Meilleures pratiques pour la gestion des pare-feu avec Panorama

10.0 (EoL)

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

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

Copyright

Last Revised

December 3, 2020

Table of Contents

Meilleures pratiques pour ajouter des pare-feu à Panorama

Le serveur de gestion Panorama™ est la solution de gestion de la sécurité réseau de Palo Alto Networks pour une gestion et une visibilité centralisées de vos pare-feu nouvelle génération. Ce document présente les meilleures pratiques pour intégrer de nouveaux pare-feu ou migrer des pare-feu existants vers Panorama afin de simplifier et rationaliser cette opération.

> Cas d'utilisation : intégration des nouveaux pare-feu nouvelle génération à Panorama
> Cas d'utilisation : migration de vos nouveaux pare-feu nouvelle génération vers Panorama

Cas d'utilisation : intégration des nouveaux pare-feu nouvelle génération à Panorama

Le premier cas d'utilisation pour démarrer avec le serveur de gestion Panorama™ est d'ajouter un pare-feu nouvellement déployé comme appareil géré à Panorama.

STEP 1 | Cliquez sur **Associate Devices (Associer des périphériques)** ou **Import (Importer)** plusieurs pare-feu pour rationaliser le processus d'intégration.

- Associez les pare-feu à un groupe d'appareils, une pile de modèles, un groupe de collecteurs et un collecteur de journaux lorsque vous les ajoutez à Panorama à partir d'un seul endroit plutôt que d'associer manuellement les pare-feu une fois qu'ils ont été ajoutés avec succès à Panorama.
- Si vous ajoutez un grand nombre de pare-feu, importez tous vos nouveaux pare-feu vers Panorama dans un fichier CSV. Ce fichier CSV vous permet d'associer tous vos pare-feu à un groupe d'appareils, une pile de modèles, un groupe de collecteurs et un collecteur de journaux plutôt que de les associer manuellement. Cette option est particulièrement avantageuse lorsque vous ajoutez un grand nombre de pare-feu et que l'association manuelle des pare-feu prendrait beaucoup de temps.

STEP 2 | Activez **Auto Push on 1st Connect (Transmission automatique à la première connexion)** et configurez **To SW Version (Vers la version logicielle)** pour appliquer automatiquement les configurations du groupe d'appareils et de la pile de modèles à vos pare-feu gérés lorsqu'ils se connectent pour la première fois avec succès à Panorama et mettez à niveau vos pare-feu gérés vers une version PAN-OS spécifique de votre choix. Cela inclut l'installation automatique de toutes les mises à jour de contenu requises pour chaque version de PAN-OS dans le chemin de mise à niveau PAN-OS.

- Si vous importez tous vos nouveaux pare-feu vers Panorama dans un fichier CSV, activez **Auto Push on 1st Connect (Transmission automatique à la première connexion)** et configurez **To SW Version (Vers la version logicielle)** dans le fichier CSV pour rationaliser le processus d'importation.
- Lorsque vous mettez en œuvre un contrôle d'accès basé sur les rôles, utilisez les admins de groupes d'appareils et de modèles pour ajouter des pare-feu aux groupes d'appareils et aux modèles dans leur domaine d'accès plutôt que d'activer les privilèges de super utilisateur pour tous les admins de Panorama.

STEP 3 | Une fois que vous avez ajouté vos pare-feu à Panorama, créez et appliquez des étiquettes pour faciliter la recherche et le filtrage des pare-feu que vous gérez. Cela vous permet de garder vos pare-feu gérés organisés au fur et à mesure que le nombre de pare-feu que vous gérez à l'aide de Panorama augmente.

STEP 4 | Si vous déployez des pare-feu sur des sites distants avec peu ou pas de personnel informatique, configurez le Zero Touch Provisioning (ZTP) pour rationaliser le déploiement de pare-feu initial en automatisant l'intégration de nouveaux pare-feu gérés sans avoir besoin d'administrateurs réseau ou informatiques sur le site distant.

Cas d'utilisation : migration de vos nouveaux pare-feu nouvelle génération vers Panorama

Le deuxième cas d'utilisation pour démarrer avec le serveur de gestion Panorama™ est la transition des pare-feu existants vers Panorama. Si possible, collaborez avec votre ingénieur commercial ou ingénieur des services professionnels de Palo Alto Networks pendant la migration pour vous assurer que vos configurations de pare-feu sont correctement migrées vers Panorama.

