Proposé par

paloalto NETWORKS

Les pare-feux logiciels

pour les nuls
A Wiley Brand

Étendez le Zero Trust aux applications cloud

Découvrez les types de pare-feux logiciels

Découvrez les cas d'usage des pare-feux logiciels

Une édition spéciale de Palo Alto Networks

Lawrence Miller

À propos de Palo Alto Networks

Palo Alto Networks est le leader mondial de la cybersécurité. Nous innovons pour déjouer les cybermenaces et pour que les organisations puissent adopter les nouvelles technologies en toute confiance. Nous offrons des services et des plateformes de cybersécurité de nouvelle génération, enrichis par une surveillance exceptionnelle des menaces et soutenus par une automatisation avancée. Qu'il s'agisse de déployer nos produits pour créer une entreprise appliquant les principes du Zero Trust, de répondre à un incident de sécurité ou de créer des synergies pour obtenir de meilleurs résultats en matière de sécurité grâce à un puissant écosystème de partenaires, nous nous engageons à faire en sorte que chaque jour soit plus sûr que le précédent. C'est pourquoi nous sommes le partenaire privilégié en matière de cybersécurité.

Chez Palo Alto Networks, nous nous engageons à réunir les meilleures personnes au service de notre mission. Nous sommes donc également fiers d'être le lieu de travail préféré dans le secteur de la cybersécurité, reconnu parmi les lieux de travail les plus appréciés de Newsweek (2021 et 2022), les meilleures entreprises pour la diversité de Comparably (2021) et les meilleurs endroits pour l'égalité LGBTQ de HRC (2022). Pour plus d'informations, rendez-vous sur le site www.paloaltonetworks.com.

Les pare-feux logiciels

Une édition spéciale de Palo Alto Networks

par Lawrence Miller

pour les nuls®

Les pare-feux logiciels pour les Nuls®, une édition spéciale de Palo Alto Networks

Publié par
John Wiley & Sons, Inc.
111 River St., Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-394-23263-5 (pbk); ISBN 978-1-394-23264-2 (ebk)

Remerciements de l'éditeur

Cet ouvrage a été réalisé avec la participation des personnes suivantes :

Éditeur : Elizabeth Kuball

Rédacteur chargé des acquisitions : Traci Martin

Responsable éditorial : Rev Mengle

Responsable de compte client : Cynthia Tweed

Éditeur de production : Tamilmani Varadharaj

Table des matières

Introduction

À mesure que les entreprises adoptent ou élaborent leurs stratégies cloud, elles se trouvent confrontées à un problème essentiel de sécurité : les pare-feux physiques nouvelle génération ne conviennent pas aux environnements cloud, tandis que les pare-feux standard proposés par les fournisseurs de services cloud ne parviennent pas à contrer les atteintes modernes à la cybersécurité. Traditionnellement, les pare-feux réseau reposent sur du matériel spécifiquement conçu pour répondre aux besoins de performance et de traitement élevés des solutions d'entreprise, en particulier les pare-feux de nouvelle génération.

Heureusement, les avancées technologiques ont modifié le paysage. Aujourd'hui, l'innovation s'articule principalement autour du logiciel. Pratiquement tout est « défini par logiciel » aujourd'hui et, comme le souligne notamment Satya Nadella, PDG de Microsoft, « chaque entreprise est devenue un éditeur de logiciels à part entière ». Les pare-feux logiciels sont désormais la solution idéale pour divers scénarios liés au cloud et à la virtualisation, y compris les clouds privés, les réseaux définis par logiciel, les environnements multicloud, hybrides, en périphérie, ainsi que les architectures basées sur des containers et la 5G.

À propos de ce livre

L'ouvrage *Les pare-feux logiciels pour les Nuls*, édition spéciale de Palo Alto Networks, comporte cinq chapitres qui abordent les points suivants :

- Le paysage des menaces modernes, les défis de sécurité et les limites des technologies et approches existantes dans les environnements hybrides et multicloud (chapitre 1).
- Le Zero Trust et comment étendre ces principes au cloud avec des pare-feux logiciels (chapitre 2)
- Les différents types de pare-feux logiciels (chapitre 3)
- Les cas d'usage des pare-feux logiciels (chapitre 4)
- Les questions clés à poser à votre fournisseur de pare-feu logiciel (chapitre 5)

Chaque chapitre est rédigé de façon indépendante du reste de l'ouvrage. Si un sujet vous intéresse, vous pouvez donc passer directement au chapitre qui s'y rapporte. Vous pouvez lire cet ouvrage dans le sens qui vous convient, mais nous vous déconseillons de le lire à l'envers ou de droite à gauche.

Il comprend également un glossaire pratique au cas où certains termes ou acronymes utilisés dans ce livre vous échapperaient.

Quelques suppositions

On dit que la plupart des hypothèses ont perdu leur utilité, mais je vais tout de même en faire quelques-unes.

Je présume essentiellement que vous travaillez dans les opérations cloud, la sécurité informatique ou que vous êtes un décideur à la recherche de méthodes plus efficaces pour sécuriser les charges applicatives de votre organisation au sein de divers environnements cloud et virtualisés. Vous êtes peut-être responsable de la sécurité des systèmes d'information (RSSI) et vous vous efforcez de garder une longueur d'avance en veillant à l'intégration des solutions et au développement constant de l'entreprise. Ou bien vous êtes un architecte d'infrastructure cloud, un ingénieur ou un développeur d'applications. Votre objectif est d'assurer que la plateforme multicloud complexe de votre entreprise – y compris son architecture, son infrastructure et ses applications – reste alignée sur les exigences d'une entreprise en pleine évolution. Ou encore, vous pourriez être un architecte ou ingénieur spécialisé dans la sécurité des réseaux, en quête des meilleures pratiques pour garantir la protection continue des applications et données métier sensibles de votre entreprise, tout en ayant une vue d'ensemble sur toute l'infrastructure.

Si l'une de ces hypothèses vous correspond, alors c'est le livre qu'il vous faut ! Dans le cas contraire, poursuivez quand même votre lecture. C'est un excellent livre et, après l'avoir lu, vous aurez une bonne compréhension des atouts des pare-feux logiciels dans les contextes modernes du cloud et de la virtualisation.

Icônes employées dans ce livre

Tout au long de ce livre, j'utilise plusieurs icônes particulières pour attirer l'attention du lecteur sur certaines informations importantes. Voici à quoi vous pouvez vous attendre :

RAPPEL

Cette icône signale des informations importantes à inscrire obligatoirement dans votre mémoire non volatile, votre matière grise ou votre crâne.

JARGON TECHNIQUE

Cette icône explique le jargon qui se cache derrière le jargon ; il s'agit de l'étoffe dont les héros (les nerds) sont faits !

CONSEIL

Les conseils sont appréciés, jamais attendus. Nous espérons que vous apprécierez ces informations utiles.

ATTENTION

Ces alertes soulignent les choses contre lesquelles vos parents vous ont mis en garde. En fait, probablement pas, mais elles offrent des conseils pratiques.

Et maintenant ?

Ce sujet est tellement vaste qu'il est impossible de tout aborder dans ce livre. Donc, si en arrivant à la fin du livre, vous vous demandez : « Où puis-je en savoir plus ? », il vous suffit de consulter `https://paloaltonetworks.com`.

DANS CE CHAPITRE

- Adopter une stratégie de cloud hybride
- Examiner les défis de sécurité dans les environnements cloud et virtualisés et l'évolution du paysage des menaces

Chapitre 1
Reconnaître les tendances et les défis actuels

Dans ce chapitre, vous allez explorer l'expansion des clouds hybrides et la portabilité des applications, ainsi que la manière dont les approches centrées sur/conçues nativement pour le cloud facilitent les activités des entreprises. Vous découvrirez également les défis spécifiques en matière de sécurité dans les environnements cloud et virtualisés, sans oublier le paysage changeant des menaces modernes, notamment les ransomwares en tant que service (RaaS) et les menaces en constante mutation, de plus en plus difficiles à détecter.

Croissance des clouds hybrides et portabilité des applications

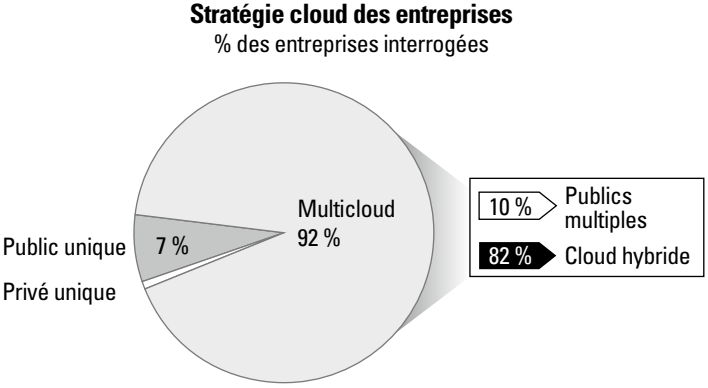
Les entreprises modernes transforment et réinventent leur mode opératoire afin de demeurer compétitives, en se focalisant sur les aspects suivants :

- **Miser sur l'innovation** pour stimuler la croissance de l'entreprise en libérant et en allouant des ressources

- **Proposer des expériences de haute qualité aux clients et collaborateurs**, dans le but de les satisfaire et d'accroître leur productivité
- **Favoriser la flexibilité et la capacité d'adaptation** des produits, des processus et de l'organisation en général pour conserver un avantage compétitif

Ces entreprises ont également élargi leur utilisation du cloud privé et des environnements virtualisés pour soutenir des stratégies de cloud hybride et multicloud, qui sont cruciales pour ces démarches opérationnelles.

Selon l'étude *Flexera 2021 State of the Cloud Report*, 92 % des entreprises ont aujourd'hui une stratégie multicloud et 82 % une stratégie de cloud hybride (voir figure 1-1).



Source : Flexera 2021 State of the Cloud Report

FIGURE 1-1 : Les entreprises ont adopté des stratégies multicloud et de cloud hybride.

Chaque cloud hybride est une forme de multicloud, mais tous les environnements multicloud ne sont pas nécessairement des clouds hybrides. Un cloud hybride fusionne des ressources virtualisées comme le calcul, le stockage et le réseau (via des plateformes comme VMware, Nutanix ou KVM [Linux Kernel-based Virtual Machine]) avec des infrastructures à la fois sur site – ou dans un cloud privé – et dans le cloud public (comme Amazon Web Services [AWS], Google Cloud Platform [GCP], Microsoft Azure ou Alibaba). Un environnement multicloud, en revanche, utilise au moins deux clouds publics différents. Les clouds hybrides et environnements multicloud permettent aux données et aux applications de passer d'un environnement cloud à l'autre.

Il fut un temps – avant l'hégémonie du cloud computing – où les applications métiers étaient surtout stockées dans un centre de données centralisé. Avec la popularité croissante des applications SaaS (logiciel en tant que service), le trafic réseau des travailleurs distants et d'autres utilisateurs sur site devait transiter par ce centre de données (technique également appelée « hairpinning »), protégé par des pare-feux en périphérie.

Ce modèle centralisé n'est plus en phase avec les besoins actuels des entreprises en matière d'innovation, de rapidité et d'expérience client/utilisateur de qualité. À mesure que les entreprises migrent vers des environnements cloud hybrides et multicloud pour gagner en adaptabilité, ces problématiques se sont amplifiées. La surface d'attaque des entreprises s'est donc élargie, rendant la protection de cet environnement complexe, hyperconnecté et composé de multiples clouds de plus en plus difficile (voir figure 1-2).

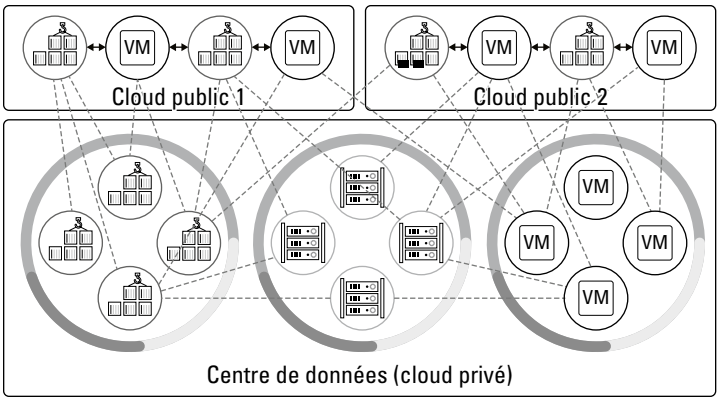


FIGURE 1-2 : Les environnements multicloud et hybrides hyperconnectés d'aujourd'hui.

Dans de nombreuses entreprises, le passage au cloud débute généralement par l'intégration d'applications SaaS tierces, que ce soit dans un but stratégique ou à cause de l'usage non autorisé de certaines technologies (Shadow IT) – voire les deux. Après cette étape, elles progressent naturellement vers la virtualisation de leur centre de données, en utilisant des technologies d'hyperviseur et de réseau défini par logiciel. Elles transfèrent ensuite leurs applications client/serveur classiques vers des machines virtuelles (VM) et des infrastructures de desktop virtuel (VDI).

Un grand nombre d'entreprises adoptent activement des solutions publiques d'infrastructure en tant que service (IaaS) pour concevoir des applications modernes dans le cadre d'une stratégie applicative ciblée.

Elles migrent ensuite leurs applications et leurs charges de travail sur site vers le cloud public, soit en les transférant telles quelles, soit en développant des solutions spécifiques au cloud, ou encore une combinaison des deux.

Enfin, les organisations exploitent souvent des solutions de plateforme en tant que service (PaaS) et d'autres innovations du cloud, comme la technologie sans serveur et la conteneurisation, qui sont désormais des composantes clés des architectures applicatives modernes. Au cours de cette transition, les entreprises découvrent rapidement que les pare-feux matériels traditionnels sur site ne sont pas adaptables à leurs centres de données virtualisés ni à leurs environnements cloud privés et publics. C'est là que les pare-feux logiciels deviennent pertinents.

RAPPEL

Le *Shadow IT* fait référence à l'emploi de technologies à l'insu ou sans l'approbation du service informatique. Cette pratique augmente les menaces liées à la sécurité et à la conformité au sein de l'entreprise, en plus de poser d'autres problèmes de gestion.

CONSEIL

Selon l'étude *ESG Research Report: Cloud-native Applications*, 88 % des organisations déploient actuellement des applications de production et des charges de travail sur des services d'infrastructure en cloud public.

Défis en matière de sécurité dans les environnements cloud et virtualisés

Les entreprises modernes mettent en œuvre des stratégies orientées vers le cloud afin de bénéficier de divers avantages tels que l'agilité, la flexibilité, l'innovation et la réduction des coûts. Cependant, le cloud et les environnements virtualisés créent également de nouveaux enjeux et risques que les entreprises se doivent de gérer. En voici quelques exemples :

- **Visibilité incomplète :** maintenir une visibilité complète représente un défi dans n'importe quel environnement, mais encore plus dans les environnements virtualisés et cloud. Habituellement, le trafic entre les machines virtuelles (VM) sur un même hôte physique ne fait que passer par l'hyperviseur, le logiciel responsable de la création et de l'exécution de ces machines. De plus, le trafic est-ouest entre les machines virtuelles au sein d'un centre de données virtualisé ou entre les clouds privés virtuels (VPC) dans des environnements cloud n'emprunte généralement pas les voies d'un pare-feu conçu pour inspecter et réguler le trafic réseau.

