GUIDE D'ACHAT DES PARE-FEU

Le guide de référence pour l'évaluation des pare-feu de réseau d'entreprise.

paloalto NETWORKS®

the network security company™

Le changement favorise l'innovation

Malgré des fonctionnalités plus évoluées et un débit sans précédent, l'efficacité des pare-feu ne cesse d'être remise en question. Les menaces évoluent rapidement et le blocage traditionnel des ports et des adresses IP ne suffit plus à les arrêter.

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 toujours 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 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. Les applications ont évolué d'une telle façon que le pare-feu, qui est au cœur de votre infrastructure de sécurité, peine à fournir le niveau de contrôle nécessaire pour protéger vos actifs 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 cybermenaces 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 que compliquer davantage les défis posés. 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 % des applications transitant par votre réseau et 20 % de la bande passante[1]. 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 autres). Cibles privilégiées des cyberdélinquants, 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 système IPS avec des techniques d'évasion classiques.

- **Applications système et personnalisées :** il s'agit des applications d'infrastructure de base comme SSL, SSH et DNS, des applications personnalisées développées en interne ou d'applications totalement inconnues. Ces applications inconnues sont généralement 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).

[1] Palo Alto Networks Application Usage and Threat Report, Janvier 2013

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.

Le 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.

Une révolution et non une évolution

Compte tenu du volume du trafic, du nombre toujours croissant d'applications et du manque de tolérance à l'égard des baisses de performance, il est impensable de continuer à ajouter des périphériques et de nouveaux « modules » logiciels pour analyser le trafic.

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 cyberattaques 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.

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.**

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 cyberattaques 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, antivirus 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.

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. **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**

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 cyberpirates 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 cyberpirates 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, 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 % des applications sont chiffrées en SSL, sous quelque forme et de quelque façon que ce soit, sur les réseaux d'entreprise[2]. 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.

[2] Palo Alto Networks Application Usage and Threat Report, Janvier 2013

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.

Utilisation sécurisée des applications
Pour sécuriser les applications et les technologies, et donc toutes les activités qui en découlent, les administrateurs de la sécurité réseau doivent mettre en place les stratégies d'utilisation appropriées, mais aussi les contrôles capables de les faire respecter.

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 cyberpirates sont souvent obligés de modifier un protocole pour exploiter une application cible. Par exemple, il est possible que pour attaquer un serveur Web, un cyberpirate 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.net, 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 cyberpirate a tout loisir d'utiliser la combinaison de port et protocole de son choix. Selon une récente analyse portant sur trois mois, 97 % 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 1*0 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.

Développement de vos activités
Dans le monde toujours connecté actuel, le contrôle des applications ne s'arrête pas au simple principe de blocage/autorisation. Il est question de sécuriser l'utilisation des applications pour renforcer le pouvoir de l'entreprise.

Appel d'offres pour sélectionner un pare-feu nouvelle génération

Généralement, lorsque les entreprises cherchent à sélectionner des pare-feu, des systèmes IPS ou d'autres composants stratégiques de l'infrastructure de sécurité, elles rédigent un appel d'offres pour décrire en détail leurs besoins. Selon le Gartner Magic Quadrant des pare-feu d'entreprise, « *du fait de l'évolution des menaces et des processus métier et informatiques, les responsables de la sécurité du réseau vont se tourner vers les pare-feu nouvelle génération au moment de renouveler leurs pare-feu et systèmes IPS* ». Alors que de nouvelles opportunités de déploiement se présentent, les entreprises doivent étendre les critères de sélection de leur appel d'offres de façon à inclure la visibilité et le contrôle des applications, avantages offerts par les solutions nouvelle génération. La section précédente passait en revue les 10 principales fonctions que doit posséder votre prochain pare-feu. La présente section vous aidera à trouver les outils permettant d'identifier et de sélectionner un pare-feu nouvelle génération.

Considérations sur l'architecture du pare-feu et les modèles de contrôle

De nombreux éléments sont à prendre en compte lors de l'évaluation d'un fournisseur pour savoir si son pare-feu a la capacité d'offrir la visibilité et le contrôle des applications requis. L'architecture du pare-feu, et plus précisément, le moteur de classification du trafic permet de savoir dans quelle mesure il est apte à identifier et contrôler les applications sans se limiter aux ports et aux protocoles. Comme nous l'avons vu auparavant, la première chose qu'un nouveau pare-feu, indépendamment de son type, doit impérativement faire est de déterminer avec précision la nature du trafic, puis se baser sur ce résultat pour élaborer l'ensemble des politiques de sécurité.

