Guide d'achat des pare-feu nouvelle génération

Le guide de référence pour évaluer les pare-feu de réseaux d'entreprise

L'évolution rapide de l'informatique a redessiné les contours du réseau. Aujourd'hui, les données et les utilisateurs sont partout. Les entreprises peinent à garder le rythme face au foisonnement des appareils. Parallèlement, les équipes informatiques misent sur le cloud, les analyses Big Data, le machine learning et l'automatisation pour accélérer le déploiement de nouvelles applications et stimuler la croissance de leur entreprise. Enfin, les applications gagnent en accessibilité. Le résultat ? Un réseau incroyablement complexe, source de risques énormes pour les entreprises. Ces dernières doivent donc prendre le problème à bras-le-corps sans pour autant freiner leur croissance.

De son côté, la cybersécurité ne tient pas la cadence des attaques qui continuent de perturber les opérations. Malgré les énormes investissements engagés, la réduction des risques ne semble pas au rendez-vous. Le déploiement d'outils et de technologies disparates expose en effet votre entreprise aux menaces. Ces outils n'étant à l'origine pas conçus pour l'automatisation, ils contraignent les analystes à reconstituer eux-mêmes les pièces du puzzle avant de pouvoir agir. C'est pourquoi une nouvelle approche s'impose.

Aujourd'hui, toute stratégie de sécurité réseau efficace passe avant tout par des pare-feu nouvelle génération (NGFW). Une approche axée sur la prévention, l'automatisation et l'analytique permet aux équipes de sécurité d'adopter facilement de bonnes pratiques de neutralisation des attaques, de réduire les tâches manuelles, de remplacer leur patchwork de produits isolés et de déployer des technologies innovantes et ultra-intégrées, garantes d'une sécurité simplifiée et renforcée.

Ce livre blanc retrace l'évolution des pare-feu et met en lumière les fonctions clés dont les produits de nouvelle génération doivent être équipés pour sécuriser votre réseau et votre entreprise. Il énonce également les questions clés à vous poser lors du processus d'appel d'offres, au moment où vous évaluerez votre prochain pare-feu nouvelle génération.

Évolution du pare-feu nouvelle génération

Pour classifier le trafic, les premiers pare-feu d'inspection avec état (stateful inspection) s'intéressaient uniquement au port de destination (par exemple, le port TCP 80 pour le trafic HTTP). Pour donner davantage de visibilité sur le trafic applicatif, de nombreux fournisseurs ont ensuite intégré différents matériels et logiciels à leurs pare-feu. Les systèmes de gestion unifiée des menaces (UTM) étaient nés. Toutefois, ces nouvelles fonctionnalités n'étant pas intégrées en natif, les systèmes UTM n'ont en rien renforcé la sécurité des entreprises.

> Gartner avait annoncé que, d'ici la fin de l'année 2019, les pare-feu nouvelle génération protégeraient 90 % des connexions Internet de la base installée des entreprises.[1]

Contrairement aux offres UTM, les pare-feu nouvelle génération centrent leur analyse sur les applications, mais aussi sur les utilisateurs et les contenus. Leur conception intégrée renforce la sécurité et simplifie les opérations. Preuve du succès de ce modèle, l'expression « pare-feu nouvelle génération » est désormais synonyme de « pare-feu » tout court.

Fonctionnalités indispensables d'un pare-feu nouvelle génération

- Identifier les applications indépendamment du port, du protocole, de la tactique de contournement ou du chiffrement utilisé
- Identifier les utilisateurs indépendamment de leur appareil ou de leur adresse IP
- Déchiffrer le trafic chiffré
- Bloquer en temps réel les menaces connues et inconnues dissimulées dans les applications
- Garantir de très hauts débits in-line

Les critères de sélection d'un pare-feu nouvelle génération concernent généralement trois domaines : fonctions de sécurité, opérations et performances. Les fonctions de sécurité font référence à l'efficacité des contrôles et à la capacité de votre équipe à gérer les risques associés aux applications traversant votre réseau sans freiner votre activité. Côté opérationnel, les politiques régissant les applications doivent être accessibles et simples à gérer. C'est là que l'automatisation a un rôle à jouer pour permettre aux équipes de sécurité de se recentrer sur des activités plus stratégiques. Enfin, sur le terrain des performances : votre pare-feu doit remplir sa mission tout en répondant à vos attentes en matière de débit. C'est pourquoi votre pare-feu devrait également intégrer les dernières innovations et faciliter leur adoption. Si les exigences et les priorités varieront au sein de ces catégories, il existe néanmoins certaines fonctionnalités incontournables dont aucune entreprise ne saurait se passer.

14 fonctionnalités indispensables de votre prochain pare-feu nouvelle génération

1. Identification des utilisateurs et autorisations d'accès adaptées

Le problème

Vos salariés, vos clients et vos partenaires se connectent à différentes bases de données sur votre réseau, mais aussi à Internet. Ces personnes, et toute la panoplie d'appareils employés, constituent la base d'utilisateurs de votre réseau. Afin d'assurer sa sécurité, votre entreprise doit pouvoir identifier ces utilisateurs au-delà de leur adresse IP et cerner le risque qu'ils représentent en fonction de l'appareil utilisé, surtout en cas d'entorse aux politiques de sécurité ou d'introduction de nouvelles menaces sur votre réseau. Par ailleurs, vos utilisateurs changent constamment de lieu et utilisent plusieurs appareils, systèmes d'exploitation et versions d'applications pour accéder à vos données. Or, les sous-réseaux d'adresses IP se rapportent uniquement à des lieux géographiques, et non à des utilisateurs individuels. Par conséquent, lorsqu'un utilisateur se déplace, même au sein de vos bureaux, vos politiques ne suivent pas.

Enfin, les annuaires d'utilisateurs ne donnent aucune donnée comportementale. De ce fait, même si un utilisateur présente des risques ou si ses identifiants sont compromis, ses niveaux d'accès resteront les mêmes, car ils dépendent de son rôle. Et modifier un annuaire prend du temps. C'est ainsi que les activités à risque ou malveillantes peuvent passer inaperçues et rendre votre entreprise vulnérable.

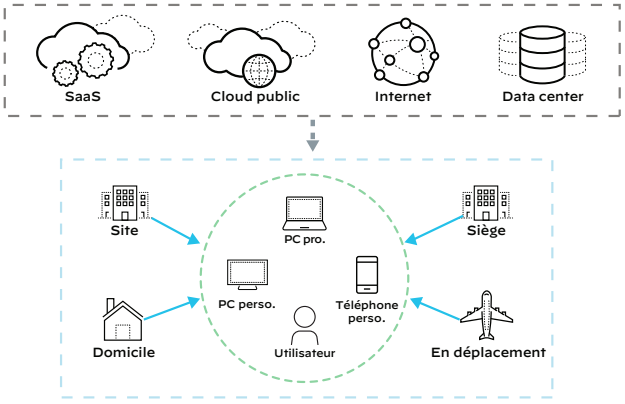

Figure 1 : différents lieux et appareils pour un même utilisateur

1. Adam Hils, Jeremy D'Hoinne, Rajpreet Kaur, « Magic Quadrant for Enterprise Network Firewalls », Gartner, 10 juillet 2017, https://www.gartner.com/en/documents/3757665/magic-quadrant-for-enterprise-network-firewalls.