- **Segmentation limitée :** la segmentation logique des réseaux physiques s'effectue en général grâce à l'usage de réseaux locaux virtuels (VLAN) paramétrés sur les commutateurs réseau. Dans les environnements virtualisés et cloud, l'utilisation de VLAN est moins fréquente. À la place, la segmentation s'opère souvent par la mise en place de réseaux virtuels ou privés virtuels distincts. Toutefois, les connexions du fond de panier ainsi que le trafic transitant par l'hyperviseur restent en général ouverts et non segmentés au sein de la couche virtuelle.
- **Protection inadéquate :** les pare-feux de base et les outils comme les groupes de sécurité réseau fournissent uniquement des fonctions de filtrage élémentaires pour les ports, les sources et les protocoles. Ils sont incapables d'inspecter le contenu même du trafic, ce qui laisse la porte ouverte à la circulation de trafic malveillant non détecté.
- **Rapidité des DevOps :** les équipes chargées du développement d'applications font face à une pression incessante pour livrer de nouvelles solutions logicielles dans les plus brefs délais. L'automatisation du passage des applications à la production est devenue courante grâce à l'utilisation de pipelines d'intégration continue et de distribution continue (CI/CD), ainsi que d'infrastructures codifiées (IaC), permettant de monter et de démonter rapidement l'infrastructure applicative à grande échelle. Par conséquent, la sécurité peine souvent à suivre le rythme effréné de l'innovation en entreprise.

Examinons de plus près certains des défis de sécurité rencontrés dans les environnements virtualisés et cloud qui offrent des brèches potentielles pour les cybercriminels.

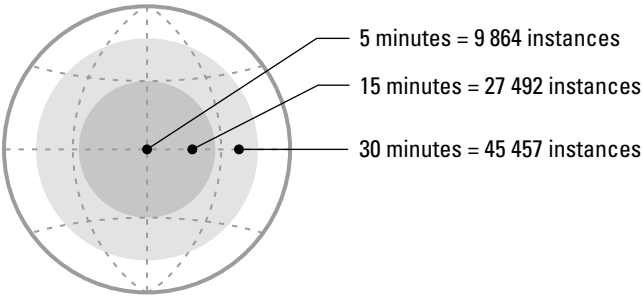
L'évolution et la modernité du paysage des menaces

Pour bon nombre d'entreprises, assurer la sécurité dans le cloud s'avère plus complexe que dans les environnements sur site traditionnels, en raison de divers facteurs. Par exemple :

- **Extension de la surface d'attaque :** la tendance à déployer des applications dans une variété d'environnements – associée au télétravail et à l'accès mobile des utilisateurs – élargit considérablement la surface d'attaque. De plus, l'expansion des applications intégrées dans la chaîne d'approvisionnement amplifie les risques, surtout lorsque les fournisseurs et partenaires négligent de maintenir un niveau de sécurité approprié au sein de leurs propres systèmes.
- **Des menaces plus sophistiquées :** les acteurs malveillants utilisent aujourd'hui des méthodes sophistiquées pour exploiter des failles et

échapper à la détection. Parmi ces techniques, on peut citer le chiffrement de logiciels malveillants, l'utilisation de canaux de commande et contrôle (C2), l'exploitation de failles « zero-day » et le recours à des variantes évolutives de logiciels malveillants, y compris celles intégrant de l'intelligence artificielle, pour éviter la détection. De plus, la montée en puissance du ransomware en tant que service (RaaS) a rendu possible la réalisation d'attaques complexes par presque n'importe quel cybercriminel, quel que soit son niveau d'expertise. Par conséquent, les attaques par ransomware, associées à l'exfiltration de données, figurent désormais parmi les menaces majeures à la sécurité du cloud.

- **Fenêtres d'action plus courtes :** le délai moyen de détection (MTTD) et le délai moyen de réponse (MTTR) sont souvent comptés en jours. Selon l'étude IBM Security *Cost of a Data Breach Report 2022*, la durée moyenne pour identifier et contenir une fuite de données est de 277 jours. Cependant, les ransomwares peuvent commencer à chiffrer les données en quelques minutes seulement après avoir infiltré le réseau et obtenu l'accès aux bases de données. Dans une étude récente menée par Unit 42 pour Palo Alto Networks, une menace avancée s'est propagée à plus de 45 000 instances en seulement 30 minutes (voir figure 1-3).



Source : Étude interne à Palo Alto Networks réalisée par Unit 42

FIGURE 1-3 : Des menaces sophistiquées prolifèrent rapidement dans les réseaux mal segmentés.

Une affaire de deux équipes

À mesure que les entreprises adoptent davantage les stratégies cloud, leurs équipes informatiques et de sécurité internes se transforment. Pour nombre d'entre elles, ce processus de transformation peut être complexe et éprouvant. Les différentes équipes au sein de l'organisation ont souvent des objectifs divergents, ce qui peut conduire à des tensions internes.

Les équipes dédiées au cloud sont généralement constituées d'architectes et d'ingénieurs spécialisés dans l'infrastructure et la sécurité cloud, ainsi que de professionnels DevOps et DevSecOps. Voici quelques-uns des défis majeurs auxquels ces équipes cloud sont confrontées :

- **Pression pour respecter les délais et la conformité :** les équipes DevOps et DevSecOps font face à une pression continue pour atteindre les objectifs métiers de manière agile, tout en respectant les réglementations gouvernementales provenant d'entités telles que le Department of Health and Human Services (HHS), la Food and Drug Administration (FDA) et la Securities and Exchange Commission (SEC) aux États-Unis. Elles doivent également respecter les normes de conformité de leur entreprise et celles de leur secteur.
- **Complexité du cloud :** le cloud représente une complexité, que l'équipe DevOps/DevSecOps travaille sur la migration d'applications existantes ou sur le développement de nouvelles applications. De plus, l'entreprise peut avoir recours à plusieurs environnements cloud, chacun ayant ses propres spécificités, allant de la conception du réseau aux architectures de calcul, de stockage et de réseau, sans oublier les modèles de responsabilité partagée en matière de sécurité.
- **Manque de spécialistes de la sécurité :** l'équipe DevOps/DevSecOps n'est pas toujours informée des menaces avancées susceptibles d'entraîner une violation de sécurité ni des solutions capables de contrer ces menaces. Souvent, cette équipe s'appuie sur les fonctionnalités de sécurité intégrées du fournisseur de services cloud (CSP), considérant qu'elles sont « suffisamment bonnes » par défaut, alors qu'elles se révèlent inefficaces face aux cybermenaces actuelles.

ATTENTION

Pour l'équipe responsable du cloud, les aspects liés au réseau et, par conséquent, à la sécurité du réseau ne font pas toujours partie des priorités. Cette attitude peut la conduire à négliger l'information sur ces produits, à ne pas interagir avec eux et même à ne pas les utiliser. De ce fait, les équipes cloud ont souvent tendance à déléguer la gestion de la sécurité du réseau à une autre équipe ou directement au fournisseur de services cloud (CSP).

Les équipes classiques de sécurité réseau sont en général composées d'architectes et d'ingénieurs spécialisés dans la sécurité des réseaux, ainsi que d'un responsable de l'infrastructure. Voici quelques-uns des défis fréquemment rencontrés par ces équipes dans les contextes du cloud et de la virtualisation :

- **Perte de contrôle :** à mesure que les applications sont transférées vers le cloud ou conçues de manière native dans celui-ci, l'équipe responsable de la sécurité du réseau voit son niveau de contrôle diminuer. L'autorité se déplace de plus en plus vers l'équipe en charge du cloud, qui est celle qui développe les plans pour la migration ou la création d'applications dans l'environnement cloud. Il arrive fréquemment que la sécurité soit omise de ces plans stratégiques ou pensée après coup.
- **Manque de visibilité :** les équipes de sécurité réseau manquent de visibilité sur les menaces dans les environnements multicloud. De nouvelles connexions réseau peuvent échapper à la surveillance et ne pas respecter les politiques de sécurité internes. De plus, la complexité des environnements cloud hybrides et multicloud peut entraîner la mise en place de diverses solutions de sécurité isolées, qui, à leur tour, créent des vulnérabilités et des lacunes dans la visibilité globale de l'infrastructure. Ce problème est dû à l'absence d'une interface unifiée pour corréler facilement les informations sur les menaces provenant de différentes sources.
- **Lutter contre l'idée que la sécurité des réseaux est trop difficile et n'en vaut pas la peine :** quand l'équipe responsable de la sécurité réseau suggère une solution de protection, elle doit démontrer que sa proposition n'entravera pas l'activité de l'entreprise et justifier l'effort supplémentaire par rapport à la sécurité de base, mais souvent jugée suffisante, offerte par le fournisseur de services cloud (CSP).
- **Manque de spécialistes du cloud :** les équipes chargées de la sécurité des réseaux manquent fréquemment d'expertise en matière d'infrastructures et/ou d'applications cloud. Souvent, elles n'ont pas les compétences nécessaires pour évaluer les produits de sécurité des réseaux en fonction de leur compatibilité avec les outils de sécurité automatisés, essentiels pour accompagner le cycle de développement des applications.

RAPPEL

L'équipe chargée de la sécurité du réseau est toujours tenue responsable des violations, mais elle n'a pas toujours l'autorité, le contrôle et la visibilité nécessaires pour résoudre les problèmes de sécurité dans le cloud, et encore moins dans plusieurs clouds. Ces problèmes sont souvent exacerbés par la réticence des équipes chargées du cloud qui craignent de ne pas respecter les délais.

Sécurité du cloud et sécurité dans le cloud

Dans un centre de données traditionnel ou un cloud privé, la sécurité de l'intégralité de l'infrastructure technologique, depuis le matériel jusqu'aux applications et aux données et leur connectivité, est de votre

ressort. Vous gérez aussi la sécurité physique (et la résilience) du centre de données, y compris le bâtiment, l'électricité, la climatisation et la connectivité Internet.

Les choses sont un peu différentes dans le cloud public. Le cadre du modèle de responsabilité partagée offre une structure claire pour distinguer les aspects de l'infrastructure technologique dans un service de cloud public (IaaS, PaaS ou SaaS) qui sont du ressort du fournisseur de services cloud (CSP) et ceux qui incombent au client. Même si le cadre du modèle de responsabilité partagée est en soi plutôt simple à saisir, sa mise en pratique – y compris les diverses options disponibles dans le cloud pour sécuriser vos services – peut s'avérer complexe et être source de vulnérabilités, même dans un environnement de cloud unique.

Par exemple, la majorité des fournisseurs de services cloud proposent des mesures de résilience des données, telles que le mirroring des disques pour prévenir la perte de données en cas de panne de disque, la haute disponibilité des machines virtuelles pour contrer les défaillances matérielles des serveurs, et des zones de disponibilité pour éliminer les risques de perte de données lors d'un incident dans un centre de données. Toutefois, ces mesures de protection des données sont mises en œuvre afin que le fournisseur de services cloud puisse honorer ses engagements de niveau de service (SLA) et assurer sa propre protection. Vous restez responsable de la sauvegarde de vos données. Si vos données sont chiffrées à la suite d'une attaque par ransomware, votre fournisseur de services cloud ne récupérera pas automatiquement une copie de vos données depuis une autre zone de disponibilité pour vous. Au lieu de cela, c'est à vous de restaurer vos données depuis une sauvegarde fiable que vous avez créée, et non le fournisseur de services cloud.

Dans chaque type de service cloud, que ce soit IaaS, PaaS ou SaaS, le fournisseur de services cloud est responsable de la gestion et de la sécurité de l'infrastructure de base de la plateforme, y compris les aspects liés au réseau, au stockage, au calcul et à la virtualisation de l'infrastructure technologique. Dans le cadre d'un modèle IaaS, c'est au client de gérer et de sécuriser tous les autres éléments, y compris les systèmes d'exploitation, les middlewares, les environnements d'exécution, les applications et les données. À l'opposé du spectre des modèles de service, dans un environnement SaaS, les clients n'ont à se soucier que de la sécurité de leurs données, tandis que le fournisseur de services cloud gère tout le reste (voir figure 1-4). Le CSP sécurise l'infrastructure de la plateforme. À cette fin, il utilise du matériel et des logiciels pour fournir des services réseau, de stockage, de calcul et de virtualisation, ainsi que des systèmes d'exploitation couramment utilisés comme Red Hat Enterprise Linux (RHEL) et Windows Server.

CONSEIL

Une autre perspective sur la sécurité du cloud et le modèle de responsabilité partagée consiste à dire que le fournisseur de services cloud assure la sécurité *du* cloud lui-même, alors que le client est en charge de la sécurité *dans* le cloud (voir figure 1-5).

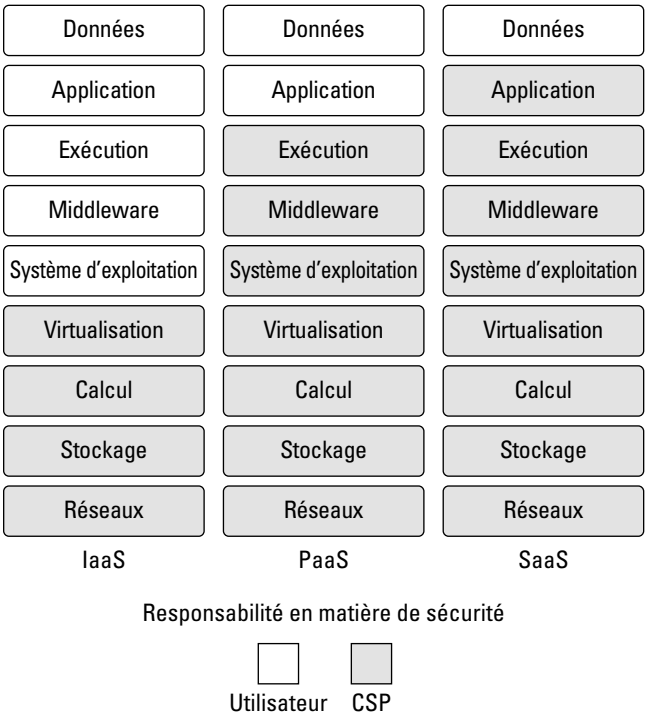


FIGURE 1-4 : Le modèle de responsabilité partagée.

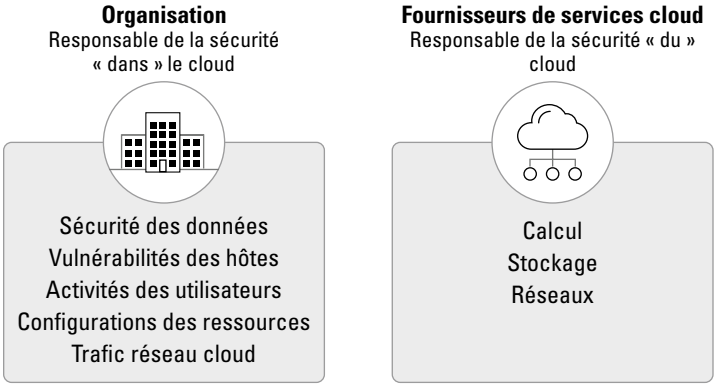


FIGURE 1-5 : Répartition des responsabilités en matière de sécurité dans le cloud public.