STEP 1 | La planification est essentielle. Avant de commencer la migration, assurez-vous de bien avoir compris ce qui suit :

- Passez en revue la matrice de compatibilité de Palo Alto Networks pour comprendre la compatibilité entre Panorama et les pare-feu, entre les collecteurs de journaux et les versions de contenu afin de vous assurer qu'aucune erreur de compatibilité n'est rencontrée pendant la migration.
- Planifiez la hiérarchie de vos groupe d'appareils et modèlesde manière à réduire la redondance et à rationaliser la gestion des paramètres qui sont partagés entre tous les pare-feu au sein d'un ensemble de pare-feu.
- Préparez un plan de test post-migration afin de vérifier le trafic critique et le trafic des applications après la migration réussie de votre pare-feu vers Panorama.

STEP 2 | Lorsque vous migrez un pare-feu vers la gestion Panorama, activez **Import devices' shared objects into Panorama's shared context (Importer les objets partagés des périphériques dans le contexte partagé de Panorama)** pour éviter de dupliquer des objets de configuration identiques.

STEP 3 | Après une migration réussie, passez en revue les **Policies (Politiques)** afin d'identifier toute règle en double. Supprimez un exemplaire de chaque règle en double avant de cliquer sur **Commit (Valider)** dans Panorama pour éviter de valider des erreurs.

STEP 4 | Lorsque vous cliquez sur **Export or push device config bundle (Exporter ou appliquer la solution de configuration des périphériques)** vers vos pare-feu gérés, activez **Merge with Candidate Config (Fusionner avec la configuration du candidat)**, **Include Device and Network Templates (Inclure les modèles de réseaux et de périphériques)** et **Force Template Values (Forcer les valeurs du modèle)** pour forcer une validation pour toute modification locale en attente sur le pare-feu, inclure tous les groupes d'appareils et les modèles dans l'application et supprimer toute configuration locale non présente dans un groupe d'appareils ou un modèle sur Panorama. Cela garantit qu'une configuration de base gérée par Panorama est appliquée à tous les pare-feu migrés vers Panorama.

STEP 5 | Effectuez vos tests post-migration pour vérifier que la migration est réussie et que tout fonctionne comme prévu. Au fil du temps, optimisez la configuration selon vos besoins. Utilisez des outils de migration comme Expedition pour évaluer périodiquement l'hygiène de votre configuration en supprimant tout objet inutilisé ou en double et l'Optimiseur de politique pour optimiser votre base de règles de politique de sécurité.

Meilleures pratiques pour la gestion de la configuration des pare-feu sur Panorama

Les pare-feu disposent de deux types de configuration : sécurité et réseau. Panorama utilise des groupes d'appareils pour gérer les configurations de sécurité, tels que les objets et les règles de politique, ainsi que des modèles et des piles de modèles pour gérer les configurations de réseau.

- Gestion des configurations de vos groupes d'appareils sur Panorama
- Gestion de la configuration de votre modèle et de votre pile de modèles sur Panorama
- Gestion des variables de modèles et de piles de modèles sur Panorama

Gestion des configurations de vos groupes d'appareils sur Panorama

Les groupes d'appareils permettent d'organiser et de réutiliser vos politiques en appliquant le principe de l'héritage et en mettant en œuvre une hiérarchie de groupes d'appareils bien définie. Bien que Panorama vous permette de réutiliser la même configuration de groupe d'appareils pour plusieurs groupes d'appareils dans une hiérarchie, vous pouvez également personnaliser toute configuration locale pour remplacer toute configuration héritée.

- Lorsque vous concevez votre hiérarchie de groupes d'appareils, tenez compte de vos besoins fonctionnels ou régionaux et comprenez la différence entre les règles « avant » et les règles « après ».

  Par exemple, créez des règles « avant » de sécurité que vous souhaitez que les pare-feu gérés appliquent sans exception, tout en créant des règles « après » de sécurité pour nettoyer le trafic qui ne correspond pas à une règle « avant » de sécurité.
- Évitez la surutilisation du groupe d'appareils **Shared (Partagé)** afin de ne pas dépasser les limites de capacité des pare-feu gérés de plus petite taille. La gestion des objets de configuration au niveau du groupe d'appareils approprié permet de réduire le nombre de pare-feu `Out of Sync (Désynchronisés)` de manière plus efficace, car tous les pare-feu deviennent `Out of Sync (Désynchronisés)` si un seul objet de configuration partagé est modifié.
- Configurez des régions personnalisées en utilisant des objets d'adresse personnalisés pour spécifier des plages d'adresses ou des géolocalisations.