La solution

Aujourd'hui, les informations sur les utilisateurs et groupes d'utilisateurs doivent être intégrées directement aux technologies chargées de sécuriser les entreprises. Votre prochain pare-feu doit donc pouvoir vérifier l'identité de vos utilisateurs à partir de multiples sources, notamment les VPN, les contrôleurs d'accès WLAN, les serveurs d'annuaires et de messagerie, et les portails captifs. En identifiant les utilisateurs des applications de votre réseau et les éventuels vecteurs de menaces, vous renforcerez vos règles de sécurité et accélérerez votre réponse aux incidents. Vous devez aussi pouvoir définir des règles visant à valider l'utilisation d'applications en fonction des utilisateurs ou de groupes d'utilisateurs, tant dans le trafic entrant que sortant. Cela consiste par exemple à n'autoriser les connexions SSH, Telnet et FTP qu'au département informatique. Une fois définies, ces règles suivent ensuite les utilisateurs où qu'ils soient (siège social, succursales ou domicile) et quel que soit l'appareil qu'ils utilisent. Cependant, définir des règles basées sur les informations des utilisateurs figurant dans l'annuaire ne suffit pas. Vous devez pouvoir modifier facilement les accès en fonction de l'évolution des circonstances, que le changement soit dû à de nouveaux indicateurs de compromission (IOC) ou à un besoin opérationnel, comme accorder des droits d'accès temporaires à un groupe d'utilisateurs.

2. Prévention des vols et détournements d'identifiants

Le problème

Les utilisateurs et leurs identifiants font partie des principales faiblesses de votre infrastructure de sécurité. D'après le rapport d'enquête Verizon 2019 sur les compromissions de données, au cours des douze mois étudiés, 29 % des tentatives de piratage se sont basées sur des mots de passe faibles ou volés.[2] Lorsqu'ils recourent à des identifiants volés, les attaquants ont plus de chances de s'infiltrer et moins de chances d'être démasqués. Pour prévenir ces vols, la plupart des entreprises misent sur la pédagogie, ce qui ne les protège pas contre les erreurs humaines. Quant aux solutions technologiques, elles se contentent généralement de filtrer les e-mails et d'identifier les sites de phishing connus.

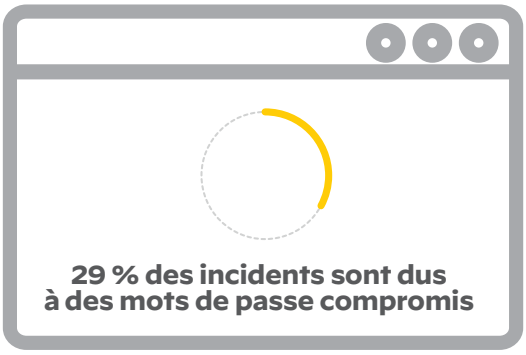

Figure 2 : vol d'identifiants d'après le rapport Verizon DBIR de 2019

Vous l'aurez compris : ces méthodes sont loin d'être infaillibles. Certains nouveaux sites malveillants passent à travers les mailles et pour échapper au filtrage d'e-mails, les attaquants envoient leurs liens malveillants sur les réseaux sociaux. Phishing, malwares, ingénierie sociale, force brute... ils n'ont que l'embarras du choix, d'autant que des fichiers d'identifiants volés sont disponibles à l'achat sur le Darknet. Ils s'en servent alors pour accéder à un réseau, s'y déplacer latéralement et obtenir des droits d'accès privilégiés à certaines applications et données.

La solution

Afin d'identifier les sites web de phishing, les entreprises doivent aujourd'hui s'équiper de pare-feu dotés d'un système de machine learning. Aujourd'hui, en cas d'identification d'un site malveillant, un pare-feu doit pouvoir se mettre à jour et bloquer le site incriminé. Seulement voilà, des sites de phishing inconnus apparaissent tous les jours. Face à ce risque, votre prochain pare-feu devra bloquer la saisie d'identifiants d'entreprise sur des sites inconnus. Pour empêcher l'utilisation d'identifiants volés, il devra également appliquer des techniques d'authentification multi- facteur (MFA) pour l'accès aux applications et données sensibles. En ce sens, un pare-feu compatible avec les principales solutions MFA du marché protégera vos applications contenant des données sensibles, même les plus anciennes.

3. Exécution sécurisée des applications et contrôle de leurs fonctions

Le problème

De plus en plus d'applications sont capables de transiter par des ports non standard ou peuvent changer dynamiquement de port, comme la messagerie instantanée, le partage de fichiers en pair à pair ou la voix sur IP (VoIP), par exemple. De leur côté, les utilisateurs accèdent à des applications très diverses, y compris des SaaS, à partir de différents lieux et appareils. Si certaines de ces applications sont approuvées, d'autres sont seulement tolérées, voire interdites. Or, les utilisateurs apprennent vite à passer outre en recourant à des ports non standard, via des protocoles RDP, SSH, etc.

Pour compliquer un peu plus la donne, de nouvelles applications proposent une richesse fonctionnelle censée fidéliser les utilisateurs, mais qui apporte avec elle son lot de risques pour votre entreprise. C'est le cas de WebEx®, un excellent outil professionnel dont les fonctions de partage de bureau permettent de prendre le contrôle du poste d'un salarié depuis une source externe. Or, ces fonctions pourront enfreindre vos politiques internes, voire la réglementation en vigueur. Autre exemple : Gmail® et Google Drive. Gmail fait souvent partie des applications autorisées. Mais une fois connectés, vos utilisateurs pourront accéder facilement à YouTube® et Google Photos, que vous n'aurez peut-être pas approuvées. Vos administrateurs sécurité ont donc besoin d'appliquer un contrôle granulaire sur l'utilisation de toutes les applications, c'est-à-dire en autorisant et en limitant certains types d'applications et de fonctions, tout en maintenant l'accès à d'autres.

2. « Rapport d'enquête de Verizon sur les compromissions de données », Verizon, 2019, https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.

