paloalto TECHDOCS

Meilleures pratiques pour une migration vers une politique basée sur les applications

Version 10.1

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

- 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

December 4, 2023

Table of Contents

Meilleures pratiques pour une migration vers une politique basée sur les applications

Nul besoin de renoncer à la meilleure sécurité pour accéder aux applications. Utilisez plutôt les logicielsExpedition et Policy Optimizer pour automatiser et réduire le temps et les efforts requis pour migrer d'une politique de sécurité basée sur des ports avec un pare-feu traditionnel vers une politique de sécurité basée sur une application avec un pare-feu nouvelle génération de Palo Alto Networks ou avec Panorama, de manière progressive et sécurisée.

- Activation en toute sécurité des applications à l'aide d'une transition progressive
- Migration d'une politique basée sur les ports vers PAN-OS à l'aide du logiciel Expedition
- Migration vers une politique basée sur les applications à l'aide de Policy Optimizer
- Prochaines étapes pour adopter les meilleures pratiques en matière de sécurité

Après avoir migré l'ancienne politique vers une politique basée sur les applications, utilisez le rapport BPA à la demande dans Strata Cloud Manager pour identifier les domaines où améliorer la sécurité, utilisez le résumé d'adoption pour identifier les lacunes dans l'adoption des capacités de sécurité et visitez le portail de documentation sur les meilleures pratiques, qui fournit des étapes spécifiques de planification, de déploiement et de maintenance des meilleures pratiques pour une multitude de fonctionnalités, capacités et objectifs de sécurité, notamment :

- Décryptage (vous ne pouvez pas vous défendre contre les menaces sur lesquelles vous n'avez aucune visibilité)
- Politique de sécurité (inclut la construction de règles de politique de sécurité, l'ordre et l'hygiène des bases de règles, le moteur App-ID Cloud Engine (ACE), l'optimiseur de politique, la recommandation de politique SaaS et la recommandation de politique IoT)
- Zero Trust (comment verrouiller votre réseau)
- DoS et protection de zone (y compris Packet Buffer Protection)
- Accès administratif (protégez l'accès aux pare-feu et périphériques de gestion)
- Meilleures pratiques IoT
- Les meilleures pratiques pour le déploiement de WildFire
- Meilleures pratiques pour les mises à jour du contenu de menace et des applications

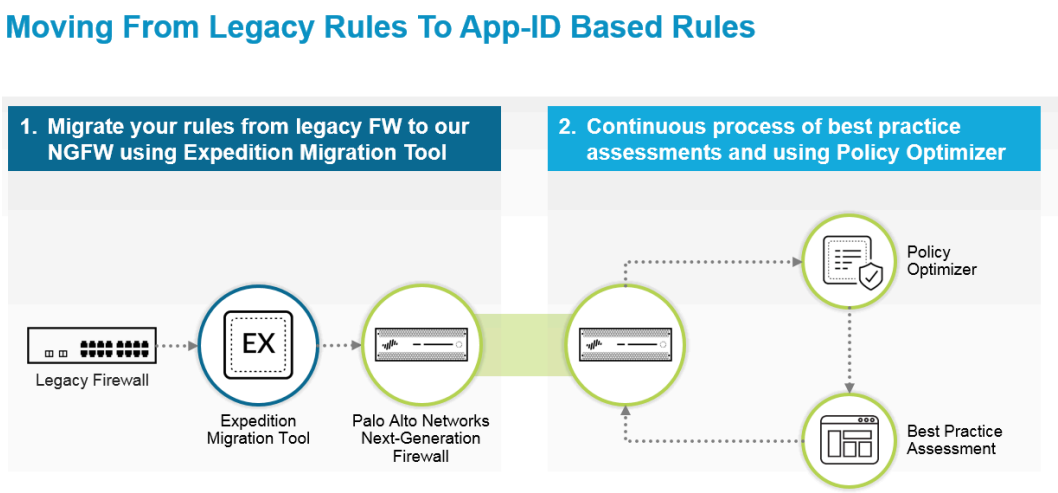
Assurez-vous également que vous disposez des abonnements appropriés pour prendre en charge la sécurité de votre réseau, y compris la prévention des menaces avancées, la sécurité DNS, le filtrage avancé des URL, la sécurité IoT, GlobalProtect, la sécurité SaaS, etc.

Activation en toute sécurité des applications à l’aide d’une transition progressive

Les vulnérabilités flagrantes de la politique de sécurité basée sur un port sont bien connues : vous ne pouvez pas savoir quelles applications utilisent un port. Ainsi, toute application malveillante peut accéder à votre réseau sur des ports ouverts tels que le port 80 (HTTP) ou le port 53 (DNS). Cela permet aux pirates d’installer plus facilement des logiciels malveillants, de se déplacer latéralement sur le réseau, d’exfiltrer des données et de compromettre votre réseau, car vous n’avez aucune visibilité sur les applications de votre réseau ni aucune possibilité d’empêcher les menaces cachées par leur trafic.

En revanche, la politique de sécurité basée sur une application utilisant App-ID™ offre une visibilité sur les applications, quels que soient le port, le protocole, le chiffrement (SSL ou SSH) ou les tactiques d’évasion, afin que vous sachiez exactement quelles applications se trouvent sur votre réseau et que vous puissiez contrôler leur trafic pour les menaces. Les politiques spécifiques aux applications permettent un accès sécurisé, car vous pouvez configurer des règles de politique de sécurité permettant uniquement aux utilisateurs appropriés d’accéder aux applications appropriées aux emplacements appropriés. Vous pouvez également leur appliquer des profils de prévention des menaces. L’utilisation d’App-ID pour classer les applications réduit la surface d’attaque, car vous n’autorisez que les applications requises pour prendre en charge vos activités sur le réseau et bloquez automatiquement les applications indésirables. Autoriser ce que vous voulez et bloquer tout le reste est beaucoup plus facile et plus sûr que d’essayer sans fin de bloquer toutes les applications individuelles que vous ne voulez pas.

Migrez par étapes vers App-ID :



1. Utilisez Expedition pour importer une base de règles traditionnelle, la nettoyer et effectuer une migration similaire vers un équipement Panorama ou un pare-feu nouvelle génération de Palo Alto Networks. Expedition est distribué en tant que machine virtuelle (VM).
2. Exécutez l’équipement ou le pare-feu PAN-OS dans votre environnement de production réseau afin qu’il puisse apprendre et classer les applications sur votre réseau.
3. Après au moins une semaine de journalisation du trafic, exécutez le Best Practice Assessment (BPA) pour définir une base de référence, puis utilisez Policy Optimizer pour commencer à convertir en toute sécurité des règles basées sur un port en règles basées sur une application et à sécuriser votre réseau. (Vous pouvez convertir certaines règles simples autorisant des applications bien connues après environ une semaine. Pour les autres règles qui voient de nombreuses applications, telles qu’une règle

générale d'accès Internet sortant, attendez au moins 30 jours pour collecter des informations sur les applications.) Adoptez une approche progressive pour convertir en toute sécurité les règles en fonction des besoins et des priorités de votre entreprise.

4. (Facultatif) Après avoir utilisé Policy Optimizer, convertissez la base de règles en App-ID, réimportez la configuration dans Expedition et utilisez les fonctionnalités d'enrichissement de règles pour simplifier et affiner la base de règles.
5. Poursuivez le déploiement d'App-ID lorsque vous introduisez de nouvelles applications sur votre réseau. Exécutez le BPA après le passage de la première conversion via les règles basées sur un port et périodiquement par la suite pour mesurer les progrès et découvrir d'autres domaines afin d'améliorer la sécurité.

Policy Optimizer est disponible à partir de PAN-OS 9.0. Si vous utilisez Panorama pour gérer vos pare-feu nouvelle génération, vous n'avez pas besoin de mettre à niveau les pare-feu gérés vers PAN-OS 9.0 pour utiliser Policy Optimizer. Il vous suffit de mettre à niveau Panorama vers PAN-OS 9.0, d'envoyer les journaux du trafic des pare-feu gérés vers Panorama ou les Log Collectors exécutant PAN-OS 9.0, et de transmettre la politique de Panorama aux pare-feu. Les pare-feu gérés doivent exécuter PAN-OS 8.1 ou version ultérieure et, s'ils se connectent à des Log Collectors, ceux-ci doivent exécuter PAN-OS 9.0. Cela fournit un raccourci pour la qualification afin que vous puissiez utiliser Policy Optimizer pour adopter rapidement une politique basée sur App-ID.

Strata Logging Service prend en charge Policy Optimizer sur les périphériques Panorama qui exécutent PAN-OS 10.0.4 ou version ultérieure avec le plug-in Cloud Services 2.0 ou version ultérieure.

Les pare-feu PA-7000 Series prennent en charge deux cartes de journalisation : la Log Processing Card (carte de traitement des journaux ; LPC) du pare-feu PA-7000 et la Firewall Log Forwarding Card (carte de transfert des journaux ; LFC) du pare-feu PA-7000 à haut rendement. Contrairement à la LPC, la LFC ne dispose pas de disques pour stocker les journaux localement. La LFC transfère plutôt tous les journaux vers un ou plusieurs systèmes de journalisation externes, comme Panorama ou un serveur syslog. Si vous utilisez la LFC, les informations relatives à l'utilisation de l'Optimiseur de politique ne s'affichent pas sur le pare-feu, parce que les journaux de trafic ne sont pas stockés localement. Si vous utilisez la LPC, les journaux du trafic sont stockés localement sur le pare-feu. Les informations relatives à l'utilisation de Policy Optimizer s'affichent donc sur le pare-feu. Dans les deux cas, le pare-feu PA-7000 peut exécuter PAN-OS 8.1 (ou une version ultérieure) tant que les Log Collectors et Panorama exécutent PAN-OS 9.0 ou une version ultérieure.

