LES 13 FONCTIONS INCONTOURNABLES DE VOTRE PROCHAIN PARE-FEU

L'évolution rapide de l'informatique a redessiné les contours du réseau. Aujourd'hui, les données et les utilisateurs sont partout. Quant aux terminaux, ils prolifèrent trop vite pour la plupart des entreprises. Parallèlement, les équipes informatiques misent sur le cloud, l'analytique 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 entreprises. 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. 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 13 fonctions clés dont les produits de nouvelle génération (NGFW, *Next-Generation Firewall*) doivent être équipés pour sécuriser votre réseau et votre entreprise.

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.

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, les initiales « NGFW » sont désormais synonyme de « pare-feu » tout court.

Les critères de sélection d'un NGFW couvrent généralement trois grandes catégories : 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 de la performance, votre pare-feu doit remplir sa mission tout en répondant à vos attentes en matière de débit. C'est pourquoi votre NGFW 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 13 fonctions incontournables dont aucune entreprise ne saurait se passer.

D'ici la fin de l'année 2019, les pare-feu nouvelle génération protègeront 90 % des connexions Internet de la base installée des entreprises.[1]

Impératifs des NGFW

1. Identifier les applications indépendamment du port, du protocole, de la tactique de contournement ou du chiffrement utilisé
2. Identifier les utilisateurs indépendamment de leur terminal ou de leur adresse IP
3. Décrypter le trafic chiffré
4. Bloquer en temps réel les menaces connues et inconnues dissimulées dans les applications
5. Garantir de très hauts débits in-line

1. Identification des utilisateurs et autorisations d'accès adaptées

Problématique

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 de terminaux 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 du terminal 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 de multiples terminaux, 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.

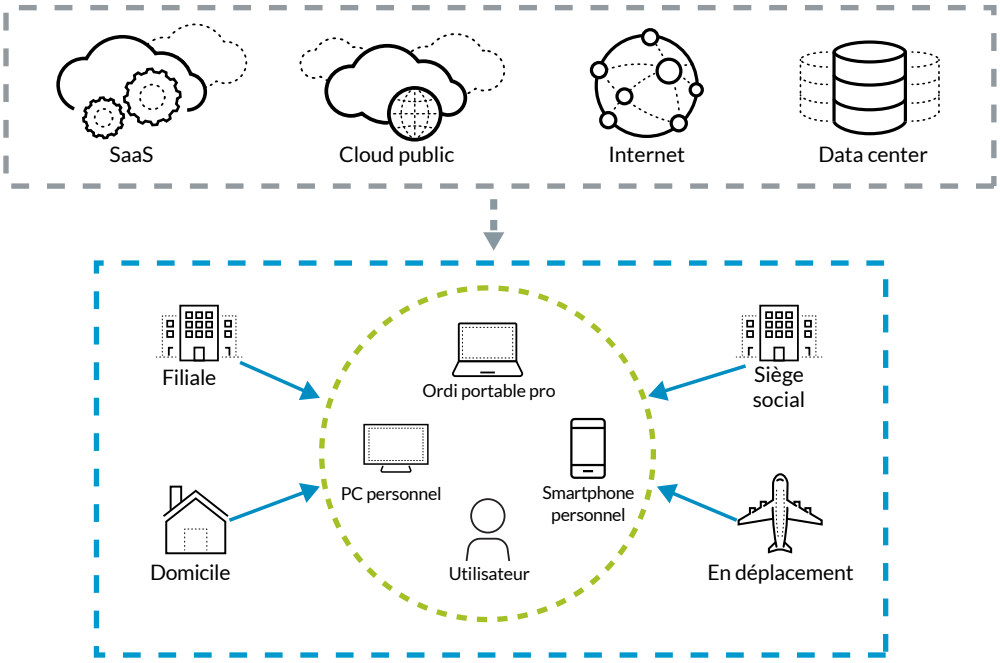

Figure 1 : Différents lieux et terminaux pour un même utilisateur

1. Adam Hils, Jeremy D'Hoinne, Rajpreet Kaur, « Magic Quadrant for Enterprise Network Firewalls », Gartner, 10 juillet 2017

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 politiques de sécurité et accélèrerez votre réponse à incident. 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 seul département informatique. Une fois définies, ces politiques suivent ensuite les utilisateurs où qu'ils soient (siège social, filiale ou domicile) et quel que soit l'appareil qu'ils utilisent. Toutefois, la question des identités utilisateurs dépasse leur simple classification à des fins de contrôle.