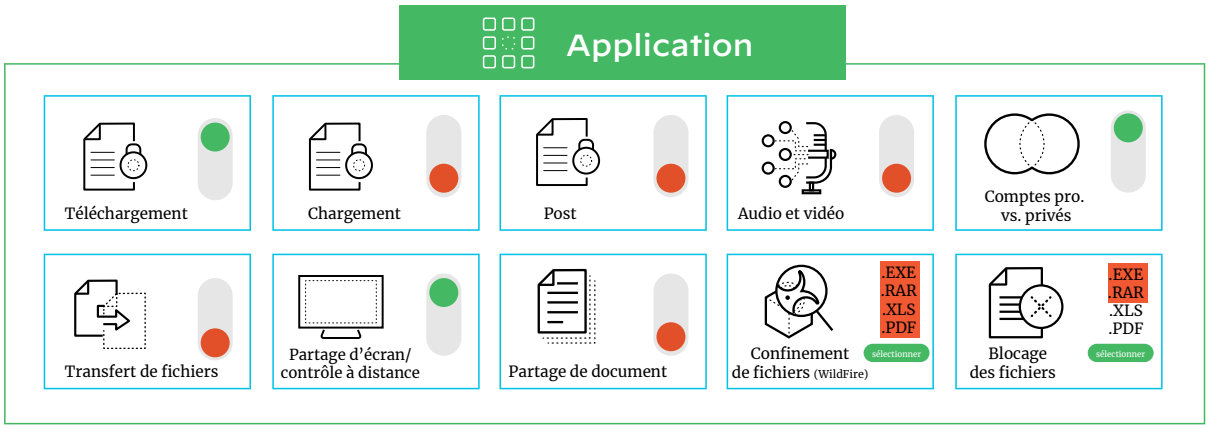

Figure 3 : contrôle de l'utilisation des applications selon la politique définie

La solution

Par défaut, votre prochain pare-feu devra continuellement classifier le trafic par application sur tous vos ports. Nul besoin de rechercher les ports couramment utilisés par chaque application. En d'autres termes, votre pare-feu fournira une visibilité complète sur l'utilisation de vos applications, ainsi que des fonctions d'analyse et de contrôle de ces usages (cf. Figure 3). Il devra donc comprendre le mode de fonctionnement des applications telles que le streaming audio, l'accès à distance et la publication de documents, mais également appliquer un contrôle strict de chacun de ces usages (permissions de chargement vs. téléchargement, chat vs. transfert de fichiers, etc.). Ce contrôle devra s'effectuer en continu. De fait, il sera impossible de classifier le trafic de façon définitive, car ces applications courantes partagent des sessions et prennent en charge de multiples fonctions. En cas d'introduction d'une nouvelle fonction en cours de session, le pare-feu devra donc procéder à un nouveau contrôle de politique. Afin de cerner les fonctions prises en charge par chaque application (et les différents risques associés), votre prochain pare-feu devra donc impérativement intégrer le suivi d'état en continu.

4. Consolidation de la cohérence des politiques

Le problème

Les pare-feu d'ancienne génération autorisent et bloquent le trafic en fonction des ports et des adresses IP. Or, les règles basées sur les ports laissent aussi passer les applications malveillantes. En effet, ces dernières peuvent aisément traverser les pare-feu traditionnels en recourant au « port hopping », aux protocoles SSL et SSH, ou en passant par des ports ouverts bien connus comme les ports 80 et 443. Au fil du temps, les entreprises accumulent des milliers de règles basées sur les ports, qu'elles migrent souvent telles quelles vers leur pare-feu nouvelle génération. Or, ces règles nuisent gravement à l'efficacité de leurs politiques. Les entreprises aimeraient alors passer à des règles basées sur les applications. Mais la pénurie de compétences en cybersécurité les prive souvent des ressources humaines nécessaires à un tel projet. Elles courent alors de graves risques de sécurité qui pourront perturber leur activité. D'ailleurs, selon Gartner, d'ici à 2023, 99 % des compromissions de pare-feu viendront d'erreurs de configuration, et non de failles intrinsèques.[3]

La solution

Recherchez un pare-feu qui puisse simplifier la gestion des règles et des politiques. Il devra identifier les applications exécutées sur votre réseau, les relier à vos règles existantes et vous aider à remplacer ces dernières. Un pare-feu nouvelle génération doit aider vos équipes de sécurité à remplacer ces règles par des politiques intuitives basées sur les applications. Parce que les règles basées sur l'identification des applications sont simples à créer, à comprendre et à modifier au fil de l'évolution de vos besoins métiers, elles réduisent les erreurs de configuration qui vous exposent à des violations de données. Bien moins lourdes à gérer, ces politiques renforcent donc votre sécurité.

5. Sécurisation du trafic chiffré

Le problème

Aujourd'hui, la plupart du trafic web est chiffré, ce qui permet aux attaquants de s'y dissimuler pour contourner les équipements de sécurité. Par conséquent, même les entreprises qui ont mis en place des mesures de sécurité exhaustives s'exposent à une intrusion si elles ne surveillent pas leur trafic chiffré. En outre, le protocole SSH est aujourd'hui si répandu que même vos utilisateurs peuvent s'en servir pour dissimuler leurs activités personnelles sur votre réseau.

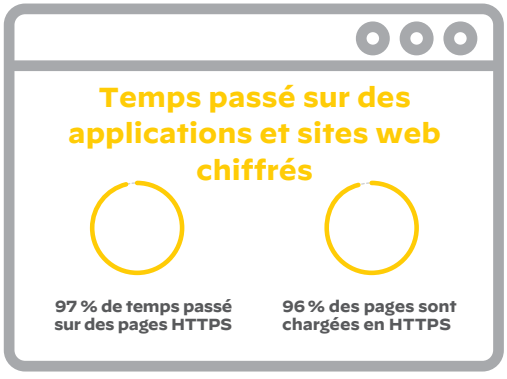

Figure 4 : le trafic chiffré d'après le rapport Google 2019[4]

3. Rajpreet Kaur, Adam Hils, John Watts, « Technology Insight for Network Security Policy Management », Gartner, 21 février 2019, https://www.gartner.com/doc/3902564/technology-insight-network-security-policy.
4. Rapport « Transparence des informations : Chiffrement HTTPS sur le Web », Google, Inc., consulté le 5 février 2020, https://transparencyreport.google.com/https/overview?hl=en.

La solution

Le déchiffrement des protocoles SSL et SSH fait partie des fonctions de sécurité incontournables. C'est pourquoi vous opterez de préférence pour un pare-feu équipé de fonctions de reconnaissance et de déchiffrement du trafic entrant et sortant sur n'importe quel port, de contrôle du déchiffrement basé sur les politiques, et des matériels et logiciels nécessaires pour déchiffrer des dizaines de milliers de connexions SSL simultanées sans dégradation des performances. Votre pare-feu doit cependant se montrer suffisamment flexible pour vous permettre de déchiffrer facilement certains types de trafic (le trafic HTTPS d'un site inconnu, par exemple), tout en laissant passer le trafic de sites de confiance sans déchiffrement (celui d'un établissement financier connu, par exemple), conformément à certaines réglementations sur le respect de la vie privée.

Un pare-feu nouvelle génération devra également sécuriser et répartir la charge des flux de données déchiffrées à travers de multiples équipements de sécurité pour un contrôle renforcé. Ce faisant, vous éliminerez le besoin d'outils de déchargement (offloaders) SSL dédiés, ce qui simplifiera votre architecture réseau et vos opérations de déchiffrement. Il doit également prendre en charge le déchiffrement de protocoles modernes tels que TLS 1.3 et HTTP/2, de plus en plus répandus. Lisez le livre blanc Déchiffrement : où, pourquoi et comment pour en savoir plus sur cette importante fonction.

6. Blocage des menaces avancées pour neutraliser les cyberattaques

Le problème

La plupart des malwares d'aujourd'hui (y compris les ransomwares) reposent sur des techniques avancées comme la dissimulation de payloads malveillants dans des fichiers légitimes et la compression de fichiers. L'objectif : contourner les systèmes de détection des équipements et outils de sécurité réseau. À l'heure où de plus en plus d'entreprises déploient des sandbox virtuelles pour leurs analyses dynamiques, les attaquants cherchent sans cesse la parade. Ils partent en quête d'activités utilisateurs légitimes, de configurations système et d'indicateurs de technologies de virtualisation qu'ils pourront détecter et exploiter. Le développement du Darknet leur facilite la tâche puisqu'il permet à tout attaquant, novice ou confirmé, d'acheter des exploits clé en main pour repérer et contourner les analyses anti-malware.