Migration d’une politique basée sur les ports vers PAN-OS à l’aide du logiciel Expedition

Utilisez Expedition pour importer une base de règles traditionnelle, la nettoyer et effectuer une migration similaire vers Panorama ou un pare-feu nouvelle génération de Palo Alto Networks en tant que première phase de votre migration vers une politique de sécurité basée sur les applications. Expedition est un excellent outil pour effectuer des opérations en bloc sur plusieurs objets dans une configuration et prend en charge l’importation de configurations traditionnelles de la plupart des principaux fournisseurs de pare-feu.

Cette rubrique résume le processus utilisé par Expedition. La Live community fournit une assistance pour le logiciel Expedition, notamment sur la façon d’obtenir l’outil et la documentation détaillée sur la façon d’utiliser l’outil.

Le support technique de Palo Alto Networks (TAC) ne fournit pas d’aide pour Expedition.

Pour plus de détails sur les processus de migration d’Expedition, reportez-vous au Guide de l’utilisateur Expedition, qui contient également des informations sur la manière d’importer des objets dans une configuration à l’aide de fichiers CSV et une configuration Iron-Skillet de Jour 1.

Pour gérer Expedition, reportez-vous au Guide de l’administrateur Expedition, qui contient également des informations sur l’interface utilisateur, ainsi qu’au Guide de renforcement Expedition, qui fournit des conseils sur la manière de protéger la machine virtuelle Expedition.

Avant de commencer une migration, assurez-vous de respecter les conditions préalables suivantes :

- Téléchargez Expedition sur un serveur d’administration prenant en charge l’exécution d’une machine virtuelle.
- Assurez-vous de la connectivité SSH et/ou SSL aux pare-feu et Panorama de Palo Alto Networks vers lesquels vous effectuez la migration. Assurez-vous que l’accès SSH est destiné à la connectivité à la CLI et l’accès SSL à la connectivité à l’interface Web et aux commandes API de poussée.
- Assurez-vous de l’accès opérationnel aux pare-feu et Panorama de Palo Alto Networks vers lesquels vous effectuez la migration, de sorte que vous puissiez appliquer la configuration similaire à l’équipement PAN-OS.

Le groupe Professional Services possède une riche expérience de migration. Vous pouvez faire appel à l’équipe des Professional Services pour vous aider à migrer une configuration de vos équipements traditionnels vers les équipements Panorama et les pare-feu nouvelle génération de Palo Alto Networks.

STEP 1 | Vérifiez la configuration du pare-feu héritée.

Comprenez les objectifs de la base de règles traditionnelle. Documentez les éléments à connaître pour la migration, tels que les interfaces désactivées sur un équipement Juniper SRX ou la vérification de l’autorisation du trafic entre les interfaces avec les mêmes niveaux de sécurité, la vérification de l’état des tunnels IPSec et la collecte de clés prépartagées sur un équipement Cisco ASA.

STEP 2 | Importez la configuration traditionnelle dans Expedition et apportez les modifications nécessaires à la configuration.

STEP 3 | Créez un nouveau **Project** (Projet) dans Expedition.

STEP 4 | Importez la configuration source (traditionnelle) migrée dans le **Project** (Projet) et inspectez-la.

Vérifiez le format de fichier, assurez-vous de la présence de tous les fichiers requis et contrôlez les journaux et événements Expedition pour vous assurer que le fichier de configuration migré est correctement chargé. Si nécessaire, modifiez le fichier source migré pour résoudre des problèmes, puis vérifiez à nouveau. Répétez cette étape jusqu'à ce que tous les problèmes soient résolus.

STEP 5 | Importez une configuration PAN-OS dans le **Project** (Projet) pour qu'elle soit la configuration de base pour la migration.

Obtenez les dernières mises à jour du contenu puis importez la configuration de base à partir d'un équipement PAN-OS existant, (un fichier de configuration existant ou le fichier de configuration PAN-OS par défaut).

Le fichier de configuration doit correspondre à la version PAN-OS que vous souhaitez utiliser. Par exemple, pour exécuter PAN-OS 9.0, importez un fichier de configuration de PAN-OS 9.0.

STEP 6 | Nettoyez la configuration migrée pour préparer la fusion avec la configuration PAN-OS de base.

- Supprimez ou remplacez des objets de service non valides. PAN-OS ne reconnaît que les ports de service TCP et UDP et Expedition migre automatiquement les objets de service TCP et UDP vers les applications. Recherchez des applications et des services non basés sur IP, tels que ping et ICMP, que certains équipements traditionnels considèrent comme des services plutôt que des applications. Remplacez-les par App-ID pour les classer comme des applications et obtenir une visibilité sur le trafic, l'inspecter et le contrôler.
- Pour simplifier la configuration et réduire sa taille, supprimez ou remplacez les autres objets non valides et inutilisés et fusionnez les objets en double.
- Recherchez et supprimez les règles désactivées pour ne pas encombrer la configuration.
- Renommez les interfaces pour qu'elles correspondent aux interfaces de l'équipement PAN-OS. Les noms d'interface importés à partir de l'équipement traditionnel ne correspondent généralement pas aux conventions de dénomination PAN-OS.
- Lorsque vous importez la configuration traditionnelle, Expedition attribue automatiquement les noms de zone. Renommez les zones afin que leurs noms décrivent leur objectif lorsque vous migrez la configuration vers le dispositif PAN-OS. Assurez-vous que les zones sont correctement appliquées aux interfaces.

  En outre, recherchez des routes statiques dans le routeur virtuel. S'il existe plusieurs routes statiques, utilisez Expedition pour les migrer vers la configuration PAN-OS. S'il n'existe que quelques routes statiques, notez-les, puis créez-les manuellement après la migration de la configuration.

STEP 7 | Fusionnez la configuration migrée avec la configuration de base PAN-OS en faisant un glisser-déposer des objets de la configuration migrée dans la configuration de base.

STEP 8 | Recherchez dans la configuration fusionnée les objets en double créés par la fusion, puis supprimez-les ou fusionnez-les.

STEP 9 | Avant d'exporter la configuration fusionnée vers un équipement PAN-OS, effacez le cache ARP des commutateurs et des routeurs connectés à l'équipement PAN-OS et sur l'équipement PAN-OS en lui-même pour mettre à jour leurs tables ARP.

Sur les équipements PAN-OS, utilisez la commande CLI **`clear arp all`**. (Si nécessaire, vous pouvez effacer le cache ARP par interface à l'aide de la commande CLI **`clear arp <interface>`**.)

STEP 10 | Exportez la configuration fusionnée vers l'équipement PAN-OS et chargez la configuration fusionnée.

La méthode que vous utilisez dépend de la façon dont vous souhaitez migrer la configuration fusionnée :

- Pour une nouvelle installation sur un équipement PAN-OS, cliquez sur **Generate XML & Set Output (Générer un fichier XML et définir le fichier généré)**, importez le fichier XML (configuration), puis chargez-le sur l'équipement PAN-OS.
- Pour une installation PAN-OS existante ou si vous souhaitez migrer la configuration petit à petit plutôt qu'en une seule fois, cliquez sur **Generate XML & Set Output (Générer un fichier XML et définir le fichier généré)**, importez le fichier XML (configuration), puis utilisez la commande CLI **`load config partial`** pour sélectionner une partie spécifique de la configuration à charger. Vous devez disposer d'un accès SSH pour utiliser la CLI sur un équipement PAN-OS.
- Si l'équipement PAN-OS est connecté à Expedition, vous pouvez également utiliser des appels API pour envoyer une partie ou la totalité de la configuration à l'équipement.

STEP 11 | Après avoir exporté la configuration fusionnée vers un équipement PAN-OS et chargé la configuration, utilisez Policy Optimizer pour convertir la politique basée sur le port en politique basée sur l'application.

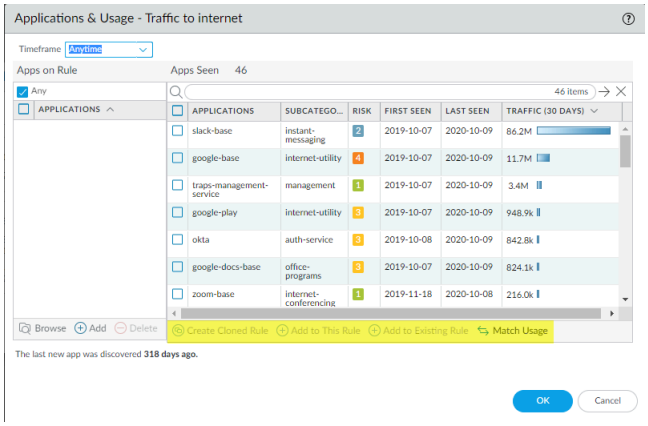
Migration vers une politique basée sur les applications à l'aide de Policy Optimizer

Après avoir utilisé Expedition pour migrer une configuration similaire vers un équipement PAN-OS, la phase suivante consiste à utiliser Policy Optimizer pour simplifier la migration vers des règles de politique de sécurité basées sur App-ID. Policy Optimizer facilite beaucoup la conversion des règles traditionnelles basées sur un port, car il automatise la présentation des informations sur les applications pour chaque règle avec le contexte nécessaire pour comprendre les informations et créer des règles intelligentes basées sur une application dans une vue unique. Policy Optimizer :

- Apprend et mémorise automatiquement toutes les applications vues dans le trafic pour chaque règle, ce qui élimine le besoin de passer au peigne fin et d'analyser des quantités de données de journaux. Même si les journaux sont remplacés, Policy Optimizer conserve les informations sur l'application afin que vous puissiez être sûr de voir toutes les applications sur une règle.
- Vous permet de migrer en toute sécurité vers App-ID sans compromettre la disponibilité des applications.
- Est natif et pris en charge sur les équipements PAN-OS. Vous n'avez donc pas à déplacer les configurations et les données entre l'équipement et un outil non natif.
- Fournit des options de tri et de filtrage faciles et intuitives pour vous aider à identifier et à hiérarchiser les règles les plus faciles et les plus sûres à convertir en premier.
- Fonctionne sur les équipements Panorama ainsi que sur les pare-feu nouvelle génération unitaires. Si vous gérez vos pare-feu nouvelle génération exécutant PAN-OS 8.1 avec Panorama, il vous suffit de mettre à niveau Panorama (et tous les Log Collectors connectés aux pare-feu gérés) vers PAN-OS 9.0 pour utiliser et bénéficier des avantages de Policy Optimizer, de sorte que vous puissiez qualifier et adopter plus rapidement Policy Optimizer que si vous deviez qualifier tous vos pare-feu.

