10

Choses que Votre Pare-feu Suivant Doit Faire

paloalto NETWORKS®

the network security company™

Introduction

Vos réseaux sont plus complexes qu'ils ne l'ont jamais été. Vos collaborateurs accèdent aux applications de leur choix au moyen d'équipements de l'entreprise ou personnels. Bien souvent, ces applications sont utilisées à des fins professionnelles et privées sans réelle prise de conscience des risques métier et de sécurité induits. Les futurs collaborateurs se renseignent sur les conditions d'utilisation des applications avant même d'accepter leur nouveau poste. Enfin, les questions que vous êtes susceptible de vous poser sur l'efficacité de votre cybersécurité doivent également être prises en compte. Votre entreprise est-elle une cible ? Les menaces sont-elles réelles ou seulement supposées ? Les mesures nécessaires ont-elles été prises ? La complexité de votre réseau et de votre infrastructure de sécurité risque de ralentir votre capacité à faire face aux menaces qui sévissent dans le cyberespace.

Dès lors que la complexité freine la prise de décision, il est utile de « revenir aux fondamentaux » afin de trouver des solutions aux problèmes identifiés. C'est dans cet esprit que nous rappelons ici trois des principaux rôles que tout pare-feu moderne doit tenir :

1) Être situé au cœur de votre infrastructure de sécurité réseau.

2) Servir de point de contrôle d'accès à tout le trafic afin d'autoriser ou de refuser le trafic en fonction des politiques définies.

3) Éliminer le risque de l'« inconnu » au moyen d'un modèle de contrôle positif de type « autoriser certaines applications et refuser implicitement tout le reste ».

Au fil des ans, les fonctions essentielles qu'exécutait votre pare-feu ont été rendues inefficaces par le trafic même qu'elles étaient censées surveiller. L'évolution des applications a conduit le pare-feu, qui est au cœur de l'infrastructure de sécurité, à manquer des contrôles nécessaire pour protéger les données numériques.

Saut de port en port, utilisation de ports non-standard et chiffrement sont autant de techniques qui rendent aujourd'hui les applications plus accessibles. Malheureusement, ces mêmes techniques sont aussi celles que les pirates informatiques utilisent soit directement dans les cyber menaces qu'ils créent, soit indirectement, en dissimulant les menaces au sein même du trafic des applications. Le fait que vos collaborateurs utilisent ces applications modernes pour accomplir leur travail ne fait qu'augmenter le défi. Parmi les applications et les menaces présentes sur votre réseau, citons notamment:

- Applications populaires : médias sociaux, partage de fichiers, vidéo, messagerie instantanée et messagerie électronique. Elles représentent près de 25 percent des applications transitant par votre réseau et 20 percent de la bande passante. Les collaborateurs utilisent certaines d'entre elles à des fins professionnelles, d'autres à des fins purement personnelles. Ces applications offrent généralement une grande capacité d'extension et intègrent souvent des fonctionnalités à haut risque. Compte tenu des risques métier et de sécurité que ces applications induisent, votre défi consiste à trouver un juste équilibre en bloquant certaines d'entre elles et en activant d'autres de manière sécurisée.

- Applications professionnelles de base : vous utilisez ces applications pour mener à bien vos activités professionnelles. Elles hébergent notamment vos actifs les plus précieux (bases de données, serveurs de fichiers et d'impression, annuaires et autre). Cibles privilégiées des cyber délinquants, ces applications font souvent l'objet d'attaques multiformes. Votre défi consiste à trouver le meilleur moyen de les isoler et de les protéger de ces attaques furtives qui déjouent facilement votre pare-feu et votre IPS avec des techniques d'évasion.
- Applications système et personnalisées : il s'agit des applications d'infrastructure comme SSL, SSH et DNS, des applications personnalisées développées en interne ou d'applications inconnues. Ces applications inconnues sont souvent utilisées pour masquer des commandes et gérer le trafic généré par des robots ou d'autres logiciels malveillants. La grande majorité de ces applications utilise un vaste éventail de ports non-standard. 85 des 356 applications utilisant le chiffrement en SSL ne passent jamais par le port 443 ni par les ports réservés à SSL (37 sautent de port en port, 28 utilisent le port tcp/80, 20 utilisent des ports autres que le port tcp/443).

