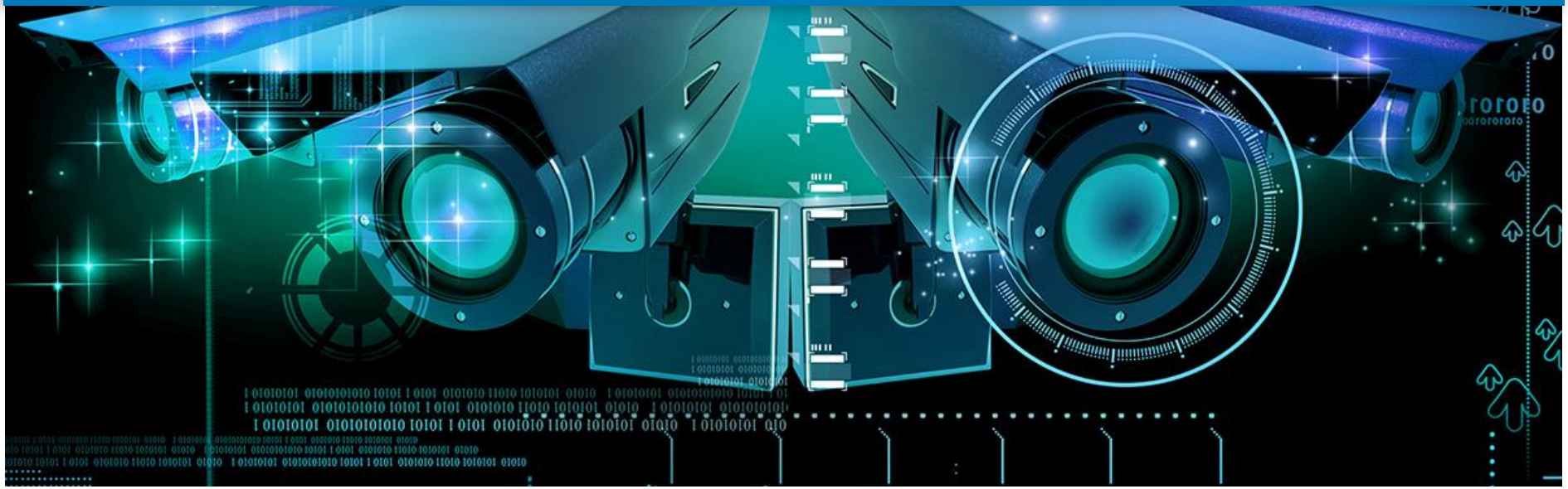

Sécurité du réseau : éléments de réponse sur les menaces avancées

Présentation

L'évolution des menaces ne marque pas la fin du pare-feu, elle appelle à sa modernisation avec des produits de plus en plus complets.

On pense bien sûr aux pare-feux de nouvelle génération, bien connu dans les grandes organisations, mais également aux systèmes de gestion unifiée des menaces.

S'ils s'adressent plus aux PME, ces derniers s'avèrent de plus en plus séduisants, avec un vaste éventail de fonctionnalités, et des performances en forte progression.

Reste à savoir si les efforts en matière seront suffisants face au défi que représente, pour les RSSI, un recours croissant au chiffrement qui rend les flux réseau de plus en plus opaques.

• Valéry Marchive

Pare-feu : Gartner recommande la standardisation sur une marque

Dans une note d'information, Gartner relève que ses clients lui demandent souvent s'il ne serait pas pertinent d'utiliser des pare-feu de plusieurs marques dans leur zone démilitarisée, « ou par couches en périphérie », afin d'assurer plusieurs rangs de défense tout en jouant sur « un chevauchement de capacités au cas où un produit en particulier ne serait plus fiable », du fait, par exemple, de la découverte d'une vulnérabilité.

Las, pour le cabinet, 99 % des brèches au niveau de pare-feu seront, au moins jusqu'en 2020, liées à des défauts de configuration, pas à des vulnérabilités natives. Dès lors, non, pour Gartner, multiplier les pare-feu de marques différentes ne permet d'améliorer significativement sa posture de sécurité.