Exigences de conformité

Le cadre réglementaire ne cesse de se complexifier, intégrant constamment de nouvelles normes et lois liées à la sécurité et à la confidentialité. Parmi celles-ci, on compte la législation américaine Health Insurance Portability and Accountability Act (HIPAA), les normes de sécurité des données de l'industrie des cartes de paiement (PCI DSS), le Règlement Général sur la Protection des Données (RGPD) de l'Union européenne (UE) et la loi brésilienne sur la protection générale des données (LGPD). Ces réglementations sont régulièrement mises à jour et adoptées à l'échelle mondiale, touchant presque tous les pays, États et juridictions.

Le transfert d'applications et de données d'un centre de données sur site vers un environnement cloud public peut fortement influencer les politiques de conformité d'une organisation. D'un côté, des critères comme la localisation des données et l'exclusivité de leur hébergement peuvent complexifier les stratégies de conformité. Toutefois, dans bien des cas, vous pouvez tirer parti des mesures de sécurité déployées par le fournisseur de services cloud sur sa propre infrastructure, ainsi que des certifications qu'il a décrochées. Ce qui ne signifie pas que vous avez carte blanche. ***Rappel :*** dans le modèle de responsabilité partagée (évoqué plus haut dans ce chapitre), vous êtes toujours responsable de la sécurité (et de la confidentialité) de vos données.

RAPPEL

Une stratégie efficace de conformité dans des environnements cloud et virtualisés nécessite que les entreprises consolident la gestion de la sécurité pour harmoniser les politiques dans tous les contextes, y compris les infrastructures sur site, les filiales, les sites distants, les environnements virtualisés, ainsi que les clouds privés, publics, hybrides, les environnements multicloud et les espaces en périphérie du réseau.

Pour relever les défis modernes en matière de sécurité réseau, les organisations doivent adopter une stratégie Zero Trust (voir figure 1-6) qui s'étend à l'ensemble de la surface d'attaque de l'entreprise, y compris les environnements sur site et dans le cloud. J'explique comment utiliser le Zero Trust dans le chapitre 2.

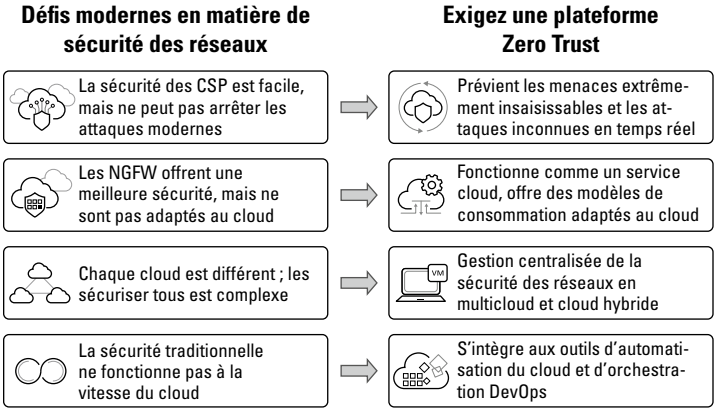


FIGURE 1-6 : Les défis modernes en matière de sécurité des réseaux requièrent une plateforme Zero Trust.

DANS CE CHAPITRE

- Définir le Zero Trust
- Démarrer avec une architecture Zero Trust et des pare-feux logiciels
- Protéger les applications cloud avec des pare-feux logiciels

Chapitre 2
Comprendre les pare-feux logiciels et le Zero Trust

Dans ce chapitre, vous découvrirez les notions de Zero Trust et d'accès avec le minimum de privilèges, le rôle des pare-feux logiciels dans l'établissement d'une stratégie Zero Trust, ainsi que la manière d'appliquer le Zero Trust aux environnements cloud et virtualisés (publics, privés, hybrides) grâce à l'utilisation de pare-feux logiciels.

Qu'est-ce que le Zero Trust ?

Le Zero Trust est une approche stratégique en matière de cybersécurité qui élimine la confiance implicite, valide en permanence les identités des utilisateurs et des objets, et applique un accès avec le minimum de privilèges tout au long d'une session numérique. Basé sur le principe « ne jamais faire confiance, toujours vérifier », le modèle Zero Trust vise à sécuriser les environnements modernes et à faciliter la transformation digitale. Il atteint cet objectif en utilisant des méthodes d'authentification robustes, en exploitant la segmentation réseau, en limitant les déplacements latéraux, en assurant une prévention des

menaces pour la couche d'application (couche 7) et en établissant des stratégies d'accès à la fois simples et intuitives, mais puissantes, basées sur le principe du moindre privilège.

RAPPEL

Dans un environnement Zero Trust, tous les éléments comme les appareils, les utilisateurs, les applications, les charges de travail et les flux de données sont perçus comme des risques potentiels qui doivent être constamment authentifiés et autorisés, et l'inspection des transactions numériques doit intervenir tout au long de la session.

QU'EST-CE QU'UN ACCÈS AVEC LE MINIMUM DE PRIVILÈGES ?

Une bonne pratique de sécurité lors de la configuration des rôles et des privilèges pour tout environnement logiciel est d'appliquer un accès avec le minimum de privilèges. Autrement dit, en suivant le principe du moindre privilège, vous vous assurez que chaque utilisateur ou groupe ne détient que les droits et autorisations d'accès strictement nécessaires pour accomplir ses fonctions au sein de l'organisation.

Les avantages du moindre privilège

Le principal avantage du moindre privilège est qu'il limite les dommages potentiels causés par une violation de la sécurité. Dans un environnement où un utilisateur dispose d'un accès à davantage de ressources que nécessaire, toute personne réussissant à pirater ce compte utilisateur obtiendra également un accès à ces systèmes. En ne donnant que les autorisations strictement nécessaires, vous réduirez les risques en cas de compromission.

L'accès avec le minimum de privilèges peut également simplifier les audits. En appliquant ce principe, vous pouvez effectuer des audits de vos stratégies d'accès afin de déterminer si certaines d'entre elles accordent aux utilisateurs plus de droits d'accès qu'ils n'en ont besoin. Vous pouvez ensuite prendre des mesures pour atténuer le risque.

Exemple d'accès avec le minimum de privilèges

Pour comprendre ce que signifie le moindre privilège dans la pratique, examinons un environnement cloud utilisé par plusieurs collaborateurs au sein d'une entreprise. Certains utilisateurs sont des développeurs, d'autres des ingénieurs informatiques. Les développeurs utilisent un ensemble de machines virtuelles (VM) destinées au développement et aux tests pour concevoir et évaluer des applications. Les ingénieurs informatiques utilisent un autre groupe de machines pour déployer des applications destinées à la production.

Pour configurer un accès avec le minimum de privilèges dans cette situation, il vous faut définir les rôles et les politiques de gestion des identités et des accès (GIA) dans le cloud de façon à ce que les développeurs soient uniquement habilités à créer, modifier et lancer les machines virtuelles qu'ils utilisent spécifiquement pour le développement et les tests. De même, les ingénieurs informatiques ne peuvent accéder qu'aux machines virtuelles de production.

Le contraire du moindre privilège dans cet exemple serait de créer des règles GIA qui donnent à tous les membres de l'équipe l'accès à toutes les VM. On peut envisager que les développeurs devront occasionnellement accéder aux machines virtuelles de production, tandis que les ingénieurs informatiques souhaiteront parfois examiner l'environnement de développement et de test. Toutefois, cette approche augmenterait l'impact potentiel d'une violation de la sécurité. Si le compte d'un développeur est compromis, par exemple, les cybercriminels pourront accéder à toutes les machines virtuelles de l'environnement auxquelles ce compte a accès. Avec la mise en place du principe du moindre privilège, seuls les environnements de développement et de test seront accessibles.

Les principes du Zero Trust remettent en question l'idée obsolète que tout ce qui est interne au réseau d'une organisation doit être automatiquement considéré comme sûr, une hypothèse sur laquelle se basent les modèles de sécurité traditionnels axés sur le périmètre. Cette confiance présumée implique que, une fois connectés au réseau, les utilisateurs — y compris les cybercriminels et les acteurs malintentionnés en interne — peuvent naviguer librement et accéder à des informations sensibles ou les exfiltrer, faute de mécanismes de sécurité spécifiques et rigoureux.

De nos jours, un grand nombre d'organisations investissent énormément de temps et de ressources pour identifier et réduire leur surface d'exposition aux attaques, laquelle ne cesse de s'agrandir. Avec la multiplication des objets connectés, des appareils mobiles et du télétravail, ce défi est devenu considérablement plus complexe.

Plutôt que de s'efforcer de contrôler une surface d'attaque en expansion constante, les principes du Zero Trust mettent l'accent sur la surface à protéger, qui regroupe les ressources vitales de l'entreprise et qui peut concerner un ou plusieurs des éléments suivants :

- Utilisateurs
- Applications
- Infrastructure

La surface à protéger dans une entreprise est nettement plus réduite que sa surface d'attaque, ce qui la rend bien plus simple à identifier (voir figure 2-1). Plutôt que de bâtir un périmètre unique à grande échelle pour défendre l'ensemble de la surface d'attaque, le Zero Trust instaure plusieurs micro-périmètres, positionnés au plus près de la surface à protéger. Ces micro-périmètres accompagnent la surface de protection via des passerelles de segmentation, qui limitent l'accès uniquement au trafic et aux applications préalablement approuvés.

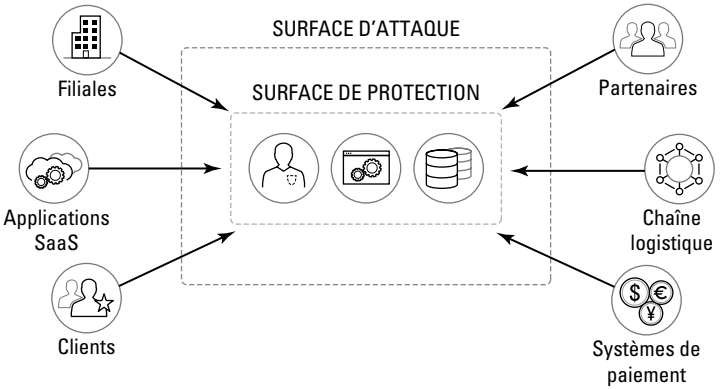


FIGURE 2-1 : Les principes du Zero Trust réduisent le nombre de points d'entrée potentiels pour les cyberattaques.

CONSEIL

Face à l'accélération de la transformation digitale, manifeste à travers une main-d'œuvre hybride en expansion, une migration incessante vers le cloud et l'évolution des pratiques de sécurité, l'adoption d'une stratégie Zero Trust est plus importante que jamais. Lorsqu'elle est correctement déployée, une architecture Zero Trust entraîne non seulement une amélioration significative du niveau global de sécurité, mais aussi une simplification de la gestion de la sécurité et une réduction des coûts opérationnels.

En quoi les pare-feux logiciels facilitent-ils la mise en place d'une architecture Zero Trust ?

Dans le cadre d'une stratégie Zero Trust, il est indispensable de créer des micro-périmètres proches des utilisateurs, des applications et de l'infrastructure en établissant ainsi une surface de protection bien définie et gérable permettant d'appliquer la sécurité. Évidemment, la surface de protection peut être particulièrement volatile et mobile, surtout dans le

cas d'applications contemporaines et cloud qui utilisent des microservices, des containers et des architectures capables de s'adapter élastiquement. Les pare-feux matériels classiques, physiques et centrés sur le périmètre, sont donc peu compatibles avec une bonne stratégie Zero Trust.

Les pare-feux nouvelle génération (NGFW) définis par logiciel peuvent être intégrés dans une stratégie Zero Trust pour créer des micro-périmètres autour des zones de protection en constante évolution au sein des différents environnements de l'entreprise. Cette stratégie concerne les centres de données physiques et virtualisés, les bureaux annexes et les sites distants, tout comme les environnements cloud privés, publics, hybrides, en périphérie et multicloud.

CONSEIL

Encore récemment, les pare-feux nouvelle génération étaient déployés uniquement sous la forme d'appliances physiques. Cependant, vous ne pouvez pas déployer des appliances matérielles dans des environnements virtualisés et de cloud public, ni les déplacer de manière dynamique avec vos données, actifs, applications et services stratégiques. Les pare-feux logiciels sont la solution idéale pour une stratégie Zero Trust, adaptée à tous types de cloud, qu'il s'agisse de cloud public, de cloud privé, de cloud hybride combinant des infrastructures sur site et dans le cloud, ou encore d'environnements multicloud.

Appliquer les principes du Zero Trust aux applications cloud

Les pare-feux réseau classiques étaient basés sur du matériel physique et destinés à établir une sécurité périmétrique entre le réseau interne de l'entreprise, considéré comme sûr, et l'Internet jugé peu fiable. Beaucoup de choses ont changé au cours des deux dernières décennies, et cette notion de confiance implicite et de périmètres bien définis n'est plus valable. En fait, elle est même dangereuse. En outre, les pare-feux matériels physiques traditionnels ne peuvent pas être déployés dans un environnement virtualisé ou cloud.

Comme évoqué précédemment, les approches Zero Trust nécessitent que l'organisation délimite des zones de protection spécifiques et instaure une micro-segmentation entre ses utilisateurs, applications et infrastructures. Même si l'environnement se réduit à un petit centre de données sur site, déployer des pare-feux matériels pour sécuriser chaque utilisateur, chaque application et chaque élément d'infrastructure serait impraticable. Dans le cloud public, c'est impossible – vous ne pouvez pas déployer votre propre matériel dans le cloud.

Les pare-feux logiciels offrent une solution pratique qui permet aux organisations de mettre en œuvre une stratégie Zero Trust dans leurs centres de données sur site et d'étendre également cette stratégie à leurs applications hébergées dans le cloud.

RAPPEL

Les pare-feux logiciels répondent au problème de déploiement du matériel dans le cloud public, mais aussi à la nature éphémère et transitoire des applications cloud et cloud natives (et des microservices associés), qui n'existent parfois que quelques secondes ou minutes, et peuvent se déplacer dynamiquement vers plusieurs machines virtuelles, containers ou régions, voire différents clouds.

DANS CE CHAPITRE

- **Prendre un bon départ avec les pare-feux virtuels**
- **Exploiter les pare-feux cloud**
- **Étendre les pare-feux logiciels aux environnements Kubernetes avec des pare-feux de containers.**
- **Renforcer vos capacités avec des services de sécurité fournis par le cloud**

Chapitre 3
Découvrir les types de pare-feux logiciels

Dans ce chapitre, nous aborderons les diverses catégories de pare-feux logiciels, notamment les pare-feux pour environnements virtuels, les containers et le cloud. Ces solutions répondent à une variété de besoins et de scénarios spécifiques au sein des entreprises.

Pare-feux virtuels

Les pare-feux nouvelle génération (NGFW) virtuels proposent l'ensemble des fonctionnalités des pare-feux physiques, mais sous la forme d'une machine virtuelle (VM). Voici quelques-unes des principales fonctionnalités des pare-feux virtuels :

- **Répondez de manière cohérente aux exigences de sécurité du cloud.** Protégez les systèmes d'exploitation, les plateformes, l'accès, le contrôle, les données et bien plus encore contre les menaces connues et inconnues, afin de respecter vos obligations en matière de sécurité dans le cadre du modèle de responsabilité partagée d'un fournisseur de services cloud (voir le chapitre 1) et de maintenir la conformité interne, sectorielle et gouvernementale.