  Strata Logging Service prend en charge Policy Optimizer sur les périphériques Panorama qui exécutent PAN-OS 10.0.4 ou version ultérieure avec le plug-in Cloud Services 2.0 ou version ultérieure.

Ces fonctionnalités créent un outil simple d'utilisation qui permet de gagner du temps et d'éviter les erreurs lors de la conversion de règles basées sur un port en règles basées sur App-ID. Policy Optimizer fournit les méthodes de conversion de règles suivantes :



- **Create Cloned Rule** (Créer une règle clonée) : le clonage d'une règle préserve la règle d'origine basée sur le port et place la nouvelle règle basée sur App-ID au-dessus de la règle clonée. Vous pouvez cloner

plusieurs règles basées sur App-ID à partir d'une règle basée sur un port. Par exemple, vous pouvez cloner plusieurs règles App-ID en fonction de sous-catégories d'applications à partir d'une règle de navigation Web générale pour regrouper les applications nécessitant un accès et un traitement des menaces similaires au lieu d'essayer de contrôler tous les accès Web pour tous les utilisateurs à tous les emplacements dans une règle générale non sécurisée.

La disponibilité des applications ne risque pas d'être compromise, car la règle basée sur le port située en dessous de la règle clonée agit comme un filet de sécurité. Si la règle basée sur App-ID clonée ne correspond pas à toutes les applications que vous devez autoriser, vous verrez que ces applications atteignent la règle basée sur le port située sous la règle clonée et vous pouvez effectuer des ajustements. Vous pouvez supprimer la règle basée sur le port lorsqu'aucun trafic que vous souhaitez autoriser ne correspond à la règle basée sur le port pendant une période raisonnable, venant ainsi terminer la conversion de cette règle en une règle basée sur App-ID.

- **Add to This Rule** (Ajouter à cette règle) : l'ajout d'applications à la règle remplace la règle basée sur le port par une règle basée sur App-ID, qui supprime la règle basée sur le port de la base de règles et ne fournit pas le filet de sécurité fourni par le clonage. Utilisez **Add to This Rule** (Ajouter à cette règle) seulement lorsque vous êtes sûr de connaître toutes les applications que vous souhaitez que la règle contrôle. Les règles qui n'ont vu que quelques applications et pour lesquelles vous êtes sûr de savoir quelles applications sont requises pour vos activités, sont candidates à la méthode **Add to This Rule** (Ajouter à cette règle). Il est plus sûr de cloner des règles ayant vu de nombreuses applications et des règles pouvant voir apparaître plus d'applications que vous devez autoriser. Si vous n'ajoutez aucune application à une règle, vous perdez la disponibilité de cette application, à moins qu'une autre règle ne l'autorise. Pendant le clonage, la règle conserve la règle basée sur le port en tant que filet de sécurité.
- **Add to Existing Rule** (Ajouter à une règle existante) : ajouter des applications à une règle existante ne remplace pas la règle initiale basée sur des ports, qui reste dans la base de règles. La méthode **Add to Existing Rule** (Ajouter à une règle existante) vous permet de sélectionner toute règle précédemment configurée et d'y ajouter des applications.

  Lorsque vous ajoutez des applications à une règle existante basée sur des applications, le pare-feu supprime ces applications de la règle basée sur des ports et les ajoute à la règle basée sur des applications sélectionnée. Les applications ajoutées utilisent la même Source, Destination, le même Service, etc., que les autres applications sur la règle basée sur des applications.

  Lorsque vous ajoutez des applications à une autre règle existante basée sur des applications, le pare-feu supprime ces applications de la règle initiale basée sur des ports et les ajoute à l'autre règle basée sur des applications. Cela convertit l'autre règle basée sur des ports en une règle basée sur des applications qui contrôle seulement les applications que vous avez ajoutées à la règle. Si vous convertissez une partie d'une règle basée sur des ports de cette façon, rendez-vous à la règle et modifiez le Service sur application-default (par défaut de l'application) pour empêcher les applications d'utiliser des ports non standards (le Service configuré sur la règle peut également ne pas correspondre à l'application).
- **Match Usage** (Mise en correspondance de l'utilisation) : la correspondance de l'utilisation d'une règle basée sur un port remplace la règle basée sur le port par une règle basée sur l'App-ID qui contient toutes les applications vues sur cette règle. Utilisez **Match Usage** (Mise en correspondance de l'utilisation) que lorsque la règle a vu un petit nombre d'applications bien connues ayant des objectifs commerciaux légitimes. Un bon exemple est le port TCP 22, qui ne doit autoriser que le trafic SSH. Si SSH est la seule application vue sur une règle basée sur un port pour le port 22, vous pouvez cliquer en toute sécurité sur **Match Usage** (Mise en correspondance de l'utilisation) et convertir la règle en une règle App-ID.

Pour **Create Cloned Rule** (Créer une règle clonée) ou **Add to This Rule** (Ajouter à cette règle), ou **Add to Existing Rule** (Ajouter à une règle existante), vous devez sélectionner au moins une application parmi les **Apps Seen** (Applications vues).

Les applications utilisées uniquement pour des événements trimestriels ou annuels peuvent ne pas apparaître dans les informations sur les applications si l'historique n'est pas assez long pour capturer leur dernière activité. Soyez conscient de ces types d'applications lorsque vous convertissez des règles.

Lorsque vous convertissez une règle basée sur un port en une règle basée sur les applications, Policy Optimizer n'apporte aucune autre modification à la règle, mis à part la conversion des services en App-ID. Dans la plupart des cas, après avoir converti une règle, vous devez modifier le **Service** sur **application-default** (par défaut de l'application) de sorte que seules les applications qui utilisent légitimement le port puissent y accéder et empêcher les applications d'évasion d'accéder au réseau en utilisant un port non standard.

Si les besoins de l'entreprise nécessitent d'autoriser des applications telles que des applications personnalisées internes sur des ports non standard entre des clients et des serveurs particuliers, limitez l'exception aux applications, sources et destinations requises. Envisagez de réécrire des applications personnalisées pour utiliser les ports application-default (par défaut de l'application).

Avant d'utiliser Policy Optimizer pour convertir les règles basées sur un port en règles basées sur App-ID, procédez comme suit :

1. Terminez la migration similaire de la configuration traditionnelle vers un équipement Panorama ou un pare-feu nouvelle génération de Palo Alto Networks à partir du logiciel Expedition.
2. Exécutez l'appareil PAN-OS sur votre réseau de production pendant environ une semaine avant de commencer à convertir les règles en App-ID afin que l'équipement puisse commencer à apprendre et à catégoriser les applications sur le réseau. Vous pouvez convertir rapidement des règles simples (par exemple, une règle du port 22 ne doit autoriser que le trafic SSH et est facile à convertir), tout en devant autoriser le pare-feu à collecter des données d'application du trafic sur une période plus longue pour d'autres règles, comme votre règle d'accès Internet (port 80/433).
3. Exécutez le Best Practice Assessment (BPA) pour établir une base de référence pour comparer les progrès.
4. Fixez des objectifs réalistes. Pensez à ce à quoi vous voulez que le résultat final ressemble. Lorsque vous atteignez l'objectif, exécutez à nouveau le BPA pour confirmer que vous avez atteint l'objectif, puis réévaluez si vous pouvez aller plus loin et rendre votre réseau encore plus sécurisé. Avec Policy Optimizer, vous ne renoncez pas à la disponibilité pour des raisons de sécurité, vous améliorez simplement la sécurité.

Convertissez étape par étape les règles. Vous pouvez convertir certaines règles simples basées sur un port qui autorisent des applications bien connues en règles basées sur App-ID après que l'équipement PAN-OS a déjà une semaine de journaux (Policy Optimizer découvre les applications vues sur les règles en lisant les journaux). Pour les autres règles qui voient de nombreuses applications, telles qu'une règle d'accès Web générale, attendez au moins 30 jours pour collecter les informations sur l'application.

Le groupe Professional Services possède une riche expérience de migration. Vous pouvez faire appel à l'équipe des Professional Services pour vous aider à déplacer une configuration de vos équipements traditionnels vers les équipements Panorama et les pare-feu nouvelle génération de Palo Alto Networks.