Surtout, multiplier les marques induit le risque de multiplier les interfaces de configuration et in fine « accroît considérablement les risques de problèmes de gestion et de configuration ».

Du coup, le risque qu'un défaut de configuration soit à l'origine d'une brèche éventuelle augmente.

Et c'est sans compter avec les coûts. Qui dit plusieurs équipementiers dit formation des équipes à plus d'environnements d'administration et d'exploitation, mais aussi « des remises potentiellement moins élevées » ou encore « des frais de gestion supplémentaires ».

Le tout risquant alors de « diminuer le budget disponible pour d'autres technologies de sécurité des réseaux ».

Et justement, Gartner conseille de ne pas compter exclusivement sur des pare-feu, mais d'investir « dans d'autres contrôles de sécurité des réseaux pour détecter et stopper plus efficacement les menaces évoluées ».

Et cela à plus forte raison que « les menaces ont évolué et se sont éloignées des traditionnelles attaques de couche 3 pour remonter désormais vers le haut de la pile, dominant les couches 4 à 7 ».

De quoi rendre de moins en moins optionnelles des systèmes de protection de type prévention des intrusions (IPS), pare-feu pour applications Web (WAF), ou encore bacs à sables (sandbox) pour le filtrage et l'analyse des contenus.

Bien sûr, Gartner relève des cas d'utilisation

exceptionnels et spécifiques justifiant l'utilisation de multiples marques de pare-feu : impératifs réglementaires, « niveau élevé de dotation en personnel, formations et ressources » permettant d'envisager une telle approche sans introduire de risque nouveau lié à la gestion de configurations supplémentaires, ou encore phase de transition vers une infrastructure réseau à définition logicielle (SDN).

Au final, Gartner estime que 15 % des entreprises utiliseront une approche en « double rangée » de pare-feu jusqu'en 2020, « gaspillant leur budget et leurs ressources dans des contrôles en double ».

• Valéry Marchive

Le chiffrement, une avancée à double tranchant pour les DSI

Si l'utilisation croissante du chiffrement constitue une avancée certaine pour la confidentialité des échanges et la sécurité des transactions, elle n'en présente pas moins de nouveaux défis aux DSI.

Selon les données produites l'an passé par le réseau Dell SonicWall Global Response Intelligence Grid, près de 65 % du trafic sur les réseaux des entreprises est aujourd'hui chiffré. Hélas, pour Florian Malecki, directeur marketing produit pour la sécurité réseau chez Dell security, « de nombreuses organisations sont aveugles face au trafic chiffré ». Et la perte de performances affichée par les équipements de protection réseau dès qu'est activée l'inspection du trafic chiffré ne permet guère d'envisager de l'inspecter dans son intégralité.

Mais une étude Vanson Bourne pour Venafi, réalisée auprès de 500 DSI aux Etats-Unis, au Royaume-Uni, en France et en Allemagne, ne fournit guère une photographie plus encourageante. 87 % de ceux-ci estiment ainsi que leurs systèmes de protection sont moins efficaces parce qu'ils ne peuvent pas inspecter le trafic chiffrer à la recherche d'activités malicieuses ou d'exfiltrations de données. Qui plus est, 90 % des sondés ont déjà été attaqués – ou s'attendent à l'être – par des pirates cachant leurs opérations grâce au chiffrement.

Selon Gartner, 50 % des attaques passant par le réseau seront caché, dès 2017, dans du trafic chiffré. Mais les entreprises elles-mêmes multiplient le recours au chiffrement, tout en accélérant la production applicative. 79 % des sondés estiment ainsi que DevOps rend plus difficile de savoir ce qui est de confiance et ce qui ne l'est pas au sein de l'organisation. Parallèlement, en 2015, selon Ponemon, il y avait plus de 23 000 clés et certificats en utilisation dans une entreprise, un chiffre en progression de 34 % depuis 2013. Mais l'administration de ceux-ci est fortement sujette à caution : plus de la moitié des DSI admettent ne pas savoir où sont stockés clés et certificats, qui les détient, ou comment ils sont utilisés.