- **Sécurisez les ressources virtualisées et les hyperviseurs.** Bloquez les mouvements latéraux des cybermenaces entre les applications et les charges de travail grâce à la segmentation, la micro-segmentation et aux inspections continues du trafic dans les environnements virtualisés et cloud.
- **Simplifiez la gestion.** Isolez et protégez les systèmes stratégiques grâce à des politiques cohérentes de prévention des menaces et de sécurité accessibles à partir de la même console dans tous vos environnements cloud (cloud privé, cloud public, multicloud et cloud hybride).
- **Adaptez votre sécurité à la taille de votre entreprise.** Intégrez le provisionnement automatisé de la sécurité directement dans les workflow DevOps et les pipelines d'intégration continue/distribution continue (CI/CD) pour favoriser la souplesse de l'entreprise.

US Signal protège les informations sensibles

US Signal est un acteur majeur dans le domaine des services de centre de données et de cloud computing. Avec huit centres de données dans le Midwest, l'entreprise héberge des solutions cloud, fournit des espaces de colocation et offre des services de sécurité de pointe alimentés par son propre réseau de fibre sécurisé et robuste.

L'enjeu

En 2020, US Signal a décidé d'étendre son empreinte cloud et ses capacités de protection des données. L'entreprise avait enregistré une croissance de 300 % de ses activités de centre de données en cinq ans et cherchait à répondre à la demande croissante de ses clients pour ses services, à une période où de nombreuses entreprises migraient vers le cloud pour favoriser le télétravail.

À l'époque, US Signal utilisait plusieurs plateformes de pare-feu de plusieurs fournisseurs. Dans le cadre de son expansion, US Signal souhaitait consolider ses plateformes et travailler avec un seul fournisseur. De cette manière, ses ingénieurs pourraient se concentrer sur un système unifié et bénéficier d'une vue globale de la structure de sécurité de l'entreprise, sans avoir à maîtriser plusieurs systèmes différents.

L'entreprise souhaitait également tirer parti de l'automatisation pour réduire davantage le risque d'erreurs humaines, diminuer les frais généraux et alléger la charge de travail de ses ingénieurs. Le provisionnement des pare-feux pour les clients était un processus lourd et fastidieux. Grâce

à l'automatisation, l'équipe serait donc en mesure d'en faire plus avec moins et d'accélérer les déploiements.

Besoins

US Signal a évalué tous les principaux fournisseurs de solutions de sécurité. Pour être prise en considération, une solution devait fonctionner dans un environnement d'hyperviseur bare-metal VMware ESXi pour vSphere. La sécurité optimale était une condition sine qua non, puisque la solution retenue devait veiller à la protection de l'infrastructure d'US Signal autant que de celle de ses clients. L'évolutivité était également cruciale pour répondre aux besoins d'expansion de l'entreprise. En outre, US Signal a jugé que les mises à jour en temps réel étaient essentielles pour doter les pare-feux virtuels des dernières fonctions de sécurité et des renseignements les plus récents sur les menaces. La facilité d'automatisation était aussi extrêmement importante, car l'entreprise déploie des pare-feux virtuels pour des centaines de clients. La gestion des licences et le niveau de prix étaient également des facteurs clés.

Solution

US Signal a choisi les pare-feux nouvelle génération (NGFW) VM-Series de Palo Alto Networks pour assurer une sécurité réseau Zero Trust complète à la fois pour son infrastructure informatique interne et pour les offres de produits qu'elle déploie auprès de ses clients. En tirant parti du provisionnement automatisé de Palo Alto Networks et de l'intégration avec les produits d'orchestration Ansible et Terraform, US Signal a déployé chaque pare-feu virtuel avec une suite complète de services de sécurité fournis par le cloud. Ces services comprennent GlobalProtect pour protéger les utilisateurs mobiles, WildFire pour l'analyse avancée des logiciels malveillants, la prévention des menaces, le filtrage avancé des URL (Uniform Resource Locator) et la sécurité DNS pour sécuriser le trafic et prévenir les attaques sophistiquées connues et inconnues.

Impact

Le déploiement des NGFW Palo Alto Networks VM-Series a eu un impact significatif, avec notamment les avantages suivants :

- Temps de provisionnement des pare-feux réduit de 97 % grâce à une automatisation avancée
- Décisions d'achat des clients accélérées grâce à des NGFW virtuels riches en fonctionnalités
- Confiance des clients renforcée par une sécurité avancée dans le cloud
- Protection contre les menaces de type « zero-day » avec des opérations ininterrompues
- Avantage concurrentiel et croissance continue grâce à des solutions de sécurité hors pair

Pare-feux cloud

Les pare-feux cloud proposent une grande partie des mêmes options que l'on retrouve dans un NGFW physique ou virtuel, mais peuvent être déployés et ajustés en quelques minutes grâce à quelques clics intuitifs pour un développeur habitué au cloud. En utilisant les pare-feux comme services cloud, les entreprises peuvent réaliser des économies en éliminant les besoins d'installation ou de maintenance du matériel de sécurité ou des pare-feux logiciels de toute leur organisation.

Les pare-feux cloud, optimisés par un pare-feu virtuel, offrent une sécurité de haut niveau pour les équipes de sécurité réseau et s'intègrent étroitement aux environnements des fournisseurs de services cloud, offrant ainsi une utilisation facile et cloud-native pour les équipes DevOps (voir figure 3-1).

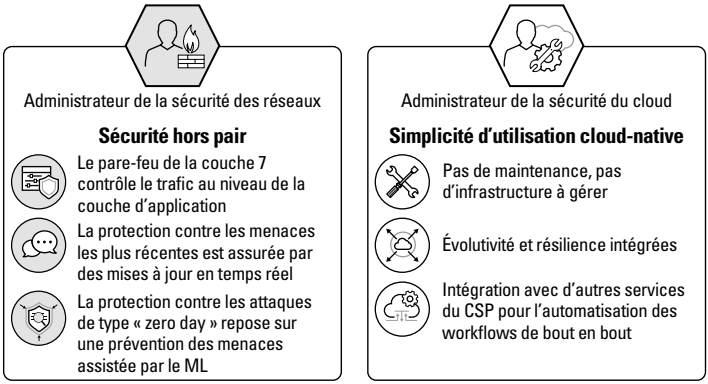


FIGURE 3-1 : Les entreprises d'aujourd'hui exigent à la fois une sécurité haut de gamme et une utilisation simple et cloud-native.

L'approche du pare-feu cloud donne aux entreprises les avantages suivants :

- Garantir une visibilité et un contrôle absolus sur tous leurs réseaux, sans devoir déployer d'appliances physiques, en abaissant par conséquent les frais de support.
- Assurer automatiquement l'évolutivité et la résilience sans avoir à gérer d'infrastructure.
- Tirer parti d'un service facile à utiliser en mode cloud avec une grande efficacité en temps réel intégrée et une mise à l'échelle contre les cyberattaques modernes.

Par exemple, Palo Alto Networks propose ces pare-feux cloud en partenariat avec des fournisseurs de services cloud, des partenariats avec des éditeurs de logiciels intégrés (ISV) appelés Cloud NGFW, pour une utilisation dans les environnements AWS et Microsoft Azure, et des partenariats OEM en marque blanche avec Google Cloud et Oracle Cloud Infrastructure.

Alors, en quoi ces pare-feux cloud diffèrent-ils des autres pare-feux logiciels ? Premièrement, ces services sont achetés directement sur les marchés où les fournisseurs de services cloud répertorient et proposent des solutions d'éditeurs indépendants de logiciels (ISV) qui fonctionnent comme des services natifs du cloud. Ces solutions sont ainsi faciles à déployer, à exploiter et à automatiser dans ces environnements. De plus, une fois les décisions d'achat prises, les utilisateurs restent dans ces portails pour configurer et déployer rapidement les pare-feux cloud, ainsi que des éléments tels que les rulestacks et les profils de sécurité automatisés. Les interfaces utilisateur cloud natives peuvent exécuter le processus de déploiement et de configuration en quelques minutes.

Lorsque ces pare-feux cloud sont étroitement intégrés au fournisseur de services cloud, les utilisateurs ont accès à des fonctionnalités de sécurité conçues spécialement pour ces environnements particuliers. Comme vous le lirez dans la section suivante sur les services de sécurité fournis par le cloud, ces fonctionnalités peuvent :

- Contribuer à stopper les menaces de type « zero-day » en temps réel.
- Sécuriser les applications lorsqu'elles se connectent à des services web légitimes grâce à la sécurité deep learning inline.
- Contrôler le trafic et n'autoriser que les applications autorisées à traverser le réseau grâce à la classification de la couche 7 (couche d'application).
- Arrêter l'exploitation des vulnérabilités et les attaques sophistiquées, les exploits inconnus, les logiciels espions, ainsi que les logiciels malveillants et les communications de commande et contrôle (C2).
- Prévenir et détecter les menaces basées sur les fichiers en utilisant des techniques d'analyse dynamique, statique et par machine learning.
- Contrer les attaques de la couche DNS les plus avancées qui exploitent les réseaux des clients et volent leurs données.

Une fois déployés dans l'environnement du fournisseur de services cloud, les pare-feux cloud répondent aux besoins de sécurité bien réels des entreprises qui déploient des applications et stockent des données

stratégiques dans le cloud public. Ces pare-feux logiciels renforcent bien entendu la sécurité et s'intègrent aux services intégrés du fournisseur de services cloud pour l'automatisation et l'évolutivité. Qui plus est, les pare-feux cloud permettent une gestion simple et cohérente des règles de pare-feu sur les sites où résident les applications.

Comme les entreprises gèrent fréquemment des applications à la fois sur site et dans des clouds publics, les pare-feux cloud sophistiqués peuvent être dotés de systèmes de gestion qui assurent une sécurité réseau complète dans l'ensemble de ces environnements. Ainsi, les entreprises peuvent éviter d'avoir plusieurs consoles pour différents sites. De nombreuses organisations ont passé des années à renforcer leur stratégie de sécurité sur site et sont naturellement réticentes à l'idée de repartir de zéro avec de nouvelles politiques et procédures spécifiques au cloud. Lorsqu'elle est bien réalisée, la gestion unifiée permet de gérer de manière centralisée tous les pare-feux nouvelle génération (NGFW) dans tous les environnements, y compris ceux des fournisseurs de services cloud spécifiques.

Pare-feux de containers

Les technologies de conteneurisation et d'orchestration sont largement utilisées dans le cloud pour fournir des applications cloud natives modernes à grande échelle. Les pare-feux réseau traditionnels n'ont pas été conçus pour répondre aux exigences de ces environnements extrêmement vastes, complexes et souples.

JARGON TECHNIQUE

Kubernetes est un système d'orchestration de containers open source très répandu. Dans Kubernetes, les containers s'exécutent sur des nœuds de ressources, qui peuvent être soit des machines physiques, soit plus fréquemment, des machines virtuelles. Les espaces de noms servent à segmenter les ressources au sein de Kubernetes. Ils peuvent isoler les pods, ainsi que les services, le stockage et les annotations. Les développeurs ont rarement affaire à des nœuds, mais les nœuds ont un impact sur le fonctionnement des pare-feux. Les pare-feux qui s'exécutent à l'extérieur du cluster Kubernetes géré ne peuvent pas déterminer quel pod de containers est la source du trafic sortant, car toutes les adresses IP source sont traduites vers l'adresse IP du nœud. Ainsi, pour un pare-feu extérieur au cluster Kubernetes, tout le trafic sortant du nœud semble identique. C'est un peu comme la traduction d'adresse réseau (NAT) sur un commutateur réseau, qui convertit toutes les adresses IP privées en une seule adresse IP publique, avant que le trafic n'atteigne le pare-feu (voir figure 3-2).

En outre, le trafic est-ouest entre les microservices au sein d'un environnement Kubernetes ne quitte jamais le périmètre du cluster ; le pare-feu n'inspecte donc pas le trafic entre les pods.

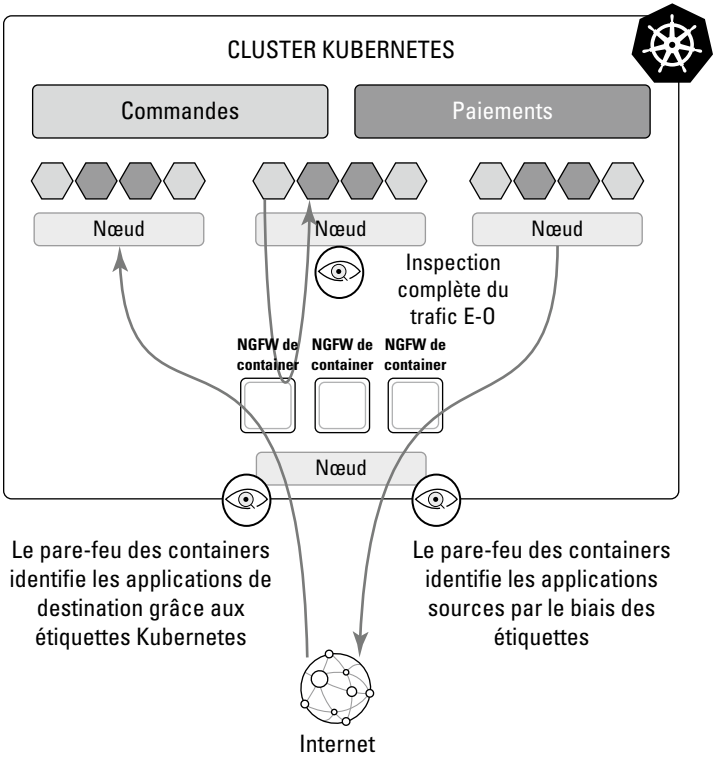


FIGURE 3-2 : En raison de l'utilisation de la NAT dans Kubernetes, tout le trafic sortant est identifié par l'adresse IP source du nœud.

Kubernetes pose des défis aux outils de sécurité traditionnels, mais il offre également de nouvelles opportunités pour renforcer la sécurité. Par exemple, les espaces de noms Kubernetes permettent de simplifier la gestion des clusters en facilitant l'application de certaines politiques à des parties spécifiques d'un cluster. Les équipes de sécurité peuvent utiliser les espaces de noms pour isoler les charges de travail et réduire le risque de propagation d'une attaque au sein d'un cluster.

Les espaces de noms peuvent aussi servir à établir des quotas de ressources, ce qui permet de minimiser les dégâts d'une éventuelle

intrusion dans le cluster qui affecterait d'autres containers et de contrer les programmes malveillants exploitant des containers mal configurés.