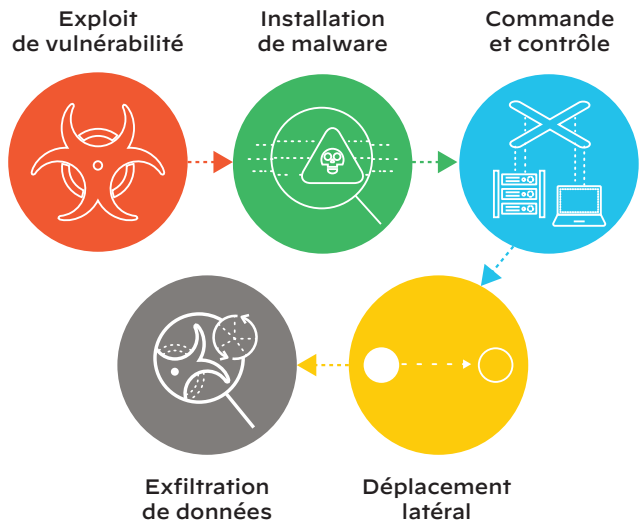

Figure 5 : Neutralisation des attaques à tous les stades

La solution

Votre pare-feu devra intégrer des services de sécurité capables de bloquer automatiquement les menaces connues, mais pas que : il devra également analyser et neutraliser automatiquement les menaces inconnues. En clair, votre entreprise a besoin d'un service qui, via de solides systèmes d'analyse et d'intégration, ainsi que différentes parties de votre infrastructure de sécurité, examine les comportements et identifie les menaces à tous les stades du cycle d'une cyberattaque, et non uniquement à leur point d'entrée sur votre réseau. En bloquant les types de fichiers à risque et l'accès aux URL malveillantes avant même qu'ils ne compromettent votre réseau, vous pouvez réduire votre niveau d'exposition. Votre pare-feu devra donc vous protéger contre les malwares, les exploits et les activités de commande et contrôle (CnC) connus, tout en vous épargnant la gestion et la maintenance de multiples équipements spécialisés. Autre impératif : la mise à jour automatique des signatures dès l'identification d'un nouveau malware. Ainsi, votre pare-feu garantira votre protection et permettra à vos équipes de sécurité et de réponse aux incidents de se concentrer sur les cas prioritaires.

Un pare-feu nouvelle génération qui utilise diverses méthodes d'analyse (analyse statique assistée par machine learning, analyse dynamique, analyse bare-metal, etc.) saura détecter les menaces inconnues avec une extrême précision et neutraliser les tentatives de contournement. Au lieu de signatures basées sur des attributs spécifiques, votre pare-feu devrait s'appuyer sur des signatures basées sur le contenu, l'objectif étant de détecter les variantes de malwares, les malwares polymorphes et les activités CnC. En outre, les signatures des activités CnC basées sur l'analyse des schémas de communications sortantes s'avèrent bien plus efficaces et évolutives lorsqu'elles sont créées automatiquement. Enfin, votre protection passe impérativement par une infrastructure de sécurité dans le cloud, car seul le cloud permet de détecter et neutraliser des menaces à très grande échelle à travers votre réseau, vos terminaux et vos environnements cloud. Cette infrastructure vous donnera également accès à un écosystème ouvert de fournisseurs innovants et de confiance.

7. Blocage des attaques DNS

Le problème

Souvent négligé, le trafic DNS représente pourtant un vecteur d'attaque particulièrement fréquent. Les attaquants s'en servent notamment pour propager des malwares, établir des communications de commande et contrôle (CnC) et exfiltrer des données. L'omniprésence du DNS leur permet également de l'exploiter à différentes étapes du cycle d'attaque. Selon l'équipe Unit 42 de Palo Alto Networks, près de 80 % des malwares utilisent le DNS pour établir des communications avec un serveur CnC. Ces dernières sont difficiles à identifier ou à bloquer compte tenu de l'opacité du trafic DNS. Une fois la connexion établie, les attaquants peuvent utiliser ce trafic pour infecter un réseau par malware ou exfiltrer des données. Par ailleurs, ils développent des algorithmes DGA qui génèrent automatiquement des milliers de noms de domaines malveillants pour établir une persistance de leurs activités CnC. À l'heure où de plus en plus d'attaques sont automatisées, ces menaces deviennent quasiment impossibles à détecter et neutraliser.

La solution

Votre entreprise ne peut se contenter de placer les domaines liés aux attaques DNS sur liste noire. Cette tactique dépend souvent de données relativement statiques qui ne bloquent que des domaines malveillants connus. Or, cela ne suffit pas pour contrer des domaines hautement dynamiques. C'est pourquoi il vous faut un pare-feu nouvelle génération qui puisse utiliser l'analyse prédictive et le machine learning de façon à identifier de manière dynamique les domaines malveillants inconnus.

8. Protection d'une population croissante de collaborateurs mobiles

Le problème

Plus vos collaborateurs se déplacent, plus ils se connectent à vos applications depuis des appareils mobiles. Souvent, ces connexions s'opèrent sur des appareils et réseaux publics exposés aux menaces avancées. Le risque est encore plus élevé lorsqu'ils travaillent hors site, sans pare-feu réseau pour bloquer les attaques. Le cloud et le BYOD (Bring Your Own Device, ou l'utilisation de son matériel personnel) ne font qu'accentuer le problème. Par ailleurs, les systèmes de sécurité de vos sites distants et succursales de petite taille manquent souvent d'homogénéité, car le déploiement de pare-feu sur ces sites et les backhauls avec le siège s'avèrent aussi inefficaces que coûteux.

Prise en charge intégrale de tous les systèmes d'exploitation

Au vu du succès des initiatives BYOD et de la prolifération des utilisateurs mobiles, une prise en charge intégrale des environnements et workloads Windows®, macOS®, Android® et Linux s'impose. Seule cette couverture totale permettra de combattre efficacement les malwares connus et inconnus, quel que soit le système d'exploitation choisi par leur utilisateur.

La solution

Vos collaborateurs mobiles et sites distants doivent pouvoir accéder à vos applications par-delà les frontières de votre réseau. Vous devez également les protéger contre les cyberattaques ciblées, les applications et sites web malveillants, le phishing, le trafic CnC et bien d'autres menaces inconnues. Face à tous ces risques, vous devez présenter un front uni. Votre prochain pare-feu devra donc offrir des niveaux de visibilité, de prévention des menaces et de contrôle des politiques de sécurité suffisants pour protéger vos utilisateurs et sites distants. Mais pour y parvenir, toutes les fonctionnalités NGFW devront opérer en mode cloud pour éviter le déploiement de matériels dédiés sur chaque site.

9. Sécurisation d'environnements cloud en mutation permanente

Le problème

Vos données et applications sont désormais partout, sur votre réseau et dans le cloud. D'après l'édition 2019 du State of the Cloud Report™ de RightScale, 84 % des entreprises recourent à plusieurs clouds publics, privés et/ou hybrides, pour une moyenne de cinq clouds différents.[5] Les entreprises doivent donc aujourd'hui sécuriser des données sensibles sur leur réseau, mais aussi sur une grande variété de clouds, sur fond d'adoption à marche forcée des applications SaaS. Le problème, c'est que les instruments et techniques de sécurité traditionnels, conçus pour les réseaux statiques, sont mal adaptés aux outils et fonctionnalités cloud-natives. Par ailleurs, les services de sécurité natifs des fournisseurs cloud comme Google Cloud Platform (GCP™), Amazon Web Services (AWS®) et Microsoft Azure® ne protègent généralement que la couche L4 de la solution dudit fournisseur.

