L'UTM de Seconde Génération

Conçu pour répondre aux attaques du début de la décennie, l'UTM de première génération n'est plus adapté à la protection des nouvelles applications d'entreprise : convergence voix/données, flux temps réel, travail collaboratif et autres services Web 2.0. Une nouvelle architecture d'UTM, à base de processeurs réseaux multicoeur, s'impose pour assurer le traitement en profondeur des échanges à très haut débit.

ARKOON
NETWORK SECURITY

Le malware actuel contourne l'UTM classique

Polymorphe et orienté profit, le code malveillant actuel se joue des passerelles de sécurité, pare-feu réseau et équipements de prévention d'intrusions traditionnels. Une nouvelle stratégie d'analyse des flux s'impose.

La première génération d'UTM (Unified Threat Management), cet équipement de sécurité tout-en-un incluant coupe-feu, antivirus et VPN, a été conçue pour bloquer les attaques de la première moitié de la décennie. Elle est obsolète à présent car son principe de fonctionnement et ses facultés ne correspondent plus aux nouvelles menaces.

Les codes malveillants d'aujourd'hui sont furtifs et nuisibles aux activités de l'entreprise ; ils provoquent un déni de service, défigurent les pages du site Web ou bien dérobent des informations et des documents confidentiels. A présent polymorphes, ils se dissimulent dans la profondeur et la complexité des applications, pour rendre leur détection plus complexe. Désormais tourné vers le profit et la revente d'informations et de documents privés, le malware est un outil au service du crime organisé.

La visioconférence est l'une des applications qui requiert un délai de latence réseau proche de zéro. (*DR : Cisco)*

Des menaces plus complexes

Dans l'entreprise, le comportement des utilisateurs n'est plus nécessairement en cause. Inutile d'ouvrir une pièce jointe pour être contaminé. Désormais, plus de 95% des malwares se diffusent sur Internet. Chaque jour, chaque internaute peut se trouver confronté, à son insu, à une page Web infectée, hébergée sur un réseau social ou sur un site compromis, lâchant son venin sur tous les visiteurs.

Une nouvelle génération d'équipement de sécurité doit prendre la relève pour bloquer ces menaces complexes et leurs prochaines mutations.

L'UTM de seconde génération relève le défi, en inspectant en profondeur les services et leurs contenus, en décodant en temps réel les protocoles et en vérifiant le comportement des sessions applicatives les unes par rapport aux autres. Son architecture multicœurs et ses logiciels embarqués protègent le réseau d'entreprise du malware moderne.

A nouvelles applications, nouvelles brèches

De nombreux vers comme nimda ou sasser ont provoqué de sérieux dégâts sur les réseaux d'entreprises non protégées par une passerelle de sécurité ou un boîtier UTM de première génération.

A présent, les nouvelles applications redistribuent la donne.

Les communications unifiées et la convergence voix/données ont induit une nouvelle génération de menaces qui jouent sur les particularités des services temps réel comme la voix, la téléphonie, la vidéo. Ces applications très sensibles au deni de service sont plus exposées que les autres.

Dans le même temps, le Web est en pleine mutation. Alors qu'il y a encore quelques années, il n'était qu'une vitrine, il devient interactif, communautaire, partagé et les technologies Web 2.0 comme Ajax apportent une convivialité et une interactivité nouvelles aux services en ligne. Hélas, à l'instar des sites sociaux, elles ouvrent autant de brèches dans le système d'informations que de nouvelles perspectives pour les utilisateurs (lire le tableau ci-dessous). La convivialité et l'interactivité proposées aux utilisateurs nécessitent des applications qui encapsulent des mécanismes de plus en plus complexes créant autant de vulnérabilités exploitables pour un attaquant.

L'entreprise prend conscience de ces nouvelles failles. Elle entend les combattre avec des parades automatisées, des boîtiers simples à installer et à administrer qui soient adaptés aux traitements des nouveaux flux en temps réel.