Dans ce modèle, le pare-feu adopte la stratégie du contrôle positif traditionnel (tout bloquer à l'exception de ce que vous autorisez explicitement). Un modèle positif permet de contrôler et d'utiliser les applications, ce qui est un élément stratégique important dans le monde toujours connecté où évoluent aujourd'hui les entreprises. Si la recherche des applications est confiée à des éléments annexes tels qu'un système IPS, cela signifie qu'un modèle de contrôle négatif est appliqué (tout autoriser à l'exception de ce qui est expressément refusé par le système IPS). Un modèle négatif sous-entend que vous pouvez uniquement bloquer les applications. Pour bien percevoir ces différences, prenons un exemple. Dans le premier cas, il s'agit d'allumer toutes les lampes d'une pièce pour que tout s'éclaire et devienne visible (contrôle positif). Dans le second, il s'agit d'utiliser une lampe torche pour s'intéresser uniquement à la petite zone sur laquelle vous dirigez la torche (contrôle négatif). Si cette méthode permet d'identifier et de bloquer les événements « néfastes », elle n'est pas pleinement efficace car elle est conçue pour examiner seulement une partie du trafic afin de préserver les performances et ne peut pas couvrir l'ensemble des cyberattaques et des applications.

Visibilité et contrôle des applications

L'appel d'offres doit préciser comment l'infrastructure de pare-feu identifie et contrôle les applications (professionnelles, personnelles ou autres) et les protocoles, quels que soient le port, le chiffrement SSL ou les autres techniques d'évasion utilisées. Prenez en compte les questions et affirmations suivantes lors de la rédaction d'un appel d'offres pour des pare-feu nouvelle génération.

- De nombreuses applications peuvent échapper à la détection en utilisant des ports non standard, en changeant dynamiquement de port ou en étant configurées pour s'exécuter sur un port différent.
  - Les mécanismes d'identification des applications font-ils partie de la classification de base du trafic dans le pare-feu (sont-ils activés par défaut) ?
  - Les mécanismes d'identification des applications dépendent-ils du port standard de l'application ?
  - Les signatures peuvent-elles être appliquées à tous les ports et ce processus est-il configuré automatiquement ou manuellement ?
- Lorsque le trafic atteint le dispositif, est-il classifié tout d'abord en fonction du port (il s'agit du port 80, donc d'un trafic HTTP) ou en fonction de l'application (il s'agit de l'application Gmail) ?
- Décrivez en détail la façon dont le pare-feu identifie précisément les applications.
  - Quels sont, outre les signatures, les mécanismes utilisés pour identifier le trafic ?
  - Décrivez la façon dont le décodeur d'applications et de protocoles est utilisé.
  - De quelle façon le déchiffrement et le contrôle SSL et SSH sont-ils mis en œuvre ?
  - Les mécanismes de classification du trafic sont-ils appliqués uniformément sur tous les ports ?
- Quels sont les mécanismes utilisés pour détecter des applications de contournement comme UltraSurf ou une connexion peer to peer chiffrée ?
- L'identification des applications a-t-elle vraiment lieu dans le pare-feu ou est-elle assurée dans un deuxième temps, après la classification basée sur les ports ?
  - Quels sont les trois principaux avantages de l'approche architecturale adoptée ?
- Un suivi de l'état des applications a-t-il été mis en place ? Si c'est le cas, comment est-il utilisé pour assurer un contrôle cohérent d'une application et de toutes les fonctions secondaires qui s'y rapportent ?
  - Donnez trois exemples de la façon dont l'état des applications intervient dans le contrôle stratégique.
- L'identification de l'application est-elle au cœur de la politique de sécurité du pare-feu ou le contrôle applicatif est-il traité comme un élément secondaire de la stratégie ?
- À quelle fréquence la base de données des applications est-elle mise à jour ? S'agit-il d'une mise à jour dynamique ou d'une mise à niveau au moment du redémarrage du système ?
- Dans les environnements virtualisés, décrivez la façon dont le trafic est identifié sur la machine virtuelle (est/ouest, nord/sud).
  - Décrivez les points d'intégration au sein de l'environnement virtualisé.
  - Décrivez les étapes inhérentes à la création des stratégies de sécurité pour les machines virtuelles nouvellement créées.
  - Décrivez les fonctionnalités disponibles pour suivre le déplacement, l'ajout et la modification des machines virtuelles.
  - Décrivez les fonctionnalités disponibles pour l'intégration avec les systèmes d'automatisation et d'orchestration.

Contrôle des applications de contournement, de SSL et de SSH

De nombreuses applications peuvent être utilisées pour contourner les contrôles de sécurité. Certaines, comme les serveurs proxy externes et les tunnels chiffrés hors VPN, sont conçues uniquement dans ce but. D'autres, comme les outils d'administration à distance des serveurs/postes de travail, sont détournées de leur usage premier et sont utilisées par des non-informaticiens et des non-techniciens pour déjouer les mécanismes de contrôle. Un grand nombre d'applications d'utilisateur final utilisent le protocole SSL comme dispositif de sécurité. Cependant, l'utilisation de ce protocole peut devenir problématique lorsqu'il sert à masquer les menaces entrantes ou le transfert de données sortantes. Actuellement, environ 26 % des applications transitant par votre réseau utilisent le protocole SSL[3] d'une manière ou d'une autre. Il est essentiel de savoir si les différents éditeurs de pare-feu nouvelle génération sont en mesure de traiter cette catégorie d'applications. Prenez en compte les questions et affirmations suivantes lors de la rédaction d'un appel d'offres pour des pare-feu nouvelle génération.