  Bien que les entreprises utilisent l'espace d'adressage RFC 1918, les politiques régissant l'ensemble du réseau 10.0.0x ne sont pas utiles. Définissez plutôt des régions personnalisées en utilisant des objets d'adresse personnalisés pour spécifier des plages d'adresses ou des géolocalisations. Cela vous permet de créer des politiques plus granulaires et plus pertinentes pour réduire votre surface d'attaque.
- Configurez le **Master Device (Périphérique principal)** pour chaque groupe d'appareils afin de permettre à Panorama de rassembler les mappages de groupes d'utilisateurs. La configuration d'un périphérique principal dans le groupe d'appareils rend les groupes d'utilisateurs disponibles lors de la création de règles de politique. De plus, vous pouvez filtrer les onglets ACC et Monitor (Surveiller) en utilisant les mappages de groupes d'utilisateurs rassemblés par Panorama.
- Associez des **Reference Templates (Modèles de référence)** pour faire référence aux objets de configuration réseau contenus dans un modèle auquel le pare-feu géré n'appartient pas afin de compléter une configuration de sécurité. Cela vous permet de tirer pleinement parti des objets de configuration communs à des groupes d'appareils et modèles sans surutiliser le groupe d'appareils **Shared (Partagé)** ni recréer des objets de configuration réseau identiques.

Gestion de la configuration de votre modèle et de votre pile de modèles sur Panorama

Utilisez les modèles et les piles de modèles pour réutiliser vos objets de configuration de pare-feu et de réseau à travers vos pare-feu gérés pour les paramètres communs tels que la journalisation et la haute disponibilité (HA) tout en vous permettant de configurer des modèles modulaires qui peuvent être combinés selon les besoins pour plusieurs pare-feu gérés dans différentes piles de modèles.

- Optez pour la modularité en créant des modèles avec des regroupements logiques de paramètres, même si la configuration est incomplète. N'oubliez pas que la configuration doit être complète et que toutes les références doivent être résolues au niveau de la pile de modèles, et non pas au niveau de chaque modèle. Vous pouvez réutiliser, référencer et remplacer des objets de différents modèles pour compléter la configuration de la pile de modèles.
- Créez des modèles spécifiques à un modèle (par exemple, la configuration de l'interface réseau) et utilisez des modèles spécifiques à un cas (par exemple, les admins, les ensembles de contrôle d'accès basés sur les rôles). Cela vous permet de mélanger et de combiner les bons modèles lorsque vous les ajoutez à une pile de modèles.
- Configurez la pile de modèles avec les configurations réseau que vous souhaitez remplacer dans un modèle ou localement sur le pare-feu géré.

Gestion des variables de modèles et de piles de modèles sur Panorama

Créez des variables de modèles et de piles de modèles pour maximiser le partage de configuration et la réutilisation des objets de configuration de réseau et d'appareils à travers vos pare-feu gérés.

- Utilisez des variables de modèles et de piles de modèles lorsque cela est approprié pour vous aider à gérer la configuration de vos pare-feu gérés avec moins de modèles et à rationaliser votre configuration.

  Par exemple, les adresses IP diffèrent généralement d'un pare-feu à l'autre. En utilisant des variables de modèles, vous pouvez créer la configuration dont vous avez besoin en spécifiant une variable au lieu d'une adresse IP. Lorsque la configuration est appliquée à vos pare-feu gérés, Panorama peut renseigner la bonne adresse IP par pare-feu en fonction de la valeur configurée par pare-feu géré.
- Créez des variables avec la valeur par défaut **`None (Aucun)`** pour vous assurer que la mauvaise configuration n'est pas accidentellement appliquée au pare-feu géré.

  Une exception notable à cela est l'adresse IP du DNS. Dans le pire des cas, le pare-feu géré devrait toujours être en mesure de résoudre les requêtes DNS.

