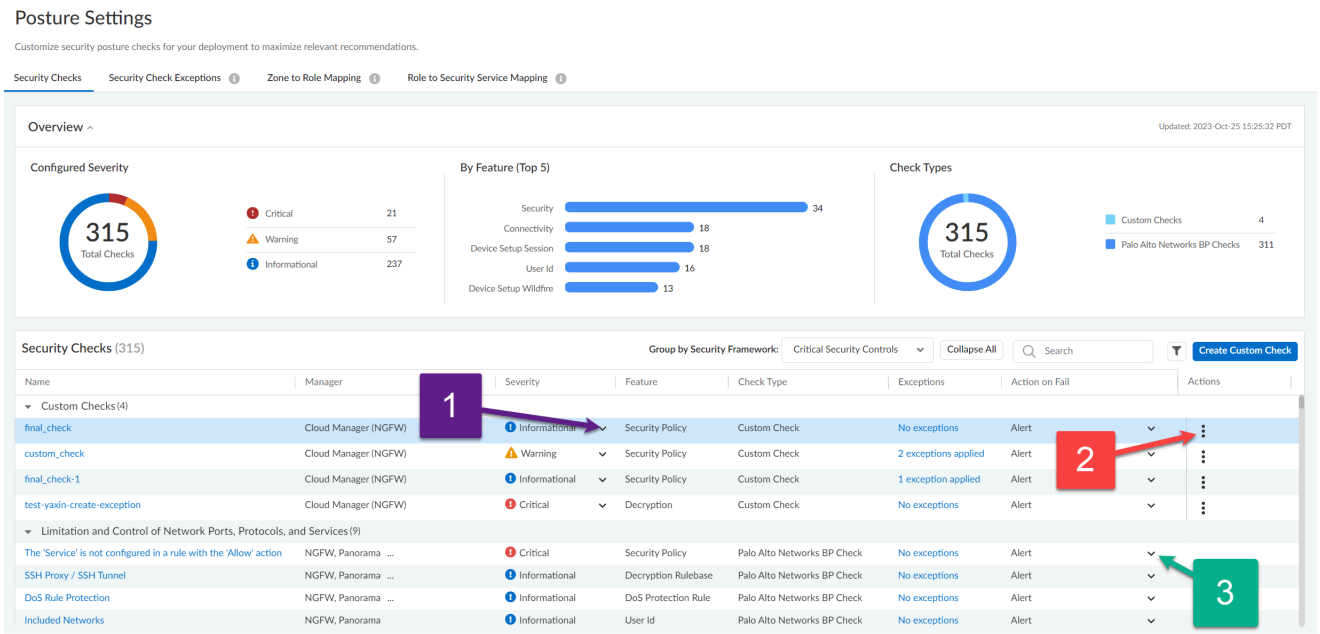
pour les vérifications que vous ne souhaitez pas voir appliquées à des parties de votre déploiement.

Dans le cadre du déploiement initial de ces contrôles, vous pouvez cloner les contrôles qui se trouvent dans le cadre du contrôle personnalisé.

3. Définissez la réponse lorsqu'une vérification échoue.
   - **Alert (Alerte)** (par défaut)—Déclenche une alerte pour l'échec de la vérification.
   - **Block (Bloquer)**—Arrêtez les mauvaises configurations potentielles avant qu'elles n'entrent dans votre déploiement. Bloc peut signifier l'un des éléments suivants selon la façon dont vous le gérez :
     - **Vérifications en ligne sur Strata Cloud Manager**—Vous empêche de valider ou de pousser une configuration non conforme, mais ne vous empêche pas d'enregistrer votre configuration localement.
     - **Vérifications en ligne en temps réel* sur Strata Cloud Manager** — Vous empêche même d'enregistrer une configuration non conforme.
     - **Panorama géré**** —Empêche la validation d'une configuration non conforme dans Panorama, mais n'empêche pas son enregistrement dans la configuration candidate de Panorama.
     - Interface Web PAN-OS, gestion des API ou des CLI—Block n'a aucun effet coercitif sur les configurations qui ne sont pas gérées par le Cloud ou par Panorama.

**En raison de leur complexité logique, certains contrôles en ligne sont exécutés de manière asynchrone selon un calendrier fixe, mais pas en temps réel. L'échec d'un contrôle en temps réel dans votre configuration vous empêchera d'enregistrer cette configuration, même localement.*

***Le Panorama CloudConnector Plugin est requis pour appliquer l'action de validation de bloc sur Panorama.*



- **Exceptions des contrôles de sécurité**

  Désactivez les vérifications individuelles pour les périphériques ou les groupes de périphériques que vous spécifiez.
- **Mappage de zone sur un rôle**

  Mapper les zones dans les NGFW aux rôles pour obtenir des recommandations personnalisées.
- **Mappage des rôles en fonction des services de sécurité**

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

Créer une vérification personnalisée

Créez votre propre vérification personnalisée à partir d'un contrôle existant. Vous pouvez également passer à l'étape 4 pour créer une vérification personnalisée à partir de zéro.

STEP 1 | Sélectionnez **Manage (Gestion)** > **Settings (Paramètres)** > **Security Posture (Posture de sécurité)**.

STEP 2 | Identifiez le chèque que vous souhaitez cloner et cliquez sur **Clone (Cloner)**.

STEP 3 | **Edit (Modifiez)** le contrôle que vous avez cloné et passez à l'étape 5 pour effectuer vos modifications.

STEP 4 | Accédez à **Manage (Gestion)** > **Settings (Paramètres)** > **Security Posture (Posture de sécurité)**, puis sélectionnez **Create Custom Check (Créer une vérification personnalisée)**.

STEP 5 | Spécifiez les **General Information (Informations Générales)** pour votre vérification. Votre vérification personnalisée doit avoir un **Nom** et une **Description**, mais vous devez également ajouter une **Recommandation** et une **Justification** pour votre vérification afin d'aider les autres à comprendre l'intention de votre vérification personnalisée et les meilleures pratiques à cet égard.

STEP 6 | Facultatif Sélectionnez un **type d'objet** : la section de votre configuration pour laquelle vous créez une vérification qui détermine quelles **propriétés de règle** vous pouvez choisir lors de la création de votre vérification.

STEP 7 | Utilisez le **Générateur logique** pour votre vérification personnalisée.

1. **Ajouter l'expression** : une seule ligne logique qui décrit les critères de correspondance pour une configuration.

Propriétés de la règle à faire correspondre	Opérateur de match	Critères spécifiques
• Généralités – Nom, description, poste et horaire • Sources–Zones, adresses, utilisateurs	• Est • N'est pas • Est vide • N'est pas vide • Commence par	[Champ texte]

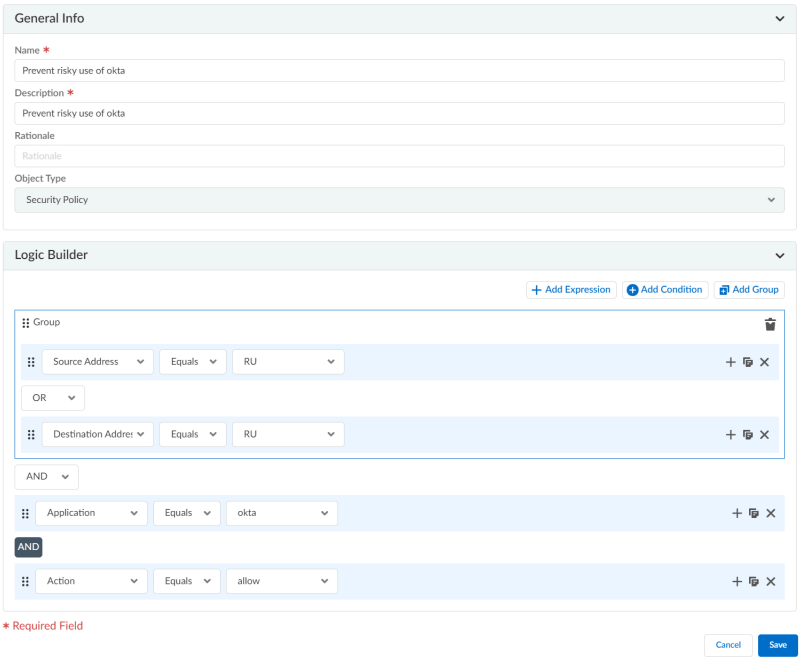
• Destinations–Zones et adresses • Applications, services et adresses URL • Actions et vérification avancée	• Se termine par • Contient • Supérieur à • In • Est égal ou supérieur à • Est égal ou inférieur à • Inférieur à • Égal • N'est pas égal à • Ne contient pas • Tout de • Certains • Aucun de	

2. **Ajouter une condition** – Utilisez des opérateurs logiques (tels que AND, OR, IF, THEN, ELSE et ELSE IF) pour connecter ou combiner des expressions, des conditions supplémentaires et des groupes.
3. **Ajouter un groupe** – Créez un ensemble d'expressions, de conditions ou les deux. Ce groupe, pris ensemble, aboutit à une condition Vrai ou Faux.

   - *Ajoute une nouvelle expression ou un état*
   - *Clone une expression ou un état*
   - *Supprime une expression ou un état*

   L'expression dans cet exemple émet un avertissement lorsqu'elle voit des règles de politique qui autorisent le trafic Okta vers et depuis des adresses IP russes. L'exemple

illustre simplement le fonctionnement du générateur de logique et ne constitue pas une recommandation.



STEP 8 | **Save (Enregistrez)** votre vérification.

Gérez vos chèques

Vous pouvez effectuer l'une des **Actions (Actions)** suivantes lors de vos vérifications de sécurité :

- **Clone***–Crée une copie d'un chèque.
- **Modifier****–Apporter des modifications à une vérification personnalisée existante.
- **Supprimer****–Supprime un contrôle personnalisé que vous avez créé.

Sélectionnez les contrôles pour lesquels vous souhaitez prendre des mesures et choisissez l'action appropriée.

- **Vous pouvez cloner une seule vérification à la fois.*
- ***Vous pouvez modifier ou supprimer des contrôles personnalisés uniquement.*
- *Vous devrez peut-être obtenir l'autorisation d'un administrateur pour modifier un contrôle personnalisé.*

Créer une exception pour un chèque

Si nécessaire, vous pouvez restreindre l'endroit où les contrôles sont appliqués dans votre déploiement.

STEP 1 | Sélectionnez **Manage (Gestion)** > **Settings (Paramètres)** > **Security Posture (État de sécurité)** > **Security Check Exceptions (Exceptions de vérification de sécurité)** et **Create Security Check Exception (Créer une exception de vérification de sécurité)**.

Sinon, sélectionnez **Manage (Gestion)** > **Settings (Paramètres)** > **Security Posture (État de sécurité)**, et identifiez le contrôle que vous souhaitez exclure et sélectionnez-le (colonne **Exceptions**).

STEP 2 | Spécifiez les informations nécessaires pour **Créer une règle spécifique** pour votre chèque. Indiquez un nom, une raison et les conditions de votre exemption.

*La fonctionnalité **Security Check Exception (Exception de vérification de sécurité)** n'est actuellement applicable qu'aux alertes, et aux tableaux de bord des **Best Practices (Meilleures pratiques)** et des **Security Posture Insights (informations sur la posture de sécurité)**.*

STEP 3 | Facultatif Ajoutez un **numéro de ticket** ou une **description** pour votre exemption afin d'aider les autres à comprendre l'intention et l'historique de votre exemption.

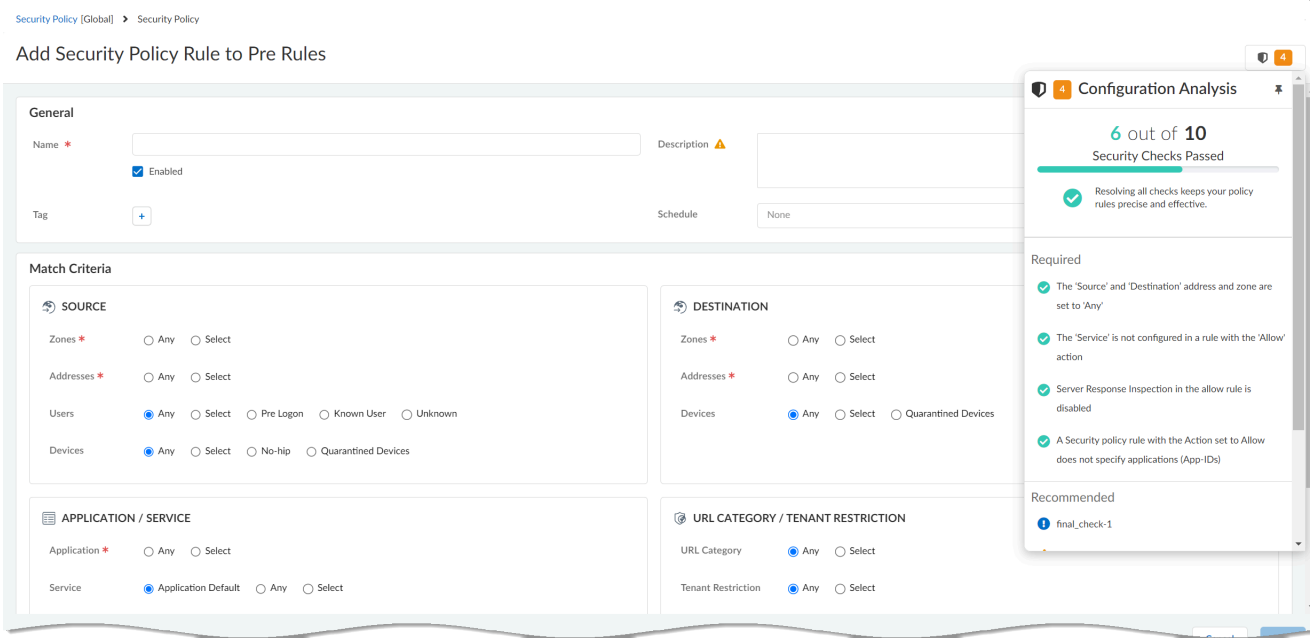
STEP 4 | **Save (Enregistrez)** votre exemption.

Vos contrôles au travail

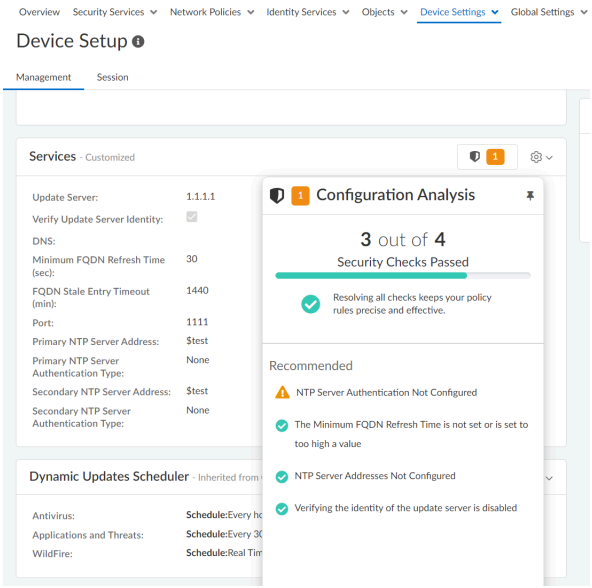
Les contrôles sur le terrain vous indiquent où votre configuration n'est pas conforme à une meilleure pratique ou à un contrôle personnalisé. Les contrôles fournissent des conseils sur les meilleures pratiques en ligne, de sorte que vous pouvez immédiatement prendre des mesures.

Vous pouvez également consulter et gérer les contrôles de sécurité où que vous soyez.

- Créez et gérez vos règles de politique – Les règles de politique de sécurité vous permettent d'appliquer des règles et de prendre des mesures, et peuvent être aussi générales ou spécifiques que nécessaire. (**Manage (Gestion)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Security Services (Services de sécurité)** > **Security Policy (Politique de sécurité)**)



- Périphériques de configuration : configurez un itinéraire de service, les paramètres de connexion, les services autorisés et les paramètres d'accès administratifs pour les interfaces de gestion et auxiliaires de vos pare-feu. (**Manage (Gestion)** > **Configuration** > **NGFW and Prisma Access (NGFW et Prisma Access)** > **Device Settings (Paramètres du périphérique)** > **Device Setup (Configuration du périphérique)**)



Si la configuration que vous essayez d'enregistrer ne répond pas à vos critères de réussite, vous aurez la possibilité de remédier au problème ou de passer outre* l'avertissement et d'enregistrer quand même vos modifications.

- **L'autorisation de passer outre est régie par les contrôles d'accès basés sur les rôles (RBAC) et doit être activée pour votre rôle afin que cette option apparaisse. Les actions relatives aux dérogations, aux contrôles personnalisés et aux exceptions sont consignées dans les journaux d'audit : **Incidents et alertes (Incidents et alertes)Log Viewer (Visionneuse de journaux)Audit (type de journal)**.*
- *Tout ce que vous faites avec les contrôles personnalisés, les dérogations et les exceptions est enregistré dans l'audit : **Incidents and Alerts (Incidents et alertes)** > **Log Viewer (Visionneuse de journaux)** > **Audit (type de journal)**.*

Gestion : Contrôle de l’accès

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ Au moins une de ces licences est nécessaire pour gérer votre configuration avec Strata Cloud Manager ; pour une gestion unifiée des NGFW et Prisma Access, vous aurez besoin des deux : ❑ licencePrisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro ❑ les crédits NGFW logiciels *(pour les NGFW logiciels de VM-Series*) → Les fonctionnalités et capacités disponibles pour vous dans Strata Cloud Manager dépendent des types de licences que vous utilisez.

Le contrôle d'accès basé sur les rôles (CABR) vous permet de définir les privilèges et les responsabilités des utilisateurs administratifs (administrateurs). Chaque administrateur doit avoir un compte utilisateur qui spécifie un rôle et une méthode d’authentification. Prisma AccessLa gestion du cloud permet de mettre en œuvre un RBAC personnalisé. Ce dernier vous permettra de gérer des rôles ou des autorisations spécifiques et d’attribuer des droits d’accès aux utilisateurs administratifs. Grâce à RBAC, vous pouvez gérer les utilisateurs et leur accès à diverses ressources au sein de la gestion du cloud.