Une solution de sécurité complète pour les environnements conteneurisés doit être capable de protéger le trafic qui franchit les limites des espaces de noms dans Kubernetes, ainsi que le trafic en direction d'autres charges de travail dans le cloud et sur site, comme les machines virtuelles, les serveurs bare-metal et les dépôts de code externes tels que GitHub. En outre, les pods Kubernetes peuvent également servir d'applications pour les clients (trafic entrant). Les pare-feux virtuels situés à l'extérieur du cluster, par exemple, ne pourront pas appliquer de manière unique des règles de trafic spécifiques à chaque application ou espace de noms. Cette fonctionnalité nécessite des informations sur l'état interne des objets tels que les espaces de noms, les pods et les containers. Cependant, ces informations ne sont pas disponibles en dehors de l'environnement Kubernetes. Ainsi, pour répondre au principe de l'architecture Zero Trust qui consiste à protéger les charges de

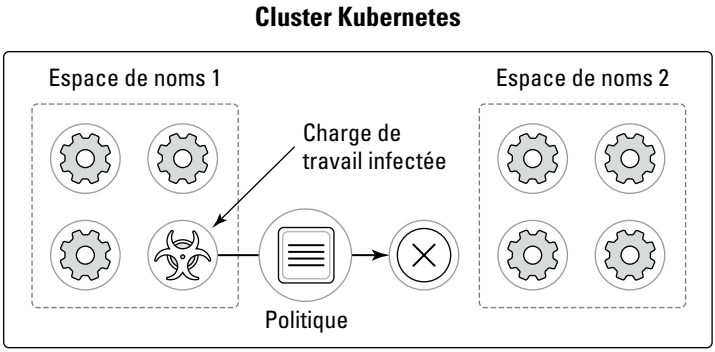


FIGURE 3-3 : Les stratégies de sécurité basées sur les espaces de noms empêchent la propagation d'une attaque au sein d'un cluster.

travail au plus près de la charge, la seule solution efficace consiste à déployer une solution de pare-feu de containers *au sein* des environnements Kubernetes (voir figure 3-3).

CONSEIL

Les configurations en cluster conviennent davantage aux grands environnements Kubernetes, là où un déploiement distribué serait trop coûteux et consommerait beaucoup de ressources.

RAPPEL

L'intégration native avec Kubernetes permet aux pare-feux de containers de se servir des données contextuelles sur ces derniers afin d'élaborer des stratégies de sécurité. Par exemple, vous pouvez utiliser les espaces de noms des containers comme critères pour identifier l'origine du trafic dans une règle de pare-feu.

Services de sécurité fournis dans le cloud

Pour que la cybersécurité soit omniprésente, elle doit être fournie sous la forme d'un service hébergé dans le cloud. Dans ce cas, les solutions de cybersécurité peuvent tirer parti de la flexibilité du cloud pour fournir une évolutivité adaptée aux entreprises modernes en pleine croissance. Elles peuvent également utiliser des renseignements sur les menaces (threat intelligence) collectés à l'échelle globale et des algorithmes de machine learning pour offrir une protection en temps réel contre des menaces, qu'elles soient connues ou non.

CONSEIL

Les services de sécurité fournis par Palo Alto Networks dans le cloud sont nativement intégrés, offrant partout une protection cohérente de haute qualité basée sur l'intelligence artificielle (IA) et le machine learning (ML). Soutenus par l'équipe de recherche sur les menaces Unit 42 de Palo Alto Networks et par un réseau de plus de 85 000 clients dans le monde, les renseignements sont partagés à partir de tous les vecteurs de menaces pour arrêter les menaces connues, inconnues et de type « zero day » 180 fois plus vite que les autres solutions. Voici les principaux services de sécurité fournis dans le cloud par Palo Alto Networks :

- **Le service de prévention des menaces avancées** empêche toutes les menaces connues et les exploits de type « zero day » sur l'ensemble du trafic en un seul passage.
- **Le sandbox WildFire avancé** gère les menaces inconnues.
- **Le service de filtrage avancé des URL** permet aux utilisateurs d'accéder en toute sécurité à l'Internet, où qu'ils se trouvent, en bloquant l'accès aux sites web malveillants connus ou non.
- **Le service de sécurité DNS** contre les attaques qui utilisent le DNS pour le trafic de commande et contrôle (C2) et le vol de données.
- **Le service de sécurité de l'Internet des Objets (IoT)** assure la visibilité, la prévention et la mise en conformité pour les appareils IoT et la technologie opérationnelle (OT).
- **Le service de sécurité Software as a Service (Logiciel en tant que service, SaaS)** fournit une visibilité complète et un contrôle précis sur toutes les actions des utilisateurs, ainsi que sur les dossiers et fichiers au sein des applications SaaS.

- **Le service de prévention des pertes de données (DLP) en entreprise** identifie, contrôle et sécurise l'ensemble des informations sensibles, tout en facilitant la conformité à travers les réseaux, les environnements cloud et les utilisateurs.
- **Le service de réseau étendu défini par logiciel (SD-WAN)** simplifie la gestion, autorise des règles précises par application et déploie des sites distants sécurisés dans le cloud.

DANS CE CHAPITRE

- Sécuriser l'infrastructure du cloud public
- Protéger votre cloud privé
- Déployer des pare-feux logiciels dans des environnements de cloud hybride et multicloud
- Étendre les pare-feux logiciels aux filiales
- Protéger les réseaux 5G

Chapitre 4
Découvrir les cas d'usage des pare-feux logiciels

Dans ce chapitre, vous découvrirez des cas d'usage fréquents des pare-feux logiciels, y compris dans les environnements de cloud public, privé, hybride et multicloud, les filiales virtualisées et les réseaux 5G.

Cloud public

Les fournisseurs de services cloud (CSP) publics vendent des ressources telles que des cycles de calcul et des unités de stockage sur un modèle de paiement à l'utilisation. Le matériel et les logiciels qui composent la plateforme demeurent invisibles pour vous. Ainsi, votre équipe n'a accès qu'à une représentation abstraite de vos applications et de vos données. Les avantages sont considérables : en évitant les investissements en capital et les cycles de mise à jour onéreux, vous profitez d'une évolutivité quasiment sans limites, d'une fiabilité élevée, d'une sauvegarde sécurisée des données et d'une flexibilité importante pour votre entreprise.

Les prochaines sections examinent quelques cas d'usage et enjeux de sécurité les plus importants dans les environnements de cloud public, ainsi que la façon dont les pare-feux nouvelle génération (NGFW) gérés par des logiciels – comme les pare-feux virtuels, les pare-feux de containers et les pare-feux cloud – permettent de surmonter ces défis.

La sécurité des applications détecte les menaces difficiles à trouver

Les pare-feux qui utilisent le protocole Internet (IP) et l'analyse des ports, ainsi que les groupes de sécurité réseau mis en place par les fournisseurs de services cloud (CSP) manquent de visibilité au niveau des applications dans le trafic réseau et ont des capacités limitées pour prévenir les menaces. De ce fait, les groupes de sécurité intégrés au cloud ne parviendront pas à identifier les menaces exploitant des ports ouverts (par exemple, les ports 80 et 443), ou visant des failles dans des applications non-web.

Les pare-feux logiciels déployés dans le cloud public sous forme de pare-feux virtuels, de containers et cloud, examinent chaque paquet entrant et filtrent le trafic suspect selon le type d'application, de contenu ou l'identité de l'utilisateur/appareil. Ils offrent une protection supérieure au simple blocage de port en sécurisant le trafic sur les ports ouverts. Ces outils offrent également des fonctionnalités de sécurité avancées, comme un système de prévention des intrusions (IPS) et le sandboxing, afin de lutter contre les failles identifiées ou non à la périphérie et au sein d'un environnement de cloud public.

RAPPEL

Les NGFW logiciels possèdent toutes les fonctionnalités des NGFW matériels. En outre, ils sont capables de suivre automatiquement l'évolution dynamique des applications et des charges de travail virtualisées et conteneurisées dans les environnements de cloud public, privé et hybride, à mesure que la demande d'applications augmente ou diminue.

La protection du trafic sortant empêche l'exfiltration

Afin d'extraire les données d'un environnement cible suite à une violation, les cybercriminels exploitent fréquemment les flux de trafic chiffrés autorisés par l'organisation, tels que le chiffrement SSL (Secure Sockets Layer) ou TLS (Transport Layer Security), pour protéger les données lorsqu'elles quittent l'environnement. Par exemple, après avoir accédé à votre environnement, un cybercriminel identifie des informations précieuses et utilise une technique de tunneling du système de noms de domaine (DNS) pour les exfiltrer de l'application compromise en cachant les données dans le trafic DNS/C2 chiffré.

CONSEIL

Les pare-feux logiciels peuvent déchiffrer le trafic pour l'inspection du contenu sortant. Le service de sécurité DNS, mentionné dans le chapitre 3, assure même l'inspection et la protection des flux de trafic chiffrés autorisés.

Le filtrage et l'inspection renforcent la sécurité des développeurs

Les offres de pare-feu natives des fournisseurs de services de cloud ont généralement des capacités limitées pour filtrer et examiner le trafic sortant de l'environnement cloud. Par conséquent, si les développeurs téléchargent un code open source compromis à partir d'un dépôt de code public, ils peuvent involontairement introduire des logiciels malveillants dans l'environnement de développement. Une fois ces vulnérabilités introduites dans le code de l'application, les cybercriminels peuvent se déplacer latéralement pour localiser les informations à exfiltrer.

CONSEIL

Les services de filtrage d'URL (Uniform Resource Locator) avancés proposés dans le cloud (abordés au chapitre 3), déployés sur des pare-feux logiciels dans le cloud public, garantissent que les développeurs n'accèdent qu'à des dépôts de qualité connue qui sont maintenus et sécurisés en interne (voir figure 4-1).

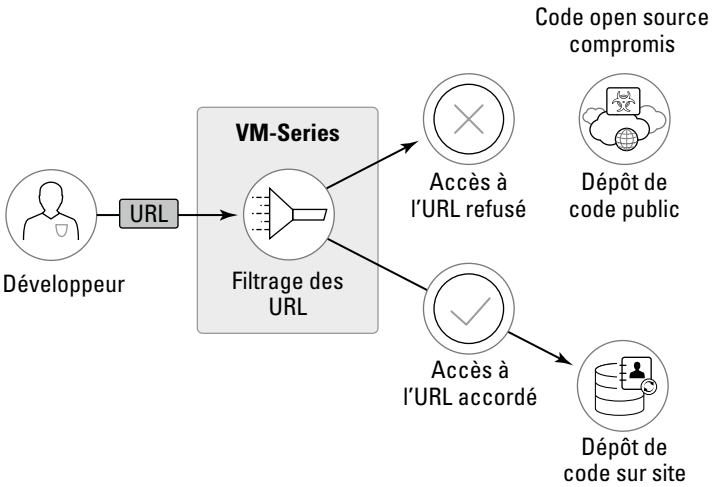


FIGURE 4-1 : Des services de filtrage avancé des URL empêchent les développeurs d'accéder à du code compromis dans un dépôt public.

Cloud privé

Si une organisation nécessite un contrôle plus poussé de ses applications et de ses données que celui proposé par le cloud public, elle peut se tourner vers le cloud privé. Ce dernier offre une multitude d'avantages semblables, mais sans les complications liées à l'architecture mutualisée, à la localisation des données et d'autres problèmes qui sont associés au cloud public. C'est pourquoi de nombreuses entreprises choisissent de conserver leurs données sensibles et leurs applications métier clés dans des clouds privés, et font appel à des clouds publics pour bénéficier d'une plus grande capacité d'adaptation.

RAPPEL

Les applications fondamentales suivantes figurent parmi les plus stratégiques pour l'entreprise :

- **L'ERP (planification des ressources de l'entreprise) et le MRP (planification des ressources de fabrication)**, où se concentrent la stratégie et les données financières de l'entreprise.
- **Le PLM (gestion des gammes de produits)**, où la propriété intellectuelle stratégique et les détails de la conception des produits sont saisis et stockés.
- **Les SGQ (systèmes de gestion de la qualité)**, qui permettent de suivre les problèmes de qualité relatifs aux processus et aux produits, informations que les entreprises préfèrent garder à l'abri des regards de la concurrence.
- **La veille stratégique ou BI (Business Intelligence)/analyse** (par exemple, Tableau) et toutes les bases de données associées auxquelles les outils de BI se connectent.
- **Les SGRH (systèmes de gestion des ressources humaines)** qui contiennent des informations personnelles d'identification (IPI) sur le personnel, la structure organisationnelle, la rémunération, etc.

Le respect des réglementations et des normes de sécurité – y compris la norme PCI DSS pour les cartes de paiement, la législation américaine HIPAA dans le domaine de la santé, les principes comptables GAAP, la loi Sarbanes-Oxley, entre autres – figure parmi les priorités majeures pour garantir la sécurité dans un environnement cloud privé, et ainsi protéger l'activité principale de l'entreprise.

Les applications clés spécifiques et les charges de travail dont l'utilisation est généralement plus prévisible sont également des candidats potentiels pour les centres de données virtuels et les environnements de cloud privé.

CONSEIL

Selon l'étude *Flexera 2022 State of the Cloud Report*, 84 % des entreprises utilisent au moins un cloud privé.

Dans les sections suivantes, nous examinons quelques-uns des principaux cas d'usage et défis liés à la sécurité dans les environnements de cloud privé, et comment les pare-feux logiciels permettent de relever ces défis.

La segmentation et la micro-segmentation empêchent les mouvements latéraux

Dans les réseaux virtualisés et les clouds privés, les équipes de sécurité réseau peinent souvent à avoir une visibilité et un contrôle efficace du trafic est-ouest, c'est-à-dire le trafic entre les machines virtuelles et au sein de celles-ci qui ne transite pas par un pare-feu de périmètre. Cette lacune génère une infrastructure virtuelle assez ouverte et uniforme, où toute charge de travail est susceptible de communiquer avec une autre. Les cybercriminels exploitent cette situation pour se propager de manière latérale au sein d'un réseau compromis. Ils établissent une présence durable, étendent leurs privilèges et identifient d'autres cibles, tout en minimisant le risque d'être détectés (voir figure 4-2).

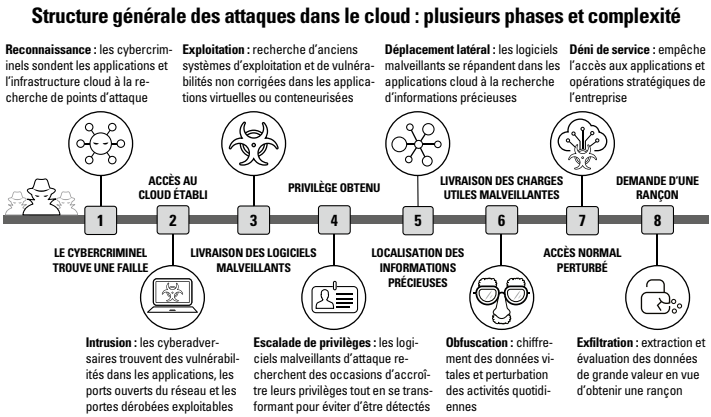


FIGURE 4-2 : Anatomie générale des attaques dans le cloud.

CONSEIL

Dans un environnement cloud privé et virtualisé, le déploiement stratégique de pare-feux logiciels, comme les pare-feux virtuels, permet de créer des zones de confiance ou, comme évoqué dans le chapitre précédent, de réduire les surfaces d'exposition en appliquant les principes Zero Trust. Ce découpage se fait en fonction du profil de risque et du

seuil de tolérance de l'organisation. Les applications stratégiques pour l'entreprise sont isolées dans des zones de confiance spécifiques, et des services de prévention des menaces sont mis en place pour examiner le trafic entrant et sortant lié à ces applications. Les données soumises à des exigences de conformité sont regroupées dans une zone de confiance distincte, où les mesures de sécurité nécessaires à la conformité sont appliquées. Ces contrôles de sécurité sont également déployables dans des environnements basés sur des containers, en utilisant des pare-feux spécifiquement conçus pour des environnements Kubernetes.

