paloalto TECHDOCS

Meilleures pratiques en matière de politique de sécurité

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

July 5, 2023

Table of Contents

Meilleures pratiques en matière de politique de sécurité

La politique de sécurité détermine le trafic que vous autorisez sur votre réseau et la manière de traiter ce trafic. Les meilleures pratiques en matière de politique de sécurité limitent le trafic que vous autorisez au trafic autorisé requis pour votre entreprise et toléré pour vos employés. Cela réduit la surface d'attaque et contribue à protéger votre réseau et les actifs de votre entreprise. Le point de vue de ce document est de savoir ce qu'il faut faire pour une meilleure sécurité réseau, que votre entreprise privilégie la sécurité ou la disponibilité critique.

Les meilleures pratiques en matière de politique de sécurité suivent le principe du moindre privilège, ce qui signifie que seules les personnes qui ont besoin d'accéder à des applications, des données et une infrastructure spécifiques sont autorisées à y accéder, et que le trafic est décrypté, inspecté et consigné de manière appropriée pour protéger les actifs, la propriété intellectuelle et d'autres éléments essentiels à votre entreprise. Tous les autres accès augmentent les risques sans atteindre les objectifs de l'entreprise.

Ce livre contient des meilleures pratiques simplifiées, étape par étape, sur la façon de :

- Planifier la politique de sécurité
- Déployer la politique de sécurité
- Maintenir la politique de sécurité

Les étapes qui nécessitent une configuration ou pour lesquelles il existe des informations conceptuelles approfondies incluent des liens vers la documentation appropriée pour plus de détails. Pour en savoir plus sur les fonctionnalités, les capacités et le fonctionnement des produits Palo Alto Networks, consultez les guides de l'administrateur du produit, les notes de mise à jour, les guides de mise à niveau, les guides d'interconnexion, etc., disponibles sur la page d'accueil de la documentation technique :

- PAN-OS
- Panorama
- Panorama Managed Prisma Access (y compris la documentation de l'application GlobalProtect)
- Prisma Access géré dans le cloud
- Prisma SD-WAN
- Services de sécurité fournis par le cloud
- Moteur d'identité sur le cloud
- GlobalProtect
- VM-Series
- Série CN
- Centre d'aide Cortex
- Guides sur le pare-feu et le matériel de l'appareil

Reportez-vous à la série de livres sur les meilleures pratiques de Palo Alto Networks pour obtenir des conseils sur les meilleures pratiques sur des sujets tels que le décryptage, le DoS et la protection de zone (y compris la protection de la mémoire tampon des paquets), et bien plus encore.

Planification des meilleures pratiques en matière de politique de sécurité

Avant de créer les meilleures pratiques Règles de politique de sécurité, assurez-vous de comprendre les meilleures pratiques de planification d'un réseau sécurisé, en particulier les principes de l'accès réseau Zero Trust (ZTNA). La politique de sécurité définit le trafic que vous autorisez et bloquez. Cependant, il faut un ensemble complet d'outils et de services pour protéger complètement votre réseau, notamment des outils qui fournissent :

- Une visibilité, telle que le décryptage, l'App-ID, l'User-ID et le Device-ID.
- Une prévention avancée des menaces, telle que la protection contre les vulnérabilités, l'antivirus, l'antispyware, le blocage des fichiers, le sandboxing, le Data Loss Prevention (prévention des pertes de données - DLP), la sécurité DNS, etc.
- Une sécurité IoT pour contrôler les périphériques non gérés et une sécurité SaaS pour contrôler les applications SaaS (CASB nouvelle génération).

Assurez-vous que vous disposez de l'ensemble d'outils approprié pour protéger votre réseau et à utiliser dans et avec la politique de sécurité.

STEP 1 | Vous ne pouvez pas vous défendre contre des menaces que vous ne pouvez pas voir. Décryptez tout le trafic possible, conformément à la conformité légale, aux réglementations locales, aux réglementations en matière de confidentialité et aux considérations commerciales, pour obtenir une visibilité sur le trafic afin de pouvoir l'inspecter et prévenir les menaces. Pour le décryptage de type Proxy de transfert SSL (sortant), mettez d'abord en œuvre le filtrage des ID utilisateur et des URL afin de pouvoir cibler efficacement le décryptage. Certains trafics ne peuvent pas être décryptés pour des raisons techniques telles que les certificats épinglés, l'authentification client et les certificats intégrés dans les périphériques IoT.

Si vous ne décryptez pas le trafic, le pare-feu ne peut pas identifier les applications de manière granulaire. Par exemple, le pare-feu peut voir que l'application conteneur est Facebook, mais ne peut pas voir l'application fonctionnelle. Vous ne savez donc pas et ne pouvez pas contrôler si l'utilisateur télécharge, publie ou autre sur Facebook. Le pare-feu ne peut pas non plus voir et inspecter la charge utile. Vous n'avez donc pas la visibilité nécessaire pour vous défendre contre le contenu malveillant. Pour tirer le meilleur parti de vos autres abonnements et obtenir la meilleure protection, vous devez décrypter le trafic pour obtenir une visibilité sur celui-ci.

Le décryptage ne nécessite pas de licence, mais pour décrypter le trafic sortant, ajoutez une licence de filtrage des URL avancé afin de pouvoir adopter une approche granulaire du décryptage et choisir facilement les types de trafic à décrypter ou non. Le filtrage des URL vous permet d'exclure les catégories que vous ne devez pas décrypter pour des raisons juridiques, personnelles, réglementaires ou autres. Le filtrage des URL vous permet également de bloquer l'accès des utilisateurs aux sites Web malveillants.

De plus, décryptez le trafic entrant pour protéger les serveurs critiques et décryptez le trafic du proxy SSH pour empêcher le trafic de gestion malveillant.

Suivez les meilleures pratiques en matière de décryptage pour préparer, déployer et maintenir le décryptage.

STEP 2 | Visualisez les processus de planification et de déploiement sous l'angle de l'accès au moindre privilège et de l'accès réseau Zero Trust.

Comprenez qui doit utiliser quelles applications pour accéder à quelles données et quelle infrastructure. Cela vous permet de créer des règles de politique de sécurité qui autorisent uniquement les personnes ayant besoin d'un accès à des fins professionnelles à accéder uniquement aux données et à l'infrastructure nécessaires tout en bloquant tous les autres accès.

Utilisez les attributs disponibles dans la politique de sécurité pour définir l'accès au moindre privilège : utilisateurs, périphériques, applications, source et destination, service et URL (pour le trafic sortant, avec le décryptage activé afin que le pare-feu ait une visibilité sur chaque application fonctionnelle, pas seulement sur l'application conteneur).

STEP 3 | Obtenez les abonnements appropriés à votre entreprise pour obtenir la meilleure prévention des menaces et la meilleure posture de sécurité.

- Filtrage des URL avancé : service fourni dans le cloud qui permet un accès sécurisé aux sites Web, protège les utilisateurs des sites dangereux et aide à prévenir les attaques d'hameçonnage des informations d'identification.
- Prévention avancée des menaces ou protection active contre les menaces existantes : la prévention avancée des menaces fournie dans le cloud utilise des modèles d'apprentissage profond et d'apprentissage automatique en ligne pour l'application en temps réel des menaces de commande et de contrôle (C2) évasives et immédiates, et inclut toutes les fonctionnalités de la prévention des menaces standard. La prévention des menaces standard protège contre les exploits C2, les logiciels malveillants et les vulnérabilités.

  Les environnements isolés ne peuvent pas utiliser la prévention avancée des menaces, car il s'agit d'un service cloud qui nécessite une connexion cloud.

  Suivez les meilleures pratiques en matière de mises à jour du contenu des menaces *pour vous assurer que vous disposez des protections les plus récentes.*
- Sécurité DNS : (vous devez acheter une licence Advanced Threat Prevention ou disposer d'une licence Threat Prevention héritée active et d'une licence DNS Security pour l'activer) Service fourni dans le cloud qui identifie et bloque les menaces dans le trafic DNS et empêche la connexion à des sites DNS malveillants et est constamment mis à jour pour empêcher de nouveaux types d'attaques basées sur le DNS.
- Prévention des pertes de données d'entreprise (DLP) : service fourni dans le cloud qui protège les données sur tous les réseaux d'entreprise, les clouds et les utilisateurs, et permet la conformité aux réglementations en matière de sécurité des données.
- Cortex Data Lake (CDL) : stockage de journaux basé sur le cloud qui évolue en fonction de votre volume de journaux et ingère les journaux des pare-feu nouvelle génération, Panorama, Prisma Access et Cortex XDR. La plupart des applications Cortex utilisent CDL pour accéder, analyser et créer des rapports sur vos données réseau enregistrées.
- WildFire : environnement d'analyse basé sur le cloud ou privé qui identifie les logiciels malveillants connus et inconnus (nouveaux) et génère des signatures que le pare-feu utilise pour identifier et bloquer le trafic malveillant.

- Sécurité SaaS : service fourni dans le cloud qui sécurise vos applications SaaS approuvées avec des licences pouvant être autonomes ou groupées :
  - La licence Data Security inclut l'API de sécurité SaaS et Enterprise DLP.
  - La licence complémentaire SaaS Security Inline fonctionne avec CDL pour découvrir et contrôler toutes les applications SaaS sur votre réseau, y compris les applications Shadow IT, et permet la recommandation de politiques SaaS à l'administrateur du pare-feu.
  - Enterprise DLP pour protéger contre la perte de données dans les applications SaaS.
- Sécurité IoT : détecte et sécurise les périphériques IoT sur votre réseau et active des recommandations automatiques de règles de politique IoT à l'administrateur du pare-feu. Suivez les meilleures pratiques en matière de sécurité IoT pour la planification, le déploiement et la surveillance.
- GlobalProtect : offre des fonctionnalités allant au-delà des fonctionnalités VPN gratuites, notamment l'application mobile GlobalProtect, les contrôles HIP, le VPN sans client et bien plus encore.

STEP 4 | Passez en revue votre plan de segmentation de réseau.

Pour Panorama Managed Prisma Access, il n'y a en réalité que deux zones, confiance et non confiance, et vous mappez toutes les zones Panorama à la zone de confiance Prisma ou de non confiance Prisma.

Sur Panorama et les pare-feu, si une zone n'est pas suffisamment granulaire et inclut des périphériques, des utilisateurs et des applications qui nécessitent un traitement de sécurité différent, envisagez de réarchitecturer vos zones pour segmenter le réseau de manière plus granulaire. Placez les utilisateurs, les applications et les périphériques nécessitant un traitement similaire dans la même zone. Les petites zones sont plus faciles à défendre que les grandes zones.

Dans certains environnements cloud, l'architecture peut limiter le nombre de zones que vous pouvez configurer.

Suivez les meilleures pratiques DoS et de protection de zone pour éviter les attaques par inondation et protéger les périphériques de chaque zone ainsi que les tampons de votre pare-feu.

Pour Cloud Managed Prisma Access, basez la microsegmentation sur l'identité.

STEP 5 | Définissez les applications que vous devez autoriser à des fins commerciales (applications sanctionnées) et les applications à autoriser à d'autres fins (applications tolérées).

Utilisez App-ID dans la politique de sécurité (aucun abonnement requis) pour identifier les applications conteneurs et leurs applications fonctionnelles (par exemple, pas seulement « facebook », mais « facebook-post », « facebook-download », etc.). Si vous utilisez la sécurité SaaS, utilisez App-ID Cloud Engine (ACE) pour identifier les applications cloud (nécessite un abonnement à la sécurité SaaS).

Le pare-feu autorise les applications que vous spécifiez dans les règles de politique de sécurité dont l'**Action** est définie sur **Allow (Autoriser)** et bloque les applications spécifiées dans les règles dont l'**Action** refuse, supprime ou réinitialise le trafic, en fonction des critères de la règle. Le trafic doit répondre à tous les critères d'une règle pour correspondre à la règle. Si une application ne correspond à aucune règle, les deux règles par défaut situées en bas de la base de règles de politique de sécurité contrôlent le trafic. Le trafic interzonal (la source et la destination se trouvent dans des zones

différentes) est refusé par défaut. Le trafic intrazonal (la source et la destination sont dans la même zone) est autorisé par défaut.

Communiquez la politique d'accès afin que les employés comprennent pourquoi ils ne peuvent pas accéder à certaines applications.

STEP 6 | Identifiez tous les utilisateurs. Contrôlez qui a accès à quelles applications et périphériques dans la politique de sécurité pour garantir qu'une politique cohérente suit chaque utilisateur partout sur le réseau.

User-ID (aucun abonnement requis) combine les informations utilisateur provenant de plusieurs sources pour identifier tous les utilisateurs de votre réseau. Pour garantir que l'identification des utilisateurs est cohérente et évolutive sur l'ensemble de votre réseau, utilisez Cloud Identity Engine (CIE) (aucun abonnement requis) comme source unique agrégée pour User-ID. CIE rassemble et synchronise les données utilisateur à partir de sources réparties sur votre réseau. Tous les pare-feu extraient exactement les mêmes informations utilisateur de CIE, qu'ils soient sur un campus ou dans le cloud. CIE fournit également une authentification en collaboration avec la plupart des principaux fournisseurs d'identité (IdP) tels qu'Okta, Azure AD, PingID, etc.

Dans PAN-OS 10.2 et versions antérieures, CIE fournit des services de synchronisation de répertoire (DSS) et d'authentification cloud (CAS). À partir de PAN-OS 11.0, vous pouvez également utiliser CIE comme points de redistribution.

Lors de la configuration des groupes d'utilisateurs, réfléchissez à qui doit accéder aux mêmes ressources de la même manière pour les mêmes objectifs commerciaux et suivez les meilleures pratiques pour le mappage de groupes d'utilisateurs et les meilleures pratiques pour les groupes d'utilisateurs dynamiques (DUG).

Utilisez le VPN GlobalProtect en mode toujours actif pour une sécurité maximale et une identification fiable des utilisateurs si possible. Utilisez GlobalProtect pour l'accès à distance et avec des passerelles internes pour collecter des informations d'identification utilisateur, quel que soit l'endroit où se trouvent vos utilisateurs.

STEP 7 | Prévoyez de joindre les profils de sécurité ou le groupe de profils de sécurité appropriés à chaque règle de politique de sécurité autorisant le trafic. (Si une règle bloque le trafic, le pare-feu n'inspecte pas le trafic bloqué.)

Les groupes de profils de sécurité sont des groupes de profils optimisés dans un but particulier que vous appliquez aux règles de politique de sécurité au lieu d'appliquer chaque profil individuellement. Cela permet de gagner du temps et d'éviter une erreur de configuration accidentelle.

STEP 8 | Planifiez comment stocker les journaux (dans CDL, sur Log Collectors (Collecteurs de journaux), etc.) et quels administrateurs informer pour différents types et différentes gravités d'événements de journaux. Prévoyez une capacité de stockage de journaux suffisante pour permettre d'enquêter sur les événements après qu'ils se soient produits.

STEP 9 | Utilisez un volet de gestion unique tel que Panorama ou Cloud Managed Prisma Access pour gérer votre déploiement et bénéficier d'une sécurité plus simple et plus cohérente.

STEP 10 | Suivez les meilleures pratiques en matière d'accès administratif pour garantir un accès moindre aux privilèges des administrateurs Panorama et du pare-feu.

STEP 11 | Les configurations du jour 1, qui sont disponibles sur le portail de support client (**Tools (Outils)** > **Run Day 1 Configuration (Exécuter la configuration du jour 1)**) et nécessitent une connexion au support, sont des modèles qui fournissent un modèle de configuration indépendant du cas d'utilisation pour démarrer votre chemin vers l'accès au moindre privilège. Les configurations du jour 1 vous aident à mettre en œuvre immédiatement les meilleures pratiques de base en matière de sécurité réseau, y compris pour les éléments critiques tels que les mises à jour dynamiques, les profils de sécurité, la journalisation, etc.

Déploiement des meilleures pratiques en matière de politique de sécurité

Le déploiement des meilleures pratiques en matière de politique de sécurité comprend les éléments suivants :

- Meilleures pratiques en matière de règles de politique de sécurité : ces meilleures pratiques sont axées sur tous les aspects de la construction des règles de politique de sécurité, comme les utilisateurs qui peuvent accéder à certaines applications et ressources spécifiques, la manière d'y accéder et l'application de profils de menace qui aident à protéger le trafic contre les logiciels malveillants.
- Meilleures pratiques en matière de base de règles de politique de sécurité : ces meilleures pratiques sont axées sur la séquence des règles de politique de sécurité dans la base de règles et sur la façon dont cela affecte le trafic que vous autorisez et bloquez.
- Meilleures pratiques de Policy Optimizer : ces meilleures pratiques sont axées sur l'utilisation de Policy Optimizer pour renforcer la base de règles et réaliser sa maintenance.
- Meilleures pratiques d'App-ID Cloud Engine : ces meilleures pratiques sont axées sur l'utilisation d'App-ID cloud dans la politique de sécurité et sur l'automatisation de l'ajout de nouveaux App-ID cloud à la base de règles. (App-ID Cloud Engine nécessite un abonnement SaaS Security Inline.)
- Meilleures pratiques en matière de recommandations de politiques : ces meilleures pratiques sont axées sur la recommandation de politiques SaaS et IoT. (La recommandation de politiques SaaS nécessite un abonnement SaaS Security Inline et la recommandation de politiques IoT nécessite un abonnement IoT Security.)

Gardez à l'esprit les principes suivants lors de la planification et du déploiement :

- Le principe du moindre privilège, qui consiste à accorder l'accès uniquement aux personnes qui en ont besoin et qui utilisent uniquement les applications appropriées, à partir des sources et vers les destinations appropriées.
- Suivez les meilleures pratiques en matière de décryptage. Décryptez le trafic dans toute la mesure permise par vos considérations professionnelles, la conformité juridique et les réglementations locales et relatives à la confidentialité le permettent afin d'obtenir une visibilité maximale sur le trafic et d'être en mesure de l'inspecter et de le contrôler. Pour le décryptage de type Proxy de transfert SSL (sortant), mettez d'abord en œuvre le filtrage des ID utilisateur et des URL afin de pouvoir cibler efficacement le décryptage.

  Pour le décryptage sortant, procurez-vous une licence Advanced URL Filtering afin que le filtrage d'URL puisse bloquer l'accès aux sites web malveillants révélés par le décryptage.

  Certains trafics ne peuvent pas être décryptés pour des raisons techniques, comme des certificats épinglés, l'authentification client, des certificats intégrés à des appareils IoT, etc.
- Inspectez tout le trafic dans les deux sens pour détecter les menaces. N'approuvez rien implicitement.

- Utilisez autant que possible l'automatisation pour vous assurer que la politique de sécurité reste à jour à l'aide de groupes d'adresses dynamiques (DAG), de listes dynamiques externes (EDL) et de fonctionnalités de surveillance VM.

  Utilisez l'étiquetage automatique pour automatiser les actions de sécurité pour les utilisateurs et les périphériques en fonction des événements de journaux. L'étiquetage automatique vous permet d'automatiser les actions à effectuer lorsqu'un événement de journal se produit, par exemple, mettre en quarantaine un périphérique potentiellement infecté ou forcer un utilisateur à utiliser l'authentification MFA.
- Évitez le ballonnement de la configuration :
  - Réutilisez des objets tels que des profils de sécurité et des groupes de profils, des étiquettes, des groupes d'applications, des filtres d'application, des groupes d'utilisateurs et des groupes d'adresses. Sur Panorama, utilisez des objets partagés pour éviter de configurer les mêmes objets pour plusieurs groupes d'appareils.
  - Avant d'ajouter une nouvelle règle de politique à la base de règles, vérifiez les règles existantes pour voir si vous pouvez ajouter de nouvelles applications, de nouveaux utilisateurs ou de nouveaux périphériques aux règles existantes au lieu de créer plusieurs règles similaires.

    Vérifiez si une règle existante est identique à celle que vous voulez ajouter, à l'exception de l'un des objets suivants : zone source, zone de destination, adresse IP source, adresse IP de destination, application, port de service ou utilisateur. Si un seul de ces objets est différent, ajoutez le nouvel objet à la règle existante au lieu de créer une nouvelle règle.

    Par exemple, imaginez que vous souhaitez autoriser une nouvelle application de comptabilité. Lorsque vous examinez la base de règles existante, vous trouvez une règle pour une autre application de comptabilité qui autorise l'accès à partir de la même source à la même destination, pour les mêmes groupes d'utilisateurs, à l'aide du port par défaut de l'application. Au lieu d'écrire une nouvelle règle pour la nouvelle application, ajoutez simplement la nouvelle application à la règle existante.

    

    Cette méthode est également utile pour consolider les règles existantes.
  - Pour le trafic sortant, créez une règle basée sur des catégories d'URL pour plusieurs applications qui nécessitent le même traitement de sécurité. Par exemple, pour autoriser tout le trafic des services financiers à faible risque (en supposant que vous souhaitiez inspecter et journaliser le trafic de la même manière), créez une règle d'autorisation qui spécifie à la fois les catégories d'URL **financial-services (services financiers)** et **low-risk (faible risque)**.
  - Utilisez Policy Optimizer pour supprimer les règles inutilisées.
- Utilisez Panorama ou Cloud Managed Prisma Access pour gérer les déploiements de pare-feu afin de pouvoir utiliser des groupes d'appareils pour appliquer une politique de sécurité cohérente à un pare-feu ou des groupes de pare-feu.

  Utilisez des règles « avant » et règles « après » de manière appropriée :
  - Règles « avant » : les pare-feu évaluent les règles « avant » avant les règles définies localement et les règles « après ». (Les règles définies localement sur des pare-feu individuels ne s'appliquent qu'à ces pare-feu.) Placez les politiques qui s'appliquent à tous les déploiements de pare-feu dans les règles « avant », comme la politique d'autorisation du DNS et d'autres services critiques et la politique d'utilisation des EDL de menace prédéfinies pour bloquer les adresses IP malveillantes et à haut risque connues.

- Règles « après » : les pare-feu évaluent ces règles après les règles « avant » et les règles définies localement.

*Dans les règles de politique de sécurité Panorama, utilisez l'onglet **Target (Cible)** pour exclure des pare-feu ou des sous-ensembles de groupes d'appareils spécifiques de la règle (**Target to all but these specified devices (Cibler tous les périphériques sauf ceux spécifiés)**). Cela vous permet de créer une règle générale plus haut dans la hiérarchie au lieu de devoir créer plusieurs règles similaires plus bas dans la hiérarchie pour prendre en compte une exception.*

- La politique de contrôle prioritaire sur l'application n'est pas la même que la politique de sécurité de couche 7. Ne l'utilisez que si vous en avez absolument besoin, car le contrôle prioritaire sur l'application supprime de nombreux contrôles de sécurité inhérents à la plateforme Palo Alto Networks. Le contrôle prioritaire sur l'application augmente les risques, car elle ne permet pas d'inspecter le trafic de la couche 7, d'utiliser des profils de sécurité pour protéger le trafic contre les menaces ou d'utiliser App-ID. Dans la plupart des cas, il est préférable de créer une application propre à l'entreprise ou d'utiliser un délai d'expiration de service personnalisé plutôt que d'utiliser le contrôle prioritaire sur l'application.

  Passez en revue votre base de règles existante. Si vous avez des règles de contrôle prioritaire sur l'application pour un trafic autre que SMB ou SIP, convertissez la règle en une règle basée sur App-ID afin de pouvoir décrypter et inspecter le trafic au niveau de la couche 7 et empêcher les menaces. Si la règle concerne le trafic SMB ou SIP, assurez-vous qu'elle respecte le principe de l'accès à moindre privilège et qu'elle est aussi restrictive que possible.

Meilleures pratiques en matière de règles de politique de sécurité

Cette section couvre la construction des règles de politique de sécurité, depuis qui peut accéder à quelles applications et ressources, de quelle manière, jusqu'à l'application de profils de menace qui aident à protéger le trafic contre les logiciels malveillants.

Les règles de politique de sécurité définissent les critères de correspondance du trafic, notamment les applications, les utilisateurs, les périphériques, la source et la destination, les URL et les services (ports). La combinaison de critères de correspondance ajoute un contexte plus granulaire à une règle, restreint la portée de la règle et réduit la surface d'attaque. Les critères de correspondance vous permettent de définir le trafic exact que vous souhaitez contrôler avec la règle et d'adhérer aux principes Zero Trust Network Access (ZTNA).

Les règles de politique de sécurité définissent également les actions à entreprendre sur le trafic qui correspond aux critères d'une règle, notamment l'autorisation ou le refus du trafic, la journalisation et le transfert des journaux, l'inspection des menaces et la planification.

Créez des règles de politique de sécurité les plus spécifiques possibles pour appliquer le principe du moindre privilège et segmenter le réseau.

- Concepts critiques pour la politique de sécurité—Comment fonctionnent les règles de politique de sécurité.
- Nom de la règle, description, commentaires d'audit et étiquettes—Meilleures pratiques pour gérer les règles de politique de sécurité.
- Sources et destinations— Meilleures pratiques pour appliquer le principe du moindre privilège pour verrouiller les sources et les destinations du trafic.

- Applications et services—Meilleures pratiques pour ajouter des applications aux règles.
- Accès au site Web (filtrage des URL)—Meilleures pratiques pour autoriser l'accès des utilisateurs à des sites Web externes.
- Actions de stratégie et autres paramètres—Meilleures pratiques pour autoriser ou refuser le trafic et appliquer QoS.
- Journalisation et transfert des journaux—Meilleures pratiques en matière de journalisation du trafic et de transfert des journaux pour un stockage et une analyse à long terme.
- Profils de sécurité—Meilleures pratiques pour appliquer des profils de sécurité aux règles de politique de sécurité.

Concepts critiques pour la politique de sécurité

Pour créer une politique de sécurité efficace, il est utile de comprendre les concepts essentiels sur le rôle des règles de politique de sécurité, leur fonctionnement dans la base de règles de politique de sécurité, la façon dont le trafic correspond aux règles et les meilleures pratiques pour la construction de règles.

- Décryptez tout le trafic autorisé par les réglementations locales, la conformité, les exigences commerciales et les considérations de confidentialité. Pour le décryptage de type Proxy de transfert SSL (sortant), mettez d'abord en œuvre le filtrage des ID utilisateur et des URL afin de pouvoir cibler efficacement le décryptage. Le décryptage du trafic offre une visibilité permettant au pare-feu d'identifier les applications fonctionnelles (par exemple, pas seulement Facebook mais la publication Facebook, le téléchargement Facebook, le partage de fichiers Facebook, etc.), d'identifier les sites Web et d'appliquer des profils de menace pour inspecter et prévenir les menaces dans le trafic. Le décryptage du trafic vous permet de bénéficier d'une protection et d'une prévention optimales grâce à vos abonnements aux alertes contre les menaces.
- **Règles d'autorisation ou de blocage :** la politique de sécurité sur les pare-feux de Palo Alto Networks est basée sur l'autorisation explicite du trafic dans les règles de politique et sur le déni de tout trafic que vous n'autorisez pas explicitement (liste verte). Le trafic que vous n'autorisez pas explicitement est implicitement refusé. L'objectif est d'autoriser uniquement les applications, les utilisateurs et les périphériques que vous souhaitez sur votre réseau et de laisser le pare-feu bloquer automatiquement ce que vous ne voulez pas.

  À mesure que vous évoluez vers une politique de sécurité basée sur une liste d'autorisation, utilisez des règles de blocage pour empêcher l'accès aux adresses IP, aux sites Web et aux applications à risque. Créez et testez des règles de blocage basées sur les listes dynamiques externes (EDL) prédéfinies pour bloquer les adresses IP à toute épreuve, les adresses IP à haut risque et les adresses IP malveillantes connues qui se cachent dans des catégories d'applications par ailleurs inoffensives et pour empêcher l'authentification auprès d'une URL ou d'un domaine malveillant. Utilisez le filtrage des URL avancé pour bloquer l'accès aux sites Web à risque.