- Décrivez le processus permettant d'identifier les applications chiffrées en SSL sur tous les ports, y compris les ports non standard.
- Quels sont les contrôles stratégiques en place permettant de déchiffrer, inspecter et contrôler de manière sélective des applications utilisant le protocole SSL ?
- L'identification, le chiffrement et l'inspection bidirectionnels SSL sont-ils pris en charge ?
- Le déchiffrement SSL est-il assuré en standard ou suppose-t-il un coût supplémentaire ? Un équipement dédié est-il requis ?
- SSH est un outil qu'utilisent fréquemment les informaticiens, les équipes de support et les techniciens pour accéder aux appareils distants.
  - Le contrôle SSH est-il assuré ? Si oui, précisez le niveau de contrôle.
- Quels sont les mécanismes utilisés pour détecter des applications de contournement comme UltraSurf ou Tor ?
- Décrivez la façon dont le produit peut automatiquement identifier une technique de contournement passant par un port non standard.

[3] Palo Alto Networks Application Usage and Threat Report, Janvier 2013

Utilisation des applications basée sur des règles

Dans le monde toujours connecté actuel, le contrôle des applications ne s'arrête pas au simple principe de blocage/autorisation. Il est question de sécuriser l'utilisation des applications pour renforcer le pouvoir de l'entreprise. De nombreuses « plateformes » (Google, Facebook et Microsoft) mettent différentes applications à la disposition de l'utilisateur après la connexion initiale. Il est impératif de déterminer la façon dont l'éditeur de pare-feu surveille l'état de l'application, détecte les changements et classifie le changement d'état. Prenez en compte les questions et affirmations suivantes lors de la rédaction d'un appel d'offres pour des pare-feu nouvelle génération.

- La classification du trafic basé sur le contrôle de l'état est-elle effectuée séparément, avant l'identification des applications ? Si tel est le cas, décrivez la façon dont, une fois l'application identifiée, les changements d'état sont contrôlés, suivis et utilisés au sein de la stratégie.
- Décrivez la façon dont la hiérarchie de la base de données des applications (plate, arborescente ou autre) expose les fonctions au sein de l'application parente afin de faciliter la mise en place de politiques plus précises.
- Décrivez les niveaux de contrôle qu'il est possible d'exercer sur des applications individuelles et leurs fonctions respectives :
  - autorisation ;
  - autorisation basée sur l'application, la fonction de l'application, la catégorie, la sous-catégorie, la technologie ou le facteur de risque ;
  - autorisation basée sur la planification, l'utilisateur, le groupe, le port ;
  - autorisation et détection des virus, des vulnérabilités des applications, des logiciels espions et des téléchargements intempestifs ;
  - autorisation et mise en forme/application de contrôles de qualité de service ;
  - refus.

- Des contrôles basés sur les ports peuvent-ils être mis en œuvre pour toutes les applications de la base des données de façon à ce qu'un administrateur puisse déterminer, par le biais d'une politique, la relation entre l'application et le port ? Par exemple :
  - Obliger les développeurs de bases de données Oracle à passer par un port ou une plage de ports spécifique.
  - S'assurer que l'équipe informatique est la seule à avoir le droit d'utiliser SSH et RDP.
  - Détecter et bloquer les logiciels malveillants au sein de l'application, même s'ils passent par un port non standard.
- Répertoriez tous les annuaires d'identités de l'entreprise pris en charge pour les contrôles basés sur les utilisateurs.
- Une API est-elle disponible pour une intégration identité-infrastructure personnalisée ou non standard ?
- Décrivez la façon dont les contrôles basés sur les politiques sont mis en œuvre par les utilisateurs et les groupes dans des environnements de services de terminal.
- Décrivez les différences des options d'utilisation des applications selon qu'il s'agit d'un environnement physique ou virtuel.

Gestion systématique des applications inconnues

Sur chaque réseau circule un certain nombre d'applications inconnues. Les applications personnalisées et développées en interne en sont l'exemple le plus manifeste, mais il peut également s'agir d'applications commerciales non encore identifiées ou, pire, de code malveillant. Au cours de l'appel d'offres et de l'évaluation, vous devez obtenir une description précise de la façon dont la solution vous permettra de gérer de manière systématique le trafic inconnu, qui représente un risque métier et de sécurité élevé. Prenez en compte les questions et affirmations suivantes lors de la rédaction d'un appel d'offres pour des pare-feu nouvelle génération.