C'est finalement sans surprise que 85 % des DSI sondés anticipent une utilisation malveillante croissante de clés et de certificats légitimes, dérobés et revenus par des cybercriminels.

• ***Valéry Marchive***

UTM vs NGFW : de vraies différences ?

Il est souvent difficile de faire la différence entre les systèmes de gestion unifiée des menaces (UTM) et les pare-feu de nouvelle génération (NGFW). Les experts reconnaissent que les lignes sont devenues floues entre les deux. Mais chercher à clairement définir l'un et l'autre peut être une erreur.

Les NGFW sont apparus il y a plus de dix ans en réponse aux entreprises qui cherchaient à combiner les capacités de filtrage traditionnelles par ports et protocoles avec des fonctionnalités de détection et prévention des intrusions (IDS/IPS) ainsi que d'analyse du trafic au niveau de la couche applicative.

Avec le temps, des capacités supplémentaires d'analyse des paquets en profondeur (DPI) et de détection de code malveillant sont venues s'ajouter.

En parallèle, les UTM sont nés du besoin des PME pour une protection plus complète que celle qu'offre un simple pare-feu. D'où l'intégration de capacités d'IDS/IPS, ainsi que de filtrage des contenus et des courriels, au sein d'une unique appliance facile à administrer.

D'autres fonctionnalités sont venues enrichir l'ensemble : serveur VPN, équilibrage de charge ou encore protection contre les fuites de données (DLP).

Selon Jody Brazil, Pdg de FireMon, les PME et les succursales ont été séduites par les UTM alors que les grandes entreprises ont préféré déployer des pare-feu de nouvelle génération. Greg Young, vice-président recherche chez Gartner, relève en outre que les grandes organisations disposaient des budgets nécessaires à l'acquisition des meilleures technologies, ainsi que des personnels capables de tirer profit des fonctionnalités avancées et des performances plus élevées des NGFW.

De leur côté, non seulement les PME préféraient disposer d'une produit tout-en-un en limitant le recours au support de leurs fournisseurs. Et tant pis si les fonctions de leurs UTM étaient seulement bonnes et pas au mieux de ce qu'offrait le marché.

Young relève en outre que les équipementiers tendent à exceller soit dans un marché, soit dans l'autre, mentionnant Fortinet pour les UTM ou encore Palo Alto Networks pour les NGFW. Peu réussissent dans les deux, mais c'est selon lui le cas de Check Point.

« La confusion vient du fait que les spécialistes des PME cherchent à convaincre les grandes entreprises sans effectuer de changements dans leur distribution ni dans la qualité de leurs produits. La confusion est le fait d'une campagne intentionnelle, mais très peu d'utilisateurs finaux se trompent sur ce dont ils ont réellement besoin. C'est soit une voiture de sport (NGFW), soit une berline familiale (UTM) ».

De son côté, Brazil reconnaît bien le risque de confusion, même pour les experts les plus expérimentés, mais il décrit l'UTM comme une compilation de fonctions de sécurité sans lien entre elles, dont le pare-feu : « l'UTM correspond généralement à un pare-feu doté d'une série de fonctions de sécurité ajoutées, comme l'anti-virus et le filtrage des pourriels. On n'y trouve pas les fonctions de contrôle d'accès qui définissent généralement un pare-feu ».

Pour lui, ce qui définit traditionnellement un NGFW, ce sont des contrôles d'accès robuste au niveau de la couche 7 du modèle ISO. Et cela même si de plus en plus de pare-feu de nouvelle génération sont enrichis de capacités de gestion du renseignement sur les menaces qui leur permettent de repousser les menaces connus à l'aide de règles actualisées automatiquement. Dès lors, il estime qu'un UTM devrait être considéré comme un NGFW lorsqu'il intègre les contrôles de la couche 7, et qu'un NGFW devrait être vu comme un UTM lorsqu'il intègre la protection contre les logiciels malveillants.

