Image: emojoez/shutterstock.com

Dossier

Sécurité informatique holistique

En collaboration avec **Boll Engineering**

Vue à 360° pour plus de sécurité

jor. Le cyberespace est un endroit dangereux. Les pirates informatiques les plus doués trouvent chaque jour de nouvelles méthodes pour infiltrer les ordinateurs de leurs victimes. Les experts en sécurité sont tout aussi ingénieux, mais ils sont notoirement à la traîne derrière les hackers. Et il n'est pas possible de compter uniquement sur un firewall. Si une entreprise travaillant avec des données sensibles souhaite se protéger au mieux, elle doit faire appel à la gestion unifiée des menaces (UTM), comme l'explique Patrick Michel, Principal Consultant chez le distributeur de solutions de sécurité informatique Boll Engineering (à lire en page 38).

Que l'on déploie un boîtier physique ou une appliance virtuelle, peu importe: seule une approche à 360° peut combattre les cyber-menaces, souligne Patrick Michel en interview (page 40). Il y définit quelles sont les cyber-menaces les plus graves, ce qui peut être fait et qui pourrait être intéressé par une appliance UTM. Il explique également comment l'UTM peut être mis en œuvre sans sacrifier les performances et pourquoi l'approche *best of breed* n'est pas la meilleure stratégie pour les PME.

Sécurité IT à 360°: combler les failles de sécurité et stopper les menaces

Les appareils UTM évoluent constamment. Ces solutions qui sont équipées d'un ensemble complet de fonctionnalités, sont synonymes de sécurité informatique globale: elles offrent une gestion WLAN intégrée et deviennent le centre de contrôle de l'ensemble du réseau de l'entreprise.

L'AUTEUR

Patrick Michel
Principal Consultant,
Boll Engineering

La sécurité des réseaux est un facteur déterminant pour toutes les entreprises, qu'il s'agisse d'une PME ou d'une grande entreprise. La pierre angulaire de tout concept de sécurité est le firewall: les modèles conventionnels Layer-4 fonctionnent sur le principe d'ouverture ou fermeture de ports réseau spécifiques aux règles définies pour chaque connexion.

L'UTM apporte une sécurité complète

Cependant, un firewall de base ne suffit pas à écarter les menaces de plus en plus sophistiquées. Cela nécessite des appareils UTM (Unified Threat Management). Un grand nombre de fonctions de sécurité sont combinées dans un système puissant. Les composants UTM typiques sont l'antivirus et l'antispam, le VPN, la détection et la protection contre les attaques (IDS/IPS) ainsi que le filtrage des URL pour bloquer les adresses Web dangereuses. Les appliances UTM sont disponibles auprès d'entreprises telles que Fortinet et WatchGuard, souvent sous forme d'appliances virtuelles ou de Software-as-a-Service.

Au fil du temps, de nouvelles fonctions ont été ajoutées aux fonctionnalités UTM classiques. Il s'agit notamment d'un firewall applicatif, également connu sous le nom d'Application Control ou firewall Layer-7. Dans ce cas, l'appliance UTM assure également l'autorisation ou le blocage ciblé d'applications, de services Web et de services réseau.

Image: matejmo / iStock.com

Détection de contenu malveillant crypté et inconnu

Une autre fonctionnalité UTM plus récente et particulièrement importante est le SSL-Scanning. Lors de la navigation sur le Web, de l'échange de courriels et de l'utilisation d'applications Web, les connexions cryptées par SSL sont pratiquement la seule option. Mais le firewall classique ne peut pas analyser le trafic crypté – y compris le code malveillant, les URL dangereuses et autres contenus indésirables.

Les antivirus, les filtres Web et autres protections n'ont de sens que si les données sont ouvertes et lisibles. Pour ce faire, l'appliance UTM doit rompre le cryptage SSL et ré-encrypter les données après l'analyse. Ce processus est appelé SSL Scanning. Techniquement, l'analyse SSL fonctionne comme suit: l'appliance UTM interrompt de manière transparente la connexion SSL entrante. Après l'analyse, elle établit une nouvelle connexion SSL avec le destinataire. Pour ce faire, elle doit générer un nouveau certificat pour le client sur la base de son propre certificat CA installé sur l'appareil. Ce processus, qui se répète à chaque session utilisateur, nécessite également un effort de calcul. De plus, le certificat CA de l'appareil UTM doit être inclus dans la liste des certificats de confiance de tous les clients. L'analyse SSL a donc également un effet sur la gestion des clients. Idéalement, les clients utilisés sont gérés de manière centralisée afin que les utilisateurs n'aient pas à confirmer le certificat CA manuellement.