Pour tenter de relever ces défis, les fournisseurs de pare-feu s'intéressent davantage aux fonctions de base des pare-feu et réfléchissent à la façon d'identifier et de contrôler le trafic en fonction de l'application proprement dite plutôt qu'à partir du port et du protocole. Les pare-feu qui utilisent cette approche axée sur les applications sont appelés des « pare-feu nouvelle génération ». Tous les fournisseurs de pare-feu reconnaissent aujourd'hui l'importance capitale du contrôle des applications dans la sécurité du réseau.

Ce nouvel intérêt pour les fonctions de base des pare-feu est dû à deux raisons. Premièrement, les applications, et les menaces qui y sont associées, se jouent facilement des pare-feu basés sur les ports et des dispositifs supplémentaires de prévention des menaces. Deuxièmement, le pare-feu est le seul élément à voir passer tout le trafic transitant par votre réseau. Il est donc logique de choisir cet emplacement pour mettre en œuvre les stratégies de contrôle d'accès. L'intérêt de cette nouvelle orientation est évident : sécurité renforcée et réduction, ou du moins stabilité, des tâches administratives liées à la gestion du pare-feu et à la résolution des incidents.

Pare-feu Nouvelle Génération

1. Identifier les applications indépendamment du port, du protocole, de la technique d'évasion ou du chiffrement.
2. Identifier les utilisateurs indépendamment de leur équipement ou de leur adresse IP.
3. Bloquer en temps réel les menaces connues et inconnues embarquées dans les applications.
4. Offrir une parfaite visibilité des applications, des utilisateurs et du contenu et proposer un contrôle granulaire des politiques.
5. Fournir un débit multi-gigabits pour un déploiement en ligne prévisible.

Définition du Pare-feu Nouvelle Génération

Pour Gartner, le pare-feu nouvelle génération est un outil novateur, axé sur l'entreprise, qui « intègre des systèmes d'inspection complets assurant la prévention des intrusions, la surveillance des applications et un contrôle granulaire des politiques ». La plupart des fournisseurs de sécurité réseau prennent en charge la visibilité et le contrôle des applications en ajoutant des signatures d'applications dans leur moteur IPS ou en proposant un module complémentaire de contrôle applicatif. Dans les deux cas, ces options viennent simplement compléter le pare-feu basé sur les ports et ne substituent en rien aux tâches essentielles que votre pare-feu doit exécuter.

L'efficacité opérationnelle de votre entreprise dépend considérablement des applications que vos collaborateurs utilisent et du contenu que ces applications elles-mêmes véhiculent. Si vous vous contentez d'en autoriser certaines et d'en bloquer d'autres, vous risquez de freiner le développement de vos activités. Si les responsables de la sécurité sont intéressés par les fonctionnalités d'un pare-feu nouvelle génération, ils doivent avant tout chercher à savoir si cette technologie les aidera ou non à sécuriser l'utilisation des applications au sein de l'entreprise. Pour cela, ils doivent se poser les questions suivantes :

- La visibilité et l'interprétation du trafic des applications transitant par le réseau seront-elles meilleures ?
- Les options de contrôle du trafic iront-elles au-delà du modèle classique « autorisation/blocage » ?
- Le réseau sera-t-il protégé contre les menaces et cyber attaques connues et inconnues ?
- Sera-t-il possible d'identifier et de gérer systématiquement le trafic inconnu ?
- Sera-t-il possible de mettre en œuvre les stratégies de sécurité voulues sans nuire aux performances ?
- Les tâches d'administration des pare-feu seront-elles minimisées ?
- La gestion des risques sera-t-elle simplifiée et plus efficace ?
- Les stratégies mises en œuvre contribueront-elles à la rentabilité de l'entreprise ?

Si la réponse à chacune des questions ci-dessus est « oui », alors votre décision de passer aux pare-feu nouvelle génération est justifiée. La prochaine étape consiste à étudier les différentes solutions proposées par les fournisseurs de pare-feu. Lors de cette comparaison, il est important d'analyser l'architecture des différentes offres ainsi que leurs impacts sur l'environnement de production en termes de fonctionnalités, d'opérations et de performances.

Considérations Sur l'architecture des Pare-feu et l'identification du Trafic

En concevant les pare-feu nouvelle génération, les fournisseurs de solutions de sécurité ont nécessairement adopté l'une des deux approches architecturales suivantes :

1. Intégrer l'identification des applications au pare-feu, qui devient le principal moteur de classification.
2. Ajouter un moteur de filtrage des signatures d'applications à un pare-feu basé sur les ports.

