10 points à tester sur votre prochain pare-feu nouvelle génération

En quête de votre prochain pare-feu ? Vous vous demandez comment gérer les risques et opportunités inhérents à la cybersécurité de votre organisation ? Et comment déterminer l'adéquation des fonctionnalités de votre pare-feu nouvelle génération aux impératifs de croissance de votre entreprise ?

C'est simple : il faut tester.

Tous les spécialistes s'accordent à dire qu'en matière de sécurité d'entreprise, il n'existe pas de recette miracle. Chaque organisation a des besoins propres qui doivent se refléter dans ses architectures de sécurité. Quant aux outils, services et fonctionnalités de sécurité, ils doivent être suffisamment flexibles pour satisfaire les spécificités du cahier des charges, tout en demeurant fidèles aux performances annoncées.

Ce document se penche sur 10 points à prendre en compte et à tester rigoureusement dans votre infrastructure de sécurité actuelle et votre prochain pare-feu nouvelle génération (NGFW). Il dessinera ainsi un cadre et une ligne directrice pour orienter les échanges entre les différentes fonctions concernées. Ce faisant, vous élargirez votre perspective pour aborder la question de l'investissement dans un pare-feu nouvelle génération sous différents angles : facilité d'implémentation, allègement de la charge opérationnelle et rapport coût-sécurité, aujourd'hui comme demain.

1. Prévention contre le vol d'identifiants

Les utilisateurs et leurs identifiants font partie des principales faiblesses de votre infrastructure de sécurité. Pour preuve, la majorité des compromissions impliquent un vol d'identifiants à un moment ou à un autre du cycle d'attaque, avec une forte probabilité de réussite pour l'assaillant. La solution ? Empêcher le vol d'identifiants en premier lieu.

Pourquoi cette fonctionnalité et pourquoi la tester ?

Prévenir le vol d'identifiants et bloquer les attaques de phishing permet de réduire l'exposition à l'une des formes les plus courantes d'attaques ciblées, qui visent généralement des salariés peu versés dans les questions techniques et usent de toutes sortes de stratagèmes pour les inciter à cliquer sur des liens malveillants inconnus.

Sortir du statu quo

La plupart des entreprises misent principalement sur la sensibilisation de leurs collaborateurs pour neutraliser ces attaques. Mais ce n'est pas suffisant.

Quant aux produits traditionnels, ils reposent pour la plupart sur la détection des sites de phishing connus et le filtrage des e-mails, deux méthodes que l'on sait facilement contournables. En ne recherchant que les sites malveillants connus, cette méthode ne parvient donc pas à bloquer les nouveaux sites de phishing. Quant aux attaquants, il leur suffit d'envoyer des liens via les réseaux sociaux pour contourner les technologies de filtrage des e-mails. Un pare-feu nouvelle génération piloté par machine learning accélère la détection des URL suspectes. Si les analyses ML identifient un site comme étant malveillant, votre pare-feu doit par conséquent être mis à jour et en mesure de le bloquer.

Ceci dit, de nouveaux sites de phishing « inconnus » font constamment leur apparition. Pour protéger votre réseau et vos utilisateurs, vous devez donc à tout prix empêcher la saisie d'identifiants sur de tels sites. Le filtrage d'identifiants permet aux organisations de limiter l'authentification aux seules applications autorisées, bloquant de fait la saisie d'identifiants sur des sites inconnus.

Les questions à intégrer à votre appel d'offre

- Le NGFW peut-il empêcher l'utilisation d'identifiants professionnels sur des sites web inconnus ?
- Peut-il bloquer la saisie d'identifiants professionnels dont une copie du hachage n'a pas été conservée sur le pare-feu ?
- Est-t-il équipé d'un système ML qui identifie et bloque le phishing d'identifiants, ainsi que les attaques JavaScript qui tentent d'infiltrer le réseau ?
- Avec quelle rapidité est-il en mesure d'analyser les sites de phishing inconnus et de mettre à jour ses systèmes de protection ?
- Enregistre-t-il les tentatives de connexion des utilisateurs dans une requête HTTP POST ?

2. Prévention contre le détournement d'identifiants

Phishing, malwares, ingénierie sociale, force brute, Darknet… les attaquants ont le choix des armes pour faire main basse sur des identifiants. Une fois en possession de ces informations, ils détiennent un précieux sésame pour infiltrer les organisations, se déplacer latéralement et élever leurs privilèges d'accès aux applications et données sensibles.

Pourquoi cette fonctionnalité et pourquoi la tester ?

La mise en œuvre d'une authentification multifacteur (MFA) sur votre pare-feu empêche les attaquants d'utiliser des identifiants volés pour se déplacer latéralement sur le réseau. La MFA permet à votre organisation de protéger tout type d'applications, y compris les applications historiques et client-serveur. Par ailleurs, une authentification qui se produit au niveau du pare-feu, avant que les utilisateurs ne se connectent aux applications, réduit considérablement le risque d'exposition.

Sortir du statu quo

Beaucoup d'organisations disposent d'une solution MFA. Toutefois, son intégration aux applications se révèle souvent difficile et chronophage. Résultat : la plupart n'utilise la MFA que pour une poignée d'applications (passerelles VPN, applications cloud, etc.), laissant les autres vulnérables au détournement d'identifiants.

Protection sur la couche réseau

La MFA est un excellent outil, à condition de protéger toutes les applications critiques. Plutôt que de modifier les applications elles-mêmes, définissez une politique MFA au niveau du pare-feu pour contrôler les accès à des applications spécifiques. Le pare-feu pourra ainsi contrôler les accès et exiger un second facteur d'authentification avant d'autoriser le passage du trafic. Même au moyen d'un terminal compromis, des attaquants déjà infiltrés dans une organisation ne pourront pas passer l'étape de l'authentification multifacteur.

Expérience utilisateur sur mesure

Les politiques MFA définies au sein du pare-feu doivent être granulaires, tant au niveau des utilisateurs que des besoins de sécurité de l'application. Cette politique peut par exemple déterminer la fréquence à laquelle les utilisateurs doivent se réauthentifier selon le niveau de sensibilité d'une application donnée.

Protection accélérée des applications

La définition des politiques MFA au niveau du pare-feu accélère l'implémentation d'applications, dans la mesure où l'application elle-même n'a pas besoin d'être modifiée. Les protections sont ainsi déployées plus rapidement, dans le respect des exigences de conformité. Une authentification multifacteur intégrée au pare-feu empêche les attaquants d'utiliser des identifiants volés ou de se déplacer latéralement sur le réseau d'une organisation. Elle permet de protéger tous types d'applications, y compris les applications historiques et client-serveur.