Renforcer les réseaux définis par logiciel grâce à la prévention des menaces

Plusieurs organisations mettent en place des solutions pour le réseau défini par logiciel (SDN) – comme VMware NSX, Cisco Application-Centric Infrastructure (ACI) ou Nutanix Flow – afin d'implémenter la segmentation dans leurs environnements virtualisés. Bien que les solutions SDN soient performantes pour limiter le trafic selon des politiques établies, elles ne disposent pas des moyens pour mettre en place une sécurité moderne ni pour détecter automatiquement les menaces au sein des flux de trafic autorisés.

Par exemple, une entreprise peut utiliser une solution SDN afin de faciliter la gestion du réseau dans un environnement virtualisé, tout en instaurant une micro-segmentation pour ses applications clés. Le SDN restreint la communication entre les charges de travail au seul trafic essentiel pour le bon fonctionnement des applications. Cependant, en plus de l'accès aux bases de données mutualisées, les applications utilisent des API et d'autres interfaces communes pour leurs opérations, communications et transactions habituelles. Un cybercriminel peut exploiter ces connexions autorisées pour se propager de manière latérale ou extraire des données de l'environnement. Les pare-feux logiciels peuvent se greffer aisément à des solutions SDN comme VMware NSX, Cisco ACI, Nutanix Flow ou autres. Ceci permet l'ajout rapide et précis de services de sécurité avancés, comme la prévention des intrusions ou un sandbox sécurisé, entre les micro-segments. L'objectif est d'inspecter et de sécuriser le trafic autorisé.

La sécurité VDI répond aux menaces qui pèsent sur les effectifs distants et distribués

Les déploiements d'infrastructure de desktop virtuel (VDI) présentent de nombreux avantages sur le plan opérationnel, mais constituent aussi un défi pour les équipes de sécurité réseau qui manquent de visibilité et de contrôle adéquats. Les menaces qui pénètrent dans le réseau via des

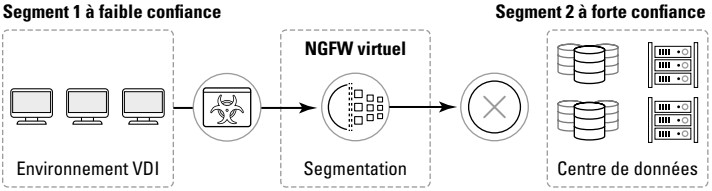


FIGURE 4-3 : Fonctionnalités de segmentation et de prévention des menaces pour protéger les ressources du centre de données et du cloud privé contre les attaques provenant de l'environnement VDI.

appareils VDI compromis peuvent se propager latéralement et viser d'autres ressources précieuses dans le cloud privé.

Prenons l'exemple d'une organisation qui déploie une VDI dans son centre de données ou son cloud privé. Puisque ces machines connectées à Internet sont gérées par les utilisateurs finaux, les points de terminaison VDI ont un niveau de confiance réduit et doivent être isolés du reste de l'environnement. Tout trafic autorisé vers des services ou des applications partagés doit être inspecté pour détecter les menaces.

CONSEIL

Les NGFW virtuels, installés en périphérie de l'environnement VDI, assurent une segmentation adéquate des postes de travail virtuels et une inspection appropriée du trafic (voir figure 4-3).

Cloud hybride et multicloud

Selon l'étude *Flexera 2022 State of the Cloud Report*, le multicloud est devenu la norme dominante, avec 89 % des entreprises adoptant une stratégie multicloud et 80 % une stratégie de cloud hybride. Au fur et à mesure que les entreprises répartissent leurs applications entre divers clouds publics et privés (45 % des applications étant hébergées sur différents clouds, selon le rapport Flexera), la gestion de la sécurité globale se complexifie et devient plus fragmentée. Chaque partie de l'environnement doit avoir son propre modèle de politique et des contrôles de sécurité spécifiques, ce qui amplifie la complexité opérationnelle, crée des failles de sécurité et provoque des retards dans les projets de migration vers le cloud.

Par exemple, une grande entreprise peut exécuter ses applications cloud natives stratégiques dans un cloud privé et dans deux environnements de cloud public différents. Pour appliquer des politiques de sécurité cohérentes dans les trois parties de cet environnement hybride, l'équipe de sécurité doit dupliquer les politiques dans les trois clouds en utilisant leurs contrôles natifs. Cette opération, fastidieuse et propice aux erreurs,

est compliquée davantage par le caractère à la fois dynamique et éphémère des environnements cloud et virtuels. L'administration de la stratégie de sécurité globale nécessite que l'équipe acquière une maîtrise des contrôles et de l'interface de gestion propres à chaque cloud, ainsi que de Kubernetes pour les applications conteneurisées – une tâche loin d'être simple.

Ce défi devient encore plus complexe dans les environnements hybrides qui incluent également des centres de données sur site. Cela peut contraindre les équipes de sécurité réseau à jongler avec la gestion de pare-feux matériels et logiciels, répartis entre plusieurs clouds publics et privés, des centres de données sur site et des filiales.

CONSEIL

Les pare-feux nouvelle génération (NGFW) pour la sécurité réseau, qui englobent les pare-feux logiciels (virtuels, conteneurisés et certains spécifiques au cloud), déployés dans des environnements multicloud et hybrides, peuvent toujours être administrés à partir d'une seule et même console. Les équipes de sécurité peuvent ainsi offrir des fonctionnalités de sécurité de haut niveau de manière uniforme à chaque environnement. Elles peuvent également déployer un modèle de politique cohérent à travers tout l'écosystème, assurant ainsi une visibilité totale et une simplification de votre stratégie de sécurité globale.

Filiale virtualisée

De nombreuses organisations adoptent la transformation digitale pour leurs filiales, leurs points de vente et même leurs infrastructures distantes clés, donnant ainsi naissance à des filiales pilotées par logiciel. Les pare-feux logiciels sont parfaitement adaptés pour assister ces organisations dans la mise en place de la segmentation au sein de leurs filiales, en recourant à des réseaux étendus sécurisés définis par logiciel (SD-WAN) pour la connectivité des filiales.

Les sections suivantes examinent quelques cas d'usage et enjeux de sécurité majeurs dans les filiales virtualisées et comment les pare-feux logiciels peuvent contribuer à surmonter ces obstacles.

Respecter la conformité grâce à la segmentation des filiales locales

Les exigences de conformité réglementaire réclament fréquemment une segmentation entre les applications et les données sensibles. Par exemple, la norme PCI DSS pour la sécurité des données dans le secteur des paiements par carte impose une segmentation de l'environnement où sont stockées les données des titulaires de carte, afin de sécuriser les

informations sensibles liées aux moyens de paiement. L'absence de ressources informatiques et de sécurité sur site, associée à un espace restreint pour l'installation du matériel, représente fréquemment des obstacles supplémentaires dans le contexte des filiales.

CONSEIL

Il est possible de déployer les pare-feux logiciels nouvelle génération (NGFW) sur des serveurs déjà en place dans les filiales, souvent appelés « équipements universels sur site client » (uCPE), éliminant ainsi le besoin d'ajouter du matériel supplémentaire. Cette approche permet aux équipes de sécurité d'élaborer une seule politique de sécurité pour mettre en place la segmentation nécessaire et la prévention des intrusions, conformément aux obligations réglementaires en vigueur pour la protection des données. L'entreprise peut piloter la sécurité de ses différentes filiales à partir d'un point central, en utilisant la même interface de gestion qui supervise la sécurité de son centre de données, de son cloud privé et de ses infrastructures en cloud public (voir figure 4-4).

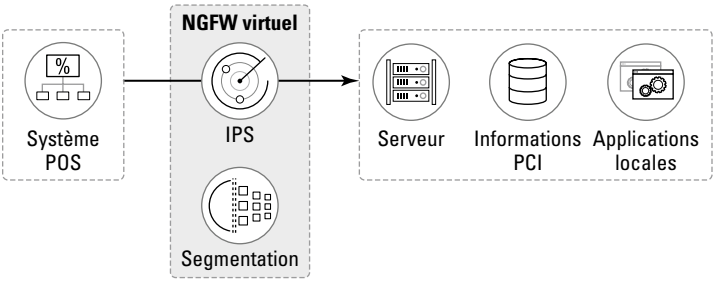


FIGURE 4-4 : Prise en charge des cadres de conformité (par exemple, PCI DSS) avec l'IPS, la segmentation et d'autres fonctions de sécurité.

La sécurité périmétrique pilotée par un logiciel simplifie le déploiement

Avec l'adoption croissante du SaaS et d'autres services à distance, de nombreuses entreprises se tournent vers le SD-WAN pour simplifier leur réseau et réduire le matériel nécessaire dans les filiales. L'installation et la configuration de pare-feux matériels classiques requièrent souvent des compétences techniques sur site qui font généralement défaut dans les filiales, sans compter le manque d'espace pour accueillir du matériel supplémentaire.

Les NGFW logiciels peuvent se substituer aux solutions matérielles dans les filiales et les sites distants, tout en fournissant un niveau de sécurité équivalent à celui du siège de l'entreprise, et en consolidant les services avec un équipement réduit. Ces solutions peuvent être installées en tant

que machines virtuelles (VM) sur des serveurs existants ou des équipements clients universels (uCPE). Elles éliminent donc le besoin d'expédier, d'installer et de gérer des pare-feux matériels distincts. Vous réduisez ainsi les frais de transport et libérez de l'espace en évitant l'ajout de nouveaux équipements. Les NGFW virtuels peuvent aussi intégrer un SD-WAN afin de renforcer la connectivité et la sécurité dans les filiales (voir figure 4-5).

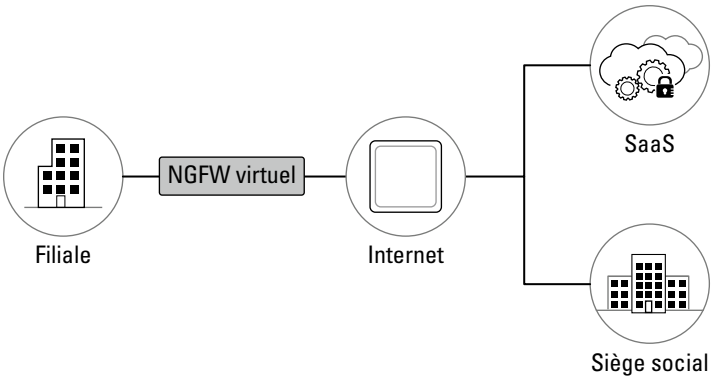


FIGURE 4-5 : Déploiement d'un périmètre pour protéger la filiale contre les menaces provenant d'Internet.

Le SD-WAN sécurisé augmente les performances et le retour sur investissement du réseau

Tandis que de plus en plus d'applications migrent vers le cloud, les réseaux étendus traditionnels (WAN) deviennent de plus en plus pertinents pour une gestion efficace de la sécurité et de la connectivité réseau. Dans le monde connecté au cloud d'aujourd'hui, l'acheminement du trafic des filiales vers un centre de données centralisé via des options de connectivité classiques comme le MPLS (Multiprotocol Label Switching) n'est plus une solution efficace.

Les NGFW virtuels permettent de créer une architecture SD-WAN en étoile qui relie les filiales, le centre de données principal, les plateformes de cloud public et les applications SaaS. Le SD-WAN peut aussi être configuré en tant que réseau maillé complet pour offrir une connectivité à la fois étoilée et de filiale à filiale (voir figure 4-6).

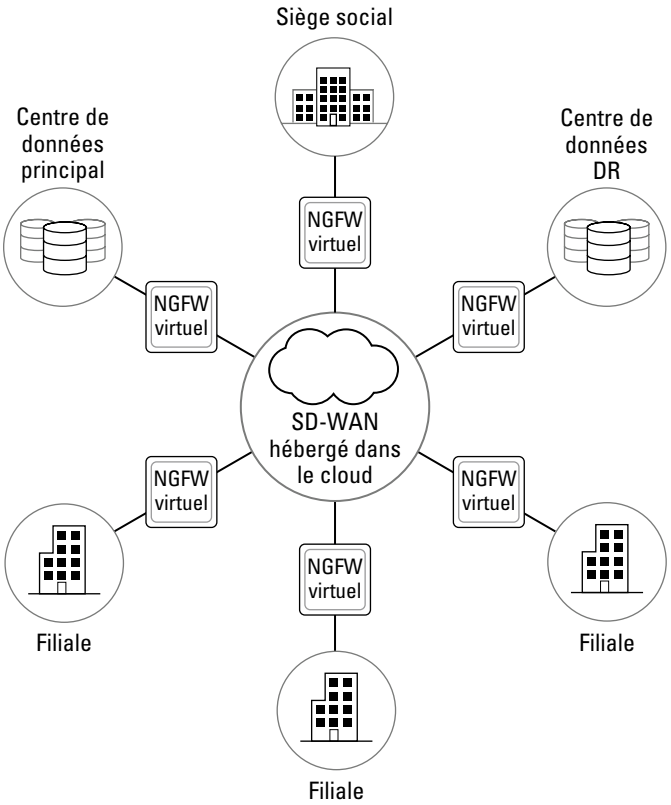


FIGURE 4-6 : Les NGFW virtuels dans une architecture en étoile.

5G

La 5G ouvre des perspectives commerciales révolutionnaires pour les fournisseurs de services et les entreprises. Elle ne se limite pas à la simple mise en place de la connectivité, mais offre également la possibilité de faire de la sécurité un levier commercial et un avantage compétitif. La montée en puissance de la 5G donne accès à des services inédits et stimulants, mais elle multiplie aussi les points d'entrée vulnérables et accentue donc les enjeux liés à la sécurité. Pour tirer pleinement parti des avantages commerciaux de la 5G tout en minimisant les risques d'attaques par des cybercriminels, les entreprises ont besoin d'une sécurité automatisée et d'une visibilité complète sur l'ensemble de leur réseau.

CONSEIL

La solution de sécurité 5G native de Palo Alto Networks permet aux entreprises de sécuriser leurs réseaux, leurs clients et leurs infrastructures cloud, tout en intégrant la philosophie du Zero Trust dans leurs environnements 5G. La sécurité 5G native couvre l'ensemble des composants essentiels de l'infrastructure mobile, qu'ils soient sur site, virtualisés ou conteneurisés. Elle s'étend aux clouds publics et privés des opérateurs télécoms ainsi qu'aux environnements de calcul multi-accès en périphérie (MEC), le tout renforcé par des pare-feux nouvelle génération optimisés par le machine learning.

ATTENTION

L'évolution majeure des architectures réseau 5G accentue encore davantage les enjeux liés à la sécurité. Elle multiplie les points d'entrée potentiels pour les intrusions, y compris les attaques à l'intérieur des tunnels mobiles, ainsi que les menaces présentes dans les applications dont le trafic transite via le réseau cellulaire. L'augmentation de la surface d'attaque rend d'autant plus crucial le besoin d'une sécurité de la couche 7, centrée sur les applications, qui soit capable d'identifier les menaces, qu'elles soient connues ou inconnues, sur tous les points du réseau et sur l'ensemble du trafic de signalisation.