  

  Soyez particulièrement prudent avec les applications de partage de fichiers, car de mauvais acteurs peuvent les utiliser pour exfiltrer des données. Bloquez la plupart des applications de partage de fichiers. Pour les applications de partage de fichiers dont vous avez besoin à des fins professionnelles, autorisez l'accès uniquement aux utilisateurs qui ont besoin de ces applications à des fins professionnelles.

  Pour une sécurité optimale, autorisez uniquement les applications utilisées à des fins professionnelles. Cependant, la plupart des entreprises doivent autoriser certaines applications non professionnelles pour les employés (applications tolérées). Réfléchissez pour déterminer les applications tolérées à autoriser et demandez-vous si ces applications représentent une menace pour l'organisation, comme la possibilité

de télécharger des données vers l'amont ou vers l'aval. Décryptez et inspectez autant de trafic que possible pour détecter les menaces.

- Les règles de politique de sécurité sont spécifiques. Si le trafic ne correspond pas à tous les critères spécifiés dans une règle de politique de sécurité, le trafic ne correspond pas à la règle. Par exemple, si une règle spécifie un utilisateur particulier, une application, ainsi qu'une source et une destination, le trafic doit répondre à tous ces critères pour correspondre à la règle. Si l'utilisateur, la source et la destination correspondent mais que l'application ne correspond pas, alors le trafic ne correspond pas à la règle.
- Les règles de politique de sécurité segmentent votre réseau en définissant qui a accès à quelles applications et infrastructures. Les règles segmentent le réseau en définissant la source, la destination, l'utilisateur, le périphérique, le service et l'URL.
- Les règles de politique de sécurité appliquent tous les profils de prévention contre les menaces attachés au trafic qui correspond aux règles.
- Les règles de politique de sécurité se trouvent dans une base de règles ordonnée (vous choisissez l'ordre des règles). Les pare-feux comparent le trafic aux règles de politique de sécurité en commençant par la première règle de la base de règles de politique de sécurité et en passant par la dernière règle de la base de règles. Lorsque le trafic correspond aux critères d'une règle, le pare-feu applique l'action de la règle sur le trafic et ne compare pas le trafic à d'autres règles. Si aucune règle ne correspond au trafic, le pare-feu abandonne le trafic (déni implicite).
- Placez des règles de politique de sécurité plus spécifiques et granulaires au-dessus des règles générales dans la base de règles pour éviter de faire de l'ombre à une règle. L'effet d'ombre se produit lorsqu'une règle générale qui inclut les mêmes critères de correspondance qu'une règle plus spécifique est placée plus haut dans la base de règles que la règle spécifique. Dans ce cas, le trafic destiné à correspondre à la règle spécifique correspond en premier lieu à la règle générale.
- Si le trafic ne correspond à aucune autre règle, deux règles de politique de sécurité par défaut situées au bas de la base de règles suppriment automatiquement tout le trafic entre différentes zones (**interzone-default**) et autorisent automatiquement tout le trafic entre la même zone (**intra-zone-default**). Vous pouvez modifier les règles par défaut interzone et intra-zone par défaut pour enregistrer le trafic, appliquer une inspection des menaces, etc. Si vous ajoutez une règle qui refuse tout le trafic plus tôt dans la base de règles (règles de pare-feu locales ou règles « avant » et les règles « après » Panorama), aucun trafic ne correspond aux règles par défaut.
- Appliquez le principe du moindre privilège d'accès à la construction des règles de politique de sécurité (être granulaire, précis) :
  - Contrôlez quels administrateurs ont accès pour administrer quelles parties de quels pare-feux et périphériques Panorama. Suivez les meilleures pratiques pour sécuriser l'accès administratif.
  - Identifiez tous les utilisateurs (aucun utilisateur inconnu ne doit se trouver sur votre réseau), identifiez les applications que vous souhaitez autoriser sur votre réseau et connaissez votre infrastructure (ressources auxquelles les utilisateurs et les applications accèdent). Cartographiez qui a besoin d'accéder à quelles applications et ressources à des fins professionnelles afin que vos règles de politique de sécurité n'autorisent aucun accès inutile. Autorisez l'accès aux ressources professionnelles et aux applications autorisées uniquement aux utilisateurs qui en ont besoin à des fins professionnelles, et n'autorisez que l'accès minimum requis.
  - Autorisez l'accès aux applications non professionnelles que vous tolérez au profit de vos employés.
  - Dans la plupart des cas, utilisez des règles d'autorisation plutôt que des règles de blocage : il est plus précis et plus facile de définir ce que vous souhaitez autoriser sur votre réseau et de dénier

implicitement le reste que de bloquer explicitement le nombre toujours croissant d'applications que vous ne désirez pas sur votre réseau.

- Optimisez la base de règles pour modifier les règles avec les applications inutilisées et pour supprimer ou désactiver les règles qui ne sont pas utilisées.

Nom de la règle, description, commentaires d'audit et étiquettes

Les champs Nom, Description, Commentaires d'audit et Étiquettes facilitent la gestion votre base de règles de politique de sécurité, la navigation dans cette base et la compréhension du rôle de chaque règle. Ils aident également les administrateurs nouveaux et expérimentés à comprendre quand ajouter une nouvelle application, un nouvel utilisateur ou un groupe d'utilisateurs à une règle existante et quand créer une nouvelle règle.

STEP 1 | **Name (Nom)** : identifie l'action de chaque règle.

Développez une convention de dénomination standard qui utilise des termes facilitant la recherche dans la base de règles. Les noms qui indiquent clairement aux administrateurs ce que fait chaque règle facilitent la compréhension du trafic contrôlé par chaque règle et rendent la recherche d'une règle particulière plus facile et plus intuitive.

STEP 2 | **Description :** décrit l'objectif de la règle afin que toute personne examinant la base de règles puisse comprendre pourquoi la règle a été créée et le résultat escompté.

Pour vous assurer que toutes les politiques ont une description dans PAN-OS et Panorama Managed Prisma Access, activez **Require description on policies (Exiger une description sur les politiques)** dans **Panorama** > **Setup (Configuration)** > **Management (Gestion)** > **Policy Rulebase Settings (Paramètres de base de règle de politique)** (**Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **Policy Rulebase Settings (Paramètres de base de règle de politique)** sur des pare-feux individuels). Pour les règles existantes sans description, ajoutez-en une la prochaine fois que vous modifierez la règle.

Dans Cloud Managed Prisma Access, assurez-vous que les administrateurs saisissent une description.

STEP 3 | **Tags (Étiquettes)** : descripteurs de haut niveau pour décrire les composants basés sur les flux, les politiques basées sur les applications, les services internes, les groupes d'utilisateurs particuliers, selon ce qui est pertinent pour votre entreprise.

Les étiquettes organisent les stratégies en groupes, ce qui vous permet de filtrer et de rechercher des stratégies en fonction des étiquettes.

Par exemple, si vous créez une étiquette appelée **`désactivée`** et que vous l'appliquez à toutes les règles désactivées, vous pouvez filtrer la base de règles et voir toutes les règles désactivées en fonction de cette étiquette. En utilisant la même étiquette, vous pouvez rechercher dans la base de règles les règles étiquetées **`désactivées`** mais qui ont été réactivées en filtrant l'étiquette **`désactivée`** et **`le numéro d'équation désactivé`**.

Pour vous assurer que toutes les politiques ont une étiquette dans PAN-OS et Panorama Managed Prisma Access, activez **Require Tag on policies (Exiger l'étiquette sur les politiques)** dans **Panorama** > **Setup (Configuration)** > **Management (Gestion)** > **Policy Rulebase Settings (Paramètres de base de règle de politique)** (**Device (Périphérique)** > **Configuration** > **Management (Gestion)** > **Policy Rulebase Settings (Paramètres de base de règle de politique)** sur des pare-feux individuels). Pour les règles existantes sans étiquette, ajoutez-en une la prochaine fois que vous modifierez la règle.

STEP 4 | Empêchez les administrateurs de valider des stratégies s'ils n'ont pas d'étiquettes ou de description.

Dans PAN-OS et Panorama Managed Prisma Access, activez **Fail commit if policies have no tags or description (Pas de validation si les politiques n'ont pas d'étiquette ou de description)** dans **Panorama** > **Setup (Configuration)** > **Management (Gestion)** > **Policy Rulebase Settings (Paramètres de base de règle de politique)** (**Périphérique** > **Setup (Configuration)** > **Management (Gestion)** > **Policy Rulebase Settings (Paramètres de base de règle de politique)** sur des pare-feu individuels). Pour les règles existantes, la validation échoue si vous n'ajoutez pas d'étiquette et de description la prochaine fois que vous modifierez la règle.

STEP 5 | **Audit Comments (Commentaires d'audit)** : suit les modifications apportées aux règles et les raisons pour lesquelles elles ont été apportées afin que vous disposiez d'un historique des modifications apportées aux règles et des justifications de ces modifications. Ceci est particulièrement utile pour documenter les règles qui ne sont utilisées qu'en cas de reprise après sinistre ou de manière limitée.

Dans PAN-OS et Panorama Managed Prisma Access, assurez-vous que toutes les stratégies incluent des commentaires d'audit, activez **Require audit comment on policies (Exiger un commentaire d'audit sur les stratégies)** dans **Panorama** > **Setup (Configuration)** > **Management (Gestion)** > **Policy Rulebase Settings (Paramètres de base de règle de politique)** (**Device (Périphérique)** > **Setup (Configuration)** > **Management (Gestion)** > **Policy Rulebase Settings (Paramètres de base de règle de politique)** sur des pare-feu individuels) et spécifiez un format de commentaire d'audit. Pour les règles existantes sans commentaires d'audit, vous devrez les ajouter la prochaine fois que vous modifierez la règle.

Les commentaires d'audit restent fidèles à la règle de manière permanente. Cliquez sur **Audit Comment Archive (Archive des commentaires d'audit)** dans la règle pour afficher l'historique, qui ne peut pas être supprimé.

Sources et destinations

Contrôler les sources et les destinations du trafic consiste à suivre le principe de l'accès à moindre privilège. Créez des règles de politique de sécurité qui spécifient la source et la destination exactes du trafic des applications auxquelles vous souhaitez faire correspondre la règle. Autoriser le trafic sur la règle à partir de sources et de destinations dont les applications n'ont pas besoin à des fins commerciales augmente la surface d'attaque, ce qui augmente le risque. Limiter strictement les sources et les destinations à celles nécessaires à des fins commerciales réduit les surfaces d'attaque et diminue le risque.

Le contrôle granulaire de la source et de la destination vous aide à mettre en œuvre un accès à moindre privilège :

- Sources : zones, adresses, utilisateurs et périphériques, sécurité 5G, abonnés, équipements et tranche de réseau.
- Destinations : zones, adresses et périphériques.

Dans la mesure du possible, utilisez des objets de groupe d'adresses et de groupe d'utilisateurs au lieu d'adresses et d'utilisateurs individuels pour réduire le nombre d'objets source et de destination. Cela simplifie la politique et la rend plus facile à comprendre. Limitez le nombre total d'objets sources et de destination pour plus de clarté dans la base de règles.

STEP 1 | Dans PAN-OS, spécifiez les zones sources et de destination aussi étroitement que possible pour éviter tout accès inutile aux données et aux applications.

Le fait de consacrer des zones à des fins particulières, comme une zone pour tous les serveurs Web, facilite la création d'une politique granulaire, car tous les serveurs de la zone nécessitent généralement la même politique de sécurité.

Panorama Managed Prisma Access utilise deux zones, confiance et non confiance. Mappez les zones Panorama à la zone approuvée Prisma ou à la zone non approuvée Prisma.

Cloud Managed Prisma Access utilise trois zones : approuvée, non approuvée et VPN sans client, qui est mappé à la zone approuvée par défaut. Dans de nombreuses intégrations SD-WAN tierces, dans Log Viewer, la zone source utilise le nom du réseau distant.

STEP 2 | Spécifiez les adresses sources et de destination aussi précisément que possible pour éviter tout accès inutile aux données et aux applications. Utilisez autant que possible des groupes d'adresses au lieu d'adresses individuelles pour simplifier la politique. Si la règle s'applique à tous les périphériques d'une zone, pour le trafic entrant, spécifiez l'adresse de destination comme **any (n'importe laquelle)** et pour le trafic sortant, spécifiez l'adresse source comme **any (n'importe laquelle)**.

- Utilisez les objets d'adresse FQDN pour référencer les systèmes internes afin que lorsque les adresses IP du système changent, la modification n'affecte pas la stratégie.
- Utilisez des Dynamic Address Groups (groupes d'adresses dynamiques) dans la politique pour vous adapter automatiquement aux changements de rôles de serveur ou de posture de sécurité en fonction des événements de journal et de l'étiquetage automatique. Réfléchissez à la manière de regrouper les serveurs et de développer une stratégie d'étiquetage adaptée à votre entreprise.

  Lorsqu'un événement de journal spécifié se produit, le pare-feu déplace les adresses IP d'un DAG à un autre en fonction de l'étiquetage automatique. Les DAG sont mis à jour automatiquement et ne nécessitent aucune action de validation. Cela vous permet d'effectuer des actions de sécurité automatisées, telles que déplacer un serveur ou un terminal potentiellement infecté depuis un DAG dans une règle de politique autorisant l'accès aux ressources critiques vers un DAG dans une règle de politique qui bloque cet accès (mise en quarantaine d'un périphérique).
- Dans les environnements de centre de données automatisés, utilisez les DAG pour contrôler l'accès aux machines virtuelles lorsque le centre de données démarre et arrête les serveurs virtualisés. Enregistrez dynamiquement les étiquettes à l'aide de l'API XML native ou de l'agent de surveillance VM Monitoring sur le pare-feu.
- Dans les environnements de centres de données, la segmentation combinée à l'automatisation peut rendre difficile la gestion des adresses IP individuelles. En dernier recours, si l'environnement est trop difficile à gérer, utilisez des sous-réseaux, mais c'est une méthode moins sécurisée.
- Utilisez les listes dynamiques externes (EDL) prédéfinies de Palo Alto Networks comme source ou destination pour bloquer le trafic vers et depuis des adresses IP à haut risque, à l'épreuve des balles et autres adresses IP malveillantes.
- Si la conformité, la politique commerciale ou d'autres raisons vous obligent à bloquer des régions géographiques, spécifiez la ou les régions comme adresse. (Pour le trafic entrant, spécifiez la région géographique comme source et **any (n'importe quelle région géographique)** comme

destination. Pour le trafic sortant, spécifiez **any (n'importe quelle région)** comme source et la région géographique comme destination.)

STEP 3 | Spécifiez les utilisateurs source avec l'ID utilisateur afin que la politique de sécurité soit valide pour l'accès sur site et à distance. Une identification cohérente des utilisateurs est essentielle pour garantir une politique cohérente, quels que soient l'emplacement de l'utilisateur et la méthode de connectivité.

- Créez des groupes d'utilisateurs en fonction du contexte. *Que doit faire l'utilisateur à des fins professionnelles ? Quelles sont les exigences d'accès courantes ?* Ce point de vue regroupe les utilisateurs en fonction des ressources auxquelles ils doivent accéder et des applications qu'ils doivent utiliser afin que vous puissiez créer des groupes logiques et leur appliquer une stratégie.

  Demandez à l'équipe de sécurité du réseau de travailler avec l'équipe qui contrôle les groupes d'utilisateurs pour garantir que les groupements ont un sens pour les contrôles de sécurité.

  Spécifiez des utilisateurs individuels dans la politique uniquement lorsque vous ne pouvez pas utiliser de groupes. Par exemple, votre PDG et quelques autres cadres supérieurs peuvent avoir besoin de divers privilèges d'accès que d'autres utilisateurs et groupes ne doivent pas avoir.
- Si votre déploiement le permet, utilisez Cloud Identity Engine (CIE) pour les actions suivantes :
  - Regroupez toutes les sources d'ID utilisateur sur tout votre réseau, à la fois dans le cloud et sur site.
  - Synchronisez les sources du répertoire.
  - Fournissez des informations d'ID utilisateur cohérentes sur l'ensemble du réseau.

  Un ID utilisateur cohérent permet à la politique de suivre les utilisateurs partout sur le réseau.

  CIE fournit l'authentification via l'intégration avec des fournisseurs d'identité tels qu'Okta, Azure AD et bien d'autres.
- GlobalProtect est la source de mappage d'ID utilisateur avec les informations utilisateur les plus précises et complètes et la plus grande précision (il existe également de nombreuses autres sources de mappage d'ID utilisateurpossibles).
- Utilisez des groupes d'utilisateurs dynamiques (DUG) dans la stratégie pour corriger automatiquement les comportements anormaux des utilisateurs et les activités malveillantes en fonction des événements de journal et de l'étiquetage automatique. Les DUG fonctionnent de manière similaire aux DAG. Réfléchissez aux activités qui justifient une mise en quarantaine ou un accès restreint et développez une stratégie d'étiquetage adaptée à votre entreprise.

  Utilisez également les DUG pour autoriser un accès périodique aux groupes d'utilisateurs. Par exemple, un DUG peut autoriser l'accès aux auditeurs trimestriels (tels que définis par un groupe d'utilisateurs pour les auditeurs) pendant les audits et bloquer l'accès à tout autre moment.
- Dans Configuration des règles de politique de sécurité, en plus de spécifier des utilisateurs et des groupes particuliers, vous pouvez spécifier si la règle s'applique à **any (n'importe quel)** utilisateur, aux utilisateurs de **pre-logon (préouverture de session)**, à un **known-user (utilisateur connu)** (authentifié) ou **unknown (inconnu)** (non authentifié) :
  - Utilisez **any (n'importe quel)** pour les règles qui s'appliquent à tous les utilisateurs du réseau, par exemple l'accès aux services de base tels que DNS, NTP, OCSP, etc.

- N’autorisez aucun utilisateur **unknown (inconnu)** sur votre réseau. Créez une règle pour bloquer les utilisateurs inconnus. Vous pouvez également utiliser **unknown (inconnu)** pour l’accès invité, à condition de n’autoriser aucun accès à votre réseau d’entreprise.
- Le VPN d’accès à distance avec préouverture de session est spécifique aux utilisateurs de GlobalProtect. Il établit un tunnel VPN avant que l’utilisateur ne se connecte au périphérique pour authentifier le terminal et permettre l’accès à des services spécifiques tels que DHCP, DNS, etc., et nécessite l’installation de certificats de machine sur chaque terminal. Les règles de politique qui autorisent l’accès des utilisateurs en préouverture de session doivent autoriser l’accès uniquement aux services d’authentification de la machine et aux services réseau nécessaires. Refusez tout autre accès aux utilisateurs de préouverture de session.

Le principe primordial est l’accès à moindre privilège. Autorisez l’accès uniquement aux utilisateurs et aux groupes qui ont besoin d’accéder aux applications et aux ressources à des fins professionnelles.

- Suivez les meilleures pratiques d’ID utilisateur.

STEP 4 | Dans Règles de politique de sécurité qui régissent les périphériques IoT (la sécurité IoT nécessite un abonnement), spécifiez les périphériques IoT à l’aide de l’ID de périphérique (PAN-OS 10.0 et versions ultérieures).

Les objets Périphérique définissent les ID des périphériques IoT et identifient les périphériques sources de la même manière que l’ID utilisateur identifie les utilisateurs sources. Les objets Périphérique disposent de six métriques à utiliser comme critères de correspondance. Un périphérique doit correspondre à toutes les métriques configurées pour correspondre à un ID de périphérique. Dans la plupart des cas, définir une ou deux métriques suffit. Plus vous définissez de métriques, plus il y a de chances que le filtre soit trop spécifique et ne corresponde pas aux périphériques avec lesquels vous souhaitez établir la correspondance. Comprenez quelles informations les périphériques envoient au pare-feu pour savoir quelles métriques configurer pour définir l’objet périphérique (tous les périphériques ne transmettent pas toutes les métriques). Les commandes opérationnelles suivantes affichent les informations que les périphériques IoT envoient au pare-feu :

- **`> show iot ip-device-mapping-mp all`** : affichez tous les mappages d’adresse IP à périphérique sur le pare-feu.
- **`> show iot ip-device-mapping-mp ip <ip-address>`** : affichez le mappage adresse IP-périphérique pour une adresse IP spécifiée.

Suivez les meilleures pratiques de sécurité IoT.

Applications et services

Par défaut, une règle de déni implicite au bas de la base de règles de politique de sécurité bloque les applications que vous n’autorisez pas explicitement dans une règle de politique de sécurité. Pour appliquer l’accès à moindre privilège, affinez les règles de politique de sécurité jusqu’à ce qu’elles spécifient uniquement les applications exactes que vous souhaitez autoriser à des fins professionnelles (applications approuvées) et pour vos employés (applications tolérées). Les règles basées sur les applications vérifient de manière précise qui utilise chaque application fonctionnelle et comment elle est utilisée, afin que vous puissiez créer des règles de politique de sécurité précises à mesure que vous évoluez vers un environnement d’accès réseau Zero Trust . Les règles basées sur le port autorisent n’importe quelle application sur le port ouvert ; évitez-les.

Vous devez activer le décryptage pour que le pare-feu voie l'application fonctionnelle au lieu de simplement l'application « -base ». Le fait de voir l'application fonctionnelle vous permet de contrôler les applications de manière granulaire. Par exemple, au lieu de voir uniquement l'application conteneur « Facebook », le pare-feu voit « publication sur Facebook », « téléchargement sur Facebook », « partage de fichiers sur Facebook », etc. Cela vous permet de configurer la politique de sécurité basée sur l'accès à moindre privilège ; au lieu de donner à tous les employés l'accès à toutes les applications fonctionnelles de Facebook, vous pouvez restreindre ou bloquer l'accès à des applications fonctionnelles spécifiques pour les utilisateurs appropriés.

Lorsque vous ajoutez une application conteneur à une règle, toutes ses applications fonctionnelles sont implicitement ajoutées à la règle. Spécifiez les applications fonctionnelles exactes que vous souhaitez autoriser pour obtenir un contrôle plus granulaire des applications que vous autorisez et des personnes que vous autorisez à les utiliser.

La manière dont vous appliquez les conseils de meilleures pratiques pour les applications dépend du fait que votre environnement soit nouveau, existant ou soit une migration. De nombreuses recommandations reflètent l'état final des meilleures pratiques. Dans certains cas, nous fournissons des conseils de transition ou des conseils sur différents environnements. Cependant, chaque environnement est unique. L'objectif est de comprendre quelles applications traversent votre réseau, quelles applications approuvées et tolérées doivent traverser votre réseau, et d'utiliser ces informations pour passer en toute sécurité à une base de règles de politique de sécurité qui autorise uniquement les applications que vous approuvez à des fins commerciales et tolérez pour l'accès des employés.

Meilleures pratiques en matière de base de règles de politique de sécurité *explique où positionner les règles dans la base de règles de la politique de sécurité.*

1. Utilisez autant que possible les **groupes d'applications** pour simplifier et renforcer la création de règles de politique de sécurité et réduire la taille de la base de règles.

   Les groupes d'applications sont des ensembles d'applications définis par l'utilisateur qui nécessitent un traitement de sécurité similaire. L'ajout d'un groupe d'applications à une règle de politique de sécurité vous permet de contrôler plusieurs applications avec une seule règle au lieu de créer une règle distincte pour chaque application. Si vous devez ajouter une application au groupe ou apporter d'autres modifications, vous ne devez effectuer la modification qu'une seule fois au lieu de l'effectuer dans chaque règle, car lorsque vous mettez à jour un groupe d'applications, les règles qui y font référence sont automatiquement mises à jour.
2. Que vous ajoutiez des applications à un groupe d'applications ou à une règle de politique de sécurité individuelle, spécifiez les applications fonctionnelles exactes souhaitées, sauf si vous utilisez un groupe pour bloquer une application conteneur (qui bloque toutes ses applications fonctionnelles) ou si vous souhaitez autoriser accès à toutes les applications fonctionnelles d'une application conteneur.
3. Les dépendances d'application se produisent lorsqu'une application a besoin d'autres applications (applications dépendantes) pour fonctionner correctement. Les dépendances des applications n'ont d'importance que pour les applications que vous autorisez, et non pour les applications que vous bloquez. Il existe deux types d'applications dépendantes :

   - Applications explicites, que le pare-feu vous montre lorsque vous ajoutez une application à la règle et que vous ajoutez manuellement pour que l'application fonctionne correctement. Par exemple,

l'application facebook-chat dépend de l'ajout manuel des applications facebook-base et mqtt-base à la règle.

- Applications implicites, que le pare-feu autorise automatiquement à prendre en charge l'application spécifiée et que vous n'avez pas besoin d'ajouter explicitement à une règle. Par exemple, en plus des applications explicites requises pour le bon fonctionnement de facebook-chat, lorsque vous ajoutez facebook-chat à une règle, le pare-feu autorise automatiquement le jacassement des applications et la navigation Web. (À moins que vous ne les ajoutiez explicitement à une règle, le jacassement et la navigation Web ne sont pas autorisés pour tout le trafic, uniquement pour le trafic de discussion sur facebook-chat.)

  Rendez-vous compte des applications que vous autorisez implicitement lorsque vous autorisez une application.

Vous pouvez voir les dépendances d'une application de plusieurs manières :

- L'objet **Applications** fournit une base de données consultable d'applications. Sélectionnez une application pour voir ses dépendances d'application explicites (**Depends on (Dépend de)**) et ses dépendances d'application implicites (**Implicitly Uses (Utilise implicitement)**).
- L'Applipedia de Palo Alto Networks est une base de données consultable d'identifiants d'application fournis par le contenu. Recherchez et sélectionnez une application pour voir ses dépendances d'application explicites (**Depends on Applications (Dépend des applications)**) et ses dépendances d'application implicites (**Implicit use Applications (Applications à usage implicite)**).
- Lorsque vous ajoutez une application à une règle de politique de sécurité, le pare-feu vous montre les applications dépendantes explicites, mais non les applications dépendantes implicites.
- Exécutez la commande **Commit Validate (Confirmer la validation)** pour afficher les dépendances des applications en fonction de l'ensemble de la base de règles de politique de sécurité plutôt que d'une seule règle.

Chaque environnement réseau et chaque entreprise étant différents, la manière de gérer les dépendances des applications ne constitue pas une recommandation unique. Il existe deux manières d'aborder les dépendances des applications, en fonction de vos exigences d'entreprise et de sécurité :

- Concentrez-vous sur la disponibilité : ajoutez toutes les applications dépendantes affichées dans une règle de politique de sécurité à la règle pour garantir que l'application fonctionne correctement. Par exemple, pour la règle qui contrôle facebook-chat, ajoutez facebook-base et mqtt-base à la règle.

  Cependant, cela peut entraîner l'ajout de certaines applications dépendantes courantes, telles que SSL, à de nombreuses règles au lieu d'une seule, ce qui ajoute de l'encombrement à la base de règles. (Même si la base de règles autorise déjà SSL, SSL apparaît comme une application dépendante pour nombreuses autres applications.) Un bon moyen d'atténuer ce problème consiste à utiliser Policy Optimizer pour supprimer les occurrences en double des applications dépendantes.
- Concentrez-vous sur la sécurité : pour autoriser le moins d'applications possible, exécutez la commande **Commit Validate (Confirmer la validation)** pour voir toutes les dépendances des applications dans la base de règles de politique de sécurité. Ajoutez les dépendances dont vous avez besoin en fonction de la sortie Commit Validate (Confirmer la validation). Prévoyez de créer des groupes d'applications pour différents ensembles de dépendances d'applications (par exemple, des dépendances VMware, des dépendances de mises à jour logicielles, etc.) contenant toutes les applications dépendantes que vous souhaitez autoriser afin de pouvoir contrôler l'accès en fonction des utilisateurs.