*RBAC n’est pas pris en charge pour les menaces de sécurité SaaS en ligne et comportementales. Tous les onglets sous **Appli détectées** et **Menaces comportementales** sont visibles par tous les utilisateurs, quels que soient leurs rôles assignés.*

AUTRES RESSOURCES RBAC

- Qui peut utiliser les services communs ? Identité et accès : Géré dans le cloud Prisma Access
- Quel est le flux général pour les services communs : Identité et accès
- À propos des rôles et des autorisations par l’entremise des services communs

Rôle administrateur

Un utilisateur sur Prisma Access est une personne ayant reçu des privilèges d'administration. Un rôle définit le type d'accès accordé à l'administrateur sur le service. Lorsque vous attribuez un rôle, vous spécifiez le groupe d'autorisations et de comptes susceptibles d'être gérés par l'administrateur. Le hub dispose des groupes d'autorisations suivantes intégrés pour les administrateurs utilisant Prisma Access.

- **Administrateur d'appli** : a un accès complet à l'appli donnée, notamment toutes les instances ajoutées à l'appli à l'avenir. Les administrateurs d'appli peuvent attribuer des rôles aux instances d'appli. Ils peuvent également activer les instances d'appli spécifiques à cette appli.
- **Administrateur d'instance** : a un accès complet à l'instance d'appli pour laquelle ce rôle est attribué. L'administrateur de l'instance peut également faire d'autres utilisateurs des administrateurs de l'instance pour celle de l'appli. Si l'appli possède des rôles prédéfinis ou personnalisés, l'administrateur de l'instance peut attribuer ces rôles à d'autres utilisateurs.
- **Super lecteur** : peut afficher tous les éléments de configuration, les journaux et les paramètres. Les super lecteurs ne peuvent pas apporter de modifications à d'autres paramètres.
- **Admin. de l'audit** : peut afficher et gérer les journaux et les paramètres de journaux uniquement. Les Admins de l'audit ne peuvent pas apporter de modifications à d'autres paramètres.
- **Admin Crypto** : peut afficher les journaux et gérer les paramètres cryptographiques tels que IKE, IPSec, la gestion des clés principales et la configuration des certificats. Crypto Admins ne peut pas afficher ou modifier d'autres paramètres.
- **Admin de la sécurité** : peut afficher les journaux et gérer tous les paramètres, sauf les paramètres cryptographiques disponibles pour le rôle Crypto Admin.
- **Admin Sécurité Web** : peut afficher les éléments de configuration liés à la sécurité Web uniquement.
- **Data Loss Prevention Admin (Administrateur de la prévention des pertes de données - DLP)** : peut accéder aux paramètres DLP de l'entreprise, mais ne peut pas pousser les modifications de configuration à Prisma Access.
- **Admin de la sécurité de données** : peut accéder aux contrôles de sécurité DLP et SaaS de l'entreprise, mais ne peut pas envoyer de modifications de configuration àPrisma Access.
- **Admin SaaS** : peut accéder aux paramètres de sécurité SaaS, mais ne peut pas envoyer de modification de configuration à Prisma Access.

Contrôle d’accès personnalisé basé sur les rôles : Configuration

Voici comment utiliser un rôle prédéfini ou créer un rôle personnalisé, attribuer un rôle à un utilisateur et gérer la portée de l’utilisateur lorsque vous accédez Prisma Access à l’application.

STEP 1 | Ajouter un rôle personnalisé via les services communs

Si vous avez besoin d’un contrôle d’accès plus granulaire que les rôles prédéfinis ne le prévoient, vous pouvez ajouter des rôles personnalisés en vue de définir quelles autorisations sont appliquées pour vos utilisateurs. Similaires aux rôles prédéfinis, les rôles personnalisés sont un ensemble d’autorisations et de jeux d’autorisations. Contrairement aux rôles prédéfinis, chaque rôle personnalisé n’est attribuable qu’aux utilisateurs de la hiérarchie sous le groupe de services aux locataires (TSG) où il est défini. Cette disposition permet d’éviter tout conflit entre des rôles personnalisés portant le même nom et définis par des clients différents.

Si vous ajoutez un rôle personnalisé au niveau supérieur (niveau parent) de la hiérarchie, ce rôle est attribué aux locataires imbriqués en dessous afin que le locataire parent puisse gérer les locataires enfants.

STEP 2 | Ajouter un accès utilisateur via les services communs

Les services communs : Accès et identité vous permet d’ajouter un accès utilisateur à la plateforme ainsi qu’aux locataires que vous avez créés.

STEP 3 | Attribuer un rôle prédéfini à un utilisateur locataire ou à un compte de service via les services communs

Si vous avez déjà ajouté des utilisateurs et souhaitez ajouter des rôles supplémentaires, vous pouvez également attribuer un lot de rôles prédéfinis. Examinez des informations supplémentaires sur les rôles et autorisations.

STEP 4 | Créer une nouvelle portée dans l’ Prisma Access Interface utilisateur de gestion du cloud

Prisma Access Gestion du cloud vous permet (en tant qu’administrateur) d’attribuer une portée de gestion à un utilisateur de gestion du cloud (non-administrateur) pour associer des autorisations en fonction de portées telles que des dossiers et des extraits.

Les permissions sont des actions autorisées dans le système. Les autorisations représentent un ensemble spécifique d’appels à l’interface de programmation d’applications (API) que vous utilisez pour lire, écrire et supprimer des objets dans les systèmes. Toutes les permissions sont regroupées en rôles.

Gestion : Gestion de la portée

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ Au moins une de ces licences est nécessaire pour gérer votre configuration avec Strata Cloud Manager ; pour une gestion unifiée des NGFW et Prisma Access, vous aurez besoin des deux : ❑ licence Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités disponibles Strata Cloud Manager dépendent des types de licences que vous utilisez.

Configurer la gestion de l'étendue pour appliquer un contrôle d'accès personnalisé basé sur les rôles. Cela vous permet de spécifier les Strata Cloud Manager administrateurs qui peuvent accéder et modifier des dossiers spécifiques, des pare-feu, Prisma Access des déploiements et configurations d'extraits. La définition de l'étendue de la gestion pour vos administrateurs cloud garantit qu'ils ne sont pas surprovisionnés et définit les privilèges d'accès en lecture et en écriture pour les dossiers, les pare-feu, Prisma Accessles déploiements et les configurations d'extraits sélectionnés. Les Services communs aux Plateformes multiples et rôles d'entreprise sont utilisés pour définir les privilèges d'accès en lecture et en écriture d'un Strata Cloud Manager administrateur.

La configuration de gestion de l'étendue est définie sur l'ensemble de votre Strata Cloud Manager locataire. La gestion de l'étendue ne peut pas être définie pour un dossier spécifique, Prisma Accessou l'étendue de configuration du pare-feu.

Seul un administrateur de gestion de cloud ou un superutilisateur peut créer un objet d'étendue. Le widget gestion de l'étendue n'est pas disponible pour les utilisateurs ayant d'autres rôles.

STEP 1 | Se connecter à Strata Cloud Manager

STEP 2 | Sélectionnez **Manage (Gestion)** > **Access Control (Contrôle d'accès)** > **Scope Management (Gestion de la portée)**.

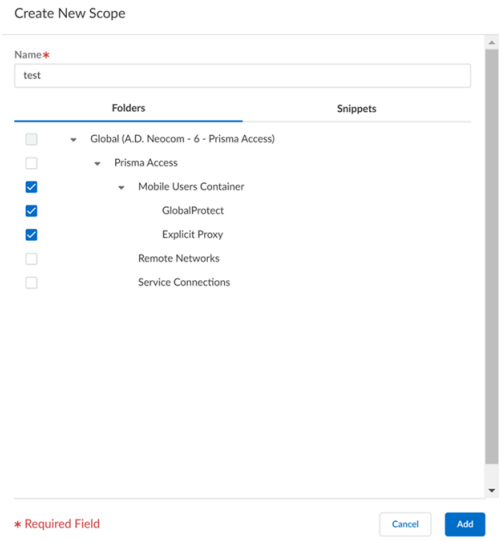
STEP 3 | **Créer une nouvelle étendue**

STEP 4 | Définir la configuration de la gestion de l’étendue.

Les configurations de la gestion de l’étendue sont étiquetées comme un `objet de l’étendue`.

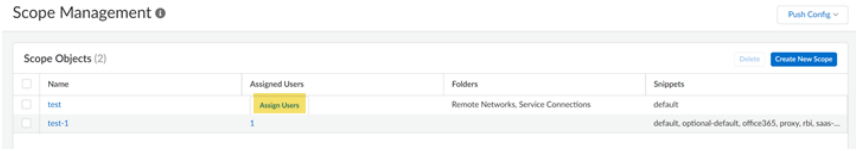
1. Saisissez un **Name (Nom)** descriptif.
2. Sélectionnez **Folders (Dossiers)** et vérifiez (activez) les dossiers, les pare-feu et Prisma Access déploiements que vous souhaitez inclure dans l’étendue.

   La sélection d’un pare-feu inclut également le dossier auquel le pare-feu sélectionné est associé dans la configuration de la gestion de l’étendue. Seul le dossier immédiatement associé est inclus, et non le dossier principal.
3. Sélectionnez **Snippets (Extraits)** et cochez (activez) les extraits que vous souhaitez inclure.
4. **Add (Ajouter)** l’objet de l’étendue.



STEP 5 | Appliquez la configuration de gestion de l'étendue aux Strata Cloud Manager administrateurs.

1. **Assign Users (Attribuer des utilisateurs)** à l'objet de l'étendue que vous avez créé à l'étape précédente.



2. Sélectionnez un **Role (Rôle)** pour l'Strata Cloud Manager administrateur. Par exemple, vous pouvez sélectionner MSP Superuser pour un utilisateur qui doit avoir accès à toutes les fonctions pour tous les locataires.

   Valeur par défaut : Aucune. Consultez les Services communs aux Plateformes multiples et rôles d'entreprise pour plus d'informations sur les privilèges d'accès en lecture et en écriture pour chaque rôle disponible.

   *Sélectionnez un adminStrata Cloud Manager spécifique et **un Rôle clair** pour supprimer le rôle Services communs actuellement attribué. Cela applique le rôle par défaut Aucun rôle à l'admin.*

3. Pour modifier une étendue existante afin d'en modifier le nom et d'ajouter ou de supprimer des dossiers, sélectionnez l'objet de la portée, modifiez-la si nécessaire, puis **Update (Mettez à jour)** la portée.
4. Pour modifier les utilisateurs affectés, pour ajouter d'autres utilisateurs ou pour modifier les utilisateurs, cliquez sur **Assigned Users (Utilisateurs assignés)** et modifiez-les au besoin, et **Close (Fermer)** La fenêtre.

Gestion : Restrictions IP

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW, notamment ceux financés par les crédits NGFW logiciels	❑ Au moins une de ces licences est nécessaire pour gérer votre configuration avec Strata Cloud Manager ; pour une gestion unifiée des NGFW et Prisma Access, vous aurez besoin des deux : ❑ licence Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro → Les fonctionnalités et capacités disponibles Strata Cloud Manager dépendent des types de licences que vous utilisez.

Spécifiez des adresses IP approuvées pour lesPrisma Access administrateurs de gestion du cloud. Seuls les administrateurs qui se connectent à partir de ces adresses IP sources (et qui s'authentifient avec succès) peuvent accéder à la Prisma Access gestion du cloud.

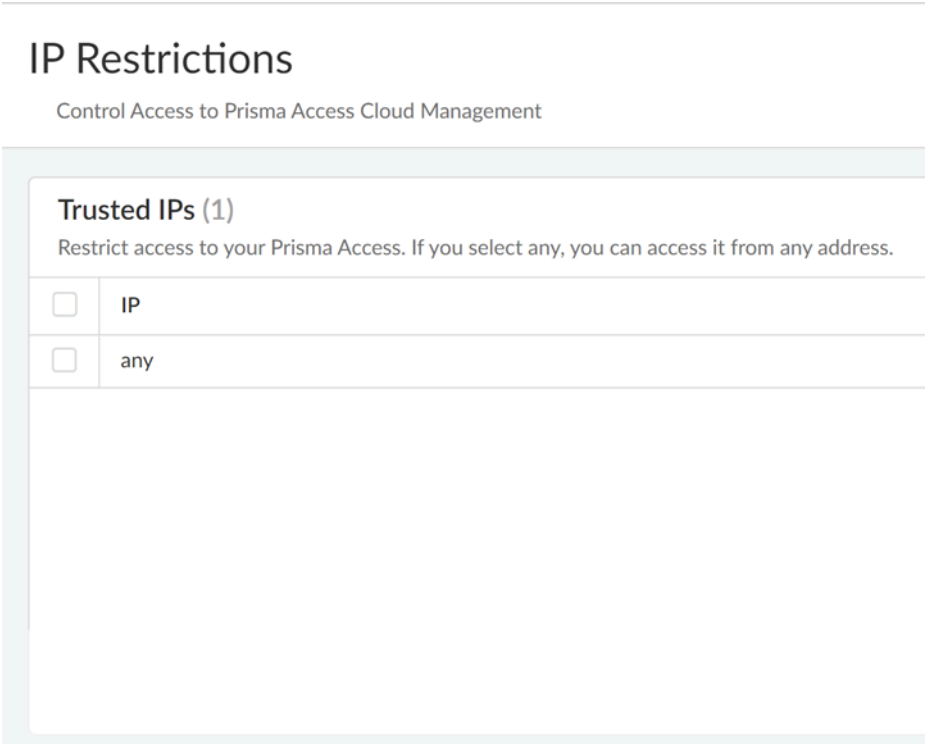
Les adresses IP doivent être des adresses publiques. Par défaut, aucune adresse approuvée n'est appliquée (la liste est définie sur **aucun**).

Pour commencer, accédez à **Gérer** > **les restrictions IP** > **du contrôle d'accès**.

Les adresses de sous-réseau ne sont pas prises en charge pour les restrictions IP. Les adresses IP et les plages d'adresses IP sont les seules à être prises en charge. Ne spécifiez aucun sous-réseau qui chevauche les adresses IP et sous-réseaux suivants, car Prisma Access réserve ces adresses IP et sous-réseaux à son usage interne :

- 169.254.169.253 et 169.254.169.254
- 100.64.0.0/10
- 169.254.201.0/24
- 169.254.202.0/24

Nous recommandons d'utiliser un groupe d'adresses IP conforme à la norme RFC 1918 et à la norme RFC 6598. Bien que l'utilisation d'adresses IP (publiques) non conformes à la norme RFC 1918 et conformes à la norme RFC 6598 soit possible, nous ne la recommandons pas en raison des conflits possibles avec l'espace public d'adresses IP sur l'internet.



Flux de travail : Strata Cloud Manager

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager) • Prisma SD-WAN	Une ou plusieurs de ces licences, selon le flux de travail : ❑ Licence AIOps for NGFW Premium ❑ Strata Logging Service est requise pour la journalisation ❑ Prisma Access ❑ Prisma SD-WAN ❑ Isolation du navigateur distant

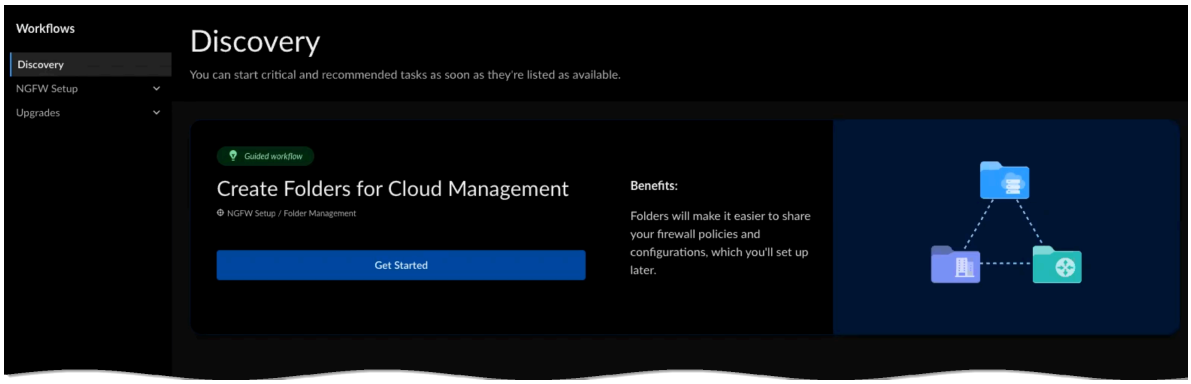
Lorsque vous accédez pour la première fois à vos flux de travail, le tableau de bord **Découverte** affiche les actions critiques et recommandées que vous pouvez entreprendre pour améliorer la posture de sécurité ou optimiser votre gestion de configuration, dès qu'elles sont à votre disposition. Continuez ici pour configurer et embarquer les NGFW et les utilisateurs mobiles et les réseaux distants Prisma Access, et planifier les mises à niveau logicielles pour les NGFW.

- Découvrir les tâches d'intégration
- Configurer Prisma Access
- Configurer les NGFW
- Configurer Prisma SD-WAN
- Mises à niveau logicielles (NGFW)
- Mises à niveau logicielles (Prisma Access)

Flux de travail : Découverte

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager) • Prisma SD-WAN	❑ Licence AIOps for NGFW Premium ou licence Prisma Access

La découverte est l'endroit où vous pouvez commencer les tâches critiques et recommandées dès qu'elles sont disponibles. Vous pouvez être guidé dans le déroulement des opérations ou accomplir des tâches par vous-même. Dans cette rubrique, vous apprendrez à utiliser le flux de travail guidé pour créer votre structure de dossiers et y affecter des périphériques, de manière simple et intuitive.



