



THÉMA

FIREWALL : UN MAILLON INDISPENSABLE

Par Marc Jacob et Emmanuelle Lamandé

A l'ère du Cloud Computing, de la mobilité... qui entraînent de nouvelles définitions du SI des entreprises, la question se pose de l'utilité des outils de protection périmétrique. Pourtant, pour nos trois experts, Joseph Graceffa, Directeur Technique associé d'Advens, Yannick Hamon, Consultant et responsable du pôle « Tests d'intrusion et audits » chez XMCO Partners, et Raphaël Marichez, Consultant chez Hervé Schauer Consultants (HSC), le firewall a plus que jamais sa place au cœur de la défense de l'entreprise. Bien sûr, il va s'agir de choisir les bonnes solutions, de les positionner aux bons endroits et de savoir les administrer dans le temps. Encore une fois, l'organisation et le bon sens sont aussi la clé d'une bonne protection contre les menaces.



Joseph Graceffa, Advens

Le phénomène d'ouverture du SI de l'entreprise, apparu depuis quelques années et qui s'accélère avec le Cloud Computing, conduit les dirigeants d'entreprises, et, en particulier, les directions des achats, toujours sur le « qui vive » en matière d'économies, à se poser des questions sur l'intérêt d'utiliser

des firewalls. Pourtant, pour nos trois experts, aucun doute, le firewall reste un outil indispensable de protection du SI. Ainsi, Joseph Graceffa considère que le rôle du firewall à l'ère du Cloud est fondamental pour la sécurité, voire encore plus important avec l'usage de machines virtualisées de plus en plus nombreuses dans le Cloud. Pour lui, il faut absolument s'assurer des contrôles d'accès réseaux à ces ressources externalisées : chaque machine ou chaque application virtualisée dans le Cloud doit avoir son firewall. De plus, reprend Yannick Hamon, « en fonction du modèle de Cloud Computing choisi, le firewall peut être contrôlé par l'entreprise ou par le fournisseur du Cloud. Cependant,

dans tous les cas, même en SaaS, les applications reposent sur des architectures N-Tiers et exposent des services sensibles (administration, supervision, base de données, serveur de fichiers...). Même dans le Cloud, l'accès à ces services doit être maîtrisé afin de limiter le risque en cas de compromission d'un serveur. Un firewall est donc toujours indispensable cependant, en fonction du modèle choisi, ce dernier sera à la charge de l'entreprise ou du fournisseur de service. Dans ce contexte, le type de firewall à déployer dépendra surtout du modèle de Cloud. Plus l'entreprise doit maintenir de composants dans l'architecture (Modèle PaaS : logiciels, bases de données) et plus le firewall doit être complet (filtrage réseau couche 3 et 4, IDS/IPS, applicatif etc.). Ainsi, le type de firewall dépend uniquement du périmètre à couvrir (réseau, application...) ».

Yannick Hamon, XMCO Partners: les 3 principaux modèles de Cloud Computing

- ▶ IaaS : l'entreprise continue de maintenir les couches logicielles (serveur, services, bases de données), seule la partie matérielle est gérée par le Cloud.
- ▶ PaaS : l'entreprise est uniquement responsable de l'application, le reste est géré dans le Cloud.
- ▶ SaaS : le Cloud prend son sens, c'est-à-dire que même l'application est gérée par le fournisseur de service.

FIREWALL

De ce fait, l'UTM qui regroupe plusieurs fonctionnalités dans une appliance est un outil apprécié de nos experts, comme l'explique Joseph Graceffa : « l'arrivée des UTM nous a démontré que l'on pouvait mettre plusieurs fonctions de sécurité sur les réseaux, ceci dans une seule boîte et donc simplifier les infrastructures de sécurité dans les SI. A l'ère du Cloud, la virtualisation du firewall paraît indispensable. De plus, compte tenu du fait que les attaques ciblent maintenant les applications, il est tout aussi pertinent d'avoir des technologies de type firewalls applicatifs, mais également à cause de la facilité avec laquelle les outils arrivent à traverser les filtres réseaux en se « cachant » dans des flux standards et légitimes. Il est, par exemple, très difficile d'empêcher un flux skype de sortir de son entreprise... De ce fait, il convient d'avoir une forte capacité de filtrage applicatif ou de contenu. Les UTM ont donc un bel avenir devant eux car, pour certains, ils couvrent l'ensemble de ces fonctionnalités : filtrage réseaux, filtrage applicatif, filtrage de contenu, virtualisation et sécurité dans la virtualisation... Reste que le débat de l'administration de l'ensemble de ces couches de sécurité demeure entier : peut-on raisonnablement penser qu'un administrateur de firewall aura la meilleure expertise pour paramétrer au mieux la couche de sécurité applicative ? En effet, il n'y connaît généralement rien en développement et est incapable d'analyser finement le site web que l'équipe marketing de l'entreprise a fait développer chez un tiers qui ne documente rien et utilise un obscur Framework personnel développé en interne. Je pense que nous reviendrons soit à des fonctions de sécurité séparées dans différents outils experts dans leur domaine, soit à un outil tout-en-un autorisant une administration fine de chaque fonctionnalité de sécurité par différents profils dans l'entreprise et avec bien-sûr une interface de management utile utilisable par tous ».