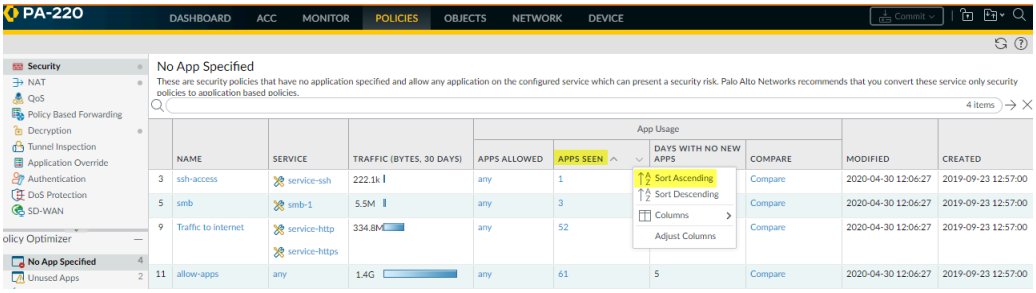
- Conversion des règles simples avec des applications bien connues après une semaine
- Règles pour commencer la conversion après 30 jours

Conversion des règles simples avec des applications bien connues après une semaine

Après une semaine de surveillance du trafic de production, vous pouvez commencer en toute sécurité à convertir des règles simples basées sur un port en règles basées sur App-ID. Les bons candidats incluent des règles pour lesquelles une seule application ou un nombre limité d'applications bien connues doivent légitimement utiliser le port, car il est assez facile de déterminer les applications que vous souhaitez autoriser avec une règle simple. Les exemples incluent le port 21 (FTP), le port 22 (SSH) et le port 53 (DNS).

Installez les dernières mises à jour du contenu avant de commencer la conversion des règles pour vous assurer que vous disposez des dernières signatures d'application sur votre équipement PAN-OS. Cet exemple vous montre comment trier les règles basées sur un port pour trouver des candidats à la conversion en toute sécurité et les options permettant de convertir ces règles basées sur un port directement en règles basées sur App-ID.

STEP 1 | Dans **Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer** > **No App Specified (Aucune application spécifiée)**, sélectionnez **Apps Seen (Applications vues)** et **Sort Ascending (Trier par ordre croissant)** (ou cliquez sur **Apps Seen [Applications vues]** pour inverser l'ordre d'affichage actuel) pour trouver les règles basées sur un port qui ont vu le moins d'applications.

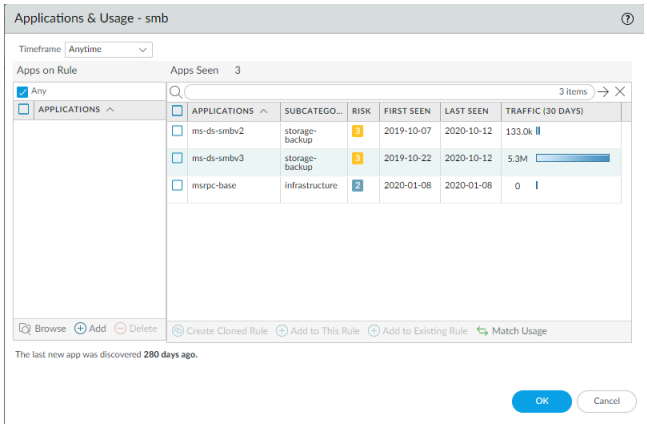


Les règles basées sur un port qui ont vu le moins d'applications sont en haut de la liste de l'affichage **No App Specified** (Aucune application spécifiée). Vous pouvez convertir en toute sécurité des règles pour des services spécifiques, tels que SSH, directement en règles basées sur une application. Vous pouvez également examiner les règles qui ont vu peu d'applications pour savoir si vous pouvez les convertir en toute sécurité.

La règle basée sur un port destinée à autoriser le trafic Server Message Block (SMB) n'a vu que trois applications depuis la migration de la configuration vers l'équipement PAN-OS et est donc candidate à la conversion.

STEP 2 | Cliquez sur le nombre indiqué dans **Apps Seen** (Applications vues) ou **Compare** (Comparer) pour examiner les applications vues sur la règle.

Applications & Usage (Applications et utilisation) affiche les applications réellement vues dans le trafic qui correspondent à la règle.



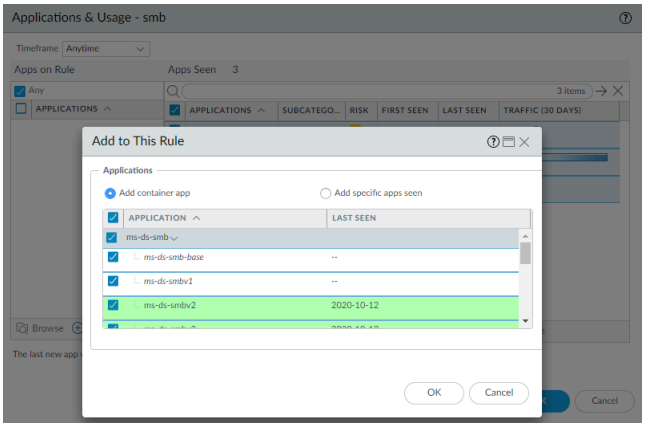
STEP 3 | Déterminez si vous souhaitez autoriser toutes les applications, certaines ou aucune applications vues sur la règle et sélectionnez les applications que vous souhaitez autoriser.

Vous pouvez faire correspondre l'utilisation exacte de la règle, anticiper en ajoutant des applications du conteneur ou sélectionner des applications individuelles à ajouter à la règle.

- Si vous souhaitez que la règle autorise toutes les applications correspondant exactement à la règle, procédez comme suit :
  1. Sélectionnez toutes les **Applications** dans **Apps Seen** (Applications vues).
  2. Cliquez sur **Match Usage** (Mise en correspondance de l'utilisation).
  3. Cliquez sur **OK** pour convertir la règle basée sur le port en une règle basée sur App-ID.
  4. Définissez le **Service** sur **application-default** (par défaut de l'application) de sorte qu'aucune application malveillante d'évasion ne puisse utiliser le port.
- Si vous souhaitez autoriser toutes les applications vues dans la règle ou certaines d'entre elles ou anticiper en ajoutant leurs applications de conteneur (toutes les applications de chaque conteneur

sont autorisées et les applications ajoutées ultérieurement à l'application de conteneur sont automatiquement autorisées), procédez comme suit :

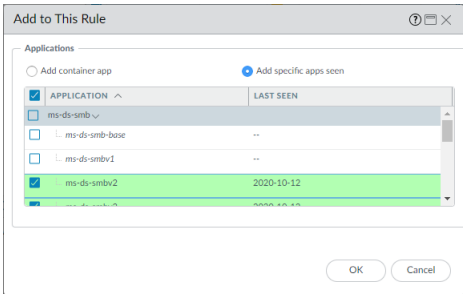
1. Sélectionnez toutes les applications et cliquez sur **Add to This Rule (Ajouter à cette règle)**.



   Les applications grises sont les applications de conteneur. Les applications vertes sont les applications vues sur la règle. Les applications blanches appartiennent à la même application de conteneur, mais n'ont pas été vues sur la règle.

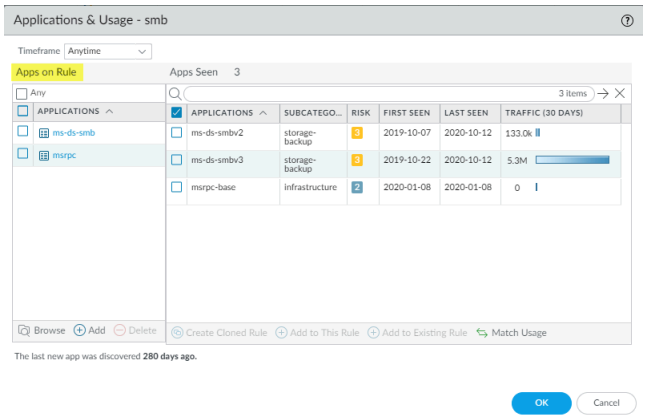
   Add container app (Ajouter une application de conteneur) est sélectionnée par défaut, par conséquent, toutes les applications du conteneur sont également sélectionnées par défaut.

2. Si vous souhaitez que la règle n'inclue que les applications qui correspondent à la règle, sélectionnez **Add container app (Ajouter une application de conteneur)**. Seules les applications vues dans la règle sont ajoutées à la règle. L'application de conteneur et les applications sur la règle qui n'ont pas obtenu de correspondance avec la règle ne sont pas sélectionnées. Cliquez sur **OK** pour sélectionner seulement les applications vues sur la règle.



   Si vous souhaitez inclure l'application de conteneur et toutes ses applications dans la règle, laissez la sélection sur **Add container app (Ajouter l'application de conteneur)** puis cliquez sur **OK**. Seules les applications de conteneur apparaissent dans **Apps on Rule (Applications d'une règle)**, car elles incluent (autorisent) toutes les applications qu'elles contiennent, qui

protègent également la règle en permettant aux applications d'être ajoutées au conteneur par la suite :

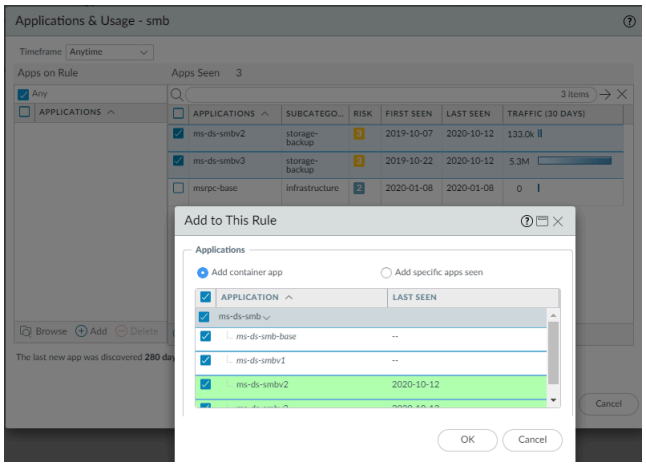


3. Cliquez sur **OK** sur l'onglet **Usage (Utilisation)** pour convertir la règle.
4. Définissez le **Service** sur **application-default** (par défaut de l'application) de sorte qu'aucune application malveillante d'évasion ne puisse utiliser le port.