Les questions à intégrer à votre appel d'offre

- La fonctionnalité MFA du NFGW permet-elle de définir une politique de contrôle des accès basée sur le niveau de sensibilité de la ressource visée ?
- Propose-t-il une variété d'options permettant d'intégrer la MFA à des technologies partenaires ?
- Gère-t-il le protocole RADIUS et les intégrations par API aux technologies MFA partenaires ?
- Peut-il appliquer des politiques MFA à tous types d'applications (web, client-serveur, terminaux, etc.) ?
- La fonctionnalités MFA du NGFW se limitent-elle à certains protocoles ?

3. À workloads virtuels dynamiques, politiques de sécurité dynamiques

Lorsqu'une politique de sécurité destinée à un environnement de data center est initialement créée et déployée sur des pare-feu, on part du principe selon lequel l'adresse IP attribuée restera la même pendant toute la durée de vie de la politique. Ces politiques sont donc statiques, immuables et appliquées de manière générique. Or, avec la virtualisation des data centers, les workloads ne sont plus rattachés à un emplacement ou à un schéma de réseau particulier.

Pourquoi cette fonctionnalité et pourquoi la tester ?

Compte tenu du caractère hautement dynamique des data centers virtualisés, les politiques de sécurité des pare-feu doivent se baser sur les attributs des workloads plutôt que sur des adresses IP statiques. Cette action peut être réalisée via des groupes d'adresses dynamiques définis sur un pare-feu nouvelle génération.

Sortir du statu quo

Des workloads éphémères sont souvent démarrés et arrêtés pour optimiser l'utilisation des ressources de calcul. De fait, ils acquièrent sans cesse de nouvelles adresses IP. Les équipes de sécurité doivent ainsi composer avec des centaines, voire des milliers de groupes d'adresses, chacun avec ses propres objets d'adresse et soumis en permanence à des ajouts, des suppressions ou des modifications. Difficile, dans ces conditions, de gérer les politiques de contrôle d'accès sur le pare-feu.

Votre pare-feu doit être en mesure d'appliquer des politiques qui s'adaptent automatiquement à la nature dynamique de data centers qui vivent au rythme des ajouts, déplacements et suppressions permanents de workloads. Des politiques adaptatives favorisent la mise en œuvre d'une sécurité homogène sur vos applications et machines virtuelles dynamiques.

Les groupes d'adresses dynamiques dissocient les politiques de sécurité des adresses IP, créant à la place des politiques de sécurité granulaires basées sur les attributs des workloads virtuels. Les politiques définies sur le pare-feu utilisent des étiquettes associées aux attributs des workloads. Par exemple, une étiquette « App-Server » peut être associée à des attributs qui identifient le serveur d'applications concerné, quelle que soit son adresse IP. Ces attributs continueront de soumettre le workload à la politique de sécurité correspondante même si ce dernier change d'emplacement.

Vous pouvez ainsi créer des politiques de sécurité associées directement aux workloads, ce qui renforce votre sécurité. Les groupes d'adresses dynamiques réduisent la dépendance entre applications et équipes de sécurité, ce qui diminue la charge opérationnelle.

Les questions à intégrer à votre appel d'offre

- Comment le NGFW crée-t-il des politiques de sécurité basées sur les attributs de workloads virtuels ?
- Peut-il créer des politiques de sécurité pour des workloads dynamiques dans des environnements cloud privés et publics ?
- Peut-il garantir la cohérence des politiques de sécurité même lorsque les adresses IP ou les emplacements des workloads changent dans le data center ?

4. Outils de gestion simples et efficaces

Pour répondre aux besoins de l'entreprise, les équipes de sécurité doivent bénéficier d'une flexibilité leur permettant d'effectuer des changements en temps réel sur le pare-feu, à la fois sur site ou depuis un outil centralisé. Un gestionnaire de pare-feu qui permet aux administrateurs locaux de n'apporter des modifications qu'à un ensemble limité de fonctionnalités rend ces derniers fortement dépendants des équipes centrales, souvent basées dans d'autres régions, pour apporter les changements souhaités. Retards, failles, visibilité limitée, accès administrateur granulaire… les conséquences sont multiples.

Pourquoi cette fonctionnalité et pourquoi la tester ?

Pour simplifier les modifications locales et maintenir une sécurité conforme aux directives de votre organisation, toutes les fonctionnalités du pare-feu doivent pouvoir être gérées et différents administrateurs doivent pouvoir y accéder en fonction de leur rôle. De leur côté, vos gestionnaires de pare-feu locaux doivent avoir les mêmes fonctionnalités que l'outil central pour permettre aux équipes locales d'accomplir leurs tâches à temps. Enfin, l'outil de gestion central doit enrichir les données locales d'une visibilité globale sur les actions des administrateurs locaux et, si besoin, annuler ces actions à distance pour maintenir la conformité du pare-feu aux directives de l'organisation.

D'où l'importance d'opter pour un pare-feu nouvelle génération capable de centraliser la gestion de tous vos pare-feu, quels que soient leurs formats et leurs emplacements. Vous pourrez ainsi simplifier la configuration, le déploiement et la gestion de vos politiques de sécurité. Ce qu'il vous faut, c'est un outil capable de corréler les journaux de pare-feu pour fournir des informations sur le réseau et la sécurité, mais aussi signaler des comportements malveillants qui peuvent souvent se fondre dans la masse.

Sortir du statu quo

Assurez un contrôle granulaire des modifications de configuration

Dans les environnements multi-pare-feu, il n'est pas rare que plusieurs administrateurs apportent simultanément des modifications de configuration. L'un pourra alors valider ses modifications alors qu'un autre n'aura pas totalement fini d'appliquer les siennes. Or, si votre gestionnaire de pare-feu ne permet pas de valider les changements de façon sélective, ces modifications incomplètes seront également déployées. On imagine alors les répercussions possibles en termes de sécurité : accès des utilisateurs à des sites bloqués, blocage des accès aux applications critiques, etc. Lorsqu'il n'est pas possible de déployer et de restaurer les configurations de façon sélective, les administrateurs doivent annuler eux-mêmes les modifications incomplètes, recommencer depuis le début et les redéployer manuellement. Or, cela augmente les coûts opérationnels et ralentit le processus de renforcement de la sécurité.

Gérer efficacement les journaux à grande échelle

Un gestionnaire centralisé permet de piloter le réseau et la sécurité à partir d'une seule et même console, offrant ainsi une vue et un contexte d'ensemble pour l'analyse des évènements de sécurité. Souvent, ce genre de gestionnaire collecte et consolide les journaux provenant de multiples pare-feu. Un débit entrant (généralement exprimé en nombre de journaux à la seconde) supérieur aux capacités d'ingestion du gestionnaire aura un impact sur les performances de ce dernier.

