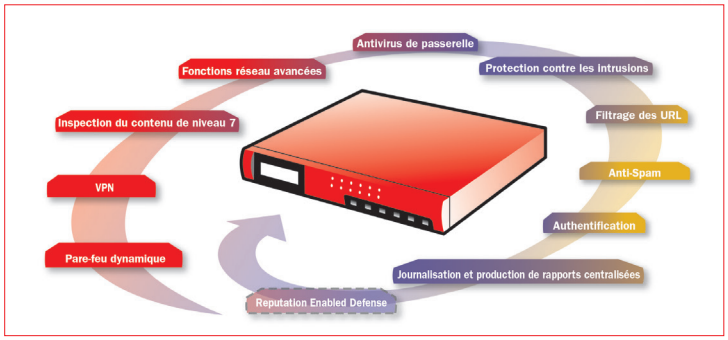
Réseaux sociaux, jeux, téléchargements, BYOD : Reprenez le contrôle de votre réseau

Malgré une hausse constante de la rapidité des réseaux, les entreprises sont toujours confrontées à des problèmes de performances. En cause, l'usage de plus en plus important par les employés d'applications web parfois très gourmandes en bande passante. La société WatchGuard, spécialiste de la sécurité et du contrôle applicatif, propose une gamme de boîtiers tout-en-un pour reprendre le réseau en main.

➤ Par Guillaume Rameaux

« Il a fallu 10 ans pour réussir à démocratiser l'usage d'internet. Aujourd'hui, tout le monde s'est approprié le web ». Et en même temps, la bande passante de l'entreprise. Le constat fait par Pierre Poggi, Country Manager France chez WatchGuard, est une réalité pour toutes les entreprises, quelle que soit leur taille. L'explosion conjuguée des terminaux mobiles, du cloud computing, des réseaux sociaux ou encore des jeux en ligne fait non seulement peser une pression de plus en plus grande sur les réseaux d'entreprise mais représente également un défi quotidien en termes de sécurité et de productivité.

Les pare-feu traditionnels ne suffisent plus et les organisations ont besoin d'outils capables d'analyser les flux au niveau applicatif. Hors de question pour autant de complexifier la gestion de l'infrastructure en empilant les solutions pour assurer une sécurité optimale. C'est à cette problématique que les boîtiers WatchGuard XTM de nouvelle génération viennent répondre. Ces appliances tout-en-un réunissent les fonctions de pare-feu classique, d'anti-virus, d'anti-spam, de filtrage d'URL et donc de contrôle applicatif. « Moins de 5 % des sociétés que l'on rencontre aujourd'hui savent faire ce contrôle des applications », explique Pierre Poggi. L'enjeu est pourtant de taille. « Quand vous avez 30 personnes qui écoutent de la musique sur Deezer, vous n'avez plus de bande passante pour Oracle », résume simplement le responsable.



Les appliances WatchGuard offrent un large éventail de fonctions

POKER ET PORNOGRAPHIE

Le blocage pur et simple n'est évidemment pas la solution. Les responsables

informatiques qui se sont aventurés dans cette voie ont dû faire face à de vives réactions d'utilisateurs, parfois bien placés dans la hiérarchie de l'entreprise. Partant d'un système d'information quasiment libre de toute restriction, la moindre tentative de contrôle peut vite prendre des allures de régression technologique. C'est pourquoi, avant toute intervention technique, WatchGuard préconise de respecter deux étapes majeures. La première est la réalisation d'un audit qui va permettre de comprendre toute l'activité qui transite sur le réseau de la société. Après deux à cinq semaines d'analyse, les résultats sont généralement très surprenants pour les dirigeants qui reçoivent le rapport.