Meilleures pratiques pour la gestion des modifications de configuration

Gérez les modifications de configuration que vos administrateurs peuvent apporter en exploitant le contrôle d'accès basé sur les rôles (RBAC) et en segmentant l'accès aux pare-feu gérés, en utilisant des structures dynamiques, telles que les listes dynamiques externes (EDL) et les groupes d'utilisateurs dynamiques (DAG), pour maintenir les règles de politique à jour, et en exploitant un contrôle granulaire sur les modifications de configuration que les administrateurs peuvent apporter aux pare-feu gérés.

- Gestion des rôles admin et des domaines d'accès depuis Panorama
- Simplification des règles de sécurité gérées par Panorama
- Gestion des modifications de configuration pour les grandes équipes
- Validation de vos modifications de configuration Panorama
- Application de vos modifications de configuration Panorama

Gestion des rôles admin et des domaines d'accès depuis Panorama

Une des clés de la réussite de la gestion de la configuration dans un environnement dynamique est de pouvoir attribuer les privilèges appropriés aux membres de votre équipe. Panorama offre un contrôle d'accès basé sur les rôles (RBAC) étendu qui permet une définition granulaire des rôles. Le RBAC peut être combiné avec des domaines d'accès pour faciliter la segmentation de l'accès aux pare-feu gérés. Cela permet de réduire votre surface d'attaque et d'éviter un abus accidentel ou malveillant des privilèges d'administrateur.

Consultez les meilleures pratiques pour l'accès administratif de sécurité afin d'obtenir des informations plus détaillées sur le contrôle adéquat de l'accès à votre Panorama et aux configurations de pare-feu gérés.

- Définissez des rôles administrateurs pour aider les administrateurs à gérer avec succès les pare-feu sans surapprovisionner leur accès.
- Créez des domaines d'accès pour vos administrateurs Panorama si vous disposez de plusieurs sous-ensembles de pare-feu servant à des fins différentes. Par exemple, si vos pare-feu de centre de données, pare-feu de périmètrie et pare-feu de succursales sont gérés par différents administrateurs Panorama, configurez et attribuez des domaines d'accès qui limitent l'accès aux seuls pare-feu qu'ils gèrent.
- Créez des administrateurs de groupes d'appareils et de modèles pour mieux contrôler l'accès administrateur aux pare-feu gérés dans un domaine d'accès et un rôle admin. Cela offre l'accès le plus granulaire qui permet à votre équipe de faire son travail sans causer de problèmes opérationnels.

Simplification des règles de sécurité gérées par Panorama

La gestion de votre politique de sécurité est l'une des tâches les plus importantes dans la gestion de votre base de règles de politique.

- Pour que votre base de règles soit sensible aux applications, utilisez une combinaison de l'optimiseur de politique et de l'utilisation de la règle de politique pour passer à des règles de politique de sécurité basées sur App-ID et User-ID.

  Créez des groupes d'utilisation dans vos règles de politique de sécurité pour les rendre plus efficaces et plus lisibles. De plus, vous pouvez utiliser les outils Expédition et Évaluation des meilleures pratiques (BPA) pour vous aider à itérer à travers les révisions de votre base de règles afin de renforcer votre posture de sécurité.
- Utilisez la Recherche globale lorsque vous évaluez votre base de règles de politique pour identifier les objets ou les règles qui peuvent déjà exister. Cela vous aidera à réduire l'encombrement inutile de votre configuration qui, au final, ralentit les validations sur Panorama.
- Dépannez vos règles de politique pour vérifier si une modification proposée de la configuration des règles de politique est déjà traitée par une règle existante qui ne nécessite qu'une modification. Cela vous permet de réduire les doublons de règles de politique et d'éviter que votre base de règles de politique ne devienne trop importante.
- Utilisez des groupes de règles à base d'étiquettes pour identifier l'objectif, la fonction, le cycle de vie ou d'autres caractéristiques des règles afin de les trier et de les regrouper rapidement. Les groupes de règles à base d'étiquettes vous permettent de distinguer visuellement les ensembles de règles au sein d'une base de règles où elles peuvent être gérées en tant que groupe. Vous pouvez aussi modifier individuellement une seule règle du groupe.
- Appliquez des commentaires d'audit pour la création et la modification de règles de politique afin de soutenir la fonction opérationnelle essentielle de soutien aux audits de sécurité. Une règle comportant une série bien documentée de commentaires d'audit permet de répondre plus facilement à une requête d'audit au lieu de s'appuyer sur des descriptions de règles ou des outils externes. De plus, vous pouvez compléter les commentaires d'audit en saisissant une description lorsque vous validez des modifications de configuration dans Panorama.
- Utilisez des constructions dynamiques comme les listes dynamiques externes, les groupes d'adresses dynamiques et les groupes d'utilisateurs dynamiques pour rationaliser votre configuration et simplifier la maintenance de votre base de règles de politique de sécurité. Au fur et à mesure que votre environnement change, vous pouvez les modifier si nécessaire sans avoir à les valider.
- Lors de la création de votre règle de politique de sécurité, évitez de sélectionner un ou plusieurs pare-feu gérés dans l'onglet **Target (Cible)**, car cela rend l'état de synchronisation de la configuration des pare-feu gérés peu fiable.