Cette saturation pourra se manifester par le figeage de l'interface utilisateur ou l'expiration des requêtes de base de données. À l'ère du numérique et du haut débit, il n'est pas rare qu'un seul pare-feu haut de gamme dépasse à lui seul les capacités d'ingestion du gestionnaire central faisant office de gestionnaire de journaux. Dans un environnement multi-pare-feu, la probabilité de rencontrer des problèmes de capacité est donc très élevée.

Le traitement des journaux à haut débit s'opère généralement via une appliance de gestion distincte. Pour la plupart des entreprises, la solution la plus appropriée consiste à combiner un gestionnaire de pare-feu à un gestionnaire de journaux. Le gestionnaire central est ainsi délesté de la gestion des journaux et peut se concentrer uniquement sur celle des pare-feu. Il interroge les gestionnaires de journaux pour fournir une visibilité centralisée et ne reçoit des journaux bruts que lorsque cela est nécessaire, ce qui réduit l'impact sur les performances.

Maintenir la sécurité à jour

Chacune des nombreuses fonctionnalités d'un pare-feu nouvelle génération est conçue pour répondre à des besoins de sécurité réseau spécifiques et favoriser la croissance d'une entreprise. Dans un environnement multi-pare-feu, les modifications manuelles des configurations sont non seulement inefficaces, mais elles créent aussi des failles de sécurité et des incohérences dans la prévention. L'automatisation permet d'apporter des réponses plus rapides et plus précises à des menaces de cybersécurité en constante évolution.

Ici, la meilleure manière d'automatiser les modifications consiste à passer par des API. Une telle démarche permet à la fois d'alléger la charge des équipes de sécurité réseau et de réduire les erreurs humaines. Mais pour y parvenir, les API doivent être suffisamment flexibles pour que toutes les fonctionnalités du pare-feu soient modifiables automatiquement.

Les questions à intégrer à votre appel d'offre

- Les administrateurs locaux peuvent-ils travailler directement sur l'équipement et modifier les configurations sans avoir à se connecter à un gestionnaire central ?
- Les administrateurs centraux peuvent-ils voir et contrôler les modifications apportées par les administrateurs locaux ?
- À partir des modifications de configuration apportées par un administrateur, pouvez-vous choisir celles à déployer sur les pare-feu ?
- Lorsque des déploiements se passent mal, pouvez-vous annuler rapidement les modifications effectuées par des utilisateurs spécifiques et restaurer une configuration opérationnelle ?
- Le gestionnaire de pare-feu central peut-il séparer la gestion des journaux de la gestion des configurations de base, tout en offrant une vue unifiée ?
- Le gestionnaire de journaux peut-il ingérer des journaux à haut débit (par exemple 50 000 journaux par seconde) ?
- Le pare-feu dispose-t-il d'API pour chaque fonctionnalité pour vous permettre d'automatiser les modifications de configuration ?

5. Automatiser pour intégrer la sécurité et prévenir des menaces en constante évolution

Concevoir des systèmes et processus et y greffer la sécurité après-coup est un modèle dépassé. Pour éviter l'accumulation d'outils de protection et de systèmes de contrôle complexes et isolés, la sécurité doit désormais être intégrée bien en amont. Les outils de détection et de réponse automatisés, ainsi que les API, intègrent vos équipements de sécurité aux écosystèmes de protection globale de votre organisation. Cette intégration permet de simplifier les opérations et d'utiliser directement les données de détection pour répondre aux attaques avant qu'elles n'aient pu atteindre leur cible et exfiltré des données sensibles de votre organisation.

Pourquoi cette fonctionnalité et pourquoi la tester ?

Les API ont la capacité d'automatiser les workflows qui exigent un certain niveau d'interopérabilité entre plusieurs équipements de sécurité, le plus souvent de divers fournisseurs. Elles délestent ainsi les équipes de la gestion manuelle, fastidieuse et propice aux erreurs de ces workflows et accélèrent la mise en œuvre de contrôles efficaces. Les outils et services de sécurité automatisés doivent être capables d'ingérer des alertes provenant de multiples sources, d'exécuter des playbooks standardisés pour accélérer la réponse aux incidents, et de s'intégrer à d'autres outils pour déclencher la prochaine action d'un workflow.

Sortir du statu quo

Selon le rapport d'enquête Verizon 2019 sur les compromissions de données, le temps entre la première action d'un attaquant et la compromission initiale d'une ressource est de l'ordre de quelques minutes.[1] Autrement dit, votre organisation a besoin d'outils capables de faire communiquer efficacement les éléments de votre infrastructure, d'identifier les menaces connues et inconnues de façon rapide et automatique, et de neutraliser ces menaces plus vite qu'elles ne peuvent progresser dans le cycle d'attaque. Pour ce faire, chaque étape du processus, de la découverte à la neutralisation totale, doit être automatisée. Chaque élément de l'infrastructure doit également pouvoir communiquer efficacement avec tous les autres pour simplifier les opérations et accélérer la réponse aux incidents.

Les API offrent un mécanisme permettant aux nombreux éléments d'un data center, souvent issus de différents constructeurs informatiques, de partager des données et de lancer les actions appropriées dans le workflow. D'où l'importance d'opter pour un fournisseur de sécurité dont les API s'intègrent à une vaste gamme de solutions partenaires, et dont l'interopérabilité est parfaitement documentée et certifiée. Au-delà du data center, cette intégration doit s'étendre aux solutions de sécurité des terminaux, de passerelles de messagerie, de sécurité sans fil, etc. Un pare-feu qui intègre des API en natif permet aux administrateurs de consulter et de modifier l'ensemble des fonctionnalités.

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

Pour prévenir les menaces encore inconnues, les outils de sécurité doivent être en mesure d'analyser et d'identifier les comportements malveillants. Et ils doivent de préférence opérer en mode cloud pour capitaliser sur l'élasticité et l'évolutivité de ces environnements. Les nouveaux outils doivent pouvoir s'intégrer à vos outils de sécurité cloud existants pour coordonner et automatiser les processus de réponse, sur site et dans le cloud. L'automatisation leur permettra d'ingérer les alertes issues de multiples sources et d'exécuter des playbooks standardisés pour accélérer la réponse aux incidents. De même, en corrélant automatiquement les données, ils pourront identifier et mettre en évidence les hôtes du réseau présentant des comportements symptomatiques de la menace en question.

Certaines organisations préfèreront automatiser la mise en quarantaine immédiate des hôtes potentiellement infectés. Un hôte dans cette situation est soumis à une politique lui refusant l'accès à toutes les parties du réseau, la seule connectivité possible étant pour des actions de remédiation. D'autres structures adopteront une approche plus nuancée en appliquant automatiquement l'authentification multifacteur à un hôte potentiellement infecté de sorte que, si l'hôte en question est sous le contrôle d'un attaquant, il ne puisse accéder ni aux données ni aux applications de l'entreprise.

