Meilleures pratiques pour l'implémentation du Zero Trust avec Palo Alto Networks

9.1

docs.paloaltonetworks.com

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

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

Copyright

Last Revised

December 18, 2019

Table of Contents

Meilleures pratiques du Zero Trust

Ce document décrit ce qu'est une stratégie Zero Trust et explique comment l'implémenter dans votre réseau à l'aide d'une méthodologie en cinq étapes vous guidant à travers les meilleures pratiques pour vous aider à identifier vos surfaces à protéger cruciales, à mapper vos flux de transaction essentiels, à développer votre réseau Zero Trust, à créer une politique Zero Trust et à en maintenir le déploiement. Les sections comprennent des liens vers des informations détaillées de Palo Alto Networks, notamment concernant la manière de configurer les pare-feu nouvelle génération (physiques et virtuels) et les fonctionnalités de sécurité de Palo Alto Networks afin de prévenir toute violation de données.

Qu’est-ce que le Zero Trust et pourquoi en ai-je besoin ?

Le Zero Trust est une approche stratégique axée sur l’entreprise permettant de sécuriser vos données, vos applications, vos actifs et vos services (DAAS) les plus essentiels, mais également vos utilisateurs, en regroupant les éléments les plus précieux de votre entreprise dans une *surface à protéger*. Une stratégie Zero Trust ne dépend pas de l’infrastructure, vous pouvez donc l’appliquer sur tous vos emplacements physiques et virtuels, comme votre réseau, votre cloud public et privé et vos terminaux. Derrière le Zero Trust se cache un concept simple : la confiance est une vulnérabilité. Dans un environnement numérique, vous ne pouvez faire confiance à quoi que ce soit, qu’il s’agisse de paquets, d’identités, de périphériques ou de services. Vous devez tout vérifier. Dans ce domaine, la confiance aveugle est tout sauf bénéfique.

Il n’existe pas de manière précise et définitive d’implémenter cette stratégie sur n’importe quel réseau, car tout dépend des spécificités de chaque environnement et de chaque surface à protéger. De plus, les objectifs de cette stratégie et les éléments DAAS changent au fur et à mesure que les entreprises évoluent. La stratégie Zero Trust varie d’une entreprise à l’autre et la stratégie de sécurité dépend des éléments que votre entreprise cherche à protéger.

L’objectif de la stratégie Zero Trust est d’éliminer la confiance de votre réseau. Ce faisant, vous pourrez empêcher plus efficacement toute violation de données, faciliter les opérations au moyen d’automatismes et d’une base de règles réduite, et simplifier le processus de conformité réglementaire et les audits, car telle est la nature des environnements Zero Trust.

Une vision axée sur le Zero Trust

En comprenant le principe du Zero Trust, vous découvrirez la véritable nature de la confiance : une vulnérabilité exploitée par les pirates. Ces derniers peuvent voler les informations d'identification, usurper les informations des en-têtes de paquet et même être des employés ou partenaires « approuvés ». Edward Snowden, par exemple, était un utilisateur approuvé qui disposait du bon logiciel antivirus et du niveau de correctif adéquat sur son poste de travail. Il utilisait également l'authentification multifacteur. Cependant, personne ne se souciait des parties du réseau qu'il visitait ou des paquets qu'il générait parce qu'il était un utilisateur approuvé. Il pouvait donc explorer le réseau à sa guise pour y trouver et en exfiltrer des données sensibles. La morale de cette histoire est que la confiance numérique mène à la trahison numérique. Par conséquent, ne faites jamais confiance aux identités, aux applications ou aux données. En adoptant un point de vue axé sur le Zero Trust :

- vous alignez votre sécurité sur vos fonctions d'entreprise, car ces dernières déterminent ce que vous devez protéger ;
- vous inspectez et journalisez tous les paquets au niveau de la couche 7 lorsqu'ils accèdent à une ressource ;
- vous accédez à toutes les ressources de manière sécurisées, peu importe leur emplacement ;
- vous appliquez une politique de sécurité cohérente sur tous vos emplacements ;
- vous gérez votre politique de sécurité et de segmentation de manière centralisée ;
- vous prenez en compte les modifications liées à l'évolution de votre entreprise.

La confiance représente un point de défaillance que vous pouvez éliminer en implémentant une stratégie Zero Trust.

- Meilleures pratiques de haut niveau en matière de Zero Trust
- Comment commencer l'implémentation du Zero Trust ?

Meilleures pratiques de haut niveau en matière de Zero Trust

Les meilleures pratiques ci-dessous ont été conçues pour vous aider à préparer et à effectuer la transition de votre réseau vers une architecture Zero Trust :

- Définissez vos résultats métier recherchés avant de développer votre environnement Zero Trust. Le modèle Zero Trust appuie et facilite les fonctions d'entreprise sécurisées.
- Concevez votre architecture de l'intérieur, et non de l'extérieur, afin de protéger en priorité les éléments les plus essentiels à votre entreprise. Vos actifs les plus précieux sont plus susceptibles de se trouver dans votre centre de données que dans votre périmètre.
- Utilisez une plateforme intégrée et gérée de manière centralisée permettant de réduire le coût total de possession plutôt qu'une collection de produits individuels qui ne fonctionnent pas bien ensemble. Palo Alto Networks partage des informations entre les éléments de la plateforme et permet une gestion centralisée et un fonctionnement simplifié à l'aide de Panorama, de GlobalProtect et de Prisma Access. Ainsi, vous profitez d'une politique, d'une prévention et d'une protection cohérentes sur tous vos emplacements.
- Utilisez les pare-feu nouvelle génération Palo Alto Networks en tant que passerelles de segmentation afin de consolider les technologies de sécurité en une seule et même plateforme et d'appliquer nativement une politique de sécurité cohérente sur tous vos emplacements au niveau de la couche 7 à l'aide d'App-ID, d'User-ID et de Content-ID. Une passerelle de segmentation segmente et contrôle le réseau en fonction des applications, des utilisateurs et des données. En outre, elle devrait fournir un contrôle d'accès granulaire et sécuriser tout le trafic traversant les micropérimètres et accédant aux surfaces à protéger.