- Fournissez une description détaillée des mécanismes d'identification et d'analyse du trafic inconnu.
- Les outils d'analyse sont-ils fournis en standard ou sous forme de solutions complémentaires ?
- Le cas échéant, quelles sont les actions possibles face à un trafic inconnu (autorisation, refus, inspection, mise en forme ou autre) ?
- Décrivez les pratiques recommandées pour la gestion du trafic d'applications inconnues.
  - Ce trafic peut-il être contrôlé par le biais de politiques, de la même manière que les applications officiellement prises en charge (autorisation, refus, inspection, mise en forme, contrôle par utilisateur, zone ou autre) ?
  - Est-il possible de « renommer » le trafic interne ?
  - Est-il possible de créer une signature pour une application personnalisée ?
- Quelle est la procédure à suivre pour soumettre des requêtes visant à créer ou à mettre à jour des signatures ?
- Une fois l'application soumise, quel est le délai prévu en termes de qualité de service ?
- Quels sont les mécanismes proposés pour savoir si le trafic inconnu est du code malveillant ?

Prévention des menaces

Les applications dans lesquelles se dissimulent les menaces sont de plus en plus diversifiées. Elles peuvent servir de vecteur d'attaque ou d'infection ou d'organisme de commande/contrôle des équipements infectés. C'est pourquoi, les analystes recommandent constamment aux entreprises de combiner les technologies IPS et de prévention de menaces traditionnelles au sein du pare-feu nouvelle génération. Prenez en compte les questions et affirmations suivantes lors de la rédaction d'un appel d'offres pour des pare-feu nouvelle génération.

- Décrivez tous les mécanismes de prévention des menaces en place (IPS, antivirus, anti-logiciels espions, filtrage des URL, filtrage des données et autre).
- Quels sont les types de licence proposés pour les mécanismes de prévention des menaces ?
- Décrivez les mécanismes de prévention des menaces développés en interne ou acquis via un fournisseur ou un service tiers.
- Comment évitez-vous les menaces embarquées dans les applications transitant par des ports non standard ?
- Les informations résultant de l'identification des applications sont-elles intégrées aux technologies de prévention des menaces ou partagées par celles-ci. Si oui, précisez le niveau d'intégration.
- Décrivez quels sont les outils de prévention des menaces (IPS, antivirus ou autre) basés sur les ports plutôt que sur les applications.
- Le moteur de prévention des menaces est-il en mesure d'analyser le contenu de fichiers compressés comme ZIP ou GZIP ?
- Le moteur de prévention des menaces peut-il analyser un contenu chiffré en SSL ?
- Décrivez la façon dont le pare-feu détecte et lutte contre les logiciels malveillants personnalisés ou polymorphes.
    - Quels sont les mécanismes utilisés pour bloquer les logiciels malveillants ?
- Décrivez le processus de recherche et de développement de préventions des menaces.

Sécurisation des utilisateurs distants

De nos jours, les utilisateurs d'un réseau moderne s'attendent à pouvoir se connecter et travailler n'importe où, bien au-delà du périmètre physique du réseau d'entreprise. Ces utilisateurs doivent rester protégés même lorsqu'ils utilisent un ordinateur, un téléphone intelligent ou une tablette hors du périmètre du réseau. Cette section a pour but d'étudier les différents moyens de sécuriser ces utilisateurs distants et de voir en quoi cette protection change lorsque l'utilisateur travaille à l'intérieur ou à l'extérieur du réseau physique. Prenez en compte les questions et affirmations suivantes lors de la rédaction d'un appel d'offres pour des pare-feu nouvelle génération.

- Décrivez en détail toutes les options disponibles, y compris les composants nécessaires, pour sécuriser les utilisateurs distants.
- S'il existe un composant client, comment celui-ci est-il distribué ?
- Décrivez les exigences en termes de dimensionnement. Combien d'utilisateurs peuvent-ils être pris en charge simultanément ?
- L'ensemble des fonctions de sécurité des utilisateurs distants est-il transparent au client ?
- Décrivez comment se fait le contrôle des stratégies pour les utilisateurs distants (stratégie du pare-feu, stratégie/équipement distincts ou autre).
- Répertoriez les fonctionnalités et les protections fournies par le biais des outils distants (SSL, contrôle des applications, IPS ou autre).
- Votre pare-feu permet-il aux utilisateurs de rester connectés où qu'ils se trouvent et donc d'assurer une application cohérente des politiques ?
- Comment traitez-vous les utilisateurs d'appareils mobiles ? Pouvez-vous assurer la cohérence des politiques, que les utilisateurs soient sur des réseaux externes ou des réseaux sans fil internes ?
- Le pare-feu est-il en mesure de prendre en charge les problèmes liés à l'utilisation d'appareils personnels et de sécuriser à la fois les équipements professionnels et personnels (ordinateurs portables, téléphones intelligents et tablettes) ?

Administration

L'administration joue un rôle crucial dans la mise en œuvre d'une sécurité réseau efficace. Lors de l'achat de votre prochain pare-feu, vous ne devez pas perdre de vue la nécessité de simplifier au maximum l'administration de la sécurité en intégrant la visibilité et le contrôle des applications. Prenez en compte les questions et affirmations suivantes lors de la rédaction d'un appel d'offres pour des pare-feu nouvelle génération.