L'automatisation et les API permettent aux entreprises de réagir aux menaces sans intervention humaine. Elles améliorent ainsi le temps de réponse et, à condition d'être implémentées correctement et associées aux bons outils, bloquent les attaques à la racine. Un fournisseur dont les pare-feu sont équipés d'API et de capacités d'automatisation permet aux équipes de sécurité de se libérer des tâches opérationnelles de base pour se recentrer sur des projets stratégiques qui profitent directement à l'organisation. Qui dit moins d'interventions humaines, dit moins d'erreurs évitables et donc une meilleure sécurité.

Les questions à intégrer à votre appel d'offre

- Le NGFW (ou son gestionnaire) peut-il créer un ticket sur un système de gestion des modifications sur la base d'un évènement malveillant détecté sur le pare-feu ?
- Le pare-feu (ou son gestionnaire) peut-il déclencher une action de mise en quarantaine d'un hôte infecté sur le réseau Wi-Fi ?
- Est-il entièrement programmable via des API ?
- Peut-il collecter des identifiants d'utilisateurs, à partir d'API de contrôleurs sans fil, concernant les hôtes se connectant aux réseaux Wi-Fi ?
- Permet-il de générer automatiquement des signatures préventives tout au long du cycle d'attaque, et ce pour toutes les données d'attaque pertinentes ?
- Peut-il corréler et identifier les hôtes infectés du réseau, puis les mettre en quarantaine pour limiter leur accès au réseau ?
- Peut-il déclencher une demande d'authentification multifacteur pour empêcher l'utilisation abusive d'identifiants et protéger les applications critiques ?

6. Protection contre les attaques furtives et inconnues

Des millions de nouveaux échantillons de malwares et de sites web malveillants sont découverts chaque année. En règle générale, les solutions traditionnelles protègent contre les menaces nouvellement détectées après que la première victime d'une organisation ait été compromise. Or, cela ne suffit pas lorsqu'on sait qu'il est possible de passer d'une à 10 000 victimes en l'espace de quelques minutes et ce, avant qu'une quelconque protection n'ait été appliquée.

De nombreuses attaques réussissent parce que les développeurs de malwares utilisent diverses techniques de contournement : dissimulation de payloads malveillants dans des fichiers légitimes, compression de fichiers, mise en sommeil du payload jusqu'à sa sortie de la sandbox, etc. Les attaquants sont parfaitement au fait des méthodes utilisées par les équipes de sécurité pour analyser les activités malveillantes dans un fichier. Ils suivent également de près les sandbox virtuelles dont les organisations se servent pour effectuer des analyses dynamiques : recherche de code utilisé dans les outils d'analyse anti-malware connus ; recherche d'activité utilisateur valide, de configurations système ou d'indicateurs de technologies de virtualisation/d'émulation spécifiques ; analyse de la taille du matériel pour connaître les espaces mémoire typiques des machines virtuelles, etc.

Aujourd'hui, les menaces sont souvent le produit de connaissances acquises sur les technologies open-source utilisées dans la plupart des hyperviseurs et des outils d'analyse anti-malware. Et le développement du Darknet n'arrange rien dans la mesure où il permet à n'importe quel attaquant, novice ou confirmé, d'acheter des kits d'exploits clé en main pour repérer et contourner les analyses anti-malware. C'est pourquoi il est plus crucial que jamais de pouvoir identifier et se protéger des malwares furtifs.

Pourquoi cette fonctionnalité et pourquoi la tester ?

Se protéger contre une nouvelle attaque seulement après qu'une première victime ait été compromise revient à lui laisser suffisamment de temps pour se propager latéralement, mettant de fait toute l'organisation en danger. Certaines solutions tentent d'éviter le « patient zéro » en confinant des fichiers pour analyse. Mais au final, une telle approche nuit à l'expérience utilisateur et ralentit l'activité.

Aujourd'hui, la plupart des malwares exploitent des techniques avancées pour contourner les solutions traditionnelles et passer au travers des dispositifs de sécurité réseau, des pare-feu et des outils de sandboxing. Bien qu'il soit impossible de créer des outils individuels pour détecter chaque malware furtif, il est essentiel d'utiliser des systèmes capables d'identifier les techniques de contournement et de les contrer automatiquement.

Sortir du statu quo

La prévention inline au service du blocage des attaques inconnues

Dans un monde où des malwares connus et inconnus peuvent se propager de manière exponentielle en quelques minutes, le recours aux analyses hors ligne et aux mises à jour périodiques de règles de pare-feu vous donnera toujours un temps de retard. Un pare-feu nouvelle génération assurant une prévention inline pilotée par machine learning au niveau du réseau peut neutraliser les nouvelles menaces sur toutes les applications. Il empêche ainsi les vols d'identifiants et autres menaces furtives pour éviter toute compromission du patient-zéro, sans compromettre la productivité de l'entreprise.

Effectuer des analyses bare-metal

Il existe de multiples façons de contrer les menaces conçues pour échapper aux environnements d'analyse. Une plateforme de sécurité efficace se doit d'en combiner plusieurs. Par exemple, combiner des analyses dynamiques en sandbox à des analyses bare-metal se révèle très efficace pour contrer les malwares qui évaluent les environnements pour vérifier s'ils sont en cours d'analyse.

Dans le cas d'une analyse bare-metal, les fichiers suspects sont envoyés vers un environnement matériel sécurisé où ils sont détonés en vue de vérifier un éventuel comportement malveillant. L'activité malveillante du fichier, qui serait restée dormante dans l'environnement virtuel, sera totalement dévoilée dans l'environnement bare-metal. Les menaces conçues pour contourner les systèmes de détection des machines virtuelles ne peuvent pas échapper aux environnements bare-metal.

Éviter les hyperviseurs open-source

Un pare-feu nouvelle génération doté d'un hyperviseur propriétaire empêche les attaquants de tester leurs malwares dans des environnements virtuels open-source connus. La plupart des attaquants recourent à cette pratique pour en tirer des enseignements et perfectionner leurs malwares.

Combattre l'automatisation par l'automatisation

Les malwares évoluent si vite que les signatures de menaces qui reposent sur des variables spécifiques (hachage, nom de fichier, URL, etc.) n'obtiennent des correspondances qu'avec les menaces connues. Or, les attaquants apportent souvent de légères modifications au code pour créer une nouvelle variante et/ou un malware polymorphe. Ce « nouveau » malware est alors considéré comme inconnu, car des protections n'ont été créées que pour le malware d'origine et non pour ses variantes ultérieures.

Les signatures de menaces basées sur le hachage sont particulièrement problématiques. Selon le rapport Verizon sur les compromissions de données, « 99 % des hachages de malwares ne sont visibles que pendant 58 secondes ou moins »[2]. Le hachage change dès que le moindre bit est modifié, et la signature ne le reconnaît plus comme un malware.