DANS CE CHAPITRE

- Stopper les menaces de type « zero day » et mettre en œuvre le principe du moindre privilège
- Obtenir une plateforme de sécurité consolidée et pérenne
- Maximiser la flexibilité et simplifier la gestion
- Sécuriser tous les réseaux et tous les clouds
- Travailler avec vos outils existants et accélérer la stratégie de sécurité
- Assurer un retour sur investissement élevé

Chapitre 5
Dix questions à poser au fournisseur de votre pare-feu logiciel

Voici dix questions cruciales pour vous assister dans l'évaluation des solutions potentielles des fournisseurs de pare-feux logiciels pour votre organisation.

Permet-il d'arrêter les menaces de type « zero day » ?

Compter sur la compromission de la première victime pour prendre des mesures contre les menaces « zero day » risque d'entraîner une diffusion latérale rapide, mettant ainsi l'intégrité globale de votre organisation en péril. Certaines solutions cherchent à bloquer les attaques « zero-day » en mettant les fichiers en attente pour analyse, mais cette méthode s'avère contre-productive, car elle dégrade l'expérience utilisateur et ralentit les opérations de l'entreprise.

CONSEIL

Cherchez un pare-feu logiciel capable de contrer les menaces « zero day » en temps réel, en s'appuyant sur l'intelligence artificielle et un machine learning avancés, et qui se met constamment à jour grâce aux informations les plus récentes issues de services de sécurité hébergés dans le cloud.

Fournit-il un contrôle d'accès à moindre privilège ?

Le contrôle d'accès à moindre privilège garantit que les utilisateurs, les applications et/ou les appareils ne disposent que des autorisations minimales nécessaires pour effectuer une tâche ou une action autorisée. Le principe du moindre privilège est essentiel à la mise en œuvre d'une stratégie Zero Trust. Par exemple, seuls des membres du service expédition et réception, équipés d'un scanner portatif intelligent et utilisant une application dédiée, peuvent être autorisés à accéder au système ERP pour les opérations liées aux bordereaux d'expédition. Vous pouvez également limiter l'accès au système de gestion des ressources humaines (SGRH) de l'entreprise aux seuls appareils de bureau des équipes RH et des cadres, en bloquant tout accès depuis les appareils mobiles.

CONSEIL

Veillez à ce que votre pare-feu logiciel effectue un contrôle continu de la confiance et une surveillance de la sécurité, dans le but d'appliquer les principes Zero Trust à toutes vos charges de travail et applications cloud. L'association des fonctions d'identification des applications, des utilisateurs, des appareils et des contenus dans un pare-feu nouvelle génération (NGFW), ainsi que des politiques de sécurité intuitives, procure un excellent niveau de contrôle d'accès selon le principe du moindre privilège.

La sécurité peut-elle être consolidée dans une seule et même plateforme ?

Une démarche basée sur une plateforme de sécurité unifiée intègre toutes les fonctionnalités essentielles, notamment une gestion centralisée, un pare-feu nouvelle génération optimisé par l'IA et le machine learning, un système d'exploitation sécurisé enrichi par des analyses et le ML, ainsi que des services de sécurité délivrés via le cloud.

CONSEIL

Une architecture de traitement à passage unique est essentielle dans un NGFW pour assurer un débit élevé et une faible latence.

CONSEIL

La centralisation des services de sécurité peut non seulement accélérer la sécurisation de votre infrastructure, mais aussi optimiser le retour sur investissement en regroupant les fonctionnalités de sécurité. Assurez-vous que les fonctionnalités de sécurité telles que les systèmes de prévention des intrusions (IPS), le sandboxing, le filtrage des URL, la protection DNS, la prévention des pertes de données (DLP), la sécurisation de l'Internet des Objets (IoT) et les fonctionnalités SD-WAN sont pleinement intégrées à la plateforme.

Peut-il assurer une protection cohérente et pérenne ?

Assimiler les avancées en matière de cybersécurité peut représenter un défi. Les organisations perdent du temps à déployer des matériels et logiciels supplémentaires à chaque fois qu'elles veulent profiter d'une nouvelle technologie de sécurité. Elles investissent dans des ressources en plus pour gérer leurs infrastructures de sécurité en expansion constante, au lieu d'améliorer leurs contrôles de sécurité pour devancer les cybercriminels et se protéger des menaces.

CONSEIL

Votre pare-feu logiciel doit permettre aux équipes de découvrir, évaluer et utiliser rapidement les nouvelles technologies de sécurité. Les équipes de sécurité doivent pouvoir collaborer entre différentes applications, échanger des informations contextuelles et des données sur les menaces, orchestrer des réponses automatisées et des applications intégrées de manière approfondie, tout en garantissant une sécurité uniforme du trafic d'application dans tous les environnements cloud – hybride, multicloud ou configurations virtualisées. Elles peuvent ainsi répondre aux scénarios de sécurité les plus complexes en utilisant les meilleures technologies actuelles et futures, et ce, sans les coûts ou la complexité opérationnelle associés à la mise en place d'une nouvelle infrastructure.

La sécurité est-elle modulable en fonction des besoins ?

L'une des grandes forces du cloud réside dans la flexibilité de ses modèles d'abonnement et son système de paiement à l'utilisation. Votre pare-feu logiciel doit offrir la même flexibilité commerciale afin que vous puissiez rapidement adapter vos mesures de sécurité selon les besoins et les nouvelles exigences.

Propose-t-il une gestion centralisée ?

Recherchez un pare-feu logiciel qui permet une gestion unifiée de tous vos pare-feux, indépendamment de leur type ou de leur localisation, que ce soit sur site ou dans le cloud. Cela réduit la complexité en simplifiant la configuration, le déploiement et la gestion de vos politiques de sécurité. Vous cherchez un outil capable de croiser les données des journaux de pare-feu afin de vous donner des informations sur les applications, le réseau et la sécurité. Il devrait également mettre en évidence les comportements malveillants qui peuvent facilement se dissimuler dans le flux d'informations ou échapper à la détection en raison des failles de sécurité de produits spécialisés, en particulier dans un contexte de responsabilité partagée.

Peut-il sécuriser n'importe quel modèle d'architecture de cloud et d'application ?

Les données et les applications se trouvent à la fois dans votre réseau et dans le cloud. Selon l'étude *Flexera 2022 State of the Cloud Report*, 89 % des entreprises utilisent plusieurs clouds publics, privés ou hybrides – plus de cinq clouds différents en moyenne. Dans les contextes SaaS, les entreprises doivent maintenant veiller à la sécurité des données sensibles, tant au sein du réseau qu'à travers différents environnements cloud. De plus, les méthodes et outils de sécurité traditionnels, conçus pour des réseaux fixes, ne sont pas compatibles avec les fonctionnalités et outils propres au cloud. En outre, les services de sécurité intégrés de fournisseurs de cloud tels qu'Amazon Web Services (AWS), Microsoft Azure et Google Cloud Platform (GCP) se limitent souvent à des protections de couche 3/4 et sont exclusifs à leur propre plateforme cloud.

Pour prospérer, votre entreprise a besoin d'une solution de sécurité cloud qui assure une uniformité de la politique du réseau au cloud, bloque l'infiltration et la propagation latérale de logiciels malveillants dans le cloud, facilite la gestion, réduit les incohérences dans les politiques de sécurité lors des changements de charges de travail virtuelles et réduit les failles de sécurité susceptibles de survenir dans des environnements cloud hybrides ou multicloud à cause de produits spécialisés. Votre pare-feu logiciel doit protéger les applications et données résidentes au même niveau de sécurité que celui établi sur votre réseau physique. Pour que les déploiements multicloud soient sécurisés, le pare-feu doit prendre en charge des environnements divers de cloud et de virtualisation, notamment tous les principaux fournisseurs de cloud publics et de cloud privé virtualisé. Le pare-feu doit être compatible avec

des services cloud natifs, comme Amazon Lambda et Azure, mais aussi des outils d'automatisation comme Ansible et Terraform, afin d'intégrer harmonieusement la sécurité aux méthodes de travail des développeurs d'applications dans votre architecture orientée « cloud first ».

RAPPEL

Avec Palo Alto Networks, vous pouvez efficacement sécuriser l'ensemble de vos environnements cloud et virtualisés grâce à des intégrations poussées qui facilitent et accélèrent vos déploiements. Vous pourrez ainsi mettre en place plus rapidement une stratégie de sécurité unifiée. Voici les intégrations poussées proposées par Palo Alto Networks :

- **Fournisseurs de services cloud**
  - Alibaba Cloud
  - AWS
  - GCP
  - IBM Cloud
  - Microsoft Azure
  - Oracle Cloud
- **Containers Kubernetes**
  - Amazon Elastic Kubernetes Service (EKS)
  - Azure Kubernetes Service (AKS)
  - Google Kubernetes Engine
  - OpenShift
  - Rancher
  - VMware Tanzu
- **Réseaux et hyperviseurs définis par logiciel**
  - Cisco Application Centric Infrastructure (ACI)
  - Linux Kernel-based Virtual Machine (KVM)
  - Microsoft Hyper-V
  - Nutanix Acropolis Hypervisor (AHV)
  - Nutanix Flow
  - OpenStack
  - VMware ESXi
  - VMware NSX

Est-il compatible avec vos outils d'automatisation et d'orchestration ?

Les pare-feux logiciels que vous déployez dans le cloud doivent opérer en harmonie avec vos développeurs d'applications. Vous devez donc intégrer les outils d'automatisation et d'orchestration que ces équipes utilisent et connaissent bien, afin de faciliter un déploiement rapide de nouvelles versions des logiciels.

CONSEIL

Les pare-feux logiciels de Palo Alto Networks prennent en charge le déploiement automatisé, la mise à l'échelle et les changements de politique grâce à des fonctionnalités natives, notamment les groupes d'adresses dynamiques (DAG) et les balises d'application, ainsi que les outils d'automatisation et d'orchestration les plus répandus : Ansible, AWS CloudFormation, modèles ARM (Azure Resource Manager), Helm Charts, Kubernetes, Terraform, etc.

Est-il prouvé qu'il accélère la stratégie de sécurité ?

Les pare-feux logiciels doivent être simples à déployer tout en étant suffisamment puissants pour répondre aux enjeux spécifiques de sécurité dans des environnements de cloud hybride et multicloud, dans le but de minimiser les interruptions et d'optimiser la productivité des équipes.

CONSEIL

D'après l'étude de Forrester de septembre 2021 intitulée *The Total Economic Impact of Palo Alto Networks VM-Series Virtual Firewalls*, le lancement des pare-feux virtuels VM-Series a en moyenne réduit de 30 % le temps requis pour instaurer une stratégie de sécurité efficace, tout en permettant une économie de 436 760 dollars sur une période de trois ans.

A-t-il des antécédents en matière de retour sur investissement ?

CONSEIL

Les pare-feux virtuels VM-Series de Palo Alto Networks offrent un retour sur investissement rapide et peuvent générer des économies de l'ordre de plusieurs millions de dollars en peu de temps. D'après l'étude de Forrester publiée en septembre 2021, intitulée *The Total Economic Impact of Palo Alto Networks VM-Series Virtual Firewalls*, les bénéfices suivants ont été constatés :

- **115 %** de retour sur investissement sur trois ans avec une période de récupération de six mois.
- Réduction de **90 %** du temps nécessaire au déploiement des pare-feux.
- **80 %** ont amélioré l'efficacité de l'équipe chargée du réseau et de la sécurité, ce qui a permis d'économiser 1,3 million de dollars sur trois ans.
- Diminution de **67** % du nombre d'employés ayant subi une interruption – seuls 6 % sont touchés par ces incidents.

Glossaire

accès avec le minimum de privilèges : accès dans lequel un utilisateur ou un objet ne se voit attribuer que le niveau minimum d'autorisations nécessaires pour effectuer une tâche autorisée.

API : *voir* interface de programmation d'application (API).

authentification multifacteur (MFA) : mécanisme d'authentification qui exige au moins deux des facteurs suivants : quelque chose que l'on sait, quelque chose que l'on possède ou quelque chose que l'on est. Par exemple, un utilisateur peut s'authentifier à l'aide de son nom d'utilisateur et de son mot de passe (ce qu'il sait) et d'un code d'accès à usage unique envoyé sur un téléphone mobile préalablement enregistré auprès de l'organisation (ce qu'il possède).

botnet : vaste réseau de terminaux infectés par des logiciels malveillants (bots) travaillant ensemble et contrôlés par un attaquant via une infrastructure C2. *Voir aussi* commande et contrôle (C2).

C2 : *voir* commande et contrôle (C2).

CI/CD : *voir* intégration continue/distribution continue (CI/CD).

cloud hybride : environnement composé de ressources provenant de plusieurs clouds publics et/ou privés qui assurent la portabilité des applications et des données entre les clouds. *Voir aussi* cloud privé *et* cloud public.

cloud privé : modèle de déploiement de cloud computing composé d'une infrastructure cloud utilisée exclusivement par une seule organisation.

cloud public : modèle de déploiement de cloud computing composé d'une infrastructure cloud ouverte au public.

commande et contrôle (C2) : trafic de communications entre des malwares et/ou des systèmes compromis et l'infrastructure du serveur à distance d'un attaquant qui sert à envoyer et recevoir des commandes malveillantes ou à exfiltrer des données.

couche d'application : au sein du modèle OSI, la couche 7 a pour responsabilités l'identification et la mise à disposition des partenaires de communication, la détermination de la disponibilité des ressources et la synchronisation des échanges de données. *Voir aussi* modèle Open Systems Interconnection (OSI).

couche réseau : dans le modèle OSI, la couche 3 est responsable du routage et des fonctions associées qui facilitent le transfert des données entre les systèmes appartenant au même réseau ou à des réseaux interconnectés. *Voir aussi* modèle Open Systems Interconnection (OSI).

couche transport : couche 4 du modèle OSI, responsable du transport et du contrôle de la transmission de bout en bout. *Voir aussi* modèle Open Systems Interconnection (OSI).

CSP : *voir* fournisseur de services cloud (CSP).

DAG : *voir* groupe d'adresses dynamique (DAG).

DDoS : *voir* déni de service distribué (DDoS).

déni de service distribué (DDoS) : tactique dans laquelle un cybercriminel utilise de nombreux systèmes (souvent des dizaines de milliers) simultanément pour lancer des attaques de déni de service. Ces systèmes sont généralement des bots regroupés dans un botnet, et l'objectif principal est de rendre le système ou le réseau ciblé indisponible. *Voir aussi* botnet.

DevOps : culture et pratique d'une meilleure collaboration entre les développeurs de logiciels et les opérations informatiques.

DLP : *voir* prévention des pertes de données (DLP).

DNS (Domain Name System) : *voir* système de noms de domaine (DNS).

DPI : *voir* inspection approfondie des paquets (DPI).

ERP : *voir* planification des ressources de l'entreprise (ERP).

fabricant de matériel informatique d'origine (OEM) : traditionnellement défini comme une entreprise dont les produits sont utilisés comme composants dans les produits d'une autre entreprise, qui vend ensuite le produit fini aux utilisateurs. La seconde entreprise est appelée revendeur à valeur ajoutée (RVA), car en augmentant ou en intégrant des fonctionnalités ou des services, elle ajoute de la valeur au produit d'origine. Le RVA (fournisseur de services cloud) travaille en étroite collaboration avec l'OEM (Palo Alto Networks), qui personnalise souvent ses produits en fonction des besoins et des spécifications de la société RVA.