La création de micropérimètres s'effectue dans la politique de couche 7 en permettant uniquement aux utilisateurs autorisés d'accéder aux surfaces à protéger dont ils ont

besoin à des fins métier, et uniquement à ces surfaces. Ainsi, vous n'avez pas besoin de modifier votre infrastructure.

- Segmentez votre réseau en fonction de ce que votre entreprise a de plus précieux afin d'empêcher tout mouvement latéral non autorisé.
- Appliquez le principe de l'accès le moins privilégié à vos surfaces à protéger. Déterminez qui doit avoir accès à quelles ressources, la manière d'y accéder et les moments auxquels cet accès est nécessaire. Fournissez uniquement le niveau d'accès strictement nécessaire à chaque utilisateur et à chaque périphérique, évaluez leur identité (y compris leur autorisation appropriée), puis mappez-y la politique de couche 7.
- Décryptez, inspectez et journalisez autant que possible chaque paquet passant par la couche 7, dans la mesure permise par les règlements et vos pratiques métier. Vous devez impérativement inspecter et journaliser le trafic de la couche 7. N'oubliez pas que les pirates savent comment contourner les contrôles de sécurité aux couches 3 et 4.
- Créez une stratégie pour regrouper des objets via l'étiquetage des charges de travail et enregistrer dynamiquement les étiquettes dans le but de soutenir l'automatisation de la politique de sécurité.
- Développez des processus afin d'effectuer, de maintenir et de garder continuellement à jour les contrôles de prévention au fur et à mesure que vous élaborez votre stratégie et que vous concevez votre réseau. Documentez les processus, éduquez et formez votre personnel, définissez des points de référence et mesurez votre progression par rapport à ces points.
- Effectuez votre transition vers un environnement Zero Trust de manière progressive, un segment à la fois, en commençant avec un ou plusieurs segments non essentiels qui vous permettront d'obtenir de l'expérience. Les segments Zero Trust et les anciens segments peuvent coexister sans problème, vous pouvez dès lors utiliser une approche itérative et sûre au lieu de tout remplacer en une fois, ce qui serait beaucoup plus risqué.

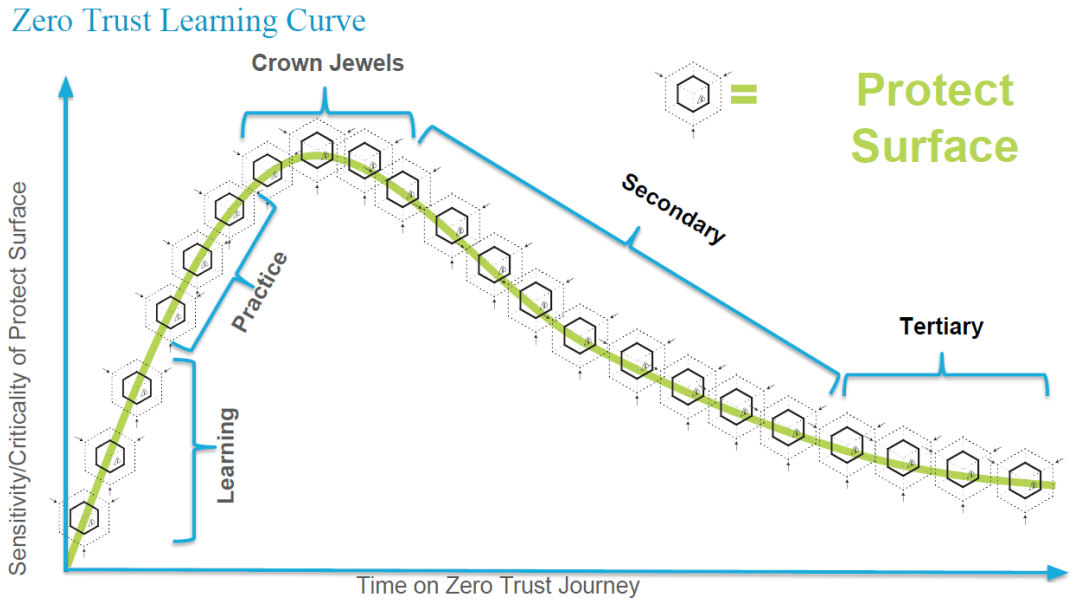
L'importance des applications diminuant, vous pouvez vous permettre d'appliquer une protection moins agressive qu'auparavant. Par exemple, vous n'avez pas besoin d'appliquer la même protection à une application de discussion qu'à celles essentielles à votre entreprise. Collaborez avec les responsables métier pour déterminer quelles applications doivent être protégées en priorité.

Comment commencer l'implémentation du Zero Trust ?

Le chemin vers la sécurité Zero Trust passe tout d'abord par l'éducation et la collaboration. Les parties prenantes qui identifieront les ressources les plus précieuses de votre entreprise et vous-même devez comprendre les concepts, les principes et les objectifs du Zero Trust.

1. Créez un centre d'excellence en matière de Zero Trust. Il s'agit d'une équipe pluridisciplinaire comprenant des chefs d'entreprise (les responsables des activités commerciales et techniques), le service informatique, la sécurité de l'information, l'infrastructure, les développeurs d'applications et d'autres parties prenantes. L'équipe définit et identifie chaque surface à protéger ainsi que les données, les applications, les actifs et les services (éléments DAAS) qui constituent chaque surface. Elle accorde la priorité aux surfaces à protéger les plus précieuses pour votre entreprise, puis elle planifie et implémente la stratégie Zero Trust. L'équipe reste impliquée dans la maintenance du déploiement au fur et à mesure que votre entreprise évolue. Les chefs d'entreprise peuvent aborder les résultats commerciaux souhaités, les exigences de conformité et la valeur des actifs commerciaux.
2. Participez à un atelier Zero Trust pour que tout le monde soit prêt et sur la même longueur d'onde. Contactez votre représentant commercial Palo Alto Networks pour plus d'informations et pour planifier un atelier.
3. Suivez La méthodologie en cinq étapes pour mapper le réseau segmenté que vous souhaitez créer.
4. Commencez la transition avec un ou plusieurs petits segments bien compris et à faible risque (qui ne sont pas essentiels aux opérations commerciales) pour expérimenter. Ne commencez pas avec des actifs critiques. Ensuite, mettez ce que vous avez appris à l'épreuve avec un ou plusieurs segments d'essai. Une fois que vous vous sentez prêt, placez vos surfaces à protéger les plus essentielles à votre activité

(les éléments DAAS qui constituent la surface à protéger) dans des micropérimètres Zero Trust, à raison d'un micropérimètre par surface à protéger. Après cela, convertissez le deuxième ensemble de surfaces à protéger le plus précieux en Zero Trust, puis le troisième, le quatrième, etc.