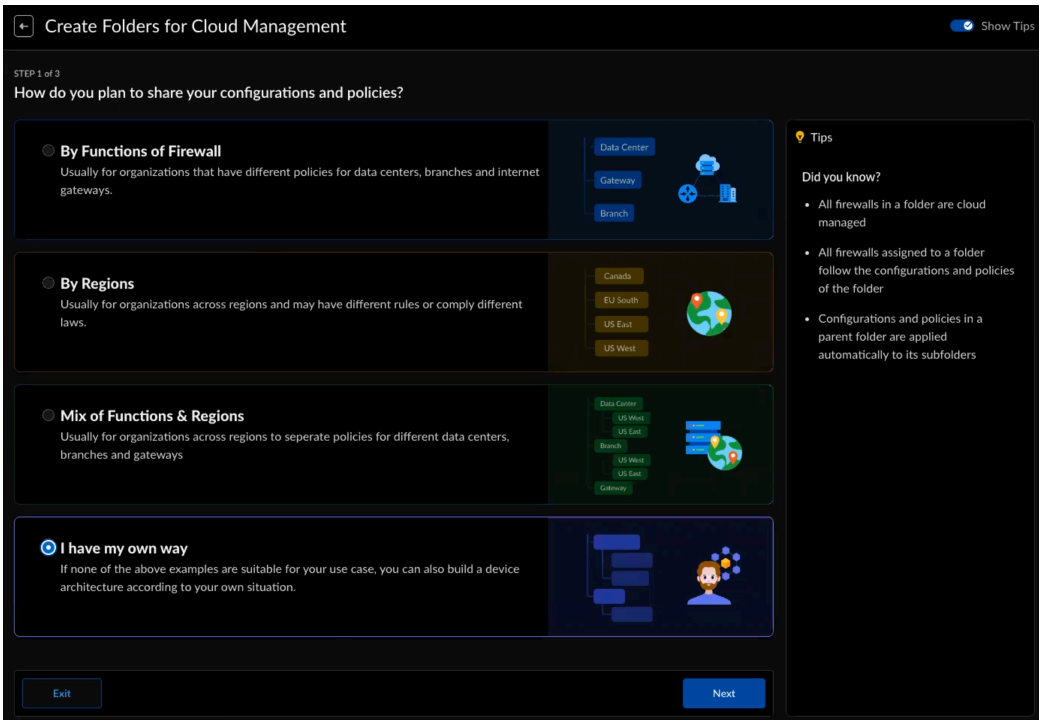
Suivez ces étapes pour créer des dossiers pour vos pare-feu :

STEP 1 | Accédez à **Workflows (Flux de travail)** > **Discovery (Découverte)** et sélectionnez **Get Started (Commencer)**.

STEP 2 | Sélectionnez le mode de partage des règles et des configurations de votre politique.

- **Par fonctions du pare-feu** : votre organisation a-t-elle des politiques différentes pour les centres de données, les succursales et les passerelles Internet ? C'est peut-être l'option qui vous convient.
- **Par région** : votre organisation couvre-t-elle des régions qui ont des règles différentes ou qui se conforment à des lois différentes ? Envisagez cette option.
- **Mélange de fonctions et régions** : votre organisation interrégionale souhaite-t-elle séparer les politiques pour différents centres de données, succursales et passerelles Internet ? Essayez cette option.
- **J'ai ma propre méthode** : si aucun des exemples ci-dessus ne convient à votre cas d'utilisation, vous pouvez également créer une architecture de périphérique en fonction de votre propre situation.

Pour cet exemple, nous allons choisir l'option **I have my own way (J'ai ma propre méthode)**.

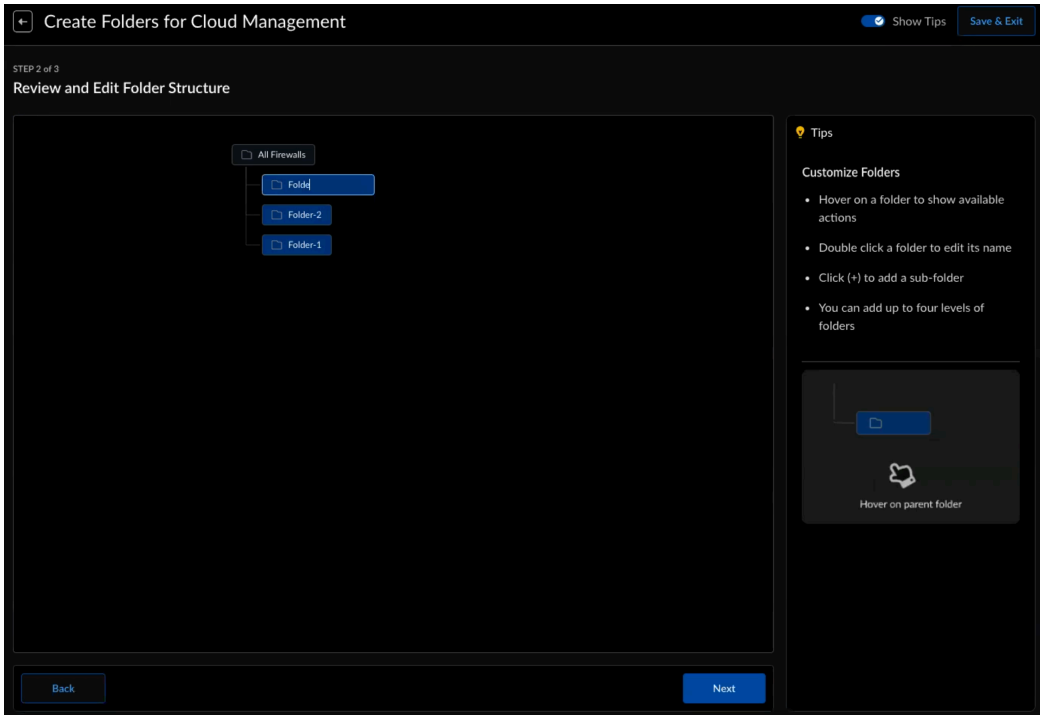


*Activez **Afficher les conseils** pour consulter les conseils d'aide qui vous aideront à prendre une décision éclairée.*

STEP 3 | Sélectionnez **Suivant** afin de construire votre structure de dossier.

STEP 4 | Utilisez les actions suivantes pour construire la structure de votre dossier en fonction du modèle que vous avez sélectionné à l'étape 1. Vous pouvez :

- **Add a new Folder (Ajouter un nouveau dossier)** : Survolez un dossier pour afficher l'option permettant d'ajouter un nouveau dossier. Cliquez sur , puis nommez votre nouveau dossier.
- **Delete Folder (Supprimer un dossier)** : Survolez un dossier pour afficher l'option de suppression du dossier. Sélectionnez pour supprimer le dossier.
- **Renommer le dossier** : double-cliquez sur un dossier pour taper un nouveau dossier. Appuyez sur la touche Entrée ou cliquez en dehors du champ de texte pour que votre nouveau nom prenne effet.
- **Expand or Collapse (Agrandir ou réduire)** les nœuds de dossiers qui ont des liens avec d'autres nœuds.

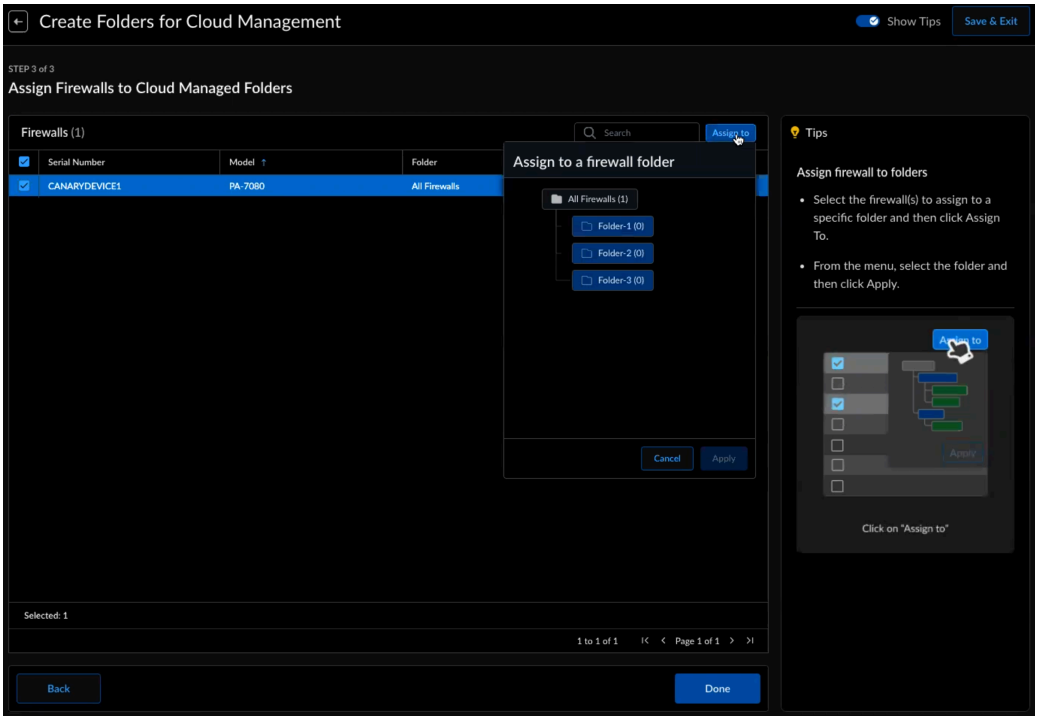


- *Les structures de dossiers peuvent avoir un maximum de quatre niveaux.*
- *Aucun dossier de premier niveau ne peut être supprimé ou renommé.*
- *Vérifiez les astuces pour obtenir des conseils sur certaines actions relatives aux dossiers.*
- *Nous enregistrerons votre travail, vous pouvez **Quitter** n'importe quand et revenir plus tard.*

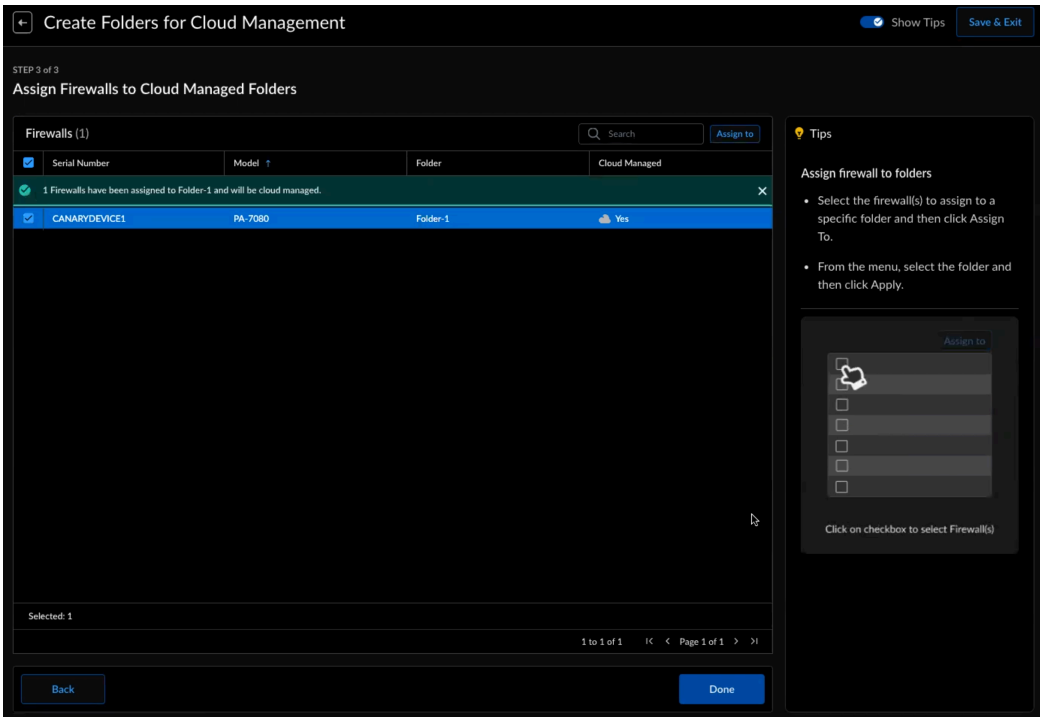
STEP 5 | Sélectionnez **Next (Suivant)** pour affecter vos pare-feux aux dossiers.

STEP 6 | Sélectionnez un ou plusieurs pare-feux dans cette liste.

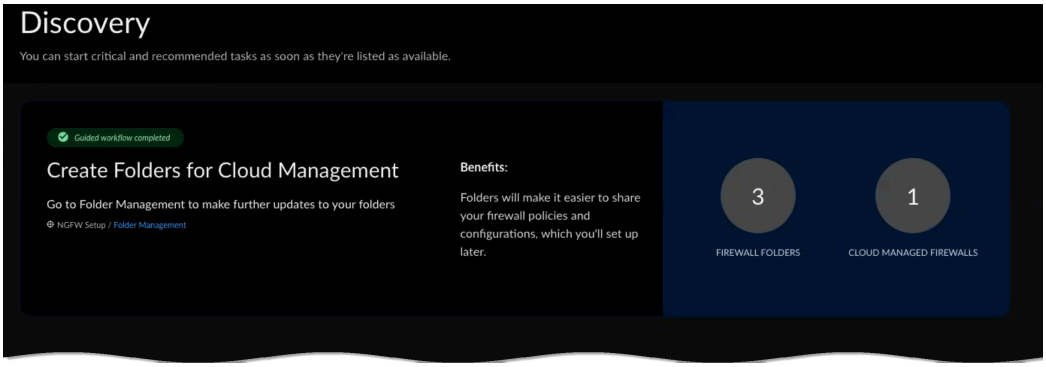
STEP 7 | Sélectionnez **Assign To (Affecter à)**, choisissez un dossier auquel vous souhaitez affecter vos pare-feux, puis sélectionnez **Apply (Appliquer)**. La gestion du cloud est activée pour les pare-feux affectés à un dossier **Cloud Managed (Géré dans le cloud)**.

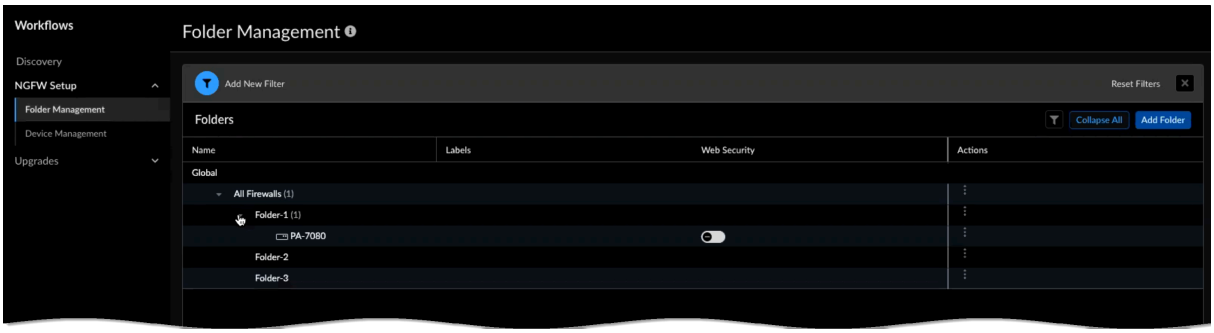


STEP 8 | Confirmez vos missions et sélectionnez **Done (Terminé)**.



Vous verrez les dossiers précédemment créés et les pare-feux que vous avez assignés sur la page principale de **Discovery (Découverte)**, ainsi que sous l'onglet **Configuration NGFW** > **(Folder Management) Gestion du dossier** .





Flux de travail : Configuration NGFW

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (Managed by Strata Cloud Manager)	❑ Une licence AIOps for NGFW Premium est requise pour la gestion du cloud pour les NGFW ❑ Une licence Strata Logging Service est requise pour la journalisation ❑ Si vous possédez une licence Prisma Access, vous pouvez utiliser **Folder Management (Gestion des dossiers)** pour afficher vos dossiers prédéfinis et activer Web Security pour un dossier

Dans le cadre de la configuration de vos NGFW pour la gestion du cloud, vous devrez impliquer vos pare-feu nouvelle génération à Strata Cloud Manager. L'intégration comprend la configuration de dossiers pour regrouper les pare-feu qui nécessitent des paramètres similaires. En savoir plus sur Flux de travail : Gestion des dossiers et utilisez la page **Device Management (Gestion des périphériques)** pour afficher les détails de tous les périphériques qui se trouvent dans votre hiérarchie de dossiers.

STEP 1 | Activez Strata Logging Service et AIOps pour les licences NGFW Premium.

La licence Strata Logging Service est requise pour la journalisation et la licence AIOps for NGFW Premium pour la gestion cloud de NGFW.

STEP 2 | Créez un ou plusieurs dossiers.

Les dossiers servent à regrouper logiquement vos pare-feu ou types de déploiement pour une gestion simplifiée de la configuration.

STEP 3 | Intégrer un pare-feu à Strata Cloud Manager.

Pour intégrer un pare-feu à Strata Cloud Manager, vous devez configurer les paramètres Panorama locaux sur le pare-feu et associer le pare-feu à votre locataire Strata Cloud Manager. Une fois intégré, vous pouvez continuer à configurer les paramètres généraux et de session du pare-feu.

STEP 4 | (HA uniquement) Configurez vos pare-feu gérés en configuration High Availability (haute disponibilité - HA) si nécessaire.

STEP 5 | Créez un ou plusieurs extraits.

Les extraits sont utilisés pour regrouper des objets de configuration qui sont appliqués à des dossiers, des déploiements ou des pare-feu individuels. Cela facilite et accélère le processus d'intégration en vous permettant de standardiser les configurations de base communes qui peuvent être rapidement appliquées et poussées.

STEP 6 | Créez vos objets de configuration.

Les objets de configuration sont des blocs de construction pour vos configurations de règles réseau et de politique.

STEP 7 | Créez et configurez les règles réseau et de politique.

STEP 8 | Push (Transmettez) les modifications de votre configuration de Strata Cloud Manager à vos pare-feu gérés.

Flux de travail : Gestion des périphériques

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• NGFW (Managed by Strata Cloud Manager)	❑ AIOps for NGFW Premium

Un NGFW Palo Alto Networks géré par Strata Cloud Manager est considéré comme un *Appareil géré dans le cloud*. Strata Cloud Manager peut gérer les pare-feu exécutant PAN-OS 10.2.3 ou une version plus récente.

Pour plus d'informations sur les prérequis pour Strata Cloud Manager, cliquez ici.

Avec le tableau de bord **Device Management (Gestion des périphériques) (Workflows (Flux de travail) > NGFW Setup (Configuration NGFW) > Device Management (Gestion des périphériques)),** vous pouvez consulter les détails importants sur les appareils et les versions de tous vos appareils gérés et sélectionner les appareils à déplacer vers la gestion du cloud.

Voir tous les détails des NGFW gérés dans le cloud

L'onglet **Cloud Managed Devices (Appareils gérés par le cloud) (Workflows (Flux de travail) > NGFW Setup (Configuration NGFW) > Device Management (Gestion des périphériques) > Cloud Managed Devices (Appareils gérés par le cloud))** affiche tous vos pare-feu intégrés SCM, les dossiers auxquels ils sont affectés et des détails importants les concernant.