Dans les deux cas, la reconnaissance des applications a bien lieu mais avec différents degrés de précision, de convivialité et de pertinence. Plus important encore, ces approches architecturales imposent un modèle de sécurité spécifique pour la stratégie d'utilisation des applications - soit positif (blocage par défaut), soit négatif (autorisation par défaut).

- Un modèle de sécurité positif (pare-feu ou autre) permet d'écrire des politiques qui autorisent certaines applications ou fonctions (comme WebEx, SharePoint et Gmail) et interdisent implicitement tout le reste. Dans ce cas, la classification du trafic intervient en amont au niveau du pare-feu (et non après coup) de façon à n'autoriser que le trafic approprié et à refuser tout le reste. En ayant une visibilité totale sur le trafic, les entreprises peuvent minimiser les tâches administratives liées au suivi de l'activité du réseau, à la gestion des politiques et à la résolution des incidents. En termes de sécurité, les implications sont de taille. Vous contrecarrez efficacement les cyber attaques connues et inconnues tout en vous laissant la possibilité d'autoriser davantage d'applications sur votre réseau. Vous renforcez le filtrage des applications inconnues au niveau du pare-feu grâce à une stratégie de type « refuser tout le reste ».
- Un modèle de sécurité négatif (IPS, anti-virus ou autre) permet de rechercher et de bloquer des éléments spécifiques (généralement des menaces ou des applications indésirables) et de laisser passer tout le reste. Dans ce cas, le trafic n'est pas classifié dans sa totalité, mais uniquement les éléments figurant dans la liste de blocage définie. Si cette technique s'avère suffisante pour détecter et bloquer certaines menaces ou applications indésirables, le modèle négatif n'est pas en mesure de contrôler l'ensemble du trafic de votre réseau et ne fait que seconder le pare-feu basé sur les ports. Au niveau de l'entreprise, un modèle de sécurité négatif se traduit par un alourdissement des tâches administratives, une multitude de politiques à gérer et une redondance des bases de données de journaux.

Ce guide se décompose ensuite en trois sections distinctes. La première section présente les 10 principales fonctions que doit posséder votre prochain pare-feu. Son but est de démontrer que l'architecture et le modèle de contrôle décrits ci-dessus permettent d'identifier et de sécuriser efficacement les applications au niveau du pare-feu. Les autres sections se penchent sur la façon dont ces 10 fonctions vous permettent de sélectionner un fournisseur lors d'un appel d'offres et d'évaluer physiquement le pare-feu.

1. Identifier et contrôler les applications sur n'importe quel port
2. Identifier et contrôler tous les moyens de contournement
3. Déchiffrer les flux SSL sortants et contrôler les flux SSH
4. Contrôler les différentes fonctions d'une même application
5. Gérer systématiquement le trafic inconnu
6. Détecter les virus et les logiciels malveillants dans toutes les applications, sur tous les ports
7. Offrir la même visibilité et les mêmes outils de contrôle pour tous les utilisateurs et équipements
8. Simplifier la sécurité réseau tout en intégrant le contrôle des applications
9. Fournir le même débit et les mêmes performances une fois le contrôle des applications activé
10. Assurer les mêmes fonctions de pare-feu qu'il s'agisse d'un environnement physique ou virtuel

Les 10 Principales Fonctions que Doit Posséder Votre Prochain Pare-feu

Les critères de sélection d'un pare-feu concernent généralement trois domaines : fonctions de sécurité, opérations et performances. En termes de sécurité, il convient d'étudier l'efficacité des contrôles et la capacité de votre équipe à gérer les risques associés au trafic réseau. D'un point de vue opérationnel, la grande question est de savoir « où a lieu le contrôle des applications et cela représente-t-il un travail de gestion important pour l'équipe chargée de la sécurité ? ». En termes de performances, la question est simple : le pare-feu est-il capable de faire ce qu'il est censé faire au débit requis par les besoins de votre entreprise ? Bien que chaque organisation ait des priorités et des besoins différents pour chacun des trois critères de sélection, globalement les 10 principales fonctions que doit posséder votre prochain pare-feu sont les suivantes :

1

Votre prochain pare-feu doit en permanence identifier et contrôler les applications sur tous les ports.