4. Dans les déploiements nouveaux et existants, bloquez immédiatement le trafic malveillant et à risque connu.

   - Bloquez le trafic potentiellement malveillant sur la base de sources fiables de renseignements sur les menaces, y compris les listes dynamiques externes (EDL) intégrées de Palo Alto Networks, qui nécessitent un abonnement Prévention des menaces avancé ou Prévention des menaces et bloquent les adresses IP à toute épreuve, les adresses IP à haut risque et les adresses IP malveillantes connues et les adresses IP connues comme nœuds de sortie Tor.
   - Bloquez le DNS crypté pour maintenir la visibilité sur le trafic et inspecter le trafic à la recherche de menaces à l'aide de profils de menace. Les attaquants utilisent le DNS pour de nombreux types d'attaques, et vous devez donc inspecter le trafic DNS. Bloquez à la fois DNS-over-HTTPS (DoH) et DNS-over-TLS (DoT), puis utilisez le service DNS de Palo Alto Networks. Si vous ne pouvez pas bloquer immédiatement le DNS crypté, gagnez en visibilité sur le trafic et passez au blocage du trafic DoH et (DoT).

     En raison de la granularité d'App-ID, vous pouvez autoriser le trafic DNS normal dans une règle et bloquer le trafic DoT et DoH dans une autre règle, car chacun a un ID d'application (App-ID) différent que vous pouvez spécifier dans une règle de politique de sécurité.

   - Les mauvais acteurs utilisent souvent des applications de partage de fichiers pour exfiltrer des données. Bloquez la plupart des applications de partage de fichiers et autorisez l'accès aux applications de partage de fichiers professionnels uniquement aux utilisateurs qui en ont besoin à des fins professionnelles. Un moyen simple d'y parvenir consiste à créer une règle qui spécifie les utilisateurs et dispose d'un filtre d'application qui inclut la sous-catégorie **file-sharing (partage de fichiers)** et/ou l'étiquette **Uploading (Téléchargement vers l'amont)**.

   La construction d'une politique de sécurité basée sur une liste verte bloque implicitement la plupart des applications indésirables, et vous n'avez donc pas besoin de nombreuses règles de blocage. Basez vos blocages sur les besoins de votre entreprise en autorisant uniquement le trafic d'applications que vous souhaitez sur votre réseau et en réfléchissant à qui doit utiliser chaque application.

5. Définissez le **service** sur **application-default (valeur par défaut de l'application)** dans la plupart des cas. Étant donné qu'App-ID est basé sur des signatures plutôt que sur un port et un protocole (qui peuvent être usurpés), App-ID est très précis. Vous n'avez donc pas besoin de spécifier le port. L'utilisation de la valeur par défaut de l'application empêche toute application, à l'exception de l'application légitime, d'utiliser le port et empêche les applications évasives d'utiliser des ports non standard. Si, à l'avenir, le port par défaut de l'application change, application-default applique automatiquement le nouveau port afin que vous n'ayez pas à reconfigurer les paramètres du port de service.

   Spécifiez uniquement les ports de service si vous disposez d'une application propre à l'entreprise, d'exigences architecturales particulières ou si les exigences de sécurité de votre entreprise l'exigent.

6. Pour les applications internes et les applications pour lesquelles il n'existe pas d'App-ID, créez des applications propres à l'entreprise pour obtenir une visibilité de couche 7 sur le trafic. N'utilisez pas la stratégie de contrôle prioritaire sur l'application, car elle contourne le traitement de couche 7 et l'inspection des menaces. Les cas d'utilisation du contrôle prioritaire sur l'application sont des situations inhabituelles avec le trafic SMB ou SIP.

7. Utilisez des **filtres d'applications** pour découvrir le trafic sur votre réseau et gérer de nouvelles applications.

   Les filtres d'applications sont des ensembles dynamiques d'applications. Les applications correspondent aux filtres d'application en fonction des attributs que vous définissez, tels que la catégorie, la sous-catégorie, le risque, les étiquettes (étiquettes prédéfinies ou étiquettes personnalisées) et les caractéristiques. Le pare-feu ajoute automatiquement de nouvelles applications à un filtre lorsqu'elles correspondent aux critères du filtre. Les règles de politique de sécurité avec un filtre d'application contrôlent automatiquement les nouvelles applications qui correspondent au filtre.

   Les filtres d'applications sont des contrôles plus souples que les groupes d'applications. Vous contrôlez exactement quelles applications se trouvent dans un groupe d'applications. Les attributs que vous définissez déterminent quelles applications se trouvent dans un filtre d'applications, ce qui peut conduire à une adhésion plus large et autoriser plus d'applications que ce dont vous avez besoin. C'est pourquoi ils conviennent parfaitement pour découvrir le trafic afin que vous puissiez le contrôler.

   Les cas d'utilisation incluent ce qui suit :

   - Dans les nouveaux déploiements où vous ne connaissez pas encore bien le trafic, utilisez des filtres d'application pour analyser différentes catégories et sous-catégories de trafic afin de pouvoir découvrir lesquels de ces types d'applications se trouvent sur votre réseau.

     Vous pouvez également créer des filtres d'application pour découvrir le trafic de différents types dans les déploiements matures.

   - Filtrage de la base de règles pour les nouvelles applications. Créez un filtre qui correspond aux nouvelles applications et placez la règle en haut de la base de règles. Utilisez Policy Optimizer pour gagner en visibilité sur les applications et les contrôler.

     Les mises à jour de contenu contrôlent les nouvelles applications. Lorsqu'une mise à jour du contenu des applications est publiée, les nouvelles applications sont considérées comme nouvelles jusqu'à la publication de la prochaine mise à jour du contenu des applications. Les sorties ont normalement lieu le troisième mardi de chaque mois ou vers ce jour-là. Une fois l'ensemble suivant de nouvelles applications publié, l'ensemble précédent de nouvelles applications n'est plus considéré comme nouveau et le filtre d'application ne leur correspond plus. Suivez les meilleures pratiques pour les mises à jour du contenu des applications et des menaces *et décidez comment gérer les nouvelles applications avant la prochaine mise à jour du contenu des applications.*

   - Dans les scénarios de migration, utilisez des filtres d'applications pour bloquer ou autoriser un large éventail de types d'applications spécifiques, puis utilisez Policy Optimizer pour les limiter aux seules applications souhaitées sur le réseau. Les filtres d'applications vous permettent également de garantir que certains types de nouvelles applications sont automatiquement autorisés lorsqu'elles correspondent à un filtre.

- Règles pérennes en traitant les nouvelles applications automatiquement lorsqu'elles correspondent à un filtre. Ceci est utile à la fois dans la phase de découverte des applications dans les migrations et les nouveaux déploiements et dans les environnements matures.

  Par exemple, créez une règle d'autorisation avec un filtre d'application basé sur l'étiquette **Palo Alto Networks**. Cela garantit que vous autorisez toutes les applications Palo Alto Networks actuelles et toutes les applications Palo Alto Networks futures.

  Un autre exemple est la création d'une règle qui filtre les nouveaux App-ID fournis par le contenu pour les gérer en toute sécurité jusqu'à ce que vous puissiez les examiner de plus près.

8. Les définitions d'application ne sont pas statiques. Les mises à jour du contenu des applications peuvent modifier la définition d'une application et donc la façon dont les règles traitent l'application. Suivez les meilleures pratiques pour les mises à jour du contenu des applications afin de vous assurer que vous avez le temps d'apporter les modifications nécessaires en raison de la mise à jour.

Accès au site Web (filtrage des URL)

Le filtrage des URL avancé nécessite une licence. Utilisez le filtrage des URL avancé avec PAN-OS, Prisma Access (généralement inclus avec la licence Prisma Access) et Cloud NGFW pour AWS.

Le filtrage des URL basé sur les catégories de sites Web simplifie la politique de sécurité sortante et vous protège des sites Web malveillants. Chaque catégorie d'URL définit un groupe de sites ayant le même type de contenu, par exemple des sites **health-and-medicine (santé et médecine)**, **games (jeux)**ou **hacking (piratage)**. Il existe également trois catégories qui définissent le niveau de risque relatif des sites au sein d'une catégorie particulière : **low-risk (risque faible)**, **medium-risk (risque moyen)** et **high-risk (risque élevé)**. La combinaison d'une catégorie avec un niveau de risque vous permet de créer des règles de politique de sécurité qui bloquent ou autorisent le trafic en fonction du risque au sein d'une catégorie d'URL.

Vous devez activer le décryptage pour profiter du filtrage des URL, car vous devez décrypter le trafic pour révéler l'URL exacte afin que le pare-feu puisse prendre l'action appropriée. Au minimum, décryptez le trafic à risque élevé et moyen.

STEP 1 | Ciblez le trafic à décrypter en fonction des catégories d'URL, car les catégories d'URL vous permettent d'identifier facilement le trafic à risque.

Décryptez d'abord les catégories d'URL les plus risquées et décryptez davantage de trafic à mesure que vous gagnez en expérience.

STEP 2 | Dans les règles de politique de sécurité qui contrôlent le trafic Internet sortant :

- Attachez des profils de filtrage des URL pour simplifier la politique de sécurité. Configurez un profil de filtrage des URL de bonnes pratiques qui bloque toutes les catégories de sites Web malveillants (pour l'accès au site et la soumission des informations d'identification de l'utilisateur) et les alertes sur toutes les autres catégories, et attachez-le à toutes les règles autorisant l'accès au Web.
- Contrôlez le trafic que vous ne pouvez pas décrypter pour des raisons juridiques, de conformité, commerciales, de confidentialité, réglementaires ou autres grâce aux catégories d'URL. Par exemple, créez une règle de politique de sécurité, avec les utilisateurs et applications appropriés, qui spécifie les catégories appropriées comme critères de correspondance et ne décrypte pas le trafic correspondant à la règle.

- Configurez des catégories d'URL personnalisées afin de pouvoir créer des exceptions aux règles de politique de sécurité basées sur le filtrage des URL. Ajoutez la catégorie d'URL personnalisée à un profil de filtrage des URL et attachez-la à la règle de politique de sécurité appropriée ou utilisez des catégories personnalisées comme critères de correspondance dans la politique de sécurité. Les exceptions vous permettent de bloquer l'accès aux catégories d'URL pour la plupart des utilisateurs mais de les autoriser pour des utilisateurs spécifiques tels que les testeurs PEN et l'infosec, de bloquer une catégorie entière telle que les réseaux sociaux mais d'autoriser l'accès à LinkedIn ou de contrôler les éléments à décrypter. Par exemple :
  - Combinez une catégorie d'URL avec une catégorie basée sur le risque comme critères de correspondance pour bloquer ou autoriser le trafic d'une catégorie d'URL en fonction du risque. Par exemple, pour bloquer l'accès aux sites financiers à risque, créez une règle de politique de sécurité qui spécifie à la fois la catégorie d'URL **financial-services (services financiers)** et la catégorie **high-risk (à haut risque)** comme critères de correspondance et définissez la règle **Action** sur **Deny (Déni)**. Placez cette règle au-dessus des règles qui autorisent l'accès à la catégorie d'URL **financial-services (services financiers)** afin que le pare-feu bloque les sites à haut risque avant d'autoriser l'accès aux sites à risque moyen et faible.
  - Si la disponibilité des ressources du pare-feu vous empêche de décrypter tout le trafic que vous pouvez décrypter légalement et à des fins professionnelles, utilisez des catégories d'URL personnalisées pour créer des règles de politique de sécurité avec un trafic à faible risque correspondant pour lequel le décryptage a peu de valeur. Par exemple, pour contourner le décryptage pour les services de diffusion à faible risque, créez une règle de politique de sécurité qui spécifie à la fois la catégorie d'URL **streaming-media (diffusion multimédia en continu)** et la catégorie **low-risk (à faible risque)** comme critères de correspondance et définissez la règle **Action** sur **Allow (Autoriser)**. Si le trafic utilise TLSv1.2 ou une version antérieure, créez une politique et un profil de non-décryptage pour le trafic afin de bloquer les mauvaises sessions. Si le trafic utilise TLSv1.3 ou version ultérieure, ne créez pas de politique ni de profil de non-décryptage pour le trafic.
- Définissez la zone source dans la règle de politique de sécurité sur un réseau interne protégé (zone de confiance). Ne spécifiez pas de zone externe ni **any (aucune)** zone comme source, car vous appliquez le filtrage des URL uniquement au trafic sortant. (L'application du filtrage des URL au trafic entrant peut même conduire à des attaques DoS.)

STEP 3 | Pour transférer les profils de filtrage des URL en toute sécurité vers les paramètres des meilleures pratiques et créer des profils de filtrage des URL conformes aux meilleures pratiques :

1. Clonez le profil de filtrage des URL par défaut (nommé **default**) et modifiez-le.
2. Renommez le profil de manière appropriée (par exemple, Profil de filtrage des URL des meilleures pratiques).
3. Définissez toutes les actions pour les catégories d'URL afin qu'elles émettent des alertes à la fois pour l'accès au site et la soumission des informations d'identification de l'utilisateur. (L'action d'autorisation par défaut ne génère pas de journaux.) Vous devez définir manuellement les

catégories d'URL sur lesquelles émettre une alerte pour générer des journaux et gagner en visibilité sur le trafic.

Lorsqu'une nouvelle catégorie est ajoutée au filtrage des URL, par défaut, la catégorie est définie pour autoriser l'accès au site et la soumission des informations d'identification de l'utilisateur. Définissez manuellement de nouvelles catégories pour émettre une alerte sur l'accès au site et la soumission des informations d'identification de l'utilisateur afin d'obtenir leurs journaux de filtrage des URL. Mettez également à jour les catégories d'URL personnalisées en conséquence.

4. Définissez toutes les actions pour les catégories d'URL malveillantes afin de bloquer à la fois l'accès au site et la soumission des informations d'identification de l'utilisateur. Faites des exceptions appropriées pour les tests PEN, la recherche sur les menaces et la sécurité des informations, si nécessaire :
   - commande et contrôle : URL et domaines que les logiciels malveillants ou les systèmes compromis utilisent pour communiquer avec le serveur distant d'un attaquant.
   - logiciels indésirables : ces sites ne répondent pas à la définition d'un virus et ne constituent pas une menace directe pour la sécurité, mais ils incitent les utilisateurs à accorder un accès à distance ou à effectuer d'autres actions non autorisées. Les sites de logiciels indésirables incluent les escroqueries, les activités illégales, les activités criminelles, les logiciels publicitaires et autres applications indésirables et non sollicitées, y compris les domaines de « typosquattage ».
   - logiciels malveillants : sites qui sont reconnus pour héberger des logiciels malveillants ou qui sont utilisés pour du trafic de commande et de contrôle.
   - phishing : sites connus pour héberger des pages de phishing d'informations d'identification et personnelles, y compris des escroqueries au support technique et des scarewares.
   - DNT : sites connus pour distribuer des DNT.
   - activité d'analyse : sondage des vulnérabilités existantes ou conduite d'attaques ciblées.
5. Certaines catégories d'URL ont un fort potentiel malveillant, mais ne sont pas forcément malveillantes. Définissez toutes les actions pour ces catégories d'URL afin de bloquer à la fois l'accès au site et la soumission des informations d'identification de l'utilisateur. Faites des exceptions appropriées pour les tests PEN, la recherche sur les menaces et la sécurité des informations, si nécessaire :
   - DNS dynamique : systèmes avec des adresses IP attribuées dynamiquement qui sont souvent utilisées pour diffuser des charges utiles de logiciels malveillants ou des logiciels malveillants de commande et de contrôle.
   - piratage informatique : sites liés à l'accès illégal ou douteux à des équipements et à des logiciels ou à l'utilisation illégale ou douteuse d'équipements et de logiciels. Comprend également les sites qui facilitent le contournement des systèmes de licences et de droits numériques.

     Faites des exceptions à cette catégorie pour les utilisateurs appropriés des tests PEN et de la recherche sur les menaces.
   - contenu insuffisant : sites Web et services qui présentent des pages de test, aucun contenu, fournissent un accès à une API non destiné à l'affichage par l'utilisateur final ou nécessitent une authentification sans afficher aucun autre contenu.
   - domaines nouvellement enregistrés : domaines que les algorithmes de génération de domaines génèrent souvent ou que des acteurs malveillants génèrent pour des activités malveillantes.

- non résolu : si le cloud PAN-DB est inaccessible et que l'URL ne se trouve pas dans le cache de filtrage des URL du pare-feu, le pare-feu ne peut pas résoudre et identifier la catégorie d'URL.

  *Pour une sécurité maximale, activez **Hold client request for category lookup (Garder en mémoire la demande du client pour la recherche de catégorie)** afin de donner au pare-feu plus de temps pour résoudre la catégorie d'URL. Cela prolonge le temps dont dispose le pare-feu pour interroger le type de catégorie à partir du cloud et entraîne une meilleure sécurité, mais peut augmenter la latence.*

- parqué : domaines qui seront souvent utilisés à des fins d'hameçonnage d'informations d'identification ou de vol d'informations personnelles.
- contournement des proxys et anonymiseurs : URL et services qui sont souvent utilisés pour contourner des produits de filtrage de contenu.
- inconnu : sites non encore identifiés par Palo Alto Networks (PAN-DB).

  Les mises à jour en temps réel de PAN-DB détectent les sites inconnus après la première tentative d'accès à un site inconnu, de sorte que le pare-feu identifie rapidement les URL inconnues et les traite ensuite en fonction de la catégorie d'URL réelle du site.

  Si la disponibilité est importante pour votre entreprise et que vous devez autoriser le trafic, demandez qu'une alerte soit envoyée en présence de sites inconnus, appliquez au trafic les profils de sécurité recommandés et enquêtez sur les alertes concernant le trafic.

6. Définissez l'action pour l'accès au site et la soumission des informations d'identification de l'utilisateur afin de bloquer les catégories d'URL suivantes en fonction des exigences légales ou commerciales et du risque de responsabilité potentiel. Si vous ne bloquez pas ces sites, émettez des alertes et appliquez des profils de sécurité stricts au trafic.
   - abus de drogues : sites qui promeuvent l'abus de drogues illégales et légales.
   - adulte : tous les sites contenant du contenu pour adultes de toute nature, y compris des jeux et des bandes dessinées ainsi que du matériel, des médias, des œuvres d'art, des forums et des services sexuellement explicites.
   - violation du droit d'auteur : domaines avec un contenu illégal qui présente un risque de responsabilité.
   - extrémisme : sites Web faisant la promotion du terrorisme, du racisme, de l'exploitation des enfants, etc.
   - jeux d'argent : sites de loteries et de jeux d'argent.
   - peer-to-peer : partage peer-to-peer de torrents, de programmes de téléchargement, de fichiers multimédias ou d'autres applications logicielles. (N'inclut pas les sites de partagiciel ou de logiciels gratuits.)
   - discutable : sites qui font la promotion d'un humour de mauvais goût et de contenus offensants ciblant des données démographiques spécifiques.

- armes : ventes, critiques, descriptions ou instructions concernant les armes et leur utilisation.

Réfléchissez également à la manière dont vous souhaitez gérer les catégories d'URL de cryptomonnaie et d'alcool et de tabac. Activez les alertes à leur sujet et appliquez des profils de sécurité stricts au trafic ou bloquez-les, en fonction des besoins de votre entreprise.

7. Bloquez l'envoi des informations d'identification de l'utilisateur pour la catégorie à haut risque. (Ne bloquez pas l'accès au site pour la catégorie à haut risque.)
8. Pour les paramètres de filtrage des URL dans le profil de filtrage des URL :
   - Désactivez l'option **Log Container Page Only (Consigner la page de conteneur uniquement)**, qui est activée par défaut. Si vous consignez uniquement les pages du conteneur, vous perdez la visibilité sur les applications fonctionnelles telles que la publication, le chargement, le téléchargement, etc. Désactivez l'option **Log Container Page Only (Consigner la page de conteneur uniquement)** pour voir le journal complet pour pouvoir voir la véritable application fonctionnelle.
   - Si votre environnement est une école qui reçoit un financement fédéral, activez l'option **Safe Search Enforcement (Mise en œuvre de la recherche sécurisée)** (exigence légale).
9. Activez l'option **User Credential Detection (Détection des informations d'identification de l'utilisateur)** (nécessite la configuration et l'activation de l'ID utilisateur).

STEP 4 | Appliquez le filtrage des URL aux règles de politique de sécurité avec DNS Sinkhole configuré dans le profil de sécurité antispyware (nécessite un abonnement Advanced Threat Protection ou un abonnement actif à la protection contre les menaces héritées et un abonnement DNS Security pour utiliser la sécurité DNS basée sur le cloud) pour voir quelles machines sont infectées et où elles essayaient de se connecter pour DNS.

Actions de stratégie et autres paramètres

Les actions de politique de sécurité précisent s'il faut autoriser ou bloquer le trafic, et comment bloquer le trafic que vous ne l'autorisez pas. La Quality of Service (qualité de service - QoS) contrôle la bande passante, si nécessaire, pour garantir que le trafic autorisé par une règle reçoit la bande passante appropriée.

STEP 1 | Définissez une action pour chaque règle de politique de sécurité.

- **Allow (Autorisez)** uniquement le trafic approuvé et toléré. Plus vous autorisez de trafic qui ne concerne pas votre entreprise, plus le risque est grand. Le pare-feu bloque le trafic que vous n'autorisez pas explicitement dans une règle de politique de sécurité.
- Plus vos règles de politique de sécurité suivent le principe de l'accès à moindre privilège, moins vous avez besoin de règles de blocage. La manière de bloquer le trafic dépend de la façon dont vous souhaitez répondre à l'application que vous bloquez.
  - Utilisez **Deny (Déni)**, qui utilise l'action par défaut de l'application, sauf si vous souhaitez que le pare-feu réponde à l'application d'une manière spécifique en réinitialisant le client, le serveur ou les deux, ou en abandonnant silencieusement le trafic.
  - Utilisez **Drop (Abandonner)** lorsque vous souhaitez refuser le service en silence, sans envoyer de réponse de réinitialisation. Lorsque vous bloquez un trafic clairement malveillant, par exemple lorsque vous bloquez sur la base des EDL prédéfinies de Palo Alto Networks, l'action **Drop (Abandonner)** empêche la partie malveillante de la communication de savoir pourquoi elle a été bloquée.

- Si vous avez un cas d'utilisation pour réinitialiser uniquement le client ou uniquement le serveur, assurez-vous de bien comprendre la directionnalité client-serveur (quelle extrémité de la communication initie la connexion), basée sur les paramètres source et de destination de la règle.

STEP 2 | Si nécessaire, appliquez QoS pour contrôler la bande passante de certaines applications.

La QoS est facultative. Comprenez les applications auxquelles vous souhaitez donner la priorité à la bande passante et les applications dont vous souhaitez limiter la bande passante si vous appliquez la QoS à la politique. Par exemple, lors d'événements populaires tels que la Coupe du Monde qui utilisent des applications de diffusion particulières, vous pouvez autoriser les employés à visualiser l'événement à l'aide de ces applications et limiter leur bande passante afin de garantir qu'une bande passante appropriée est disponible pour les activités professionnelles. Autre exemple : lorsque des mises à jour sont publiées pour des applications populaires, le téléchargement massif peut avoir un impact sur la disponibilité de la bande passante. Pour éviter cela, appliquez QoS pour limiter la bande passante disponible pour le trafic de téléchargement de cette application.

Journalisation et transfert des journaux

La journalisation et le stockage des journaux sont essentiels pour enquêter sur les incidents. Communiquez avec votre :

- Security Operations Center (SOC) pour veiller à capturer les bonnes informations pour enquêter sur les événements si nécessaire.
- Équipe d'audit de conformité pour veiller à capturer les bonnes informations pour les audits et la conformité.
- Équipe juridique pour vous assurer que vous ne stockez pas de texte en clair ou d'autres données qui enfreignent les réglementations locales, la conformité, les exigences commerciales, la confidentialité, etc.

STEP 1 | Tenez compte de la capacité de stockage des journaux dont vous avez besoin maintenant et à l'avenir et dimensionnez votre capacité de stockage des journaux en conséquence.

- Planifiez la capacité de stockage de manière à pouvoir conserver les journaux suffisamment longtemps pour enquêter sur les menaces. La durée dépend de vos procédures d'enquête.
- Assurez-vous que votre SOC peut ingérer des journaux où que vous les stockiez. Cortex Data Lake (CDL) centralise le stockage et l'analyse des journaux, puis fournit une solution qui évolue en fonction de votre volume de journaux.
- Ne dupliquez pas les mêmes journaux pour les stocker à plusieurs endroits. Utilisez soit CDL, soit un espace de stockage séparé tel que des collecteurs de journaux. Lorsque vous déplacez des

journaux d'un espace de stockage à un autre, n'utilisez pas de duplication. Au lieu de cela, préparez et exécutez un basculement brutal.

Si vous activez le transfert des journaux en double sur les pare-feux ou sur Panorama, les journaux système et de configuration ne sont pas envoyés à CDL, et les journaux CDL seront donc incomplets. Pour cette raison, n'activez pas le transfert des journaux en double pour la sauvegarde des journaux.

Si vous devez diviser le stockage des journaux, faites-le en séparant le transfert des journaux de manière cohérente. Par exemple, envoyez tous les journaux Prisma Access à CDL et envoyez tous les journaux de pare-feu aux collecteurs de journaux.

STEP 2 | Pensez à ce que vous souhaitez enregistrer, à la manière dont vous souhaitez l'enregistrer et à ce que vous ne souhaitez pas enregistrer ou ne pouvez pas enregistrer pour des raisons de conformité ou d'espace de stockage.

Pour la plupart des applications, enregistrez toutes les informations possibles pour faciliter les enquêtes du Security Operating Center (SOC). Cependant, pour certaines applications et dans certaines circonstances, vous ne pouvez pas créer de journaux complets :

- Évaluez si la règle nécessite une journalisation en fonction de la conformité, des exigences commerciales, des exigences d'audit telles que la norme ISO, des considérations de confidentialité (par exemple, PII, RGPD) et des exigences du SOC. Soyez prudent lorsque vous enregistrez les numéros de sécurité sociale, les informations d'identification, les informations personnelles, etc., en texte clair si les applications ne cryptent pas ces informations.
- Les services de base tels que DNS, NTP, Syslog, etc. créent des milliers de petites sessions qui génèrent de nombreux journaux inutiles, ce qui a un impact sur le stockage des journaux et rend les enquêtes sur les incidents plus difficiles. Pour ces services, configurez uniquement le transfert des journaux des menaces, sauf si vous disposez de la capacité de stockage nécessaire pour prendre d'autres journaux.

STEP 3 | Dans les règles de politique de sécurité, enregistrez le trafic à la fin de la session plutôt qu'au début pour éviter de journaliser les applications transitoires.

L'option **Log At Session Start (Consigner au démarrage de session)** consomme également plus de ressources que la journalisation uniquement à la fin de la session. Dans la plupart des cas, vous **Log At Session End (vous connectez en fin de session)** uniquement. Activez à la fois **Log At Session Start (Se connecter au début de la session)** et **Log At Session End (Se connecter en fin de session)** uniquement pour savoir si une application ne correspond pas à une règle de politique de sécurité, pour les sessions de tunnel de longue durée telles que les tunnels GRE (vous ne pouvez pas voir ces sessions dans l'ACC à moins de vous connecter au début de la session) et pour gagner en visibilité sur les sessions OT/ICS (Operational Technology/Industrial Control Systems), qui sont également des sessions de longue durée.

Policy Optimizer et Cloud App-ID Engine (ACE) ne comptent pas les règles enregistrées au début de la session dans leurs statistiques.

STEP 4 | Consignez le trafic qui correspond à la règle intra-zone par défaut, qui autorise tout le trafic au sein d'une zone par défaut, et à la règle de déni interzone, qui bloque tout le trafic entre les zones que la règle de politique de sécurité n'autorise pas explicitement par défaut.

STEP 5 | Configurez les profils de transfert de journaux et attribuez-les aux règles de politique de sécurité pour envoyer les journaux au stockage approprié, tel que CDL ou les collecteurs de journaux, et pour alerter les administrateurs concernés des événements, en particulier des événements de menace critique, élevée et moyenne.

Cloud Managed Prisma Access transmet tous les journaux à CDL.

- Assurez-vous que chaque règle de politique de sécurité est associée à un profil de transfert des journaux.

  Créez un profil de transfert des journaux par défaut de base pour toutes les nouvelles règles de politique de sécurité, nommez-le **`par défaut`** et assurez-vous qu'il enregistre les menaces. Si vous nommez le profil **`par défaut`**, le pare-feu l'applique automatiquement à toutes les nouvelles règles de politique de sécurité, ce qui garantit que toutes les nouvelles règles ont des profils de transfert des journaux.