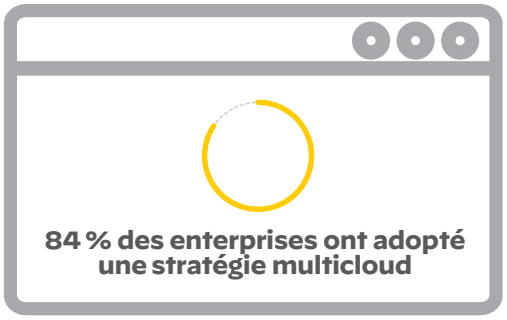

Figure 6 : la stratégie multicloud d'après le rapport RightScale

La solution

Votre entreprise a besoin d'une solution de sécurité cloud capable d'étendre vos politiques du réseau vers le cloud et d'empêcher les malwares de s'infiltrer et de se propager latéralement (est-ouest) dans les environnements cloud. Cette solution devra simplifier votre gestion et aligner vos politiques de sécurité sur les variations dynamiques de vos workloads virtuels. En ce sens, votre prochain pare-feu devra assurer le même niveau de sécurité que votre réseau physique. Pour la sécurisation de déploiements multicloud, ce pare-feu devra prendre en charge une grande variété d'environnements virtuels et cloud, y compris tous ceux des principaux fournisseurs de cloud public et de cloud privé virtualisé. Cela comprend une intégration aux services cloud natifs comme Amazon Lambda et Azure, et aux outils d'automatisation comme Ansible® et Terraform® de façon à intégrer la sécurité à tous vos projets de développement « cloud-first ».

10. Stratégie « Zero Trust »

Le problème

Les modèles de sécurité traditionnels se basent sur le principe (dépassé) selon lequel tout ce qui se situe à l'intérieur d'un réseau est digne de confiance. Ils ne font donc que sécuriser le périmètre du réseau, laissant libre cours aux intrus de compromettre des données sensibles et stratégiques. À l'ère du digital, la confiance ne devient ni plus ni moins qu'une vulnérabilité.

La solution

Préférez un pare-feu nouvelle génération capable d'agir comme une passerelle de segmentation pour l'implémentation d'une architecture « Zero Trust ». Le Zero Trust est une stratégie de cybersécurité qui éradique toute notion de confiance. Autrement dit, plus question de considérer le moindre appareil, système ou individu comme sûr. Une approche « Zero Trust » nécessite de : 1) identifier les données, ressources, applications et services essentiels à votre activité ; 2) déterminer les accès selon le rôle de chacun ; 3) adopter un modèle du moindre privilège par la segmentation des réseaux, une politique de sécurité complète sur la couche 7, le contrôle des accès utilisateurs et la prévention des menaces.

5. « 2019 State of the Cloud Report », RightScale, 27 février 2019, https://resources.flexera.com/web/media/documents/rightscale-2019-state-of-the-cloud-report-from-flexera.pdf.

Accès sécurisés des utilisateurs où qu'ils soient, inspection de tout le trafic, politiques d'accès soumises au principe du moindre privilège, détection et prévention des menaces avancées… votre prochain pare-feu nouvelle génération devra être présent sur tous ces fronts, ce qui est la base d'une stratégie « Zero Trust ». Il réduira ainsi considérablement les possibilités d'accès à vos données et applications les plus critiques, que la menace se situe à l'intérieur ou à l'extérieur de votre entreprise. Visionnez ce webinaire pour tout savoir sur l'implémentation d'une approche « Zero Trust ».

11. Homogénéité des politiques sur site, dans le cloud, sur les réseaux distants et mobiles

Le problème

Les entreprises ont adopté de nombreux produits spécialisés pour répondre à leurs besoins en matière de réseau et de sécurité. Le problème, c'est que ces produits ont leur propre politique et leur propre interface à gérer. Finalement, ils coûtent donc plus cher, compliquent les processus et entraînent des failles de sécurité. De plus, n'étant pas reliés, ils ne communiquent pas entre eux sur les accès au réseau et aux applications ni sur les violations des politiques, et ne fusionnent pas les journaux de données. Les entreprises peinent également à déployer de nombreux pare-feu à la fois, à homogénéiser leurs politiques de sécurité et à modifier en urgence des milliers de pare-feu. Failles de sécurité, performances réseau amoindries, personnel insuffisant, manque de moyens financiers… Que de points négatifs.

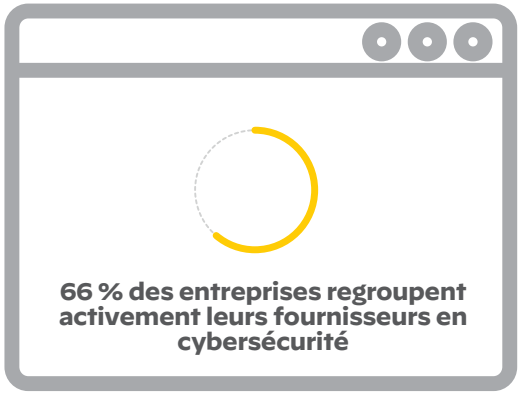

Figure 7 : la consolidation des fournisseurs en cybersécurité d'après ESG Research

La solution

Selon ESG Research, 66 % des entreprises regroupent activement les différents fournisseurs en cybersécurité avec lesquels elles font affaire.[6] Pour cela, vous devez mettre en place des politiques de sécurité homogènes et centralisées pour des dizaines de milliers de pare-feu répartis sur vos sites et dans le cloud (notamment les sites et utilisateurs distants, ainsi que les applications SaaS) grâce à un système de gestion centralisé, à la consolidation des tâches essentielles et à des fonctionnalités plus efficaces. Par exemple, vous devez pouvoir visualiser tout votre trafic réseau, gérer vos configurations, appliquer des politiques globales et générer des rapports de trafic et d'incident depuis une seule et même console. Vos fonctions de reporting doivent fournir une vue détaillée des comportements de vos utilisateurs, de vos applications et de votre réseau pour permettre à vos équipes de sécurité de prendre les bonnes décisions.

Lorsque ces fonctions sont fournies par le cloud, vos équipes bénéficient du réseau et de la sécurité nécessaires dans une architecture qui gère à la fois le trafic, les applications et les utilisateurs, où qu'ils soient. Dans un contexte de mutation permanente des menaces, il n'est pas toujours aisé de s'appuyer sur un seul et même fournisseur de sécurité pour répondre à des besoins très divers. D'où le besoin capital d'intégrer et d'exploiter les innovations et analyses d'autres solutions. Vous veillerez donc à bien évaluer l'extensibilité et la programmabilité des offres des fournisseurs. Cet e-book vous expliquera comment mieux sécuriser vos activités sur le cloud et comment accélérer et fluidifier votre réseau.

12. Automatisation des tâches courantes pour se concentrer sur les menaces prioritaires

Le problème

D'après un rapport de 2017 de Cybersecurity Ventures, il y aura 3,5 millions de postes à pourvoir dans la cybersécurité d'ici à 2021.[7] Pour ne rien arranger, les entreprises concernées sont excessivement tributaires de processus manuels pour leurs opérations de sécurité quotidiennes (traçage des données, recherche des faux positifs, gestion de la remédiation, etc.). De fait, l'analyse et la corrélation manuelles d'un très grand nombre d'évènements de sécurité ralentissent les efforts de neutralisation, augmentent le risque d'erreurs et sont incapables de faire face à une augmentation de la charge. Il n'est alors pas rare que les équipes de sécurité se retrouvent submergées par le volume d'alertes et passent à côté de menaces critiques. La pénurie croissante de compétences en cybersécurité ne fait que compliquer la donne. Si les analyses Big Data savent mettre en lumière les corrélations, les patterns cachés et d'autres informations dont les équipes de sécurité ont besoin pour agir, encore faut-il que ces données soient pertinentes. En clair, il est essentiel de disposer de données techniquement analysables et issues de toutes les sources possibles (réseaux, terminaux, applications SaaS, clouds publics, clouds privés, data centers, etc.).