Quel que soit le réseau utilisé (Cloud, réseau virtuel ou périmétrique...), les mesures de sécurité traditionnelles s'appliquent toujours

Pour Raphaël Marichez, sur un plan purement logique, un réseau virtuel reste un réseau, et les mesures de sécurité traditionnelles comme les firewalls s'y appliquent



Raphaël Marichez, HSC

toujours : simplement, elles s'appliquent à la couche virtualisée, sans que cela ne permette d'en faire l'économie sur la couche support. En général, dans une offre Cloud, ces cloisonnements et filtrages entre réseaux virtuels, entre réseaux d'administration, etc., font partie des activités qui sont sous-traitées.

Le client d'une offre Cloud n'a donc, en théorie, plus à se préoccuper des fonctions de filtrage, du moins pour la partie externalisée.

Cependant, il subsiste nécessairement un SI minimal qui n'est pas externalisé, qu'il convient donc de protéger de manière traditionnelle : cloisonnement des réseaux et DMZ.

Par ailleurs, l'externalisation dans un Cloud impacte le niveau applicatif : la navigation internet et plus généralement les flux applicatifs entre les postes de travail (y compris nomades) et l'extérieur (y compris dans le Cloud) représentent l'essentiel des communications informati-

SPECIAL FEATURE

FIREWALLS ARE AN ESSENTIAL PART OF THE CHAIN

BY MARC JACOB AND EMMANUELLE LAMANDÉ



Cloud computing and mobility have changed the contours of company IT systems and raised the issue of peripheral protection. However, our three experts – Joseph Graceffa, associate technical director, Advens, Yannick Hamon, consultant and intrusion testing and audit manager, XMCO Partners, and Raphaël Marichez, consultant with Hervé Schauer Consultants (HSC) – consider that the firewall is more than ever a key element in a company's protection set up. Of course the right solutions have to be selected, they have to be put in the right place and they have to be managed correctly on an ongoing basis. Once again, the right organisation and good sense are the key to successful threat protection.

THÉMA

FIREWALL



ques. Ces interconnexions constituent donc également l'essentiel des possibilités d'attaques et des vulnérabilités liées au réseau. Des firewalls applicatifs et d'autres mesures de sécurité au niveau du SI résiduel de l'entreprise sont donc, comme avant, chargés d'assurer l'innocuité, autant que faire se peut, des flux entrants et sortants.

Finalement, la problématique fonctionnelle n'a pas beaucoup évolué ; ce sont les chemins empruntés par les flux réseau qui ont changé, entraînant dans le même temps une augmentation de la complexité et de l'imbrication des réseaux. Tout à fait d'accord, complète Joseph Graceffa, même si de nombreux opérateurs internet proposent des offres de firewall, le filtrage d'accès réseaux ne doit pas se cantonner à l'accès Internet ou les accès à distance. Il est de plus en plus courant de mettre en œuvre des firewalls dans les réseaux internes, pour séparer les infrastructures, les applications des bases de données, les utilisateurs de certaines applications, voire même de segmenter le réseau LAN en fonction des missions de chacun dans l'entreprise... Ainsi, il faudrait pratiquement positionner un firewall devant chaque application. Bien sûr, reprend Yannick Hamon, le firewall doit être situé au plus proche de la donnée. Il ne suffit pas de mettre un firewall à l'entrée du Cloud car celui-ci n'est pas une zone de confiance. Idéalement, il faudrait mettre un firewall sur chaque serveur, mais l'administration deviendrait alors plus complexe. D'ailleurs, explique Raphaël Marichez, cette complexité croissante augmente les coûts bruts d'exploitation ; les coûts marginaux ne peuvent donc être réduits que lorsque l'économie d'échelle est suffisamment efficace pour compenser les coûts bruts. La sécurité, quant à elle, pâtit de cette complexité croissante entraînant une inflation des vulnérabilités et des vecteurs d'attaque, et l'impact potentiel résultant d'une compromission, à l'inverse des coûts marginaux, augmente avec le facteur d'échelle. Le résultat de l'équation avantages/inconvénients n'est pas garanti malgré les discours marketing. Comme le conclut Joseph Graceffa, « serait-ce là les prochaines réussites commerciales et techniques à venir pour certains éditeurs de firewall ? Probablement ! »