  Il est plus facile de remplacer ou de modifier le profil pour les quelques règles qui nécessitent un traitement de journalisation différent, comme les journaux pour le trafic lié à la conformité, aux informations personnelles, aux réglementations locales, aux exigences commerciales, etc., ou les journaux pour les services courants tels que DNS ou NTP. plutôt que d'attacher un profil de transfert des journaux à chaque nouvelle règle individuellement.

  *Pour les règles de politique de sécurité qui régissent la sécurité IoT, utilisez le profil prédéfini de transfert des journaux **IoT Security Default Profile - EAL Enabled**, qui fournit à la sécurité IoT tous les types de journaux dont elle a besoin, y compris les journaux d'application améliorés.*

- Utilisez le **Log Forwarding for Security Services (Transfert des journaux pour les services de sécurité)** dans Policy Optimizer pour identifier les règles de politique de sécurité auxquelles aucun profil de transfert des journaux n'est associé (sélectionnez **None (Aucun)** dans le filtre). Ajoutez un profil de transfert des journaux approprié à chaque règle qui n'en a pas.

STEP 6 | À des fins d'enquête, assurez-vous de connaître la véritable source et la destination du trafic, et non seulement l'adresse IP d'un périphérique proxy tel qu'un équilibreur de charge, un périphérique NAT ou un serveur DNS malveillant situé entre la véritable source et le pare-feu. S'il existe un périphérique proxy entre le pare-feu et la véritable source, en fonction de votre architecture réseau et de l'application :

- Placez des pare-feux devant les équilibreurs de charge pour voir la véritable adresse IP source.
- Effectuez une packet capture (capture de paquet - pcap) pré-NAT en configurant une étape de réception dans les paramètres de packet capture (capture de paquet - pcap).
- Appliquez un profil de filtrage des URL qui permet de consigner le champ X-Forwarded-For (XFF) dans la règle de politique de sécurité (onglet **URL Filtering Settings (Paramètres de filtrage des URL)** dans **Objects (Objets)** > **Profiles (Profils)** > **URL Filtering (Filtrage d'URL)**). Le champ XFF affiche l'adresse IP source d'origine. Le journal XFF se trouve dans le journal de filtrage des URL.

Profils de sécurité

Les profils de sécurité analysent le trafic autorisé pour y rechercher de menaces telles que les virus, les logiciels malveillants, les logiciels espions, les types de fichiers malveillants et d'autres menaces connues

et inconnues, et préviennent ces menaces. Attachez des profils de sécurité aux règles de politique de sécurité qui permettent au trafic d'appliquer la prévention des menaces au trafic qui correspond à la règle.

Utilisez les configurations du jour 1 pour les modèles qui fournissent immédiatement des profils de sécurité des meilleures pratiques ne dépendant pas des cas d'utilisation au trafic autorisé. Les configurations du jour 1 sont disponibles sur le portail de support client (**Tools (Outils)** > **Run Day 1 Configuration (Exécuter une configuration du jour 1)**) et nécessitent une connexion au support. À partir de là, passez au blocage des menaces des meilleures pratiques, comme décrit ici.

Pour identifier et prévenir les menaces, le pare-feu doit avoir une visibilité sur le trafic des applications. Décryptez autant de trafic que le permettent les réglementations locales, les considérations commerciales, les considérations de confidentialité et les capacités techniques. Pour le décryptage de type Proxy de transfert SSL (sortant), mettez d'abord en œuvre le filtrage des ID utilisateur et des URL afin de pouvoir cibler efficacement le décryptage. Si vous ne décryptez pas le trafic, le pare-feu ne peut pas analyser les en-têtes cryptés et les informations de la charge utile.

Suivez les meilleures pratiques de mise à jour du contenu des menaces pour vous assurer que les signatures de votre profil de sécurité sont à jour.

Obtenez l'abonnement au service cloud Advanced Threat Prevention pour prévenir en temps réel les menaces, notamment les menaces de commande et de contrôle inconnues et les menaces de vulnérabilité zero day. Advanced Threat Prevention est disponible pour PAN-OS et pour les déploiements Prisma Access 3.2 Innovation et Innovation ultérieurs. Si vous exécutez une version antérieure de Prisma Access, utilisez l'abonnement Prévention des menaces standard.

Les environnements isolés ne peuvent pas utiliser la prévention avancée des menaces, car il s'agit d'un service cloud qui nécessite une connexion cloud.

Les recommandations de profils de sécurité des meilleures pratiques pour Prisma Access géré dans le cloud diffèrent légèrement des recommandations pour PAN-OS et Prisma Access géré par Panorama. De plus, dans Cloud Managed Prisma Access, vous ne pouvez pas appliquer de profils de sécurité individuels aux règles de politique de sécurité ; vous pouvez uniquement appliquer des groupes de profils. Les groupes de profils incluent les profils de sécurité que vous incluez dans le groupe.

Les conseils sur les meilleures pratiques se concentrent sur ce qu'il faut faire pour optimiser la sécurité, ce qui est l'objectif ultime de vos profils de sécurité. Cependant, pour garantir la disponibilité des applications critiques pour l'entreprise, commencez par bloquer le trafic malveillant connu et par émettre une alerte sur la plupart des autres trafics. Suivez les conseils de transition des profils de sécurité des meilleures pratiques pour passer en toute sécurité des alertes aux profils de sécurité des meilleures pratiques qui bloquent le trafic et soyez prudent lorsque vous passez de l'alerte au blocage pour éviter d'avoir un impact sur les applications critiques pour l'entreprise.

Le moment de faire passer un paramètre de profil de sécurité d'alerte à blocage est lorsque vous êtes sûr que le profil est correctement réglé, que vous avez fait toutes les exceptions nécessaires et que vous ne déclencherez pas par inadvertance une signature qui bloque une application critique pour l'entreprise.

Cette section simplifiée vous montre les paramètres des meilleures pratiques. La création de profils de sécurité conformes aux meilleures pratiques fournit des informations plus approfondies sur les raisons des paramètres.

- Profil antivirus (inclut la signature WildFire et les actions d'apprentissage automatique en ligne)
- Profil antispyware (inclut les politiques DNS/la mise en entonnoir et l'analyse cloud en ligne)

  Pour fournir une couverture complète, souscrivez un abonnement au filtrage des URL avancé et un abonnement à DNS Security pour gagner en visibilité et vous protéger contre les URL malveillantes, les domaines et les abus du protocole DNS.
- Profil de protection contre les vulnérabilités (inclut une analyse cloud en ligne)
- Profil de blocage des fichiers
- Profil d'analyse WildFire

STEP 1 | Clonez le profil antivirus par défaut prédéfini, renommez-le et modifiez-le pendant que vous transférez le profil antivirus en toute sécurité vers les paramètres des meilleures pratiques.

Pour transférer le profil antivirus en toute sécurité vers un profil de bonnes pratiques :

1. Les faux positifs sont rares. Déployez immédiatement le profil antivirus des meilleures pratiques pour les applications qui ne sont pas critiques pour votre entreprise.
2. Pour les applications critiques pour l'entreprise, commencez par émettre une alerte pour vous assurer que vous n'affectez pas la disponibilité des applications critiques. Passez au blocage lorsque vous êtes sûr que le profil antivirus ne bloque pas ces applications.
3. Si vous disposez d'un déploiement existant ou si vous migrez et que vous disposez d'un blocage existant, répliquez-le, car vous comprenez déjà le trafic et la raison du blocage.
4. Si vous traitez les applications internes différemment des applications externes, vous aurez peut-être besoin d'un profil antivirus pour le trafic Internet et d'un profil antivirus différent pour le trafic interne.

Surveillez les journaux des menaces pour voir si des applications critiques pour l'entreprise provoquent des alertes ou des blocages. Surveillez les journaux des envois WildFire si vous disposez d'un abonnement Advanced WildFire ou d'un abonnement WildFire existant et utilisez les paramètres d'action WildFire.

Un profil antivirus conforme aux meilleures pratiques bloque les logiciels malveillants, les virus et les robots DNT connus :

- Activez la recherche de signature en temps réel globalement sur le périphérique et dans le profil antivirus pour conserver les fichiers jusqu'à ce que le pare-feu reçoive la dernière signature antivirus en temps réel du cloud :
  - Activez globalement : **Device (Périphérique)** > **Setup (Configuration)** > **Content-ID** > **Content-ID Settings (Paramètres Content-ID)** > **Realtime Signature Lookup (Recherche de signature en temps réel)**, activez **Hold for WildFire Real Time Signature Look Up (Attente pour recherche de signature WildFire en temps réel)** et définissez **Action On Real Time Signature Timeout (Action après expiration de la signature en temps réel)** sur **reset-both (réinitialiser les deux)**. Vous devez activer la recherche de signature en temps réel à l'échelle mondiale pour l'activer dans les profils antivirus.

- Activez dans le profil antivirus : **Objects (Objets)** > **Security Profiles (Profils de sécurité)** > **Antivirus** et activez **Hold for WildFire Real Time Signature Look Up (Attente pour recherche de signature WildFire en temps réel)**.

  La conservation des fichiers pour garantir que WildFire obtient les dernières signatures antivirus vous protège contre tout logiciel malveillant de type « zero-day » et les signatures antivirus obsolètes auxquelles vous pourriez être exposé si vous transférez des fichiers sans les conserver pour les dernières signatures.

- Définissez les actions à entreprendre lorsque le pare-feu détecte des virus dans certains protocoles. L'action la plus sûre consiste à réinitialiser le client et le serveur pour garantir que la session est terminée :

  - Modifiez la **Signature Action (Action de signature)** sur **reset-both (réinitialiser les deux)** pour les protocoles smtp, pop3 et imap, dont l'action par défaut est d'alerter. Laissez la **Signature Action (Action de signature)** pour les autres protocoles sur **reset-both (réinitialiser les deux)**.
  - Modifiez la **WildFire Signature Action (Action de signature WildFire)** sur **reset-both (réinitialiser les deux)** pour les protocoles smtp, pop3 et imap, dont l'action par défaut est d'alerter. Laissez la **WildFire Signature Action (Action de signature WildFire)** pour les autres protocoles sur **reset-both (réinitialiser les deux)**.
  - Modifiez la **WildFire Inline ML Action (Action WildFire Inline ML)** sur **reset-both (réinitialiser les deux)** protocoles smtp, pop3 et imap, dont l'action par défaut est d'alerter. Laissez la **WildFire Inline ML Action (Action WildFire Inline ML)** pour les autres protocoles sur **reset-both (réinitialiser les deux)**.

Attachez un profil de bonnes pratiques à toutes les règles d'autorisation.

Un abonnement WildFire est requis pour configurer les actions WildFire Signature et WildFire Inline ML.

Dans Cloud Managed Prisma Access, Antivirus et WildFire sont regroupés dans un seul profil au lieu d'avoir des profils distincts.

STEP 2 | Clonez le profil antispyware par défaut prédéfini, renommez-le et modifiez-le pendant que vous transférez le profil antispyware en toute sécurité vers les paramètres des meilleures pratiques. En plus des politiques de signature antispyware, le profil contrôle également les politiques DNS Sinkhole.

Pour faire passer le profil antispyware en toute sécurité vers un profil de bonnes pratiques, dans **Signature Policies (Politiques de signature)** :

1. Les faux positifs sont relativement rares. Pour les applications qui ne sont pas essentielles à vos activités, bloquez dès le départ les signatures de sévérité élevée et critique.
2. Les signatures de sévérité moyenne peuvent générer des faux positifs et nécessitent donc une surveillance initiale. Émettez une alerte sur les signatures de gravité moyenne pour le trafic interne et bloquez les signatures de gravité moyenne pour le trafic externe. Surveillez les journaux de menaces (**Monitor (Surveiller)** > **Logs (Journaux)** > **Threat (Menace)**) pour voir si vous pouvez bloquer les applications pour lesquelles vous recevez des alertes ou si vous devez les autoriser.
3. Pour les applications critiques pour l'entreprise, définissez l'**Action** sur **alert (alerte)** pour garantir la disponibilité des applications. Cependant, lorsque vous protégez déjà des applications similaires avec un profil antispyware qui bloque les signatures critiques, élevées et/ou moyennes et que vous êtes certain que ce profil répond à vos besoins professionnels et à vos besoins en matière de

sécurité, vous pouvez utiliser un profil similaire pour bloquer les logiciels antispyware et protéger les applications similaires.

4. Activez la capture de paquets uniques pour toutes les signatures de gravité pendant la transition afin de pouvoir examiner les événements plus en détail si nécessaire si vous disposez des ressources nécessaires. Lorsque vous passez aux profils respectant les meilleures pratiques, si des événements faibles et informatifs génèrent trop d'activités de packet capture (capture de paquet - pcap) (volume de trafic trop important) et que ces informations ne sont pas particulièrement utiles, vous pouvez désactiver la packet capture (capture de paquet - pcap) pour ces sévérités.

   *Les packet captures (captures de paquet - pcap) consomment des ressources du plan de gestion. Vérifiez les ressources système (par exemple, **Dashboard (Tableau de bord)** > **System Resources (Ressources système)**) pour comprendre leur utilisation avant et après la mise en œuvre de la packet capture (capture de paquet - pcap) afin de vous assurer que votre système dispose de ressources suffisantes pour effectuer toutes les packet captures (capture de paquet - pcap).*

5. Créez des exceptions si nécessaire pour corriger les faux positifs confirmés avant de mettre en œuvre des profils antispyware complets conformes aux meilleures pratiques.

Si vous traitez les applications internes différemment des applications externes, vous aurez peut-être besoin d'un profil antispyware pour le trafic Internet et d'un profil antispyware différent pour le trafic interne.

Effectuez la transition des **DNS Policies (Politiques DNS)** du profil vers les meilleures pratiques dès que vous êtes sûr de comprendre le trafic que vous bloquez :

- Définissez la **Policy Action (Action de politique)** pour les signatures DNS sur **sinkhole** afin d'identifier les hôtes potentiellement compromis qui tentent d'accéder à des domaines suspects en localisant les hôtes et en les empêchant d'accéder à ces domaines. Définissez **packet capture (capture de paquet - pcap)** sur **extend-capture**.

  Sur les systèmes PAN-OS, définissez l'adresse DNS Sinkhole comme FQDN, par exemple, Sinkhole.paloaltonetworks.com, de sorte que si l'adresse IP change, le paramètre reste valide. Pour Prisma Access, utilisez l'adresse IP sinkhole.

- Supprimez tous les types de domaines de **sécurité DNS** et définissez **packet capture (capture de paquet - pcap)** sur **extended-capture (capture étendue)** pour les domaines de commande et de contrôle et sur **single-packet (paquet unique)** pour tous les autres types de domaine, à l'exception des domaines parqués (PAN-OS 10.0 et versions ultérieures).
- Bloquez tous les types d'enregistrements DNS, qui sont utilisés par les requêtes DNS cryptées, pour empêcher les clients de crypter le bonjour du client pendant le processus de résolution DNS.

Définissez l'**Inline Cloud Analysis (Analyse cloud en ligne)** du profil (nécessite un abonnement Prévention des menaces et PAN-OS 10.2 et versions ultérieures) sur **Enable cloud inline analysis**

(Activer l'analyse cloud en ligne) sur tout le trafic sortant. Définissez l'**Action** sur **reset-both (réinitialiser les deux)** pour tous les modèles.

Dans le profil antispyware de transition, si vous disposez de contrôles antispyware existants qui bloquent le trafic et répondent aux besoins de votre entreprise, mettez en œuvre ces contrôles immédiatement, car vous comprenez déjà le trafic et la raison de son blocage.

Un profil antispyware conforme aux meilleures pratiques détecte le trafic de commande et de contrôle (C2), empêche les systèmes compromis d'établir une connexion sortante et permet au gouffre DNS d'identifier les hôtes infectés. Utilisez GlobalProtect pour mettre automatiquement en quarantaine un périphérique compromis dans PAN-OS et avec Panorama Managed Prisma Access, et vous pouvez également mettre en quarantaine les périphériques compromis dans Cloud Managed Prisma Access.

Pour les **Signature Policies (Politiques de signature)** :

1. Définissez l'**Action** pour les gravités critique, élevée et moyenne sur **reset-both (réinitialiser les deux)** et définissez **packet-capture (capture de paquets)** sur **single-packet (paquet unique)**.
2. Définissez l'**Action** pour les gravités faibles et informatives sur **default (par défaut)** et désactivez **packet-capture (capture de paquets)**.

Pour les **DNS Policies (Politiques DNS)**, utilisez les mêmes paramètres recommandés pour la période de transition. Définissez la **Policy Action (Action de politique)** sur sinkhole pour toutes les sources de signature, définissez **packet capture (capture de paquet - pcap)** sur **extended-capture (capture étendue)** pour les **domaines de contenu de Palo Alto Networks** et les domaines de commande et de contrôle, puis définissez **packet capture (capture de paquet - pcap)** sur **single-packet (paquet unique)** pour tous les autres domaines de sécurité DNS, à l'exception des domaines parqués.

Les paramètres de bonnes pratiques pour **Inline Cloud Analysis (Analyse cloud en ligne)** sont les mêmes que les paramètres de transition. Activez la fonctionnalité sur tout le trafic sortant et définissez l'action sur **reset-both (réinitialiser les deux)**.

Utilisez le service de sécurité DNS pour vous protéger contre les menaces avancées basées sur DNS (nécessite une licence de sécurité DNS et Advanced Threat Prevention ou un abonnement Prévention des menaces ancien actif).

Attachez un profil de bonnes pratiques à toutes les règles d'autorisation.

STEP 3 | Clonez le profil de protection contre les vulnérabilités strict prédéfini, renommez-le et modifiez-le à mesure que vous transférez le profil de protection contre les vulnérabilités en toute sécurité vers les paramètres des meilleures pratiques.

Les profils de protection contre les vulnérabilités assurent la protection contre les dépassements de capacité de la mémoire tampon, l'exécution non autorisée de code et d'autres tentatives d'exploitation

des vulnérabilités côté client et côté serveur. Pour faire passer en toute sécurité le profil de protection contre les vulnérabilités vers un profil de bonnes pratiques :

1. Les taux de faux positifs sont faibles. Définissez des règles pour que les applications qui ne sont pas critiques pour votre entreprise soient bloquées (**reset-both (réinitialiser les deux)**) immédiatement.
2. Pour les applications critiques pour l'entreprise, commencez par émettre une alerte pour vous assurer que vous n'affectez pas la disponibilité des applications critiques. Passez au blocage lorsque vous êtes sûr que le profil de protection contre les vulnérabilités ne bloque pas ces applications.
3. Si vous disposez d'un déploiement existant ou si vous migrez et que vous disposez d'un blocage existant, répliquez-le, car vous comprenez déjà le trafic et la raison du blocage.
4. Définissez des signatures dans la catégorie **brute-force (force brute)** pour les gravités critique, élevée et moyenne pour les alerter et les affiner jusqu'à ce que vous puissiez passer confortablement au blocage. Définissez **packet capture (capture de paquet - pcap)** sur **extend-capture**.
5. Définissez les signatures pour les règles de gravité critique et élevée pour **reset-both (réinitialiser les deux)** et définissez **packet capture (capture de paquet - pcap)** sur **single-packet (paquet unique)**.
6. Définissez les signatures pour les règles de gravité moyenne sur **alert (alerte)** et définissez **packet capture (capture de paquet - pcap)** sur **extended-capture (capture étendue)**.
7. Définissez les signatures sur **default (par défaut)** pour les règles de gravité faible et informative et définissez **packet capture (capture de paquet - pcap)** sur **single-packet (paquet unique)**.
8. Pour **Inline Cloud Analysis (Analyse cloud en ligne)**, utilisez les mêmes critères d'alerte et de blocage des applications métier que ceux que vous utilisez pour les règles initiales de protection contre les vulnérabilités. Si vous disposez de contrôles existants, répliquez-les pour bloquer le trafic. Pour les nouveaux contrôles, émettez une alerte pendant au moins une semaine avant de passer au blocage. Passez au blocage dès que possible.

*Les packet captures (captures de paquet - pcap) consomment des ressources du plan de gestion. Vérifiez les ressources système (par exemple, **Dashboard (Tableau de bord)** > **System Resources (Ressources système)**) pour comprendre leur utilisation avant et après la mise en œuvre de la packet capture (capture de paquet - pcap) afin de vous assurer que votre système dispose de ressources suffisantes.*

Surveillez les journaux des menaces pour voir si des applications critiques pour l'entreprise provoquent des alertes ou des blocages. Surveillez les journaux des envois WildFire si vous disposez d'un abonnement WildFire et utilisez les actions WildFire.

Le profil de protection contre les vulnérabilités des meilleures pratiques contrôle la manière de gérer les vulnérabilités côté client et côté serveur pour les gravités d'événements critiques, élevées, moyennes, faibles et informatives. Dans le profil, configurez six règles :

1. Créez les trois mêmes règles qui empêchent les attaques par force brute dans le profil de transition et définissez l' **Action** sur **reset-both (réinitialiser les deux)** et **packet capture (capture de paquet - pcap)** sur **single-packet (paquet unique)**.
2. Combinez les gravités client simple critique, client simple élevée, client simple moyenne, serveur simple critique, serveur simple élevée et serveur simple faible en une seule règle. Définissez l'

Action sur **reset-both (réinitialiser les deux)** et définissez **packet capture (capture de paquet - pcap)** sur **single-packet (paquet unique)**.

*Pour les profils qui contrôlent le trafic interne (est-ouest), le blocage des événements de gravité moyenne peut avoir un impact sur les applications métier. Si le blocage affecte les applications métier, créez une règle distincte dans le profil pour les événements de gravité moyenne avec l'**Action** définie sur **alert (alerte)**. Appliquez ce profil uniquement au trafic interne.*

3. Pour les gravités simples-client-low et simple-server-low, définissez l'**Action** sur **default (par défaut)** et définissez **packet capture (capture de paquet - pcap)** sur **single-packet (paquet unique)**.
4. Pour les gravités d'informations simples sur le client et sur le serveur simple, définissez l'**Action** sur **default (par défaut)** et **disable (désactivez)** la packet capture (capture de paquet - pcap). (L'activité informationnelle peut générer un volume relativement élevé de trafic de packet capture (capture de paquet - pcap) qui n'est pas particulièrement utile par rapport aux captures de paquets potentiellement menaçantes.)
5. Définissez les actions **Inline Cloud Analysis (Analyse cloud en ligne)** sur **reset-both (réinitialiser les deux)**.

Pour contrôler les profils de protection contre les vulnérabilités de manière plus granulaire et affiner la protection contre les vulnérabilités pour un cas d'utilisation particulier, créez des règles distinctes dans le profil pour chaque gravité pour la détection côté client et côté serveur. Lorsque les paramètres d'action et de packet capture (capture de paquet - pcap) sont identiques, il est logique de les combiner en une seule règle pour simplifier la configuration.

Attachez un profil de bonnes pratiques à toutes les règles d'autorisation.

STEP 4 | Faites passer vos profils de blocage de fichiers de l'alerte au blocage de tous les types de fichiers potentiellement malveillants.

Cloud Managed Prisma Access ne prend pas en charge les profils de blocage des fichiers pour les règles de politique de sécurité.

Les profils de blocage des fichiers bloquent les types de fichiers potentiellement malveillants utilisés dans les cyberattaques. Pour transférer en toute sécurité les profils de blocage des fichiers vers les paramètres de meilleures pratiques vers un profil de meilleures pratiques :

- Pour les applications critiques pour l'entreprise, émettez des alertes pour tous les types de fichiers et passez dès que possible à un profil de blocage des fichiers conforme aux meilleures pratiques. Si

vous avez déjà mis en place des contrôles de blocage, reproduisez-les et continuez à bloquer le trafic que vous souhaitez déjà bloquer à coup sûr.

- Pour les applications qui ne sont pas critiques pour l'entreprise, démarrez la transition vers un profil de blocage de fichiers conforme aux meilleures pratiques :
  - **Trafic entrant et sortant** : bloquez les fichiers 7z, bat, chm, class, cpl, dll, dlp, hta, jar, ocx, pif, scr, torrent, vbe et wsf. Activez les alertes pour tous les autres fichiers.
  - **Trafic interne** : bloquez les fichiers 7z, bat, chm, class, cpl, dlp, hta, jar, ocx, pif, scr, torrent, vbe et wsf (identique au profil entrant/sortant, sauf qu'il émet des alertes sur les fichiers .dll au lieu de les bloquer). Activez les alertes pour tous les autres fichiers.
  - Bloquez tous les types de fichiers suivants que vous pouvez bloquer pour les utilisateurs qui n'en ont pas besoin à des fins professionnelles : cab, exe, flash, msi, Multi-Level-Encoding, PE, rar, tar, encrypted-rar et encrypted-zip.

Si nécessaire, créez des exceptions pour les groupes informatiques et autres qui ont besoin d'un accès professionnel légitime à l'un de ces types de fichiers. Si vous bloquez déjà d'autres types de fichiers, continuez à les bloquer.

Passez à un profil de blocage des fichiers basé sur les meilleures pratiques aussi rapidement que vous êtes à l'aise pour le faire.

Le profil **strict file blocking (blocage des fichiers strict)** prédéfini bloque les types de fichiers généralement utilisés dans les cyberattaques et qui n'ont pas de véritable cas d'utilisation pour le téléchargement vers l'amont et vers l'aval. Cependant, quelques protocoles utilisés à des fins malveillantes peuvent également être requis pour des activités telles que les mises à jour Windows. Le profil **strict file blocking (blocage des fichiers strict)** bloque les fichiers .exe., .dll, .pe et .cab. Pour faire des exceptions afin d'autoriser les protocoles pour une activité spécifique telle que les mises à jour Windows :

1. Créez une règle de politique de sécurité spécifique qui autorise uniquement les utilisateurs qui ont besoin d'accéder à des fins professionnelles et les applications métier qui utilisent les protocoles que vous souhaitez bloquer pour le reste du trafic.
2. Attachez un profil de blocage des fichiers qui autorise les protocoles requis à la règle.
3. Placez la règle au-dessus d'une règle de politique de sécurité avec un profil de blocage des fichiers qui bloque les protocoles pour tout autre trafic.

Cette méthode vous permet d'utiliser des types de fichiers potentiellement malveillants en toute sécurité, ce qui active les applications métier tout en bloquant le trafic malveillant. Affinez les profils et la base de règles pour autoriser toutes les exceptions requises.

Attachez un profil de bonnes pratiques à toutes les règles d'autorisation.

STEP 5 | Attachez le profil d'analyse WildFire par défaut à toutes les règles d'autorisation pour détecter et empêcher les logiciels malveillants de type « zero-day ».

Pour obtenir des mises à jour en temps réel et d'autres fonctionnalités avancées, souscrivez un abonnement WildFire avancé (PAN-OS 10.0 ou version ultérieure) ou un abonnement WildFire.

Déployez le profil WildFire par défaut, qui constitue le profil des meilleures pratiques. WildFire n'a aucun impact sur le trafic réseau, et aucune période de transition n'est donc requise. (Cependant, les paramètres d'action WildFire des meilleures pratiques dans le profil antivirus ont un impact sur le trafic qui génère des signatures qui entraînent une action de réinitialisation ou de suppression ou une

suspension pour la recherche de la dernière signature antivirus.) Attachez un profil d'analyse WildFire à toutes les règles d'autorisation pour envoyer tous les fichiers à WildFire pour analyse.

Dans Cloud Managed Prisma Access, WildFire et Antivirus sont réunis dans un seul profil, que vous ajoutez à un groupe de profils Prisma Access.

STEP 6 | Les groupes de profils de sécurité sont constitués de profils de sécurité individuels combinés dans un groupe nommé, ce qui vous permet d'appliquer des profils de sécurité plus facilement et de manière cohérente aux règles de politique de sécurité.

Créez des groupes de profils de sécurité pour différentes conditions, en fonction de la logique de votre base de règles :

- Chaque groupe de profils doit avoir un objectif distinct, tel que la création de groupes de profils spécifiques au flux de trafic. Par exemple, un groupe de profils pour le trafic entrant n'a pas besoin d'un profil de filtrage des URL, contrairement à un groupe de profils pour le trafic sortant.