2. Prévention des vols et détournements d'identifiants

Problématique

Les utilisateurs et leurs identifiants font partie des principales faiblesses de votre infrastructure de sécurité. D'après le rapport d'enquête Verizon 2017 sur les compromissions de données, au cours des douze mois étudiés, 81 % 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.

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. Les attaquants 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.

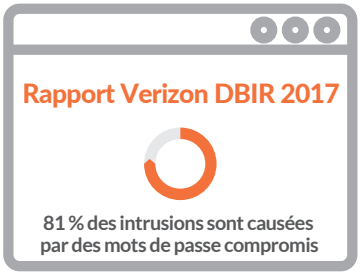

Figure 2 : Compromissions de mots de passe d'après le rapport Verizon DBIR de 2017

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 protègera vos applications contenant des données sensibles, même les plus anciennes.

3. Exécution sécurisée des applications et contrôle de leurs fonctions

Problématique

VoIP, messagerie instantanée, partage de fichiers peer-to-peer... de plus en plus d'applications utilisent des ports non standard, quand elles ne recourent pas au « port hopping ». De leur côté, les utilisateurs accèdent à des applications très diverses, y compris des SaaS, à partir de différents lieux et terminaux. 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.

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). Par exemple, il pourra décortiquer l'utilisation des différentes fonctions d'une application (streaming audio, accès distant, publication de documents, etc.) et y appliquer un contrôle granulaire (téléversement vs. téléchargement, chat vs. transfert de fichiers, etc.). Ce contrôle doit s'effectuer en continu. De fait, il est impossible de classifier le trafic de façon définitive car

2. "2017 Data Breach Investigations Report," Verizon, 2017, www.knowbe4.com/hubfs/rp_DBIR_2017_Report_execsummary_en_xg.pdf.

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 doit 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.

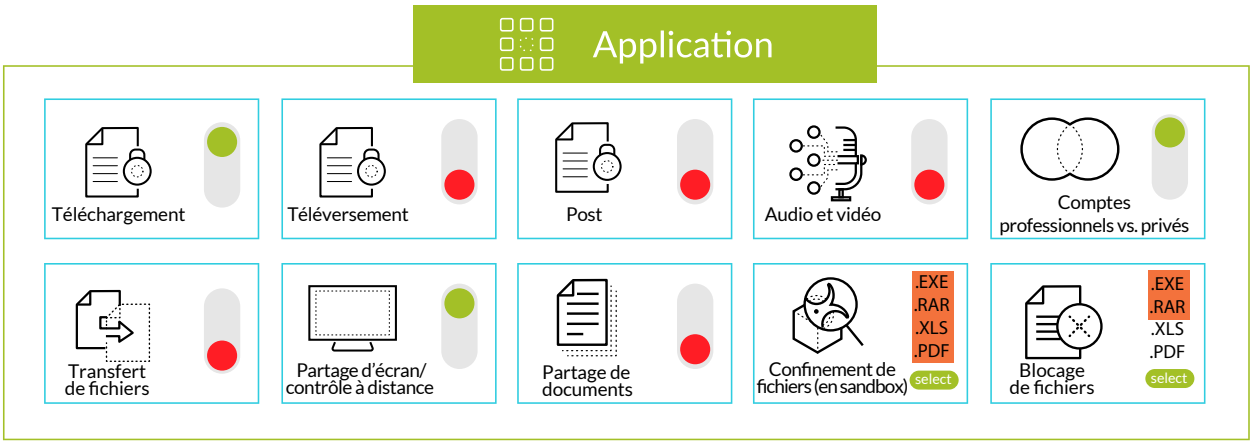

Figure 3 : Politique de contrôle de l'utilisation d'une application

4. Comblement des écarts critiques dans les politiques

Problématique

Les pare-feu traditionnels 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 tel quel vers leur pare-feu de 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'après le cabinet Gartner, jusqu'en 2023, 99 % des compromissions de pare-feu viendront d'erreurs de configuration, et non de failles intrinsèques à ces derniers.[3]

Solution

Au moment des choix, optez pour un pare-feu qui simplifie la gestion de vos règles et politiques. Ce pare-feu devra identifier les applications exécutées sur votre réseau, les relier à vos règles existantes et vous aider à remplacer ces dernières 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

Problématique

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.

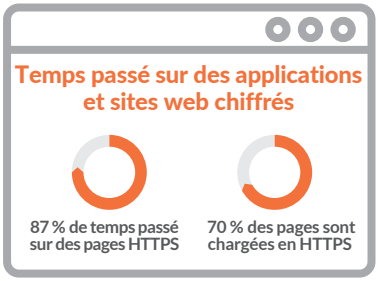

Figure 4 : Le trafic chiffré d'après le rapport Google 2019[4]

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. Cela dit, votre prochain pare-feu devra également 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

3. Rajpreet Kaur, Adam Hils, John Watts, « Technology Insight for Network Security Policy Management », Gartner, 21 février 2019, www.gartner.com/doc/3902564/technology-insight-network-security-policy.
4. « Transparence des informations : chiffrement HTTPS sur le Web », Google, consulté le 8 mars 2019, transparencyreport.google.com/https/overview?hl=en.