MENACES WEB 2.0	PRÉCISIONS	CONSÉQUENCES POSSIBLES
Remote file inclusion	Exécution de scripts profitant d'une vulnérabilité de php	Défiguration de site web
SQL injection	Accès frauduleux aux SGBD par séquences d'échappement	Détournement de bases de données, d'annuaires
Cross-site scripting	Script malicieux transmis à l'insu de l'utilisateur	Vol de cookie ou d'informations confidentielles
Path traversal	Accès frauduleux aux répertoires non publics du serveur	Détournement de bases de données, d'annuaires
Code injection / Feed injection	Ajout de traitements nocifs via un flux de données	Propagation de vers, virus, spams, vol d'informations
Social engineering	Vol de l'identité/mot de passe en jouant sur la confiance de la victime	Accès illicite aux systèmes d'information

Les principales failles web 2.0 auxquelles l'entreprise est confrontée.

L'environnement de l'UTM évolue

Lorsque les premiers boîtiers UTM ont été commercialisés, il s'agissait surtout de bloquer les virus, les vers, les chevaux de Troie et les courriers non sollicités ainsi que plusieurs attaques protocolaires, déjà identifiées, maîtrisables par les règles d'un pare-feu réseau.

La mise à jour régulière de l'UTM permet d'actualiser son niveau de sécurité face à de telles menaces. Mais le processus reste statique : lorsqu'un nouveau malware est identifié, on l'inscrit en tant que nouvel enregistrement d'une liste noire ou dans une base de signatures virales. L'actualisation de la base contribue à mieux filtrer les messages électroniques et les flux IP entrants sur le réseau de l'entreprise. Elle évite la propagation des derniers codes malveillants statiques, mais laisse passer les codes dynamiques et polymorphes.

La contrefaçon de site web permet aux hackers de recueillir les informations confidentielles des internautes.

L'UTM doit gagner en intelligence pour bloquer les menaces des nouvelles applications. Il ne peut plus seulement comparer des photographies de codes (des signatures) mais doit observer plusieurs films en parallèle. Il doit analyser les échanges dynamiques, au travers d'un examen des flux mené en temps réel. Il doit regarder les applications en profondeur, décoder les protocoles et faire la corrélation entre les différents flux pour détecter les comportements malicieux et les codes malveillants.

Des trafics à distinguer

Pour y parvenir, une nouvelle réserve de puissance devient nécessaire. Il s'agit, en effet, de reconnaître des trafics (souvent encapsulés) afin de bloquer d'éventuelles attaques, connues ou non, en temps réel. Et, cela, sans générer de fausse alerte. Par exemple, si un canal de communication vers l'extérieur est ouvert par un service d'agrégation d'informations - un mashup sensé délivrer des actualités ou des tableaux de chiffres -, on peut craindre une injection de code malicieux qui cherchera à capter ces informations, à en extraire d'autres, à modifier le comportement de l'application à l'insu de l'utilisateur et de l'entreprise.

Une seconde génération d'UTM s'impose

Les équipements du réseau d'entreprise sont désormais conçus pour traiter des échanges en temps réel.
En moins de cinq ans, les échanges d'informations sur le réseau d'entreprise ont changé de façon radicale. De gros fichiers multimédias et plusieurs flux temps réel remplacent les transferts asynchrones de petits volumes. Cette évolution fait apparaitre trois changements qui perturbent les équipements du réseau et de sécurité.

Relever le niveau de sécurité

Premièrement, les applications de streaming en temps réel utilisent des paquets de données plus petits, ce qui accroît le travail d'inspection des entêtes. Deuxièmement, le contenu doit être analysé à la volée, sans interrompre ni ralentir les flux de données. L'approche 'store-and-forward' d'analyse des contenus (antivirus, antispam...) retenue pour examiner les transferts d'e-mail et les échanges web ne fonctionnera pas pour le trafic en temps réel. Enfin, le caractère temps réel de ces applications leur confère une sensibilité extrême au déni de service. En effet, la perte d'un paquet (ou d'une information) dans une connexion VoIP peut rapidement rendre la communication inaudible et donc engendrer un déni de service. Cette hyper sensibilité rend nécessairement ces nouvelles applications plus vulnérables.
Les échanges menés sur le réseau, en temps réel désormais, impactent aussi la planification et le déploiement des équipements. Les pannes du réseau réduisent la productivité ; par conséquent, l'objectif de toute direction informatique devient l'activité continue. De nouvelles technologies clé concernent l'infrastructure dynamique, la redondance d'équipements et la bascule à chaud qui doivent être soutenues par les appliances modernes pour garantir des niveaux de services constants.