- Si vous souhaitez sélectionner les applications à autoriser dans une application de conteneur, sélectionnez ces applications puis cliquez sur **Add to This Rule (Ajouter à cette règle)**. Par exemple, si vous décidez de ne pas autoriser msrpc-base, de sélectionner uniquement ms-ds-smbv2 et ms-ds-smbv3 et **Add to Rule** (Ajouter à la règle), Policy Optimizer vous montre les applications associées dans l'application de conteneur (ms-ds-smb grise) et vous offre la possibilité de protéger la règle en ajoutant ces applications :

  1. Sélectionnez les applications que vous souhaitez autoriser, puis cliquez sur **Add to This Rule** (Ajouter à cette règle).

     Par exemple, si vous décidez de ne pas autoriser msrpc-base, de sélectionner uniquement ms-ds-smbv2 et ms-ds-smbv3 et **Add to This Rule** (Ajouter à cette règle), Policy Optimizer vous montre les applications associées dans l'application de conteneur (ms-ds-smb grise) et vous offre la possibilité de protéger la règle en ajoutant ces applications :

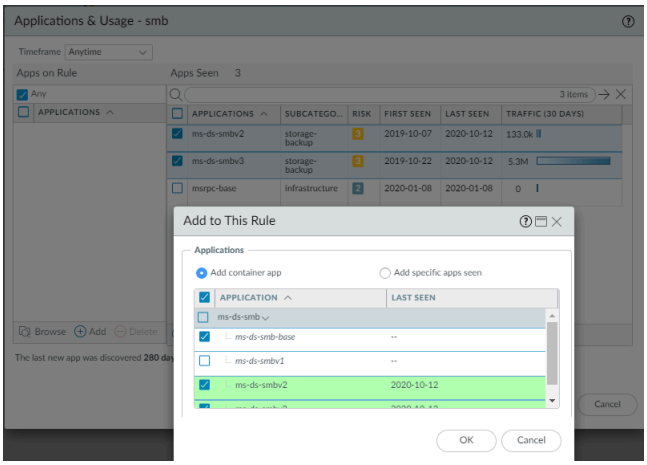


     Les applications vertes sont les applications vues sur la règle. Les applications blanches appartiennent à la même application de conteneur, mais n'ont pas été vues sur la règle.

2. Vous pouvez autoriser toutes les applications ou sélectionner les applications à autoriser.

   Pour autoriser l'application de conteneur et toutes ses applications actuelles et futures, cliquez sur **OK**. **Apps on Rule** (Applications d'une règle) montre les applications sélectionnées. Cliquez sur **OK** pour convertir la règle.

   Pour n'autoriser que les applications sélectionnées, désélectionnez les applications indésirables. Si vous désélectionnez une application dans un conteneur, l'application de conteneur est également désélectionnée pour ne pas autoriser automatiquement ses applications enfant.



3. Cliquez sur **OK**. **Apps on Rule** (Applications d'une règle) montre les applications sélectionnées.
4. Cliquez sur **OK** pour convertir la règle.
5. Définissez le **Service** sur **application-default** (par défaut de l'application) de sorte qu'aucune application malveillante d'évasion ne puisse utiliser le port.

Règles pour commencer la conversion après 30 jours

Après 30 jours de surveillance du trafic de production, vous pouvez commencer en toute sécurité à convertir le reste des règles basées sur un port en règles basées sur App-ID et à nettoyer la base de règles. Un bon point de départ consiste à supprimer les règles inutilisées afin de réduire la surface d'attaque. Après cela, commencez à convertir les règles en App-ID dans le périmètre avec votre règle d'accès Internet sortant (port 80/443), car cette règle observe probablement plus de trafic avec plus d'applications que toute autre règle, ce qui signifie également que c'est la règle qui présente le plus de risque.

Installez les dernières mises à jour du contenu avant de commencer la conversion des règles pour vous assurer que vous disposez des dernières signatures d'application sur votre équipement PAN-OS.

Policy Optimizer propose de nombreuses méthodes intuitives pour trier, filtrer et hiérarchiser les règles à convertir en premier. Une fois que vous avez supprimé les règles inutilisées et converti la règle d'accès Web en App-ID, les règles que vous choisissez de hiérarchiser dépendent de votre entreprise et de vos exigences de sécurité. Réfléchissez aux applications critiques pour votre entreprise, au risque d'incident et aux possibles conséquences en fonction de vos priorités.

Les sections suivantes fournissent des idées et des méthodes d'utilisation d'options de tri et de filtrage simples, mais puissantes, pour identifier et hiérarchiser les règles à convertir après les 30 premiers jours :

- Suppression des règles inutilisées (règles pour lesquelles aucun trafic ne correspond)

- Conversion des règles les plus stables (règles qui ne voient aucune nouvelle application sur une période donnée)
- Conversion des règles d'accès Internet (règles qui contrôlent le trafic sur le port HTTP 80 et le port HTTPS 443)
- Conversion des règles qui voient le plus de trafic (règles qui génèrent le plus de trafic sur une période donnée)
- Conversion des règles avec peu d'applications vues sur une période donnée (facile à identifier et à convertir)

Suppression des règles inutilisées

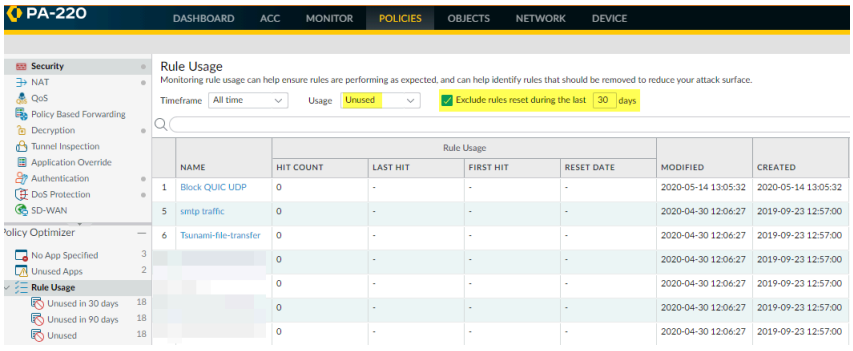
La base de règles migrée contient souvent des règles qui ne sont pas utilisées, car aucun trafic d'applications ne correspond à ces règles. Les règles inutilisées encombrent la base de règles et offrent des voies d'attaque aux adversaires. Supprimez ces règles pour nettoyer la base de règles et réduire la surface d'attaque ou modifiez-les afin qu'elles s'appliquent au trafic d'applications et servent un but légitime dans la base de règles.

Les règles inutilisées peuvent exister pour un certain nombre de raisons. Les règles régissant les services et les applications utilisés autrefois par l'entreprise, mais remplacées par d'autres applications, peuvent figurer dans la base de règles. Une règle qui précède une règle inutilisée peut contrôler les applications qui correspondraient autrement à la règle inutilisée. Dans certains cas, les règles inutilisées sont d'anciennes règles créées par des administrateurs qui ne font plus partie de l'entreprise et pour lesquelles aucun administrateur actuel ne connaît l'intention de ces règles.

Affichez les règles sur n'importe quel **Timeframe (Laps de temps)** choisi à partir de **Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer** > **Rule Usage (Utilisation d'une règle)**. Définissez **Usage** sur **Unused** (Inutilisé) pour filtrer les règles qui ont vu le trafic d'applications.

STEP 1 | Identifiez les règles inutilisées.

Dans **Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer** > **Rule Usage (Utilisation d'une règle)**, définissez **Timeframe (Laps de temps)** sur **All time (Tout le temps)**, et **Usage (Utilisation)** sur **Unused (Inutilisé)** (pour afficher uniquement les règles avec un nombre d'utilisations égal à zéro), et cochez la case **Exclude rules reset during the last 30 days (Exclure la réinitialisation des règles au cours des 30 derniers jours)** (pour empêcher l'affichage des règles de réinitialisation récentes qui n'ont peut-être pas vu le trafic au cours des derniers jours, mais qui peuvent le voir sur une période plus longue). Une liste de règles qui n'ont pas vu le trafic d'applications sur le **Timeframe** (Laps de temps) sélectionné.



STEP 2 | Évaluez les règles qui n'ont pas vu de trafic et déterminez si elles sont nécessaires ou si vous pouvez les désactiver.

Dans cet exemple, l'entreprise a utilisé le Tsunami file transfer (Transfert de fichiers Tsunami) par le passé, mais une enquête montre qu'elle n'utilise plus Tsunami. Il n'y a donc aucune raison d'autoriser le trafic d'applications Tsunami sur le réseau.

STEP 3 | Cliquez sur **Disable** (Désactiver) ou sur **Delete** (Supprimer) la règle.

Dans **Policies** > **Security** (Sécurité), sélectionnez la règle de transfert de fichier Tsunami puis cliquez sur **Disable** (Désactiver) ou **Delete** (Supprimer) la règle.

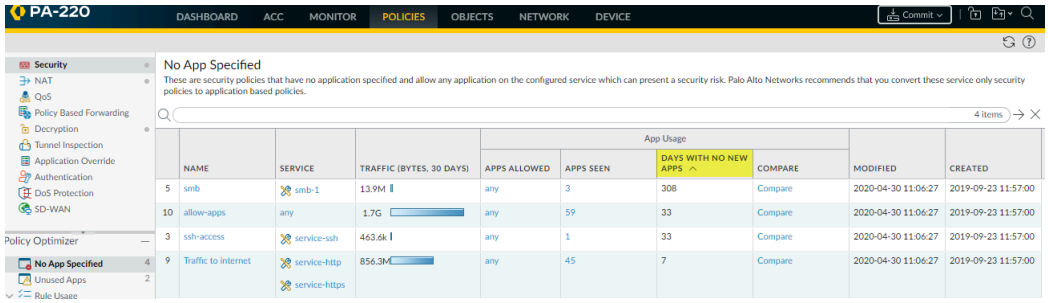
Il est plus prudent de désactiver la règle au cas où votre entreprise aurait besoin de l'application, même si elle n'a vu aucun trafic. (Cela peut se produire si vous ne tenez pas compte des événements trimestriels et annuels lorsque vous déterminez si l'entreprise utilise une application ou si l'application est requise pour un sous-traitant ou un partenaire dont le trafic n'accède que de façon périodique au réseau.) Après une période raisonnable, supprimez les règles inutilisées que vous avez désactivées précédemment.