  C'est ce que l'on appelle communément le ciblage de politiques. Le ciblage de politiques est évalué sur le pare-feu et non sur Panorama. Par conséquent, les pare-feu gérés pour lesquels une règle de politique n'est pas appliquée peuvent s'afficher comme étant `Out of Sync (Désynchronisés)` de façon erronée. Concevez la hiérarchie de vos groupes d'appareils pour minimiser ou éviter la nécessité de cibler les politiques.

Gestion des modifications de configuration pour les grandes équipes

Des erreurs de configuration se produisent lorsqu'une grande équipe utilise Panorama pour une gestion centralisée de la configuration. Panorama permet une manipulation granulaire en utilisant les opérations de configuration de rétablissement, d'importation, d'exportation, de chargement, de fusion et de remplacement. Ces opérations sont réalisées au niveau d'un groupe d'appareils ou d'un modèle.

- Lorsque vous essayez de rétablir rapidement la configuration Panorama à un état précédemment connu, pensez à ne rétablir que le groupe d'appareils ou le modèle impacté au lieu de la totalité de la configuration Panorama.

  Cela vous permet de préserver les modifications apportées par d'autres administrateurs qui n'ont pas apporté de modifications à la configuration du groupe d'appareils ou du modèle impacté. En outre, vous pouvez exporter la configuration pour la modifier hors ligne, puis la réimporter dans Panorama lorsque vous êtes prêt.
- Exportez les modifications de configuration en cours de groupes d'appareils et de modèles afin d'appliquer les modifications de configuration d'urgence aux pare-feu gérés. Après l'exportation, rétablissez la configuration Panorama pour effectuer les modifications d'urgence. Lorsque les modifications sont appliquées avec succès aux pare-feu gérés, vous pouvez importer la configuration Panorama qui inclut les modifications de configuration en cours.
- Si vous consolidez plusieurs configurations Panorama, fusionnez tactiquement vos configurations de groupes d'appareils et de modèles pour consolider la configuration sur un seul Panorama.

Validation de vos modifications de configuration Panorama

Panorama vous propose de nombreuses façons de contrôler le processus de validation. Il est utile de les comprendre et de les adopter dans vos opérations quotidiennes.

- Lorsque vous validez des modifications de configuration Panorama, sélectionnez **Commit Changes Made by (Valider les modifications apportées par)** pour ne valider que vos propres modifications et non celles des autres administrateurs. Cela garantit que les autres modifications de configuration en cours ou non encore approuvées ne sont pas validées par erreur dans Panorama.
- Lorsque vous validez des modifications de configuration, demandez aux administrateurs de cliquer sur **Preview Changes (Prévisualiser les modifications)** et de passer en revue le résumé des modifications. Une vérification visuelle des modifications de configuration permet souvent de détecter les erreurs et de gagner du temps dans la maintenance opérationnelle ultérieure.

Application de vos modifications de configuration Panorama

Panorama propose de nombreuses façons de contrôler l'application des modifications de configuration vers les pare-feu gérés. Il est utile de les comprendre et de les adopter dans vos opérations quotidiennes.

- Avant que les administrateurs n'appliquent des modifications de configuration aux pare-feu gérés, demandez-leur de passer en revue la sélection de la portée de l'application afin de vérifier que la liste des pare-feu cibles est correcte : **Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** > **Edit Selections (Modifier les sélections)**.