Plutôt que d'utiliser des signatures basées sur des attributs spécifiques, les pare-feu nouvelle génération doivent s'appuyer sur des modèles de machine learning prédictifs intégrés ou des signatures basées sur le contenu afin de détecter les variantes de malwares, les malwares polymorphes et les activités de commande et de contrôle (CnC). Les signatures basées sur le contenu détectent des patterns qui leur permettent d'identifier des familles entières de malwares, y compris des malwares connus ayant été modifiés. Elles parviennent ainsi à neutraliser automatiquement des dizaines de milliers de variantes créées à partir d'une même famille de malwares, au lieu d'essayer de créer des signatures pour chaque variante.

Quant aux communications CnC, elles présentent un autre défi dans la mesure où les attaquants les programment de façon à changer automatiquement de DNS ou d'URL. Les signatures automatisées basées sur ces artefacts deviennent donc rapidement obsolètes et inefficaces. Par contraste, les signatures basées sur l'analyse des patterns de communications CnC sortantes s'avèrent bien plus efficaces et évolutives lorsqu'elles sont créées automatiquement.

Utiliser plus d'une méthode d'analyse

Les attaquants les plus déterminés et les plus expérimentés n'hésitent pas à créer un code ex nihilo pour lancer de nouvelles attaques. La menace sera alors considérée comme inconnue et s'infiltrera sans se faire repérer dans l'environnement de sa victime.

C'est à ce moment que le compte à rebours commence. Des protections doivent être créées et distribuées sur tous les produits de sécurité plus vite que la menace ne peut se propager. Pour ce faire, il est possible d'automatiser divers aspects des analyses, y compris les analyses statiques avec machine learning, les analyses dynamiques et les analyses bare-metal. Identification précise des menaces, prévention rapide, amélioration de l'efficacité, meilleur usage des compétences spécialisées, renforcement de la sécurité… les avantages d'une telle automatisation sont nombreux.

Les questions à intégrer à votre appel d'offre

- Le NGFW assure-t-il une prévention pilotée par machine learning pour détecter les fichiers et variantes de malwares inconnus, y compris les exécutables et les attaques sans fichier qui utilisent des scripts comme PowerShell® ?
- Offre-t-il une prévention inline pilotée par machine learning pour les attaques basées sur des sites web malveillants, y compris les attaques JavaScript et le phishing d'identifiants ?
- À quelle vitesse votre système cloud d'analyse des malwares distribue-t-il les signatures après la génération du verdict ?
- Utilise-t-il des technologies sans signature pour empêcher des attaques inconnues ?
- Votre sandbox cloud peut-elle effectuer des analyses bare metal ?
- Votre système cloud d'analyse anti-malware utilise-t-il un hyperviseur propriétaire pour contrer les malwares capables de reconnaître les sandbox ?
- Après avoir analysé les malwares, votre système crée-t-il des signatures préventives ? Exemples :
  - » Signatures antivirus basées sur le contenu pour neutraliser des familles entières de malwares, y compris des variantes connues et inconnues
  - » Signatures anti-spyware basées sur des patterns pour détecter les communications CnC connues et inconnues
- Votre système peut-il effectuer des analyses anti-malware sur des fichiers Windows®, Android®, macOS® et Linux ?

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

7. Personnalisation du pare-feu nouvelle-génération

Les pare-feu peuvent importer des listes de règles et de politiques prédéterminées qui leur permettent d'agir contre les objets décrits dans ces listes. Les administrateurs ont ensuite la responsabilité de mettre à jour les pare-feu pour refléter les nouvelles menaces, protections et rôles définis dans les politiques. Face aux méthodes avancées des attaquants (automatisation, contournement, etc.), la sécurité doit pouvoir évoluer à vitesse machine.

Pourquoi cette fonctionnalité et pourquoi la tester ?

La meilleure façon de renforcer la sécurité de votre organisation consiste à intégrer l'automatisation et les listes dynamiques à votre pare-feu nouvelle génération. Les fournisseurs de pare-feu nouvelle génération offrent souvent des listes dynamiques que l'on peut mettre à jour manuellement ou par intégration à des sources externes de Threat Intelligence. Par conséquent, il suffit d'apporter les modifications des règles et des politiques à la liste dynamique. Tous les pare-feu qui y sont rattachés importeront alors régulièrement et automatiquement les protections les plus à jour.

Sortir du statu quo

Listes dynamiques

Lorsque de nouvelles menaces sont détectées, il incombe à l'administrateur du pare-feu de créer une règle ou une politique permettant au pare-feu de répondre de manière appropriée. Cette opération doit être effectuée pour chaque objet à risque, voire chaque pare-feu du réseau – un processus manuel, laborieux et souvent propice aux erreurs.

L'utilisation de listes dynamiques réduit considérablement les efforts manuels et améliore le temps de réponse. Aujourd'hui, les listes dynamiques incluent généralement des protections contre les adresses IP malveillantes connues et à haut risque validées par votre fournisseur de pare-feu nouvelle génération. Elles protègent également des adresses IP à haut risque provenant de données tierces corrélées qui n'ont pas été validées par votre fournisseur. Vous pouvez activer cette protection au niveau qui convient le mieux à votre organisation.

Dynamic User Groups (DUG)

Ces groupes d'utilisateurs dynamiques vous aident à créer des politiques qui permettent de remédier automatiquement aux comportements utilisateurs anormaux et de neutraliser les activités malveillantes, tout en maintenant une visibilité sur les utilisateurs. Une fois le groupe créé et les modifications validées, le pare-feu nouvelle génération enregistre les utilisateurs et les étiquettes associées, puis met à jour les appartenances. Les mises à jour des appartenances aux DUG sont automatiques. Utiliser des DUG plutôt que des objets de groupe statiques vous permet de répondre aux changements de comportement des utilisateurs et aux menaces potentielles sans avoir à modifier manuellement une quelconque politique.

Les groupes d'utilisateurs dynamiques facilitent l'application automatique des politiques et contribuent à renforcer la sécurité. Créés sur le pare-feu nouvelle génération, ils permettent de répondre immédiatement aux besoins, d'appliquer une sécurité adaptée au comportement de l'utilisateur, et de tirer un trait sur les droits d'accès excessifs. Les DUG donnent à un administrateur la possibilité de modifier l'appartenance d'un utilisateur, à la volée et directement sur le pare-feu, sans attendre que les modifications soient appliquées dans l'annuaire. Vous pouvez désormais modifier les accès des utilisateurs en fonction des changements d'activité.

Flux CTI tiers

Les organisations reçoivent des flux de Cyber Threat Intelligence (CTI) externes pour se mettre à jour sur les dernières menaces et les sources d'attaque. Ces flux fournissent une masse d'informations sur les indicateurs de compromission (IOC) bruts. Les nouvelles menaces sont ainsi rapidement connues et diffusées afin de ne laisser aux attaquants aucune chance de compromettre une organisation.