**Firewalls de nouvelle génération :
nouveaux concepts marketing
ou véritables avancées ?**

essayant, à partir de techniques parfois peu, voire pas innovantes, d'améliorer l'efficacité des boîtiers, de réduire les erreurs d'exploitation et, éventuellement, de diminuer les faux-positifs, encore que ce dernier aspect semble de moins en moins considéré ces derniers temps. Il ne s'agit que d'une augmentation incrémentale du niveau des technologies « arme contre bouclier », et ne saurait constituer ne serait-ce que l'embryon d'une révolution. Par contre, Yannick Hamon estime que ces nouveaux types de firewall, en couplant un firewall traditionnel avec un firewall applicatif, amènent un apport supplémentaire en termes de sécurité. En effet, ils permettent d'inspecter le contenu des flux et d'intégrer des notions de comptes utilisateurs qui peuvent être utilisés afin de filtrer l'accès en fonction des comptes Active Directory. Enfin, Joseph Graceffa est un fervent « supporter » de ces technologies : « ces firewalls apportent en fait une vision et une organisation de la politique de sécurité basée sur les utilisateurs, les ressources cibles et les usages de celles-ci. Enfin, ils amènent une vue qui peut être comprise du business et des fonctionnels de l'entreprise et non plus une vision centrée sur « adresse IP / ports » qui ne résonnent qu'aux oreilles des administrateurs réseaux & sécurité. Un peu comme l'ont fait les premiers acteurs du VPN SSL, où on parlait d'accès et d'usage de ressources plutôt que de règles d'accès réseaux. Couplés à des systèmes de fédération d'identité et d'IAM, de plus en plus développés en entreprise, on peut maintenant rêver d'avoir une politique d'accès basée sur les utilisateurs, leurs métiers, leurs contraintes et leurs objectifs de sécurité. Enfin, ces nouveaux acteurs du firewall offrent des capacités avancées de contrôle des usages des applications qui permettent de fixer clairement dans une organisation que le DG a le droit à Facebook ou Youtube sous toutes les formes et que les utilisateurs du service clients n'auront accès qu'à leur CRM favori... »

**Administration des firewalls :
une question d'outils
et d'organisation**

L'administration des firewalls, comme pour tout outil de sécurité, est un problème crucial. Joseph Graceffa explique de façon consensuelle : « tout réside dans le choix de bon outil et d'une organisation sans faille ! » Yannick Hamon entre dans le détail : « dans un premier temps, les administrateurs doivent définir les politiques de sécurité... »

FIREWALL



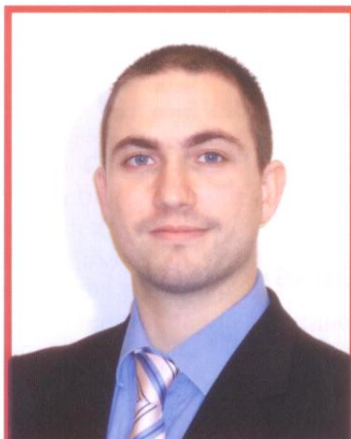
wall est un élément maître de la sécurité d'une entreprise et son accès doit être restreint et maîtrisé. Il n'est pas rare lors de tests d'intrusion de trouver des firewalls implémentant encore des mots de passe par défaut.

Dans un second temps, les règles nécessaires au métier doivent être étudiées et approuvées par l'équipe sécurité. Dans les grandes entreprises, des nouveaux projets sont lancés chaque semaine. Des dizaines de flux métiers doivent être ouverts. L'administrateur doit donc travailler main dans la main avec les études et architectes afin de comprendre le rôle de chaque flux au lieu d'ajouter « bêtement » sans réflexion.