La méthodologie en cinq étapes

La méthodologie en cinq étapes pour l'implémentation d'une stratégie Zero Trust vous propose un parcours clair et logique pour protéger votre environnement, vos données, vos applications, vos actifs, vos services et vos utilisateurs. La manière dont vous appliquez la méthodologie dépend des éléments que vous cherchez à protéger et de vos exigences commerciales (autrement dit, les éléments essentiels à votre entreprise), mais le résultat est toujours le même :

- Segmentez votre réseau de manière efficace et efficiente afin d'empêcher tout mouvement latéral.
- Protégez vos données et systèmes critiques contre les applications et utilisateurs non autorisés.
- Protégez vos applications critiques contre tout accès et utilisation non autorisés.
- Appliquez votre politique de manière transparente sur votre réseau, votre cloud et vos terminaux afin d'en garantir la cohérence et de simplifier sa gestion.

Peu importe l'infrastructure, la méthodologie en cinq étapes représente un moyen efficace d'implémenter une stratégie Zero Trust, que ce soit sur le cloud, sur un réseau privé ou sur des terminaux.

Étape 1 : définition de votre surface à protéger

Une surface à protéger correspond à ce que votre entreprise a de plus précieux. Ce sont les données, les applications, les actifs et les services (DAAS) que vous devez protéger pour garantir le fonctionnement normal de votre entreprise. En définissant votre surface à protéger, vous pouvez concentrer vos efforts sur la protection des éléments les plus cruciaux pour votre entreprise, au lieu d'essayer d'identifier et de protéger l'ensemble de la surface d'attaque ou de vous concentrer uniquement sur le périmètre. En outre, la surface à protéger est beaucoup plus petite que la surface d'attaque ou le périmètre, elle est donc plus facile à protéger.

Définissez votre surface à protéger en fonction des éléments DAAS les plus essentiels à votre entreprise :

- **D**onnées. Quelles données doivent être protégées ? Pensez à votre propriété intellectuelle, comme le code ou les processus propriétaires, les données d'identification, les informations de carte de paiement et les données médicales personnelles, comme les informations de la loi américaine sur la transférabilité et la responsabilité des assurances de santé (HIPAA).
- **A**pplications. Quelles applications utilisent des informations sensibles ? Lesquelles sont essentielles au bon fonctionnement de votre entreprise ?
- **A**ctifs. Quels actifs sont les plus sensibles ? Selon la nature de votre entreprise, il peut s'agir des contrôles SCADA, des terminaux de point de vente (TPV), de l'équipement médical ou de fabrication ou encore de groupes de serveurs critiques.
- **S**ervices. Quels services, comme les services DNS, DHCP et Active Directory sont susceptibles d'être exploités lors d'attaques visant à perturber les opérations informatiques et à nuire à votre entreprise ?

Chaque élément DAAS essentiel fait partie d'une surface à protéger (ou, dans certains cas, est une surface à protéger en lui-même). Par exemple, si votre entreprise fournit des soins de santé, alors les données médicales personnelles sont capitales. Les *données* correspondent aux informations des patients. Les *applications* sont celles utilisées pour accéder aux données médicales personnelles, comme EPIC. Les *actifs* sont les serveurs qui stockent les données et les équipements générant les données médicales personnelles, comme les scanners médicaux ou les postes de travail des médecins. Enfin, par *services*, on entend ceux utilisés pour accéder aux données, comme l'ouverture de session unique et Active Directory.

Au fur et à mesure que vous progresserez dans la méthodologie en cinq étapes, vous placerez chaque surface à protéger dans son propre micropérimètre (segmenté par un pare-feu nouvelle génération physique ou virtuel de Palo Alto Networks utilisé comme passerelle de segmentation). Ainsi, vous pourrez contrôler avec précision qui pourra accéder aux éléments, la manière d'y accéder et à quel moment ils y auront accès. Sécurisez chaque surface à protéger de la manière la plus adéquate. Un micropérimètre est plus facile à gérer et à protéger qu'un périmètre large comprenant des éléments DAAS auxquels des utilisateurs disposant de diverses conditions d'accès doivent accéder. Cela permet également de rapprocher la protection des données critiques.

Protégez en priorité les éléments essentiels au bon fonctionnement de votre entreprise. Vos actifs les plus précieux se trouvent souvent dans votre centre de données ou dans le cloud. Une fois que vous avez implémenté le modèle Zero Trust dans au moins une surface à protéger non essentielle pour vous entraîner, attelez-vous à la défense des surfaces les plus critiques. Au début, il est possible que vous ne connaissiez pas toutes les applications présentes dans votre centre de données, mais vous savez lesquelles sont les plus importantes. Ensuite, passez au prochain ensemble de surfaces à protéger de votre liste des priorités. Répétez le processus jusqu'à ce que vous ayez atteint vos objectifs de sécurité.