Problématique : Les développeurs d'applications ne respectent plus la méthodologie de développement standard port/protocole/application. De plus en plus d'applications sont capables de transiter par des ports non-standard ou peuvent changer dynamiquement de port (messagerie instantanée, partage de fichiers peer to peer ou VoIP, par exemple). Par ailleurs, les utilisateurs sont de plus en plus expérimentés et peuvent forcer

les applications comme RDP et SSH à s'exécuter sur des ports non-standard. Pour appliquer des politiques spécifiques aux applications afin de pallier aux lacunes des ports, votre prochain pare-feu doit supposer que n'importe quelle application peut s'exécuter sur n'importe quel port. Ce concept justifie à lui seul la migration vers les pare-feu nouvelle génération. C'est aussi la raison pour laquelle un modèle de contrôle négatif ne permet pas de résoudre ce problème. Si une application peut transiter par n'importe quel port, un pare-feu basé sur un contrôle négatif nécessite d'avoir cette information à l'avance ou d'exécuter en permanence toutes les signatures sur la totalité des ports.

Solution : Il est évident que, si n'importe quelle application peut s'exécuter sur n'importe quel port, votre prochain pare-feu doit, par défaut, classifier le trafic par application, sur tous les ports et tout le temps. La classification du trafic sur les ports est un thème récurrent qui sera abordé à plusieurs reprises dans ce document dans la mesure où le filtrage des ports continuera à être déjoué par les techniques qui ont cours depuis des années.

2

Votre prochain pare-feu doit identifier et contrôler les techniques d'évasion.

Problématique : Quelques-unes des applications de votre réseau risquent de servir à déjouer les politiques de sécurité mises en place pour protéger les actifs numériques de votre entreprise. Deux catégories d'applications sont concernées : celles qui sont spécifiquement conçues pour contourner les points de contrôle (serveurs proxy externes, tunnels chiffrés hors VPN) et celles qu'il est possible d'adapter facilement aux mêmes fins (outils d'administration à distance de serveurs/postes de travail).

- Les applications passant par des serveurs proxy externes et des tunnels chiffrés hors VPN servent principalement à déjouer les contrôles de sécurité en place au moyen de différentes techniques d'évasion. Ces applications n'apportent aucune valeur métier à votre réseau puisqu'elles visent à contourner la sécurité, mettant ainsi en danger les activités et la sécurité de l'entreprise.
- Les outils d'administration de serveurs/postes de travail à distance, comme RDP et Teamviewer, aident généralement les administrateurs à s'acquitter efficacement de leurs tâches. Ils permettent également aux collaborateurs de contourner le pare-feu et de se connecter à leur ordinateur personnel ou à tout autre poste extérieur au réseau. Les cyber pirates savent bien que ces applications sont fréquemment utilisées. D'ailleurs, le « Verizon Data Breach Report (DBIR) » et le « Mandiant Report » ont tous deux exposé publiquement des cas où ces outils d'accès à distance avaient été utilisés au cours d'une ou de plusieurs phases d'attaque.

Soyons plus précis. Ces applications ne présentent pas toutes les mêmes risques : les applications d'accès à distance ont des utilisations légitimes, tout comme certaines applications transitant dans des tunnels chiffrés. Malheureusement, les cyber pirates se servent de plus en plus de ces mêmes outils pour lancer leurs attaques persistantes et incessantes. Si elles n'ont pas la capacité de contrôler ces techniques d'évasion, les entreprises ne peuvent pas appliquer leurs politiques de sécurité et s'exposent à des risques dont elles pensaient être à l'abri.

Solution : Plusieurs types d'applications de contournement sévissent, chacune utilisant des techniques légèrement différentes. Il existe des serveurs proxy externes, publics et privés, qui utilisent à la fois les protocoles HTTP et HTTPS (voir le site proxy.org pour consulter une base de données de ces serveurs proxy publics). Les serveurs proxy privés sont souvent configurés avec des adresses IP non-classifiées (ordinateurs personnels) au moyen d'applications comme PHProxy ou CGIProxy. Les applications d'accès à distance comme RDP, Teamviewer ou GoToMyPC sont souvent utilisées à bon escient mais, compte tenu des risques inhérents qu'elles induisent, elles doivent faire l'objet d'une attention particulière. Dans la plupart des cas, les logiciels de contournement (comme Ultrasurf, Tor et Hamachi) n'ont aucune raison professionnelle de traverser votre réseau. Quelle que soit la stratégie de sécurité choisie, votre prochain pare-feu doit disposer de techniques spécifiques pour identifier et contrôler toutes ces applications indépendamment du port, du protocole, du chiffrement ou de toute autre technique d'évasion. Considération supplémentaire : ces applications sont régulièrement mises à jour, ce qui les rend encore plus difficiles à détecter et à contrôler. Vous devez donc en tirer deux leçons. Votre prochain pare-feu doit pouvoir identifier ces applications, mais vous devez aussi veiller à mettre constamment à jour son intelligence applicative.