Informations sur le périphérique	Description
Nom	Le nom du NGFW et le(s) dossier(s) sous lequel (lesquels) il est organisé.
Étiquettes	Toutes les étiquettes attachées au NGFW.
État de la synchronisation de la configuration	L'état de synchronisation du NGFW : • Synchronisé • Désynchronisé
État HA	L'état HA du NGFW intégré : • **Active (Actif)** - État opérationnel de gestion du trafic normal.

Informations sur le périphérique	Description
	• **Passive (Passif)**- État de sauvegarde normal. • **Initiating (En cours d'initialisation)** - Le pare-feu est dans cet état pendant 60 secondes maximum après le démarrage. • **Non-functional (Non fonctionnel)** - État d'erreur. • **Suspended (Suspendu)** - Un administrateur a désactivé le pare-feu. • **Tentative (Provisoire)** - Pour un événement de surveillance des liaisons ou des chemins dans une configuration active/active.
Numéro de série	Le numéro de série du NGFW intégré.
Modèle	Le numéro de modèle du NGFW intégré.
Type	Le type de NGFW intégré : • VM • PA
Adresse	L'adresse IP du NGFW intégré.
Licence	Les informations de licence du NGFW intégré • Assorti • Mal assorti
Version du logiciel | Appli et menace | Antivirus | Filtrage des URL	Affiche les versions logicielle et du contenu installées actuellement sur le pare-feu. Pour plus de détails, voir Mises à jour logicielles ou de contenu du pare-feu.
Dictionnaire des appareils	Un fichier à importer pour les pare-feu. Le fichier dictionnaire fournit le Strata Cloud Manager et l'administrateur de pare-feu avec une liste d'attributs de périphérique à sélectionner lors de l'importation des règles de politique de sécurité recommandées.
Actions	Les actions du pare-feu intégré : • Récupérer les informations de licence • Redémarrer • Modifier le mode de routage • Gestion de la configuration locale • Forcer l'amorçage

Supprimer un NGFW des appareils gérés dans le cloud

L'onglet **Available Devices (Appareils disponibles)** affiche tous vos NGFW disponibles pour être intégrés à SCM et les NGFW déjà gérés par Strata Cloud Manager.

Pour plus d'informations sur le processus d'intégration pour Strata Cloud Manager, cliquez ici.

Vous pouvez utiliser l'onglet des périphériques disponibles pour déplacer des appareils vers et depuis Strata Cloud Manager.

STEP 1 | Connectez-vous à Strata Cloud Manager.

STEP 2 | Sélectionnez **Workflows (Flux de travail)** > **NGFW Setup (Configuration NGFW)** > **Device Management (Gestion des périphériques)** > **Available Devices (Périphériques disponibles)**.

1. Sélectionnez **Back to Available Devices (Retour aux périphériques disponibles)** pour déplacer un pare-feu hors de Strata Cloud Manager.

Restaurer l'instantané de la version de configuration locale sur le pare-feu

Vous pouvez restaurer n'importe quelle version et télécharger les détails de configuration au format XML.

STEP 1 | Connectez-vous à Strata Cloud Manager.

STEP 2 | Sélectionnez **Workflows (Flux de travail)** > **NGFW Setup (Configuration NGFW)** > **Device Management (Gestion des périphériques)**, puis sélectionnez **Local Configuration Management (Gestion de la configuration locale)** dans **Actions**.

STEP 3 | **Load (Chargez)** la version pour restaurer la configuration locale.

STEP 4 | Cliquez sur **Yes (Oui)** pour remplacer la configuration locale sur le pare-feu par la version de configuration. Une nouvelle tâche de validation est créée.

Vous pouvez utiliser la vue **Jobs (Tâches)** pour résoudre les opérations ayant échoué, examiner les avertissements associés aux validations terminées ou annuler les validations en attente.

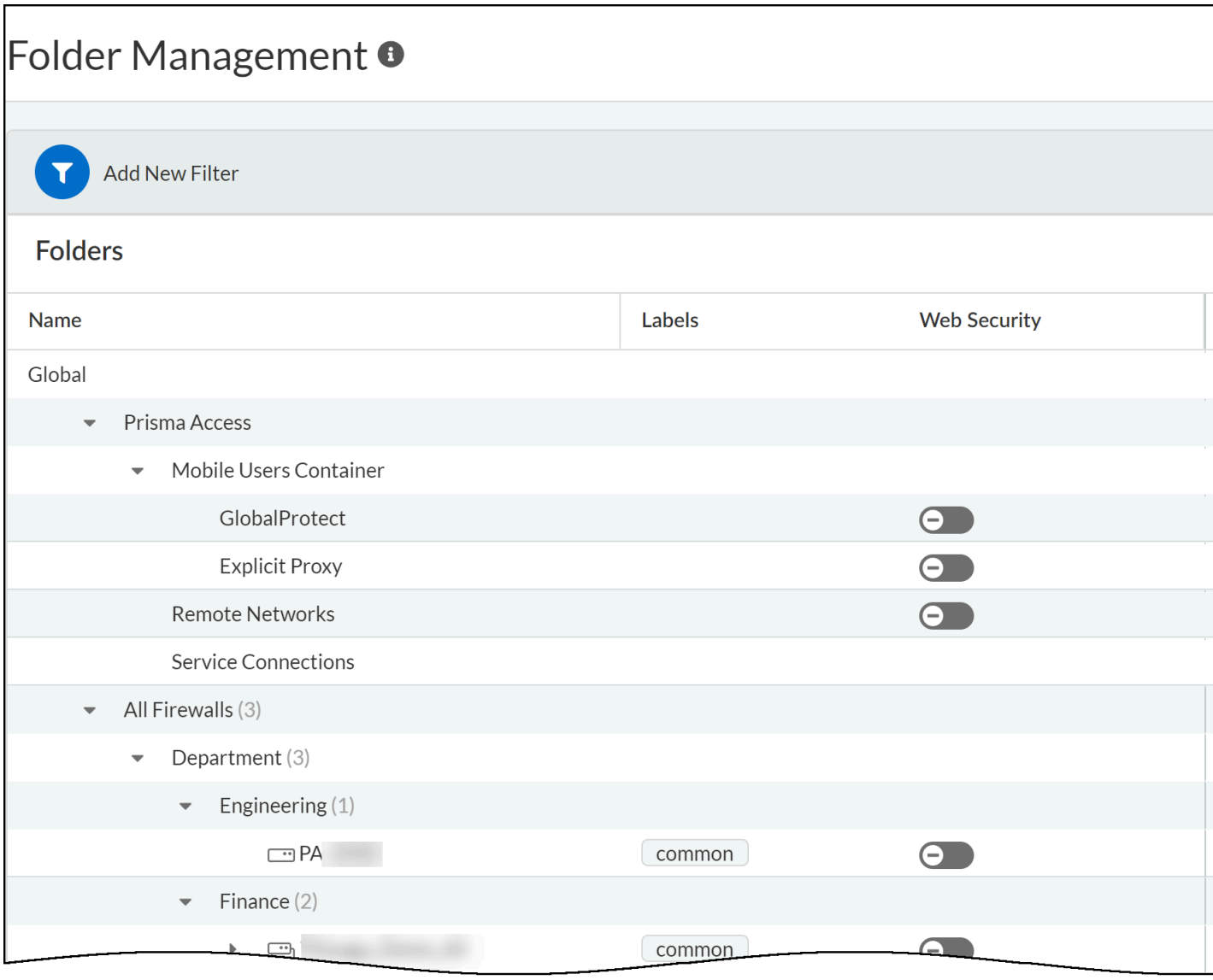
STEP 5 | **Download (Téléchargez)** la vue Détails de configuration pour la version sélectionnée.

Flux de travail : Gestion des dossiers

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager)	☐ Licence AIOps for NGFW Premium ☐ Licence Prisma Access

Les dossiers sont utilisés pour regrouper logiquement vos pare-feux ou types de déploiement (utilisateurs mobiles Prisma Access, réseaux distants ou connexions de service) afin de simplifier la gestion de la configuration. Vous pouvez créer un dossier contenant plusieurs dossiers imbriqués afin de regrouper les pare-feu et les déploiements nécessitant des configurations similaires. Les dossiers déjà imbriqués peuvent également contenir plusieurs dossiers imbriqués.

Les dossiers pour Prisma Access et vos NGFW sont séparés ; vous ne pouvez pas regrouper les NGFW dans un dossier avec des déploiements Prisma Access. Cependant, vous pouvez facilement appliquer des paramètres partagés globalement dans tous les dossiers ou utiliser Gestion : Extraits pour appliquer facilement des paramètres standard et des exigences de politique dans plusieurs dossiers.

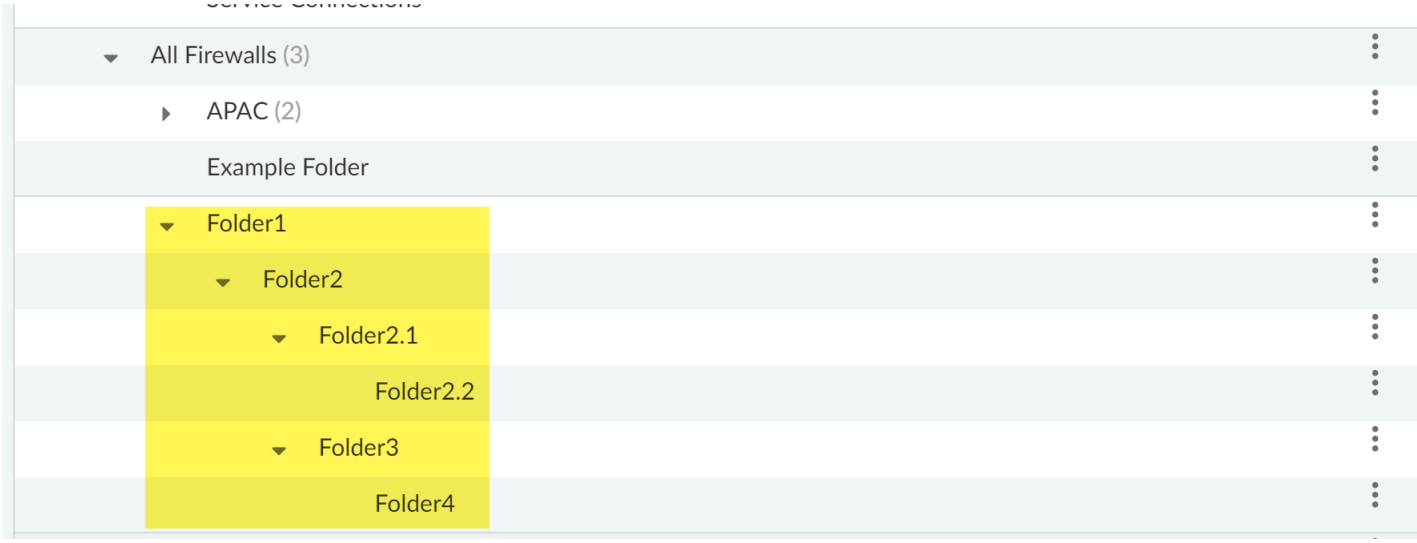


- NGFW
- Prisma Access

Gestion des dossiers (NGFW)

Afin de faciliter la gestion des dossiers et des pare-feux, vous pouvez appliquer des étiquettes afin de filtrer et de cibler des groupes spécifiques de pare-feux en vue de modifier leur configuration. De plus, chaque dossier affiche la version du logiciel actuellement installée, les versions de publication de contenu dynamique et la version de l'application GlobalProtect des pare-feux associés au dossier.

Pour les dossiers de pare-feux, Strata Cloud Manager prend en charge jusqu'à quatre dossiers imbriqués dans une hiérarchie de dossiers donnée, avec le dossier par défaut `Tous les pare-feux` étant toujours le niveau le plus élevé de toute hiérarchie de dossiers. Par exemple, tenez compte de ce qui suit lorsque vous concevez la hiérarchie de vos dossiers. Dans l'exemple ci-dessous `Dossier1`, `Dossier2`, `Dossier3` et `Dossier4` sont imbriqués sous le dossier `Tous les pare-feux` et vous ne pouvez pas ajouter de dossiers supplémentaires à cette hiérarchie de dossiers particulière. De plus `Dossier2.1` et `Dossier2.2` sont imbriqués sous `Dossier2` et vous ne pouvez pas non plus ajouter de dossiers supplémentaires.



Créer un dossier

Créez un dossier pour regrouper logiquement vos pare-feux afin de simplifier la gestion de la configuration. Vous pouvez créer un dossier sous la commande `Pare-feux` ou sous un autre dossier existant.

STEP 1 | Se connecter à Strata Cloud Manager.

STEP 2 | Choisissez **Workflows (Flux de travail)** > **NGFW Setup (Configuration du NGFW)** > **Folder Management (Gestion des dossiers)** et **Add Folder (Ajouter un dossier)**.

STEP 3 | Attribuer au dossier un **Nom descriptif**.

STEP 4 | (Facultatif) Entrez une **Description (Description)** pour le dossier.

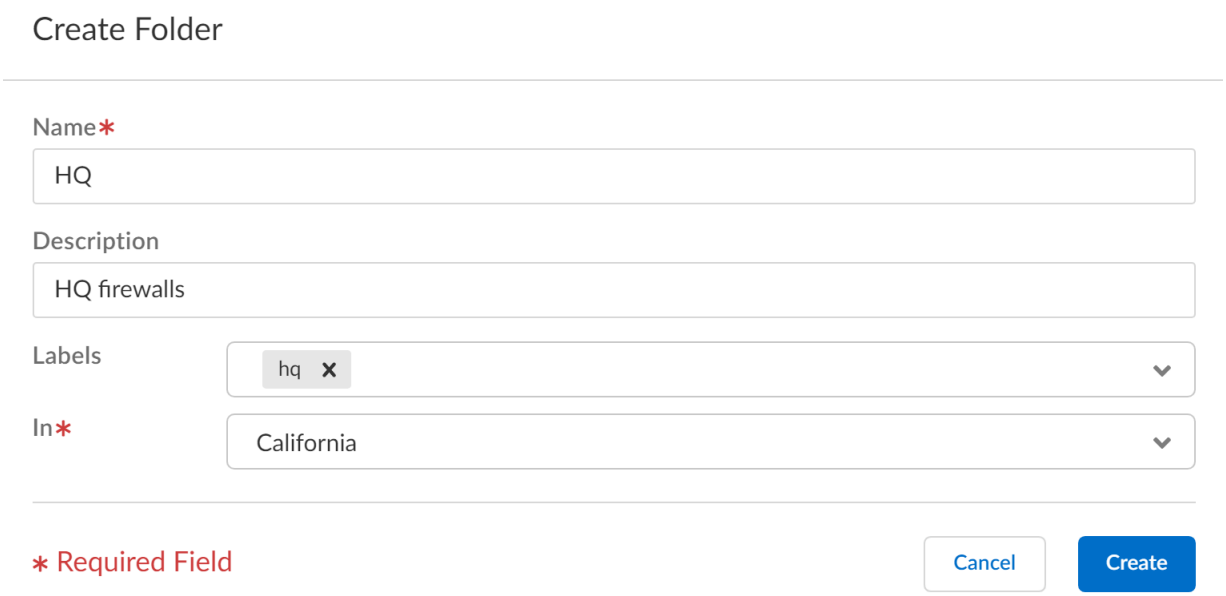
STEP 5 | (Facultatif) Attribuez un ou plusieurs **Étiquettes**.

Vous pouvez sélectionner une étiquette existante ou en créer une nouvelle en tapant l'étiquette que vous souhaitez créer.

STEP 6 | Spécifiez l'emplacement de création du dossier **In (Dans)**.

Sélectionnez **All Firewalls (Tous les pare-feux)** ou sélectionner un dossier existant pour y imbriquer le dossier.

STEP 7 | **Create (Créer)** le dossier.

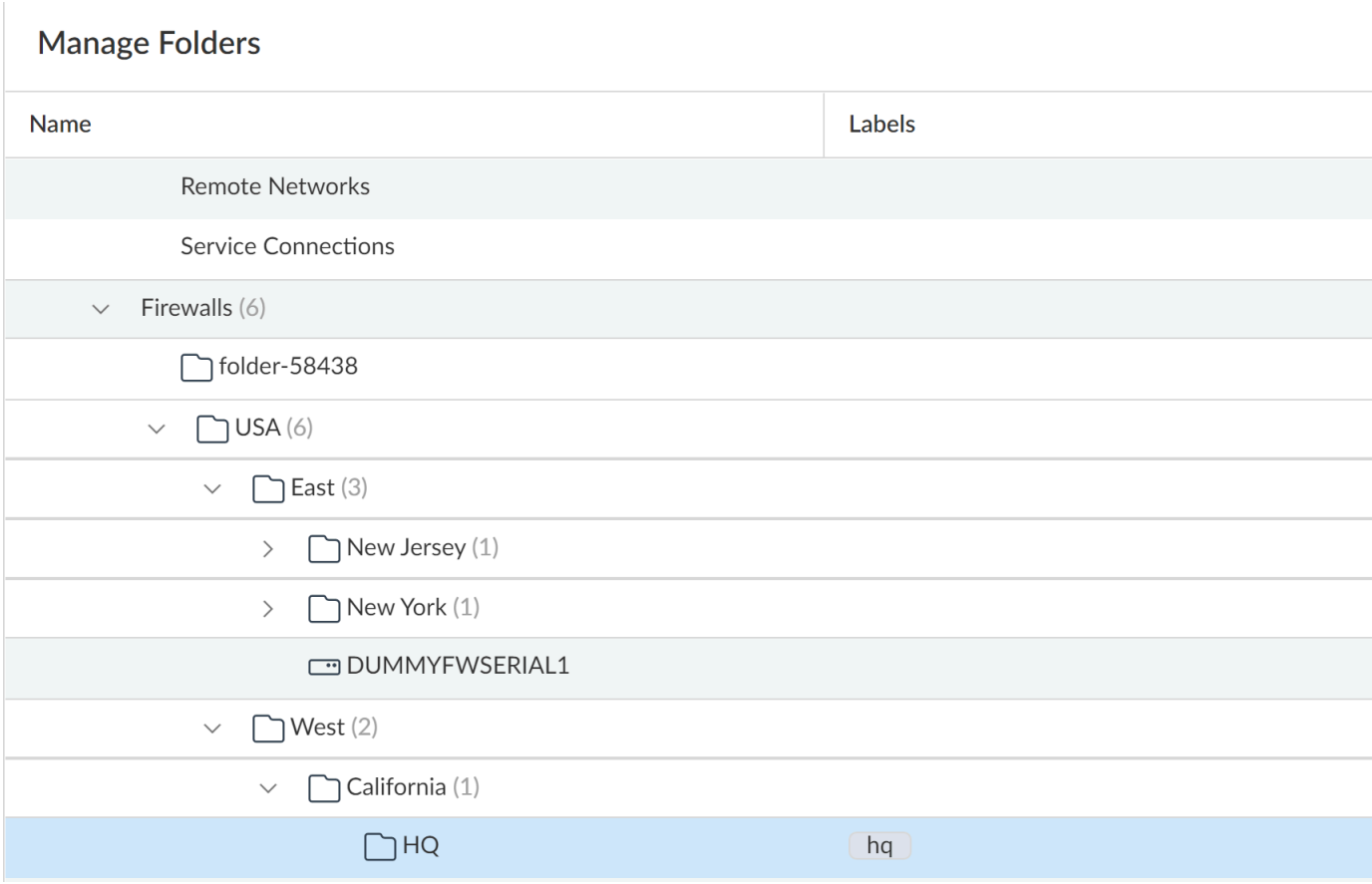


Modifier un dossier

Il est possible de modifier un dossier existant pour en éditer le nom et la description, et pour ajouter ou modifier les étiquettes. De plus, vous pouvez déplacer ou supprimer le dossier selon vos besoins.