Utilisez les outils suivants pour obtenir une meilleure connaissance de votre trafic réseau et pour vous aider à identifier les éléments DAAS qui constituent vos surfaces à protéger les plus essentielles :

- La connaissance de l'entreprise de votre équipe. Par exemple, les chefs d'entreprise peuvent déterminer la valeur stratégique des applications.
- Insérez au moins un pare-feu nouvelle génération de manière transparente dans votre réseau en mode câble virtuel (vwire) pour mieux connaître votre trafic. Vwire est un mode relais ne requérant aucune modification de la topologie, car les interfaces vwire ne possèdent pas d'adresse IP ou MAC. Consultez les journaux du trafic pour afficher et analyser le trafic réseau. Si vous disposez déjà de pare-feu gérés dans votre réseau, utilisez les journaux Panorama.
- Consultez les journaux dans Cortex Data Lake et utilisez des outils de découverte d'actifs tiers de l'un des partenaires intégrés de Palo Alto Networks et qui fonctionnent avec Cortex.
- Utilisez Prisma SaaS pour découvrir les utilisateurs, les actifs et les données des applications SaaS et obtenir une meilleure connaissance de ces applications.
- Si votre pare-feu nouvelle génération ou votre Panorama gérant vos pare-feu exécute PAN-OS 9.0, utilisez Policy Optimizer pour vous aider à identifier les applications clés sur les règles de politique de sécurité existantes. (Policy Optimizer vous montre même toutes les applications sur les règles basées sur les ports.) Si vous ne pouvez pas utiliser Policy Optimizer, utilisez Expedition pour gagner en visibilité dans vos applications.
- Exploitez des outils de mappage des dépendances d'application pour découvrir automatiquement ces dépendances (à savoir les ressources utilisées par une application, comme les bases de données, les équilibreurs de charge, les serveurs, etc.).

Étape 2 : mappage des flux de transaction de votre surface à protéger

Mappez les flux de transaction (les interactions) entre vos éléments DAAS critiques et les utilisateurs pour comprendre leurs interdépendances : qui a des raisons commerciales pour accéder à chaque élément, de quelle manière ils y accèdent et à quel moment. Ce mappage vous permettra de comprendre et d'architecturer votre réseau. Il vous aidera également à découvrir comment créer des politiques de sécurité permettant uniquement aux utilisateurs autorisés d'accéder à des données et des actifs spécifiques via les applications spécifiées (le principe de l'accès le moins privilégié).

Il existe de nombreuses manières de mapper des flux de transaction. En outre, certaines techniques de définition de votre surface à protéger s'appliquent également au mappage des flux de transaction de cette dernière :

- Exploitez les diagrammes de flux si vous les possédez (les entreprises ont parfois besoin de créer de tels diagrammes à des fins de conformité ou d'audit).

- Collaborez avec les représentants commerciaux et les architectes d'application, de réseaux et d'entreprise pour comprendre l'objectif des applications et le flux de transaction qu'ils envisagent.
- Insérez au moins un pare-feu nouvelle génération de manière transparente dans votre réseau en mode câble virtuel (vwire) pour mieux connaître votre trafic. Consultez les journaux du trafic pour afficher et analyser le trafic.
- Utilisez des outils tiers provenant des partenaires intégrés de Palo Alto Networks.
- Utilisez les informations des journaux provenant de Cortex Data Lake pour gagner en visibilité dans vos flux de transaction et mapper ces derniers. Cortex Data Lake regroupe les journaux du pare-feu nouvelle génération, des pare-feu VM-Series de Prisma Access et de Traps.
- Pour les applications, mappez les flux de travail, y compris le flux des données d'application dans tout le réseau, les objets informatiques requis par chaque application et les personnes utilisant les applications.
- Concernant les données, déterminez qui les utilise, les endroits où elles sont collectées, stockées, utilisées et transférées, ainsi que la manière dont elles sont stockées, cryptées, archivées ou détruites après leur utilisation.
- Pour les actifs, découvrez leur emplacement, qui les utilise et quand, et comment ils s'intègrent aux flux de travail.
- Quant aux services, mappez leurs flux de travail dans tout l'environnement.

En plus de révéler qui utilise quelles applications et quand et comment elles sont utilisées, le mappage des flux de transaction fournit une visibilité granulaire qui aide à la conformité et à la planification de la reprise après sinistre. Elle vous offre également l'occasion d'optimiser vos flux de travail et d'examiner qui possède des raisons commerciales légitimes pour accéder aux éléments DAAS de chaque surface à protéger.

En apprenant à connaître les flux de transaction traversant votre réseau, vous découvrirez qui utilise chaque surface à protéger, comment elles sont utilisées, où elles sont situées et quels éléments interagissent pour activer chacune des applications critiques. Ainsi, vous saurez comment segmenter votre réseau et où insérer des contrôles.

Étape 3 : développement d'un réseau Zero Trust

Maintenant que vous comprenez votre surface à protéger et vos flux de transaction, commencez à développer votre réseau Zero Trust en fonction de ce que votre entreprise a de plus précieux. Concevez les surfaces à protéger essentielles que vous avez identifiées à l'Étape 1 : définition de votre surface à protéger de l'intérieur. Lorsque vous développez votre architecture, assurez-vous qu'elle est facile à utiliser et à maintenir, et suffisamment flexible pour s'adapter aux modifications des surfaces à protéger et à l'évolution de l'entreprise. Exécutez l'outil Best Practice Assessment pour définir une configuration de base des bonnes pratiques et mesurer votre progression vers vos objectifs Zero Trust.