- Un serveur ou un dispositif distinct est-il nécessaire pour assurer l'administration des équipements ?
- Décrivez toutes les options d'administration prises en charge : interface à ligne de commande ? navigateur Internet ? client logiciel ? serveur centralisé ?
  - Pour chacune des options d'administration proposées, évaluez l'effort à fournir pour passer d'une méthode d'administration à une autre.
- Décrivez l'architecture d'administration centralisée et les options de déploiement.
- De quels outils de visibilité disposez-vous, outre le visualiseur de journaux et les rapports, pour avoir une vue d'ensemble complète des applications, des utilisateurs et du contenu traversant le réseau ?
  - Les outils de visibilité sont-ils inclus dans l'offre de base ou font-il l'objet de coûts/licences supplémentaires ?
  - Les outils de visibilité sont-ils déployés en même temps que tous les autres ou s'agit-il d'un équipement/d'un logiciel à part ?
- Décrivez en détail les efforts à fournir et les étapes requises pour commencer à « avoir une vue globale du trafic des applications » sur le réseau.
- Est-il possible d'activer le contrôle stratégique des applications et du pare-feu et les fonctions de prévention des menaces par le biais d'une seule politique dans l'éditeur de politiques du pare-feu ?
- Décrivez les fonctions de journalisation et de génération de rapports. Sont-elles intégrées ? Si oui, dans quelle mesure l'activation de la journalisation risque-t-elle de nuire aux performances ?
  - L'analyse complète des journaux est-elle incluse dans l'offre de base ou demande-t-elle un coût supplémentaire/une autre licence/un équipement ou logiciel distinct ?
- Est-il possible de personnaliser les outils de génération de rapports pour mieux comprendre la façon dont le réseau est utilisé et identifier des modifications dans son utilisation ?
  - Ces outils impliquent-ils un coût supplémentaire/une autre licence/un équipement ou logiciel distinct ?
- Décrivez la façon dont l'accès à l'administration est assuré lorsque l'équipement subit une charge de trafic importante.
- Décrivez les relations existant entre l'administration d'un seul équipement et l'administration centralisée de plusieurs équipements.
- Expliquez en quoi diffère l'administration des instances physiques et virtuelles.

Performances

Dans le monde de l'entreprise, les performances constituent un élément essentiel du déploiement de la sécurité. Le contrôle des applications requiert un examen plus rigoureux du trafic que le filtrage des ports et consomme donc beaucoup plus de ressources. Lorsque la prévention des menaces et le contrôle des stratégies viennent s'ajouter à ce même trafic, la charge pesant sur le pare-feu s'alourdit encore. Il est donc indispensable d'étudier les performances du réseau lorsque toutes les fonctions de sécurité sont activées et d'analyser un échantillon diversifié du trafic réel. Prenez en compte les questions et affirmations suivantes lors de la rédaction d'un appel d'offres pour des pare-feu nouvelle génération.

- Vérifiez que le produit est un logiciel seul, un serveur OEM ou une solution propriétaire.
- Étudiez l'architecture matérielle afin de voir si la puissance de traitement est adaptée à une classification et une inspection continues du trafic au niveau des applications.
- Décrivez la combinaison de trafic utilisée pour générer les mesures de performances publiées pour :
  - Pare-feu + journalisation
  - Pare-feu + contrôle des applications
  - Pare-feu + contrôle des applications + prévention des menaces
- À combien est évalué le débit pour :
  - Pare-feu + journalisation
  - Pare-feu + contrôle des applications
  - Pare-feu + contrôle des applications + prévention des menaces

Autres considérations à prendre en compte dans l'appel d'offres

De toute évidence, chaque entreprise aura d'autres exigences à respecter en plus des éléments répertoriés dans ce document. Citons entre autres : la rentabilité de l'entreprise, les références des clients, la facilité de déploiement, la prise en charge du réseau et de l'acheminement. Dans le cadre d'un appel d'offres, il est recommandé de procéder de façon très systématique afin d'inciter les fournisseurs à démontrer que leurs offres répondent bien aux attentes formulées.

Performances
Il est donc indispensable d'étudier les performances du réseau lorsque toutes les fonctions de sécurité sont activées et d'analyser un échantillon diversifié du trafic réel.

Évaluation des pare-feu nouvelle génération à l'aide d'un test formel

Dès qu'un seul ou un nombre restreint de fournisseurs ont été retenus à la suite de l'appel d'offres, il vous reste à évaluer physiquement le pare-feu à l'aide de modèles de trafic, d'objets et de politiques représentatifs de l'environnement de l'entreprise. Cette section fournit quelques recommandations sur la façon d'évaluer systématiquement un pare-feu nouvelle génération. Cette évaluation vous donnera la possibilité de voir comment, en situation réelle, un éditeur de pare-feu est à même de répondre à vos principales attentes. Notez que les tests suggérés ci-dessous ne font que survoler les fonctionnalités requises d'un pare-feu nouvelle génération et servent de base à l'élaboration d'une étude beaucoup plus détaillée.