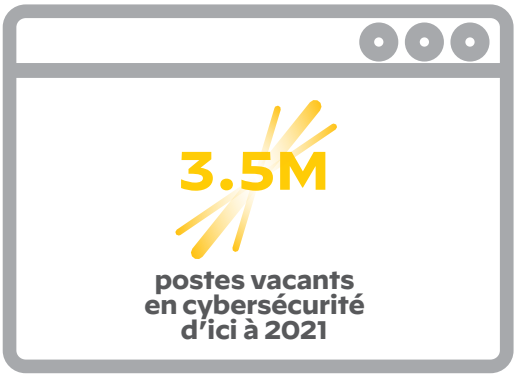

Figure 8 : les postes en cybersécurité d'après Cybersecurity Ventures

6. « The Cybersecurity Technology Consolidation Conundrum », 26 mars 2019, https://www.esg-global.com/blog/the-cybersecurity-technology-consolidation-conundrum.
7. « Cybersecurity Jobs Report 2018-2021 », Cybersecurity Ventures, 31 mai 2017, http://cybersecurityventures.com/jobs.

La solution

Une analytique précise est le point de départ d'une mise en œuvre automatisée et simplifiée de bonnes pratiques comme le modèle « Zero Trust ». Accélération du déploiement des applications, amélioration des processus, traque des menaces… quels que soient les objectifs, vous pouvez rationaliser les tâches courantes et ainsi vous recentrer sur vos véritables priorités. Les trois axes de votre automatisation :

1. **Automatisation des workflows :** Le pare-feu doit exposer les API standard pour permettre sa configuration à partir d'autres outils et scripts utilisés. Dans le cloud, il doit s'intégrer à des outils comme Ansible et Terraform. Il doit également pouvoir initier des workflows sur d'autres équipements de votre écosystème de sécurité, à l'aide d'API et sans intervention manuelle.
2. **Automatisation des politiques :** Le pare-feu doit pouvoir adapter les politiques en fonction des changements dans votre environnement, notamment les mouvements d'applications entre différentes machines virtuelles. Il doit également pouvoir ingérer les données de Threat Intelligence de sources externes et agir automatiquement en conséquence.
3. **Automatisation de la sécurité :** Votre environnement doit pouvoir identifier les menaces inconnues et transmettre leurs caractéristiques à votre pare-feu afin de bloquer automatiquement toute nouvelle menace.

Certaines menaces peuvent néanmoins rester enfouies dans la masse de données. Dans ce cas, seule une analyse plus approfondie à travers les différents sites et types de déploiement permettra de les détecter. Là encore, l'automatisation vous permet d'identifier les menaces avec précision, d'accélérer la prévention, d'améliorer votre efficacité, de renforcer votre sécurité et de mieux utiliser les compétences de vos équipes.

13. Coordination de la détection et des analyses avec d'autres outils de sécurité

Le problème

Vos adversaires les plus tenaces ne se limiteront pas à une seule partie de votre architecture. Leur but est bel et bien de passer par vos terminaux pour accéder à votre réseau, vos environnements cloud et vos autres structures pour en exfiltrer de précieuses données. En ce sens, si votre système de sécurité se porte uniquement sur une partie de votre infrastructure, les résultats n'en seront qu'insuffisants. En effet, les possibilités d'analyse seront alors limitées et vos analystes contraints de passer d'une interface à l'autre pour tenter manuellement de faire le lien entre les différentes attaques. Inutile de préciser qu'il s'agit d'un processus aussi chronophage que faillible.

La solution

Plus le nombre de fonctions de sécurité indispensables augmente, plus les plateformes et les appareils qui peuvent les faire coïncider deviennent intéressants. Si votre pare-feu peut faire office de capteur et de point de contrôle pour une plateforme d'analyse plus complète axée sur le machine learning (par exemple, une solution XDR), votre équipe de sécurité pourra détecter, pallier et prévenir les attaques les plus complexes de manière nettement plus efficace. Une bonne intégration permettra à vos équipes réseau et de sécurité de comprendre parfaitement l'étendue de chaque attaque, de partager des informations en contexte sur les menaces et d'automatiser les tâches de contrôle et de réponse aux incidents entre le pare-feu et les autres points de contrôle.

14. Consolidation de la connectivité et de la sécurité

De plus en plus d'entreprises se tournent vers le numérique et transfèrent leurs applications sur le cloud. Les équipes informatiques font alors face à un nouveau défi : permettre aux sites et succursales de leur entreprise d'accéder aux ressources essentielles de manière fiable, sécurisée et rapide. Les entreprises l'ont bien compris : le SD-WAN ou Software-defined wide area networking promet d'augmenter la bande passante tout en améliorant la connectivité et les performances. Gartner avait annoncé que le SD-WAN serait inclus dans 75 % des actualisations des infrastructures WAN avant 2020.[8] Cependant, malgré tous ses avantages, il présente également son lot d'inconvénients, notamment un niveau de sécurité médiocre ou en option, une complexité imprévue dans l'architecture et le déploiement et des performances incertaines.

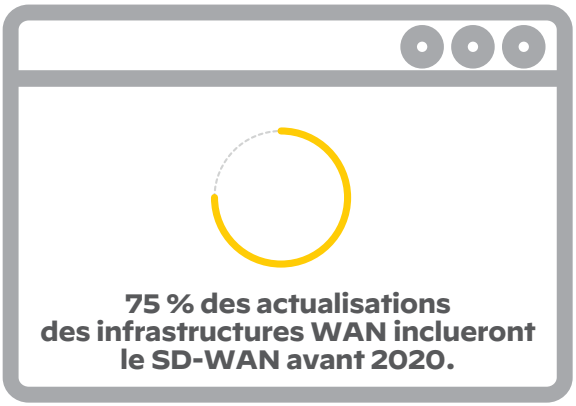

Figure 9 : l'adoption du SD-WAN d'après Gartner

La solution

Votre prochain pare-feu devra assurer une sécurité homogène de vos data centers, de vos environnements cloud et de vos succursales. Pour adopter le SD-WAN en toute sécurité, vous devez installer un pare-feu qui puisse l'intégrer nativement afin de consolider connectivité et sécurité. Cela pourra également vous aider à homogénéiser vos politiques de sécurité sur votre réseau et dans vos succursales. Grâce à la configuration et la surveillance du SD-WAN, ainsi qu'aux workflows de politiques relatives aux utilisateurs et aux applications au sein du pare-feu (disponibles sur une même console), vous pourrez éviter les failles de sécurité et gagner en sécurité, en simplicité et en efficacité. Cet e-book vous expliquera comment bénéficier d'une sécurité homogène grâce au SD-WAN.

8. Mike Toussaint, Ted Corbett, Andrew Lerner, « 6 Critical Questions to Ask on SD-WAN », Gartner, 6 juin 2018, https://www.gartner.com/en/documents/3877766/6-critical-questions-to-ask-on-sd-wan.

Recours à l'appel d'offres pour sélectionner un pare-feu nouvelle génération

Questions utiles et facteurs à prendre en compte

Les pare-feu nouvelle génération doivent proposer des fonctions qui assurent une sécurité optimale, mais doivent aussi s'intégrer parfaitement à d'autres outils de prévention, de détection et de réponse dans l'ensemble de votre infrastructure. Dans cette section, nous exposons les critères de sélection sous forme de checklist pour vous aider à évaluer la qualité des pare-feu que vous envisagez d'acquérir. Cette checklist vous servira de point de départ. À vous ensuite de l'adapter selon vos besoins afin d'identifier les fournisseurs qui seront le plus à même de protéger votre entreprise.