Le sandboxing, une autre fonctionnalité UTM récente, peut également être utilisé pour détecter les codes malveillants qui n'ont pas été détectés comme nuisibles par le moteur antivirus. Les fichiers avec du code actif sont exécutés dans un environnement virtuel isolé. Un fichier n'est transmis que si aucune action dangereuse ne s'est produite. Le sandbox étant très gourmand en ressources CPU, les appareils UTM utilisent généralement le cloud pour ce service. Comme le processus prend du temps, le sandbox est particulièrement adapté aux pièces jointes d'e-mails qui ne sont de toute façon pas délivrées en temps réel.

Se défendre contre les invités indésirables

Certains appareils UTM disposent d'un firewall géo-IP, également connu sous le nom de géoblocage. Cela permet de bloquer complètement les communications en provenance de certains pays. Par exemple, si vous ne voulez pas servir des clients asiatiques dans votre boutique en ligne, vous pouvez le faire en les bloquant géographiquement. Cependant il n'est pas toujours logique de bloquer

Image: ipopba / iStock.com

certains pays afin de prévenir un éventuel piratage informatique. Les pirates n'opèrent pas nécessairement via les systèmes du pays dans lequel ils se trouvent.

Le blocage d'adresses IP spécifiques en fonction de leur réputation est similaire au géoblocage. Les fournisseurs d'UTM tiennent à jour des listes de systèmes identifiés comme dangereux. Un bon exemple est l'adresse IP des botnets.

Le réseau sous contrôle

Certains fabricants d'UTM ont intégré un contrôleur sans fil dans leurs appareils en plus des fonctions de sécurité. L'appliance UTM gère donc également tous les aspects du WLAN, qui bénéficie ainsi de la même sécurité que le LAN. Par exemple, le contrôleur sans fil de l'appareil UTM vous permet d'utiliser la norme de sécurité WPA Enterprise. Lorsque la connexion est établie, non seulement la *Pre-shared Key* est vérifiée comme pour le WPA2, mais aussi le login utilisateur. Cela rend le WLAN plus sûr. Bien que cela soit également possible avec des solutions sans fil dédiées, l'intégration directe dans un firewall simplifie l'administration et l'utilisation de ces fonctions. Les appareils UTM avec contrôleurs sans fil intégrés sont particulièrement adaptés aux PME et aux sites distants.

Une autre caractéristique récente des appareils UTM est le SD-WAN. L'appareil peut combiner plusieurs ports Internet en une seule connexion VPN redondante et facile à configurer avec basculement automatique. Cela vous permet de remplacer un réseau privé MPLS coûteux, par un accès Internet plus accessible.

Fortinet est le premier fabricant à aller plus loin: outre la sécurité et le contrôleur sans fil, la gestion intégrée des switches permet de gérer l'ensemble de la structure réseau via l'interface de l'appareil UTM. Par exemple, les subdivisions logiques du réseau (VLAN) peuvent être définies directement via l'interface de l'UTM, simultanément sur le firewall et sur les switches. Auparavant, un VLAN devait être configuré séparément sur les deux systèmes. L'intégration permet également de visualiser l'ensemble du réseau jusqu'au Endpoint. Il en résulte une vue d'ensemble sans précédent: tous les environnements – LAN, WLAN et sécurité – peuvent être exploités de manière uniforme.

UTM – Même sans matériel

Presque tous les fournisseurs d'UTM offrent leurs solutions non seulement sous la forme de périphériques matériels, mais aussi sous la forme d'appliances virtuelles qui peuvent être exploitées dans son propre datacenter ou dans un environnement cloud tel que AWS ou Azure. Chaque fournisseur dispose de services cloud et fournit un service UTM sous forme de Software-as-a-Service. L'un des avantages est que les employés mobiles sont également intégrés sans effort et que le même niveau de sécurité est garanti partout. Aucun matériel ne doit être installé et géré localement. L'accès au réseau et la gestion des fonctions de sécurité se font via une interface Web.

Presque tous les fournisseurs UTM offrent leurs solutions non seulement sous la forme de périphériques matériels, mais aussi d'appliances virtuelles.