3

Votre prochain pare-feu doit déchiffrer et inspecter le trafic SSL tout en contrôlant SSH.

Problématique : Aujourd'hui, 26 percent des applications sont chiffrées en SSL, sous quelque forme et de quelque façon que ce soit, sur les réseaux d'entreprise. Du fait de l'utilisation croissante de HTTPS dans des applications à haut rendement et à haut risque (Gmail ou Facebook, par exemple), et de la possibilité d'activer manuellement SSL sur de nombreux sites, les équipes chargées de la sécurité doivent faire face à une perte de visibilité de plus en plus importante. Un pare-feu nouvelle génération doit être suffisamment flexible pour ne pas s'intéresser à certains types de flux SSL (trafic issu d'organismes financiers et médicaux) et, au contraire, appliquer des politiques pour en déchiffrer d'autres (flux SSL transitant via des ports non-standard ou flux HTTPS issus de sites Web non classifiés d'Europe de l'Est). Le protocole SSH est utilisé quasiment partout dans le monde et peut être facilement configuré par les utilisateurs à des fins non professionnelles de la même manière qu'un outil d'accès à distance. De plus, le fait que SSH soit chiffré facilite la dissimulation des activités non-professionnelles.

Solution : La capacité à déchiffrer le trafic SSL est un élément essentiel, non seulement parce que le protocole SSL représente une part de plus en plus importante du trafic d'entreprise, mais aussi parce qu'il permet d'activer d'autres fonctionnalités clés par la suite. Il convient donc d'examiner certains éléments clés comme la reconnaissance et le déchiffrement de SSL sur n'importe quel port, que ce soit en entrée ou en sortie, le contrôle stratégique du déchiffrement et les éléments matériels et logiciels nécessaires pour déchiffrer des dizaines de milliers de connexions SSL simultanément sans dégradation des performances. Il faut, par ailleurs, tenir compte de la capacité à identifier et à contrôler les flux SSH. Dans ce domaine, il est important de savoir si SSH est utilisé pour la redirection des ports (local, distant et X11) ou pour un usage natif (SCP, SFTP et accès à l'interpréteur), afin d'appliquer les politiques de sécurité adéquates.

4

Votre prochain pare-feu doit permettre un contrôle des différentes fonctions d'une même application.

Problématique : Les développeurs de plateformes d'application comme Google, Facebook, salesforce.com ou Microsoft proposent aux utilisateurs un vaste éventail de fonctionnalités destinées à les fidéliser, mais représentant des profils de risque très différents. Par exemple, s'il est intéressant d'autoriser WebEx, outil professionnel d'une grande valeur, l'utilisation de WebEx Desktop Sharing (prise en main d'un poste de travail depuis une source extérieure) peut constituer une violation à une règle de conformité interne ou réglementaire. Citons encore l'exemple de Google Mail (Gmail) et de Google Talk (Gtalk). Une fois connecté à Gmail, dont l'accès a été autorisé par une politique de sécurité, l'utilisateur peut très facilement passer à Gtalk, dont l'usage risque d'être interdit. Votre prochain pare-feu doit donc pouvoir reconnaître et délimiter chaque fonctionnalité individuellement de façon à vous permettre de mettre en place une stratégie appropriée.

Solution : Votre prochain pare-feu doit en permanence identifier chaque application, contrôler les changements pouvant indiquer l'utilisation d'une autre fonction. La classification du trafic « une fois pour toutes » n'est plus possible car ces applications populaires partagent des sessions et prennent en charge plusieurs fonctions. Si une nouvelle fonction est introduite au cours de la session, le pare-feu doit noter le changement dans les tables d'état et revérifier la politique de sécurité. Votre prochain pare-feu doit impérativement assurer un suivi permanent des états des fonctions afin d'identifier clairement les fonctions prises en charge par chaque application et les différents risques qui y sont associés.

5

Votre prochain pare-feu doit systématiquement gérer le trafic inconnu.

Problématique : Bien qu'en faible volume, un trafic d'origine inconnue circule sur tous les réseaux et représente un risque potentiel élevé pour vous et votre entreprise. En ce qui concerne le trafic inconnu, plusieurs points importants sont à prendre en compte. Est-il classifié ? Est-il possible d'en réduire le volume à l'aide de politiques de sécurité ? Votre pare-feu est-il en mesure de décrire les applications propres à l'entreprise de manière à ce que votre politique de sécurité les « reconnaissent » ? Votre pare-feu vous aide-t-il à déterminer si le trafic inconnu constitue une réelle menace ?