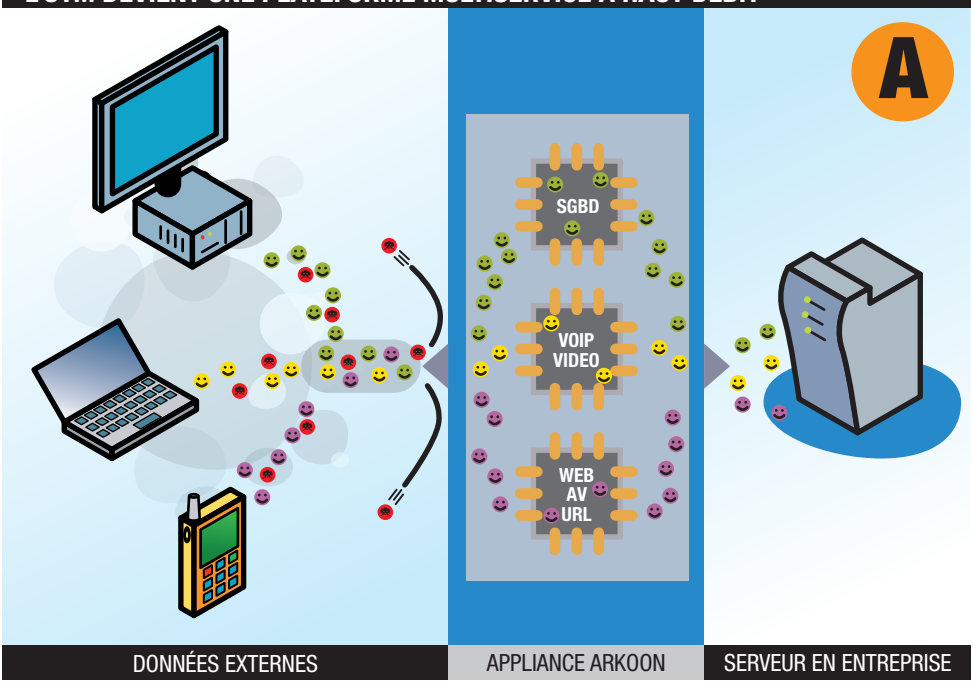
Pour en finir avec les interruptions non plannifiées

Dans l'univers temps réel, le responsable des infrastructures dépend d'outils de supervision visuels et ergonomiques lui permettant de conserver le contrôle de son réseau. Une gestion des configurations garantit le déploiement cohérent des règles de sécurité au travers du réseau global. Une gestion habile des alertes évite l'avalanche de notifications lorsqu'un problème intervient en un point précis du réseau. Les événements sont journalisés et sauvegardés dans des bases de données où des outils d'extraction viennent puiser les informations nécessaires aux audits et à l'analyse après incident.

L'architecture multicœur amplifie l'UTM

Les appliances de sécurité réseau reposent, de façon historique, sur des architectures x86. L'emploi d'une plateforme banalisée a permis de maintenir les coûts au plus bas. Les fournisseurs ont pu ainsi concentrer les investissements R&D sur la sécurité du réseau plutôt que sur le développement matériel et ses évolutions.
L'architecture Intel remonte, néanmoins, à une période où tout ce qui était placé derrière l'unité centrale pouvait être considéré comme des périphériques, mémoire RAM et disques durs inclus. Les performances d'Entrées/Sorties n'étaient pas prioritaires, le réseau local le plus surchargé ne dépassant pas le débit de 10 Mbps.
A présent, les réseaux multi-gigabit exigent des matériels capables de traiter de grands volumes d'informations en temps réel. Le goulet d'étranglement des Entrées/Sorties de l'architecture x86 classique ne peut plus être contourné.