STEP 1 | Se connecter à Strata Cloud Manager.

STEP 2 | Choisir **Workflows (Flux de travail)** > **NGFW Setup (Configuration du NGFW)** > **Folder Management (Gestion des dossiers)** et développez le menu Actions.



STEP 3 | Modifiez le dossier si nécessaire.

- **Modifier** le dossier
  1. Modifier le dossier **Name (Nom)**.
  2. (Facultatif) modifier le dossier **Description (Description)**.
  3. Sélectionner ou créer **Labels (Étiquettes)**.

     Vous pouvez attribuer des étiquettes complètement différentes au dossier ou ajouter des étiquettes supplémentaires.
  4. **Save (Enregistrer)**.
- **Move (Déplacer)** le dossier et sélectionnez la **Destination**.

Vous pouvez déplacer un dossier de la manière suivante.

- Il est possible de déplacer un dossier pour l'imbriquer sous un autre dossier.
- Vous pouvez déplacer un dossier imbriqué sous le dossier `Pare-feu`.
- Vous pouvez déplacer un dossier imbriqué d'un dossier à un autre.

Move (Déplacer) le dossier après avoir sélectionné la destination du dossier.

- **Delete Folder (Supprimer un dossier)** et cliquez sur **OK (D'ACCORD)** pour confirmer.

Vous ne pouvez supprimer qu'un dossier auquel aucun pare-feu n'est associé et qui n'est pas imbriqué en dessous.

Gestion des dossiers (Prisma Access)

Les dossiers Prisma Access sont prédéfinis ; vous pouvez les utiliser pour spécifier l'étendue de la configuration et vous assurer que les types de déploiement Prisma Access (utilisateurs mobiles, réseaux distants et connexions de service) reçoivent tous les paramètres globaux, puis les paramètres requis ou spécifiques à chaque type.

Toutes les configurations définies dans un dossier sont héritées de tous les dossiers imbriqués dans cette hiérarchie de dossiers. Par exemple, vous pouvez configurer des paramètres communs à GlobalProtect, Explicit Proxy, Remote Networks et Service Connections sous le dossier **Prisma Access**. De même, vous pouvez configurer des paramètres communs à GlobalProtect et Proxy explicite sous la commande **Conteneur d'utilisateurs mobiles** et ainsi de suite.

Vous ne pouvez pas modifier la hiérarchie des dossiers pour Prisma Access.

Au niveau du dossier, vous pouvez également activer sécurité Web pour le déploiement d'un utilisateur mobile, d'un réseau distant ou d'une connexion de service Prisma Access.

Flux de travail : Configuration Prisma SD-WAN

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma SD-WAN	❑ Licence Prisma SD-WAN

Vous pouvez configurer des sites de succursales, des sites de centres de données et des périphériques ION dans Prisma SD-WAN en utilisant Strata Cloud Manager.

Sélectionnez **Workflows (Flux de travail)** > **Prisma SD-WAN Setup (Configuration)**.

Vous pouvez configurer des flux de travail pour :

- Sites de succursales

  Configurez des sites de succursales dans votre réseau à l'aide de l'onglet **Sites de succursales**. Une entreprise peut avoir une ou plusieurs succursales au sein d'un réseau. Lorsque vous créez une succursale, vous pouvez sélectionner un domaine par défaut et un ensemble de règles de politique et configurer les réseaux WAN, les catégories de circuits, les étiquettes de circuits et les spécifications de circuits.

- Centres de données

  Configurez des sites de centre de données sur votre réseau à l'aide de l'onglet **Centres de données**. Les sites de centres de données sont connectés à des sites de succursales et vous pouvez héberger des applications et des services d'entreprise dans un centre de données.

- Périphériques

  Configurez les périphériques ION sur votre réseau à l'aide de l'onglet **Périphériques**. Les périphériques ION peuvent être déployés sur un site de succursale ou sur un site de centre de données. Ils sont disponibles sous des formes matérielles et logicielles qui répondent aux besoins de n'importe quel emplacement et de n'importe quel scénario de déploiement. Vous devez connecter, revendiquer, attribuer et configurer les périphériques ION pour vos sites de succursales et de centres de données.

Flux de travail : Configuration Prisma Access

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	☐ Licence Prisma Access

Sélectionnez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration)** pour commencer à configurer votre Prisma Access.

- Configurez l'infrastructure de service pour permettre la communication entre les emplacements de votre réseau distant, les utilisateurs mobiles et le siège social ou les centres de données que vous prévoyez de connecter à Prisma Access via des connexions aux services. Une connexion au service fournit la connectivité au centre de données.
- Intégrez les utilisateurs mobiles et déterminez comment vous les connectez à Prisma Access.
- Intégrez les réseaux distants pour sécuriser les emplacements réseau distants, tels que les succursales, et les utilisateurs de ces succursales. Un pare-feu nouvelle génération ou un périphérique tiers conforme à IPSec, y compris SD-WAN, qui peut établir un tunnel IPSec vers le service est requis sur le site distant.
- Ajoutez des connexions aux services pour permettre aux utilisateurs mobiles et aux utilisateurs sur vos réseaux de succursale d'accéder aux ressources présentes dans votre siège (QG) ou votre centre de données (DC). Outre l'accès aux ressources de l'entreprise, les connexions de service permettent à vos utilisateurs mobiles de se rendre dans les succursales.

Flux de travail : Prisma Access

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	☐ Licence Prisma Access

Avant de pouvoir utiliser Prisma Access pour sécuriser vos réseaux distants et vos utilisateurs mobiles, vous devez configurer un sous-réseau d'infrastructure.

Prisma Access utilise le sous-réseau pour créer le réseau principal pour la communication entre vos réseaux de succursales, les utilisateurs mobiles et l'infrastructure de sécurité Prisma Access, ainsi qu'avec les réseaux du siège social (QG) et des centres de données que vous prévoyez de connecter à Prisma Access via des connexions aux services. Si vous utilisez le routage dynamique pour vos réseaux distants ou vos connexions de service, vous devez également configurer un numéro d'AS privé BGP conforme au RFC 6696.

Utilisez les recommandations et exigences suivantes lorsque vous ajoutez un sous-réseau d'infrastructure pour Prisma Access.

- Utilisez un sous-réseau conforme au RFC 1918. Bien que Prisma Access prend en charge l'utilisation d'adresses IP (publiques) non conformes au RFC 1918, elle n'est pas recommandée en raison de conflits possibles avec l'espace d'adressage IP public Internet.

- Ne spécifiez aucun sous-réseau qui chevauche 169.254.169.253, 169.254.169.254 et la plage de sous-réseaux 100.64.0.0/10, car Prisma Access réserve ces adresses IP et sous-réseaux à son usage interne. Ce sous-réseau est une extension à votre réseau existant et ne peut donc pas se chevaucher avec les sous-réseaux IP que vous utilisez au sein de votre réseau d'entreprise ou avec les pools d'adresses IP que vous attribuez pour les Prisma Access pour les utilisateurs ou les Prisma Access pour les réseaux. Étant donné que l'infrastructure de service nécessite un grand nombre d'adresses IP, vous devez désigner un sous-réseau /24 (par exemple, 172.16.55.0/24).
- Entrez un sous-réseau Infrastructure que Prisma Access peut utiliser pour assurer la communication entre vos emplacements de réseau distant, les utilisateurs mobiles et le siège social ou les centres de données que vous prévoyez de connecter à Prisma Access via des connexions aux services. Utilisez un sous-réseau conforme au RFC 1918 pour le sous-réseau d'infrastructure.

Référez-vous à Prisma Access Configuration pour plus d'informations.

Configurer le DNS de l'infrastructure

Prisma Access vous permet de spécifier des serveurs DNS (Domain Name System) pour résoudre à la fois les domaines internes à votre organisation et les domaines externes. Prisma Access mandate la requête DNS en fonction de la configuration de vos serveurs DNS.

La configuration de l'infrastructure DNS vous donnera accès à des services sur votre réseau d'entreprise, tels que des serveurs LDAP et DNS, en particulier si vous prévoyez de configurer des connexions de service pour fournir un accès à ce type de ressources au siège ou dans les centres de données. Les requêtes DNS pour les domaines de la liste de domaines interne sont envoyées à vos serveurs DNS locaux pour s'assurer que les ressources sont disponibles pour les utilisateurs Prisma Access distants du réseau et les utilisateurs mobiles.

Cela va configurer des listes de domaines internes qui s'appliquent à tout le trafic. Si vous préférez, vous pouvez consulter le Guide de l'admin pour voir comment créer des listes de domaines internes qui s'appliquent uniquement à des déploiements d'utilisateurs mobiles spécifiques ou à des sites de réseau distant.

Les avantages de la configuration DNS pour l'infrastructure sont :

- Activer Prisma Access pour résoudre vos domaines internes
- Configurer DNS pour résoudre les domaines internes et externes
- Utilisez un caractère générique (*) avant les domaines de la liste de domaines, par exemple, *.acme.local ou *.acme.com

Reportez-vous à la section DNS pour Prisma Access pour plus d'informations.

Flux de travail : Utilisateurs mobiles

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licence Prisma Access ❑ Licence Strata Logging Service

Avant de configurer les utilisateurs mobiles, assurez-vous de disposer des licences requises (licence Prisma Access pour les utilisateurs mobiles et licence Strata Logging Service avec espace de stockage pare-feu approprié). Si les utilisateurs mobiles se connectent à d'autres réseaux connectés, vous aurez besoin de la licence ZTNA (Zero Trust Network Access) ou Enterprise Edition Prisma Access qui fournira le nœud d'accès d'entreprise (CAN) nécessaire pour vous connecter.

Vous allez préalablement choisir votre type de connexion, ou vous pouvez utiliser à la fois GlobalProtect, proxy explicite, ou les deux. Pour les deux types de connexion, quelques paramètres sont requis. Vous devez les définir initialement pour permettre à Prisma Access d'approvisionner l'environnement de vos utilisateurs mobiles.

1. Se connecter à Prisma Access.

   Déterminez comment les utilisateurs mobiles de l'emplacement que vous configurez doivent se connecter à Prisma Access. Vous pouvez diviser votre licence d'utilisateur mobile entre GlobalProtect et les connexions proxy explicites ; certains utilisateurs peuvent se connecter via GlobalProtect et d'autres via proxy explicite.

   L'application GlobalProtect installée sur les périphériques des utilisateurs mobiles envoie le trafic à Prisma Access.
2. Configurer l'infrastructure.

   Configurez les paramètres d'infrastructure de base, puis configurez les paramètres d'infrastructure spécifiques à votre type de connexion (GlobalProtect ou proxy explicite).

   Un fichier de configuration automatique du proxy (PAC) sur les périphériques des utilisateurs mobiles redirige le trafic du navigateur vers Prisma Access.
3. Choisissez l'emplacement de Prisma Access.

   La carte affiche les régions globales où vous pouvez déployer des Prisma Access pour les utilisateurs : Amérique du Nord, Amérique du Sud, Europe, Afrique, Moyen-Orient, Asie, Japon et ANZ (Australie et Nouvelle-Zélande). En outre, Prisma Access fournit plusieurs emplacements dans chaque région pour s'assurer que vos utilisateurs peuvent se connecter à un emplacement qui offre une expérience utilisateur adaptée à la région des utilisateurs. Pour obtenir les meilleures performances, sélectionnez Tout. Sinon, sélectionnez les emplacements spécifiques dans chaque région sélectionnée où vos utilisateurs auront besoin d'accès. En limitant votre déploiement à une seule région, vous pouvez avoir un contrôle plus granulaire sur vos régions déployées et exclure les régions requises par votre politique ou les règles de l'industrie.
4. Ajoutez les emplacements de Prisma Access.

   Configurez les paramètres pour ajouter les emplacements de Prisma Access que vous souhaitez pour soutenir vos utilisateurs.
5. Authentifiez les utilisateurs mobiles.

   Configurez l'authentification utilisateur de sorte que seuls les utilisateurs légitimes aient accès à vos services et applications. Pour tester votre configuration, vous pouvez ajouter des utilisateurs que Prisma Access authentifie localement, ou vous pouvez passer directement à la configuration de l'authentification au niveau de l'entreprise.

Après avoir poussé votre configuration initiale à Prisma Access, Prisma Access commence à approvisionner votre environnement utilisateur mobile. Cela peut prendre jusqu'à 15 minutes. Lorsque vos emplacements d'utilisateurs mobiles sont opérationnels, vous pouvez les vérifier sur

la page de configuration des utilisateurs mobiles, la page Présentation sommaire et dans Prisma Access Informations.

Référez-vous à Prisma Access Utilisateurs mobiles pour plus d'informations.

Flux de travail : Réseaux distants

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	Licence Prisma Access

Alors que vous vous préparez à connecter des réseaux distants à Prisma Access, vous devrez savoir combien de sites vous allez intégrer. Ces informations vous aideront à déterminer les exigences de connectivité, telles que la manière d'acheminer le trafic via Prisma Access. Lorsque vous planifiez votre déploiement de réseau à distance, vous devez savoir quelles applications passeront par Prisma Access afin de configurer de manière appropriée les meilleures règles de politique de sécurité. Il est tout aussi important de définir la configuration de votre profil de menace. De plus, vous devez envisager d'appliquer une analyse cohérente des menaces, des URL et des WildFire à toutes les règles pour une stratégie cohérente d'atténuation des menaces.

Pour plus d'informations, consultez Prisma Access Réseaux distants.

Flux de travail : Connexions aux services

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	Licence Prisma Access

Les connexions aux services permettent aux utilisateurs mobiles et aux utilisateurs sur vos réseaux de branche d'accéder aux ressources présentes dans votre siège social ou votre centre de données. Outre l'accès aux ressources de l'entreprise, les connexions de service permettent à vos utilisateurs mobiles de se rendre dans les succursales.

Choisissez **Workflows (Flux de travail)** > **Prisma Access Setup (Configuration)** > **Connexions aux services**, pour ajouter une connexion de service.

Le premier tunnel que vous créez est le tunnel principal pour la connexion au service. Répétez ce flux de travail pour configurer un tunnel secondaire si vous le souhaitez. Lorsque les deux tunnels sont opérationnels, le tunnel principal est prioritaire sur le tunnel secondaire. Si le tunnel de connexion au service principal tombe en panne, la connexion revient au tunnel secondaire jusqu'à ce que le tunnel principal soit rétabli. En fonction du périphérique IPSec que vous utilisez pour établir le tunnel, Prisma Access fournit des paramètres de sécurité IKE et IPSec intégrés et recommandés. Vous pouvez utiliser les paramètres recommandés pour démarrer ou les personnaliser selon les besoins de votre environnement.

Pour plus d'informations, consultez Prisma Access Connexions aux services.

Flux de travail : Isolation du navigateur distant

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Innovation Prisma Access 5.0 ❑ Licence Prisma Access avec abonnement à la licence Utilisateurs mobiles ou Réseaux distants ❑ Licence d'isolation du navigateur distant

L'isolation du navigateur distant de Palo Alto Networks est une solution qui isole et transfère toutes les activités de navigation des appareils gérés et des réseaux d'entreprise de vos utilisateurs vers une entité externe telle que Prisma Access, qui sécurise et isole le code et le contenu potentiellement malveillants dans leur plateforme.

Intégré nativement avec Prisma Access, RBI vous permet d'appliquer facilement des profils d'isolement aux politiques de sécurité existantes. Tout le trafic isolé fait l'objet d'une analyse et d'une prévention des menaces fournies par les services de sécurité fournis dans le cloud (CDSS) tels que la prévention avancée des menaces, l'Advanced WildFire, le filtrage des URL avancé, les sécurités DNS et SaaS.

Lorsque vous vous préparez à intégrer vos utilisateurs à RBI, passez aux catégories d'URL que vous souhaitez activer pour la navigation isolée par vos utilisateurs. Réfléchissez aux actions du navigateur que vous souhaitez interdire à vos utilisateurs d'effectuer, telles que les fonctions copier-coller, les saisies au clavier et les options de partage telles que le téléchargement et l'impression de fichiers.

Pour plus d'informations, consultezIsolation du navigateur distant.

Flux de travail : Mises à niveau logicielles

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • NGFW (Managed by Strata Cloud Manager)	• Au moins une de ces licences est nécessaire pour gérer votre configuration avec Strata Cloud Manager ; pour une gestion unifiée des NGFW et de Prisma Access, vous aurez besoin de licences NGFW et Prisma Access : ❑ Prisma Access licence ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Pro

Utiliser Strata Cloud Manager pour planifier et gérer vos mises à niveau logicielles pour NGFW et Prisma Access. Voici les flux de travail que vous pouvez effectuer :

- Recommandations de mise à niveau : Créez des recommandations de mise à niveau pour déterminer la meilleure version logicielle pour vos périphériques pouvant être mis à niveau. Les recommandations de mise à niveau du logiciel analysent les fonctionnalités activées sur les pare-feu et fournissent une recommandation personnalisée.
- Mise à jour du tableau de bord de Prisma Access : Choisissez une fenêtre horaire préférée pour certaines mises à niveau de Prisma Access.
- NGFW – Planificateur : Planifiez une mise à jour du logiciel PAN-OS pour mettre à niveau ou rétrograder vos pare-feu vers une version cible de PAN-OS à la date et à l'heure de votre choix
- NGFW
- Prisma Access

Mises à niveau logicielles (NGFW)

Choisissez **Workflows (Flux de travail)** > **Software Upgrades (Mises à niveau logicielles)** > **Upgrade Recommendations (Recommandations de mise à niveau)** pour planifier la mise à niveau de vos périphériques en les analysant et en créant des recommandations de mise à niveau.