Le trafic inconnu est souvent source de menaces pour le réseau. Les cyber pirates sont souvent obligés de modifier un protocole pour exploiter une application cible. Par exemple, il est possible que pour attaquer un serveur Web, un cyber pirate modifie tellement l'en-tête HTTP que le trafic en découlant ne sera plus reconnu comme du trafic Web. Une anomalie de la sorte laisse vite penser à une attaque. De même, les logiciels malveillants utilisent souvent des protocoles personnalisés au sein de leur modèle de commande et de contrôle, ce qui permet aux administrateurs de la sécurité d'extraire toutes les infections de logiciels malveillants inconnus.

Solution : Par défaut, votre prochain pare-feu doit essayer de classifier tout le trafic sur l'ensemble des ports. C'est l'un des points où l'architecture et le modèle de contrôle de sécurité dont nous avons parlé au préalable prennent toute leur importance. Les modèles positifs (blocage par défaut) classifient tout ; les modèles négatifs (autorisation par défaut) ne classifient que ce qu'on leur demande de classifier. La classification totale n'est qu'une infime partie du défi que pose le trafic inconnu. Votre prochain pare-feu doit vous offrir une visibilité totale sur le trafic inconnu, sur tous les ports et depuis un emplacement [d'administration] unique. Il doit être capable d'analyser rapidement le trafic de façon à déterminer s'il s'agit (1) d'une application interne ou propre à l'entreprise, (2) d'une application commerciale sans signature ou (3) d'une menace. En outre, votre prochain pare-feu doit disposer de tous les outils requis non seulement pour surveiller le trafic inconnu, mais aussi pour le gérer systématiquement en le contrôlant au moyen de politiques, en créant une signature personnalisée, en analysant le PCAP d'une application commerciale de manière approfondie ou en procédant à une investigation rigoureuse pour savoir s'il s'agit d'une menace.

6

Votre prochain pare-feu doit détecter les menaces dans toutes les applications, sur tous les ports.

Problématique : Pour optimiser leur efficacité, les entreprises adoptent une multitude d'applications hébergées en interne ou en dehors de leur site physique. Qu'il s'agisse d'une application hébergée externe comme SharePoint, Box, Google Docs, Microsoft Office365 ou d'une application extranet hébergée par un partenaire, votre entreprise est susceptible d'utiliser une application qui passe par des ports non-standard, utilise SSL ou partage des fichiers. Ces applications augmentent certes l'efficacité de l'entreprise, mais représentent aussi un vecteur important de menaces. De plus, certaines de ces applications, comme SharePoint par exemple, reposent sur des technologies qui sont des cibles régulières d'infection (IIS ou SQL Server). S'il ne convient pas de bloquer ces applications, il ne faut pas non plus les laisser passer aveuglément compte tenu des risques potentiels qu'elles font courir à l'entreprise et à la sécurité du cyberespace.

L'utilisation de ports non-standard est devenue une pratique courante dans le monde de la délinquance informatique. Dans la mesure où les logiciels malveillants résident sur le réseau et que les communications font généralement intervenir un client malveillant (le programme malveillant) et un serveur malveillant (l'organe de commande et de contrôle), le cyber pirate a tout loisir d'utiliser la combinaison de port et protocole de son choix. Selon une récente analyse portant sur trois mois, 97 percent des logiciels malveillants inconnus transitant par FTP passaient par des ports non-standard.

Solution : L'utilisation sécurisée consiste à autoriser les applications et à les analyser pour détecter la présence éventuelle de menaces. Ces applications peuvent communiquer par le biais d'une combinaison de protocoles. SharePoint, par exemple, utilise les protocoles CIFS, HTTP et HTTPS, et requiert une stratégie de pare-feu bien plus sophistiquée qu'un « simple blocage de l'application ». La première étape consiste à identifier l'application (indépendamment du port ou du chiffrement). Il est ensuite nécessaire de déterminer les fonctions à autoriser ou à bloquer, puis d'analyser tous les composants pour détecter d'éventuelles menaces : vulnérabilités, virus, logiciels malveillants et espions, voire données confidentielles, juridiques ou sensibles.

7

Votre prochain pare-feu doit offrir la même visibilité et les mêmes outils de contrôle pour tous les utilisateurs, indépendant de leur emplacement ou de leur équipement.