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. Pour en savoir plus sur cette fonctionnalité essentielle, lisez notre livre blanc intitulé **Déchiffrement : où, pourquoi et comment**.

6. Blocage des menaces avancées pour neutraliser les cyberattaques

Problématique

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 virtuels 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.

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 traque 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 ou elles 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 à incident de se concentrer sur les cas prioritaires.

Figure 5 : Neutralisation des attaques à tous les stades

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 logiciels malveillants, 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

Problématique

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 tunnélisées. 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.

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. La neutralisation des attaques DNS passe donc par un pare-feu nouvelle génération capable d'utiliser les analyses prédictives et le machine learning pour identifier les domaines malveillants inconnus.

8. Protection d'une population croissante de collaborateurs mobiles

Problématique

Plus vos collaborateurs se déplacent, plus ils se connectent à vos applications métiers depuis des terminaux mobiles. Souvent, ces connexions s'opèrent sur des appareils et réseaux publics exposés aux menaces avancées. Le risque est encore plus élevé lorsque vos utilisateurs travaillent hors site, sans pare-feu réseau pour bloquer les attaques. Le cloud et le BYOD (Bring Your Own Device) 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.

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 distribués. Mais pour y parvenir, toutes les fonctionnalités NGFW devront opérer en mode cloud pour éviter le déploiement de matériels dédiés sur chaque site.

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.

9. Sécurisation d'environnements cloud en mutation permanente

Problématique

Vos données et applications sont désormais partout, sur votre réseau et dans le cloud. D'après l'édition 2018 du State of the Cloud Report™ de RightScale, 81 % 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.

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 ».

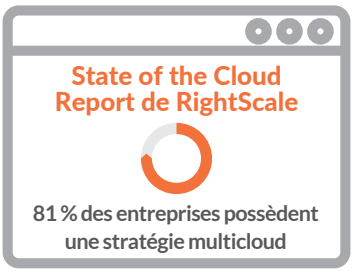

Figure 6 : Conclusions du rapport RightScale sur les stratégies multicloud

5. « 2018 State of the Cloud Report », RightScale, 2018, www.suse.com/media/report/rightscale_2018_state_of_the_cloud_report.pdf.

10. Stratégie « Zero Trust »

Problématique

Les modèles de sécurité traditionnels se basent sur le principe dépassé selon lequel vous pouvez faire confiance à tout ce qui se situe à l'intérieur de votre réseau. Cependant, les attaques et les menaces internes ne cessent de se perfectionner. Pour empêcher qu'elles ne se propagent une fois à l'intérieur du réseau, vous devez implémenter de nouvelles mesures de sécurité. Or, les modèles traditionnels n'ont été conçus que pour sécuriser votre périmètre réseau. Par conséquent, les menaces qui parviennent à le contourner deviennent invisibles. Une fois infiltrés, les attaquants peuvent alors se camoufler et se déplacer à leur guise pour exfiltrer des données sensibles. À l'ère du numérique, la confiance n'est ni plus ni moins qu'un signe de faiblesse.

Solution

Au moment des choix, préférez un NGFW capable d'agir comme une passerelle de segmentation pour l'implémentation d'une architecture « Zero Trust ». L'approche Zero Trust part d'un postulat radical : aucun utilisateur, aucune application et aucune donnée n'est digne de confiance. Par conséquent, leurs actions dans un environnement devraient toujours être sous surveillance. Principal objectif de ce modèle : empêcher les attaquants d'exploiter des vulnérabilités des applications traditionnellement dites « de confiance ». Cette approche consiste à limiter la portée d'une attaque et à bloquer les mouvements latéraux en définissant une microsegmentation basée à la fois sur les utilisateurs, les données et la géolocalisation. 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 pare-feu nouvelle génération doit être présent sur tous ces fronts. 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. Pour tout savoir sur l'implémentation d'une approche « Zero Trust », visionnez ce webinaire.

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

Problématique

En règle générale, chaque produit de sécurité est livré avec sa propre application de gestion, si bien que vos équipes de sécurité opérationnelle doivent se familiariser avec chaque interface pour configurer votre sécurité. D'après le rapport ResearchCorp 2017 consacré aux services IT aux États-Unis, environ 72 % des entreprises recourent aux produits d'au moins trois fournisseurs pour sécuriser leur infrastructure réseau.[5] Or, ces produits isolés ne communiquent pas entre eux. 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. Ce qui non seulement complique leur sécurité mais place aussi les équipes IT sous une pression extrême.

