STORMSHIELD

AVIS D'EXPERT

FIREWALL D'ENTREPRISE : BACK TO BASICS

Stéphane Prevost
Product Marketing Manager, Stormshield

L'importance de l'utilisation d'un firewall en entreprise n'est aujourd'hui plus à démontrer. Mais pour faire face à la sophistication des menaces actuelles, le firewall de bordure ne suffit plus. Dans un contexte en perpétuelle évolution, comment intégrer un firewall dans une architecture réseau ? Comment l'utiliser au mieux ?

Emplacement d'un firewall, segmentation réseau, approche *Zero Trust*, gestion centralisée et supervision ; pour tout savoir de l'utilisation optimale d'un firewall dans votre architecture réseau.

LA COMPRÉHENSION DU BESOIN ET DU PÉRIMÈTRE À PROTÉGER

Le firewall est un des piliers de la sécurité périmétrique dans les entreprises. Historiquement pensée comme une muraille impénétrable en bordure de réseau, sa fonction a depuis largement évolué. Pour répondre à l'évolution des menaces et bloquer toutes les tentatives de déplacement latéral prisé par les malwares, les administrateurs systèmes ont dû revoir leur utilisation des firewalls, en ajoutant de nouvelles couches de protection.

Car l'emplacement adéquat d'un firewall dans une architecture réseau dépend du besoin de sécurisation. Et le traditionnel firewall en bordure de réseau, même s'il est toujours un indispensable de l'arsenal de sécurité, ne suffit plus pour répondre à un bon niveau de protection. En effet, l'évolution des modes de travail (nomadisme, télétravail, SaaS et autres infrastructures cloud) couplée à la sophistication des cyber-menaces a obligé les entreprises à étendre l'usage des firewalls. Il est désormais nécessaire d'aller plus loin et de déployer des firewalls à différents endroits du périmètre de sécurité de l'entreprise. Mais ce périmètre de sécurité évolue et est composé d'éléments hétérogènes, internes comme externes.

Mais alors, **quels sont les emplacements stratégiques pour un firewall ?** En coupure d'internet, en bordure ou au cœur de réseau, dans le cloud… les possibilités sont multiples et dépendront de vos objectifs de sécurité et capacités de vos firewalls. À noter que, suivant le principe de défense en profondeur, il est conseillé de positionner au moins deux firewalls pour créer une zone de confiance (DMZ, *demilitarized zone*). Une double barrière qui permet une étanchéité supplémentaire au niveau des flux (potentiellement malveillants). L'objectif est de mettre en place plusieurs niveaux de confiance, depuis Internet jusqu'au LAN, voire aux datacenters et autres environnements cloud.

Et les firewalls de nouvelle génération (NGFW) permettent d'aller encore plus loin dans la sécurité des architectures réseaux, notamment avec la segmentation réseau et l'approche Zero Trust. Explications.

L'IMPORTANCE DE LA SEGMENTATION RÉSEAU ET DU *ZERO TRUST*

Pourquoi segmenter les réseaux est si important ? Parce que le mode opératoire des cyber-criminels intègre une phase de reconnaissance. Après avoir compromis et infiltré une machine, ces derniers scannent les équipements connectés sur le réseau dans le but de préparer un éventuel rebond. Pour éviter toute progression, une segmentation stricte doit être appliquée sur le réseau principal et dans les sous-réseaux. En divisant cet ensemble en zones distinctes, l'administrateur peut alors appliquer un contrôle strict au niveau des accès et des flux.

La mise en place d'une DMZ, dont il était question plus haut, est un « *cas particulier de la segmentation*, selon **Simon Dansette**, Product Manager chez Stormshield. *Elle présente l'intérêt de pouvoir compartimenter le réseau pour un besoin spécifique en bloquant toutes possibilités de déplacement latéral* ». Et comme le rappelle **Sébastien Viou**, Directeur Cybersécurité et Management Produits chez Stormshield, « *la rupture protocolaire est un principe visant à rompre tous les flux réseau, transport et applicatif par leur interprétation et leur réécriture. En substance, il doit être impossible de réaliser du routage direct entre les deux firewalls* ». Le principe de double barrière n'a donc pas pour principe d'empiler plusieurs firewalls « *en pensant que le premier bloque les vulnérabilités de l'autre* », mais bien « de *créer des zones de confiances et d'appliquer des règles de sécurité cohérentes tout en y maîtrisant les échanges* ». Dans les environnements industriels sensibles, cette segmentation réseau permet plusieurs actions. D'une part, elle isole les environnements IT et OT et stoppe ainsi le déplacement latéral d'un ransomware qui aurait infecté une infrastructure IT et qui chercherait à se propager

dans les environnements de production. D'autre part, cette segmentation peut aller jusqu'au cœur de l'OT, au plus près des machines et automates, avec l'application d'un filtrage granulaire des flux, pouvant aller jusqu'à la commande envoyée.