Conversion des règles les plus stables

Convertissez les règles basées sur un port qui n'ont pas vu de nouvelles applications depuis une période raisonnable, ce qui signifie que les règles se sont stabilisées et que vous êtes moins susceptible de voir de nouvelles applications sur celles-ci. Clonez ces règles pour vous assurer que si plusieurs applications correspondent ultérieurement à la règle, la règle basée sur le port reste dans la base de règles aussi longtemps que nécessaire en tant que filet de sécurité.

Tenez compte des applications utilisées uniquement pour les événements trimestriels, annuels et autres lorsque vous estimez que les nouvelles applications correspondront à la règle ou non.

STEP 1 | Dans **Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer** > **No App Specified (Aucune application spécifiée)**, triez les règles (par ordre décroissant) pour afficher les règles avec le plus grand nombre de **Days with No New Apps (Jours sans nouvelles applications)** en haut de la liste.



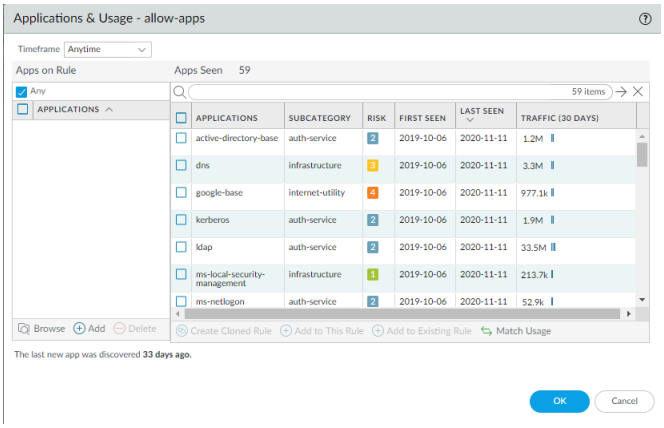
Les trois premières règles n'ont vu aucune nouvelle application pendant plus de 30 jours et sont candidates à la conversion en App-ID. (Conversion des règles simples avec des applications bien

connues après une semaine décrit les règles de conversion avec peu de **Apps Seen [Applications vues]**, comme la règle SMB, cet exemple porte donc sur la règle d'autorisation des applications.)

*Vérifiez la **Modified date** (Date de modification), car les règles qui n'ont pas été modifiées depuis longtemps sont également susceptibles d'être plus stables. Les règles récemment modifiées peuvent ne pas avoir vu toutes les applications pouvant correspondre à la règle.*

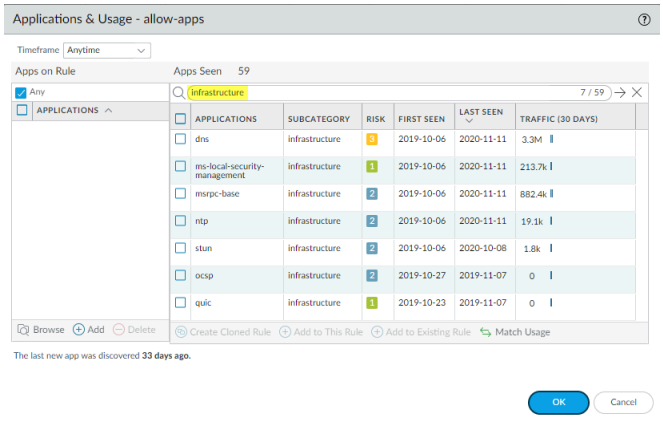
Étant donné que plusieurs applications ont été observées sur la règle, clonez-la au lieu de la convertir directement en règle basée sur App-ID.

STEP 2 | Cliquez sur le nombre de **Apps Seen (Application vues)** pour ouvrir la boîte de dialogue **Applications & Usage (Applications et utilisation)**.



STEP 3 | Triez et filtrez les **Apps Seen** (Applications vues) sur la règle pour déterminer comment gérer les applications.

Le tri ou le filtrage par sous-catégorie vous aide à comprendre le trafic observé sur les règles qui voient plusieurs applications. Par exemple, vous pouvez filtrer par sous-catégorie d'infrastructure pour voir toutes les applications d'infrastructure et cloner une règle basée sur App-ID pour les contrôler.



STEP 4 | Suivez les étapes 4 à 7 dans Conversion des règles d'accès Internet pour créer une règle clonée qui contrôle chaque sous-catégorie (ou les sous-catégories associées) des applications que vous souhaitez traiter de manière similaire.

Conversion des règles d’accès Internet

Une règle d’accès Internet contrôle le trafic sur les ports 80 (HTTP) et 443 (HTTPS). Cette règle voit généralement le plus grand nombre d’applications et la plus grande quantité de trafic en octets. Une règle d’accès Internet basée sur les ports peut autoriser les applications que vous ne souhaitez pas autoriser sur votre réseau, et l’exposer aux attaques. Contrôlez et autorisez de manière sécurisée les applications que vous autorisez sur ces ports en convertissant la règle d’accès Internet basée sur les ports en un ensemble de règles basées sur les applications. Pour cela, vous devez savoir quelles applications sont sanctionnées par votre entreprise pour une utilisation professionnelle et quelles applications votre entreprise tolère dans d’autres situations.

Une bonne méthode de conversion consiste à regrouper les applications nécessitant un traitement similaire dans la même règle au lieu de créer des règles distinctes pour chaque application afin d’éviter le grossissement de la base de règles. Utilisez Policy Optimizer pour trier les applications vues sur une règle par sous-catégorie d’applications afin de voir toutes les applications d’une règle d’une sous-catégorie particulière, sélectionner les applications utilisées par votre entreprise, puis cloner une règle pour contrôler ces applications. Policy Optimizer offre de nombreuses options de tri et de filtrage pour organiser et analyser les applications vues sur une règle.

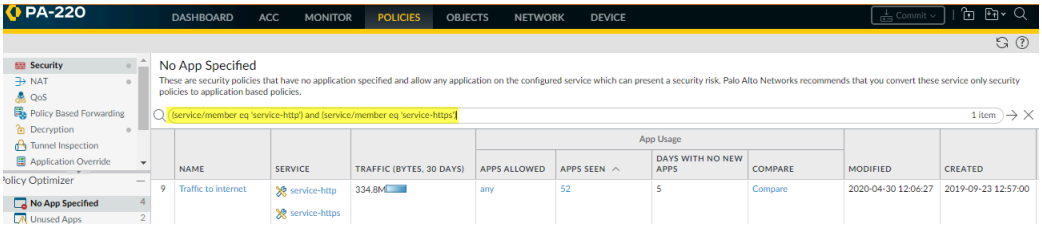
Clonez la règle au lieu de la convertir directement pour garantir la disponibilité des applications. Le clonage d’une règle conserve la règle d’origine basée sur le port et place la règle basée sur l’application clonée directement au-dessus de la règle basée sur le port dans la base de règles de sécurité. Créez différentes règles d’accès Internet à partir de la règle d’origine basée sur le port pour les groupes d’applications que vous souhaitez traiter différemment, sans risquer de compromettre la disponibilité des applications. Repérez facilement quelles applications correspondent à la règle clonée et quelles applications filtrent vers la règle d’origine basée sur le port et ajustez les règles selon vos besoins. Lorsqu’aucune application que vous souhaitez autoriser ne correspond à la règle basée sur le port pendant suffisamment de temps pour vous assurer que vous avez comptabilisé toutes les applications requises par l’entreprise, vous pouvez désactiver (ou supprimer) la règle basée sur le port, qui termine la conversion sans risquer de compromettre la disponibilité des applications.

Utilisez la même méthode pour convertir d’autres règles ayant vu plusieurs applications bien connues. Utilisez les informations de **Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer** > **No App Specified (Aucune application spécifiée)** afin d’aider à hiérarchiser les règles à convertir après avoir converti les règles d’accès Internet. Par exemple, vous pouvez les hiérarchiser en combinant la plupart des **Apps Seen** (Applications vues) et le plus de trafic au cours des 30 derniers jours (**Traffic (Bytes, 30 days)** (Trafic [octets 30 jours]) pour convertir les règles les plus utilisées, ou vous pouvez examiner les **Days with No New Apps** (Jours sans nouvelles applications) et la **Modified date** (Date de modification) pour trouver des règles qui ont vu de nombreuses applications, mais sont également plus stables.

Cet exemple vous montre comment cloner une règle basée sur une application qui contrôle les applications professionnelles à partir d’une règle d’accès Internet basée sur un port. Utilisez le même processus de clonage pour créer des règles basées sur une application en toute sécurité pour différentes sous-catégories et applications individuelles vues sur n’importe quelle règle basée sur un port.

STEP 1 | Accédez à **Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer** > **No App Specified (Aucune application spécifiée)** et recherchez la ou les règles basées sur un port qui contrôlent l'accès Internet.