Les passerelles de segmentation, à savoir les pare-feu nouvelle génération Palo Alto Networks physiques ou virtuels reliant vos segments réseau et appliquant la politique de couche 7, constituent la pierre angulaire de votre architecture. Faites passer tout le trafic à travers une passerelle de segmentation, placez ces passerelles au plus près des ressources qu'elles protègent et utilisez-les de concert avec d'autres fonctionnalités Palo Alto Networks pour les automatiser autant que possible. Grâce aux pare-feu nouvelle génération, vous pouvez :

- créer un micropérimètre dans la politique de couche 7 autour de chaque surface à protéger afin d'empêcher tout mouvement latéral. En effet, le micropérimètre fournit des contrôles de politique granulaires pour les utilisateurs (User-ID) accédant aux applications (App-ID) et aux ressources via la passerelle de segmentation, en fonction de la manière (Content-ID) et du moment de l'accès. Vous pouvez également segmenter votre réseau en fonction de ses flux de transaction et de la manière dont vos utilisateurs et applications accèdent aux données et aux services ;
- regrouper les fonctionnalités de sécurité en un seul et même point de contrôle pour tout le trafic entrant et sortant de la surface à protéger. La passerelle de segmentation devrait appliquer la politique, crypter et décrypter le trafic et appliquer des protections telles que :

    - la sécurité DNS (utilisez le service de sécurité DNS, qui fournit plusieurs sources de renseignements sur les menaces en temps réel, des analyses en temps réel des requêtes DNS pouvant être mises à l'échelle à l'infini et des signatures DNS avancées),
    - la prévention des intrusions (profils de protection contre les vulnérabilités, antispyware et antivirus),
    - le blocage de types de fichier potentiellement dangereux,
    - la prévention de menaces inconnues et de jour 1 (WildFire),
    - le filtrage des URL,
    - la prévention des pertes de données (DLP) ;
- décrypter et inspecter le trafic de la couche 7 en temps réel ;
- journaliser chaque paquet de la couche 2 à la couche 7. Vous pouvez ensuite envoyer les journaux à Cortex Data Lake à partir de Panorama pour les pare-feu gérés, de pare-feu individuels (pare-feu non gérés par Panorama), de Prisma Access (anciennement connu sous le nom de service cloud GlobalProtect™) et de Traps afin de centraliser et de regrouper vos stockages de journaux sur site et virtuels (cloud privé et public) pour les pare-feu physiques et VM-Series ;
- utiliser des API pour intégrer étroitement des outils de défense tiers de partenaires ;
- automatiser des boucles de rétroaction qui détectent les événements et automatisent les réponses :
    - Étiquetez les charges de travail et utilisez des étiquettes comme critères de filtrage pour déterminer les membres de groupes d'adresses dynamiques dans la politique de sécurité. Ceci vous permet d'automatiser des actions sur la base d'événements de transfert des journaux vers un serveur HTTP(S). Un événement de transfert des journaux déclenche l'action en ajoutant ou en supprimant de manière dynamique et en temps réel des membres d'un groupe d'adresses dynamiques utilisé dans une politique de sécurité. La politique de sécurité détermine si l'accès est autorisé ou non aux membres du groupe d'adresses dynamiques. Le pare-feu applique ensuite l'action. Par exemple, vous pouvez configurer un entonnoir DNS dans un profil de sécurité antispyware afin de mettre automatiquement en quarantaine les systèmes potentiellement compromis qui tentent d'accéder à l'entonnoir. Utilisez des étiquettes et le transfert des journaux pour ajouter et supprimer dynamiquement ces systèmes d'un groupe d'adresses dynamiques associé à une règle de politique bloquant et journalisant tout le trafic vers l'adresse de l'entonnoir. Vous pouvez ensuite enquêter sur les systèmes potentiellement compromis lorsque vous recevez des alertes de journaux.
    - Utilisez Cortex XDR pour automatiser l'analyse de votre réseau, découvrir les comportements anormaux indiquant une intrusion potentielle et, le cas échéant, recevoir des alertes pour vous permettre d'enquêter et de résoudre le problème. Cortex XDR offre une visibilité sur votre trafic réseau, simplifie les enquêtes sur les menaces en mettant en corrélation les journaux et vous permet d'identifier la cause première des alertes et d'y répondre immédiatement. Utilisez les API de Cortex XDR pour l'intégrer à Demisto et automatisez les réponses à l'aide des programmes de réponse Demisto adaptés aux flux de travail de votre entreprise. Ainsi, vous pourrez profiter de temps de réponse réduits de plusieurs jours à quelques minutes.
    - Utilisez WildFire pour automatiser la découverte de nouveaux logiciels malveillants. Lorsque WildFire découvre de tels logiciels où que ce soit dans le monde, il ne lui faut au maximum que cinq minutes pour mettre à jour vos profils de sécurité afin de vous protéger contre cette nouvelle menace.
- utiliser des modèles et des piles de modèles dans Panorama pour automatiser le déploiement de politiques.
- utiliser des outils comme Ansible, Terraform et Python pour automatiser, orchestrer et accélérer la protection des déploiements de Prisma Cloud.

Palo Alto Networks vous permet de développer votre environnement Zero Trust et d'appliquer une sécurité uniforme sur tous vos emplacements :

- Panorama centralise le contrôle des politiques de gestion pour plusieurs pare-feu nouvelle génération et améliore l'efficacité opérationnelle par rapport à une gestion individuelle des pare-feu.
- Centre de données et réseau d'entreprise : utilisez des pare-feu nouvelle génération pour segmenter le réseau en micropérimètres pour vos surfaces à protéger.

- Cloud public : exploitez Prisma Access, qui utilise des pare-feu nouvelle génération sur site ou VM-Series, et Prisma Cloud (une solution de sécurité de l'infrastructure cloud basée sur l'API) pour implémenter une politique Zero Trust dans les environnements cloud. Les clouds privés virtuels (VPC) définissent les limites de protection pour segmenter les charges de travail.
- Cloud privé : utilisez des pare-feu VM-Series pour implémenter une politique Zero Trust.
- Filiales et utilisateurs mobiles : utilisez Prisma Cloud pour fournir une sécurité basée sur le cloud et pour éviter les allers-retours aux ressources du réseau d'entreprise. Configurez Prisma Access pour les utilisateurs et Prisma Access pour les réseaux afin de sécuriser les filiales.

