

Stream Scanning
Le Scan à la Volée NETGEAR®

Introduction

La prolifération des technologies Web 2.0 a considérablement renforcé le rôle de l'Internet dans l'activité des petites et moyennes entreprises. Cependant, ces technologies ont également permis le développement de nouvelles stratégies d'attaque, la connectivité généralisée offrant aux pirates un vaste champ d'application, ces derniers comptant également sur la confiance des internautes dans les systèmes de sécurité. Les sites d'échange peer-to-peer favorisent le partage de fichiers en masse entre utilisateurs anonymes ; accepter l'installation d'un plug-in pour visualiser le contenu d'un site donné dans un navigateur est devenu très courant ; les sites des réseaux communautaires les plus populaires ont habitué leurs utilisateurs à cliquer en toute confiance sur les liens contenus dans le corps des e-mails. La banalisation de la navigation sur Internet a créé des boulevards que les pirates n'ont qu'à exploiter.

Selon une récente étude Gartner, en 2007 le nombre de menaces hébergées sur le Web a augmenté de 800 % et l'on a dénombré plus de 275 cas de vulnérabilité des navigateurs aux plug-ins. Une autre étude récente a révélé que 79 % des menaces véhiculées par le Web sont hébergées par des sites légitimes qui ont été piratés et infectés. Les 21 % restants concernent des menaces identifiées sur des sites malveillants auxquels les concepteurs ont offert une apparence respectable attirant principalement les victimes de ces attaques grâce à des campagnes de "marketing" e-mail.

Le Défi

L'Internet est désormais au coeur des activités quotidiennes des petites et moyennes entreprises, le courrier électronique et la navigation Web représentant 90% de leurs applications critiques. Si la plupart des entreprises ont conscience que leur réseau est susceptible d'être infiltré par des malwares (programmes malveillants) véhiculés par le trafic Web, la majorité n'a pas pris la mesure du problème.

En moyenne, les fournisseurs de solutions de sécurité reçoivent chaque jour plus de 20 000 échantillons de malwares différents, et plus de la moitié de toutes les menaces réseau dont ils ont connaissance ont été véhiculées par HTTP. De plus en plus, il suffit qu'un utilisateur se connecte à une messagerie Web ou qu'il visite un site pour qu'il se retrouve infecté par un cheval de Troie ou un spyware (logiciel espion) hébergé sur l'Internet. Le courrier électronique est également une source non négligeable de malwares. L'e-mail est souvent utilisé pour attirer l'utilisateur jusqu'à une attaque hébergée sur le Web.

Le nombre croissant de menaces véhiculées par l'Internet a rendu indispensable le développement d'une solution de sécurité réellement fiable au niveau de la passerelle, qui analyse à la fois le trafic entrant et sortant pour détecter et supprimer les menaces avant qu'elles n'atteignent le poste de travail des utilisateurs. Pourtant, sécurité élevée et connexion réseau ont toujours été difficilement compatibles, car généralement, l'amélioration de la sécurité suppose une dégradation des performances. Les utilisateurs exigent de la rapidité, tout particulièrement pour la navigation Internet. Si l'adoption d'une solution de sécurité Web implique une latence, des temps d'attente trop importants, les utilisateurs seront les premiers à s'en plaindre.

Batch-Scanning contre Stream Scanning

La plupart des solutions de sécurité, du PC jusqu'à la passerelle, utilisent la technologie du "batch-scanning", le scan par lots de données. Cette méthode signifie que l'analyse commence uniquement après réception complète du fichier, et que la restitution ne peut commencer que lorsque l'analyse complète du fichier est terminée (voir Figure 1). Par conséquent, pour l'utilisateur final, cela implique souvent un temps d'attente important, voire même parfois des dépassements de délai pendant le transfert et l'analyse du fichier.

La technologie du batch-scanning a été élaborée à une époque où les virus se propageaient par les supports amovibles. Elle emploie donc des algorithmes qui partent du principe qu'un accès aléatoire au volume à analyser est possible. Cette technologie s'est révélée réellement efficace pour ce type de support. Cependant, appliquée aux menaces véhiculées par le trafic Web en temps réel, cette approche déjà ancienne implique un niveau de latence inacceptable.