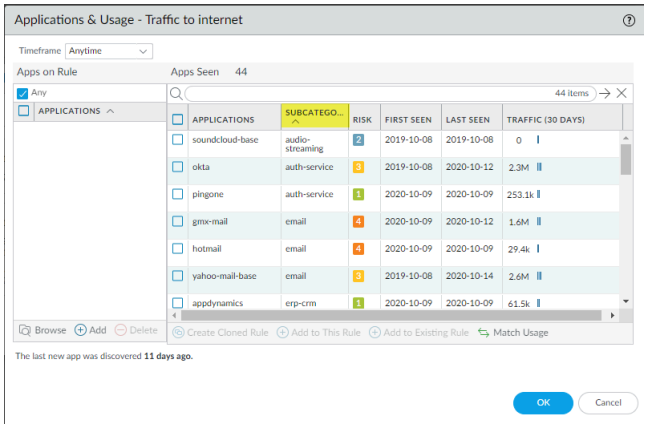
Utilisez le filtre **`(service/member eq 'service-http') and (service/member eq 'service-https')`** pour trouver la ou les règles basées sur un port configurées avec **service-http** et **service-https**, qui est la règle d'accès Internet.



STEP 2 | Cliquez sur **Compare (Comparer)** ou sur le nombre de **Apps Seen (Application vues)** pour ouvrir la boîte de dialogue **Applications & Usage (Applications et utilisation)**.

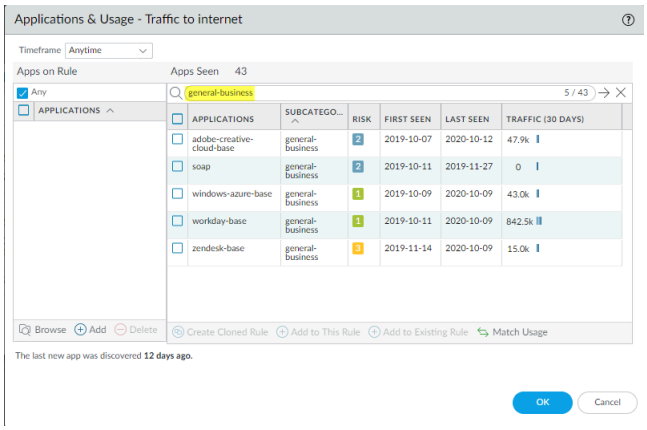
STEP 3 | Triez les **Apps Seen** (Applications vues) par sous-catégorie d'applications pour regrouper les applications similaires qu'il peut être approprié de contrôler dans la même règle de politique de sécurité.

Triez par **Subcategory** (Sous-catégorie) pour regrouper les applications vues sur la règle :



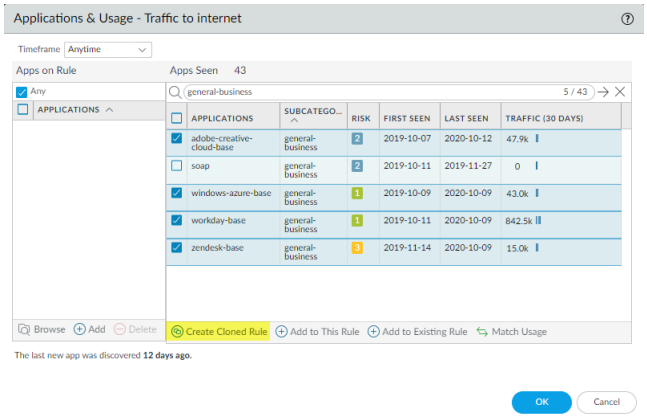
Vous pouvez également filtrer par sous-catégorie particulière pour ne voir que les applications appartenant à cette sous-catégorie. Dans cet exemple, filtrez pour afficher uniquement les applications

professionnelles vues sur la règle pour créer une règle basée sur App-ID permettant de contrôler les applications professionnelles :



STEP 4 | Sélectionnez les applications que vous souhaitez autoriser, puis cliquez sur **Create Cloned Rule** (Créer une règle clonée) pour cloner la nouvelle règle basée sur une application à partir de la règle basée sur le port.

Dans cet exemple, l'entreprise utilise quatre applications parmi toutes les applications mais n'a pas utilisé une des applications pendant une longue durée, ce que vous pouvez voir dans les colonnes **Last Seen** (Vu en dernier) et **Traffic (30 Days)** (Trafic [30 jours]). En fonction de l'utilisation et des applications sanctionnées par l'entreprise, l'entreprise choisit de ne pas autoriser l'application qu'elle n'utilise pas.

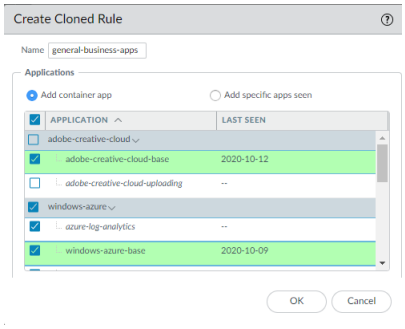


STEP 5 | Dans la boîte de dialogue **Clone** (Cloner), sélectionnez les applications associées à chaque application de conteneur que vous souhaitez autoriser.

Donnez un **nom** à la nouvelle règle qui décrit son objectif : dans cet exemple, il s'agira d'applications professionnelles. Décidez si vous souhaitez autoriser uniquement des applications spécifiques provenant de chaque application de conteneur ou si vous souhaitez autoriser l'application de conteneur. Autoriser l'application de conteneur autorise toutes les applications présentes dans le conteneur. Cela protège la règle en autorisant automatiquement les nouvelles applications si elles sont ajoutées à l'application de conteneur, ce qui garantit la disponibilité des applications. Toutes les applications sont sélectionnées par défaut. Les application de conteneur sont grises, les applications ayant été vues sur la

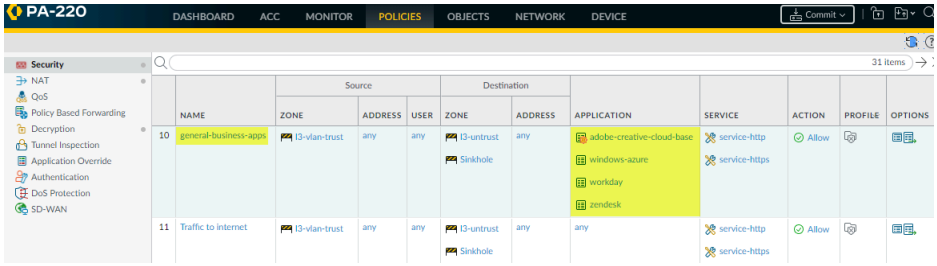
règle sont vertes et les applications de l'application de conteneur qui n'ont pas été vues sur la règle sont en italique et blanches.

Dans l'image illustrant cet exemple, vous pouvez voir les applications de conteneur grises « adobe-creative-cloud » et « windows-azure », les applications vues sur la règle en vert (« adobe-creative-cloud-base » et « windows-azure-base »), et deux applications qui n'ont pas été vues sur la règle en italique (« adobe-creative-cloud-uploading » et « azure-log-analytics »). Cet exemple indique que l'application « adobe-creative-cloud-uploading » est désélectionnée, ce qui désélectionne automatique son application de conteneur (« adobe-creative-cloud ») alors que toutes les applications « windows-azure » sont toujours sélectionnées, par conséquent, l'application de conteneur « windows-azure » reste sélectionnée.



Désélectionnez une application si vous ne souhaitez pas que les utilisateurs aient accès à cette application en particulier. Cependant, si de nouvelles applications sont ajoutées à l'application de conteneur « adobe-creative-cloud », le pare-feu ne les autorisera pas automatiquement, car l'application de conteneur est désélectionnée. Inversement, si de nouvelles applications sont ajoutées à l'application de conteneur « windows-azure », le pare-feu les autorisera automatiquement, ce qui protège la règle.

STEP 6 | Cliquez sur **OK** pour revenir à l'onglet Usage (Utilisation) de la règle de politique de sécurité puis cliquez de nouveau sur **OK** pour créer la règle. Le pare-feu place la règle au-dessus de la règle basée sur les ports dans la règle de politique de sécurité (**Policies [Politiques]** > **Security**).



Si vous sélectionnez une application de conteneur, Policy Optimizer ajoute seulement l'application de conteneur à la règle, car l'application de conteneur comprend toutes les applications. L'engrenage rouge pour « adobe-creative-cloud-base » indique que c'est une application individuelle, et non pas une application de conteneur.

STEP 7 | Cliquez sur le **Name** (Nom) de la règle ou sur un **Service** et définissez le **Service** sur **application-default** (par défaut de l'application) pour empêcher les applications d'évasion d'accéder à un port non standard.

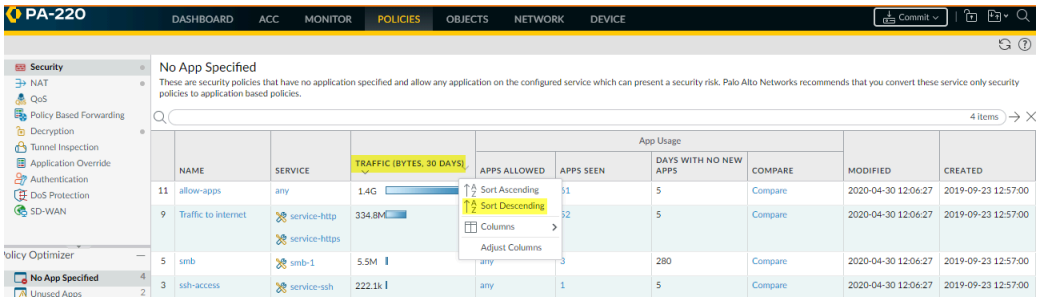
STEP 8 | Dès que vous avez besoin d'autoriser d'autres applications professionnelles sanctionnées, ajoutez-les à la règle des applications professionnelles et supprimez les applications de la règle si vous ne les utilisez plus.