Enfin, les règles des firewalls doivent être simplifiées. Aujourd'hui, la majorité des protocoles utilisés par les logiciels n'utilisent plus de ports ouverts dynamiquement (i.e : ouverture des ports 1024-65534), d'autres nécessitent, par défaut, uniquement un peu de configuration (i.e : Oracle 9 ou NFS) ».

Encapsulation : quel champ d'action pour le firewall ?

Pour Raphaël Marichez, il est illusoire d'espérer pouvoir abandonner la sécurité sur les flux réseau traditionnels qui soutiennent les réseaux virtuels (encapsulés). La sécurité étant une chaîne constituée de maillons, une vulnérabilité du réseau sous-jacent entraîne la défaillance de la sécurité de l'ensemble des réseaux virtuels qui en dépendent. Il faut rappeler que le principal objectif d'un firewall est de restreindre l'accès à un service donné et de ne pas exposer d'éventuels services d'administration ou dangereux, analyse



Yannick Hamon, XMCO Partners

Yannick Hamon. Il ne faut pas tout mélanger : si le service exposé propose des fonctionnalités d'encapsulation, ce service doit être renforcé ou surveillé par un composant tiers (IDS/IPS/Analyse de logs) pour limiter l'impact : ce n'est pas le rôle d'un firewall. Le pare-feu est un élément de sécurité, tout comme les

antivirus ou les proxy/reverse-proxy..., ceux-ci ne couvrent pas tous les risques informatiques, mais sont indispensables. Toutefois, pour Joseph Graceffa, un firewall doit pou-

voir analyser les flux le traversant et doit savoir identifier toute tentative d'encapsulation ou, du moins, proposer un moyen pour bloquer toute activité non reconnue ou non autorisée.

Pas d'alternative aux firewalls !

Pour nos trois experts, il n'y a aucun doute, il n'y a pas d'alternative au déploiement des firewalls. Selon Joseph Graceffa, dans l'état de l'art actuel, il est illusoire de penser que les réseaux, les applications et les utilisateurs assureront par eux-mêmes le contrôle d'accès... on peut juste penser que la fonctionnalité de contrôle d'accès sera présente à tous les étages, et plus ou moins automatisée ou autonome, mais sera bien présente. Il ne faut pas oublier que les firewalls ne sont qu'un outil et non un objectif en soi. Il ne faut pas chercher une alternative, comme si l'on pouvait choisir entre un outil et un autre, rappelle Raphaël Marichez. « C'est l'ensemble des outils qui seul permet d'atteindre un objectif de sécurité. Les firewalls s'inscrivent d'ores et déjà dans des systèmes de gestion (systèmes de management) permettant d'assurer que l'ensemble de mesures de sécurité atteint un objectif visé. Les firewalls n'en sont qu'un maillon, mais il semble impossible de s'en passer : le principe de la virtualisation repose sur un cloisonnement des réseaux virtuels ou des applications virtuelles au sein de supports physiques mutualisés.

Les fonctions de cloisonnement ne peuvent donc pas être évitées, que ce soit au sein de l'univers nouvellement virtualisé ou au sein de l'univers des réseaux traditionnels, sans oublier bien entendu l'isolation des univers les uns des autres.

Il ne faut pas non plus oublier les flux d'administration des équipements de sécurité tels que les firewalls eux-mêmes : avec les imbrications liées au cloud, il est obligatoire d'assurer des protections périmétriques (fonctionnelles ou logiques) autour des firewalls eux-mêmes. En termes clairs, il faut « firewaller » les firewalls. Cela est exacerbé avec l'informatique nomade: l'administration à distance des postes nomades, à relier avec le concept de dé-périmétrisation, n'est ni plus ni moins qu'un contournement formidablement consensuel et ostentatoire des structures de firewalls traditionnels qui ont mis plusieurs années à se construire convenablement. Sans même pouvoir abandonner les premiers firewalls, il faut construire des firewalls autour des nouveaux SI virtualisés ». Toutefois, reprend Yannick Hamon, il n'existe véritablement pas de solutions alternatives aux firewalls d'autant que la dé-périmétrisation n'est pas encore d'actualité et ne sera certainement jamais implémentée en entreprises.