Les boîtiers XTM sont capables d'analyser le trafic applicatif en profondeur

Vidéo et musique en streaming, poker en ligne ou même sites pornographiques, internet est loin de doper la productivité des employés et son utilisation est souvent bien différente des préoccupations business de l'entreprise. La démarche de WatchGuard consiste donc à ne rien bloquer dans un premier temps. Une fois l'audit réalisé, l'étape suivante est de rédiger une charte informatique (voir encadré) qui encadrera les usages des salariés. « À partir du moment où l'on a une bonne connaissance des comportements au sein de l'entreprise, on est capable de mettre en place une politique permissive avant d'être restrictive », poursuite Pierre Poggi. Et c'est là un des grands points forts du contrôle applicatif réalisé par WatchGuard. Un boîtier XTM est capable d'identifier la signature d'une application, web ou native, et d'en autoriser une partie tout en interdisant une autre. L'idée est de ne pas nuire à la productivité des employés qui peuvent par exemple utiliser les fonctionnalités de messagerie instantanée de Facebook ou MSN pour collaborer avec leurs collègues. Il devient alors possible de tolérer le chat sur Facebook mais d'interdire l'utilisation des jeux. L'administrateur de la solution dispose ainsi d'une granularité qui lui permet de trouver le bon équilibre entre sécurité et performance côté réseau et liberté côté utilisateurs.

La productivité sera par ailleurs largement améliorée grâce à une meilleure utilisation de la bande-passante et donc à de meilleures performances. « On découvre régulièrement des entreprises où 50 % de la bande passante est sacrifiée pour la musique. Il y a même des gens qui, pour écouter de la musique, vont sur YouTube et chargent des clips en haute définition qu'ils ne regardent même pas ». Difficile effectivement dans ces conditions pour l'application critique ou métier de se faire une place sur le réseau.

800 000 APPLIANCES DÉPLOYÉES ET CONNECTÉES

Pour ce qui est de la sécurité du SI, l'analyse précise des paquets entrants a également son importance. Alors que la majorité des virus ont pendant longtemps été diffusés par le biais des mails, la menace s'est aujourd'hui déportée sur le web et les applications. « Certains clients ont décidé de bloquer les sites web de mauvaise réputation. Cette méthode n'est pas suffisante car de nombreux sites de bonne réputation se font hacker et diffusent du code malveillant », prévient Pierre Poggi. Les très populaires Joomla et Wordpress par exemple, sont à la base de plusieurs millions de sites web. Lorsqu'une faille est

découverte sur une de ces plateformes, des sites réputés peuvent rapidement devenir des nids à malware. « C'est pour cette raison que le pare feu doit être capable d'analyser l'intégralité du flux et pas seulement se limiter au blocage des URL ».

WatchGuard emploie par ailleurs une seconde méthode pour prémunir ses clients contre les sites web piratés. Avec plus de 800 000 appliances déployées dans le monde, la société a accès à une gigantesque source d'informations. Quand un des boîtiers repère du code malveillant dans un paquet, elle fait remonter l'information de manière anonyme à l'autorité de réputation WatchGuard qui dégrade automatiquement la note du site émetteur. L'information est ensuite renvoyée à tous les autres boîtiers qui vont rejeter à leur tour le flux de ce site sans utiliser la moindre ressource pour l'analyser. Une technique qui, en plus d'assurer la sécurité de tous les clients, permet de soulager les plus petites machines disposant de moins de capacités de traitement.

FILTRER LES APPLICATIONS, LES TERMINAUX OU LES UTILISATEURS

Autre problématique à gérer pour les DSI : le phénomène BYOD (Bring Your Own Device). Tablettes, smartphones ou ordinateurs portables, les employés veulent connecter leurs terminaux au réseau de l'entreprise. « J'ai vu des gens venir dans des collectivités locales avec des petits hub ethernet pour brancher leur netbook à côté de leur ordinateur de bureau, raconte Pierre Poggi. Il y en a d'autres qui vont chercher le port RJ45 derrière l'imprimante pour accéder au réseau ». Là encore, le blocage total n'est pas une solution et il de-

✔ Définir les règles du jeu avec une charte Informatique

Ni juriste, ni avocat. WatchGuard n'a pas la prétention de remplacer l'expertise juridique d'un spécialiste du droit. L'éditeur essaie néanmoins de faire comprendre l'importance de la charte informatique dans les entreprises. WatchGuard invite pour cela ses clients finaux à des séminaires d'information organisés en partenariat avec le cabinet d'avocats Fidal. « Ce n'est pas WatchGuard qui va écrire leur charte, explique Pierre Poggi. C'est tellement important d'un point de vue juridique, qu'il faut la faire rédiger par quelqu'un dont c'est le métier ». La grande majorité des participants à ces réunions n'ont pas fait cette démarche, certains se contentant même d'envoyer par mail à tous les salariés une charte informatique trouvée sur internet.