  Vous pouvez également utiliser des pare-feu nouvelle génération sur site avec le service d'abonnement GlobalProtect pour étendre la politique de sécurité et son application aux utilisateurs distants et aux filiales.
- Terminaux : protégez les terminaux à l'aide d'un pare-feu nouvelle génération pour la segmentation et la première couche de protection, et de Traps pour la seconde couche. Appliquez une politique cohérente au moyen de GlobalProtect (installation sur site) ou des VPN de Prisma Access (installé à l'aide de Panorama et géré pour vous depuis le cloud) afin d'étendre la politique aux terminaux distants et de l'autoriser à se déplacer avec l'utilisateur. Prisma Access nécessite l'application GlobalProtect sur les terminaux des utilisateurs mobiles. Dans tous les cas, installez cette application sur les terminaux gérés et utilisez le VPN sans client GlobalProtect sur les terminaux non gérés (ceux sur lesquels vous ne pouvez ou ne voulez pas affecter un agent, comme des systèmes partenaires ou des périphériques personnels). Appliquez l'authentification multifacteur lorsque cela s'avère nécessaire pour protéger les actifs de grande valeur.
- Applications SaaS : utilisez Prisma SaaS pour scanner, analyser, classifier et protéger les applications SaaS. Redirigez le trafic des applications SaaS pour les périphériques non gérés via votre pare-feu nouvelle génération (le trafic des périphériques gérés passe par Prisma Access, GlobalProtect ou un pare-feu nouvelle génération).

Étape 4 : création de la politique Zero Trust

Une politique Zero Trust se compose de règles de mise en liste blanche, c'est-à-dire des règles qui permettent uniquement aux utilisateurs autorisés d'accéder à des ressources spécifiques via les applications spécifiées à des moments et des endroits précis. Si le trafic enfreint l'une des règles, le pare-feu le bloque automatiquement. C'est important, car :

- il est beaucoup plus simple de déterminer les applications que vous souhaitez autoriser pour soutenir votre entreprise plutôt que d'entreprendre la tâche sans fin d'identifier et de bloquer toutes celles que vous ne voulez pas autoriser ;
- toutes les violations et activités malveillantes se produisent sur des règles d'autorisation. Concentrez-vous sur la protection du trafic autorisé, et autorisez exclusivement le trafic nécessaire à votre entreprise.

La politique Zero Trust est fondée sur la méthode Kipling. En répondant aux six questions posées par Rudyard Kipling (qui, quoi, quand, où, comment et pourquoi), vous pourrez déterminer si vous devez autoriser ou bloquer tel ou tel trafic et décider de la manière de créer une politique de sécurité capable d'assurer la protection de chacune des surfaces à protéger. Palo Alto Networks offre les fonctionnalités nécessaires pour implémenter la méthode Kipling dans la politique de sécurité :

- **Qui** doit avoir accès à une ressource ?
  - User-ID identifie les utilisateurs et vous permet de contrôler qui a accès à une ressource dans la politique. En appliquant le principe de l'accès le moins privilégié (qui doit connaître ces informations ?), autorisez uniquement l'accès pour les individus, les groupes et les périphériques qui ont de véritables raisons d'accéder à une ressource.
  - Créez une politique d'authentification pour vérifier l'identité des utilisateurs qui tentent d'accéder à des ressources. Une telle politique permet également de déterminer si l'authentification multifacteur (MFA) est nécessaire ou non.

- Utilisez la MFA pour protéger les services et les applications sensibles en requérant au moins un facteur d'authentification supplémentaire en plus du mot de passe dans le portail captif, comme un code à usage unique transmis à un téléphone portable ou par e-mail, avant que le pare-feu n'autorise l'accès à des services, des applications et des ressources sensibles. Pour les utilisateurs distants, configurez GlobalProtect pour faciliter les notifications de MFA (vous devez également configurer la MFA sur le pare-feu).
- Pour les périphériques utilisant GlobalProtect, configurez des profils d'informations sur l'hôte (HIP) afin de définir la politique d'accès pour les hôtes, de l'appliquer à ces hôtes et d'empêcher les périphériques ne respectant pas vos normes de sécurité et de maintenance d'accéder aux ressources. Par exemple, vous pouvez utiliser un HIP pour vous assurer que le cryptage est activé sur les terminaux, que les signatures antivirus de l'hôte sont à jour, etc. Si un hôte ne répond pas aux exigences du HIP, la politique de sécurité bloque son accès.

- **Quelle** application est utilisée pour accéder à la ressource ?
  - Créez une politique de couche 7 basée sur les applications à l'aide de l'App-ID, qui identifie les applications, peu importe le port, le protocole ou les tactiques d'évasion, afin d'autoriser uniquement les applications adéquates sur votre réseau. Une politique basée sur la couche 3 et la couche 4 s'appuie sur les adresses IP, que des personnes malveillantes peuvent usurper, et laisse les ports ouverts de sorte que des applications d'évasion peuvent y accéder.
  - Configurez le service sur application-default (par défaut de l'application) pour autoriser en toute sécurité des applications sur leurs ports par défaut et empêcher des applications d'évasion d'accéder à votre réseau via des ports non standard.
  - Si le pare-feu exécute PAN-OS 9.0 ou version ultérieure, ou si un appareil Panorama exécutant PAN-OS 9.0 ou version ultérieure gère des pare-feu exécutant PAN-OS 8.1 ou version ultérieure, utilisez Policy Optimizer pour examiner les règles de politique existantes (à la fois les règles basées sur les applications et les règles traditionnelles basées sur un port), identifier les rôles inutilisés et identifier les règles comportant des applications inutilisées. Pour les pare-feu exécutant des versions plus anciennes de PAN-OS, utilisez Expedition pour examiner les règles de politique. (Si vous devez migrer une configuration traditionnelle vers un périphérique PAN-OS, reportez-vous à la section Bonnes pratiques pour une migration vers une politique basée sur les applications.)
- **Quand** les utilisateurs accèdent-ils à la ressource ?

  Pour les applications auxquelles les utilisateurs n'accèdent qu'à certaines heures, appliquez un calendrier (**Objects [Objets]** > **Schedules [Calendriers]** sur les pare-feu et appareils Panorama) sur la règle de politique pour bloquer tout accès suspect en dehors des heures de travail. Souvent, les adversaires attaquent ou tentent d'exfiltrer des données en dehors des heures ouvrables normales afin de réduire le risque d'être découverts.
- **Où** la ressource est-elle située ?