Problématique : Les utilisateurs sont de moins en moins cantonnés aux quatre murs de l'entreprise et accèdent souvent au réseau de l'entreprise par le biais de téléphones intelligents ou de tablettes. Autrefois l'apanage des collaborateurs itinérants, le travail à distance concerne désormais une part importante du personnel. Qu'ils se trouvent dans un café, à leur domicile ou sur un site client, les utilisateurs s'attendent à pouvoir se connecter à leurs applications par WiFi, 3G et 4G ou tout autre moyen à leur disposition. Quel que soit le lieu où se trouve l'utilisateur, ou l'application qu'il utilise, les mêmes principes de contrôle du pare-feu doivent s'appliquer. Si votre prochain pare-feu permet la visibilité et le contrôle des applications sur le trafic interne mais pas sur le trafic externe de l'entreprise, il laissera passer des flux à hauts risques.

Solution : Rien de plus simple sur le plan conceptuel : votre prochain pare-feu doit proposer une visibilité totale et un contrôle cohérent sur le trafic et ce, quel que soit l'endroit où se trouve l'utilisateur. Loin de nous l'idée d'imposer aux entreprises une stratégie rigoureusement identique dans les deux cas. Certaines sociétés laisseront leurs collaborateurs utiliser Skype lors de leurs déplacements, mais pas dans l'enceinte de l'entreprise. D'autres pourront très bien interdire à leurs utilisateurs de télécharger des documents depuis salesforce.com si le chiffrement du disque dur n'est pas activé. Votre prochain pare-feu doit être capable de tout cela sans latence pour l'utilisateur final, sans sollicitation abusive ou inutile de l'administrateur et sans coût supplémentaire démesuré pour l'entreprise.

8

Votre prochain pare-feu doit simplifier la sécurité réseau tout en intégrant le contrôle des applications.

Problématique : De nombreuses entreprises s'efforcent de ne pas intégrer de flux d'informations, politiques et tâches administratives supplémentaires à leurs processus de sécurité dans la mesure où les administrateurs sont déjà totalement surchargés. Si votre équipe de sécurité est déjà débordée, comment imaginer que l'ajout d'équipements et la gestion des nouvelles interfaces (sans oublier les informations et politiques associées) l'aideront à réduire les tâches d'administration et à écourter les délais de réponse en cas d'incident ? Plus la stratégie est distribuée, plus elle est difficile à gérer (exemple : le pare-feu basé sur les ports autorise le trafic par le port 80, le système IPS détecte/bloque les menaces et les applications et la passerelle Web sécurisée

applique le filtrage des URL). Quelle politique les administrateurs doivent-ils suivre pour sécuriser l'utilisation de WebEx ? Comment identifient-ils et gèrent-ils les conflits de politiques entre ces différents équipements ? Étant donné qu'un pare-feu traditionnel basé sur les ports comporte des politiques de base incluant des milliers de règles, l'ajout de milliers de signatures d'applications à des dizaines de milliers de ports ne fera qu'accroître la complexité.

Solution : Dans la mesure où les applications, les utilisateurs et le contenu sont essentiels à votre activité, votre prochain pare-feu doit permettre de mettre en œuvre des politiques qui n'entravent en rien vos initiatives. En partageant le contexte entre les applications, les utilisateurs et le contenu à tous les niveaux (visibilité, contrôle de politiques, journalisation et création de rapports), vous simplifierez considérablement votre infrastructure de sécurité. Si en plus du filtrage des ports et des adresses IP au niveau du pare-feu, vous appliquez des politiques distinctes pour contrôler les applications et mettez en œuvre un système de prévention des intrusions et un logiciel luttant contre les programmes malveillants, vous compliquerez inutilement la gestion des stratégies et finirez par freiner le développement de vos activités.

9

Votre prochain pare-feu doit fournir le même débit et les mêmes performances une fois le contrôle des applications activé.

Problématique : De nombreuses entreprises se refusent à choisir entre performances et sécurité. L'activation de fonctions de sécurité sur le pare-feu sous-entend trop souvent une baisse significative du débit et des performances. Si votre pare-feu nouvelle génération est bien conçu, vous n'aurez plus à faire de compromis.