  Les groupes de profils spécifiques au flux de trafic facilitent la création d'exceptions si vous souhaitez traiter différemment le trafic interne et externe. Par exemple, vous souhaiterez peut-être bloquer quelque chose pour le trafic interne que vous utilisez et autoriser le trafic externe. Dans ce cas, vous utiliserez des profils différents pour le trafic interne et externe. La nécessité ou non de profils séparés dépend de la manière dont vous souhaitez traiter le trafic.
- Pour faciliter la transition des profils d'alerte au blocage, créez des groupes de profils pour l'alerte initiale et des groupes de profils pour les meilleures pratiques de blocage. Cela facilite l'alerte sur les menaces dans toutes les règles d'autorisation. Au fur et à mesure que vous êtes suffisamment à l'aise pour passer de l'alerte au blocage, les groupes de profils facilitent la modification, car il vous suffit d'échanger un objet au lieu de chaque profil individuel.
- Pensez à créer un groupe de profils par défaut en nommant le groupe **`default (par défaut)`**. Par exemple, créez un groupe avec des profils qui émettent des alertes mais ne bloquent pas la plupart du trafic, en vous basant sur les meilleures pratiques en matière de conseils de transition de profil de sécurité. Le pare-feu applique automatiquement le groupe de profils par défaut à toutes les nouvelles règles de politique de sécurité autorisant le trafic. (Le pare-feu n'applique pas le profil par défaut aux règles existantes.) Cela garantit que toutes les nouvelles règles d'autorisation disposent d'un certain niveau de prévention des menaces. Modifiez ou remplacez le profil par défaut si nécessaire.

Meilleures pratiques en matière de base de règles de politique de sécurité

La base de règles de politique de sécurité est une liste ordonnée de vos règles de politique de sécurité. L'ordre des règles détermine comment le pare-feu gère le trafic.

Les pare-feu comparent le trafic aux règles de politique de sécurité, en commençant par la première règle en haut de la base de règles de politique de sécurité. Lorsque le trafic correspond aux critères d'une règle, le pare-feu exécute l'action de la règle sur le trafic et ne compare le trafic à aucune autre règle. Si aucune règle ne correspond au trafic, le pare-feu abandonne le trafic (déni implicite). La façon dont vous ordonnez les règles dans la base de règles est critique, car le pare-feu agit sur le trafic lors de la première correspondance de règles, puis cesse de comparer le trafic à la base de règles.

Si vous avez migré la politique de sécurité à partir du pare-feu d'un autre fournisseur, le pare-feu précédent pourrait avoir évalué le trafic différemment par rapport à sa base de règles. Par exemple, l'ordre des règles n'a peut-être pas fait de différence sur votre ancien pare-feu, mais elles sont cruciales sur les pare-feu Palo Alto Networks.

Comprendre comment vous voulez gérer différents types de trafic et #unique_18 vous aide à évaluer comment ordonner des règles dans la base de règles. Concevez et optimisez votre base de règles de politique de sécurité de manière logique, comme décrit dans cette section. Pour les bases de règles existantes, si la base de règles n'est pas optimisée autant qu'elle pourrait l'être, planifiez et testez les modifications conformément aux conseils de cette section. Si vous prévoyez de déployer les changements par phases, faites-les au(x) moment(s) approprié(s).

Cette section couvre :

- Classer les règles de politique de sécurité dans la base de règles
- Éviter le gonflement de la base de règles
- Positionner pour faire des exceptions à une règle
- Prévenir et corriger l'effet d'ombre des règles
- Utiliser les hiérarchies de groupes de périphériques sur Panorama pour simplifier la base de règles

STEP 1 | Classez les règles de politique de sécurité logiquement dans la base de règles.

Étant donné que le pare-feu exécute l'action d'une règle de politique sur le trafic lorsque ce trafic correspond aux critères de la règle, l'ordre des règles est critique et détermine quelle règle correspond au trafic, et donc, quelle action le pare-feu prend sur le trafic et comment le pare-feu inspecte le trafic :

1. Placez les règles qui bloquent le trafic malveillant en haut de la base de règles pour éviter d'autoriser accidentellement un mauvais trafic plus tard dans la base de règles. Si vous possédez une licence Advanced Threat Prevention active ou Threat Prevention active, créez des règles de blocage basées sur les listes dynamiques externes (EDL) prédéfinies et testez-les pour vous assurer qu'elles ne bloquent pas le trafic que vous souhaitez autoriser. Sur Panorama, placez ces règles dans les règles « avant » afin qu'elles s'exécutent avant toute règle spécifique au pare-feu.
2. Autorisez les applications d'infrastructure de base et les services communs tels que DNS et NTP près du haut de la base de règles pour éviter de les bloquer accidentellement. Ces règles autorisent généralement le trafic de n'importe quelle zone source vers n'importe quelle zone de destination et s'appliquent à tout et à tous.

   Sur Panorama, placez ces règles dans les règles « avant » afin qu'elles s'exécutent avant toute règle définie localement sur le pare-feu.
3. La logique pour toutes les autres règles est de placer les règles les plus spécifiques près du haut de la base de règles et les règles les plus générales plus près du bas de la base de règles. Si vous placez des règles générales avant des règles spécifiques dans la base de règles, le trafic que vous avez l'intention de faire correspondre à la règle spécifique risquerait à la place de correspondre à la règle générale, ce qui pourrait appliquer une action différente et une inspection différente au trafic que vous souhaitez. C'est ce qu'on appelle l'effet d'ombre : une autre règle a un « effet d'ombre » sur la règle à laquelle vous souhaitez que le trafic corresponde.
4. Si vous n'avez pas encore converti ou ne pouvez pas convertir toutes vos règles de politique de sécurité basées sur les ports et les services en règles basées sur App-ID, placez les règles basées sur App-ID avant les règles basées sur les ports et les services.

STEP 2 | Gardez la base de règles aussi petite que possible pour une gestion plus facile et pour éviter un gonflement de la base de règles.

1. Si cinq des six objets suivants sont identiques dans plusieurs règles, combinez ces règles en une seule règle :

   - Source Zone (Zone source)
   - Destination Zone (Zone de destination)
   - Source IP address (Adresse IP source)
   - Adresse IP de destination
   - Service port (Port de service)
   - Application

   Par exemple, si trois règles spécifient des applications différentes mais ont les mêmes zones source et de destination, adresses IP source et destination et port de service, vous pouvez combiner les règles en une seule règle qui spécifie les applications de chacune des règles d'origine.

2. Utilisez les objets de groupe pour simplifier la création de politique et réduire la taille de la base de règles.

   Utilisez les groupes d'application et les groupes d'adresses pour aider à consolider les règles qui s'appliquent à tous les membres du groupe.

   Si vous utilisez à la fois des objets individuels et des objets de groupe dans une politique, sachez que l'appartenance d'un objet à un groupe peut entraîner un effet d'ombre sur des règles si l'objet est spécifié individuellement dans une règle et également spécifié dans une règle comme faisant partie d'un groupe d'objets. Dans ce cas, le pare-feu risquerait de ne pas prendre l'action prévue, car le trafic pourrait correspondre à la mauvaise règle en premier. Si possible, combinez les règles, sauf si votre processus de contrôle des modifications nécessite une politique spécifique pour suivre l'accès. Si vous souhaitez traiter un objet différemment des autres objets d'un groupe, supprimez l'objet du groupe.

3. Désactivez ou supprimez les règles de la base de règles de politique de sécurité lorsque vous n'en avez plus besoin.

   Les règles de politique de sécurité peuvent devenir inutiles lorsqu'une organisation change d'application ou d'infrastructure, ou lorsque vous n'avez plus besoin de règles de test temporaires. Si vous ne désactivez pas ou ne supprimez pas ces règles, elles risquent de provoquer des actions inattendues sur le trafic. Il est plus sûr de désactiver d'abord une règle afin de pouvoir l'activer à nouveau si sa désactivation cause des problèmes. Lorsque vous désactivez des règles, appliquez une étiquette avec la date à laquelle vous avez désactivé les règles. Utilisez périodiquement la fonctionnalité Rule Usage (Utilisation d'une règle) de Policy Optimizer pour vérifier combien de temps chaque règle a été inutilisée. Après un laps de temps où vous êtes certain que vous n'avez vraiment pas besoin de la règle, supprimez-la.

   *Prenez connaissance des règles avec des applications que vous utilisez uniquement pour des événements périodiques tels que des réunions trimestrielles ou des conférences annuelles. Il peut être approprié de configurer un **Schedule (Planning)** qui active la règle uniquement pendant la période d'événement.*

4. Utilisez Policy Optimizer pour optimiser la base de règles. Policy Optimizer trouve des règles inutilisées, des règles avec des applications inutilisées, des règles qui n'ont pas été utilisées au fil du

temps et des règles qui n'ont pas de profils de transfert de journaux, en plus de vous permettre de gérer de nouvelles applications SaaS dans la politique de sécurité si vous disposez d'un abonnement SaaS Security.

5. Sur Panorama, utilisez des groupes de périphériques globaux communs qui s'appliquent à plusieurs VSYS et pare-feu au sein de l'entreprise pour des règles de politique de sécurité communes et globales telles que des règles qui contrôlent les services de base communs et tout autre service ou application que vous souhaitez appliquer à de larges groupes de périphériques. Créez la hiérarchie des groupes de périphériques de façon à ne pas avoir à répéter les règles entre les groupes : utilisez la hiérarchie pour écrire une règle une seule fois et l'appliquer à tous les groupes de pare-feu appropriés.
6. Examinez périodiquement la base de règles de la politique de sécurité dans le cadre de la maintenance régulière.

STEP 3 | Pour faire une exception à une règle, placez la règle plus spécifique devant la règle plus générale.

Par exemple, vous souhaitez bloquer l'accès de vos employés à des sites Web malveillants, alors vous créez une règle de politique de sécurité générale qui bloque l'accès à tous les sites Web malveillants pour tous les employés. Cependant, votre équipe InfoSec et vos testeurs PEN doivent y avoir accès à des fins de test. Dans ce cas, vous créez une règle qui autorise l'accès aux sites Web malveillants requis pour ces utilisateurs uniquement (décryptage du trafic, application des profils de menaces les plus stricts à la règle et spécification des applications utilisées pour les tests) et placez cette règle au-dessus de la règle générale dans la base de règles.

Lorsque les testeurs InfoSec et Pen essayent d'accéder aux sites malveillants pour les tester, ils y sont autorisés, mais aucun autre utilisateur ne correspond aux critères de la règle, donc la règle générale les bloque. Si vous placez la règle d'accès à l'équipe InfoSec et aux testeurs Pen après la règle de blocage générale, la règle générale fait de l'ombre à la règle spécifique, et le trafic InfoSec / testeurs Pen correspond à la règle générale et est bloqué.

STEP 4 | Empêchez que des règles générales fassent de l'ombre à des règles plus spécifiques.

L'effet d'ombre se produit lorsque vous placez une règle générale qui inclut les mêmes critères de correspondance qu'une règle plus spécifique plus haut dans la base de règles que la règle spécifique, de sorte que le trafic destiné à correspondre à la règle spécifique correspond plutôt à la règle générale en premier, et n'est jamais comparé à la règle spécifique. Ainsi, le pare-feu exécute l'action et l'inspection configurées dans la règle générale lorsque l'intention est d'exécuter l'action et l'inspection dans la règle spécifique. La règle générale fait de l'*ombre* à la règle spécifique.

Une règle à effet d'ombre peut avoir un effet d'ombrer sur plus d'une autre règle dans la base de règles.

La façon la plus simple d'empêcher un effet d'ombre est de construire la base de règles correctement dès le départ. Cependant, les bases de règles existantes et les bases de règles migrées peuvent avoir des règles à effet d'ombre. Pour prévenir et réparer l'effet d'ombre :

1. Comprenez les mesures que vous souhaitez prendre sur le trafic et comment vous souhaitez l'inspecter.

   Si l'action et l'inspection dans la règle spécifique sont la manière dont vous souhaitez gérer le trafic, déplacez la règle spécifique au-dessus de la règle générale dans la base de règles. Si l'action et

l'inspection dans la règle générale sont la façon dont vous souhaitez gérer le trafic, alors vous n'avez pas besoin de la règle spécifique.

2. Placez les règles de politique de sécurité plus spécifiques au-dessus des règles générales dans la base de règles. Si vous placez la règle générale en premier, elle fait de l'ombre à la règle spécifique, par exemple :

   1. Créez une règle générale qui bloque tout accès à Facebook.
   2. Créez une règle spécifique qui permet aux groupes de marketing et de relations publiques d'accéder à Facebook, mais placez la règle en dessous de la règle Facebook générale dans la base de règles.
   3. La règle générale bloque tous les accès à Facebook, quel que soit le groupe d'utilisateurs, de sorte que le trafic ne correspond jamais à la règle spécifique qui autorise l'accès aux groupes spécifiques que vous souhaitez autoriser.

   Le correctif consiste à déplacer la règle spécifique au-dessus de la règle générale dans la base de règles.
3. Examinez et résolvez les règles touchées par un effet d'ombre pour vous assurer que le pare-feu exécute l'action que vous souhaitez et inspecte le trafic de la manière que vous souhaitez.

   Lorsque vous écrivez une nouvelle règle de politique de sécurité :

   1. Sélectionnez une option de validation, puis effectuez une action **Commit (Valider)** sur le pare-feu ou **Validate Commit (Confirmer la validation)** sur Panorama pour vérifier les problèmes de configuration. Ne validez pas la configuration. Résolvez les problèmes que le contrôle de validation découvre avant de poursuivre.
   2. Appuyez sur **Commit (Valider)** ou **Commit and Push (Valider et appliquer)** pour la configuration.
   3. Lorsque la validation se termine, sélectionnez **Tasks (Tâches)** dans le ruban en bas à droite pour ouvrir le Gestionnaire des tâches.
   4. Dans la colonne **Type**, cliquez sur **Commit All (Valider tout)** pour afficher le **Job Status (État du travail)**. (Commit and Push (Valider et appliquer) ne fournit pas d'informations sur l'effet d'ombre.)
   5. Cliquez sur le message de colonne **Status (Statut)** pour ouvrir les **Last Push State Details (Détails de l'état de la dernière transmission)** et sélectionnez l'onglet **Rule Shadow (Effet d'ombre sur les règles)**. S'il n'y a pas d'onglet **Rule Shadow (Effet d'ombre sur les règles)**, alors le pare-feu n'a pas de règles touchées par un effet d'ombre.
   6. Le côté gauche de **Last Push State Details (Détails de l'état de la dernière transmission)** montre les règles qui font de l'ombre aux autres règles. Le nom de chaque règle à effet d'ombre est un lien vers la règle. Pour chaque règle à effet d'ombre, cliquez sur le numéro dans la colonne **Count (Nombre)** pour afficher les règles sur lesquelles elle a un effet d'ombre. Les noms des règles touchées par un effet d'ombre sont listés, mais ce ne sont pas des liens vers ces règles-là.
   7. La liste des règles à effet d'ombre n'est pas persistante dans les opérations de validation. Il est donc crucial pour vous de capturer la liste des règles touchées par un effet d'ombre pour chaque règle à effet d'ombre. Par exemple, extrayez l'état via une API à l'aide d'un script, copiez-collez

la liste dans un éditeur de texte, prenez une capture d'écran, prenez une photographie ou notez le nom des règles à effet d'ombre et des règles touchées par un effet d'ombre.

*L'opération **Commit (Valider)** pour la configuration PAN-OS valide les règles à effet d'ombre. Si un effet d'ombre de règles est détecté, elle génère un message d'avertissement qui identifie les règles affectées. Si vous effectuez une autre opération de validation avant de capturer la liste des effets d'ombre, les informations sur les effets d'ombres sont perdues. Assurez-vous de capturer ces informations immédiatement.*

8. Trouvez chaque règle touchée par un effet d'ombre et chaque règle à effet d'ombre dans la base de règles de politique de sécurité et capturez la configuration de chaque règle.
9. Comparez chaque règle à effet d'ombre avec les règles sur lesquelles elle a un effet d'ombre côte à côte et comprenez le but de chaque règle. Cela vous permet d'évaluer ensemble les règles connexes et de comprendre comment vous souhaitez gérer les applications que les règles contrôlent.
10. Lorsque vous comprenez comment gérer les applications dans une règle à effet d'ombre et ses règles touchées par un effet d'ombre, combinez les règles pour simplifier la base de règles, désactiver ou supprimer les règles en double, et déplacez des règles spécifiques au-dessus des règles générales pour résoudre l'effet d'ombre.
11. Itérez pour corriger tout effet d'ombre restant.
12. Répétez le processus pour chaque règle à effet d'ombre.

Sur les systèmes de test hors production, vous pouvez conserver des règles à effet d'ombre et des règles touchées par un effet d'ombre afin de tester de nouvelles règles de politique et d'autres objectifs de test.

STEP 5 | Sur Panorama, positionnez les règles de politique de sécurité de manière appropriée dans les hiérarchies de groupes de périphériques.

Positionnez des règles pour ne pas avoir à répéter inutilement la même règle dans plusieurs groupes de périphériques. Les règles communes à plusieurs groupes de périphériques appartiennent au-dessus de ces groupes dans la hiérarchie, de sorte qu'une règle s'applique à tous les groupes.

- Construisez la hiérarchie d'une manière réfléchie qui ne donne accès qu'aux groupes de pare-feu auxquels vous avez l'intention d'avoir accès. Pensez à l'accès dont chaque pare-feu a besoin lorsque vous construisez des groupes de périphériques et pensez à l'accès dont chaque groupe de périphériques a besoin lorsque vous créez la hiérarchie des groupes de périphériques. La clé de la construction est le point commun : quels pare-feux ont besoin d'un accès similaire, quels groupes de pare-feux ont besoin d'un accès similaire et comment construire une hiérarchie qui permet aux groupes plus élevés dans la hiérarchie de contenir des règles qui s'appliquent aux niveaux inférieurs et d'éliminer la nécessité de dupliquer des règles.
- Placez les règles qui s'appliquent à tous les pare-feu dans le groupe le plus élevé de la hiérarchie afin d'éviter la duplication de règles.
- Placez les règles applicables aux ensembles de groupes de pare-feu suffisamment haut dans la hiérarchie pour ne pas avoir à dupliquer de règles.

Le Guide de l'administrateur Panorama fournit des informations détaillées sur les groupes de périphériques, notamment un exemple d'illustration d'une hiérarchie de groupes de périphériques.

Meilleures pratiques de Policy Optimizer

Policy Optimizer vous aide à convertir les règles de politique de sécurité basées sur les ports en règles basées sur les applications et à passer à des règles de politique d'accès à moindre privilège :

- Découvrez et convertissez des règles basées sur des ports (l'application est **any (n'importe)** laquelle au lieu d'une application spécifique) en règles basées sur des applications qui suivent le principe du moindre accès aux privilèges (**Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer** > **Rules Without App Controls (Règles sans contrôles d'application)**).
- Découvrez et supprimez les applications inutilisées des règles surapprovisionnées (**Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer** > **Unused Apps (Applications inutilisées)**).
- Découvrez et éliminez les règles que vous n'utilisez pas et comprenez l'utilisation des règles de politique (**Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer** > **Rule Usage (Utilisation des règles)**).
- Découvrez de nouvelles applications qui correspondent aux filtres d'applications et aux groupes d'applications utilisés dans les règles de politique de sécurité. Évaluez les nouvelles applications et si vous souhaitez les autoriser ou les bloquer (**Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer** > **New App Viewer (Nouveau visualiseur d'application)**).

  Si vous disposez d'un abonnement SaaS Security Inline et utilisez l'App-ID Cloud Engine (ACE), utilisez Policy Optimizer pour intégrer les ACE App-ID à votre base de règles de politique de sécurité.
- Découvrez les règles de politique de sécurité qui n'ont pas de profil de transfert des journaux attaché et ajoutez des profils de transfert des journaux à ces règles (**Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer** > **Log Forwarding for Security Services (Transfert des journaux pour les services de sécurité)**).

Policy Optimizer est disponible dans PAN-OS 9.0 et versions ultérieures pour les pare-feu Panorama et PAN-OS (les pare-feu peuvent être sur PAN-OS 8.1 si Panorama exécute PAN-OS 9.0 ou versions ultérieures). Prisma Access ne prend pas en charge Policy Optimizer.

Pour la compatibilité avec Cortex Data Lake, Panorama exécutant PAN-OS 10.0.3 ou version ultérieure avec le plug-in Cloud Services 2.0 Innovation ou version ultérieure installé.

Les meilleures pratiques de Policy Optimizer couvrent les éléments suivants :

- Utilisation de Policy Optimizer—Principaux cas d'utilisation, comment ajouter des applications aux règles de politique de sécurité, règles de tri et de filtrage et utilisation des filtres d'application et des groupes d'applications.
- Flux de travail de base de règles Policy Optimizer—Comment planifier une transition vers des règles basées sur des applications, convertir des règles basées sur des ports en règles basées sur des applications, éliminer les règles inutilisées et supprimer les applications inutilisées pour resserrer la base de règles.

Décryptez *dès que possible tout le trafic autorisé par les réglementations locales, la conformité, les exigences de votre entreprise et les considérations relatives à la confidentialité pour fournir des informations plus précises sur les applications et gagner en visibilité sur les applications que vous contrôlez avec Policy Optimizer. Sans décryptage, le pare-feu peut souvent identifier les applications parentes, mais il ne peut généralement pas identifier les applications fonctionnelles. Par exemple, le pare-feu voit « facebook », mais pas facebook-post, facebook-download, facebook-file-sharing, etc. Vous devez décrypter le trafic pour obtenir une visibilité et un contrôle sur les applications fonctionnelles. Pour le décryptage de type* Proxy de transfert SSL *(sortant), mettez d'abord en œuvre le filtrage des ID utilisateur et des URL afin de pouvoir cibler efficacement le décryptage.*

Utilisation de Policy Optimizer

Cette section décrit les principaux cas d'utilisation de Policy Optimizer et comment utiliser l'outil. Flux de travail de base de règles Policy Optimizer décrit les flux de travail.

Les cas d'utilisation de Policy Optimizer incluent les éléments suivants :

- **Migration à partir de règles basées sur des applications basées sur des ports** : affichez les applications de couche 7 qui correspondent à chaque règle basée sur des ports, sélectionnez les applications que vous souhaitez autoriser et convertissez chaque règle en une ou plusieurs règles basées sur des applications.
- **Nouveaux déploiements** : découvrez les applications sur votre réseau et passez à une politique basée sur les applications au fil du temps.
- **Déploiements matures** : examinez votre base de règles, convertissez des règles générales basées sur des filtres d'applications en règles strictes basées sur des groupes d'applications qui autorisent uniquement les applications que vous sanctionnez et éliminez les règles et applications inutilisées.
- **DevOps** : comprenez les applications nouvelles ou modifiées dans votre environnement de test. Déterminez comment les gérer dans les règles de politique de sécurité avant d'apporter des modifications à votre environnement de production. Testez les règles nouvelles et modifiées avant de les appliquer dans un environnement de production.

STEP 1 | Collaborez avec les personnes compétentes pour comprendre les applications sanctionnées que vous souhaitez autoriser sur votre réseau à des fins professionnelles et les applications tolérées que vous souhaitez autoriser pour les employés.

Soyez conscient des applications critiques pour l'entreprise. Sachez quelles applications ne sont utilisées que périodiquement pour des événements trimestriels, annuels ou autres et évaluez les règles pertinentes suffisamment longtemps pour voir l'activité de ces applications. Connaître la logique métier pour autoriser les applications vous aide à comprendre comment construire une politique de sécurité. Pour mieux comprendre les applications, recherchez les App-ID fournis par le contenu dans applipedia ou dans **Objects (Objets)** > **Applications** sur le pare-feu ou Panorama.

STEP 2 | Apprenez à trier, filtrer et examiner les informations et statistiques de Policy Optimizer en utilisant différentes mesures à des fins différentes.

Les statistiques de Policy Optimizer ne sont pas communiquées en temps réel. Il faut environ une heure ou plus, selon le volume de trafic des applications et la taille de la base de règles, pour mettre à jour la liste des applications. Après avoir ajouté une application à une règle, attendez au moins une heure avant

de générer les journaux du trafic pour voir les informations journalisées de l'application. Si vous ne voyez pas les informations, patientez un moment et vérifiez à nouveau.

*Policy Optimizer ignore le trafic des règles avec **Log at Session Start (Journalisation en début de session)** uniquement pour éviter de compter les applications transitoires. (Pour les règles avec **Log at Session End (Journalisation en fin de session)** également, Policy Optimizer récupère les statistiques des règles.)*

STEP 3 | Comprenez comment utiliser les filtres d'application et les groupes d'applications dans la politique de sécurité.

Utilisez les filtres d'application dans les règles de politique de sécurité pour découvrir des applications sur votre réseau. Convertissez ensuite ces règles de filtres d'applications en groupes d'applications afin de pouvoir spécifier les applications exactes à autoriser.

- Utilisez les **groupes d'applications** autant que possible pour simplifier et renforcer les règles de politique de sécurité et réduire la taille de la base de règles.

  Les groupes d'applications sont des ensembles définis par l'utilisateur d'applications spécifiques que vous souhaitez contrôler en une seule règle avec un traitement de sécurité similaire. Ajoutez des applications aux règles en utilisant des groupes d'applications (la rubrique liée se concentre sur les applications ACE, mais s'applique à toutes les applications) pour contrôler plusieurs applications avec une seule règle au lieu de créer une règle distincte pour chaque application. Réutilisez les groupes d'applications dans différentes règles pour donner aux différents utilisateurs, aux différentes sources et destinations un accès différent aux applications. La réutilisation des groupes automatise l'ajout d'applications à plusieurs règles (lorsque vous apportez une modification à un groupe d'applications, la modification est reflétée dans chaque règle incluant le groupe d'applications).
- Utilisez **les filtres d'application** pour les actions suivantes :
  - Découvrez des applications sur votre réseau.
  - Règles pérennes en traitant les nouvelles applications automatiquement lorsqu'elles correspondent à un filtre. Ceci est utile à la fois dans la phase de découverte des applications dans les migrations et les nouveaux déploiements et dans les environnements matures.

    Par exemple, créez une règle d'autorisation avec un filtre d'application basé sur l'étiquette **Palo Alto Networks**. Cela garantit que vous autorisez toutes les applications Palo Alto Networks actuelles et toutes les applications Palo Alto Networks futures.

    Un autre exemple est la création d'une règle qui filtre les nouveaux App-ID fournis par le contenu pour les gérer en toute sécurité jusqu'à ce que vous puissiez les examiner de plus près.
  - Dans les bases de règles matures, ajoutez des applications aux règles en utilisant des filtres d'application pour bloquer les types d'applications indésirables. Utilisez les groupes d'applications pour autoriser délibérément le trafic (la rubrique liée se concentre sur les applications ACE, mais s'applique à toutes les applications).

  Les filtres d'applications sont des ensembles dynamiques d'applications. Les applications correspondent aux filtres d'application en fonction des attributs que vous définissez, tels que la catégorie, la sous-catégorie, le risque, les étiquettes (étiquettes prédéfinies ou étiquettes personnalisées) et les caractéristiques. Le pare-feu ajoute automatiquement de nouvelles applications à un filtre lorsqu'elles correspondent aux critères du filtre. Les règles de politique de sécurité avec

un filtre d'application contrôlent automatiquement les nouvelles applications qui correspondent au filtre.

Les filtres d'application sont des contrôles plus lâches que les groupes d'applications. Vous contrôlez exactement quelles applications se trouvent dans un groupe d'applications. Les attributs que vous définissez contrôlent les applications dans un filtre d'application, ce qui peut conduire à autoriser plus d'applications que vous devez autoriser. C'est pourquoi les filtres sont les meilleurs éléments pour découvrir le trafic et pour bloquer les sous-catégories de trafic des applications. Réutilisez les filtres d'application dans différentes règles pour donner aux différents utilisateurs, aux différentes sources et destinations un accès différent aux applications.