Recommandations de mise à niveau

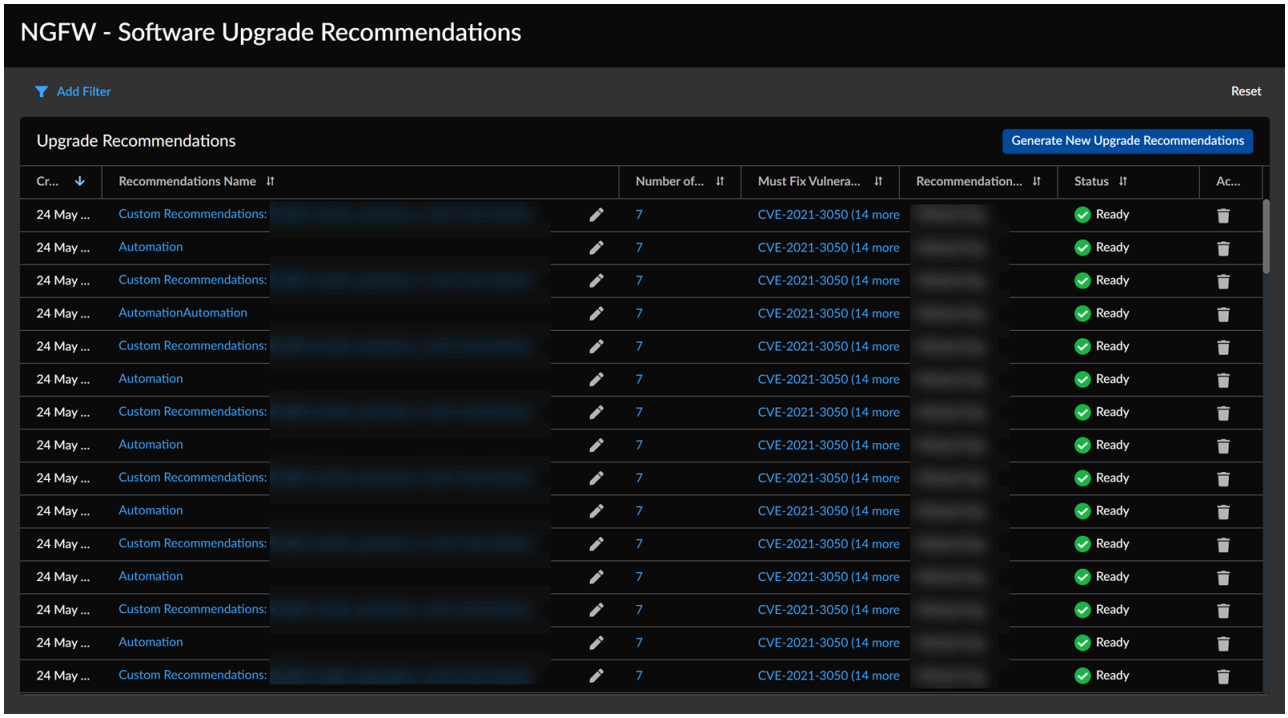
Dans **Workflows (Flux de travail)** > **Software Upgrades (Mises à niveau logicielles)** > **Upgrade Recommendations (Recommandations de mise à niveau)**, vous pouvez créer des recommandations pour déterminer la meilleure version logicielle pour vos périphériques qui peuvent être mis à niveau. Les recommandations de mise à niveau logicielle analysent les fonctionnalités activées sur les pare-feu et fournissent une recommandation personnalisée qui comprend :

- Meilleure version logicielle pour vos périphériques que vous pouvez mettre à niveau.

- Informations sur les nouvelles fonctionnalités, les changements de comportement, les vulnérabilités et les problèmes logiciels dans chaque version logicielle recommandée.

Les types de recommandations de mise à niveau sont les suivants :

- Recommandations générées par le système qui sont générées chaque semaine et qui contiennent les options de mise à niveau suggérées.
- Recommandations personnalisées générées par l'utilisateur en fonction des appareils sélectionnés pour des CVE spécifiques dans Résumé des avis de sécurité.
- Recommandations générées par l'utilisateur en fonction du téléchargement d'un fichier de support technique (TSF) d'un pare-feu.



Pour chaque plan dans **Upgrade Recommendations (Recommandations de mise à niveau)**, vous pouvez :

- Affichez le nombre de périphériques nécessitant une mise à niveau et les vulnérabilités à corriger.
- Modifiez le nom d'un rapport de recommandation pour différencier les rapports personnalisés.
- Filtrez les rapports de recommandations par date de création, nom du plan et recommandations générées par.
- Supprimez une recommandation de mise à niveau qui a échoué ou qui n'est plus nécessaire.

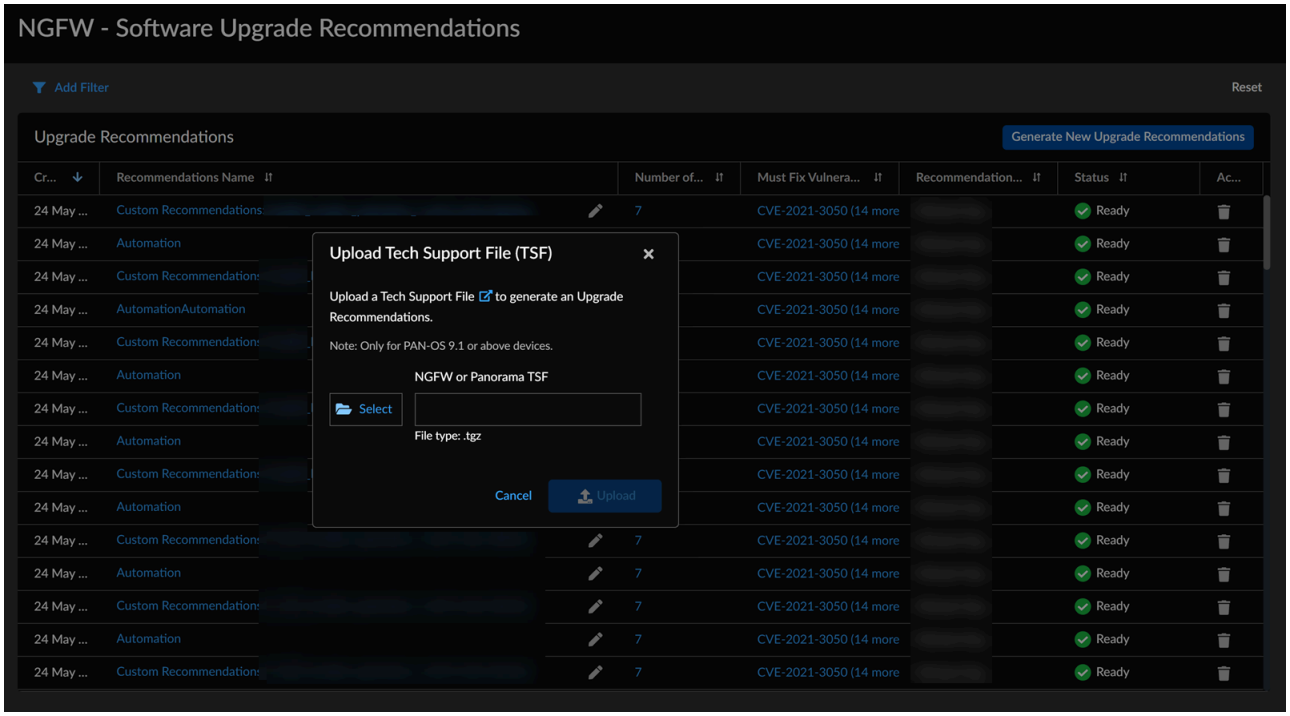
Cliquez sur un rapport de recommandation pour afficher le rapport détaillé avec les options de mise à niveau des appareils. Sélectionnez une option de mise à niveau pour afficher plus de détails sur **New Features (Nouvelles fonctionnalités)**, **PAN-OS Known Vulnerabilities (Vulnérabilités connues de PAN-OS)**, **Changes of Behavior (Changements de comportement)** et **PAN-OS Known Issues (Problèmes connus de PAN-OS)**. Pour un problème connu sous **PAN-OS Known Issues (Problèmes connus de PAN-OS)**, la valeur sous **Associated Case Count (Nombre de cas associés)** est obtenu par le nombre de clients qui ont signalé ce problème.

Cliquez sur **Export (Exporter)** pour télécharger ce rapport au format CSV.

Générer des recommandations de mise à niveau logicielle à la demande

1. Accédez à **Workflows (Flux de travail) > Software Upgrades (Mises à niveau logicielles) > Upgrade Recommendations (Recommandations de mise à niveau)**.
2. **Generate New Upgrade Recommendations (Générer de nouvelles recommandations de mise à niveau)**.
3. **Select (Choisir)** un dossier de support technique (TSF) et **Upload (Télécharger)**.

   - *Vous pouvez télécharger le TSF d'un seul périphérique à la fois et il doit s'agir du TSF au format de fichier .tgz.*
   - *Les recommandations de mise à niveau logicielle prennent en charge le TSF à partir de périphériques dotés de la version 9.1 ou ultérieure de PAN-OS pour la génération de rapports.*



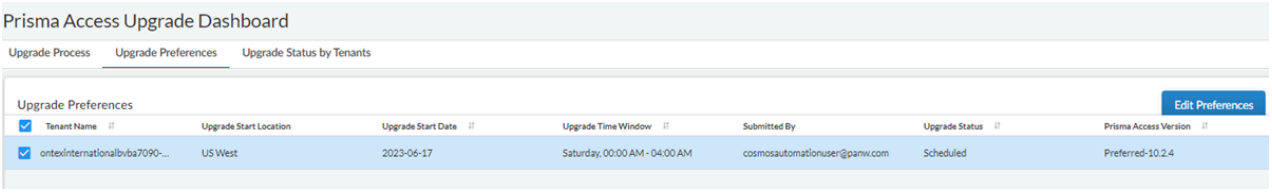
4. Affichez les recommandations de mise à niveau logicielle une fois que l'état s'affiche sous la forme **Ready (Prêt)**. Vous pouvez également consulter le **Status (État)** pour voir s'il y a des erreurs liées au téléchargement, au format de fichier ou au traitement du fichier TSF.

Mises à niveau logicielles (Prisma Access)

Sélectionnez **Workflows (Flux de travail)** > **Software Upgrades (Mise à niveau logicielle)** > **Prisma Access** pour afficher des informations sur le processus de mise à niveau du plan de données Prisma Access.

Vous pouvez :

- Comprendre le processus de mise à niveau du plan de données Prisma Access.
- Choisissez vos préférences de mise à niveau :



Sélectionnez un nom de locataire pour choisir vos préférences de mise à niveau. Pour plus d'informations, consultez Choisir une fenêtre préférée pour certaines mises à niveau Prisma Access.

Flux de travail : Navigateur Prisma Access

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access avec Licence groupée Prisma Access Browser ❑ Super utilisateur ou rôle Prisma Access Browser https://docs.paloaltonetworks.com/common-services/identity-and-access-access-management/manage-identity-and-access/about-roles-and-permissions

Choisissez **Workflows (Flux de travail)** > **Prisma AccessSetup (configuration** > **Prisma Access Browser** pour commencer à intégrer votre Prisma Access Browser.

Prisma Access Secure Enterprise Browser (Prisma Access Browser) est la seule solution qui sécurise à la fois les périphériques gérés et non gérés, grâce à un navigateur d'entreprise intégré en mode natif qui étend la protection aux périphériques non gérés. Reportez-vous à la section Qu'est-ce que le navigateur Prisma Access ?

L'intégration est une série d'étapes permettant de configurer les éléments suivants :

- Authentification des utilisateurs et groupes
- Intégration de Prisma Access
- Routage
- Appliquez les applications SSO
- Téléchargez et distribuez
- Politique du navigateur

Navigateur Prisma Access intégré sur le Strata Cloud Manager.

Rapports : Strata Cloud Manager

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • Prisma SD-WAN	❑ Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Prisma SD-WAN ❑ Crédits NGFW logiciels *(pour les logiciels VM-Series NGFW)* ❑ Licence de rapport WAN Clarity ❑ Un rôle qui a la permission de télécharger, partager et planifier des rapports.

Obtenez des rapports sur les modèles de trafic du réseau, l'utilisation de la bande passante et les données de votre abonnement de sécurité dans Strata Cloud Manager. Les rapports fournissent des informations exploitables sur votre réseau, que vous pouvez utiliser à des fins de planification et de surveillance. Les rapports sont pris en charge dans certains tableaux de bord Prisma Access et NGFW, dans l'aperçu Activity Insights et dans Prisma SD-WAN. Les utilisateurs de Prisma Access et de NGFW qui ont un accès complet à l'utilisation du tableau de bord, peuvent télécharger les données du tableau de bord sous forme de PDF, partager le rapport au sein de leur organisation et planifier des rapports pour les envoyer à leur boîte de messagerie à intervalles réguliers. Les rapports sont un service d'abonnement sous licence dans Prisma SD-WAN. Vous pouvez télécharger et consulter les rapports des contrôleurs, des sites et des circuits dans Prisma SD-WAN.

Voir ces rapports dans Strata Cloud Manager :

- Prisma Access et NGFW : vous pouvez générer des rapports à partir des Tableaux de bord Prisma Access et NGFW et des informations sur les activités. Ces icônes  en haut à droite du tableau de bord indiquent que les rapports sont pris en charge pour ce tableau de bord. Vous pouvez également générer, télécharger, partager et planifier des rapports directement à partir du menu**Reports (Rapports)**.
- Prisma SD-WAN - Consultez les éléments portant sur les rapports WAN Clarity suivants :
  - Rapports de la succursale WAN Clarity
  - Rapports du centre de données WAN Clarity
  - Rapports de l'utilisation de la bande passante
- Prisma Access et NGFW

- Prisma SD-WAN

Rapports (Prisma Access et NGFW)

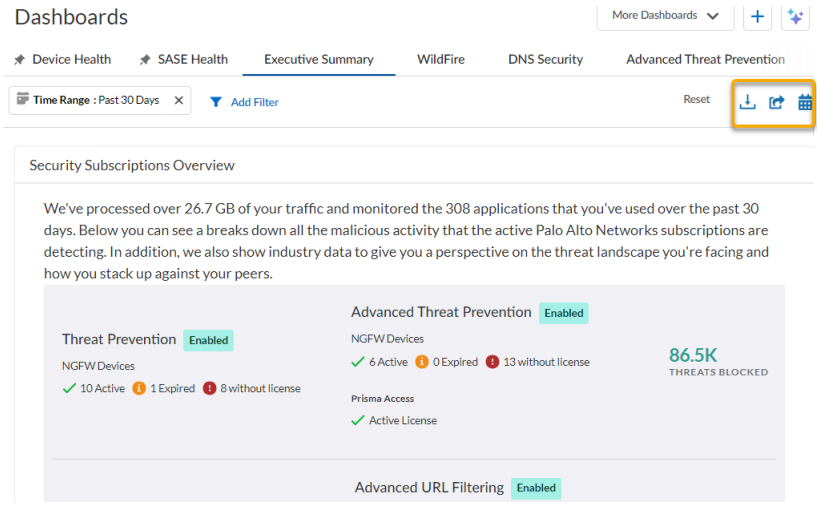
Les tableaux de bord et le résumé d'Activity Insights peuvent être partagés au sein de votre organisation sous forme de rapports PDF. Vous pouvez également programmer les rapports de manière à ce qu'ils soient envoyés à votre boîte de réception électronique et à celle de vos collègues à intervalles réguliers (quotidiens, hebdomadaires ou mensuels).

Pour que vous puissiez facilement partager des rapports avec les membres de votre organisation, configurez le moteur d'identité Cloud (Synchronisation d'annuaire) pour cette appli. Le moteur d'identité Cloud permet aux applis d'accéder en lecture seule à vos informations Active Directory. Une fois le Moteur d'identité cloud configuré, vous pouvez facilement ajouter des destinataires à un rapport planifié. Les destinataires de votre rapport sont contrôlés par Cloud Identity Engine, et s'il ne trouve pas de correspondance, il effectue une étape de validation supplémentaire en vérifiant le domaine d'adresse e-mail par rapport aux domaines d'adresse e-mail associés à votre compte de support. Ces contrôles permettent de s'assurer que les rapports ne sont pas envoyés en dehors de votre organisation.

Vous pouvez télécharger, partager ou planifier un rapport directement à partir du menu **Reports (Rapports)** ou de la page du**Tableau de bord individuel** et **Insights > (Aperçus >)** > **Activity Insights (des Informations sur l'activité)** > **Overview (Aperçu)** de la page. Les rapports sont partagés et téléchargés au format PDF.

Pour télécharger, partager ou planifier un rapport :

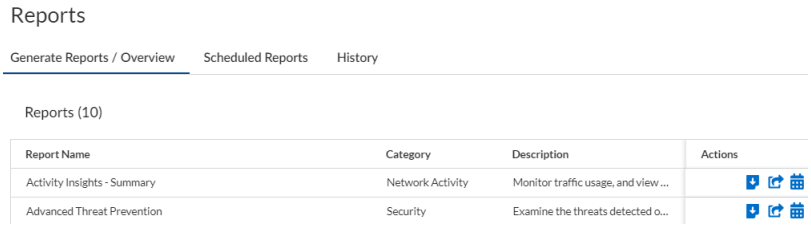
STEP 1 | Cliquez sur l'une de ces icônes, sur le **Dashboard (Tableau de bord)** ou à partir de la page **Insights > (Aperçus >)** > **Activity Insights (des Informations sur l'activité)** > **Aperçu** de la page.