  Même si la hiérarchie des groupes d'appareils est conçue correctement et que les modifications de configuration sont bien planifiées, il peut y avoir des scénarios où les modifications de configuration n'ont pas besoin d'être appliquées à tous les pare-feu à un moment donné en raison des différentes fenêtres de maintenance Il est toujours préférable de passer en revue la liste des pare-feu cibles pour s'assurer que les modifications de configuration ne sont appliquées qu'aux pare-feu gérés prévus.
- Utilisez le paramètre **Force Template Values** (Forcer les valeurs du modèle) (**Commit (Valider)** > **Push to Devices (Appliquer aux périphériques)** > **Edit Selections (Modifier les sélections)**) avec modération. En cas d'application avec ce paramètre activé, cela écrase l'ensemble de la configuration du pare-feu géré, y compris toute configuration de pare-feu locale.

Meilleures pratiques pour la surveillance et la visibilité sur Panorama

Concevez votre infrastructure de journalisation pour une ingestion et un stockage optimal des journaux en fonction de vos besoins organisationnels. Ensuite, utilisez le centre de commande des applications (ACC), les rapports récapitulatifs au format PDF et les rapports personnalisés pour identifier l'activité du réseau et les menaces qui doivent être étudiées et résolues.

- Conception de votre infrastructure de journalisation
- Surveillance du centre de commande des applications (ACC) et des journaux sur Panorama
- Génération de rapports standards et personnalisés sur Panorama

Conception de votre infrastructure de journalisation

Il est recommandé de planifier et de concevoir votre infrastructure de journalisation avant de déployer de nouveaux pare-feu gérés. Le serveur de gestion Panorama offre plusieurs modes de gestion des périphériques et de collecte des journaux. Le mode Panorama vous permet à la fois de gérer la configuration de votre pare-feu et d'ingérer et de stocker les journaux. Si vous souhaitez que votre Panorama ait une seule fonction, le mode Collecteur de journaux est conçu uniquement pour l'ingestion et le stockage des journaux tandis que le mode Gestion uniquement est conçu uniquement pour la gestion de la configuration du pare-feu.

- Utilisez le Guide de dimensionnement et de conception de Panorama pour calculer le taux de journalisation et déterminer vos besoins en matière de stockage de journaux. Cela est important pour décider de la capacité de stockage de journaux de vos collecteurs de journaux et peut reposer sur de nombreux facteurs tels que les exigences réglementaires.

  Consultez votre ingénieur avant-vente (SE) lors du dimensionnement de votre infrastructure de journalisation. Il vous apportera l'expertise technique nécessaire pour interpréter et personnaliser votre déploiement en fonction de vos besoins.
- N'utilisez pas le mode hérité si vous déployez un appareil virtuel Panorama en raison des nombreuses limitations et restrictions de journalisation associées à ce mode. Bien qu'il convienne à un environnement de laboratoire ou de démonstration, évitez d'utiliser un Panorama en mode hérité dans votre environnement de production.
- Utilisez une interface distincte pour la collecte de journaux sur vos pare-feu gérés. Cela vous aidera à maintenir les performances de votre interface de gestion qui communique avec Panorama. Comme bonne pratique de sécurité, configurez une liste d'IP autorisées pour toutes les interfaces.

Surveillance du centre de commande des applications (ACC) et des journaux sur Panorama

Le centre de commande des applications (ACC) est un outil de visualisation interactif conçu pour vous aider à comprendre rapidement les événements de votre réseau. L'ACC contextualise les journaux de vos pare-feu gérés pour vous permettre de mieux comprendre les tendances de trafic et les informations exploitables sur les menaces que vous pouvez utiliser dans vos enquêtes.

- ❑ Apprenez à utiliser toutes les interactions de données à votre disposition dans l'ACC.
  - Utilisez les filtres de l'ACC pour rechercher des informations spécifiques telles que des adresses ou des utilisateurs.
  - Appliquez des filtres globaux pour faire pivoter l'affichage de l'ACC autour des détails qui vous intéressent le plus et exclure les informations sans lien.
  - Si vous utilisez GlobalProtect, consultez le widget **GlobalProtect Activity (Activité GlobalProtect)** pour afficher les rapports HIP basés sur les journaux de correspondance HIP afin de comprendre l'état de sécurité des périphériques finaux qui accèdent à votre réseau.
  - Une fois que vous avez réduit les informations qui vous intéressent, cliquez sur **Export (Exporter)** pour exporter vos données ACC au format CSV ou les widgets au format PDF pour les partager avec votre équipe intéressée par une enquête plus approfondie ou des corrections.
- ❑ Personnalisez l'ACC pour vous assurer qu'il est adapté à l'activité spécifique du réseau que vous souhaitez surveiller.