Transformer des données CTI en protections concrètes est un peu comme créer des règles et des politiques basées sur l'activité observée sur le pare-feu. Les deux sont des processus manuels chronophages que de nombreuses équipes de sécurité peinent à gérer. Les données de Threat Intelligence doivent être d'actualité et au bon format, ce qui peut nécessiter des conversions. Les données doivent également être corrélées pour valider le caractère malveillant d'un IOC, mettre en lumière des schémas d'attaques plus vastes par recoupement de plusieurs IOC, et ajouter le contexte nécessaire (priorité et pertinence des menaces nouvellement identifiées, par exemple). Une fois que les données ont été validées et contextualisées, les équipes de sécurité peuvent créer et distribuer les protections nécessaires pour faire face à des menaces spécifiques sur différents points de contrôle. Les fournisseurs peuvent également appliquer les protections aux points de contrôle. Toutefois, la consolidation avec le trafic local n'est pas aussi efficace. Si ces étapes ne sont pas suivies, les flux CTI ne restent que de simples amas de données inertes.

L'automatisation est indispensable pour baser votre sécurité sur la Threat Intelligence la plus actualisée, réduire les interventions manuelles et éliminer les erreurs humaines. Grâce au contexte obtenu de sources externes sur de nouvelles attaques inconnues, vous pouvez créer des protections pour prendre de vitesse les attaquants.

Les questions à intégrer à votre appel d'offre

- Le NGFW prend-il en charge les listes dynamiques et les groupes d'utilisateurs dynamiques pour automatiser l'application des politiques et renforcer la sécurité ?
- Peut-il incorporer des flux CTI tiers ou personnalisés de manière dynamique sans avoir à appliquer de politique ?
- Votre architecture de sécurité prend-elle en charge l'agrégation, la consolidation et la déduplication des flux CTI avant de transmettre les IOC au pare-feu ?
- Votre architecture de sécurité s'intègre-t-elle au pare-feu nouvelle génération pour automatiser le délai de suppression des indicateurs de menace expirés et éviter ainsi d'utiliser des données CTI obsolètes ?
- Votre architecture de sécurité permet-elle de cibler les indicateurs de menace à partir de récentes campagnes APT (Advanced Persistent Threats) et d'incorporer les flux CTI de manière proactive au pare-feu nouvelle génération ?
- Votre architecture de sécurité permet-elle d'attribuer un score de fiabilité aux informations CTI de façon à réduire la surcharge opérationnelle due au traitement des faux positifs ?

8. Prévention contre les nouvelles attaques

Les types d'attaques et le nombre d'appareils exposés atteignent aujourd'hui des proportions sans précédent. Phishing, détournement d'identifiants, attaques sur les réseaux sociaux, déni de service, ransomwares, backdoors, malwares CnC... les menaces sont protéiformes. Sans parler de l'Internet des objets (IoT), dont les appareils souvent peu sécurisés constituent autant de proies faciles pour les attaquants. Selon le rapport 2020 d'Unit 42 sur les menaces de l'IoT, 57 % des objets connectés sont vulnérables aux attaques de gravité moyenne à élevée, ce qui en fait une des cibles les plus faciles pour les attaquants. Ces derniers n'hésitent donc pas à s'en servir comme porte d'entrée vers d'autres systèmes du réseau.

Pourquoi cette fonctionnalité et pourquoi la tester ?

Aucun produit de sécurité ne peut, à lui seul, venir à bout de tous les types d'attaque. Tout comme il existe plusieurs étapes dans le cycle d'une attaque, les couches de défense doivent se superposer pour prévenir les nouveaux types d'attaques. La capacité de votre organisation à détecter et à prévenir des attaques de type malwares et ransomwares passe par une automatisation native et une interopérabilité entre vos produits de sécurité. La mise en œuvre d'une défense multi-niveau représente le moyen le plus efficace de contrer les attaques, chaque élément ajouté à l'architecture de sécurité devant agir en renfort des protections déjà présentes sur tout le réseau.

Selon Unit 42, l'équipe de Threat Intelligence de Palo Alto Networks, 30 % des appareils d'entreprise en réseau (hormis les smartphones) sont des objets connectés. Ces derniers posent un énorme risque de sécurité dans la mesure où ils sont souvent déployés avec des vulnérabilités intrinsèques, sont difficiles voire impossible à corriger et bénéficient parfois d'un accès illimité au réseau d'une organisation.

Sortir du statu quo

Il n'y a pas de solution miracle

Une protection efficace contre les nouvelles attaques exige une visibilité sur le trafic réseau et un contrôle des applications, ainsi que des politiques basées sur les utilisateurs et les contenus. Elle passe également par des produits de sécurité capables de protéger l'environnement contre les exploits connus et inconnus, les malwares et le trafic CnC, et les accès aux URL malveillantes et sites de phishing connus.

Chaque minute compte

Seule l'automatisation peut prendre les assaillants de vitesse et les empêcher de compléter leur cycle d'attaque au sein de votre organisation. Pour identifier et bloquer les menaces inconnues, les fichiers et URL malveillants doivent être détonés, analysés et décortiqués afin de détecter toute activité malveillante. Lorsque c'est le cas, des protections doivent être créées et automatiquement distribuées dans toute l'infrastructure de sécurité – sur le réseau, le cloud et les terminaux. Tous les points d'entrée reçoivent ainsi les informations nécessaires pour se protéger contre la dernière version de la menace.

Combiner les actions de prévention

L'efficacité de votre prévention dépend de votre capacité à exploiter l'automatisation et à partager des informations entre divers outils de sécurité. Ces outils interagissent par la suite pour détecter les malwares et les exploits connus et inconnus dans votre environnement, puis identifier et mettre en quarantaine les hôtes infectés de façon à empêcher toute propagation de l'attaque.

La Threat Intelligence doit occuper une place prépondérante dans vos efforts de prévention. Quant à votre pare-feu, il doit être capable de mettre à jour dynamiquement les mesures de prévention contre les adresses IP, domaines et URL malveillants en fonction des informations CTI et des IOC collectées.

Réduire l'exposition aux risques de sécurité IoT

Face à la multitude d'appareils en réseau, il peut être difficile pour les équipes de sécurité de tenir le rythme, sachant que chaque nouveau type d'appareil constitue une menace en puissance. Classification des appareils IoT, application des derniers correctifs logiciels, segmentation du réseau. surveillance active de l'environnement : toutes ces mesures permettent de limiter les accès des appareils IoT aux seules ressources nécessaires et de les placer sur les bons segments de réseau. Ce faisant, elles réduisent non seulement la surface d'attaque globale, mais également les risques pour d'autres ressources et réseaux.