«Un framework de sécurité intégré crée une sécurité globale»

Patrick Michel, Principal Consultant chez BOLL Engineering, distributeur de solutions de sécurité informatique, parle dans cette interview des aspects de la sécurité des réseaux et de la façon dont une approche à 360 degrés peut combattre efficacement les cybermenaces. Interview: Joël Orizet

La cybersécurité est l'un des «Hot Topics» depuis des années. A quels dangers les entreprises sont-elles confrontées?
Les cybercriminels saisissent toutes les occasions d'attaquer les réseaux d'entreprise et de causer des dommages – de l'espionnage de secrets industriels au chantage à l'aide de ransomwares, en passant par l'utilisation des ressources informatiques à leurs propres fins ou encore la paralysie de l'entreprise toute entière. Les attaques deviennent de plus en plus sophistiquées – et de nouvelles méthodes d'attaque sont constamment imaginées.

Comment les différentes menaces peuvent-elles être combattues avec succès?
D'une part, les entreprises doivent déterminer où se situent les plus grands risques et comment s'en servir pour réaliser leurs investissements. D'autre part, presque toutes les entreprises utilisent des firewalls pour protéger et segmenter leurs réseaux ou datacenters. Ils assurent également la protection des clients. Les fonctions utilisées vont du simple firewall et de l'analyse de contenu au SD-WAN. La liste s'allonge et les fonctions de sécurité informatique deviennent de plus en plus complexes. L'utilisation des différentes fonctions dépend des vecteurs d'attaque contre lesquels le firewall doit protéger. Les appliances UTM avancées qui offrent une approche intégrale ou une fusion transparente de mécanismes complémentaires sont réunis sur une seule plate-forme.

Les appareils UTM ont de nombreuses fonctions. Comment parvenir à une sécurité efficace sans sacrifier les performances?
Fortinet, le fournisseur de solutions de sécurité IT, apporte une réponse intelligente à cette question. Ce dernier garantit la performance de ses systèmes grâce à des processeurs ASIC dédiés, qui déchargent le CPU des fonctions particulièrement gourmandes. Une combinaison qui garantit des performances suffisantes à un prix attractif, même dans des environnements exigeants.

Les appareils UTM sont-ils principalement destinés aux PME ou répondent-ils également aux besoins des grandes entreprises?
Les fabricants de firewalls pour entreprise implémentent généralement un sous-ensemble de fonctions UTM communes dans leurs plates-formes et ne sont généralement pas adaptés au marché des PME. Ensuite, il y a les fabricants qui n'offrent que des firewalls UTM pour les PME. Enfin, il existe des fabricants tels que Fortinet qui s'adressent à tous les segments avec une seule plate-forme.

Quels sont les aspects qui plaident en faveur des appareils UTM par rapport à une approche *best of breed*?
Les appareils UTM offrent de nombreuses fonctions dans un seul appareil, ce qui en fait la solution parfaite pour les PME exigeantes avec des budgets limités. Il convient également de noter que la connexion directe des points d'accès sans fil, des switches et des logiciels de protection Endpoint aux firewall UTM est de plus en plus courante. Il en résulte la solution Security Fabric. Cela simplifie l'administration et offre des fonctions de sécurité et d'automatisation jusqu'au niveau des ports de communication et des postes client. Les PME bénéficient ainsi de fonctions de sécurité qui ne seraient disponibles que par le biais de solutions *best of breed* bien plus coûteuses. Il s'agit d'un facteur important étant donné la complexité et la fusion croissantes du réseau et de la sécurité.

«Les appareils UTM offrent de nombreuses fonctions dans un seul appareil, ce qui en fait la solution parfaite pour les PME exigeantes avec des budgets limités.»

Patrick Michel, Principal Consultant, Boll Engineering

Presque tous les fournisseurs UTM proposent également leurs solutions sous forme d'appliances virtuelles pouvant être exploitées dans un environnement cloud. Qu'en pensez-vous?
C'était et c'est toujours une évolution logique car la virtualisation des serveurs et les offres telles que l'Infrastructure-as-a-Service (IaaS) sont de plus en plus courantes. En fin de compte, des firewalls sont également nécessaires. Comme ils ne peuvent pas être installés physiquement, des logiciels applicatifs sont utilisés. Aujourd'hui c'est une norme.

Que pensez-vous des fournisseurs de Software-as a-Service qui offrent des fonctionnalités classiques de firewall UTM dans le cloud?
Il s'agit d'une approche passionnante et d'une étape logique dans la forte cloudification des centres de données et des services. Je pense que les fournisseurs d'appareils plus classiques vont également dans cette direction. Ils se concentrent déjà sur la gestion cloud des appareils. L'étape suivante sera la fonctionnalité de firewall UTM dans le modèle cloud Software-as-a-Service.