L'UTM DEVIENT UNE PLATEFORME MULTISERVICE À HAUT DÉBIT

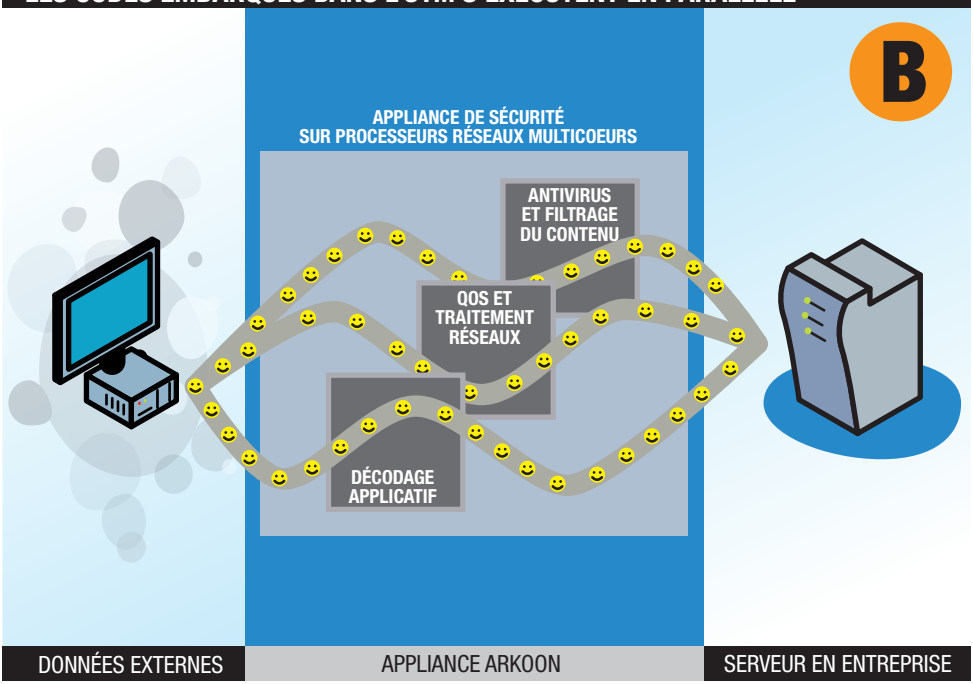


Une bonne réponse réside dans le processeur réseau. Conçu spécifiquement pour un traitement efficace des paquets de données des trafics réseaux, ce microprocesseur y délivre des performances largement supérieures aux appliances de sécurité x86. Les processeurs réseaux multicœur rehaussent encore le niveau. Ils deviennent une nouvelle fondation pour structurer les appliances de sécurité des années à venir.

A Les postes de travail soumettent des requêtes de données et des appels téléphoniques via l'UTM qui doit reconnaître chaque connexion pour la filtrer de façon adéquate, sans délai de latence.

B Grâce à un décodage protocolaire et applicatif, les sessions sont reconnues et les mauvais comportements sont isolés, tandis que les contenus sont filtrés simultanément

LES CODES EMBARQUÉS DANS L'UTM S'EXÉCUTENT EN PARALLÈLE



Siège social
1 Place Verrazzano
CS 30603
69258 Lyon Cedex 09
Tél : +33 (0)4 72 53 01 01
Fax : +33 (0)4 72 53 12 60

Ile de France
Immeuble Le Pelissier
220 Av. Pierre Brossolette
92240 Malakoff
Tel : +33 (0)1 57 63 67 00
Fax : +33 (0)1 57 63 67 37

www.arkoon.net

Un livre blanc réalisé par speedfire www.speedfire.com