Les questions à intégrer à votre appel d'offre

- Le NGFW peut-il bloquer les exécutables et les autres types de fichiers à risque provenant d'applications et d'URL inconnues pour prévenir les ransomwares ?
- Peut-il neutraliser les cyberattaques visant les appareils IoT ?
- Peut-il importer automatiquement et dynamiquement tous les IOC connus (adresses IP, domaines, URL, etc.) dans la liste de blocage pour agir de manière proactive face aux familles de ransomwares connus ?
- Une intégration de la Threat Intelligence au pare-feu nouvelle génération permet-elle des mises à jour dynamiques des URL malveillantes de la catégorie « ransomwares » dans la base de données de filtrage d'URL ?
- Une intégration de la Threat Intelligence au pare-feu nouvelle génération permet-elle des mises à jour dynamiques pour les domaines malveillants liés aux ransomwares sous forme de signatures DNS à ajouter automatiquement à une liste de blocage ou à détruire ?
- Votre logiciel de protection des terminaux fournit-il des informations complémentaires sur les menaces et les comportements suspects au pare-feu, et vice versa ?
- Le pare-feu offre-t-il une visibilité sur tous les appareils IoT du réseau, y compris ceux jamais détectés auparavant ?
- Peut-il séparer le trafic IoT du reste du réseau pour empêcher les appareils compromis de servir de tremplin aux attaques ?
- Recommande-t-il des politiques basées sur l'évaluation des risques et applicables automatiquement ?

9. Protection homogène des utilisateurs et des applications où qu'ils se trouvent

De plus en plus mobiles et géographiquement dispersés, les utilisateurs ont besoin d'accéder à des applications depuis des sites distants éparpillés dans le monde entier. Alors que de plus en plus d'applications sont aujourd'hui hébergées dans le cloud, les sites distants exigent une connectivité et une sécurité équivalentes à celles des QG d'entreprises. Cependant, de nombreuses organisations manquent de visibilité sur le trafic lorsque les utilisateurs accèdent à Internet et aux applications cloud hors site, ce qui engendre un risque de sécurité.

Pourquoi cette fonctionnalité et pourquoi la tester ?

Votre organisation doit protéger tous ses utilisateurs de manière homogène, c'est-à-dire sans avoir à créer différents profils de sécurité selon leur lieu de connexion. Étant donné que les politiques de sécurité sont toujours plus efficaces lorsqu'elles peuvent être administrées comme un tout, un ensemble d'outils et un cadre de politique communs donneront davantage de contrôle et de maîtrise aux équipes de sécurité.

Sortir du statu quo

Le SD-WAN (Software-Defined Wan Area Networking) est désormais incontournable pour les entreprises distribuées. Son principe : utiliser des liaisons standards pour permettre une gestion et un contrôle intelligents des connexions entre les sites distants et les instances cloud. Un pare-feu nouvelle génération doit pouvoir fonctionner comme un équipement SD-WAN de périphérie sur un site distant, et comme un hub SD-WAN sur un site central. Quant aux fonctionnalités SD-WAN elles-mêmes, elles doivent être simples à activer et pilotées depuis une interface centralisée.

Grâce au SD-WAN, chaque appareil est géré en central. Le routage est basé sur des politiques applicatives, de telle sorte que les gestionnaires WAN peuvent créer et mettre à jour des règles de sécurité en temps réel à mesure que les exigences du réseau évoluent. Par ailleurs, la combinaison du SD-WAN et du Zero Touch Provisioning (ZTP), une fonctionnalité qui permet d'automatiser les déploiements et les configurations, réduit davantage la complexité, les dépenses et le besoin en ressources nécessaires à la mise en place de nouveaux sites. Enfin, le SD-WAN permet d'accéder aux ressources cloud sans backhaul du trafic par un data center central, ce qui améliore l'expérience utilisateur.

Votre organisation doit fournir une protection homogène à tous ses utilisateurs, qu'ils travaillent sur site ou à distance. Côté déploiement, les options disponibles doivent être suffisamment flexibles pour permettre une couverture uniforme de tous les utilisateurs et emplacements. Ainsi, peu importe où ils se trouvent, les utilisateurs peuvent se connecter facilement à un service cloud ou à un pare-feu pour leur sécurité, tout en bénéficiant de la même protection contre les menaces connues et inconnues.

Les questions à intégrer à votre appel d'offre

- Le NGFW peut-il fournir une politique de sécurité cohérente pour les utilisateurs mobiles ?
- Pouvez-vous protéger les utilisateurs qui ne se situent pas derrière un pare-feu nouvelle génération ?
- Peut-il fonctionner comme un équipement SD-WAN de périphérie ?
- Intègre-t-il des fonctions ZTP (Zero Touch Provisioning) ?
- Peut-il utiliser plusieurs pare-feu physiques/virtuels pour assurer une connexion VPN permanente ?
- Peut-il s'appuyer sur le cloud pour rapprocher la protection au plus près de vos utilisateurs ?

10. Adoption d'une approche Zero Trust

Le modèle de sécurité du réseau qui consistait à classer les utilisateurs comme « fiables » ou « non fiables » ne fonctionne plus. Quiconque accède à votre réseau, qu'il s'agisse d'un attaquant, d'un collaborateur interne mal intentionné ou d'un utilisateur aux droits d'accès trop permissifs, est libre de se déplacer latéralement. Du vol d'identifiants et de données à l'exfiltration d'informations de propriété intellectuelle, en passant par la propagation de malwares, votre réseau se retrouve exposé à toutes sortes de menaces. Il est donc essentiel de le segmenter et de définir des politiques de contrôle d'accès. Comme son nom l'indique, le Zero Trust consiste à tirer un trait sur la notion de confiance. Son mot d'ordre : « ne jamais faire confiance, toujours vérifier ».

Pourquoi cette fonctionnalité et pourquoi la tester ?

Aujourd'hui, le moyen le plus efficace de sécuriser les réseaux consiste à adopter une approche Zero Trust qui applique un contrôle d'accès basé sur le principe du moindre privilège et inspecte tous les utilisateurs, appareils, contenus et applications sur tous les sites. La méthodologie Zero Trust établit un cadre pour la mise en place d'un réseau segmenté. Le Zero Trust se révèle une arme de prévention puissante lorsqu'il est appliqué à toute l'entreprise, du réseau aux terminaux en passant par le cloud. En s'appuyant sur une approche intégrée, les équipes de sécurité peuvent automatiser et rationaliser la gestion des politiques Zero Trust dans toute l'entreprise (création, administration, déploiement, maintenance, etc.).