Identification des utilisateurs et autorisations d'accès adaptées

Votre pare-feu nouvelle génération peut-il :

- assurer une politique de sécurité homogène pour vos utilisateurs mobiles ?
- protéger les utilisateurs qui ne travaillent pas derrière un pare-feu nouvelle génération ?
- assurer une connexion VPN permanente grâce à plusieurs pare-feu physiques/virtualisés ?
- se servir du cloud pour protéger davantage les utilisateurs ?

Prévention du vol et de l'usage malveillant d'identifiants

Votre pare-feu nouvelle génération peut-il :

- bloquer l'utilisation d'identifiants sur des sites inconnus ?
- empêcher les utilisateurs de saisir leurs identifiants sans stocker une copie du hâchage ?
- anaylser rapidement les sites de phishing auparavant inconnus et les enregistrer pour améliorer le système de protection ?
- enregistrer les tentatives de saisie d'identifiants au moment du post HTTP ?
- prendre en charge la MFA (authentification à facteur multiple) dans le cadre d'une politique de contrôle d'accès basée sur le degré de sensibilité des ressources ?
- proposer de nombreuses solutions MFA ?
- prendre en charge l'intégration d'API aux solutions MFA ?
- prendre en charge la politique MFA pour tout type d'application (web, client-serveur, terminaux virtuels, etc.) ?
- prendre en charge la fonction MFA sur tous types de protocoles ?

Exécution sécurisée des applications et contrôle de leurs fonctions

- Votre pare-feu peut-il détecter les applications qui peuvent échapper à la détection au moyen de ports non standard, du « port hopping » ou en étant configurées pour être exécutées sur un autre port ?
- En matière de classification de trafic, la première tâche exécutée par le pare-feu est-elle basée sur l'identité de l'application ou le port réseau ?
  - » Les mécanismes d'identification des applications font-ils partie de la classification de base du trafic dans le pare-feu (sont-ils activés par défaut) ?
  - » Les mécanismes d'identification des applications dépendent-ils du port standard leur correspondant ?
  - » Les signatures peuvent-elle être appliquées à tous les ports ? Le processus est-il configuré automatiquement ou manuellement ?
- Lorsque le trafic atteint l'appareil, est-il classifié tout d'abord en fonction du port (par exemple le port 80, donc un trafic HTTP) ou en fonction de l'application (par exemple Gmail®)?
- Décrivez en détail la façon dont le pare-feu identifie précisément les applications :
  - » Outre les signatures, quels sont les mécanismes utilisés pour classifier le trafic ?
  - » Quelle est la portée du décodeur d'applications et de protocoles ?
  - » Comment le déchiffrement et le contrôle SSL et SSH sont-ils mis en œuvre ?
  - » Les mécanismes de classification du trafic sont-ils appliqués uniformément sur tous les ports ?
- Quels sont les mécanismes utilisés pour détecter des applications de contournement comme UltraSurf ou le P2P anonyme ?
- L'identification des applications a-t-elle lieu dans le pare-feu ou est-elle assurée dans un deuxième temps, après la classification basée sur les ports ?
- Le suivi de l'état des applications est-il disponible ? Si oui, comment son exécution assure-t-elle le contrôle homogène des applications et des fonctions secondaires associées ?
- L'identité des applications est-elle le fondement des politiques de sécurité du pare-feu ou le contrôle des applications est-il traité comme un élément secondaire de la politique ?
- À quelle fréquence la base de données d'applications est-elle mise à jour ? S'agit-il d'une mise à jour dynamique ou d'une mise à niveau par redémarrage du système ?

Consolidation de la cohérence des politiques

- La classification du trafic par inspection avec état est-elle effectuée séparément, plus précisément avant l'identification des applications ? Lorsqu'une application est identifiée, comment ses changements d'états sont-ils contrôlés, suivis et utilisés dans le cadre de la politique ?
- Comment la hiérarchie de la base de données d'applications (plate, multiniveaux ou autre) expose-t-elle les fonctions au sein de l'application parente pour faciliter la mise en place de stratégies plus granulaires ?
- Quels niveaux de contrôle est-il possible d'exercer sur des applications individuelles et leurs fonctions respectives ?
- Les contrôles fondés sur les ports peuvent-ils être mis en œuvre pour l'ensemble des applications dans la base des données de façon à ce qu'un administrateur puisse déterminer, par le biais d'une politique, la relation entre l'application et le port ? Par exemple :
  - » S'assurer que l'équipe informatique est la seule à avoir le droit d'utiliser SSH et RDP.
  - » Détecter et bloquer les malwares au sein de l'application, même s'ils passent par un port non standard.
- Quels sont les annuaires d'identités de l'entreprise pris en charge par les contrôles basés sur les utilisateurs ?
- Une API est-elle disponible pour une intégration identité-infrastructure personnalisée ou non standard ?
- Comment les contrôles basés sur les politiques sont-ils mis en œuvre par les utilisateurs et les groupes dans des environnements de services terminaux ?
- Le cas échéant, en quoi les options d'activation des applications varient-elles selon qu'il s'agit d'un environnement physique ou virtuel ?

Sécurisation du trafic chiffré

- Quel processus permet d'identifier les applications chiffrées sur tous les ports, y compris les ports non standard ?
- Quels sont les contrôles stratégiques en place permettant de déchiffrer, inspecter et contrôler de manière sélective des applications utilisant le protocole SSL ?
- L'identification, le déchiffrement et l'inspection bidirectionnels SSL sont-ils pris en charge ?
- Le déchiffrement SSL est-il assuré en standard ou suppose-t-il un coût supplémentaire ? Un équipement dédié est-il requis ?
- Le contrôle SSH (mode d'accès aux appareils distants) est-il pris en charge ? Si oui, quelles sont les possibilités de contrôle ?
- Quels sont les mécanismes utilisés pour détecter des applications de contournement comme UltraSurf ou Tor ?
- Comment le produit peut-il automatiquement identifier une solution de contournement passant par un port non standard ?

Blocage des menaces avancées pour neutraliser les cyberattaques

- Votre système d'analyse sur le cloud permet-il de détecter les malwares évasifs visant les sandbox par le biais de différentes techniques, notamment l'analyse bare-metal ?
- Votre système d'analyse sur le cloud exploite-t-il un hyperviseur personnalisé pour combattre efficacement les malwares visant les sandbox ?
- Suite à l'analyse des malwares, votre système d'analyse crée-t-il des signatures de prévention des menaces ? Par exemple :
  - » Des signatures AV basées sur le contenu permettant de prévenir l'apparition de variantes de malwares connus et inconnus ?
  - » Des signatures antispyware basées sur les patterns permettant de détecter toute communication avec des infrastructures CnC connues et inconnues ?
- Votre système d'analyse sur le cloud prend-il en charge l'analyse des malwares pour les fichiers des systèmes d'exploitation Windows®, Android® et macOS® ?
- Votre pare-feu nouvelle génération bloque-t-il l'accès des applications et URL inconnues aux exécutables et autres types de fichiers à risque en vue de prévenir les attaques de ransomwares ?
- Votre pare-feu nouvelle génération inscrit-il automatiquement sur liste noire tous les IOC connus (adresses IP, domaine et URL) en vue de détecter les familles de ransomware connues de manière proactive ?
- L'intégration de la Threat Intelligence du cloud à votre pare-feu nouvelle génération permet-elle la mise à jour dynamique des URL malveillantes associées aux ransomewares dans la catégorie malware de la base de données de filtrage ?
- Votre pare-feu nouvelle génération et votre logiciel de protection des terminaux peuvent-ils échanger des informations sur les menaces et les comportements des ransomwares ?