Conversion des règles qui voient le plus de trafic

Le tri des règles ayant enregistré le plus de trafic au cours des 30 derniers jours (**Traffic [Bytes, 30 days]**) (Trafic [octets 30 jours]) vous montre les règles actuelles les plus actives. (Une période plus longue peut vous induire en erreur en privilégiant les anciennes règles qui restent en haut de la liste, car elles ont des totaux cumulés élevés, même si elles ne voient plus beaucoup de trafic.) La conversion de ces règles en règles basées sur App-ID protège la plus grande quantité de trafic pour votre effort.

Si plusieurs règles voient beaucoup de trafic, utilisez les informations de **Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer** > **No App Specified (Aucune application spécifiée)** afin de hiérarchiser les règles à convertir en premier. Par exemple, vous pouvez hiérarchiser les règles avec le plus de **Apps Seen** (Application vues) (potentiellement les règles les plus risquées) ou les règles avec le plus de **Days with No New Apps** (Jours sans nouvelles applications) et la plus ancienne **Modified date** (Date de modification) (règles de trafic élevé les plus stables).

STEP 1 | Dans **Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer** > **No App Specified (Aucune application spécifiée)**, triez les règles par ordre décroissant par **Traffic (Bytes, 30 days)** (Trafic [octets 30 jours]) pour placer les dernières règles actives en haut de la liste.



STEP 2 | Sélectionnez une règle pour commencer la conversion et cliquez sur le nombre de **Apps Seen** (Applications vues).

STEP 3 | Dans la boîte de dialogue **Applications & Usage (Applications et utilisation)**, triez et filtrez les **Apps Seen (Applications vues)** sur la règle pour déterminer comment gérer les applications.

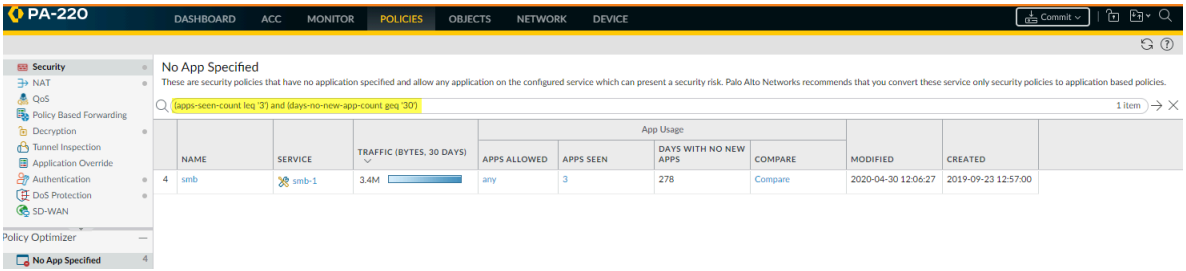
Triez ou filtrez par sous-catégorie d'applications pour regrouper les applications qui peuvent nécessiter un traitement similaire et peuvent être contrôlées dans une règle basée sur une application. Triez par **Traffic (30 days)** (Trafic, 30 jours) pour voir la quantité de trafic récent sur des applications individuelles afin de hiérarchiser les applications actuellement les plus actives.

STEP 4 | Suivez les étapes 4 à 7 dans Conversion des règles d'accès Internet pour créer une règle clonée qui contrôle chaque sous-catégorie (ou les sous-catégories associées) des applications que vous souhaitez traiter de manière similaire.

Conversion des règles avec peu d'applications vues sur une période donnée

Les règles avec relativement peu de **Apps Seen** (Applications vues) et avec aucune nouvelle application pendant une période suffisamment longue peuvent être faciles à convertir, relativement stables et faciles à identifier à l'aide de filtres.

STEP 1 | Dans **Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer** > **No App Specfied (Aucune application spécifiée)**, filtrez les règles pour n'afficher que les règles avec un petit nombre de **Apps Seen (Applications vues)** et qui n'ont vu aucune application au cours d'une période donnée.



Cet exemple filtre les règles qui ont vu trois applications ou moins **`(apps seen count leq '3')`** et pour lesquelles aucune application n'a été vue depuis au moins 30 jours **`(days no new app count geq '30')`**.

STEP 2 | Sélectionnez une règle à convertir et cliquez sur le nombre de **Apps Seen** (Applications vues).

STEP 3 | Dans la boîte de dialogue **Applications & Usage (Applications et utilisation)**, indiquez si vous souhaitez autoriser toutes les applications et si elles doivent figurer dans la même règle, c'est-à-dire, si elles nécessitent un traitement similaire en termes d'accès et de sécurité.

Si vous souhaitez autoriser toutes les applications et qu'elles nécessitent un traitement similaire, vous pouvez cliquer sur **Match Usage** (Mise en correspondance de l'utilisation) et remplacez la règle basée sur le port par la nouvelle règle basée sur App-ID.

Si vous souhaitez autoriser toutes les applications, mais qu'elles nécessitent un traitement différent, clonez la règle pour chaque ensemble d'applications nécessitant un traitement différent. Par exemple, si une règle basée sur un port autorise trois applications, dont deux applications de messagerie et une application d'infrastructure, vous souhaiterez peut-être cloner une règle pour les applications de messagerie et une autre pour l'application d'infrastructure.

Si vous souhaitez autoriser certaines applications et en refuser d'autres, procédez comme suit :

- Clonez une ou plusieurs règles pour les applications que vous souhaitez conserver et surveillez la règle d'origine basée sur le port pour vous assurer que les applications que vous ne souhaitez pas conserver sont les seules à correspondre à cette règle. Lorsque le temps nécessaire est écoulé pour vous assurer qu'aucune application que vous souhaitez autoriser ne correspond à la règle basée sur le port, vous pouvez la désactiver ou la supprimer. Les étapes 4 à 7 dans Conversion des règles d'accès Internet indiquent comment créer une règle clonée.
- Si vous êtes certain de savoir quelles applications vous souhaitez autoriser et quelles applications vous souhaitez bloquer, procédez comme suit :
  - Si les applications que vous souhaitez autoriser nécessitent un traitement similaire, utilisez **Add to This Rule** (Ajouter à cette règle) pour remplacer la règle basée sur le port par une règle basée sur une application qui autorise uniquement les applications que vous avez ajoutées à la règle. Les applications que vous n'ajoutez pas à la règle sont bloquées, sauf si vous les autorisez dans une autre règle.
  - Si les applications que vous souhaitez autoriser nécessitent un traitement différent, clonez les règles basées sur une application pour les applications que vous souhaitez autoriser à partir de la règle basée sur le port. Si vous pensez toujours que vous pouvez bloquer les applications restantes, vous pouvez désactiver (ou supprimer) la règle basée sur le port.

Prochaines étapes pour adopter les meilleures pratiques en matière de sécurité

Une fois que vous avez terminé votre première tentative de conversion des règles basées sur un port en règles basées sur une application, suivez les étapes ci-dessous pour renforcer votre base de règles de la politique de sécurité et la sécurité du réseau :

- Utilisez la fonctionnalité d'enrichissement de règles Expedition qui utilise l'apprentissage machine pour examiner et consolider la configuration de votre politique.
- Exécutez régulièrement le Best Practice Assessment (BPA) pour mesurer les progrès accomplis dans la réalisation de votre objectif d'adoption de l'App-ID et identifier d'autres vulnérabilités. Lorsque vous atteignez votre objectif, utilisez le BPA pour identifier les domaines dans lesquels vous pouvez continuer à améliorer l'adoption et protéger davantage votre réseau.
- Policy Optimizer convertit les règles basées sur un port en règles basées sur App-ID, mais ne change rien aux règles. Après avoir converti les règles traditionnelles en règles basées sur App-ID, renforcez les règles pour réduire la surface d'attaque et augmenter la visibilité :
  - Définissez le **Service** sur **application-default** (par défaut de l'application) pour empêcher les applications d'utiliser des ports non standard. Pour les applications personnalisées internes, définissez les ports par défaut, puis appliquez **application-default** (par défaut de l'application).
  - En périmétrie (passerelle Internet), pour les applications Web, utilisez les catégories de Filtrage des URL pour empêcher l'accès aux sites Web à risque.
  - Configurez User-ID pour contrôler qui a accès aux applications.
  - Configurez le Transfert des journaux pour centraliser les journaux de plusieurs équipements PAN-OS, envoyer des alertes par e-mail à des administrateurs ou des groupes spécifiques pour des alertes spécifiques et conserver les journaux pour l'analyse historique.
  - Configurez les profils de sécurité respectant les meilleures pratiques pour Antivirus, Antispyware, Protection contre les vulnérabilités, Blocage des fichiers et Analyse WildFire, et appliquez-les aux règles de politique de sécurité App-ID.
  - Pensez à utiliser les modèles Iron-Skillet, disponibles sur GitHub, pour effectuer le démarrage et amorcez votre configuration initiale des meilleures pratiques.
- Maintenez le déploiement de l'App-ID. Au fur et à mesure que vous ajoutez des règles pour les nouvelles applications, notamment les applications personnalisées internes, créez des règles basées sur App-ID qui permettent de protéger votre réseau. Ne réutilisez aucune règle basée sur un port qui ne vous donne aucune visibilité sur le trafic d'applications et ne vous permet pas de les inspecter et de les contrôler. Apprenez-en plus sur App-ID dans le Guide de l'administrateur PAN-OS.
- Au fur et à mesure que vous renforcez la base de règles de la politique de sécurité, envisagez d'appliquer d'autres protections à votre réseau, telles que les meilleures pratiques pour le déchiffrement du trafic et pour la protection DoS et de zone.

Si vous avez besoin d'aide pour migrer la configuration de votre équipement traditionnel vers les équipements de Palo Alto Networks, contactez le groupe de Professional Services de Palo Alto Networks qui possède une riche expérience de migration que vous pouvez exploiter pour réussir la migration et la conversion en App-ID.