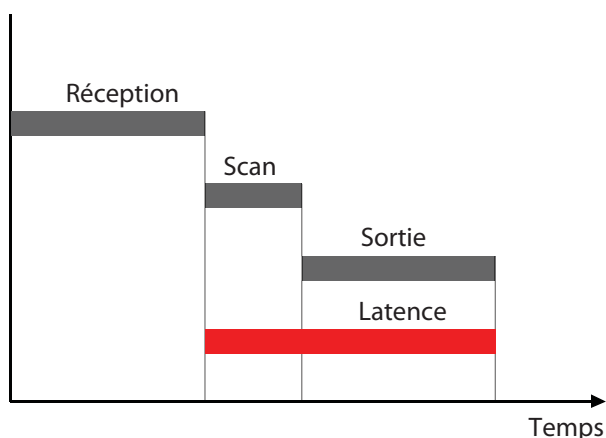


Figure 1 : Batch-Scanning Classique

À l'inverse, le Stream Scanning (scan à la volée) s'appuie sur la simple observation que le trafic réseau circule par flux. Plutôt que d'attendre l'arrivée d'un fichier complet, le moteur de Stream Scanning NETGEAR lance la réception et l'analyse du trafic dès l'entrée du flux sur le réseau (voir Figure 2). Lorsqu'un nombre minimum suffisant d'octets a été reçu, le scan peut commencer. Le moteur de scan poursuit son analyse dès que des octets supplémentaires sont disponibles, tandis qu'un autre processus restitue les octets analysés. Ce traitement multiple en simultané permet de réaliser un scan complet avec un impact minimal sur les performances du réseau. Cette méthode de scan des fichiers est bien plus rapide que celle des solutions de sécurité classiques, la progression des performances est indubitable. La technologie de Stream Scanning NETGEAR offre également un niveau d'évolutivité élevé: le gain en performance s'accroît à mesure qu'augmente le volume du trafic. Les structures peuvent ainsi faire face à un pic du trafic, comme il s'en produirait dans l'éventualité d'une attaque Web.

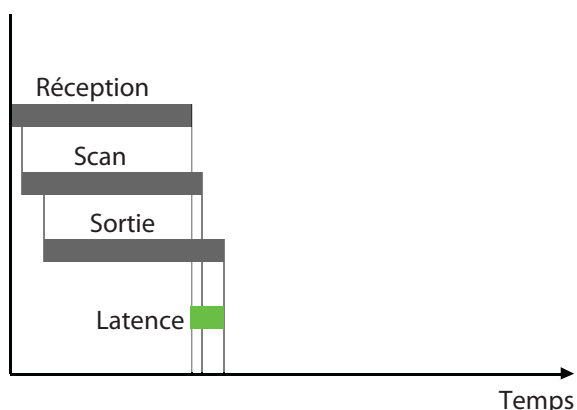


Figure 2 : Stream-scanning NETGEAR

La technologie de Stream Scanning NETGEAR a été soumise à des tests comparatifs exigeants. Les résultats sont unanimes: la technologie NETGEAR est toujours cinq fois plus efficace que les solutions classiques traitant le trafic par lots. Elle a été appliquée avec succès dans de nombreux secteurs industriels : administrations publiques, santé, commerce... le déploiement concernant de petites structures de moins de 50 utilisateurs mais également des réseaux très étendus géographiquement et comportant des milliers d'utilisateurs. Quelle que soit la taille du réseau, la technologie de Stream Scanning NETGEAR apporte une protection complète à la pointe du progrès, pour faire face aux menaces Web et e-mail avec la garantie d'un niveau de latence minimal.

Conclusion

Dans un environnement professionnel dynamique, les petites et moyennes entreprises doivent aujourd'hui arbitrer entre connexion réseau et sécurité. Les solutions de sécurité doivent impérativement mettre l'entreprise à l'abri de la vague incessante des menaces véhiculées par Internet, sans pour autant étrangler le flux des communications. L'architecture de la technologie de Stream Scanning NETGEAR, en attente de brevet, répond à cette exigence de compromis. NETGEAR propose le scan d'un volume important de trafic réseau pour détecter en temps réel les atteintes à la sécurité, sans impact majeur sur l'efficacité des communications réseau de l'entreprise.

NETGEAR ProSecure STM : Solution de management des menaces Web et E-mail

Le boîtier ProSecure STM fait appel à une technologie exclusive qui détecte et bloque les attaques de façon appropriée à la rapidité et à l'étendue de leur propagation. Par cette approche, il est possible de détecter le spam et les attaques de malwares dès leur apparition, et de bloquer en temps réel tous les messages associés.

Le boîtier ProSecure STM intègre la technologie Netgear de Stream Scanning (Scan à la Volée), en attente de brevet, qui permet d'analyser les flux de données au moment où ils entrent sur le réseau. Grâce à la technologie Stream Scanning, les boîtiers NETGEAR STM peuvent traiter un volume important de données en temps réel, une seule analyse suffisant pour identifier le spam, les malwares, les atteintes à la sécurité ou les applications inappropriées. Il est ainsi possible de garantir aux utilisateurs du réseau un contenu e-mail et Web sûr, sans temps d'attente.

Le boîtier ProSecure STM utilise un système de défense comportemental et proactif qui supprime l'intervalle existant jusqu'alors entre l'exploitation d'une vulnérabilité et sa correction. La solution NETGEAR intègre une analyse chirurgicale qui permet d'identifier les caractéristiques suspectes du trafic réseau entrant et sortant, et de les neutraliser jusqu'à ce qu'elles puissent être examinées de manière approfondie.