Solution

Pour appliquer des politiques de sécurité homogènes à travers des dizaines de milliers de pare-feu sur site et dans le cloud (sites distants, utilisateurs mobiles et applications SaaS compris), vous avez besoin d'une gestion centralisée, de fonctionnalités simplifiées et d'une consolidation de vos principales tâches de sécurité. 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 fonctionnalités sont en mode cloud, vos équipes peuvent mettre sur pied une architecture de sécurité couvrant les moindres recoins de votre réseau étendu face aux menaces connues et inconnues. 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.

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

Problématique

D'après une enquête de l'Enterprise Strategy Group, 51 % des professionnels de la cybersécurité pensent que leur entreprise souffre d'une pénurie de compétences dans ce domaine.[6] Pour ne rien arranger, ces entreprises 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.).

6. « 2017 U.S. IT Services Report », ResearchCorp.org, 2017, www.fidelus.com/wp-content/uploads/2017/12/researchcorp-fidelus_us_it_servicesreport_full_report.pdf.

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 de routine et ainsi vous recentrer sur vos véritables priorités. Les trois axes de votre automatisation :

- **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. En outre, le pare-feu doit pouvoir initier des workflows sur d'autres équipements de votre écosystème de sécurité, à l'aide d'API et sans intervention manuelle.
- **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.
- **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.

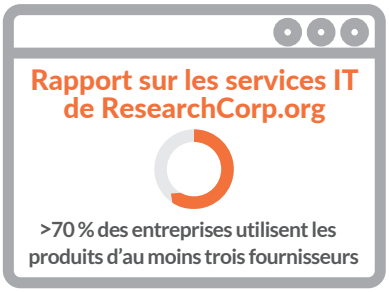

Figure 7 : Conclusions du rapport ResearchCorp 2018 sur la sécurité réseau multi-fournisseur

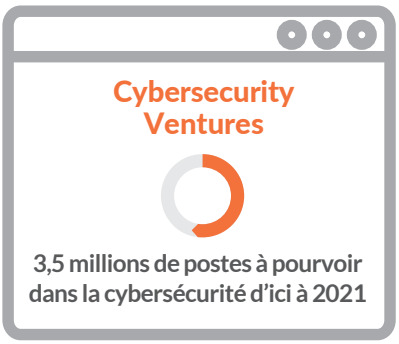

Figure 8 : Les emplois dans la cybersécurité d'après Cybersecurity Ventures

13. Déploiement simplifié des innovations en sécurité

Problématique

Dans le domaine de la cybersécurité, il est souvent difficile de profiter rapidement des dernières innovations. Dès qu'une nouvelle technologie émerge, les entreprises passent un temps fou à déployer de nouveaux matériels et logiciels. Elles finissent ainsi à passer plus de temps à gérer l'expansion de leur infrastructure de sécurité qu'à améliorer leurs contrôles de sécurité pour garder une longueur d'avance sur les attaquants.

Solution

Pour répondre à vos besoins croissants en sécurité, deux options s'offrent à vous : ajouter des produits isolés ou intégrer de nouvelles fonctionnalités à un équipement existant. Si votre pare-feu peut faire office de capteur et point de contrôle pour les technologies d'autres fournisseurs, vous pourrez alors rapidement adopter des innovations sans déployer ni gérer un nombre incalculable de nouveaux équipements. En somme, votre prochain pare-feu devra permettre à vos équipes de découvrir, évaluer et utiliser rapidement les nouvelles technologies de sécurité. Une parfaite intégration leur permettra de collaborer entre différentes applications, de partager des informations contextualisées sur les menaces et d'automatiser les tâches de contrôle et de réponse à incident. Vos équipes de sécurité bénéficieront ainsi des meilleures technologies disponibles pour résoudre les problèmes de sécurité les plus complexes, sans le déploiement laborieux et coûteux d'une nouvelle infrastructure pour chaque nouvelle fonctionnalité. Pour découvrir comment une plateforme de sécurité continue, ouverte, intégrée et basée sur l'IA peut vous aider à déployer de nouvelles applications et fonctionnalités innovantes, visionnez cette vidéo.

Prêts à évaluer votre prochain pare-feu ? C'est **à vous de jouer**.

Palo Alto Networks
Oval Tower, De Entrée 99 -179
1101HE Amsterdam
Pays-Bas
+31 20 888 1883
www.paloaltonetworks.fr