Visibilité et contrôle des applications

Cette section a trois objectifs. Premièrement, vérifier que la première tâche réalisée par le dispositif testé est bien la classification du trafic selon l'identité de l'application, et non le port réseau. Deuxièmement, vérifier que le dispositif testé identifie les applications indépendamment des techniques d'évasion telles que saut de port en port, utilisation de ports non standard ou toute autre méthode de contournement censée faciliter l'accessibilité. Troisièmement, vérifier que l'identité de l'application est bien à la base de la stratégie de pare-feu et qu'elle n'est pas simplement un élément d'une stratégie auxiliaire.

Identification des applications

- Assurez-vous que le pare-feu peut identifier différentes applications. Pour exécuter ce test, l'idéal est de déployer le dispositif testé en mode « TAP » ou transparent sur le réseau cible.
- Vérifiez, au moyen de graphiques, de synthèses et d'études détaillées, que le dispositif testé identifie correctement le trafic des applications.
  - Évaluez les contraintes administratives associées à cette tâche.
- Évaluez les étapes à suivre pour activer l'identification des applications. Combien de temps faut-il à un utilisateur pour élaborer une stratégie et commencer à « voir » le trafic des applications ? Des mesures supplémentaires doivent-elles être prises pour rendre visibles les applications qui changent de port continuellement ou utilisent des ports non standard ?

Identification des applications qui changent dynamiquement de port ou passent par des ports non standard

- Vérifiez que le pare-feu est en mesure d'identifier et de contrôler les applications transitant par des ports autres que le port par défaut desdites applications. Par exemple, SSH sur le port 80 et telnet sur le port 25.
- Assurez-vous que le pare-feu peut identifier les applications changeant dynamiquement de port à l'aide d'une application connue pour procéder de la sorte comme Skype, AIM ou l'une des nombreuses applications peer to peer.

Identité des applications : fondement de la stratégie de sécurité du pare-feu

- Assurez-vous que, lors de l'élaboration de la stratégie du pare-feu, c'est bien l'identité de l'application et non le port qui est au cœur de la stratégie.
  - La stratégie de contrôle des applications a-t-elle tout d'abord besoin d'une règle axée sur les ports ?
  - L'élément chargé du contrôle applicatif est-il un éditeur de politiques partiellement ou totalement distinct ?
- Créez une politique visant à autoriser certaines applications et à en bloquer d'autres, puis vérifiez que les applications sont bien contrôlées comme prévu.
- Une politique fondée sur les applications respecte-t-elle le principe « refuser tout le reste » sur lequel repose un pare-feu ?

Identification et contrôle des outils de contournement

- Assurez-vous que le dispositif testé peut identifier et contrôler les applications utilisées pour déjouer les contrôles de sécurité. Il s'agit notamment des serveurs proxy externes (PHproxy, Kproxy), des outils d'assistance à distance (RDP, LogMeIn!, TeamViewer, GoToMyPC) et des tunnels chiffrés hors VPN (Tor, Hamachi ou UltraSurf).
- Assurez-vous que chaque moyen de contournement est correctement identifié pendant le test.
- Vérifiez qu'il est possible de bloquer toutes les solutions de contournement, même lorsqu'elles passent par un port non standard.

Identification et contrôle des applications utilisant SSL ou SSH

Le nombre d'applications utilisant, pour quelque raison que ce soit, le chiffrement SSL et SSH ne cesse d'augmenter. Vous devez donc évaluer la capacité du pare-feu à identifier et à contrôler ce type d'application.

- Vérifiez que le dispositif testé peut identifier et déchiffrer les applications connues pour utiliser le chiffrement SSL.
- Assurez-vous que le dispositif testé peut identifier et déchiffrer les applications, et qu'il peut ensuite appliquer une stratégie de sécurité à l'application déchiffrée.
- Validez le fait que, si l'application déchiffrée est « autorisée », elle sera de nouveau chiffrée avant d'être transmise.
- Assurez-vous qu'il est possible de procéder au déchiffrement et à l'inspection des flux SSL entrants et sortants.
- Vérifiez que les flux SSH sont correctement identifiés, indépendamment du port.
- Assurez-vous que le contrôle SSH établit la distinction entre la redirection de ports (locaux, distants ou X11) et l'utilisation native (SCP, SFTP ou accès à l'interprétateur).

Identification et contrôle des applications partageant la même connexion

Déterminez si les mécanismes de classification des applications scrutent en permanence l'état des applications, à la recherche de changements. Plus important encore, vérifiez que le changement d'état est correctement classifié. De nombreuses « plateformes » (comme Google, Facebook et Microsoft) activent différentes applications dès que l'utilisateur se connecte. Le suivi des changements d'état des applications est un rôle essentiel d'un pare-feu nouvelle génération.

- L'utilisation d'une application telle que WebEx ou SharePoint permet de confirmer que le dispositif testé identifie l'application initiale.
- Sans quitter l'application, passez à une fonction distincte (comme WebEx Desktop Sharing, SharePoint Administration et SharePoint Documents), puis vérifiez que le changement d'état est pris en compte et que la nouvelle application/fonction est correctement identifiée.
- Validez la politique appliquée et l'inspection réalisée sur la fonction de cette application.