Utilisez autant que possible les groupes d'applications et les filtres d'applications au lieu d'ajouter des applications individuelles aux règles. À partir de PAN-OS 10.1, vous pouvez ajouter des applications à des groupes d'applications et des filtres directement depuis Policy Optimizer, ce qui est une bonne pratique, car cela vous donne une visibilité sur toutes les applications qu'une règle voit.

Avant PAN-OS 10.1, ajoutez des applications aux groupes et aux filtres avec **Objects (Objets)** > **Application Groups (Groupes d'applications)** et **Objects (Objets)** > **Application Filters (Filtres d'application)**.

STEP 4 | Décidez des applications à ajouter à une règle en fonction de son objectif. Le but de la règle permet de déterminer qui a besoin d'accéder aux applications et comment accorder l'accès (source, destination, inspection, journalisation).

STEP 5 | Réutilisez les objets de filtre d'application et de groupe d'applications dans la politique pour donner à différents groupes d'utilisateurs différents niveaux d'accès à ces applications et/ou traiter différemment des combinaisons de sources et de destinations.

User-ID fait partie intégrante de la création des meilleures pratiques en matière de politique de sécurité basée sur le principe de l'accès au moindre privilège. Sans User-ID, vous ne pouvez pas spécifier qui peut utiliser les applications.

La réutilisation des objets de groupe d'applications et de filtres d'applications réduit le gonflement de la base de règles en simplifiant la base de règles.

Flux de travail de base de règles Policy Optimizer

Cette section décrit la transition entre les règles basées sur les ports et les règles et workflows basés sur les applications pour l'outil Policy Optimizer. Utilisation de Policy Optimizer décrit les principaux cas d'utilisation et comment utiliser l'outil.

L'objectif final est de verrouiller les règles afin qu'elles n'autorisent que les applications sanctionnées et les applications que vous tolérez pour l'utilisation des employés. Conjointement à cela, verrouillez les utilisateurs qui ont des raisons commerciales légitimes d'accéder à différentes applications. Utilisez les journaux de trafic et l'ACC pour vous aider à restreindre la portée des règles à des utilisateurs spécifiques afin d'éviter de surapprovisionner l'accès des utilisateurs. Travailler avec les propriétaires d'applications et d'autres groupes pour comprendre qui a des raisons commerciales d'accéder aux applications.

STEP 1 | Planifiez une transition progressive des règles basées sur les ports aux règles basées sur les applications et comprenez les concepts et méthodes clés de transition.

Planification et méthodologie des migrations et des nouveaux déploiements :

- Pour les migrations de règles basées sur les ports vers des règles basées sur les applications, commencez par votre base de règles de politique de sécurité basée sur les ports. Pour les nouveaux

déploiements et les nouvelles migrations, créez des règles basées sur des filtres d'application pour gagner en visibilité sur différents types d'applications et ajoutez une règle de récupération de la totalité en bas de la base de règles afin de ne pas bloquer accidentellement les applications stratégiques. Appliquez à ces règles les profils de prévention des menaces des meilleures pratiques (dans les deux sens) et les profils de filtrage des URL (trafic sortant). Comme les applications correspondent aux règles de récupération de la totalité, suivez les conseils de l'étape 2 pour prioriser les règles à convertir et à affiner en premier, et combien de temps observer les règles avec différents types d'applications avant de les faire passer à des règles basées sur les applications.

Policy Optimizer vous montre les applications spécifiques de couche 7 (App-ID) qui correspondent à chaque règle basée sur le port.

- Exécutez des rapports d'évaluation des meilleures pratiques directement dans AIOps pour définir une référence afin de comprendre votre état actuel des meilleures pratiques. Exécutez des rapports périodiques pour mesurer les progrès. La progression signifie moins de règles basées sur les ports, moins de règles inutilisées et moins de règles avec des applications inutilisées au fil du temps.

Planification et méthodologie des déploiements existants :

- Si le déploiement consiste en règles basées sur les ports ou principalement en règles basées sur les ports, suivez les conseils précédents pour migrer vers une politique basée sur les applications.
- Si le déploiement se compose principalement de règles basées sur des applications, placez une règle de récupération de la totalité au bas de la base de règles de politique de sécurité pour découvrir et gagner en visibilité les applications qui ne correspondent pas à d'autres règles, avec des profils de sécurité stricts pour arrêter le trafic malveillant. Suivez les conseils de priorisation à l'étape 2 pour resserrer les règles.

Après avoir déplacé des applications de règles basées sur des ports vers des règles basées sur des applications, sélectionnez les règles basées sur des ports dans Policy Optimizer et **Reset Rule Hit Counter (Réinitialiser le compteur d'accès de la règle)**. Cela réinitialise le compteur **Days with no new apps (Jours sans nouvelles applications)** afin que vous puissiez voir quand plus de nouvelles applications correspondent aux règles originales basées sur les ports et évaluer si vous souhaitez les autoriser ou les bloquer.

Après avoir affiné une règle, attendez que **Days with no new apps (Jours sans nouvelles applications)** atteigne au moins sept jours avant de revenir sur la règle pour continuer à l'affiner. Lorsque les règles de récupération de la totalité et les règles basées sur les ports ne voient plus les applications que vous souhaitez autoriser, désactiver ou supprimer. Soyez attentif aux applications que votre entreprise utilise uniquement pour des événements périodiques avant de désactiver ou de supprimer une règle.

STEP 2 | Hiérarchisez et convertissez les règles de politique de sécurité basées sur les ports (règles avec l'application définie sur **any (n'importe laquelle)**) en règles basées sur les applications de couche 7.

Donner la priorité aux règles à convertir des règles basées sur les ports aux règles basées sur les applications à quelle phase de la transition. Ces techniques sont valables pour les migrations et les

nouveaux déploiements, et pour les déploiements applicatifs existants où vous devez resserrer votre base de règles :

1. Dans les déploiements nouveaux et existants, bloquez immédiatement le trafic malveillant et risqué connu.
2. Implémentez des règles de récupération de la totalité basées sur les filtres d'application.
3. Conversion des règles simples avec des applications bien connues après une semaine. Par exemple, les règles qui contrôlent le port 21 (FTP), le port 53 (DNS), le port 22 (SSH) sont de bons candidats pour une conversion rapide. Moins les applications sont connues dans une règle basée sur un port, plus vous pouvez être sûr de la convertir en règle basée sur une application.
4. Après 30 jours, convertissez les règles les plus stables. Les règles qui ne voient pas de nouvelles demandes sur une période de 30 jours et qui contrôlent relativement peu de demandes sont de bons candidats.
5. Après au moins 30 jours, commencez à convertir les règles d'accès à Internet (ssl, navigation web) et les règles qui voient le plus de trafic.
6. Après une période appropriée pour les applications vues sur la règle, convertissez les règles avec peu d'applications vues.
7. Lorsque vous convertissez des règles, examinez chaque règle lorsque les **Days with no new Apps (Jours sans nouvelles applications)** atteignent au moins sept jours (plus long pour les règles complexes ou les règles avec de nombreuses applications) et gérez les nouvelles applications selon les besoins.

Les règles de clonage sont le moyen le plus sûr de passer de règles basées sur les ports à des règles basées sur les applications. Le clonage préserve la règle d'origine basée sur le port et place la règle clonée directement au-dessus de la règle d'origine. Cela vous permet de découper des règles spécifiques basées sur des applications à partir de la règle d'origine sans risquer la disponibilité de l'application, comme le montre cet exemple de cas d'utilisation du clonage pour migrer votre navigation web et votre trafic SSL vers des règles basées sur des applications. Les applications qui ne correspondent pas aux règles clonées continuent de correspondre à la règle d'origine basée sur les ports. Lorsque la règle d'origine cesse de voir les applications que vous souhaitez sur votre réseau pendant une période appropriée, vous pouvez désactiver ou supprimer la règle d'origine en toute sécurité.

Utilisez correctement les groupes d'applications et les filtres d'applications lorsque vous convertissez des règles.

Pour les scénarios de migration, suivez les meilleures pratiques pour la migration vers une politique basée sur les applications.

STEP 3 | Lorsque vous examinez les règles, utilisez des filtres d'application pour bloquer les types d'applications que vous savez que vous ne voulez pas sur votre réseau. Bloquez le trafic en fonction des sous-catégories, des étiquettes et des caractéristiques. Utilisez les filtres d'application pour faire des exceptions aux règles de blocage. N'utilisez pas le risque comme critère de filtrage bloquant, utilisez le risque pour déterminer comment inspecter, enregistrer et contrôler le trafic de manière appropriée.

En plus des règles de blocage recommandées pour arrêter le trafic malveillant connu, révisez régulièrement vos règles et bloquez d'autres trafics que vous ne voulez pas :

1. Identifiez les types d'applications que vous ne voulez pas sur votre réseau et créez des filtres d'application qui leur correspondent. Créez des règles de blocage basées sur ces filtres d'application

et placez-les devant toute règle de récupération de la totalité (ou clonez la règle à partir d'une règle existante et placez la règle clonée directement au-dessus de la règle d'origine dans la base de règles).

2. Déterminez s'il existe des applications spécifiques au sein des types d'application bloqués que vous souhaitez autoriser sur votre réseau. Clonez la règle de blocage, définissez l'**Action** sur **Allow (Autoriser)** et supprimez toutes les applications, sauf les applications que vous souhaitez autoriser. Placez la règle d'autorisation directement au-dessus de la règle de blocage pour créer des exceptions à la règle de blocage.
3. Surveillez la règle de blocage pour voir si vous souhaitez autoriser d'autres applications bloquées. Si vous avez créé une règle d'autorisation pour les exceptions, ajoutez des applications que vous souhaitez autoriser à cette règle. Sinon, créez une nouvelle règle d'autorisation pour les applications et placez-la directement au-dessus de la règle de blocage dans la base de règles.

Par exemple, les applications de partage de fichiers peuvent présenter un risque élevé. Décryptez le trafic et, dans la règle de politique de sécurité, autorisez uniquement les applications de partage de fichiers spécifiques que vous utilisez à des fins professionnelles pour les utilisateurs nécessaires et inspectez et enregistrez le trafic. Dans la règle suivante de la base de règles, utilisez un filtre d'application basé sur la sous-catégorie **file-sharing (partage de fichiers)** pour bloquer toutes les applications de partage de fichiers que vous n'autorisez pas explicitement et délibérément.

STEP 4 | Supprimer les applications inutilisées des règles surapprovisionnées.

Comprenez le but d'une application avant de la supprimer d'une règle.

- Comparez les **Apps Used (Applications utilisées)** aux **Apps Allowed (Applications autorisées)**. Si la règle autorise plus d'applications que la règle n'en utilise, examinez les applications inutilisées et déterminez si vous pouvez les supprimer.
- Prenez connaissance des applications utilisées uniquement pour des événements trimestriels, annuels ou autres événements périodiques. Assurez-vous de capturer un historique assez long de la règle pour voir ces applications. Prenez également en compte les applications qui sont actives dans votre environnement de test et qui ont été ajoutées à votre environnement de production en prévision de la sanction de l'application.

STEP 5 | Supprimez les règles inutilisées de la base de règles de politique de sécurité.

Les règles inutilisées encombrent et compliquent la base de règles. L'utilisation des règles vous montre des informations sur les règles non utilisées sur différentes périodes. Évaluez les applications dans les règles pour voir si vous en avez besoin même si elles n'ont pas été utilisées. Avant de supprimer les règles inutilisées, prenez en compte les éléments suivants :

- **Règles de blocage sans correspondance** : ne désactivez ni ne supprimez ces règles. Par exemple, une règle de blocage utilisant une menace EDL ne reçoit aucune correspondance. C'est bien, mais vous voulez continuer à bloquer au cas où du trafic malveillant tenterait d'accéder à votre réseau.
- **Règles temporaires** : par exemple, règles pour les sous-traitants ou les auditeurs. Au lieu de supprimer ces règles, s'il y a un temps d'accès régulier, configurez une planification pour contrôler quand la règle est en vigueur. Si l'accès est intermittent, désactivez les règles et activez-les en cas de besoin.
- **Règles de politique désactivées** : appliquez une étiquette avec la date à laquelle les règles ont été désactivées. Si les règles ne sont pas utilisées dans un délai donné, par exemple plus d'un an, la règle peut être supprimée. Ajoutez une **Description** pour indiquer pourquoi la règle est désactivée et pourquoi ou quand elle doit être activée, par exemple, pour l'accès des auditeurs ou des sous-traitants.

- **Applications utilisées de manière périodique** : certaines applications ne sont utilisées que pour des événements trimestriels, annuels ou autres. Capturez un historique suffisamment long des règles qui contrôlent ce type d'applications pour être sûr que les applications ne sont plus utilisées.

STEP 6 | Assurez-vous que chaque règle a un profil de transfert des journaux approprié attaché.

Identifiez les règles sans profils de transfert des journaux et ajoutez-y des profils (**Policies (Politiques)** > **Security (Sécurité)** > **Policy Optimizer** > **Log Forwarding for Security Services (Transfert des journaux pour les services de sécurité)**).

STEP 7 | Convertissez les règles générales basées sur des filtres d'application en règles étroites basées sur des groupes d'applications.

Utilisez les statistiques d'utilisation des règles pour comprendre comment les règles sont utilisées et utilisez Policy Optimizer pour ajouter des applications aux groupes d'applications (PAN-OS 10.1 et versions ultérieures; pour PAN-OS 10.0 et versions antérieures, ajoutez des applications aux groupes d'applications dans**Objects (Objets)** > **Application Groups (Groupes d'applications)**) et créez des règles plus strictes.

L'objectif final est d'autoriser uniquement les applications que vous approuvez au lieu d'autoriser un plus large éventail d'applications correspondant à un filtre d'application. Utilisez les filtres d'applications pour découvrir les applications sur votre réseau et bloquer de larges sous-catégories d'applications, et utilisez les groupes d'applications pour spécifier les applications exactes que vous souhaitez autoriser. Pour convertir des règles basées sur des filtres d'application en règles basées sur des groupes d'applications avec Policy Optimizer :

- Examinez les applications qui correspondent aux règles basées sur des filtres d'application et déterminez les applications que vous souhaitez autoriser.
- Pour chaque règle basée sur un filtre d'application, sélectionnez les applications à autoriser et ajoutez-les à un groupe d'applications dans une règle clonée ou existante.
- Après avoir déplacé des applications de règles basées sur des filtres d'applications vers des règles basées sur des groupes d'applications, sélectionnez ces règles dans Policy Optimizer et **Reset Rule Hit Counter (Réinitialiser le compteur d'accès de la règle)**. Cela réinitialise le compteur **Days with no new apps (Journées sans nouvelles applications)**. Ainsi, vous pouvez voir quand de nouvelles applications correspondent aux règles basées sur des filtres d'application.
- Surveillez les règles basées sur les filtres d'application jusqu'à ce que le compteur **Days with no new apps (Journées sans nouvelles applications)** atteigne un seuil indiquant qu'une règle ne voit plus de nouvelles applications. Le seuil dépend de votre environnement et des types d'applications auxquels le filtre d'application correspond. Prenez en compte les applications utilisées uniquement à certaines périodes, telles que les événements trimestriels ou annuels, et laissez le filtre en place assez longtemps pour voir ces applications afin de pouvoir les ajouter aux groupes d'applications appropriés. Si la règle de filtre d'application ne correspond à aucune application que vous souhaitez autoriser sur votre réseau, désactivez ou supprimez la règle, selon la politique de votre entreprise.

STEP 8 | Examinez et mettez à jour les règles de politique de sécurité lorsque de nouvelles applications entrent dans votre environnement.

Examinez régulièrement les nouveaux App-ID dans New App Viewer (Nouveau visualiseur d'application). Ajoutez des applications à des groupes d'applications existants et nouveaux ou pour ajouter des applications directement à des règles de politique de sécurité existantes. Continuez à convertir les filtres d'application en groupes d'applications.

Meilleures pratiques d'App-ID Cloud Engine

L'App-ID Cloud Engine (ACE) identifie des milliers d'applications SaaS que le pare-feu a précédemment identifiées comme du trafic SSL ou de navigation web, et non comme des applications spécifiques. ACE donne à ces applications SaaS des App-ID spécifiques afin que vous puissiez gagner en visibilité sur celles-ci, les contrôler et les utiliser explicitement dans la politique de sécurité.

ACE nécessite PAN-OS 10.1 ou version ultérieure et un abonnement SaaS Security Inline. ACE est disponible dans Prisma Access Cloud Services 3.0 Innovation pour Panorama Managed Prisma Access et est également disponible dans Cloud Managed Prisma Access.

Les App-ID ACE sont pris en charge uniquement dans la politique de sécurité. Vous ne pouvez pas utiliser les ID d'application ACE dans tout autre type de règle de politique.

Le pare-feu télécharge l'intégralité du catalogue des App-ID ACE, mais il ne télécharge que les signatures des App-ID ACE pour les applications vues dans l'environnement.

ACE contrôle les applications SaaS dans les flux sortants et agit comme un broker de sécurité d'accès au cloud (CASB). Dans les nouveaux déploiements, ACE identifie les applications SaaS sur votre réseau pour simplifier le passage à une politique basée sur les applications de couche 7.

Dans les déploiements existants, ACE fournit des outils pour comprendre et gérer en toute sécurité les nombreuses applications SaaS potentiellement identifiées comme du trafic SSL ou de navigation web et les contrôler explicitement dans la politique de sécurité.

Décryptez *dès que possible tout le trafic autorisé par les réglementations locales, la conformité, les exigences de votre entreprise et les considérations relatives à la confidentialité pour fournir des informations plus précises sur les applications et gagner en visibilité sur les applications ACE. Sans décryptage, le pare-feu peut souvent identifier les applications parentes, mais il ne peut généralement pas identifier les applications fonctionnelles. Par exemple, le pare-feu voit « facebook », mais pas facebook-post, facebook-download, facebook-file-sharing, etc. Vous devez décrypter le trafic pour obtenir une visibilité et un contrôle sur les applications fonctionnelles. Pour le décryptage de type Proxy de transfert SSL (sortant), mettez d'abord en œuvre le filtrage des ID utilisateur et des URL afin de pouvoir cibler efficacement le décryptage.*

STEP 1 | Comprenez comment les App-ID ACE fonctionnent sur le pare-feu avant d'activer ACE.

Lisez la section Traitement ACE et utilisation des politiques pour découvrir comment le pare-feu gère les App-ID ACE, notamment :

- Comment et quand le pare-feu télécharge des App-ID ACE.
- Les différences entre les App-ID ACE et les App-ID fournis par le contenu.
- Comment le pare-feu résout les conflits entre les App-ID ACE, les App-ID fournis par le contenu et les App-ID personnalisés, y compris les applications conteneurs (par exemple, facebook) et leurs applications fonctionnelles (par exemple, facebook-post, facebook-download, etc.).
- Le comportement HA.
- Le comportement de Panorama lors de la validation ou de la poussée.

ACE identifie les applications SaaS spécifiques que le pare-feu a précédemment identifiées comme du trafic SSL ou de navigation web. Lorsque vous activez ACE :

- Si vous disposez d'une règle de politique de sécurité qui autorise le trafic SSL et de navigation web, les App-ID ACE téléchargés correspondent à cette règle, à moins qu'ils ne correspondent à un filtre d'application utilisé dans une règle. Les App-ID ACE correspondent à un filtre d'application en fonction des critères du filtre, y compris les étiquettes, tout comme les App-ID fournis par le contenu. Si un App-ID ACE correspond à un filtre d'application dans une règle, l'application est ajoutée implicitement à la règle. Cette règle contrôle l'application ACE au lieu de la règle SSL/de navigation web, y compris l'action de la règle (autoriser ou refuser), les utilisateurs qui peuvent accéder à l'application, les sources et destinations, et la manière dont l'application est inspectée et journalisée.
- Jusqu'à ce que vous ajoutiez explicitement un App-ID ACE à une règle ou qu'un App-ID ACE corresponde à un filtre d'application qui l'ajoute implicitement à une règle, une application ACE continue de correspondre à la règle d'autorisation SSL/de navigation web, comme avant l'activation d'ACE.
- Si vous n'avez aucune règle autorisant le trafic SSL et de navigation web, suivez les conseils de l'étape 3 pour découvrir et contrôler des App-ID ACE.

Si vous utilisez explicitement un App-ID ACE dans la politique, le pare-feu traite l'application de la même manière qu'il traite les applications fournies par le contenu.

STEP 2 | Examinez votre base de règles de politique de sécurité pour rechercher les règles qui utilisent des filtres d'application avant d'activer ACE.

Les filtres d'applications autorisent les applications en fonction de critères de filtrage correspondants, y compris les étiquettes. Dès lors, ils ajoutent automatiquement des applications aux règles et vous devez examiner ces règles pour voir les applications précises que chaque filtre autorise et les utilisateurs qui ont accès à ces applications. Lorsqu'un App-ID ACE correspond à un filtre d'application dans une règle, cette règle peut ne pas autoriser les mêmes utilisateurs que la règle SSL et de navigation web. Les utilisateurs qui avaient accès à l'application dans la règle SSL et de navigation web peuvent perdre l'accès à l'application, car elle ne correspond plus à cette règle et ces utilisateurs ne sont pas spécifiés dans la règle explicite.

Il est essentiel de comprendre qui doit utiliser quelles applications à des fins professionnelles, en particulier dans les environnements comportant un grand nombre de règles, d'applications et de groupes d'utilisateurs. Par exemple, si vous utilisez l'étiquette ***Web Apps (Applis web)*** *dans un groupe d'applications dans une règle, l'étiquette ajoute implicitement les applications ACE correspondantes à la règle. Ces applications ACE ne correspondent pas à la règle SSL et de navigation web et seuls les utilisateurs spécifiés dans la règle* ***Web Apps (Applis web)*** *peuvent y accéder.*

Si aucune règle n'a de filtres d'application, il n'y a aucun risque que les applications ACE correspondent automatiquement aux règles existantes une fois que vous avez activé ACE, car vous n'avez pas encore ajouté explicitement d'applications ACE aux règles.

Si vous utilisez des filtres d'application dans les règles de politique de sécurité, lorsque vous activez ACE :

- Pour les règles de déni, les applications ACE qui correspondent à la règle sont bloquées, ce qui est précisément ce que vous voulez faire avec les applications qui correspondent à la règle de déni. La

règle est plus efficace, car vous bloquez désormais les applications SaaS non autorisées que le pare-feu ne pourrait pas identifier sans ACE.

- Pour les règles d'autorisation, surveillez de près les applications autorisées par la règle. L'ajout implicite d'applications avec un filtre repose sur des critères et non sur l'ajout délibéré d'applications spécifiques par un administrateur. Les règles les plus impactées sont celles présentant des filtres basés sur des étiquettes larges telles que **Web App (Appli web)**, qui s'appliquent à la majorité des App-ID ACE et fournis par le contenu.

  Dans les déploiements existants, gardez à l'esprit que si vous disposez d'une règle autorisant le trafic SSL et de navigation web, vous autorisez toutes les applications qu'ACE identifie désormais. Utilisez des filtres d'application pour bloquer *les types de trafic qui doivent absolument être bloqués et continuer à autoriser le reste des applications pendant que vous déterminez ce que vous souhaitez autoriser et ce que vous souhaitez bloquer.*

Les étapes 3, 4 et 5 vous montrent comment utiliser les filtres d'application pour ajouter des App-ID ACE aux règles en toute sécurité.

STEP 3 | Autorisez explicitement les applications ACE à l'aide de filtres d'application afin que vous puissiez évaluer les applications de manière contrôlée.

Il est plus facile de créer des filtres d'application pour autoriser les types d'applications que vous souhaitez sur votre réseau que d'examiner périodiquement toutes les nouvelles applications ACE pour déterminer celles à autoriser. Les filtres d'application vous permettent d'examiner côte à côte les mêmes types d'applications et de déterminer celles que vous souhaitez autoriser à des fins professionnelles.

1. Créez un filtre d'application basé sur l'étiquette **App-ID Cloud Engine**, qui correspond à tous les App-ID ACE (applications identifiées comme SSL ou de navigation web avant ACE). Attachez le filtre à une règle de politique de sécurité avec les profils de sécurité et la journalisation appropriés, et placez la règle au bas de la base de règles de politique de sécurité. Cela garantit que la règle correspond à tous les App-ID ACE nouveaux et existants et les autorise, à moins qu'ils ne soient spécifiés dans une règle antérieure. Cela permet également de s'assurer que les règles de blocage du pare-feu prennent effet avant que le pare-feu ne compare le trafic à la règle d'autorisation ACE.
2. À mesure que vous vous familiarisez avec les applications ACE, créez des règles de filtres d'application plus spécifiques basées sur des sous-catégories, des étiquettes, des risques et des caractéristiques pour qu'elles correspondent à des groupes d'applications plus restreints. Placez ces règles d'autorisation directement au-dessus de la règle d'autorisation ACE générale basée sur l'étiquette **App-ID Cloud Engine**. En limitant les applications qui correspondent à un filtre, vous pouvez examiner côte à côte des applications plus similaires et déterminer celles que vous souhaitez autoriser à des fins professionnelles.
3. Consultez fréquemment la nouvelle visionneuse d'applications dans Policy Optimizer pour voir quels App-ID ACE téléchargés correspondent aux règles de politique de sécurité et pour obtenir une meilleure visibilité sur ces applications. Évaluez les applications et déterminez si vous devez les autoriser ou les bloquer.

   N'ajoutez pas d'utilisateurs à des règles dotées de filtres d'application pour les élargir, car cela autorise un accès plus important que nécessaire aux applications. Le surapprovisionnement de l'accès utilisateur augmente les risques et va à l'encontre des principes d'accès réseau Zero Trust. Autorisez uniquement les utilisateurs qui ont besoin d'un accès à des fins professionnelles.

STEP 4 | Utilisez des filtres d'application pour bloquer les types d'applications que vous ne souhaitez pas autoriser sur votre réseau en fonction de sous-catégories, d'étiquettes et de caractéristiques. N'utilisez pas le risque comme critère de filtre de blocage (le risque est une évaluation du risque relatif au sein d'une catégorie ou d'une sous-catégorie, pas nécessairement d'une utilisation malveillante). Utilisez le risque pour déterminer la manière d'inspecter, de journaliser et de contrôler le trafic de manière appropriée.

Le blocage basé sur des filtres d'application est plus simple que l'examen périodique de toutes les nouvelles applications ACE pour déterminer les applications à autoriser ou non sur le réseau. Avec des filtres d'application, le pare-feu bloque immédiatement les nouvelles applications que vous ne voulez pas autoriser.

1. Déterminez les types d'applications ACE que vous ne souhaitez pas autoriser sur votre réseau. Créez des règles de blocage basées sur ces types d'applications et placez-les au-dessus des règles fourre-tout.
2. Déterminez si ces types contiennent des applications spécifiques que vous souhaitez autoriser sur votre réseau. Si vous souhaitez autoriser certaines applications :
    1. Clonez la règle de blocage.
    2. Définissez l'**Action** sur **Allow (Autoriser)**.
    3. Supprimez toutes les applications de la règle, à l'exception des applications que vous souhaitez autoriser.
    4. Spécifiez les utilisateurs qui ont besoin d'accéder aux applications autorisées, ajoutez les profils de sécurité appropriés et configurez la journalisation.
    5. Placez la nouvelle règle d'autorisation directement au-dessus de la règle de blocage pour créer des exceptions à la règle de blocage.
3. Surveillez la règle de blocage pour voir s'il y a d'autres applications spécifiques que vous souhaitez autoriser. Le cas échéant, ajoutez-les à une règle d'autorisation existante ou créez une nouvelle règle d'autorisation pour ces exceptions.

Par exemple, les applications de partage de fichiers peuvent présenter un risque élevé. Autorisez uniquement les applications de partage de fichiers que vous utilisez à des fins professionnelles et uniquement pour les utilisateurs qui en ont besoin, et inspectez et journalisez le trafic. Dans la règle suivante de la base de règles de politique de sécurité, utilisez un filtre d'application basé sur la sous-catégorie **file-sharing (partage de fichiers)** pour bloquer toutes les applications de partage de fichiers que vous n'autorisez pas explicitement et délibérément. Surveillez la règle de blocage pour vous assurer qu'elle ne bloque pas les applications de partage de fichiers que vous souhaitez autoriser.