Un des critères essentiels du Zero Trust repose sur l'application d'une politique en couche L7 via un pare-feu nouvelle génération servant de passerelle de segmentation. Cette politique est rédigée de façon à refléter la structure même de votre entreprise, c'est-à-dire la manière dont le trafic traverse votre réseau et les interdépendances de vos données, utilisateurs et applications.

Sortir du statu quo

Une approche Zero Trust permet d'identifier une « surface de protection » pour les données, ressources, applications et services (DaaS) les plus critiques du réseau.

Le pare-feu nouvelle génération facilite la microsegmentation des périmètres. Il sert également de point de contrôle et de réseau de capteurs pour une visibilité complète sur le trafic. S'il est important de sécuriser le périmètre traditionnel, il est encore plus crucial de bénéficier d'une visibilité et d'un contrôle précis pour surveiller le trafic nord-sud et est-ouest. Des instruments comme la MFA et d'autres méthodes de vérification améliorent votre capacité à vérifier et valider l'identité des utilisateurs.

Le modèle Zero Trust passe nécessairement par une protection multi-niveau. D'où l'importance d'incorporer des outils capables de bloquer les menaces avancées et de fournir des informations sur ce qui se passe sur votre réseau. Vous devez non seulement définir des politiques pour empêcher l'accès non autorisé à certaines ressources ou données, mais également utiliser la visibilité dont vous bénéficiez pour identifier les anomalies (changements de comportement d'un utilisateur dus à sa fonction, activité malveillante, etc.) et mettre à jour les politiques. Bref, cette visibilité doit vous aider à réagir rapidement lorsqu'une activité malveillante est identifiée.

Les questions à intégrer à votre appel d'offre

- Le NGFW peut-il fonctionner comme une passerelle de segmentation ?
- Offre-t-il une visibilité sur le trafic et permet-il de le déchiffrer et de l'inspecter entièrement ?
- Êtes-vous en mesure de rédiger et d'appliquer sur le pare-feu une politique en couche L7 basée sur le contexte ?

Bonus : fournir des options de déploiement flexibles, y compris sous forme de containers

Pour de nombreuses entreprises, les équipements physiques restent des points de contrôle essentiels pour le trafic entrant et sortant du data center, sans parler de leur rôle moteur dans la puissance des réseaux. De leur côté, les appliances virtuelles offrent une visibilité sur le trafic est-ouest des data centers définis par logiciel et permettent de faire évoluer la sécurité au rythme de ces environnements dynamiques.

Cependant, l'adoption rapide des containers ajoute une nouvelle variable à l'équation. De par leur connexion aux applications historiques sur site, les applications cloud-native doivent être soumises aux mêmes règles de protection et de conformité de la part des équipes de sécurité.

Pourquoi cette fonctionnalité et pourquoi la tester ?

Les solutions traditionnelles sont limitées. Bien que certaines s'intègrent aux outils d'orchestration des containers, leur visibilité se limite souvent au nœud ou au cluster et elles tendent à se limiter au filtrage de base des ports et des protocoles. De leur côté, les pare-feu cloud-native ne proposent qu'un blocage de port de base pour la microsegmentation des containers, sans possibilité de prévenir les menaces. Quant aux pare-feu nouvelle génération traditionnels, ils ne disposent pas nativement du contexte sur les containers et de l'intégration au framework d'orchestration nécessaires pour fournir une sécurité avancée dans ces environnements agiles et dynamiques.

Sortir du statu quo

Une gestion efficace des environnements de containers cloud-native demande de pouvoir étendre la visibilité et le contrôle du pare-feu nouvelle génération au trafic « pod à pod » et « container à container ». Objectif : inspecter les menaces au sein d'un cluster et renforcer la protection des data centers containerisés. Par ailleurs, les containers accèdent souvent à des ressources web (par exemple des référentiels GitHub®) pour extraire le code source. Raison de plus pour établir une visibilité et un contrôle sur le trafic web applicatif afin de s'assurer que les containers ne communiquent qu'avec le référentiel approprié et que le trafic résultant n'est pas usurpé ou malveillant. Les pare-feu nouvelle génération capables d'opérer dans les environnements physiques, virtuels et containerisés contribuent à assurer une protection homogène de data centers de plus en plus hybrides.

Les questions à intégrer à votre appel d'offre

- Le NGFW offre-t-il une sécurité homogène du réseau et une prévention des menaces adaptées aux applications hébergées sur site, aux environnements virtualisés et aux containers ?
- Peut-il être déployé en natif dans Kubernetes® pour intégrer son provisionnement dans le cadre d'un processus d'intégration et de déploiement continus (CI/CD) ?
- S'intègre-t-il aux solutions SDN (Software-Defined Networking) pour permettre la segmentation des sites distants et pour respecter les exigences de conformité PCI ?

Sécurité complète

Les attaquants recourent à des techniques de plus en plus sophistiquées pour lancer des attaques ciblées, automatisées, furtives et capables de s'étendre à de multiples environnements.

C'est pourquoi votre pare-feu nouvelle génération et les divers produits qui composent votre infrastructure de sécurité doivent vous fournir une protection complète, y compris les éléments ci-après.

Technologies hors pair

Utilisez des technologies de pointe capables de bloquer les menaces connues et inconnues, de manière rapide et automatique, à chaque étape du cycle d'attaque. Ces produits doivent offrir une protection cohérente et adaptée face aux risques liés aux données et aux utilisateurs, quel que soit leur emplacement. Quant à votre écosystème de sécurité, il doit pouvoir se mettre à jour de façon flexible pour vous adapter à l'évolution des risques et des workloads.

Efficacité opérationnelle

Les livraisons automatisées et les intégrations par API réduisent le temps consacré aux tâches manuelles sujettes à erreurs. Vous devez être en mesure de piloter la sécurité sur divers environnements sans grever les ressources ou les budgets, et sans ajouter de complexité. Les équipes de sécurité pourront ainsi se recentrer sur les projets stratégiques les plus déterminants pour l'organisation.

Service compétent et réactif

Des équipes de service et de support compétentes et réactives accélèrent la prise en main de la solution et vous aident à renforcer votre sécurité en continu bien après la migration initiale. À la clé : une rentabilisation optimale de votre investissement et des niveaux de sécurité toujours plus élevés.

Lorsque vous planifiez votre prochain achat ou évaluez votre pare-feu actuel, il est important de tester les différentes fonctionnalités du pare-feu avec toutes les équipes de sécurité de votre organisation.

Une fois testés, les 10 points évoqués dans ce document vous aideront à déterminer l'adéquation de votre prochain pare-feu aux besoins de votre organisation actuels et futurs, en gardant à l'esprit les innovations à venir.

Prêt à évaluer votre prochain pare-feu ? Testez-le par vous-même.

paloalto NETWORKS

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

+31 20 888 1883

www.paloaltonetworks.fr

10-things-to-test-in-your-future-next-generation-firewall-wp-062420-fr