Le sujet n'est pourtant pas à prendre à la légère pour un employeur qui est légalement responsable des activités de ses salariés. Sur la quarantaine d'événements qui ont été organisés jusqu'à présent, cinq personnes ont admis avoir fait venir les gendarmes après avoir identifié des contenus pédophiles sur le réseau de la société. « Mais ce n'est pas parce que vous avez la preuve de quelque chose que vous pouvez l'utiliser contre un salarié », tempère le responsable. D'où la nécessité de se protéger en fixant les règles du jeu à l'aide d'une charte informatique qui informera les employés du contrôle effectué sur leurs activités.

« Nous sommes pour la neutralité du web mais on se rend compte au fil du temps que l'utilisation d'internet est devenu un grand n'importe quoi dans les entreprises. Le téléchargement illicite est véritablement un sport national ». Effet pervers de la loi Hadopi, les particuliers ont aujourd'hui tendance à télécharger au travail pour éviter de recevoir les fameux courriers d'avertissements. La réglementation a également vulgarisé les outils de masquage de flux comme Ultrasurf et a rendu des outils comme Rapidshare et Megaupload très populaires. « Il y a un vrai besoin de recadrage. Surtout que la génération Y qui arrive dans les entreprises est née avec ses pratiques et est parfaitement à l'aise avec ces outils ».

Plus d'un quart des personnes présentes aux séminaires ne sont pas des informaticiens. Directeurs généraux, responsables financiers ou encore responsables des ressources humaines sont directement concernés par ces problèmes et ne savent pas comment les gérer. Pour en savoir plus sur ces questions, vous pouvez consultez la liste des événements WatchGuard à venir : http://www.WatchGuard.com/international/fr/press/events.asp

vient indispensable de pouvoir faire la distinction entre l'employé nomade qui souhaite accéder à son application métier et celui qui va consulter son compter Twitter personnel. La mise en place d'un XTM va résoudre ce problème puisque chaque device passant par le boîtier va hériter de toute la politique de sécurité mise en place pour le reste du parc informatique. Il est également possible de spécifier une interdiction d'accès pour certains appareils bien précis comme des iPads ou des Galaxy.

Et si les ordinateurs personnels s'invitent dans l'entreprise, il existe un phénomène inverse qui inquiète tout autant les DSI : la prise en main du matériel de la société depuis le domicile de l'employé. Une des principales demandes des responsables informatiques et des directions est effectivement le contrôle des applications de prise en main des machines à distance (LogMeIn, TeamViewer, GoToMyPC). Le cas typique : un employé se connecte à son ordinateur de bureau, lance des téléchargements (souvent illégaux) et récupère les fichiers sur un disque externe le lendemain matin lorsqu'il retourne travailler. Des téléchargements nocturnes qui viennent perturber les processus de batch ou de sauvegarde, généralement programmés la nuit pour justement profiter d'un réseau libre de l'activité des salariés.

Les solutions WatchGuard permettent d'éviter ces comportements sans pour autant se priver de l'aspect pratique de ces outils. Si le filtrage peut être configuré par rapport à une application ou à un type de terminal, il peut également l'être selon certains créneaux horaires ou en fonction de l'utilisateur. Le contrôle applicatif peut, en effet, être affiné sur des groupes identifiés dans l'annuaire LDAP ou Active Directory et ainsi laisser les équipes marketing accéder aux réseaux sociaux, les divisions financières aux applications comptables ou le support informatique utiliser un de ces outils de prise en main à distance. « La sécurité, c'est passer son temps à gérer les exceptions ». ■