  Ajoutez l'emplacement de la ressource de destination à la politique. Si nécessaire, restreignez également la source (la zone et l'adresse IP) du trafic.
- **Pourquoi** les utilisateurs accèdent-ils aux données ? Quelle est la valeur de ses données si elles sont perdues (toxicité) ?

  Classifiez les données pour comprendre leur toxicité : pourquoi les données valent-elles la peine d'être protégées ? Devriez-vous déclarer les pertes si un pirate parvenait à exfiltrer les données ? Configurez le filtrage des données pour empêcher les informations sensibles de quitter votre réseau et utilisez des outils de classification des données pour fournir des métadonnées sur vos données. Comprendre la toxicité de vos données vous aide à déterminer comment les protéger, ce que vous devez en faire après les avoir utilisées et comment les étiqueter pour les utiliser dans une politique.
- **Comment** devriez-vous autoriser l'accès à la ressource ?

  Appliquez le Content-ID et les meilleures pratiques pour protéger vos ressources contre les menaces dans le trafic des applications :
  - Appliquez le principe de l'accès le moins privilégié à votre politique de sécurité. Accordez exclusivement un accès aux utilisateurs disposant de raisons commerciales légitimes, et ce,

uniquement pour applications dont ils ont besoin pour leurs activités professionnelles, aux moments adéquats et de la manière appropriée.

- Journalisez l'ensemble du trafic interne et externe passant par la couche 7. Les règles de politique du pare-feu autorisent la journalisation par défaut. Transférez les journaux à Cortex Data Lake (voire à Panorama ou à des collecteurs de journaux) pour les consolider et ainsi permettre des analyses plus complètes et plus faciles.
- Appliquez la politique et la prévention des menaces de manière cohérente sur tous vos emplacements (réseau, cloud et terminaux) et pour tous les utilisateurs locaux et distants afin de garantir que la politique suit l'utilisateur où qu'il aille, pour toutes les applications et toutes les ressources. Une politique incohérente augmente les vulnérabilités, est difficile à comprendre et à maintenir, et risque de nuire aux exigences et audits de conformité. Utilisez des pare-feu nouvelle génération physiques et des pare-feu VM-Series virtuels en tant que passerelles de segmentation pour appliquer une politique Zero Trust, de couche 7 et de méthode Kipling cohérente dans votre réseau et votre cloud. Utilisez Prisma Access (cloud) et GlobalProtect (installation sur site et avec Prisma Access) pour étendre la politique Zero Trust cohérente aux terminaux. Pour les terminaux non gérés (ceux sur lesquels vous ne voulez ou ne pouvez pas affecter un agent), utilisez le VPN sans client GlobalProtect pour appliquer une politique cohérente. Créez et réutilisez des modèles et des piles Panorama pour appliquer une politique cohérente sur tous les emplacements semblables, comme vos centres de données ou vos périmètres.
- Configurez des profils de sécurité (des profils de protection contre les vulnérabilités pour les profils IPS, antivirus et WildFire pour vous protéger contre les logiciels malveillants, y compris ceux de type « jour 1 » ; des profils antispyware pour empêcher les menaces de type « command-and-control » ; des profils de blocage des fichiers pour bloquer les types de fichiers à risque ou vous alerter sur ceux-ci ; et un filtrage des URL afin de contrôler l'accès aux sites web, d'aider à prévenir les attaques par hameçonnage et d'appliquer la recherche sécurisée sur les moteurs de recherche) et appliquez-les à tout le trafic autorisé. Suivez les meilleures pratiques pour les profils de sécurité du pare-feu du centre de données et du pare-feu du périmètre.
- Utilisez les meilleures pratiques WildFire pour détecter et prévenir les attaques par logiciel malveillant de type « zero-day ».
- Utilisez les meilleures pratiques en matière de décryptage pour décrypter autant de trafic que les règlements et exigences commerciales vous permettent de décrypter afin d'inspecter le plus de trafic possible. Vous ne pouvez pas protéger votre réseau des menaces que vous ne voyez pas.
- Utilisez le service de sécurité DNS pour fournir un accès en temps réel et pouvant être mis à l'échelle à l'infini aux signatures DNS, une analyse en temps réel des requêtes DNS et des signatures DNS avancées générées à l'aide d'un apprentissage machine et d'une analyse prédictive.
- Pour répondre à la question du « comment », vous devez également déterminer ce que vous devez faire de vos données une fois que vous les avez utilisées : les abstraire par cryptage, tokenisation ou masquage, ou les éliminer en les archivant ou en les supprimant. Archivez les données périmées (environ 80 % des données de la plupart de systèmes n'ont pas été utilisées depuis plus de deux ans).
- Utilisez Cortex XDR pour affiner et améliorer votre politique.

Grâce à la méthode Kipling, vous pouvez créer une politique de sécurité protégeant chacune des surfaces à protéger de manière appropriée, car elle vous permet de comprendre qui doit avoir accès aux ressources, la manière utilisée pour y accéder, quand un tel accès est nécessaire et quelles protections doivent être appliquées. Pour élaborer des règles de politique, vous devez concevoir des missions d'entreprise selon la méthode Kipling. Par exemple :

	Qui	Quoi	Quand	Où	Pourquoi	Comment
Méthode	User-id	App-ID	Limites de temps	Objets système	par application	Content-ID

	Qui	Quoi	Quand	Où	Pourquoi	Comment
Sur site	Utilisateurs d'Epic	Epic	indifférent	Serveur Epic	Toxique (données de grande valeur)	Décryptage, inspection (profils de sécurité), journalisation du trafic
Cloud	Ventes	Salesforce	Heures ouvrables	États-Unis	Toxique (données de grande valeur)	Décryptage, inspection (profils de sécurité), journalisation du trafic

Dans tous les cas, le pare-feu n'autorise que le trafic qui satisfait à toutes les conditions posées par la méthode de Kipling et qui réussit l'inspection. Il refuse automatiquement l'accès au trafic qui ne répond pas à l'une des règles.