A terme, Brazil s'attend à ce que les NGFW se banalisent, faisant de pare-feu et de pare-feu de nouvelle génération des synonymes. Mais les UTM devraient continuer de constituer des produits importants pour les PME, tout particulièrement pour les organisations qui privilégient simplicité de déploiement.

Et justement, les différences de performances et d'administration devraient empêcher la convergence entre UTM et NGFW.

« L'idée d'une passerelle de sécurité réseau *convergée* va continuer de séduire. Et les équipementiers vont continuer d'ajouter des fonctionnalités pour réduire le coût total de possession pour les clients et augmenter leur chiffre d'affaires. Mais les questions de performances et d'administration vont continuer de pousser au déploiement de systèmes dédiés dans les réseaux des

entreprises. Dès lors, il continuera d'y avoir des pare-feu d'entreprise qu'il ne convient pas de considérer comme des UTM ».

Mike Rothman, analyste et président de Securosis, a une approche plus radicale. Pour lui, UTM et NGFW sont pour l'essentiel la même chose ; les différences relèvent pour l'essentiel de la sémantique marketing. Un marketing qu'il considère d'ailleurs responsable de la confusion. Mais uniquement : pour lui, l'adoption du terme NGFW par les analystes n'a pas aidé.

Rothman relève ainsi que les premiers UTM souffraient de problèmes de performances lorsqu'il s'agissait de passer des besoins d'une PME à ceux d'une grande entreprise, et tout particulièrement lorsqu'il s'agissait d'appliquer à la fois des règles positives (contrôle d'accès au niveau du pare-feu), et négatives (IPS). Mais selon lui, les premiers NGFW peinaient avec la prévention de menaces.

Dès lors, il estime que les disparités perçues ont été utilisées pour segmenter le marché, et continuent de l'être alors même que ces questions ne sont plus pertinentes.

Et pour Rothman, la confusion ne tient pas uniquement à la comparaison de types de produits, mais également au terme de pare-feu de nouvelle génération, dont il pense qu'il minimise les fonctions des équipements : « ce que fait un NGFW va bien au-delà du pare-feu. Un pare-feu est là pour contrôler les accès. Un NGFW cherche aussi les menaces, comme un IPS, pour les bloquer. Nous préférons parler de passerelle de sécurité réseau. C'est un terme plus descriptif ».

Au-delà, Rothman estime que les UTM modernes peuvent faire tout ce que font les NGFW, à condition d'être configurés de manière adéquate. « Du point de vue d'un client, ces appareils font les mêmes choses. Le NGFW assure contrôle d'accès et prévention des menaces, comme l'UTM, simplement de manière un peu différente dans certains appareils.

Au final, l'industrie doit se concentrer sur ce qui compte : l'appareil va-t-il supporter les volumes de trafic qu'il sera appelé à gérer lorsque tous les services sont activés ? C'est la seule question qui compte ».

Malgré leurs divergences, ces experts s'accordent à considérer que les entreprises ne devraient pas chercher à

faire la différence entre UTM et NGFW : elles doivent se concentrer sur la recherche de produits qui correspondent à leurs besoins.

Et à plus forte raison, selon Rothman, que les différences sont appelées à s'estomper encore plus avec des spécialistes de l'UTM qui enrichissent leurs produits de capacités d'inspection au niveau applicatif, et des constructeurs de NGFW qui élargissent leurs gammes afin de séduire les PME.

Et pour Young, en définitive, « il n'est pas question que de technologie. Le sujet est la différence entre la sécurité d'une PME et celle d'une grande entreprise. C'est une question d'usages ».

• Michael Heller

Ce qui fait un véritable pare-feu de nouvelle génération

Originellement, le terme de pare-feu de nouvelle génération se réfère à une combinaison de pare-feu conventionnel, de pare-feu applicatif, et de technologies de prévention/détection d'intrusion (IPS/IDS). Mais cela remonte si loin que cela peut désormais s'appliquer à la plupart des pare-feu du marché. Dès lors, dire que l'on souhaite quelque chose de « nouvelle génération » lorsque l'on veut renouveler son pare-feu n'aide pas particulièrement à affiner la recherche.