Contrôle des fonctions d'une même application

Déterminez la capacité du dispositif testé à identifier et à contrôler des fonctions spécifiques d'une application. Le contrôle au niveau fonctionnel sécurise l'utilisation d'une application, mais permet aussi de prévenir les risques métier et de sécurité qui peuvent y être associés. Le transfert de fichiers est l'exemple le plus courant, mais il peut également s'agir de fonctions administratives, de fonctionnalités VoIP, de publication sur les médias sociaux et d'échange de messages instantanés avec l'application parente.

- Assurez-vous que le dispositif testé fournit une visibilité totale sur toute la hiérarchie d'applications (depuis l'application de base jusqu'aux fonctions complémentaires).
- Vérifiez que le contrôle de la fonction de transfert de fichiers se fait correctement en identifiant et en contrôlant une application qui effectue des transferts de fichiers.
- Assurez-vous que le dispositif testé est capable de bloquer le chargement/téléchargement de fichiers par application et type de fichier. Par exemple, un utilisateur ne doit pas pouvoir transférer un document Word via une application de messagerie Web.

Gestion systématique du trafic inconnu

Bien qu'en faible pourcentage, un trafic inconnu circule toujours sur les réseaux. Vous devez pouvoir évaluer le temps qu'il faut pour identifier la nature du trafic inconnu et prendre la mesure qui s'impose.

- Assurez-vous qu'une visibilité du trafic inconnu est disponible et que les informations suivantes sont fournies :
  - Volume du trafic
  - Utilisateur et/ou adresses IP
  - Port utilisé
  - Contenu associé : fichier, menace ou autre.
- Quel est l'effort à fournir pour étudier le trafic inconnu ?
- Pouvez-vous établir une stratégie de pare-feu (autoriser, bloquer, inspecter et autre) pour le trafic inconnu ?
- Assurez-vous que des options permettent d'identifier et de contrôler plus précisément le trafic applicatif inconnu.
  - Est-il possible de « renommer » le trafic ?
  - L'utilisateur peut-il créer un mécanisme d'identification sur mesure ?
  - Le fournisseur proposera-t-il un mécanisme d'identification personnalisé ? Si oui, dans quel délai ?

Réduction de la surface d'attaque
Pour protéger votre réseau, vous devez simultanément restreindre l'exposition aux menaces et lutter efficacement contre les menaces présentes dans le trafic applicatif autorisé.

Prévention des menaces

Pour protéger votre réseau, vous devez simultanément restreindre l'exposition aux menaces et lutter efficacement contre les menaces connues et inconnues présentes dans le trafic applicatif autorisé. Vous devez déterminer la capacité du dispositif testé à imposer des mesures de sécurité dans un environnement réel pour lutter notamment contre les menaces précédemment inconnues et les menaces embarquées par des applications passant par des ports non standard ou masquées par une compression. Le tout bien sûr sans dégrader les performances de l'entreprise.

- Confirmez la granularité des profils de prévention des menaces. S'agit-il d'un profil global (uniquement) ou est-il possible de définir des profils individuels en fonction du trafic, de la menace, de l'utilisateur ou autre ?
- Vérifiez que les techniques de prévention des menaces (IPS, filtrage des logiciels malveillants et du contenu) sont en permanence appliquées aux applications (et menaces) transitant éventuellement par des ports non standard. Le dispositif testé doit non seulement contrôler les applications sur les ports non standard, mais aussi prévenir et arrêter les menaces transitant par ces mêmes ports.
- Vérifiez que le dispositif testé détecte les logiciels malveillants et les fichiers non approuvés même lorsqu'ils sont compressés (fichiers ZIP ou GZIP).
- Déterminez quel processus permet d'identifier et de bloquer les logiciels malveillants inconnus.
- Vérifiez les performances du dispositif testé lorsque tous les mécanismes de prévention des menaces sont activés afin d'évaluer la mise en place concrète de ces fonctionnalités.

Sécurisation des utilisateurs distants

Commencez par déterminer si le dispositif testé est en mesure de protéger les utilisateurs distants avec la politique de sécurité appliquée en interne. Évaluez ensuite les tâches administratives requises ainsi que la complexité du déploiement.

- Vérifiez que le dispositif testé peut protéger les utilisateurs distants utilisant plusieurs connexions VPN SSL ou une liaison terrestre.
- Confirmez la simplicité du déploiement et de l'administration en créant un groupe d'utilisateurs distants et en déployant une politique test.
- Le dispositif testé peut-il fournir des politiques basées sur le type d'équipement ?
- Le dispositif testé peut-il lutter contre les logiciels malveillants mobiles et les vulnérabilités des systèmes d'exploitation mobiles ?
  Le dispositif testé peut-il assurer le contrôle des applications mobiles ?
- Finalisez cette phase de test en surveillant les utilisateurs distants via le visualiseur de journaux.

Administration

Vous devez également évaluer la complexité du dispositif testé (administration des différents équipements) et la difficulté de la tâche à accomplir (nombre d'étapes, clarté de l'interface et autre).