STEP 5 | Convertissez les règles générales basées sur des filtres d'application en règles étroites basées sur des groupes d'applications.

Les statistiques d'utilisation des règles montrent comment les règles sont utilisées dans votre environnement. Utilisez Policy Optimizer pour ajouter des applications aux groupes d'applications (PAN-OS 10.1 et versions ultérieures) ou ajoutez manuellement des applications aux groupes d'applications pour créer des règles plus strictes.

L'objectif final est d'autoriser uniquement les applications que vous approuvez au lieu d'autoriser un plus large éventail d'applications correspondant à un filtre d'application. Utilisez des filtres d'application pour découvrir des applications sur votre réseau et utilisez des groupes d'applications pour spécifier les applications exactes que vous souhaitez autoriser. Pour utiliser Policy Optimizer

afin de convertir des règles basées sur des filtres d'application en règles basées sur des groupes d'applications :

- Examinez les applications qui correspondent aux règles basées sur des filtres d'application et déterminez les applications que vous souhaitez autoriser.
- Pour chaque règle basée sur un filtre d'application, sélectionnez les applications à autoriser et ajoutez-les à un groupe d'applications dans une règle clonée ou existante.
- Après avoir déplacé les applications vers des règles basées sur des groupes d'applications, sélectionnez les règles basées sur des filtres d'application d'origine dans Policy Optimizer, puis appuyez sur **Reset Rule Hit Counter (Réinitialiser le Compteur d'accès à la règle)**. Cela réinitialise le compteur **Days with no new apps (Journées sans nouvelles applications)**. Ainsi, vous pouvez voir quand de nouvelles applications correspondent aux règles basées sur des filtres d'application.
- Surveillez les règles basées sur les filtres d'application pour voir quand le compteur **Days with no new apps (Journées sans nouvelles applications)** atteint un seuil indiquant qu'une règle ne voit plus de nouvelles applications. Le seuil dépend de votre environnement et des types d'applications auxquels le filtre d'application correspond. Tenez compte des applications utilisées uniquement à certaines périodes, comme les événements trimestriels ou annuels, et laissez le filtre en place suffisamment longtemps pour qu'il puisse voir ces applications. Si la règle de filtre d'application ne correspond à aucune application que vous souhaitez autoriser sur votre réseau, désactivez ou supprimez la règle, selon la politique de votre entreprise.

*Conservez la règle basée sur l'étiquette **App-ID Cloud Engine** au bas de la base de règles en tant que règle fourre-tout pour autoriser les nouvelles applications ACE. Une fois que vous êtes passé de règles basées sur des filtres d'application à des règles basées sur des groupes d'applications, tous les nouveaux App-ID ACE correspondent à la règle fourre-tout. Examinez périodiquement la règle pour déterminer les applications à ajouter aux règles et groupes d'applications existants, les applications qui nécessitent de nouvelles règles et les applications que vous souhaitez bloquer.*

STEP 6 | Consultez fréquemment la **New App Viewer (Nouvelle visionneuse d'applications)** pour obtenir une visibilité et un contrôle explicite sur les nouveaux App-ID ACE précédemment identifiés comme applications SSL ou de navigation web. Utilisez les nouveaux App-ID ACE explicitement dans la politique plutôt que comme applications SSL ou de navigation web.

Examinez les nouveaux App-ID ACE que le pare-feu télécharge régulièrement dans la nouvelle visionneuse d'applications de Policy Optimizer. Utilisez Policy Optimizer pour ajouter des applications à des groupes d'applications existants et nouveaux ou pour ajouter des applications directement à des règles de politique de sécurité existantes. Continuez à utiliser Policy Optimizer pour convertir les filtres d'application en groupes d'applications.

Meilleures pratiques en matière de recommandations de politiques

Les recommandations de politique SaaS et de politique IoT permettent aux administrateurs de SaaS Security et d'IoT Security de créer des recommandations de politique de sécurité et de les soumettre aux éléments suivants :

- Pare-feu PAN-OS et Panorama (recommandations de politique SaaS et IoT).
- Prisma Access géré par Panorama (recommandation de politique SaaS et IoT).
- Prisma Access géré dans le cloud (recommandation de politique SaaS uniquement).

Les services basés sur le cloud, tels que la recommandation de politique SaaS et IoT, ne peuvent pas être utilisés dans des environnements isolés, car ils nécessitent une connexion au cloud.

Dans les environnements isolés, pour IoT Security, envisagez d'utiliser Panorama comme moteur de gestion pour interagir avec le service cloud et recevoir des recommandations de politique. Envoyez ensuite les recommandations aux pare-feu gérés qui ne disposent pas d'une connectivité cloud. Cette solution ne s'applique qu'aux recommandations de politique elles-mêmes. Des fonctions telles que le mappage périphérique-IP nécessitent toujours une connectivité cloud pour les périphériques gérés.

La recommandation de politique SaaS contrôle les applications SaaS non approuvées dans PAN-OS et Prisma Access. La recommandation de politique IoT contrôle les périphériques réseau non gérés dans PAN-OS et Prisma Access géré par Panorama. Leurs flux de travail présentent de nombreuses similitudes.

Exigences :

- Recommandations en matière de politique SaaS :
  - Licence SaaS Security Inline

    La licence SaaS Security Inline inclut l'App-ID Cloud Engine (ACE), qui fournit des milliers d'ID d'application SaaS pour les recommandations de politique. La recommandation de politique SaaS nécessite le déploiement d'ACE.
  - PAN-OS version 10.1 ou ultérieure pour PAN-OS et Prisma Access géré par Panorama.
  - La prévention des pertes de données d'entreprise (Enterprise Data Loss Prevention, DLP) permet de mettre en œuvre les meilleures pratiques en matière de prévention des pertes de données et de gagner en visibilité sur les données.
  - Configurez Azure AD pour User-ID afin de spécifier les utilisateurs dans les recommandations de règles de politique (vous ne pouvez pas créer de règles de politique basées sur un utilisateur sans User-ID).
- Recommandations en matière de politique IoT :
  - Licence IoT Security.
  - Prérequis pour IoT Security.
  - Assurez-vous de la prise en charge correcte de PAN-OS et/ou de Prisma Access géré par Panorama.
  - Activez Device-ID dans chaque zone dans laquelle vous souhaitez contrôler les périphériques IoT. (Device-ID est à IoT Security ce que User-ID est à SaaS Security : Device-ID correspond au « qui » d'IoT Security.)

Panorama ne peut envoyer des recommandations de politique SaaS et IoT qu'aux pare-feu disposant des licences appropriées, de sorte qu'elles doivent être installées sur des pare-feu qui utilisent des recommandations de politique IoT et SaaS. Si les périphériques gérés ne disposent pas des licences appropriées, l'envoi échoue.

En plus des licences, pour fonctionner correctement et selon les meilleures pratiques, les recommandations de politiques IoT et SaaS nécessitent :

- Un certificat de périphérique valide sur chaque appareil qui utilise la recommandation de politique SaaS ou IoT.
- Une connexion à Cortex Data Lake (CDL) pour une visibilité sur le trafic.
- Un transfert des journaux vers CDL configuré dans chaque recommandation de règle de politique de sécurité. Pour la sécurité SaaS, transférez au minimum les journaux de trafic, les journaux de filtrage des URL et les journaux des menaces.

La recommandation de politique SaaS vous aide à contrôler les applications non approuvées.

Pour sécuriser les applications SaaS approuvées*, utilisez l'*API de sécurité SaaS*. L'API SaaS Security assure la sécurité des* applications SaaS prises en charge couramment approuvées *et vous permet de* gérer la politique de ces applications SaaS*.

- Concepts de recommandation en matière de politique— Des idées essentielles pour comprendre avant de recommander des politiques.
- Flux de travail de recommandation de politique— Des flux de travail SaaS et IoT et des meilleures pratiques en matière de flux de travail.

Concepts de recommandation en matière de politique

Les recommandations en matière de politique SaaS et IoT présentent de nombreuses similitudes dans leurs flux de travail et leurs objectifs. Les flux de travail et le processus de réflexion pour la recommandation de politique dans PAN-OS et Prisma Access présentent également de nombreuses similitudes. Passez en revue Meilleures pratiques en matière de règles de politique de sécurité pour mieux comprendre les meilleures pratiques concernant les composants des règles.

Prisma Access géré dans le cloud ne prend pas en charge la recommandation de politique IoT.

Les administrateurs de SaaS Security et d'IoT Security soumettent des recommandations de politique à PAN-OS et à Prisma Access. Les administrateurs de PAN-OS importent les recommandations de politique SaaS et les recommandations de politique IoT dans PAN-OS et Prisma Access géré par Panorama. Les administrateurs de Prisma Access géré dans le cloud importent les recommandations de politique SaaS dans la plateforme cloud. Différents administrateurs doivent souvent coopérer pour recommander et mettre en œuvre des règles de politique. Une bonne communication entre les administrateurs est donc essentielle.

Les meilleures pratiques générales en matière de recommandation de politique IoT sont les suivantes :

- Découvrez si les périphériques détectés appartiennent à votre réseau.
- Assurez-vous que les applications détectées que vous voyez pour les périphériques sont appropriées pour ces derniers.
- Comprenez les vulnérabilités des périphériques détectés.
- Prévoyez assez de temps pour qu'IoT Security collecte suffisamment de données sur les périphériques afin de les identifier avec un niveau de confiance élevé.

Les meilleures pratiques générales en matière de recommandation de politique SaaS sont les suivantes :

- Ayez connaissance des applications et des types d'applications qui doivent et ne doivent pas se trouver sur votre réseau. Créez une liste formelle des applications et des types d'applications approuvés, tolérés et non approuvés, et étiquetez les applications de manière appropriée au fur et à mesure que vous gagnez en visibilité sur celles-ci. Affichez les données d'utilisation des applications non approuvées et utilisez des filtres pour voir qui utilise les applications et comment elles sont utilisées. Utilisez les outils **Visibility (Visibilité)** pour afficher les applications détectées, puis étiquetez les applications détectées.
- Comprenez les données que vous souhaitez rechercher dans les fichiers afin de pouvoir créer des profils DLP appropriés pour les recommandations en matière de règles de politique.
- La plupart des recommandations en matière de règles de politique SaaS visent à bloquer le trafic. L'application du principe de l'accès à moindre privilège aux applications SaaS est plus complexe que de l'appliquer uniquement aux applications de contenu, car il y a des dizaines de milliers d'applications SaaS à contrôler. Si les recommandations en matière de politique SaaS sont trop strictes, elles risquent d'avoir un impact sur les applications métier. Assurez-vous de bien comprendre les applications et les types d'applications que vous avez l'intention de bloquer avant de les bloquer.

  Utilisez des filtres pour vous concentrer sur les catégories à haut risque telles que les applications de transfert de fichiers et de CMS, ainsi que pour vérifier quelles applications sont les plus utilisées. Concentrez-vous d'abord sur ces catégories et sous-catégories.
- Utilisez autant de composants contextuels que possible afin de créer des recommandations de politique d'accès à moindre privilège. Implémentez User-ID à l'aide de Cloud Identity Engine (CIE) (nécessite Azure AD) pour créer les exceptions d'accès nécessaires aux utilisateurs et aux groupes. Utilisez Enterprise DLP pour éviter la perte de données sensibles.
- Pour Prisma Access géré dans le cloud, si la politique d'administration de votre organisation le permet, ajoutez l'application SaaS Security à la console de gestion cloud. Utilisez la console de gestion cloud pour gérer les recommandations de politique SaaS (ainsi que SaaS Security et d'autres applications cloud) au lieu d'utiliser des applications autonomes pour bénéficier des avantages suivants :
  - Gérez tous les éléments de sécurité du cloud à partir d'une même interface plutôt que de différentes interfaces d'application.
  - Un administrateur peut effectuer toutes les actions de recommandation de politique SaaS, y compris l'ajout de la règle à la base de règles Prisma Access. Si vous gérez depuis l'application autonome, vous pouvez créer la recommandation de politique, mais vous devez passer à une autre application ou passer le relais à un autre administrateur pour ajouter la règle à Prisma Access.

  Pour utiliser SaaS Security et Enterprise DLP dans la console de gestion cloud, vous devez activer la sécurité Web dans la console. (Il s'agit d'une fonctionnalité gratuite, pas d'un abonnement.)

Vous pouvez créer des recommandations de politique SaaS à l'aide de recommandations de politique prédéfinies et en créant des recommandations de politique créées par l'utilisateur.

Flux de travail de recommandation de politique

Ce flux de travail est valide pour IoT Security ainsi que pour l'application SaaS Security (PAN-OS, Prisma Access géré par Panorama) et la console de gestion cloud (Prisma Access géré dans le cloud). Chaque étape indique quels administrateurs sont impliqués. Il est utile que chaque administrateur comprenne les responsabilités des autres administrateurs impliqués dans les recommandations de politique.

STEP 1 | (*Tous les administrateurs*) Créez des lignes de communication ouvertes entre les administrateurs qui administrent différentes parties de la recommandation de politique.

La recommandation de politique nécessite souvent que différents administrateurs travaillent ensemble pour recommander, importer et intégrer de nouvelles règles de politique SaaS Security et IoT Security dans la base de règles PAN-OS ou Prisma Access. Concevez un processus qui garantit une bonne communication lorsqu'un administrateur d'IoT Security or de SaaS Security transmet une recommandation de politique à un administrateur de Panorama, de pare-feu ou de Prisma Access. Le transfert se produit après qu'un administrateur d'IoT Security or de SaaS Security a créé une nouvelle règle, modifié une règle existante ou supprimé une règle et autorisé (envoi dans SaaS Security) ou activé (IoT Security) la règle.

Le flux de travail d'administration est le suivant :

1. Les **administrateurs de SaaS Security** créent de nouvelles recommandations de règles, ajoutent des applications, des utilisateurs / groupes d'utilisateurs et des profils DLP, puis définissent l'action. Ils examinent les recommandations de règles, puis les soumettent à PAN-OS, Prisma Access géré par Panorama ou Prisma Access géré dans le cloud. Consultez les directives relatives à la collaboration et à la création des administrateurs de SaaS Security.

   Les **administrateurs d'IoT Security** évaluent les recommandations de règles générées automatiquement, les modifient si nécessaire, créent des ensembles de politiques (groupes de recommandations de règles sur la base du trafic provenant de périphériques IoT dans le même profil de périphérique) et les soumettent à PAN-OS et à Prisma Access géré par Panorama.
2. Les **administrateurs de PAN-OS et de Prisma Access** importent les recommandations de politique SaaS et IoT. Ils évaluent les recommandations de règles, les importent et ajoutent des groupes de profils de sécurité et d'autres objets aux règles. Ils trient également les règles dans la base de règles de politique de sécurité. Lorsque Panorama envoie des recommandations de politique aux pare-feu et à Prisma Access, les administrateurs de pare-feu et de Prisma importent les règles recommandées.

   Les administrateurs doivent communiquer pour ajouter les objets appropriés aux règles recommandées et comprendre l'objectif de ces règles.

   Pour Prisma Access géré dans le cloud, le même administrateur peut gérer à la fois les recommandations de politique SaaS et les tâches de Prisma Access, en particulier si l'administrateur gère les deux applications sur la console de gestion cloud.
3. Les **administrateurs de SaaS Security et de IoT Security** mettent à jour ou suppriment une recommandation de règle, puis soumettent la modification à PAN-OS ou à Prisma Access.

   Les **administrateurs de PAN-OS et de Prisma Access** voient la mise à jour ou la suppression de la règle et importent la règle mise à jour ou suppriment la règle de PAN-OS ou de Prisma Access.

La communication entre les administrateurs est indispensable pour que toutes les parties comprennent l'objectif des règles recommandées, l'objectif des mises à jour de règles et la raison pour laquelle une règle est supprimée. La communication entre les administrateurs permet de s'assurer que les recommandations de politique SaaS et IoT ne restent pas dans PAN-OS ou Prisma Access en attente qu'un administrateur remarque leur présence et les importe dans la base de règles.

STEP 2 | (*Administrateur de SaaS Security et de IoT Security*) Les administrateurs de SaaS Security doivent évaluer les risques liés aux applications SaaS non approuvées et les administrateurs de IoT Security

doivent comprendre les profils de périphériques, qui décrivent les types de périphériques non gérés sur le réseau et leur comportement.

IoT Security apprend automatiquement les périphériques non gérés sur le réseau et crée un profil de périphérique pour chaque ensemble de périphériques similaires. Le profil décrit les caractéristiques des périphériques.

Familiarisez-vous avec les applications SaaS et les périphériques IoT sur votre réseau :

- SaaS : attendez au moins sept jours ouvrables de données avant d'analyser une application en vue d'une recommandation de politique. Rassemblez suffisamment de données pour comprendre l'application et son utilisation métier.

  IoT : surveillez la liste des profils de périphériques pour voir ceux qui sont éligibles à la recommandation de politique. Vous pouvez créer une recommandation de politique lorsque le niveau de confiance d'un profil de périphérique atteint 90 %, ce qui indique un niveau de confiance élevé quant au comportement du périphérique. Certains périphériques produisent moins de trafic et peuvent prendre du temps avant d'atteindre un niveau de confiance élevé. Laissez le temps à IoT Security de collecter suffisamment de données pour atteindre un taux de confiance de 90 %.
- SaaS : comprenez comment et pourquoi les utilisateurs utilisent des applications SaaS spécifiques et s'il existe des raisons commerciales d'autoriser ces applications.

  IoT : déterminez si les périphériques détectés appartiennent à votre réseau. Si votre entreprise effectue des opérations bancaires, la présence d'un périphérique médical sur votre réseau peut indiquer un problème.
- SaaS : évaluez les attributs de sécurité et de confidentialité, de gestion des identités et des accès et de conformité des applications SaaS en fonction de la tolérance au risque.

  IoT : dans les environnements médicaux, évaluez le risque de conformité des périphériques IoT médicaux.
- SaaS :étiquetez les applications approuvées, tolérées et non approuvées afin de les catégoriser.

STEP 3 | (*Administrateur de SaaS Security*) Configurez des recommandations de politique SaaS prédéfinies. (Les administrateurs d'IoT Security passent à l'étape 5.)

Les recommandations en matière de règles de politique SaaS prédéfinies bloquent l'accès aux applications, l'accès aux comptes personnels, ainsi que le partage et l'accès au contenu, et appliquent un accès en lecture seule aux utilisateurs appropriés. L'ajout d'applications à des recommandations prédéfinies est un moyen facile de commencer à verrouiller les applications SaaS.

Pour utiliser SaaS Security et Enterprise DLP dans la console de gestion cloud, vous devez activer la sécurité Web *dans la console. (Il s'agit d'une fonctionnalité gratuite.)*

Dans la console de gestion cloud, le même administrateur peut être en mesure de créer des recommandations de politique SaaS et de les importer dans Prisma Access*.*

1. Sélectionnez une règle prédéfinie. (**Discovered Apps (Applications détectées)** > **Policy Recommendations (Recommandations de politique)** dans la console de gestion cloud ou **Visibility (Visibilité)** > **Security Rules (Règles de sécurité)** dans la console de SaaS Security.)
2. Sélectionnez et ajoutez des applications à la règle. Si la règle ne s'applique pas à tous les utilisateurs, ajoutez des utilisateurs et des groupes d'utilisateurs. Assurez-vous de bien comprendre

les applications et les types d'applications que vous avez l'intention de bloquer avant de les bloquer, et de comprendre qui doit utiliser certaines applications à des fins professionnelles.

Concentrez-vous d'abord sur les types d'applications à risque, tels que les applications de partage de fichiers, de gestion de contenu, de collaboration et de productivité. Réduisez les téléchargements vers les sites de partage de fichiers afin que seuls les utilisateurs qui ont besoin de télécharger des fichiers à des fins professionnelles aient accès uniquement aux applications de partage de fichiers utilisées à des fins professionnelles.

3. Si vous disposez d'une licence Enterprise DLP (bonne pratique), ajoutez un profil DLP pour inspecter le trafic à la recherche d'informations sensibles et vous protéger contre les accès non autorisés, notamment les profils prédéfinis pour les applications DLP prises en charge.
4. Vérifiez que la règle fait ce que vous souhaitez qu'elle fasse de la manière dont vous souhaitez le faire.
5. **Save (Enregistrez)** la règle par défaut.
6. **Enable (Activez)** la règle pour la soumettre à PAN-OS ou à Prisma Access. Vous devez activer des règles pour que les administrateurs de PAN-OS ou de Prisma Access puissent les importer.

   Communiquez sur la ou les règles activées avec l'administrateur responsable de la vérification, de l'évaluation et de l'importation des recommandations de politique SaaS.

STEP 4 | (*Administrateur de SaaS Security*) Configurez des recommandations de politique SaaS définies par l'utilisateur. (Les administrateurs d'IoT Security passent à l'étape 5.)

Utilisez les filtres de la vue Applications détectées pour rechercher des applications et leurs métriques d'utilisation et pour vous aider à déterminer s'il faut bloquer ou autoriser une application. Concentrez-vous sur les catégories d'applications les plus à risque, telles que les applications de transfert de fichiers, de gestion de contenu, de collaboration et de productivité. Les applications à haut **Risk**

(Risque) qui ont également une **Usage (Utilisation)** élevée ont tendance à avoir le potentiel de risque le plus élevé. Sélectionnez des applications pour voir qui utilise l'application et comment ils l'utilisent.

Lorsque vous configurez des recommandations de politique et que vous les soumettez, PAN-OS et Prisma Access créent automatiquement les profils HIP, étiquettes et groupes d'applications *associés. Si vous disposez d'une licence Enterprise DLP sur les pare-feu cibles, le profil DLP est également créé (sinon, l'envoi échoue). L'envoi échoue si l'administrateur de SaaS Security ajoute d'autres types de profils à une recommandation de règle et que ces profils n'existent pas déjà sur le pare-feu. Si les objets de profil attachés existent sur le pare-feu, l'envoi réussit. (L'administrateur de PAN-OS ou de Prisma Access peut ajouter des profils aux recommandations de règles importées. Dans Prisma Access géré dans le cloud, vous ne pouvez ajouter que des groupes de profils, et non des profils individuels.)*

Les licences appropriées pour les profils doivent se trouver sur tous les pare-feu qui importent des recommandations de politique SaaS.

Les groupes d'utilisateurs de CIE sont cohérents dans l'ensemble de votre organisation. Si vous n'utilisez pas CIE ou si vous ne pouvez pas synchroniser depuis CIE, la configuration ***Users & Groups (Utilisateurs et groupes)*** *n'est pas disponible dans SaaS Security et vous ne pouvez pas baser les recommandations de politique SaaS sur les utilisateurs. La meilleure pratique consiste à utiliser CIE et à créer une politique d'application en fonction des personnes qui ont besoin d'accéder aux applications à des fins professionnelles.*

Pour appliquer SaaS Security et Enterprise DLP, vous devez activer la sécurité Web *dans la console de gestion cloud. (Il s'agit d'une fonctionnalité gratuite.)*

Dans la console de gestion cloud, le même administrateur peut être en mesure de créer des recommandations de politique SaaS et de les importer dans Prisma Access*.*

Pour configurer les recommandations en matière de politiques SaaS des meilleures pratiques :

1. Créez de nouvelles recommandations de politique de SaaS Security :
   - Console de SaaS Security : **Visibility (Visibilité)** > **Security Rules (Règles de sécurité)** > **Create New Rule (Créer une nouvelle règle)**
   - Console de gestion cloud : **Discovered Apps (Applications détectées)** > **Policy Recommendations (Recommandations de politique)** > **Add Policy (Ajouter une politique)**
2. Suivez les meilleures pratiques pour spécifier le Name (Nom) et la Description de la règle.
3. Ajoutez des applications à la règle.

   Utilisez les filtres de catégorie, de risque et de fonctionnalités pour rechercher des applications SaaS. Ajoutez des applications à la règle directement à partir des résultats du filtre. Concentrez-vous d'abord sur les applications les plus à risque et les plus utilisées.
4. Sélectionnez l'**User Activity (Activité utilisateur)** à détecter. Toutes les applications sélectionnées pour la règle doivent prendre en charge les activités utilisateur sélectionnées. Si une application ne prend pas en charge une activité, l'interface renvoie une erreur.

5. Configurez le reste des paramètres de la règle :
   - **Users & Groups (Utilisateurs et groupes)** : vous devez utiliser et synchroniser à partir de CIE afin de spécifier les utilisateurs et les groupes dans la recommandation de politique SaaS.
   - **Device Posture (Posture du périphérique)** : spécifiez les types de périphériques qui peuvent accéder aux applications de la règle. Lorsqu'une règle est importée dans PAN-OS ou Prisma Access, la posture du périphérique crée automatiquement un objet Host Information Profile (profil d'informations sur l'hôte - HIP) pour les périphériques mobiles.
   - **Data Profile (Profil de données)** : vous devez disposer d'une licence Enterprise DLP dans SaaS Security et sur des pare-feu ciblés pour utiliser cette fonctionnalité. Avec un abonnement Enterprise DLP, vous pouvez créer des règles pour un profil DLP spécifique et bloquer des applications uniquement si elles contiennent des données qui correspondent au profil.
   - **Response (Réponse)** :**Allow (Autoriser)** ou **Block (Bloquer)** le trafic qui correspond à la règle. La plupart des recommandations sont des règles de blocage qui permettent d'empêcher le surapprovisionnement de l'accès.
6. Vérifiez que la règle fait ce que vous souhaitez qu'elle fasse de la manière dont vous souhaitez le faire.
7. **Save (Enregistrez)** la règle.
8. **Enable (Activez)** la règle pour la soumettre à PAN-OS ou à Prisma Access. Vous devez activer des règles pour que les administrateurs de PAN-OS ou de Prisma Access puissent les importer.

   Communiquez sur la ou les règles activées avec l'administrateur de PAN-OS ou de Prisma Access qui est responsable de la vérification, de l'évaluation et de l'importation des recommandations de politique SaaS.

   La création de recommandations de règles de politique SaaS fournit davantage de détails sur le flux de travail.

STEP 5 | (*Administrateur d'IoT Security*) Configurez les recommandations de politique IoT (PAN-OS et Prisma Access géré par Panorama uniquement) dans l'application IoT Security.

IoT Security génère automatiquement des recommandations de politique IoT en fonction du comportement des périphériques qui appartiennent à un profil de périphérique lorsqu'IoT Security atteint un score de confiance (le niveau de confiance d' IoT Security dans l'identification d'un périphérique) de 90 % ou plus pour le profil. Le score de confiance augmente au fil du temps, à mesure qu'IoT Security recueille davantage d'informations sur les périphériques. Vous pouvez modifier les règles générées automatiquement avant de les soumettre à Panorama, aux pare-feu ou à Prisma Access.

IoT Security ne fournit pas de recommandations de politique pour les périphériques informatiques tels que les PC, les smartphones ou les tablettes, mais IoT Security identifie ces périphériques.

Utilisez les recommandations de politique automatiques pour créer des ensembles de règles de politique en fonction du comportement des périphériques IoT dans le même profil de périphérique sur plusieurs

locataires IoT Security. Un ensemble de règles de politique inclut les recommandations de règles de politique que vous sélectionnez pour contrôler les périphériques dans un profil de périphérique.

1. Créez de nouvelles recommandations de politique IoT Security de l'une des deux manières suivantes :
   - Accédez à la page Profiles (Profils), placez le curseur sur le nom d'un profil, puis cliquez sur **Create Policy Set (Créer un ensemble de politiques)** dans la fenêtre contextuelle.
   - **Profiles (Profils)** > **<profile-name>** > **Behaviors (Comportements)**, sélectionnez **Outbound Behaviors (Comportements sortants)**, sélectionnez **Create Policy (Créer une politique)**, puis cliquez sur **Next** (Suivant).
2. **Select Policies (Sélectionner des politiques)** affiche les recommandations de politique générées automatiquement pour le profil de périphérique sélectionné, y compris les applications utilisées par les périphériques.
   1. Assurez-vous que les applications que vous voyez dans la liste sont appropriées pour les périphériques. Par exemple, vous ne devriez pas voir l'application iTunes lorsque vous regardez des imprimantes ou des appareils photo. Si vous voyez des applications inattendues dans la liste, le périphérique est peut-être compromis.