Blocage des attaques DNS

- L'intégration de la Threat Intelligence du cloud à votre pare-feu nouvelle génération permet-elle la mise à jour dynamique des domaines malveillants associés aux ransomewares sous forme de signatures DNS en vue de les inscrire sur liste noire ou de les mettre en entonnoir ?

Protection d'une population croissante de collaborateurs mobiles

- De manière précise, quelles sont les options disponibles, y compris les composants nécessaires, pour sécuriser les utilisateurs distants ?
  - » S'il existe un composant client, comment celui-ci est-il distribué ?
- Quels sont vos besoins en matière de volume ? Combien d'utilisateurs peuvent-ils être pris en charge simultanément ?
- L'ensemble des fonctions de sécurité des utilisateurs distants est-il transparent pour le client ?
- Comment le contrôle des politiques se fait-il pour les utilisateurs distants (politique du pare-feu, politique/équipement distincts, autre) ?
- Quelles sont les fonctionnalités et les protections fournies par le biais des outils distants (SSL, contrôle des applications, IPS, etc.) ?
- Votre pare-feu permet-il aux utilisateurs de rester connectés où qu'ils se trouvent et donc d'assurer une application cohérente des politiques ?
- Comment gérez-vous les utilisateurs d'appareils mobiles ? Pourrez-vous appliquer une politique uniforme si des utilisateurs travaillent sur des réseaux externes et des réseaux sans fil internes ?
- Le pare-feu peut-il prendre en charge les problèmes liés à l'utilisation d'appareils personnels et sécuriser à la fois les équipements professionnels et personnels (ordinateurs portables, téléphones et tablettes) ?

Sécurisation d'environnements cloud en mutation permanente

- Comment le pare-feu nouvelle génération crée-t-il des politiques de sécurité en fonction des attributs VM des workloads ?
- Comment le pare-feu nouvelle génération peut-il créer des politiques de sécurité pour les workloads dynamiques dans les clouds privés et publics ?
- Le pare-feu nouvelle génération peut-il créer des politiques de sécurité homogènes pour les workloads même si les adresses IP et les lieux associés changent dans le data center ?
- Dans les environnements virtualisés, comment le trafic est-il classifié sur la machine virtuelle (est/ouest, nord/sud) ?
  - » Quels sont les points d'intégration au sein de l'environnement virtualisé ?
  - » Quelles sont les étapes de l'élaboration des politiques de sécurité pour les machines virtuelles nouvellement créées ?
  - » Quelles sont les fonctionnalités disponibles pour suivre le déplacement, l'ajout et la modification des machines virtuelles ?
  - » Quelles sont les fonctionnalités disponibles pour l'intégration avec les systèmes d'automatisation et d'orchestration ?

Stratégie « Zero Trust »

- Votre pare-feu nouvelle génération vous permet-il de rédiger des politiques contextualisées de façon à définir qui peut accéder à votre surface de protection ?
- Comment le pare-feu nouvelle génération exploite-t-il la segmentation du réseau ? Comment prévient-il les déplacements latéraux ? Comment assure-t-il la prévention des menaces sur la couche 7 ? Et comment simplifie-t-il le contrôle granulaire des accès utilisateurs ?
- Le pare-feu nouvelle génération inspecte-t-il l'ensemble du trafic à la recherche de contenu malveillant, d'activités non autorisées et de journaux jusqu'à la couche 7, à travers tout le réseau et les environnements cloud ?

Homogénéité des politiques sur site, dans le cloud, sur les réseaux distants et mobiles

- Les administrateurs locaux peuvent-ils intervenir directement sur l'appareil et en modifier la configuration sans se connecter à un outil de gestion centralisée ?
- Les administrateurs centralisés peuvent-ils surveiller et consulter les changements effectués par leurs homologues locaux ?
- Pouvez-vous décider de quels changements de configuration d'administrateur vous souhaitez appliquer sur les pare-feu ?
- En cas d'erreur, pouvez-vous rapidement restaurer la dernière configuration fonctionnelle ?
- Le gestionnaire central des pare-feu peut-il dissocier gestion des journaux et gestion de la configuration de base, tout en offrant une visibilité unifiée ?
- Vos gestionnaires peuvent-ils ingérer des journaux à haut débit (par exemple, 50 000/s) ?
- Votre pare-feu dispose-t-il d'API pour chaque fonctionnalité, vous permettant d'automatiser les changements de configuration ?

Automatisation des tâches de routine pour se recentrer sur les menaces prioritaires

- Votre fournisseur de système de sécurité propose-t-il une fonction permettant de générer automatiquement des signatures de prévention des menaces tout au long du cycle d'attaque pour toutes les données concernées ?
- Votre pare-feu peut-il identifier et faire le lien entre les hôtes infectés, puis les mettre en quarantaine de manière à limiter leur accès au réseau ?
- Votre pare-feu peut-il déclencher la MFA de façon à empêcher le détournement d'identifiants, et sécuriser les applications clés ?
- Votre pare-feu peut-il faire le lien entre les menaces constatées sur le réseau et les informations obtenues grâce à la threat intelligence ?

Coordination de la détection et de l'analyse des autres outils de sécurité

Votre pare-feu ou votre gestionnaire peut-il :

- Créer un ticket sur un système de gestion des changements pour signaler une activité malveillante au sein du pare-feu lui-même ?
- Provoquer la mise en quarantaine d'un hôte infecté sur le réseau sans fil ?

Votre pare-feu nouvelle génération peut-il :

- être intégralement programmé par le biais d'API ?
- collecter par le biais d'API et à partir de contrôleurs sans fil les identifiants utilisateurs des hôtes qui se connectent aux réseaux sans fil ?
- intégrer activement des flux CTI personnalisés ou provenant de tiers au pare-feu sans l'intervention d'une politique ?

Votre architecture de sécurité :

- prend-elle l'agrégation, la consolidation et la déduplication des flux CTI avant de transmettre les indicateurs à votre pare-feu ?
- peut-elle s'intégrer à votre pare-feu nouvelle génération afin d'automatiser l'expiration des indicateurs de menaces et ainsi éviter l'utilisation d'une CTI obsolète ?
- vous permet-elle de cibler les indicateurs de menaces issus de récentes campagnes d'attaques APT et d'intégrer les flux CTI de manière proactive à votre pare-feu nouvelle génération ?
- vous permet-elle d'enrichir votre CTI cloud et vos IOC de données basées sur une évaluation de fiabilité afin de réduire le nombre de faux positifs ?

Consolidez la connectivité et la sécurité

- Quelle fonctionnalité le pare-feu nouvelle génération prend-il en charge pour sécuriser les communications de bout en bout ?
- Comment le pare-feu nouvelle génération sécurise-t-il l'accès direct à Internet ?
- Comment le pare-feu nouvelle génération applique-t-il les politiques de sécurité aux services et applications cloud disponibles sur les sites distants ?
- Comment le pare-feu nouvelle génération renforce-t-il la sécurité de l'accès aux applications et services cloud sur un site distant ?

Prêt à évaluer votre prochain pare-feu ? À vous de jouer

paloalto NETWORKS

Oval Tower, De Entrée 99 - 197
1101HE Amsterdam, Pays-Bas

+31 20 888 1883

www.paloaltonetworks.com