- Confirmez le mode d'administration du dispositif testé. L'administration d'un élément individuel requiert-elle un équipement ou un serveur distinct ? Le dispositif testé peut-il être géré par le biais d'un navigateur ou nécessite-t-il un « client lourd » ?
- Vérifiez la disponibilité des outils de visualisation qui, en donnant une vue synthétique des applications, menaces et URL, vous aident à mieux connaître votre réseau.
  - Les journaux sont-ils centralisés ou stockés dans des bases de données distinctes pour chaque fonction (pare-feu, contrôle des applications et IPS) ?
  - Évaluez l'effort administratif qu'exige l'analyse des journaux à des fins de visibilité et d'investigation.
- Assurez-vous qu'il est possible d'activer les contrôles stratégiques des applications, les contrôles stratégiques du pare-feu et les fonctions de prévention des menaces à partir du même éditeur de politiques.
  - Une règle de pare-feu fondée sur les ports est-elle créée et appliquée avant le contrôle des applications ?
  - En cas d'utilisation de plusieurs stratégies (pare-feu, contrôle applicatif et IPS), existe-t-il des outils de rapprochement qui permettraient de détecter des lacunes ?

Performances avec les services activés

Le contrôle des applications exige beaucoup plus de ressources que le filtrage traditionnel des ports. Il est donc essentiel de vérifier les performances du dispositif testé lors de l'identification et du contrôle des applications.

- Vérifiez que le dispositif testé est une solution logicielle, un serveur OEM ou une solution propriétaire.
- S'il s'agit d'une solution propriétaire, étudiez l'architecture matérielle pour vérifier que la puissance de traitement répond aux exigences de performance réseau lorsque tous les services sont activés.
- Testez-le ! Évaluez les performances réelles dans un environnement de test en utilisant des modèles de trafic représentatifs de l'environnement réseau cible.

Remarques concernant les environnements physiques et virtuels

Si le déploiement concerne un data center localisé, suivez les étapes de test ci-dessus pour vous assurer que les fonctionnalités du pare-feu sur une plateforme virtuelle sont correctement testées. Pour les environnements virtualisés, d'autres points sont à prendre en compte :

- Quel processus permet de gérer la politique sur des instances de machines virtuelles ? Combien d'étapes ce processus comporte-t-il ?
- Est-il possible de créer les mêmes types de politiques pour les instances physiques et virtuelles ?

- Les fonctionnalités prises en charge sont-elles rigoureusement identiques, qu'il s'agisse d'instances physiques ou virtuelles ?
- Vérifiez que le dispositif testé peut sécuriser tout le trafic circulant entre les machines virtuelles sur le même serveur virtualisé.
- Vérifiez que le dispositif testé peut déployer des politiques pour les applications, les utilisateurs et le contenu sur une même instance virtuelle.
- Vérifiez que le dispositif testé peut continuer à appliquer les politiques même en cas de migration des machines virtuelles hébergées.
- Confirmez et validez l'interaction avec le système d'administration de la plateforme de virtualisation.
- Confirmez et validez l'interaction avec les systèmes d'automatisation et d'orchestration.

Autres points à prendre en compte pour l'évaluation

Le processus d'évaluation et de test des produits de sécurité réseau variera d'une entreprise à une autre et, dans la plupart des cas, sera plus poussé que ce qui est décrit dans ce document. Le test pourra, par exemple, concerner la facilité de déploiement (mode TAP, mode transparent ou autre), la prise en charge du réseau (couche 2, couche 3 ou mode mixte) et la prise en charge de l'acheminement (RIP, OSPF ou BGP). Pour procéder à l'évaluation d'un pare-feu, il est généralement recommandé de sélectionner un ensemble précis de critères et de faire subir la totalité des tests à chacun des dispositifs retenus. Il faut ensuite documenter les résultats en détail pour arriver au choix définitif de la manière la plus systématique possible.

Utilisation sécurisée des applications avec les pare-feu nouvelle génération

Dans le passé, il était impensable d'autoriser un collaborateur à utiliser une application externe ou personnelle à des fins professionnelles. Aujourd'hui, les collaborateurs sont continuellement connectés et veulent profiter des applications les plus récentes, mêlant bien souvent utilisation personnelle et utilisation professionnelle. Pour résumer, bloquer ces applications reviendrait à bloquer le développement des activités de l'entreprise.

Ce guide, *10 principales fonctions que doit posséder votre prochain pare-feu*, démontre que le pare-feu est l'emplacement idéal pour sécuriser l'utilisation des applications et ceci à l'aide des politiques des modèles de contrôle positif traditionnels qui permettent aux administrateurs de définir, selon l'entreprise, les applications à autoriser et à bloquer. Après avoir utilisé les outils décrits dans ce document, vous comprendrez facilement que tenter de sécuriser l'utilisation des applications par le biais d'un modèle de contrôle négatif et d'un élément accessoire de type IPS est totalement irréaliste.

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.

the network security company™

www.paloaltonetworks.com