Ou

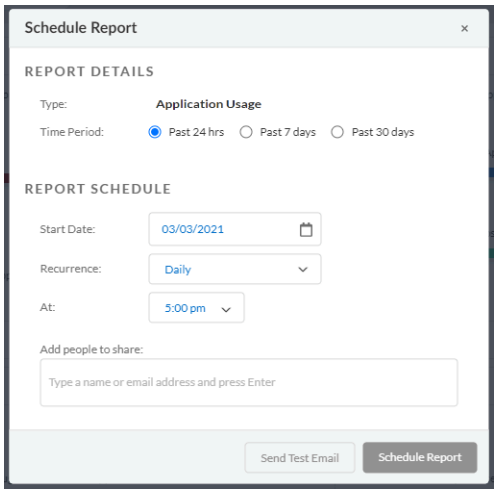
Cliquer sur **Strata Cloud Manager** > **Reports (Rapports)** > **Generate Reports/Overview (Générer des rapports/Aperçu)** et sélectionnez l'une de ces icônes dans la liste des formats de rapport. Par défaut, les rapports sont générés avec les données des dernières 24 heures ou des 30 derniers jours en fonction du type de tableau de bord pour lequel vous

générez un rapport. Vous pouvez personnaliser la période pour laquelle vous souhaitez recueillir des données dans le rapport lorsque vous planifiez le rapport.

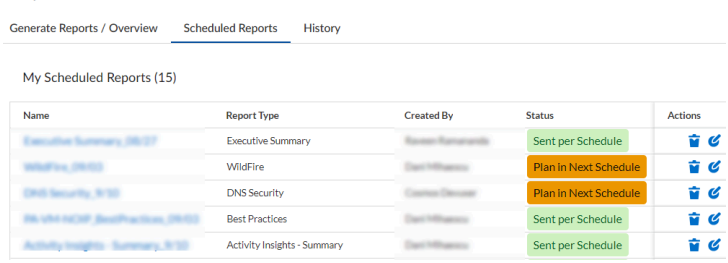


STEP 2 | Si vous planifiez un rapport, vous devrez continuer à définir les paramètres du rapport, notamment :

- la **Time Period (Période)** pour laquelle les données doivent être collectées
- la **Recurrence (Récurrence)**, qui correspond à la fréquence à laquelle vous souhaitez que le rapport soit livré (quotidienne, hebdomadaire ou mensuelle)



Vous pouvez afficher, modifier ou supprimer tous les rapports planifiés à partir du **Strata Cloud Manager** > **Reports (Rapports)** > **Scheduled Reports (Rapports programmés)** onglet.



History (Histoire) Affiche tous les rapports téléchargés au cours des 30 derniers jours.

Rapports (Prisma SD-WAN)

Prisma SD-WAN Les rapports WAN Clarity fournissent une vue globale de la répartition du trafic et de l'utilisation de la bande passante dans votre réseau. Vous pouvez télécharger l'ensemble des rapports ou les consulter à partir du Prisma SD-WAN contrôleur, ce qui permet de comparer les tendances d'une semaine à l'autre, ainsi que les sites et les circuits.

Les rapports sont disponibles pour une utilisation immédiate sous la forme d'un service d'abonnement sous licence. Contactez l'équipe commerciale de Prisma SD-WAN pour activer l'abonnement.

Les Prisma SD-WANrapports WAN Clarity comprennent :

- Rapports de succursale WAN Clarity
- Rapports des centres de données WAN Clarity
- Rapport de l'utilisation de la bande passante agrégée

Pour consulter les rapports :

STEP 1 | Sélectionnez les **Reports (Rapports)** > **Prisma SD-WAN**.

STEP 2 | Cliquez sur **View Reports (Afficher les rapports)** sur **WAN Clarity Reports (Rapports Wan Clarity**.

STEP 3 | Sélectionnez une **Time Range (Plage de temps)** et sélectionnez l'une des options suivantes dans le champ **Report for (Rapport pour)**.

- **Branche**
- **Centre de données**
- **Utilisation de la bande passante agrégée**

Favoris : Strata Cloud Manager

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Toute application prise en charge par le locataire ou le Groupe de services aux locataires (TSG) ❑ Un rôle en fonction de vos besoins

La fonctionnalité Favoris vous permet d'enregistrer les éléments importants et d'y accéder rapidement en cas de besoin à partir de n'importe quel emplacement dans Strata Cloud Manager. Vous pouvez personnaliser les noms de vos éléments de menu préférés dans votre propre liste privée en organisant, modifiant et supprimant le contenu de votre liste.

Gérez vos favoris comme suit :

- Ajouter des favoris
- Voir les favoris
- Modifier les favoris
- Supprimer les favoris

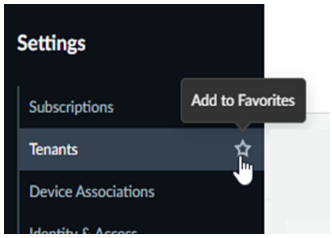
Ajouter des favoris

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Toute application prise en charge par le locataire ou le Groupe de services aux locataires (TSG) ❑ Un rôle en fonction de vos besoins

Si vous avez des éléments de menu ou des pages dans Strata Cloud Manager où vous devez régulièrement vous aller, sans plus vouloir les rechercher ou y naviguer, vous pouvez enregistrer ces éléments dans une liste de favoris.

STEP 1 | Accédez à l'élément de menu ou à la page que vous souhaitez enregistrer.

STEP 2 | Survolez l'élément pour afficher l'icône en forme d'étoile.



STEP 3 | Sélectionnez l'étoile pour ajouter cet élément à vos **Favorites (Favoris)**.

Les éléments de menu de très haut niveau ne peuvent pas être ajoutés aux favoris. Seuls les sous-menus peuvent être ajoutés aux favoris.

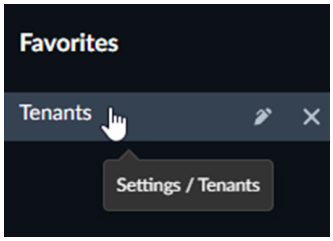
Voir les favoris

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Toute application prise en charge par le locataire ou le Groupe de services aux locataires (TSG) ❑ Un rôle en fonction de vos besoins

Après avoir ajouté des favoris, vous pouvez afficher vos favoris et leur emplacement d'origine.

STEP 1 | Choisissez **Favorites (Favoris)**.

STEP 2 | Survolez l'élément pour afficher l'icône de l'emplacement.



STEP 3 | Le chemin d'accès à l'emplacement réel et le nom du menu s'affichent.

En cliquant sur l'élément dans votre liste de favoris, vous accédez à son emplacement d'origine.

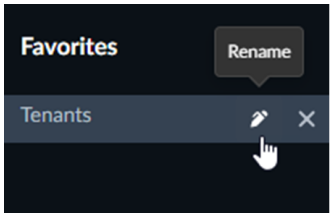
Modifier les favoris

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Toute application prise en charge par le locataire ou le Groupe de services aux locataires (TSG) ❑ Un rôle en fonction de vos besoins

Après avoir ajouté des favoris, vous pouvez les modifier pour les personnaliser.

STEP 1 | Choisissez **Favorites (Favoris)**.

STEP 2 | Survolez l'élément afin d'afficher l'icône de modification.



STEP 3 | Renommer l'élément.

Lorsque vous renommez un élément dans votre liste de favoris, vous ne renommez pas l'élément d'origine dans son emplacement d'origine.

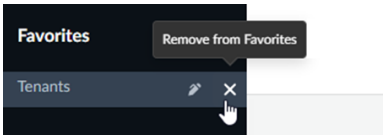
Supprimer les favoris

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)* • NGFW *(avec la gestion de la configuration Strata Cloud Manager ou Panorama)*	❑ Chacune de ces licences inclut l'accès à Strata Cloud Manager : ❑ Prisma Access ❑ AIOps for NGFW Premium license (use the Strata Cloud Manager app) ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro ❑ Toute application prise en charge par le locataire ou le Groupe de services aux locataires (TSG) ❑ Un rôle en fonction de vos besoins

Après avoir ajouté des favoris, vous pouvez supprimer les favoris de votre liste.

STEP 1 | Choisissez **Favorites (Favoris)**.

STEP 2 | Passez la souris sur l'élément pour afficher l'icône de suppression.



STEP 3 | Cliquez sur l'icône pour supprimer l'élément favori de la liste.

La suppression de l'élément de votre liste de favoris ne supprime pas l'élément d'origine de son emplacement d'origine.

Paramètres : Strata Cloud Manager

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	☐ Toute application prise en charge par le locataire ou le Groupe de services aux locataires (TSG) ☐ Un rôle en fonction de vos besoins ☐ Strata Logging Service pour gérer les journaux

À partir de **Settings (Paramètres)**, vous pouvez gérer les processus relatifs à tous les services offerts dans Strata Cloud Manager. Ces processus comprennent :

Abonnements

Consultez les abonnements approuvés pour votre produit.

Abonnements gérés.

Device Associations

Le plus souvent utilisé dans l'intégration des périphériques et des applis, **Device Associations** il vous permet de :

- Associer de nouveaux périphériques à un locataire
- Associer des applis à vos périphériques
- Gérer les associations des périphériques et des applications

Démarrer avec les associations de périphériques.

Produits

Si vous disposez d'un environnement à locataire unique, affichez, lancez et gérez vos produits :

- Obtenir des informations sur les produits
- Renommer l'instance
- Gérer le partage
- Ajouter un locataire

Démarrer avec la Gestion des produits.

Locataires

Si vous êtes un fournisseur de services de sécurité gérés (MSSP) ou une entreprise distribuée, vous pouvez créer et gérer votre hiérarchie d'organisations et d'unités professionnelles, représentées par des locataires. À partir du **Tenants (Locataires)**Vous pouvez :

- Ajouter un locataire

- Modifier un locataire
- Gérer les licences de locataire
- Supprimer un locataire
- Passez d'un déploiement à locataire unique à un déploiement à plusieurs locataires

Démarrez avec la gestion des locataires.

Identité et accès

Contrôler l'authentification et l'autorisation des rôles et des permissions des utilisateurs pour toutes les applications et l'accès basé sur l'API. Grâce à Identité et Accès, vous pouvez gérer :

- Accès des utilisateurs
- Comptes de service
- Rôles
- Intégration d'un fournisseur d'identité tiers

Démarrez avec Identité et Accès.

Journaux d'audit

Consulter les enregistrements de toutes les actions initiées par les utilisateurs de Strata Cloud Manager

Afficher les journaux d'audit.

Gestion des licences ION

Générez des jetons d'autorisation pour les périphériques ION virtuels. Il s'agit d'un ensemble de contrôles visant à empêcher l'ajout non autorisé de périphériques virtuels dans un environnement.

Gérer les licences ION.

Préférences des utilisateurs

Personnalisez vos préférences en fonction de vos besoins. Par exemple, choisissez votre mode d'affichage.

Configurer les préférences des utilisateurs.

Liste d'adresses IP de confiance

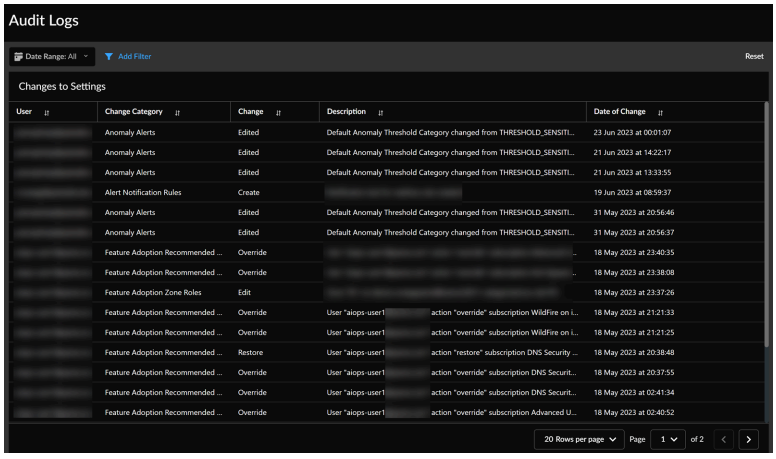
Utilisez les listes d'adresses IP de confiance pour restreindre l'accès à vos applications en spécifiant les adresses IP autorisées pour chaque locataire.

Configuration d'une liste d'adresses IP de confiance.

Paramètres : Journaux d'audit

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Strata Cloud Manager	❑ L'un des éléments suivants : • AIOps for NGFW Free appli • AIOps for NGFW Premium (utilisez l'appli Strata Cloud Manager) • Strata Cloud Manager Essentials • Strata Cloud Manager Pro ❑ L'un des rôles prédéfinis suivants : Auditeur, administrateur d'entreprise, administrateur de la sécurité des données, administrateur de déploiement, administrateur IAM, administrateur IAM multi-locataire, utilisateur de gestion multi-locataire, utilisateur de surveillance multi-locataire, super utilisateur multi-locataire, administrateur de réseau, administrateur de sécurité, analyste SOC, super utilisateur, support de niveau 1, support de niveau 2, administrateur de visualisation seulement.

Sous **Settings (Paramètres) > (Audit Logs) Journaux d'audit**, vous pouvez voir une liste d'actions initiées par les utilisateurs de Strata Cloud Manager. Il fournit des journaux sur les modifications apportées, le propriétaire de la modification, la date et l'heure de la modification, ainsi que la description de la modification. Vous pouvez utiliser ces journaux à des fins de conformité et de dépannage. Vous pouvez filtrer les journaux d'audit par plage de dates avec capacité, par utilisateur, catégorie et type de modification.



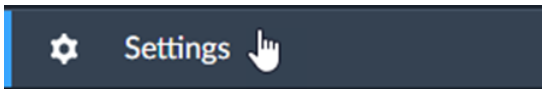
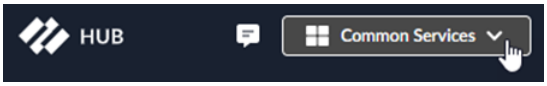
Paramètres : Liste d’adresses IP de confiance

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Strata Cloud Manager	❑ Rôle IAM https://docs.paloaltonetworks.com/common-services/identity-and-access-access-management/manage-identity-and-access/about-roles-and-permissions de super utilisateur, super utilisateur multilocataire, administrateur IAM multilocataire ou tout rôle personnalisé avec l’ensemble d’autorisations « Liste d’adresses IP approuvées »

Les applications fournies dans le cloud offrent la commodité d’être accessibles depuis n’importe quel endroit dans le monde. Cependant, cela expose à des risques tels que l’accès à l’aide d’identifiants volés, d’attaques par dictionnaire et d’autres formes d’attaques par force brute pour accéder aux applications.

Bien que la gestion des identités et des accès https://docs.paloaltonetworks.com/common-services/identity-and-access-access-management/manage-identity-and-access atténue certains de ces risques, vous pouvez utiliser des listes d’adresses IP approuvées pour restreindre davantage l’accès à vos applications en spécifiant les adresses IP autorisées pour chaque locataire.

Par défaut, lors de la création d’un nouveau locataire, l’accès est autorisé à la fois à l’interface Web et à l’API à partir de n’importe quelle adresse IP. La liste IP de confiance est une liste d’adresses IP de confiance autorisées à accéder à un locataire. Vous pouvez utiliser une liste d’adresses IP approuvées pour limiter l’accès à un seul locataire ou pour limiter l’accès à un locataire parent et à ses enfants dans une hiérarchie multilocataire. Dans une hiérarchie multilocataire, vous ajoutez la liste d’adresses IP approuvées sur le locataire parent, la liste est héritée du locataire parent par ses locataires enfants et est appliquée de haut en bas.

Gérer une liste d’adresses IP de confiance à partir de Strata Cloud Manager	Gérer une liste d’adresses IP de confiance à partir de hub
Pour gérer une liste d’adresses IP de confiance à partir de Strata Cloud Manager, sélectionnez **Settings (Paramètres)** > **Trusted IP List (Liste IP de confiance)**.  Vous pouvez gérer les listes d’adresses IP de confiance à partir de Strata Cloud Manager et l’interface Web Strata Cloud Manager et	Pour gérer une liste d’adresses IP de confiance à partir de hub, sélectionnez **tenant view of the hub (vue locataire du concentrateur)** > **Common Services (Services communs)** > **Trusted IP List (Liste des adresses IP approuvées)**.  Vous pouvez gérer les listes d’adresses IP de confiance à partir du hub, mais le hub est exempté de l’application de l’IP de

Gérer une liste d'adresses IP de confiance à partir de Strata Cloud Manager	Gérer une liste d'adresses IP de confiance à partir de hub
l'API autoriseront l'accès uniquement à ces adresses IP de confiance.	confiance, donc votre accès à hub ne se limite pas aux adresses IP de confiance. Si votre adresse IP est bloquée par un locataire sur Strata Cloud Manager auquel vous devriez avoir accès, vous pouvez aller à la hub et déverrouillez votre accès si vous disposez des autorisations répertoriées.

- Ajouter des adresses IP de confiance
- Supprimer les adresses IP de confiance
- Déverrouiller l'accès

Ajouter des adresses IP de confiance

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Strata Cloud Manager	☐ Rôle IAM https://docs.paloaltonetworks.com/common-services/identity-and-access-access-management/manage-identity-and-access/about-roles-and-permissions de super utilisateur, super utilisateur multilocataire, administrateur IAM multilocataire ou tout rôle personnalisé avec l'ensemble d'autorisations « Liste d'adresses IP approuvées »

Une fois que vous avez activé votre licence, créé vos locataires et géré l'accès des utilisateurs à Strata Cloud Manager, vous pouvez restreindre davantage l'accès à vos locataires en ajoutant des adresses IP de confiance à une liste d'adresses IP de confiance. Par défaut, n'importe quelle adresse IP est autorisée à accéder.

Ajoutez des adresses IP de confiance à l'aide de Strata Cloud Manager.

STEP 1 | Sélectionnez **Settings (Paramètres)** > **Trusted IP List (Liste d'adresses IP de confiance)**.

STEP 2 | Recherchez ou faites défiler pour trouver et sélectionner votre locataire.

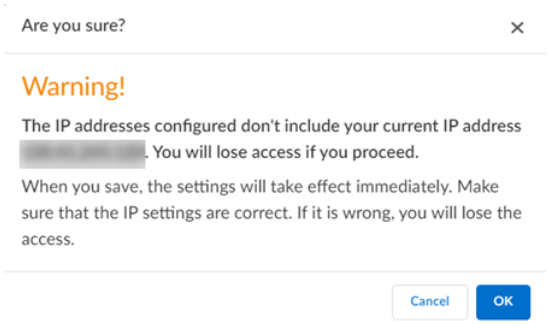
STEP 3 | Sélectionnez **Add New (Ajouter nouveau)**.

STEP 4 | Entrez une **IP Address (Adresse IP)** qui peut vous permettre d'accéder à ce locataire.