Solution : Là aussi, l'architecture joue un rôle important, mais de façon différente. Associer un pare-feu basé sur les ports à d'autres fonctions de sécurité utilisant des technologies différentes donne lieu à des redondances au niveau des couches réseau, des moteurs d'analyse et des politiques, d'où une baisse des performances. D'un point de vue logiciel, le pare-feu doit dès le début être conçu dans cette optique. Dans la mesure où il est nécessaire d'exécuter sur des volumes de trafic importants et avec une faible latence des tâches exigeant une puissance de calcul importante (identification des applications et prévention des menaces sur tous les ports), la plateforme matérielle de votre prochain pare-feu doit être optimisée pour des tâches spécifiques comme la mise en réseau, la sécurité et l'analyse du contenu.

10

Votre prochain pare-feu doit assurer les mêmes fonctions qu'il s'agisse d'un environnement physique ou virtuel.

Problématique : La croissance exponentielle de la virtualisation et de l'informatique dématérialisée fait naître de nouveaux défis de sécurité que les pare-feu traditionnels ont du mal à relever du fait de l'hétérogénéité des fonctionnalités, de la diversité de l'administration et du manque de points d'intégration dans l'environnement de virtualisation. Pour protéger le trafic à destination et en provenance du data center et au sein des environnements virtualisés, votre prochain pare-feu doit assurer exactement les mêmes fonctions qu'il s'agisse d'un environnement physique ou virtuel.

Solution : L'ajout et le retrait dynamiques des applications au sein d'un data center virtualisé rendent plus difficiles l'identification et le contrôle des applications à l'aide des ports et des adresses IP. Outre les fonctionnalités déjà décrites dans les 10 principales fonctions que doit posséder votre prochain pare-feu pour les plateformes physiques et virtualisées, votre prochain pare-feu doit parfaitement s'intégrer à l'environnement de virtualisation afin de simplifier la création des stratégies d'utilisation des applications à mesure de l'ajout et du retrait des machines virtuelles et des applications. C'est la seule façon de donner aux architectures de data center la flexibilité opérationnelle nécessaire à leur évolution tout en gérant les risques et la conformité.

Les Pare-feu Doivent Sécuriser les Applications pour Renforcer le Pouvoir de l'entreprise

Les utilisateurs adoptent de nouvelles applications et technologies pour s'acquitter au mieux de leurs tâches, mais négligent souvent les risques métier et de sécurité induits. En bloquant ces applications, il arrive que les équipes chargées de la sécurité freinent le développement des activités de l'entreprise.

Les applications aident les collaborateurs à accomplir leur travail et à conserver leur efficacité face à des enjeux personnels et professionnels. Il va donc de soi que l'utilisation sécurisée des applications devient une priorité. Pour sécuriser les applications et les technologies, et donc toutes les activités qui en découlent, les administrateurs chargés de la sécurité du réseau doivent mettre en place les politiques d'utilisation appropriées, mais aussi les contrôles capables de les faire respecter.

Dans la section 10 principales fonctions que doit posséder votre prochain pare-feu, nous avons passé en revue les fonctionnalités essentielles qui aideront les entreprises à sécuriser l'utilisation des applications et, au final, l'ensemble de leurs activités. La prochaine étape consiste à passer à l'action : sélection d'un fournisseur via la procédure d'appel d'offres, évaluation formelle des différentes solutions et, pour finir, achat et déploiement d'un pare-feu nouvelle génération.

À Propos de Palo Alto Networks

Palo Alto Networks est le spécialiste de la sécurité réseau nouvelle génération. Grâce à sa plateforme innovante, les entreprises, prestataires de services et organismes publics peuvent sécuriser leurs réseaux en déployant en toute sécurité des applications de plus en plus nombreuses et de plus en plus complexes et en se protégeant des cybermenaces. La plateforme Palo Alto Networks repose essentiellement sur son pare-feu nouvelle génération qui fournit une visibilité et un contrôle des applications, des utilisateurs et du contenu via son architecture matérielle et logicielle propriétaire. Les produits et services Palo Alto Networks répondent à une grande variété de spécifications en matière de sécurité des réseaux, que ce soit au niveau du data center ou du périmètre du réseau, mais aussi à l'échelle de l'entreprise distribuée qui comprend diverses succursales et un nombre croissant d'appareils mobiles. Les produits Palo Alto Networks sont utilisés par plus de 13 500 clients à travers une centaine de pays. Pour plus d'informations, consultez le site **www.paloaltonetworks.com**.

paloalto NETWORKS®

the network security company™

4301 Great America Parkway
Santa Clara, CA 95054

Accueil: +1.408.753.4000
Ventes: +1.866.320.4788
Assistance: +1.866.898.9087

www.paloaltonetworks.com