Compte tenu de tous les autres changements survenant dans l'informatique d'entreprise – de l'adoption des architectures scale-out aux conteneurs en passant par les environnements intégrés de fourniture hybride de services – ceux qui cherchent à acquérir un pare-feu feraient bien de chercher des fonctionnalités particulièrement avancées : administration centralisée, application distribuée des règles, élasticité, intégration avec les systèmes de gestion des menaces, des risques, et de la conformité.

La combinaison de l'administration centralisée avec l'application distribuée des règles est une évolution naturelle des pare-feu à l'heure des architectures orientées micro-services et des systèmes scale-out. En positionnant de multiples points d'application des règles dans l'environnement, sous la forme d'appliances virtuelles, de conteneurs ou d'agents embarqués, un tel système distribue le travail de filtrage du trafic. Des ressources de calcul et de réseau peuvent être assignées à chaque point d'application des règles, en fonction du trafic, depuis et vers les parties de l'environnement qu'ils protègent. De nouvelles instances peuvent être activées lorsque les besoins augmentent, sous la forme de conteneur applicatifs ou de machines virtuelles supplémentaires.

De telles technologies de pare-feu avancées permettent à l'application des règles de suivre les traitements virtualisés ou conteneurisés au fil de leurs mouvements. Elles s'avèrent critiques dans les environnements de cloud privé, mais également de cloud public.

La distribution des points de terminaison consiste en un environnement micro-segmenté, centré sur le contrôle étroit de quels utilisateurs et services peuvent communiquer avec quels composants applicatifs – ainsi que quand et dans quelles circonstances. Tout ce qui ne

relève pas de la couche frontale à l'utilisateur de la fonction est pour l'essentiel fermé à tout sauf à un petit ensemble prédéfini de partenaires de communication autorisés. Ce type de liste blanche hautement granulaire améliore considérablement la protection de l'infrastructure contre les tentatives de mouvement latéral engagées par les attaquants, à partir de systèmes compromis.

Qu'est-ce qu'un pare-feu véritablement avancé ?

La question de l'élasticité est critique. Un véritable pare-feu de nouvelle génération devrait être capable de monter en capacité à mesure qu'évoluent les besoins pour ses services, avec en option des pare-feu distribués. Même s'il reste des points de l'infrastructure où il est inévitable de positionner des pare-feu, à l'âge des appliances virtuelles et des fonctions réseau virtualisées en conteneurs, personne ne devrait avoir à sur-dimensionner à la commande pour l'achat d'un pare-feu, afin de tenir compte de ses besoins à trois ans. Chacun devrait pouvoir dimensionner selon ses besoins actuels et compter sur les capacités d'élasticité de sa solution, en misant sur des conteneurs supplémentaires, sur des machines virtuelles assurant l'équilibrage de charge, etc.

Bien sûr, il reste des échelles où des matériels et composants spécifiques sont nécessaires pour obtenir les performances souhaitées, mais elles sont de moins en moins nombreuses. Toutefois, pour ces situations, le sur-dimensionnement à long terme peut-être une stratégie payante. Les pare-feu en mode Cloud seront en tout cas de plus en plus importants comme première ligne de filtrage pour toutes les entreprises. Ils n'éliminent pas le besoin pour des protections en local, mais ils réduisent la charge et change le rôle et l'échelle de cette technologie.

Le Cloud sera également crucial à la mise en place de défenses robuste d'une autre manière : il va permettre de tirer profit des menaces affectant d'autres organisations comparables. Un pare-feu véritablement avancé devrait pouvoir s'appuyer sur des flux de renseignements sur les menaces. Ceux-ci l'aident à identifier les menaces clés dès qu'elles émergent et peuvent également faciliter le maintien en conformité réglementaire.

• John Burke, Nemertes research

AUTEURS

Le document consulté provient du site www.lemagit.fr

Cyrille Chausson | *Rédacteur en Chef*

Valéry Marchive | *Journalistes*

Linda Koury | *Directeur Artistique*

Neva Maniscalco | *Designer*

TechTarget
22 rue Léon Jouhaux, 75010 Paris
www.techtarget.com