- Le champ prend en charge la notation CIDR. Seules les adresses IPv4 sont autorisées.
- Vous pouvez utiliser une seule adresse IP ou une plage avec un masque de sous-réseau tel que 12.12.12.1/30.
- L'adresse IP et la plage sont validées, de sorte que les erreurs sont affichées pour les éléments non pris en charge.
- Le **Added By field (Ajouté par champ)** se remplit automatiquement.

STEP 5 | **Save (Enregistrer)**.

La modification prend effet immédiatement, alors assurez-vous que votre adresse IP est correcte, sinon vous risquez de perdre l'accès au locataire.



STEP 6 | Une fois que vous avez ajouté une liste d'adresses IP de confiance sur le locataire parent, la liste est héritée du locataire parent vers ses locataires enfants et est appliquée de haut en bas. Un locataire enfant peut également ajouter sa propre liste d'adresses IP approuvées.

Supprimer les adresses IP de confiance

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Strata Cloud Manager	❑ Rôle IAM https://docs.paloaltonetworks.com/common-services/identity-and-access-access-management/manage-identity-and-access/about-roles-and-permissions de super utilisateur, super utilisateur multilocataire, administrateur IAM multilocataire ou tout rôle personnalisé avec l'ensemble

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
	d'autorisations « Liste d'adresses IP approuvées »

Après avoir ajouté des adresses IP de confiance à une liste d'adresses IP de confiance pour votre locataire, vous pouvez revenir à un accès illimité en supprimant les adresses IP de confiance.

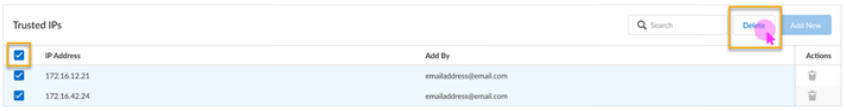
Supprimez les adresses IP de confiance à l'aide de Strata Cloud Manager.

STEP 1 | Sélectionnez **Settings (Paramètres)** > **Trusted IP List (Liste d'adresses IP de confiance)**.

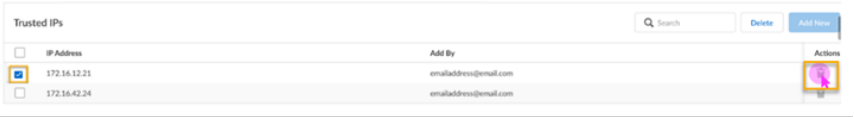
STEP 2 | Recherchez ou faites défiler pour trouver et sélectionner votre locataire.

STEP 3 | Utilisez l'une des options suivantes :

- Supprimez plusieurs adresses IP : cochez la case **IP Address (Adresse IP)** pour mettre en évidence toutes les adresses IP en même temps, puis activez le bouton **Supprimer**.



- Supprimez une adresse IP unique : activez la case à cocher individuelle de l'IP, puis supprimez de **Actions** > **Delete (Supprimer)**.



Lorsque vous avez hérité d'une liste d'adresses IP de confiance d'un locataire parent, vous ne pouvez pas la supprimer d'un locataire enfant, car ces listes sont héritées. On ne peut supprimer une liste d'adresses IP de confiance d'un locataire secondaire que si on l'a ajoutée directement au niveau secondaire.

STEP 4 | Sélectionnez **OK** à l'invite.

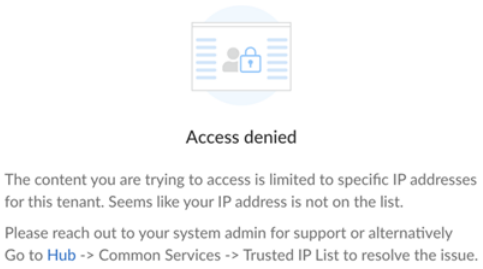
Le changement prend effet immédiatement. Si vous supprimez toutes les adresses IP approuvées, l'accès IP retourne à **Any (N'importe quelle**.

Déverrouiller l'accès

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Strata Cloud Manager	❑ Rôle IAM https://docs.paloaltonetworks.com/common-services/identity-and-access-access-management/manage-identity-and-access/about-roles-and-permissions de super utilisateur, super utilisateur multilocataire, administrateur IAM multilocataire ou tout rôle personnalisé avec l'ensemble

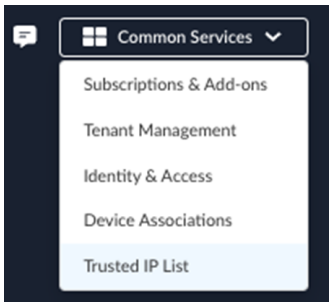
Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
	d'autorisations « Liste d'adresses IP approuvées »

Après avoir ajouté des adresses IP approuvées à une liste d'adresses IP approuvées pour votre locataire, cet accès est appliqué par Strata Cloud Manager. Si votre adresse IP ne figure pas dans la liste des adresses IP approuvées du locataire, un message d'accès refusé s'affiche si vous essayez d'y accéder.

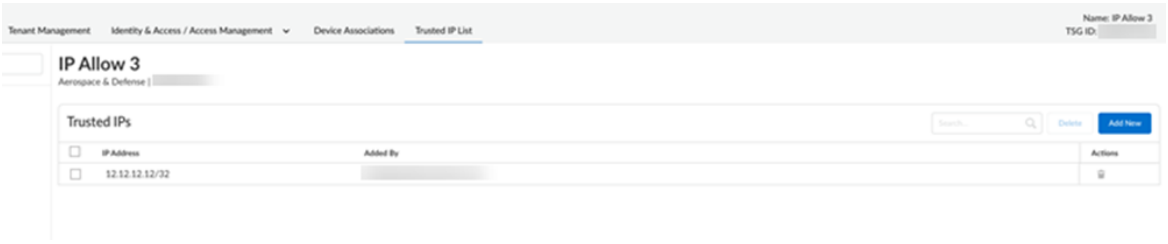


Si votre adresse IP est bloquée par un locataire auquel vous devriez avoir accès, vous pouvez accéder à hub pour vous déverrouiller si vous disposez des autorisations répertoriées.

STEP 1 | De la hub, sélectionnez **tenant view of the hub (vue locataire du concentrateur)** > **Common Services (Services communs)** > **Trusted IP List (Liste des adresses IP approuvées)**.



STEP 2 | Ajoutez votre adresse IP à la liste des adresses IP de confiance.



Paramètres : Préférences des utilisateurs

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Strata Cloud Manager	L'une des options suivantes : ❑ AIOps for NGFW Free ou licenceAIOps for NGFW Premium ❑ Strata Cloud Manager Essentials ❑ Strata Cloud Manager Pro

Dans **Settings (Paramètres) > User Preferences (Préférences de l'utilisateur)**, vous pouvez personnaliser Strata Cloud Manager pour répondre à vos besoins spécifiques en modifiant les Préférences de l'utilisateur . Ces paramètres sont les suivants :

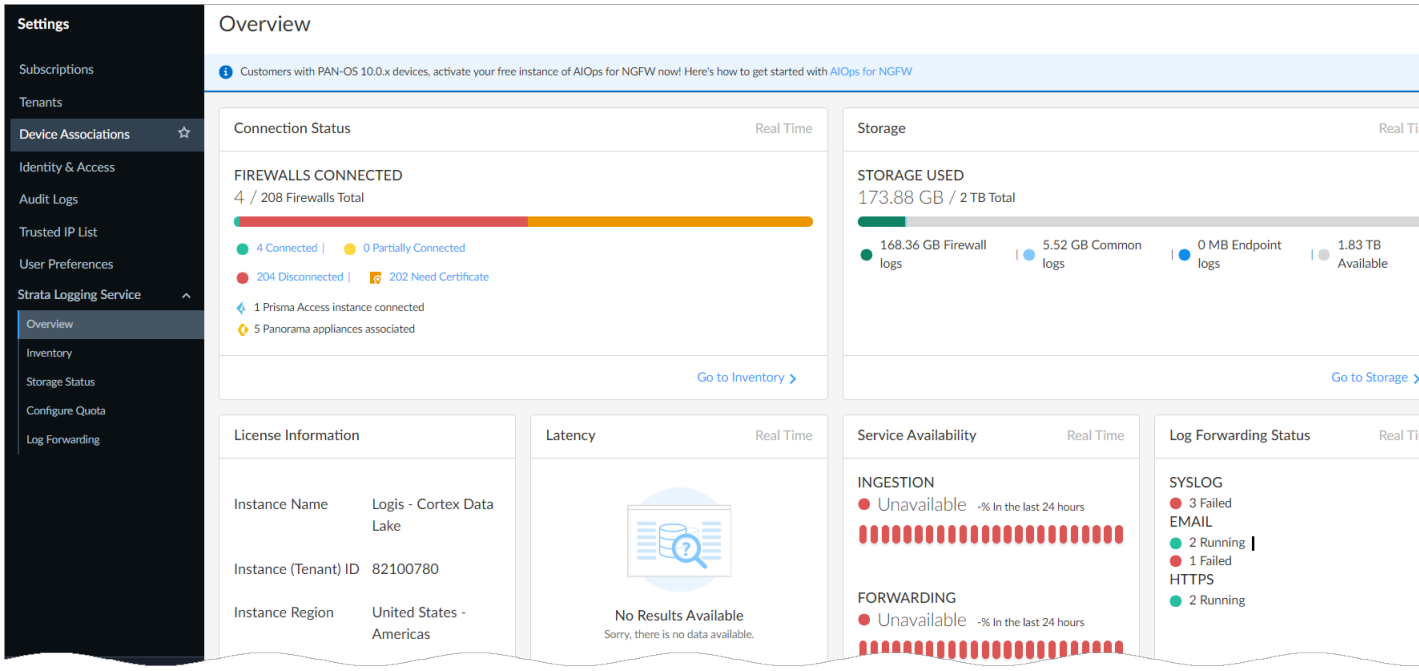
- **Light/Dark/System Mode (Mode clair/sombre/système)** - choisissez entre les modes d'affichage sombre et clair ou choisissez de suivre vos propres paramètres système.

Paramètres :Strata Logging Service

Où puis-je l'utiliser ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by PAN-OS or Panorama) • NGFW (Managed by Strata Cloud Manager)	❑ Strata Logging Service

Strata Logging Service (précédemment Cortex Data Lake) est un système de journalisation basé sur le cloud qui stocke des journaux réseau améliorés et contextualisés générés par nos produits de sécurité, y compris nos NGFW, Prisma Access et Cloud NGFW pour AWS. Avec Strata Logging Service, vous pouvez acquérir des volumes de données de plus en plus importants sans avoir à planifier le calcul et le stockage au niveau local, tout en étant prêt à évoluer dès le départ. Apprenez comment activer et déployerStrata Logging Service dans votre produit.

De plus, vous pouvez également accéder aux journaux et les gérer à l'aide de l'appliStrata Logging Service disponible sur le concentrateur https://apps.paloaltonetworks.com/apps. Les données de journalisation sont les mêmes dans les deux applis Strata Logging Service et Strata Cloud Manager, à l'exception de leurs différences d'interface Web.



Utiliser Strata Logging Service pour :

- Vérifier l'état d'une instance Strata Logging Service -cliquez sur **Strata Logging Service** > **Overview (Aperçu)**
- Afficher et intégrer les pare-feux, Cloud NGFW, Prisma Access ou les appliances Panorama - cliquez sur **Strata Logging Service** > **Inventaire**
- Affichez le quota de stockage des journaux alloué, l'espace de stockage disponible et le nombre de jours pendant lesquels les journaux sont conservés en fonction de votre taux de journaux entrants - cliquez sur **Strata Logging Service** > **État de stockage**
- Configurer le quota de stockage des journaux- cliquez sur **Strata Logging Service** > **Configure Quota (Configurer le quota)**
- Recherchez, filtrez et exportez les données du journal- cliquez sur **Incidents & Alerts (Incidents et alertes)** > **Log Viewer (Visionneuse du journal des incidents)**. La Visionneuse de journaux a les mêmes fonctionnalités qu'Explore dans l'appli Strata Logging Service.
- Transférer les données du journal vers des serveurs externes pour un stockage à long terme, un SOC ou un audit interne - cliquez sur **Strata Logging Service** > **Log Forwarding (Transfert de journal)**

Expérience d'application

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	L'une de ces licences : licence ❑ Prisma Access ❑ licence ADEM Observability ou licence AI-Powered ADEM

Utilisez la page **Application Experience (Expérience des applications)** pour gérer vos utilisateurs DEM autonomes et vos sites distants. Consultez les journaux d'audit pour voir quels administrateurs se sont authentifiés auprès de Prisma Access pendant la **Time Range (Plage de temps)** sélectionnée.

Reportez-vous à la section Gérer les mises à niveau des agents DEM autonomes pour en savoir plus sur les **options de mise à niveau.**

Gestion de l'agent de terminaison

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	L'une de ces licences : licence ❑ Prisma Access ❑ licence ADEM Observability ou licence AI-Powered ADEM

Utilisez cet onglet pour obtenir des détails sur tous vos utilisateurs ADEM enregistrés, par exemple si l'utilisateur est en ligne (le périphérique de l'utilisateur envoie des messages de maintien de connexion au service ADEM) ou hors ligne (le service ADEM n'a pas reçu de message de maintien de connexion du périphérique de l'utilisateur au cours des dix dernières minutes), lorsque le périphérique de l'utilisateur a été vu pour la dernière fois, le nom d'utilisateur, le type d'appareil et le nom d'hôte de l'utilisateur ADEM, ainsi que la version de l'agent ADEM qu'il exécute.

Toutes les lignes du tableau de cet onglet représentent un utilisateur unique dans une ligne distincte. Chaque combinaison utilisateur/périphérique est considérée comme un utilisateur unique. Par exemple, si 2 utilisateurs sont connectés à 3 périphériques chacun, le nombre d'utilisateurs uniques sera de 6. Par conséquent, un nom d'utilisateur peut être dupliqué sur plusieurs lignes en fonction du nombre de périphériques auxquels il est connecté.

Dans le titre du tableau de ce widget, le nombre correspondant au **Total Endpoint Agents (total des agents de terminal)** indique le nombre total de périphériques surveillés. Le nombre **Users (d'Utilisateurs)** correspond au nombre total d'utilisateurs, quel que soit le nombre de périphériques sur lesquels ils sont connectés. Cela est dû au fait que la consommation de licences est basée sur le nombre total d'utilisateurs, quel que soit le nombre de périphériques sur lesquels chaque utilisateur est connecté.

Utilisez les cases à cocher à gauche du **Last logged in User (Dernier utilisateur connecté)** pour effectuer une configuration groupée en sélectionnant la ligne des terminaux. La suppression d'une entrée en la sélectionnant dans le tableau Gestion des agents de terminaux libérera l'entrée de licence.

Nom de colonne	Description
Dernier utilisateur à s'être connecté	Plusieurs utilisateurs peuvent se connecter à un périphérique. Cette colonne répertorie l'ID de l'utilisateur le plus récent qui s'est connecté à GlobalProtect à l'aide de ce périphérique.
Périphérique	Le système d'exploitation exécuté sur ce périphérique.
Nom d'hôte	Le nom d'hôte du périphérique.
Vu en dernier	Le dernier message envoyé depuis le périphérique au serveur DEM.
Première apparition	Le premier message reçu de ce périphérique par le serveur DEM.
État de l'utilisateur	État de connexion de l'utilisateur actuel.
État de surveillance	Si les tests d'appli sont en cours d'exécution sur le périphérique.
Version de l'agent de terminaison	La version de l'agent ADEM installée sur le périphérique.

Gestion de l'agent du site à distance

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	L'une de ces licences : licence ❑ Prisma Access ❑ licence ADEM Observability ou licence AI-Powered ADEM

Cet onglet vous donne des détails sur les périphériques Prisma SD-WAN ION des succursales qui sont activés pour la gestion de l'expérience numérique. Utilisez cet onglet pour obtenir des détails sur tous vos sites distants ADEM enregistrés, tels que le modèle de périphérique, le nom de l'hôte, l'état du site, l'état de surveillance (si la surveillance est activée pour le site), le nom d'hôte du serveur High Availability (haute disponibilité - HA) (s'il y en a un) et la version de l'agent du site distant.

Nom de colonne	Description
Nom du site distant	Site de la succursale Pisma SD-WAN.
Modèle de périphérique	Numéro de modèle du périphérique Prisma SD-WAN ION.
Nom d'hôte	Nom d'hôte du périphérique ION.
Nom d'hôte de l'homologue HA	Si un périphérique ION de secours à High Availability (haute disponibilité - HA) a été configuré sur ce site.
Vu en dernier	Le dernier message envoyé depuis le périphérique ION au serveur DEM.
Première apparition	Le premier message reçu du périphérique ION par le serveur DEM.
État du site	État de connectivité du périphérique ION du site avec l'agent DEM.
État de surveillance	Si le site est configuré pour exécuter des tests d'appli.
Version de l'agent du site distant	La version de l'agent ADEM installée sur le périphérique ION.

Profils de score d'état de santé

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	L'une de ces licences : licence ❑ Prisma Access ❑ licence ADEM Observability ou licence AI-Powered ADEM

Voir les détails du score de l'état du domaine dans cet onglet.

Nom de colonne	Description
Nom des indicateurs de score d'état de santé du domaine	Répertorie les domaines pour lesquels les métriques du score de l'état sont calculées. Cliquez sur le nom d'un domaine dans cette colonne pour afficher ses paramètres, tels que les seuils inférieur et supérieur. Cliquez également sur l'impact (pourcentage du score

Nom de colonne	Description
	total de l'expérience) du domaine sur le score total lorsque les chiffres franchissent le seuil. Actuellement, ces métriques sont en lecture seule telles que définies par l'Administrateur. Ils ne peuvent pas être modifiés.
Type	Type de domaine
Cas d'utilisation associé	Le tableau de bord ou widget sur lequel s'affiche le score d'expérience calculé.

Journaux d'audit ADEM

Où puis-je utiliser ceci ?	De quoi ai-je besoin ?
• Prisma Access (Managed by Strata Cloud Manager)	L'une de ces licences : licence ❑ Prisma Access ❑ licence ADEM Observability ou licence AI-Powered ADEM

Afficher les journaux d'audit pour tous les événements déclenchés par les appels à l'API.

Nom de colonne	Description
Heure de l'événement	Heure à laquelle l'événement a été déclenché et a entraîné la création du journal.
Messagerie	Adresse email de la personne ayant été informée de la création du journal.
Description	L'appel à l'API qui a provoqué le déclenchement de l'événement et donc la création du journal.