Federal Information Security Modernization Act (FISMA) : loi fédérale américaine définissant un cadre global pour protéger les informations, les opérations et les biens du gouvernement.

FISMA : *voir* Federal Information Security Modernization Act (FISMA).

fournisseur de logiciels indépendant (ISV) : éditeur de logiciels qui n'est pas détenu ou contrôlé par un fabricant de matériel (ou dans les cas exposés dans ce livre, le fournisseur de services cloud) ; entreprise dont la fonction principale est de distribuer des logiciels.

fournisseur de services cloud (CSP) : entreprise tierce proposant des services de plateforme, d'infrastructure, d'application et/ou de stockage de données basés sur le cloud.

gestion des identités et des accès (GIA) : service logiciel ou cadre qui permet aux organisations de définir des identités d'utilisateurs ou de groupes dans des environnements logiciels et d'y associer des autorisations.

GIA : *voir* gestion des identités et des accès (GIA).

groupe d'adresses dynamique (DAG) : un groupe d'adresses dynamique est composé de manière dynamique à l'aide de recherches de balises et de filtres basés sur les balises. Les groupes d'adresses dynamiques sont très utiles si vous avez une infrastructure virtuelle étendue où les changements d'emplacement ou d'adresse IP des machines virtuelles (VM) sont fréquents. *Voir aussi* machine virtuelle (VM) *et* protocole Internet (IP).

Health Insurance Portability and Accountability Act (HIPAA) : loi fédérale américaine définissant les exigences en matière de sécurité et de confidentialité pour les systèmes médicaux et les données de santé.

HIPAA : *voir* Loi américaine sur la responsabilité et la portabilité en matière d'assurance santé (Health Insurance Portability and Accountability Act - HIPAA).

hyperviseur : dans un environnement virtualisé, programme de supervision qui contrôle l'allocation des ressources et l'accès aux communications et aux appareils périphériques.

IA : *voir* intelligence artificielle (IA).

IaaS : *voir* infrastructure en tant que service (IaaS).

informations personnelles d'identification (IPI) : données (telles que le nom, l'adresse, le numéro de sécurité sociale, la date de naissance, le lieu de travail, etc.) qui peuvent être utilisées seules ou avec d'autres informations pour identifier, contacter ou localiser une personne.

infrastructure de desktop virtuel : système d'exploitation pour desktop s'exécutant dans une machine virtuelle (VM) sur un serveur physique. *Voir aussi* machine virtuelle (VM).

infrastructure en tant que service (IaaS) : modèle de service basé sur le cloud dans lequel le client gère les systèmes d'exploitation, les applications, les ressources de calcul, le stockage et le réseau, mais le fournisseur de services se charge de l'infrastructure cloud physique sous-jacente.

inspection approfondie des paquets (DPI) : méthode avancée d'analyse et de gestion du trafic réseau allant au-delà des en-têtes initiaux des paquets.

intégration continue/distribution continue (CI/CD) : environnement DevOps soutenu par l'automatisation, où les modifications apportées au code source de l'application et à la configuration de l'infrastructure sont effectuées, intégrées et déployées de manière automatique. *Voir aussi* DevOps.

intelligence artificielle (IA) : capacité d'un ordinateur à interagir avec son environnement, à en tirer des enseignements et à effectuer automatiquement des actions sans être explicitement programmé.

interface de programmation d'application (API) : ensemble de protocoles, de routines et d'outils servant à développer et à intégrer des applications.

Internet des objets (IoT) : réseau d'objets physiques connectés, intégrés dans des composants électroniques, des systèmes d'exploitation, des logiciels, des capteurs et une connectivité réseau.

IoT : *voir* Internet des objets (IoT).

IP : *voir* protocole Internet (IP).

IPI : *voir* informations personnelles d'identification (IPI).

IPS : *voir* système de prévention des intrusions (IPS).

ISV : voir fournisseur de logiciels indépendant (ISV).

logiciel en tant que service (SaaS) : modèle de distribution de logiciels basé sur le cloud dans lequel un fournisseur tiers héberge des applications qu'il met à la disposition des clients sur Internet. Le fournisseur héberge et gère les serveurs, les bases de données et le code qui constituent les applications.

machine learning (ML) : méthode d'analyse des données qui permet aux ordinateurs d'examiner un jeu de données et d'effectuer automatiquement des actions basées sur les résultats sans être explicitement programmées.

machine virtuelle (VM) : instance d'un système d'exploitation s'exécutant dans le cadre d'un hyperviseur. *Voir aussi* hyperviseur.

malware : logiciel ou code malveillant généralement conçu pour endommager ou désactiver un système informatique, en prendre le contrôle ou voler des informations qu'il renferme.

MFA : *voir* authentification multifacteur (MFA).

ML : *voir* apprentissage automatique (ML).

MNO : *voir* opérateur de réseau mobile (ORM).

modèle Open Systems Interconnection (OSI) : modèle de référence des réseaux composé de sept couches : physique, liaison de données, réseau, transport, session, présentation et application.

MPLS : *voir* Multiprotocol Label Switching (MPLS).

multicloud : environnement composé de ressources provenant de plusieurs clouds publics et/ou privés, mais qui ne fournit pas nécessairement la portabilité des applications et des données entre les clouds (autrement dit, les différents environnements cloud peuvent fonctionner de manière cloisonnée). À noter que si tous les environnements cloud hybrides sont également des environnements multicloud, tous les environnements multicloud ne sont pas nécessairement des environnements cloud hybrides. *Voir aussi* cloud hybride, cloud privé *et* cloud public.

Multiprotocol Label Switching (MPLS) : méthode de transmission de paquets à travers un réseau qui utilise des étiquettes insérées entre les en-têtes des couches 2 et 3 du paquet.

NAT : *voir* traduction d'adresse réseau (NAT).

NGFW : *voir* pare-feu nouvelle génération (NGFW).

Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS) : ensemble d'exigences standard développées pour la protection des données personnelles dans le cadre des transactions par carte bancaire et en espèces.

OEM : *voir* fabricant de matériel informatique d'origine.

opérateur de réseau mobile (ORM) : fournisseur de services de communications sans fil qui possède ou contrôle tous les éléments nécessaires pour vendre et fournir des services à un utilisateur final. Également appelé fournisseur de services sans fil, opérateur sans fil, société cellulaire ou opérateur de réseau mobile.

OSI : *voir* modèle Open Systems Interconnection (OSI).

PaaS : *voir* plateforme en tant que service (PaaS).

pare-feu cloud : fournisseur proposant à la fois des services cloud et des solutions de sécurité. Son interface utilisateur native cloud est conçue pour être conviviale et facile à utiliser. Elle est optimisée par un pare-feu virtuel nouvelle génération (NGFW) offrant une sécurité de pointe contre toutes sortes de cybermenaces, qu'elles soient connues ou inconnues. Cette solution peut être gérée de deux manières : d'une part, en tant que fournisseur de logiciels indépendant (ISV) ou fabricant de matériel informatique d'origine (OEM) ; et d'autre part, elle peut être prise en charge par la solution du fournisseur de services cloud (CSP). Les solutions ISV de Palo Alto Networks comprennent notamment Cloud NGFW pour AWS et Cloud NGFW pour Azure ; elles sont optimisées par des pare-feux virtuels VM-Series. Les solutions OEM de Palo Alto Networks comprennent notamment Google Cloud IDS et Oracle OCI Network Firewall, tous deux optimisés par des pare-feux virtuels VM-Series. *Voir aussi* fournisseur de services cloud (CSP), pare-feu de containers, fournisseur de logiciels indépendant (ISV), fabricant de matériel informatique d'origine (OEM), pare-feu logiciel *et* pare-feu virtuel.

pare-feu de containers : catégorie de pare-feux logiciels offrant des fonctionnalités de pare-feu nouvelle génération (NGFW) dans un format de container d'application déployé et géré dans des environnements Kubernetes et toutes les plateformes cloud (privés, publics et hybrides) qui contiennent des applications de container gérées avec Kubernetes ou des adaptations cloud de Kubernetes (par exemple, Amazon EKS, Azure Kubernetes Services [AKS], Google Kubernetes Engine, OpenShift, Rancher, VMware Tanzu, et ainsi de suite). Le pare-feu de containers nouvelle génération CN-Series est le pare-feu pour containers de Palo Alto Networks. *Voir aussi* pare-feu cloud, pare-feu logiciel *et* pare-feu virtuel.

pare-feu logiciel : gamme de pare-feux nouvelle génération (NGFW), comprenant des pare-feux virtuels, des pare-feux de containers et des pare-feux cloud, spécialement conçus pour être déployés avec une agilité DevOps dans des environnements virtuels et tous les types de clouds (privés, publics et hybrides). *Voir aussi* pare-feu cloud, pare-feu de containers, DevOps *et* pare-feu virtuel.

pare-feu nouvelle génération (NGFW) : plateforme de sécurité réseau qui intègre entièrement les fonctions traditionnelles de pare-feu et de prévention des intrusions (IPS) réseau avec d'autres fonctions de sécurité avancées qui fournissent une inspection approfondie des paquets (DPI) pour une visibilité complète, une identification précise des applications, des contenus et des utilisateurs, ainsi qu'un contrôle renforcé basé sur des stratégies. *Voir aussi* inspection approfondie des paquets (DPI) *et* système de prévention des intrusions (IPS).

pare-feu virtuel : catégorie de pare-feux logiciels offrant des fonctionnalités de pare-feu nouvelle génération (NGFW) dans un format de machine virtuelle (VM) pouvant être déployé dans des environnements virtuels et dans tous les types de clouds (privés, publics et hybrides). Peut également être le NGFW de référence pour les pare-feux cloud qui sont profondément intégrés avec des interfaces utilisateur natives cloud pour faciliter l'utilisation et les

déploiements. Le pare-feu virtuel nouvelle génération VM-Series est la solution de pare-feu virtuel de Palo Alto Networks. *Voir aussi* pare-feu cloud, pare-feu de containers *et* pare-feu virtuel.

PCI DSS : *voir* norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS)

planification des ressources de l'entreprise (ERP) : progiciel utilisé pour recueillir, stocker, gérer et interpréter des données provenant de nombreuses activités commerciales.

plateforme en tant que service (PaaS) : modèle de service basé sur le cloud dans lequel le client bénéficie d'un accès à une plateforme pour déployer des applications et gérer un nombre limité de paramètres de configuration, mais le système d'exploitation, le calcul, le stockage et le réseau, et l'infrastructure de cloud physique sous-jacente sont maintenus par le fournisseur de services.

prévention des pertes de données (DLP) : application ou appareil permettant de détecter le stockage ou la transmission non autorisé(e) de données sensibles.

protocole Internet (IP) : protocole de la couche 3 (réseau) de l'OSI qui est à la base de l'Internet moderne. *Voir aussi* modèle Open Systems Interconnection (OSI).

RAN : *voir* réseau d'accès radio (RAN).

Règlement général sur la protection des données (RGPD) : loi sur la confidentialité des données qui renforce les exigences en matière de protection des données pour les résidents de l'Union européenne (UE) et traite de l'exportation de données personnelles en dehors de l'UE.

réseau d'accès radio (RAN) : partie d'un système de télécommunication mobile qui connecte des appareils cellulaires sans fil (tels qu'un téléphone mobile) à un réseau central mobile public et/ou privé via un réseau backbone existant.

réseau défini par logiciel (SDN) : approche du réseau qui sépare le contrôle du réseau et les processus de gestion du matériel sous-jacent et les rend accessibles sous forme de logiciel.

réseau étendu (WAN) : réseau informatique qui s'étend sur une zone géographique large et peut connecter plusieurs réseaux locaux.

réseau étendu défini par logiciel (SD-WAN) : nouvelle approche du réseau étendu (WAN) qui sépare le contrôle du réseau et les processus de gestion du matériel sous-jacent et les rend accessibles sous forme de logiciel. *Voir aussi* réseau étendu (WAN).

RGPD : *voir* Règlement général sur la protection des données (RGPD).

SaaS : *voir* logiciel en tant que service (SaaS).

SDN : *voir* réseau défini par logiciel (SDN).

SD-WAN : *voir* réseau étendu défini par logiciel (SD-WAN).

surface d'attaque : volume total des appareils et des connexions que les cybercriminels peuvent potentiellement utiliser pour pénétrer les défenses du réseau.

surface de protection : données, applications, ressources, services et infrastructures qui doivent être protégés dans le cadre d'une architecture Zero Trust. *Voir aussi* Zero Trust.

système de noms de domaine (DNS) : service de répertoire décentralisé et hiérarchique qui convertit les noms de domaine en adresses IP pour les ordinateurs, les services et d'autres ressources informatiques connectées à un réseau ou à Internet. *Voir aussi* protocole Internet (IP).

système de prévention des intrusions (IPS) : périphérique matériel ou application logicielle qui détecte et bloque les intrusions présumées au sein d'un réseau ou d'une machine hôte.

traduction d'adresse réseau (NAT) : processus de conversion des adresses IP internes et privées d'un réseau en adresses IP externes et publiques. *Voir aussi* protocole Internet (IP).

Uniform Resource Locator (URL) : couramment appelée « adresse web ». Identifiant unique de toute ressource connectée au web.

URL : *voir* Uniform Resource Locator (URL).

VDI : *voir* infrastructure de desktop virtuel (VDI).

VM : *voir* machine virtuelle (VM).

WAN : *voir* réseau étendu (WAN).

Zero Trust : approche stratégique de la cybersécurité qui élimine la confiance implicite, valide en permanence les identités des utilisateurs et des objets, et applique un accès avec le minimum de privilèges. *Voir aussi* accès avec le minimum de privilèges.

Optez pour une stratégie de sécurité intégrée à une plateforme cloud

Les entreprises modernes ont besoin de solutions de sécurité simples à utiliser et qui ne ralentissent pas les équipes de développement cloud. Les équipes chargées de la sécurité du réseau doivent pouvoir déployer et gérer ces solutions en toute confiance afin de protéger l'entreprise contre des menaces de plus en plus sophistiquées. Les pare-feux logiciels offrent les mêmes capacités robustes que les pare-feux matériels de nouvelle génération (NGFW) et peuvent être déployés dans divers environnements : sur site, filiales, clouds publics, clouds privés, ainsi que dans des configurations de cloud hybride ou multicloud. L'ouvrage *Les pare-feux logiciels pour les Nuls* vous montre comment sécuriser n'importe quel réseau et tous les clouds.

Dans ce livre...

- Mettre en œuvre une stratégie Zero Trust
- Appliquer un accès avec le minimum de privilèges
- Protéger les environnements conteneurisés
- Simplifier la sécurité multicloud
- Protéger les filiales distantes
- Sécuriser les applications cloud

paloalto NETWORKS

Lawrence Miller a exercé au grade de premier maître dans la marine américaine et travaille depuis plus de 25 ans dans les départements informatiques de divers secteurs. Il a co-écrit *« CISSP pour les Nuls »* et plus de 200 livres *Pour les Nuls* portant sur diverses questions de sécurité et de technologie.

Rendez-vous sur Dummies.com®
pour voir des vidéos, des tutoriels en photos, des articles pratiques, ou pour faire des achats !

ISBN: 978-1-394-23263-5

pour les nuls®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.