En plus de la politique de sécurité, d'authentification et de décryptage, utilisez les meilleures pratiques relatives à la protection DoS et à la protection de zone pour protéger les serveurs essentiels contre les attaques par déni de service (DoS).

Pour les pare-feu que vous n'avez pas encore configurés, utilisez les modèles de configuration IronSkillet de jour 1 pour implémenter une politique de meilleures pratiques de jour 1, puis ajustez cette politique pour qu'elle convienne au maximum à vos surfaces à protéger.

Étape 5 : surveillance et maintenance du réseau

La sécurité est un processus itératif, car la journalisation et la surveillance permettent de déceler les aspects sujets à amélioration et parce que votre entreprise et votre réseau évoluent avec le temps. Respectez les processus opérationnels que vous avez conçus lors du développement de votre réseau afin de maintenir et de garder à jour les contrôles de prévention.

- Décryptez, inspectez et journalisez tout le trafic (interne et externe) passant par la couche 7.
- Transférez les journaux à Cortex Data Lake à partir de Panorama pour les pare-feu gérés, de pare-feu individuels (pare-feu non gérés par Panorama), de Prisma Access et de Traps afin de centraliser et de regrouper vos stockages de journaux sur site et virtuels (cloud privé et public). Ainsi, vous pourrez en apprendre davantage sur le trafic de votre réseau et vos surfaces à protéger.
- Mettez la politique à jour et ajoutez éventuellement de nouvelles surfaces à protéger en fonction des renseignements obtenus de Cortex XDR, qui utilise les données du Cortex Data Lake et l'apprentissage machine pour automatiser l'analyse de votre réseau sur la base du comportement normal de ce dernier et l'identification de tout comportement anormal pouvant être dû à une intrusion ou à une autre menace. Les menaces ciblant les éléments DAAS non inclus dans une surface à protéger peuvent mettre en évidence celles que vous n'aviez pas prises en compte lorsque vous avez initialement défini vos surfaces à protéger.
- Utilisez Cortex XDR pour gagner en visibilité sur votre trafic réseau, pour simplifier les enquêtes sur les menaces en mettant en corrélation les journaux et pour vous permettre d'identifier la cause première des alertes et d'y répondre immédiatement.
- Utilisez les API de Cortex XDR pour l'intégrer à Demisto et automatisez les réponses à l'aide des programmes de réponse Demisto adaptés aux flux de travail de votre entreprise. Ainsi, vous pourrez profiter de temps de réponse réduits de plusieurs jours à quelques minutes.
- Utilisez Prisma Cloud pour regrouper vos données de configuration, les informations sur les activités des utilisateurs et celles sur le trafic réseau, mais également pour obtenir une meilleure visibilité sur

ces données et informations. Prisma Cloud analyse les données et fournit des informations précises et exploitables.

- Suivez les Meilleures pratiques pour les mises à jour du contenu de menace et des applications pour obtenir des App-ID nouveaux et modifiés et pour garder vos signatures de menaces à jour.
- Utilisez l'outil Best Practice Assessment pour mesurer votre progrès vers une configuration selon les meilleures pratiques et pour soutenir votre transition vers une position de sécurité respectant les meilleures pratiques.
- Surveillez l'activité réseau, utilisez des rapports prédéfinis et générez des rapports personnalisés pour gagner en visibilité sur votre environnement.
- Maintenez la cohésion de l'équipe pluridisciplinaire pour aider à maintenir votre déploiement Zero Trust au fur et à mesure que votre réseau et votre entreprise évoluent, et pour éduquer et former les nouveaux membres de l'équipe afin de s'assurer qu'ils comprennent la stratégie et l'implantation.
- Continuez à automatiser les actions et les réponses à mesure que les fonctionnalités d'automatisation évoluent.

Ressources Zero Trust

Vous trouverez ci-dessous des documents techniques, des livres blancs, des diffusions web, des vidéos et d'autres ressources vous fournissant plus d'informations et de contexte pour votre stratégie Zero Trust. En plus des informations contenues dans ce document et dans les ressources listées ci-dessous, vous pouvez faire appel à l'équipe d'experts-conseils des Professional Services de Palo Alto Networks pour vous aider à concevoir et à implémenter votre stratégie Zero Trust.

- Comment créer un réseau Zero Trust (diffusion web à la demande)
- Briser le mythe entourant l'implémentation du Zero Trust (diffusion web à la demande)
- Aperçu du Zero Trust
- Zero Trust (page web de Palo Alto Networks sur le Zero Trust)
- Meilleures pratiques pour l'exécution du Zero Trust (feuille de route pour la transformation)
- Zero Trust : implémentation simplifiée en cinq étapes (livre blanc)
- Zero Trust : pour que cloud rime avec sécurité
- Sécurité cloud Zero Trust (vidéo)
- La vérité sur le Zero Trust (infographie)

Documentation technique de Palo Alto Networks

Transition vers les meilleures pratiques :

- Démarrage avec le BPA
- Comment exécuter un BPA (vidéo)
- Comment comprendre les résultats d'un BPA (vidéo)
- Page de la communauté Live de l'outil Best Practice Assessment

Portail de documentation des meilleures pratiques :

- Getting Started with Best Practices
- Politique de sécurité des passerelles Internet exemplaire
- Politique de sécurité exemplaire pour le centre de données
- Bonnes pratiques pour une migration vers une politique basée sur les applications
- Meilleures pratiques pour sécuriser l'accès administratif
- Meilleures pratiques pour les mises à jour du contenu de menace et des applications
- Pratiques exemplaires en matière de déchiffrement
- Protection DoS et Protection de Zones Respectant les Meilleures Pratiques
- Les meilleures pratiques pour le déploiement de WildFire

Expedition

IronSkillet (modèles de configuration de jour 1)

Support client

Évaluation de la posture de prévention (évaluation consultative gratuite de vos capacités de prévention)

Partenaires technologiques NextWave de Palo Alto Networks