  Cela vous aidera à améliorer votre efficacité lorsque vous enquêtez sur un utilisateur ou un hôte particulier. Vous pourrez ainsi disposer d'informations contextuelles complètes sans avoir à changer d'onglet ou à faire défiler trop loin.
  - Ajoutez un nouveau widget à l'ACC et sélectionnez **Content Activity (Activité de contenu)**.
  - Ajoutez un nouveau widget à l'ACC et sélectionnez **URL Filtering (Filtrage des URL)**.
  - Par défaut, le widget **Threat Activity (Activité des menaces)** est affiché. S'il n'est pas affiché, ajoutez un nouveau widget et sélectionnez **Threat Activity (Activité des menaces)**.
- ❑ Sélectionnez **Objects (Objets)** > **Regions (Régions)** et créez des régions personnalisées avec des plages d'adresses IP à utiliser dans vos règles de politique de sécurité. L'utilisation de régions personnalisées rend plus pertinents les événements réseau corrélés dans l'ACC.

  Par exemple, vous avez configuré des régions personnalisées pour vos succursales et vous remarquez que certaines adresses IP sont responsables d'une grande quantité de trafic suspecte. En exploitant les régions personnalisées, vous pouvez corréler cette activité réseau suspecte avec une succursale spécifique et prendre des mesures pour enquêter et prendre des mesures correctives.

Génération de rapports standards et personnalisés sur Panorama

Le serveur de gestion Panorama™ vous permet de centraliser et d'agréger toutes les informations à travers votre déploiement de pare-feu afin de générer des rapports PDF et de créer des rapports personnalisés.

- Identifiez et classez toutes les applications SaaS utilisées par votre organisation comme étant **Sanctioned (Approuvées)** ou **Unsanctioned (Non approuvées)**.

  Panorama et les pare-feu gérés considèrent toute application sans l'étiquette Sanctioned (Approuvée) comme non approuvée pour une utilisation sur le réseau. Les applications SaaS non approuvées peuvent entraîner une exposition à des menaces, ainsi que la perte de données privées et sensibles. Il est important de classer vos applications SaaS pour mieux étudier l'activité du réseau.

  1. Sélectionnez **Objects (Objets)** > **Applications (Applications)**.
  2. Créez une application SaaS personnalisée, au besoin.
  3. Sélectionnez une ou plusieurs de vos applications SaaS et cliquez sur **Edit Tags (Modifier les étiquettes)**.
  4. Dans la liste déroulante Add Tags (Ajouter des étiquettes), sélectionnez **Sanctioned (Approuvée)** ou **Unsanctioned (Non approuvée)**.
  5. Répétez les étapes 1 à 4 jusqu'à ce que vos applications SaaS soient étiquetées selon vos besoins.
  6. Sélectionnez **Commit (Valider)** > **Commit and Push (Valider et appliquer)** puis cliquez sur **Commit and Push (Valider et appliquer)** pour les modifications de configuration.
- Configurez le rapport d'activité des utilisateurs et le rapport d'utilisation des applications SaaS sur la base de groupes d'utilisateurs pour obtenir un niveau de granularité plus élevé dans vos rapports.

  Par exemple, votre service des finances stocke une grande quantité de données dans GitHub. L'utilisation de groupes d'utilisateurs dans vos rapports d'activité des utilisateurs et d'utilisation des applications SaaS vous permet d'identifier plus facilement ce comportement suspect. Sinon, ce comportement suspect peut passer inaperçu si le rapport est exécuté pour l'ensemble de l'organisation.
- Configurez des rapports personnalisés spécifiques et axés sur des objectifs, et limitez le nombre de colonnes à ce qui est nécessaire.

  Des paramètres de rapport précis vous permettent d'identifier plus facilement l'activité du réseau qui doit faire l'objet d'une enquête.

  Lorsque vous créez un rapport personnalisé, utilisez si possible le générateur de requêtes pour affiner rapidement les résultats.

  Par exemple, un rapport ciblé pour un emplacement de bureau est beaucoup plus efficace et exploitable qu'un rapport pour l'ensemble des emplacements de bureaux. Si vous avez besoin d'un rapport qui englobe plusieurs bureaux, il est préférable d'exécuter quelques rapports différents avec des requêtes spécifiques pour chaque bureau.