«Le principe de double barrière n'a donc pas pour principe d'empiler plusieurs firewalls en pensant que le premier bloque les vulnérabilités de l'autre, mais bien de créer des zones de confiances et d'appliquer des règles de sécurité cohérentes tout en y maîtrisant les échanges.»

Pour s'assurer de la légitimité des utilisateurs et machines se connectant sur les réseaux, les entreprises peuvent appliquer en complément le concept dit de *Zero Trust*. **Cette philosophie Zero Trust repose sur le principe que les utilisateurs et les composants du réseau ne doivent pas être présumés de confiance par défaut, mais doivent prouver leur identité et leur légitimité à chaque demande d'accès aux ressources.** Ainsi, l'architecture *Zero Trust Network Access* (ZTNA) inclut aussi bien les utilisateurs que les appareils dans l'authentification et l'autorisation d'accès au réseau. L'accès est alors granulaire et spécifique au besoin de l'utilisateur. « *Dans une architecture Zero Trust, le firewall doit d'abord s'intégrer avec des technologies d'authentification forte, pour identifier l'utilisateur. Mais il doit également vérifier que le poste de travail à authentifier est sain* » explique Simon Dansette. C'est au travers de cette philosophie que les derniers modèles de firewalls permettent d'appliquer un contrôle d'accès utilisateur plutôt que de filtrer seulement en fonction de l'IP (comme le faisaient les firewalls traditionnels). Les règles de filtrage de trafic permettent alors de mettre en place des politiques de sécurité granulaires et en temps réel. Pour Simon Dansette, « *il existe aujourd'hui des interactions entre les solutions de type EDR et les firewalls pour autoriser un utilisateur à se connecter. Ces mécanismes permettent d'aller plus loin dans le processus d'authentification* ». Le firewall de nouvelle génération devient alors un élément-clé de l'architecture *Zero Trust*.

Application de règles spécifiques ou communes, mise à jour des équipements, monitoring et supervision, qu'ils soient physiques ou virtualisés, la multiplication des firewalls dans les entreprises oblige les administrateurs systèmes à repenser leur gestion passant d'une gestion unitaire à une gestion centralisée. Un outil devenu aujourd'hui nécessaire.

LA NÉCESSAIRE GESTION CENTRALISÉE DES FIREWALLS

Qu'ils soient en bordure ou en cœur de réseau, au plus près d'un équipement industriel ou hébergé dans le cloud, le nombre de firewalls et leurs emplacements se sont démultipliés à tel point que leur gestion peut vite s'avérer complexe. Déploiement, configuration, maintenance, gestion des correctifs… Selon Simon Dansette, la gestion centralisée permet de « *réduire la complexité de gestion des différentes connexions aux firewalls et de réduire le temps d'administration réseau, et donc les coûts inhérents* ».

La gestion centralisée permet également de simplifier le processus de conformité aux normes de sécurité, en garantissant que toutes les politiques de sécurité soient appliquées uniformément à tous les firewalls du réseau. Pour les MSSP et revendeurs informatiques, elle s'avère être un atout. Car **la gestion centralisée permet de gérer la configuration de plusieurs firewalls en un unique outil et de pouvoir, à partir d'une même plateforme, tous les administrer**. Les modifications seront facilement et rapidement effectuées, apportant sécurité pour leurs clients et gain de productivité pour leurs équipes.

La centralisation de la gestion des logs permet également une visualisation des indicateurs en une même interface, facilitant ainsi la surveillance et le reporting. Lorsque les logs sont collectés, stockés et archivés dans une plateforme unique, l'administrateur système trouvera et corrigera plus aisément les problèmes de configuration. Pour Simon Dansette, « *la centralisation apporte une vision d'ensemble permettant plus facilement d'analyser là où est le problème et ensuite d'aller corriger sur le firewall incriminé. L'étape de troubleshooting est facilitée pour les administrateurs systèmes et permet de gagner du temps dans des instants où le stress est important* ».

Et demain ? Force est de constater que les points de protection réseaux ne sont pas les seuls à se multiplier en entreprise ; les points de protection des terminaux suivent la même tendance. Pour autant, le constat récurrent de la réussite des cyberattaques démontre le manque d'efficacité de cette approche. Car la multiplication des solutions de détection provoque des événements multiples et nombreux avec des comportements difficiles à interpréter et corréler pour les administrateurs. Un manque de visibilité qui limite la réactivité et qui se traduit dans les faits par une baisse du niveau de protection. Pour y répondre et développer une gestion plus globale, les offres XDR (*eXtended Detection & Response*) se sont développées. Avec une triple promesse : réduire les risques, corréler les événements remontés par les différentes solutions de cybersécurité et améliorer la productivité opérationnelle cyber des organisations.