      Connaissez vos périphériques et vos profils de périphériques afin de pouvoir créer des recommandations appropriées pour les régir.
   2. Vérifiez les **Alerts Raised (Alertes déclenchées)**. Examinez les applications avec un nombre élevé d'alertes avant de les ajouter à l'ensemble de politiques, en particulier si les alertes sont de gravité élevée ou critique.
   3. Sélectionnez les politiques que vous souhaitez appliquer aux périphériques. Ces politiques sont incluses dans l'ensemble de politiques pour le profil de périphérique.

      Si vous ne voyez pas d'application que vous souhaitez inclure dans l'ensemble de politiques, **Add Rule (Ajoutez une règle)** pour sélectionner manuellement une application et un type de destination, puis **Create (Créez)** la règle.
   4. Par défaut, la règle s'applique à toutes les destinations (**Any (Toutes)**) détectées dans le trafic pour le profil de périphérique. Si vous souhaitez restreindre les destinations d'une application, cliquez sur **Destination** > **Any (Toutes)**, désactivez l'option **Allow any destination (Autoriser n'importe quelle destination)**, puis décochez les destinations que vous ne souhaitez pas autoriser dans la liste.
   5. Lorsque vous êtes convaincu que l'ensemble de politiques contient les règles souhaitées, sélectionnez **Next (Suivant)**.
3. Dans **Firewall Configuration (Configuration de pare-feu)** > **Policy configurations (Configurations de politique)**, modifiez les recommandations générées automatiquement selon vos besoins. **Policy configurations (Configurations de politique)** affiche les applications sélectionnées.
   - Suivez les meilleures pratiques pour spécifier le Name (Nom) et la Description de l'ensemble de politiques. Assurez-vous que le nom identifie l'action de la règle et que la description indique l'objectif de la règle.
   - Laissez **Services** réglé sur **application-default** pour empêcher les applications d'utiliser des ports non standard, ce qui indique un comportement évasif et potentiellement malveillant.

- Ajoutez des profils de sécurité et des groupes de profils de sécurité, des profils de transfert des journaux et d'autres objets dans Panorama ou sur des pare-feu, et non dans l'application IoT Security.

4. Passez en revue l'ensemble de politiques. Lorsque vous êtes sûr qu'il est configuré comme vous le souhaitez, appuyez sur **Create (Créer)** pour créer l'ensemble de politiques et l'enregistrer.
5. Cliquez sur **Activate Policy Set (Activer l'ensemble de politiques)** pour que la recommandation de règles de politique puisse être importée sur Panorama et des pare-feu individuels.

   Communiquez sur la ou les règles activées avec l'administrateur de PAN-OS ou de Prisma Access qui est responsable de la vérification, de l'évaluation et de l'importation des recommandations de politique IoT.

L'option Create an IoT Policy Set (Créer un ensemble de politiques IoT) *fournit davantage de détails sur le flux de travail.*

STEP 6 | (Administrateurs de Panorama et de pare-feu) (Administrateur de Prisma Access géré dans le cloud pour SaaS Security uniquement) Évaluez, importez et, si nécessaire, modifiez les recommandations de règles de politique.

Étant donné que la console de gestion cloud permet de gérer toutes les applications cloud en un seul endroit, l'administrateur de Prisma Access géré dans le cloud peut être le même administrateur que celui qui a créé les recommandations de politique de sécurité SaaS.

Avant d'importer des règles :

- Créez des groupes de profils de sécurité sur Panorama, les pare-feu et/ou la console de gestion cloud que vous pouvez appliquer aux recommandations de politique de SaaS Security et d'IoT Security importées. À tout le moins, créez des groupes de profils qui alertent sur la plupart du trafic et bloquent le trafic malveillant connu afin de maintenir la disponibilité. Au fur et à mesure que vous comprenez mieux les recommandations de politique au fil du temps, suivez les meilleures pratiques en matière de profil de sécurité pour rendre les groupes de profils aussi stricts que possible sans mettre en danger la capacité d'accéder aux applications et aux périphériques critiques de l'entreprise.

  Pour les groupes de profils SaaS, connaissez les types d'applications et comprenez qui utilise les applications afin de déterminer les profils à utiliser et leur degré de rigueur dès le début.

  Pour les groupes de profils IoT, connaissez vos périphériques et vos profils de périphériques afin de pouvoir créer des groupes de profils de sécurité appropriés pour les gouverner. Comprenez ce que signifie l'application dans la règle afin de pouvoir appliquer les profils de sécurité appropriés au groupe.

  Lorsque vous créez des groupes de profils de sécurité, consultez l'administrateur d'IoT Security et/ou de SaaS Security pour vous assurer que les groupes de profils de sécurité ont un sens pour les recommandations de politique IoT et SaaS.
- Dans les déploiements d'IoT Security, activez Device-ID dans chaque zone dans laquelle vous souhaitez contrôler les périphériques IoT. Device-ID est aux périphériques IoT ce que User-ID est aux utilisateurs et App-ID est aux applications : un identifiant unique. Dans les zones où Device-ID n'est pas activé, vous ne pouvez pas appliquer la politique de sécurité sur les périphériques IoT.

- La recommandation de politique SaaS nécessite l'App-ID Cloud Engine (ACE), qui identifie des dizaines de milliers d'applications SaaS afin que vous puissiez créer une politique de sécurité pour les contrôler. ACE nécessite le transfert de journaux vers Cortex Data Lake. Suivez les meilleures pratiques en matière de transfert de journaux lorsque vous créez le profil CDL.

  Si vous utilisez des App-ID ACE dans une règle de politique de sécurité, même si la règle ne s'applique qu'à un seul utilisateur ou groupe d'utilisateurs, le pare-feu applique l'App-ID ACE à tous les utilisateurs. (Une fois que vous utilisez l'App-ID ACE dans la politique, le pare-feu applique l'App-ID de la même manière qu'il applique les App-ID fournis par le contenu.)

Pour importer des recommandations de politique SaaS et IoT :

1. Vérifiez régulièrement les règles importées. Actualisez la page de recommandation de politique IoT ou SaaS pour vous assurer que vous voyez les dernières recommandations de politique :
   - Panorama : **Panorama** > **Policy Recommendation (Recommandation de politique)** > **SaaS** ou **Panorama** > **Policy Recommendation (Recommandation de politique)** > **IoT**.
   - Pare-feu : **Device (Périphérique)** > **Policy Recommendation (Recommandation de politique)** > **SaaS** ou **Device (Périphérique)** > **Policy Recommendation (Recommandation de politique)** > **IoT**.
   - Prisma Access géré dans le cloud (recommandation de politique SaaS uniquement) : Sélectionnez **Policy Recommendation (Recommandation de politique)** > **Manage (Gérer)** > **Web Security (Sécurité Web)** > **Web Access Policy (Politique d'accès Web)**, puis sélectionnez l'onglet **Policy Recommendations (Recommandations de politique)** pour afficher les **New SaaS Rule Recommendations (Nouvelles recommandations de règles SaaS)**.
2. Sélectionnez et évaluez de nouvelles règles. Assurez-vous que tous les objets, adresses, etc., de la règle importée ont un sens. Si vous n'êtes pas sûr d'un élément de la recommandation, contactez l'administrateur d'IoT Security ou de SaaS Security pour vous assurer que vous comprenez l'objectif de la règle et de ses composants.

   Pour les recommandations de règles de politique SaaS, assurez-vous que l'accès des utilisateurs aux applications n'est pas trop vaste.

3. Le processus d'importation de règles vous permet de modifier la règle et de la positionner dans la base de règles de politique de sécurité. Sélectionnez une ou plusieurs règles à importer, puis procédez comme suit :

   - Pare-feu Panorama et PAN-OS : **Import Policy Rule (Importer la règle de politique)**.

     Vous pouvez importer jusqu'à dix règles de politique IoT à la fois.

   - Prisma Access géré dans le cloud (recommandation de politique SaaS uniquement) : **Actions** > **Import (Importer)**.

     Ne terminez pas l'importation de la règle tant que vous n'avez pas effectué les étapes suivantes pour ajouter des profils de sécurité et de transfert de journaux, évaluer la règle et sélectionner son ordre dans la base de règles de politique de sécurité.

   Lorsque vous importez une règle, PAN-OS et Prisma Access créent automatiquement certains des objets de la règle dans la règle de politique :

   - L'importation de recommandations de politique IoT crée automatiquement l'objet Device (Périphérique), y compris les mappages périphérique-IP, en fonction du profil de périphérique IoT.

     Une fois que Panorama a importé l'objet Device (Périphérique) et l'a envoyé aux pare-feu gérés, ceux-ci extraient le mappage périphérique-IP directement à partir du cloud. Panorama n'est pas impliqué dans l'actualisation du mappage périphérique-IP.

   - L'importation de recommandations de politique SaaS crée automatiquement tous les profils HIP, étiquettes et groupes d'applications requis. Pour les profils Enterprise DLP, les périphériques cibles doivent disposer d'une licence Enterprise DLP. Tous les autres profils ne peuvent être importés que s'ils existent déjà sur le périphérique cible.

4. Ajoutez un groupe de profils de sécurité à chaque règle.

   L'utilisation de groupes de profils au lieu de profils individuels est plus rapide, plus facile et évite d'omettre accidentellement un profil d'une règle. Cela vous permet également de commencer avec un groupe de profils qui alerte principalement et de le remplacer facilement par un groupe

de profils plus strict à mesure que vous acquérez de l'expérience avec les applications SaaS et les périphériques IoT.

L'application de profils à des règles d'application SaaS et de périphérique IoT diffère :

- **Recommandations relatives aux règles de politique de SaaS Security** :
  - PAN-OS et Prisma Access géré par Panorama : appliquez des profils de meilleures pratiques de prévention avancée des menaces et de filtrage des URL avancé au trafic des applications SaaS.
  - Prisma Access géré dans le cloud : vous pouvez appliquer des groupes de profils de sécurité aux recommandations de politique, mais pas des profils de sécurité individuels. Ajoutez des profils de sécurité à un groupe de profils et appliquez le groupe à une règle.

    Les recommandations de profils de sécurité des meilleures pratiques pour Prisma Access géré dans le cloud diffèrent légèrement des recommandations pour PAN-OS et Prisma Access géré par Panorama.
- **Recommandations relatives aux règles de politique d'IoT Security** : pour éviter les comportements malveillants, assurez-vous que les profils de sécurité sont appropriés pour le périphérique. Collaborez avec l'administrateur d'IoT Security pour comprendre le comportement et les alertes des différents périphériques affichés dans les profils de périphériques. Appliquez des profils aux recommandations de politique IoT en fonction du comportement et des alertes. Recherchez les faiblesses courantes des périphériques IoT, telles que la faiblesse des informations d'identification du fabricant, les connexions à des URL à risque, l'obsolescence des antivirus, l'accès à des périphériques malveillants, les protocoles non sécurisés et les systèmes d'exploitation en fin de vie, ainsi que les périphériques qui ne sont pas corrigés ou qui ne peuvent pas être corrigés.
  - Appliquez des profils de protection contre les vulnérabilités et des profils antispyware (pour empêcher les logiciels malveillants de commande et de contrôle) à tous les périphériques.
  - Si un périphérique a du trafic sortant vers Internet, en particulier vers des destinations inconnues, appliquez le filtrage des URL avancé et la prévention avancée des menaces. Si le périphérique peut envoyer des fichiers, ajoutez des profils Advanced WildFire et Blocage de fichiers.

- Si le périphérique dispose de ports serveur et accepte les connexions entrantes, appliquez la protection DoS en plus des profils Blocage de fichiers, Advanced WildFire et Prévention avancée des menaces.

5. Ajoutez un profil de transfert de journaux à chaque règle.

   - Pour les recommandations de politique IoT, ajoutez le profil de transfert de journaux prédéfini **IoT Security Default Profile - EAL Enabled** qui fournit tous les types de journaux requis par IoT Security, y compris les journaux d'application améliorés.
   - La recommandation de politique SaaS exige qu'ACE identifie les applications SaaS. ACE nécessite le transfert de journaux vers CDL, de sorte que les règles de politique de sécurité basées sur les applications SaaS nécessitent également le transfert de journaux vers CDL.

   > *Une fois que vous avez importé des règles, vous pouvez appliquer des profils de transfert de journaux à plusieurs règles à la fois à l'aide des **Log Forwarding for Security Services (Transfert de journaux pour les services de sécurité)** dans Policy Optimizer (Optimiseur de politique) afin d'identifier les règles de politique de sécurité qui n'ont pas de profil de transfert de journaux attaché (sélectionnez **None (Aucun)** dans le filtre).*

6. Dans Panorama et Prisma Access géré dans le cloud, indiquez s'il s'agit d'une règle « avant » ou d'une règle « après ». (Ne s'applique pas aux pare-feu autonomes.)

   L'ordre de priorité pour l'évaluation des règles est règles « avant », puis règles spécifiques au déploiement, puis règles « après ». Les règles « avant » et les règles « après » de Prisma Access géré dans le cloud résident dans le dossier de configuration partagé. Les règles « avant » et les règles « après » de Panorama résident dans **Policies (Politiques)** > **Security (Sécurité)**. Dans Panorama, vous pouvez spécifier des groupes de périphériques pour la règle.

7. Sélectionnez la règle que vous souhaitez appliquer à la règle importée dans la base de règles de politique de sécurité. Suivez les meilleures pratiques en matière de base de règles.

   > *Ne choisissez pas **No Rule Selection (Aucune sélection de règle)**, ce qui place la règle en haut de la base de règles de politique de sécurité. Le haut de la base de règles n'est souvent pas le bon endroit pour une nouvelle règle. Par exemple, une nouvelle règle d'autorisation ne sera pas soumise à des règles critiques qui bloquent le trafic malveillant connu. Une nouvelle règle de blocage peut bloquer l'accès des utilisateurs légitimes si elle n'est pas placée après une règle d'autorisation pour les utilisateurs légitimes de l'application. Classez chaque règle de manière appropriée dans la base de règles.*

8. Vérifiez la règle et si vous en êtes satisfait, importez-la.

   - **Prisma Access géré dans le cloud—Import (Importer)**.
   - **Pare-feu autonomes et Panorama—OK**.

     Après avoir importé les règles, les administrateurs de Panorama doivent les envoyer aux pare-feu gérés et les administrateurs de pare-feu doivent les importer avant qu'elles ne deviennent actives sur le pare-feu. Actualisez **Device (Périphérique)** > **Policy Recommendation**

(Recommandation de politique) > **IoT** ou **Device (Périphérique)** > **Policy Recommendation (Recommandation de politique)** > **SaaS** pour afficher les recommandations les plus récentes.

Les administrateurs de pare-feu peuvent avoir besoin de modifier les règles après les avoir importées. Les administrateurs de pare-feu doivent vérifier auprès des administrateurs de Panorama, SaaS Security ou IoT Security s'ils ne sont pas sûrs de l'objectif de la règle.

Vérifiez la base de règles de politique de sécurité pour vous assurer que la règle est dans le bon ordre.

9. (IoT Security uniquement) Après avoir importé la règle, affichez le **Device Object (Objet de périphérique)** pour vérifier les filtres d'attribut du périphérique.

   Utilisez les attributs de périphérique IoT dans la politique de sécurité pour mieux identifier les périphériques. L'importation d'une règle de politique IoT importe automatiquement les attributs associés au périphérique et crée son Device-ID. Le Device-ID est aux périphériques IoT ce que l'User-ID est aux personnes. Bien qu'il existe six attributs de périphérique, les pare-feu ne reçoivent souvent qu'un seul attribut d'un périphérique. Si l'objet Device (**Objects (Objets)** > **Devices (Périphérique)**) spécifie des attributs que le périphérique n'envoie pas au pare-feu, le trafic ne correspond pas au périphérique et la règle ne contrôle pas le périphérique, alors spécifiez uniquement les attributs que les périphériques envoient au pare-feu.

   

   *Cliquez sur le **Device-ID** dans la règle pour afficher l'objet de périphérique associé.*

   Exécutez la commande CLI **`show iot ip-device-mapping-mp all`** ou **`show iot ip-device-mapping-mp ip <IP-address>`** pour vérifier que le pare-feu reçoit les attributs importés avec la règle. Si le pare-feu ne reçoit pas d'attribut configuré dans l'objet de périphérique, supprimez l'attribut de l'objet de périphérique.

Pour connaître les procédures de configuration détaillées, reportez-vous au Guide de l'administrateur approprié :

- **IoT Security** :
  - Procédure d'importation
  - Importation d'un ensemble de politiques dans Panorama
  - Configuration de Device-ID
- **SaaS Security** :
  - Prisma Access géré par Panorama et PAN-OS :importation de recommandations de politique SaaS (pour les pare-feu autonomes ; sur Panorama, vous spécifiez également si la règle importée est une règle « avant » ou une règle « après » et vous transmettez la règle aux pare-feu après l'avoir importée dans Panorama.)
  - Prisma Access géré dans le cloud : affichez les recommandations de politique SaaS, importez de nouvelles recommandations de politique SaaS.

STEP 7 | (Tous les administrateurs) Mettez à jour et supprimez les recommandations de politique si nécessaire pour maintenir la base de règles de politique de sécurité à jour.

L'importation de recommandations de politique est un processus continu. Les administrateurs recommandent de nouvelles règles, modifient des règles et suppriment les anciennes. Le nombre de périphériques IoT augmente et les postures des périphériques changent au fil du temps. Le nombre

d’applications SaaS augmente et les applications que votre entreprise marque comme approuvées, tolérées et non approuvées changent avec le temps. Créez des listes de contrôle d’éléments quotidiens, hebdomadaires et mensuels afin de surveiller et de maintenir la visibilité sur les périphériques IoT et les applications SaaS.

Procédures d’importation des recommandations de politique mises à jour :

- IoT Security : Les recommandations relatives aux règles de modification et de mise à jour de la politique IoT incluent à la fois les étapes IoT Security et PAN-OS.
- SaaS Security :
  - SaaS Security Inline :modifier les recommandations de règles de politique SaaS actives montre comment modifier une règle existante dans SaaS Security.
  - Prisma Access géré dans le cloud :mettez à jour les recommandations de règles de politique SaaS importées sur Prisma Access géré dans le cloud.

    Si le même administrateur est à la fois l’administrateur de la recommandation de politique SaaS et l’administrateur de Prisma Access, vous pouvez activer les mises à jour automatiques pour appliquer automatiquement les modifications de recommandation de règle.
  - Prisma Access géré par Panorama et PAN-OS : Importer la recommandation de politique SaaS mise à jour montre comment rechercher et importer des recommandations de politique de SaaS Security mises à jour.

Procédures de suppression des recommandations de politique supprimées :

- IoT : Les recommandations relatives aux règles de suppression et de retrait de politique incluent à la fois les étapes d’IoT Security et de PAN-OS.
- SaaS Security :
  - SaaS Security Inline :supprimer les recommandations de règles de politique SaaS montre comment supprimer une règle existante dans SaaS Security.
  - Prisma Access géré dans le cloud :retirer les recommandations de règles de politique SaaS supprimées sur Prisma Access géré dans le cloud.
  - Prisma Access géré par Panorama et PAN-OS :retirer la recommandation de politique SaaS supprimée.

Maintenance des meilleures pratiques en matière de politique de sécurité

Une fois que vous avez planifié et déployé les meilleures pratiques en matière de politique de sécurité, réalisez la maintenance de votre déploiement de meilleures pratiques au fur et à mesure que votre réseau et ses applications, ses utilisateurs, ses périphériques et son infrastructure évoluent.

STEP 1 | Maintenez tous les abonnements de sécurité à jour pour éviter les lacunes dans la couverture.

STEP 2 | Tenez-vous au courant des mises à jour du contenu de menace et des applications et suivez les meilleures pratiques pour les mises à jour du contenu de menace et des applications.

STEP 3 | Consultez les notes de version pour connaître les dernières fonctionnalités, les modifications apportées au comportement par défaut, les problèmes, etc.

STEP 4 | Créez des listes de contrôle de maintenance quotidiennes, hebdomadaires et mensuelles (et pour toute autre période dont vous avez besoin).

La maintenance du déploiement des politiques de sécurité est une tâche récursive, car de nouvelles applications, de nouveaux utilisateurs et de nouveaux périphériques IoT sont continuellement ajoutés et supprimés de votre environnement au fil du temps. Par exemple, les listes de contrôle peuvent inclure :

- L'évaluation des mises à jour du contenu de menace et des applications.
- L'utilisation de Policy Optimizer pour la gestion des applications.
- L'examen des recommandations et des mises à jour relatives aux politiques IoT et SaaS. Au fil du temps, la posture des appareils IoT peut évoluer et les applications SaaS utilisées peuvent changer ou devoir être traitées différemment et nécessiter une mise à jour. Maintenez à jour les étiquettes approuvées/tolérées/non approuvées pour les applications.
- La définition des heures d'exécution des outils d'analyse de la posture de sécurité.
- L'examen des changements de comportement et des problèmes documentés dans les notes de version.
- Le passage en revue les règles de politique de sécurité pour voir si vous pouvez les renforcer ou si elles ne sont plus nécessaires.

STEP 5 | Réalisez la maintenance d'App-ID dans la politique de sécurité :

- Passez en revue les App-ID fournis par le contenu nouveaux et modifiés et ajustez les règles si nécessaire.
- Au fur et à mesure que vous ajoutez de nouvelles applications à votre réseau, incluez-les dans des règles de politiques spécifiques et granulaires. Utilisez des étiquettes et des filtres d'application pour automatiser l'ajout d'applications approuvées, y compris les nouvelles applications App-ID Cloud Engine, aux règles.
- Lorsque votre entreprise cesse d'utiliser une application, supprimez cette dernière des règles d'autorisation afin d'empêcher toute utilisation non autorisée.
- Examinez régulièrement les applications autorisées par vos règles de politique de sécurité.

STEP 6 | Réalisez la maintenance de User-ID dans la politique de sécurité :

- Au fur et à mesure que vous ajoutez de nouveaux utilisateurs à votre réseau, ajoutez-les aux groupes d'utilisateurs appropriés pour contrôler leur accès et les inclure dans la politique, ou ajoutez-les directement aux règles s'ils n'appartiennent à aucun groupe.
- Lorsque les utilisateurs quittent l'entreprise ou que leur contrat prend fin, supprimez-les des groupes d'utilisateurs pour empêcher l'accès. Supprimez des personnes des règles si elles n'ont pas été ajoutées dans le cadre d'un groupe.
- Continuez à suivre les meilleures pratiques pour le mappage de groupe d'utilisateurs et les meilleures pratiques pour les groupes d'utilisateurs dynamiques (DUG) lorsque vous ajoutez et supprimez des utilisateurs de groupes et de règles de politique.

STEP 7 | Effectuez la maintenance des profils de sécurité et des groupes de profils et mettez-les à jour au fur et à mesure de l'évolution de votre réseau et de vos objectifs. Lorsque vous ajoutez de nouvelles règles d'autorisation, assurez-vous qu'elles sont associées aux profils de sécurité appropriés.

STEP 8 | Mettez à jour le transfert des journaux selon vos besoins pour les nouvelles règles et applications :

- Appliquez un profil de transfert des journaux approprié à chaque nouvelle règle de politique de sécurité ou utilisez un profil de transfert des journaux par défaut pour appliquer automatiquement un profil de transfert des journaux aux nouvelles règles. Si vous utilisez un profil par défaut, vérifiez la règle pour vous assurer qu'il est approprié et, si ce n'est pas le cas, remplacez-le par un profil approprié.
- Passez régulièrement en revue ce que vous journalisez ou non, ainsi que la méthode de journalisation. Assurez-vous que vous journalisez le trafic et toutes les informations que vous souhaitez journaliser pour les opérations du centre des opérations de sécurité (SOC).
- Mettez à jour les profils de transfert des journaux au fur et à mesure que les administrateurs rejoignent et quittent l'entreprise.
- Au fur et à mesure que de nouvelles applications entrent sur votre réseau, mettez à jour le transfert des journaux pour les prendre en charge.

STEP 9 | Utilisez des outils d'analyse de la posture de sécurité pour vérifier le déploiement de vos meilleures pratiques :

- Dans PAN-OS et Prisma Access, utilisez Strata Cloud Manager pour vérifier la politique de sécurité au fur et à mesure que vous la créez.
- Exécutez régulièrement l'évaluation des meilleures pratiques (BPA) à la demande de Strata Cloud Manager pour mesurer les progrès vers un déploiement des meilleures pratiques.
- Exécutez l'examen du cycle de vie de la sécurité (SLR) tous les trimestres pour obtenir une meilleure visibilité sur votre réseau.

STEP 10 | Utilisez des outils de pare-feu pour vérifier l'activité et ajuster la politique de sécurité si nécessaire.

- Utilisez les informations des journaux dans PAN-OS (s'applique également à Panorama Managed Prisma Access) et Cloud Managed Prisma Access pour examiner et surveiller le trafic.
- Utilisez le Centre de commande des applications pour afficher des résumés graphiques des applications, des utilisateurs, des menaces, des URL et du contenu qui traversent votre réseau.
- Utilisez les rapports App-Scope pour comprendre les changements dans l'utilisation des applications et l'activité des utilisateurs, l'utilisation de la bande passante et les menaces réseau.
- Créez des rapports personnalisés pour afficher les données exactes que vous souhaitez examiner.

STEP 11 | Consultez régulièrement Policy Optimizer pour examiner la base de règles et rechercher et corriger les règles inutilisées, les règles surapprovisionnées et les règles avec des applications inutilisées. Ajoutez la vérification de Policy Optimizer à votre maintenance régulière.

STEP 12 | Utilisez les outils et services SecOps pour surveiller l'ensemble de votre posture de sécurité de manière proactive, aider à prévenir les menaces et enquêter sur les problèmes :

- Cortex XSIAM associe l'analyse SOC pour une surveillance proactive à des capacités SIEM.
- Cortex XSOAR est une solution complète pour l'orchestration et l'automatisation de la sécurité et la réponse aux incidents de sécurité (y compris des playbooks de réponse) pour une gestion complète des renseignements sur les menaces et une collaboration en temps réel.
- Cortex XDR fournit une plateforme de détection et de réponse étendue qui surveille et gère les événements et les données du cloud, du réseau et des terminaux.
- Services SOC tels que l'évaluation de la posture de prévention SecOps, l'optimisation et des ateliers d'apprentissage.

STEP 13 | Les ressources suivantes fournissent plus d'informations sur les plateformes, les fonctionnalités et l'assistance de Palo Alto Networks :

- Le portail de documentation sur les meilleures pratiques de sécurité contient des livres autonomes portant notamment sur les meilleures pratiques de sécurité IoT, les meilleures pratiques d'accès administratif et les meilleures pratiques de décryptage, ainsi que des liens vers des rubriques sur les meilleures pratiques dans divers guides de l'administrateur.

- Guides de l’administrateur :
  - Guide de l’administrateur PAN-OS
  - Guide de l’administrateur Prisma Access (Panorama Managed et Cloud Managed Prisma Access)
  - Guide de l’administrateur de sécurité SaaS
  - Guide de l’administrateur de sécurité IoT
- Portails de documentation :
  - Portail de documentation sur les services de sécurité fournis par le cloud (CDSS)
  - Portail de documentation sur Cloud Identity Engine (CIE)
  - Portail de documentation sur GlobalProtect
  - Portail de support client de Palo Alto Networks
- Surveillance du déploiement de sécurité IoT à l’aide des meilleures pratiques
- Structure de la solution IoT Security (résumé du fonctionnement de la solution IoT Security)
- Sécurité SaaS sur Prisma Access (Panorama Managed et Cloud Managed)
- Résolution des problèmes sur SaaS Security Inline

