SONICWALL

PRÉSENTATION : LA NÉCESSITÉ D'UNE SÉCURITÉ COMPLÈTE POUR VOS ACCÈS SANS FIL ET MOBILES

Détectez et prévenez les cyberattaques sur les réseaux câblés, sans fil et mobiles.

Résumé

De nos jours, les entreprises ont besoin de fournir à leurs employés un accès haut débit aux ressources sur des réseaux câblés, sans fil et mobiles.
Cependant, les cybercriminels se servent de chacun de ces vecteurs pour lancer des attaques évoluées reposant sur des menaces chiffrées et des attaques de type zero-day. Les entreprises peuvent perdre le contrôle de leurs données dans des environnements distants utilisant des réseaux sans fil et mobiles qui se connectent aux services Cloud. L'interruption de l'accès entraîne une perte de productivité, favorise le « shadow IT », ou informatique de l'ombre, et crée des brèches dans le système de sécurité de l'entreprise.

L'accès aux ressources en tout lieu

Les employés d'aujourd'hui sont nomades. Ils ont besoin d'accéder en permanence aux ressources de l'entreprise, où qu'ils soient, en utilisant l'appareil de leur choix. Les entreprises adoptent aussi le BYOD, l'Internet des objets, la mobilité et les projets Cloud. Pour rester compétitives, elles doivent fournir un accès transparent aux ressources sur tous les réseaux, qu'ils soient câblés, sans fil ou mobiles. Les réseaux câblés évoluent et passent à 2,5 Gb, 5 Gb et 10 Gb. Les appareils filaires ne sont toutefois pas les seuls à se connecter au réseau. Les terminaux varient des ordinateurs de bureaux aux ordinateurs portables, aux tablettes et aux smartphones. Avec le nombre croissant de terminaux BYOD et

> Non seulement l'accès doit être possible partout, tout le temps et sur n'importe quel appareil, il doit aussi être rapide et sécurisé.

IoT, jamais autant d'appareils n'ont été connectés au réseau de l'entreprise.

Les entreprises sont de plus en plus dépendantes de la connectivité sans fil haut débit dans leurs environnements. Les travailleurs mobiles et distants se connectent par le biais de VPN depuis leur domicile, des succursales, des bureaux partagés, des aéroports, des hôtels et des cafés. Par conséquent, les employés s'attendent désormais à la même expérience utilisateur et à un accès hautes performances, non seulement sur les réseaux câblés, mais aussi sur les réseaux sans fil et mobiles. Lorsque les employés sont en déplacement, ils ont besoin des mêmes applications professionnelles que quand ils sont connectés aux réseaux câblés au bureau.

Les cyberattaques utilisent les réseaux câblés, sans fil et mobiles

Si la connectivité haut débit en tout lieu est aussi importante pour les utilisateurs que les organisations, la sécurité des données qui transitent sur le réseau est cruciale. Au bout du compte, les organisations ont besoin d'étendre les fonctionnalités complètes de détection et de prévention des failles de sécurité de manière transparente sur les réseaux câblés, sans fil et mobiles.

Quel que soit le type de réseau, la plupart des attaques sont désormais chiffrées, ce qui constitue l'un des défis majeurs de la lutte contre les cyberattaques. La tendance au chiffrement TLS/SSL a le vent en poupe depuis quelques années. Le trafic Web a augmenté, tout comme le chiffrement. Le nombre de connexions Web est passé de 5 300 milliards en 2015 à 7 300 milliards en 2016, d'après le réseau SonicWall Capture Threat Network. La majorité des sessions Web détectées par le Capture Threat Network pendant l'année était chiffrée en TLS/SSL, ce qui représentait 62 % du trafic Web. Ce nombre continuera d'augmenter avec le nombre de sites utilisant le chiffrement pour sécuriser les connexions.

En outre, les menaces évoluées telles que les exploits zero-day et les malwares personnalisés prolifèrent. Les organisations de toute taille sont la cible de cybercriminels qui n'ont de cesse de chercher, trouver et exploiter les failles des logiciels vulnérables. Leur objectif est d'accéder aux réseaux, aux systèmes et aux données, souvent en causant de sérieux dégâts en quelques minutes. Pour mieux détecter ces menaces inconnues, les professionnels de la sécurité déploient des technologies de détection contre les menaces avancées, par exemple les sandbox virtuelles, qui analysent le comportement des fichiers suspects et repèrent les programmes malveillants dissimulés. Les menaces actuelles sont toutefois de plus en plus malignes. Les logiciels malveillants sont désormais conçus pour détecter la présence des sandbox virtuelles et se soustraire à leur vigilance. Les environnements de sandboxing actuels doivent être aussi complets et dynamiques que les menaces qu'ils cherchent à éradiquer. Aujourd'hui, il est devenu impératif de déchiffrer, analyser et sandboxer les fichiers suspects dans tout le trafic sur tous les réseaux, qu'ils soient câblés, sans fil ou mobiles.

Travail d'équipe à distance

Les organisations peuvent perdre le contrôle de leurs données dans des environnements distants utilisant des réseaux sans fil et mobiles qui se connectent aux services Cloud. De nombreuses entreprises comptent des équipes distantes qui ont besoin d'utiliser des outils collaboratifs comme SharePoint ou Dropbox pour partager des fichiers et travailler en commun. Les collaborations de projets impliquent généralement des parties prenantes externes telles que des fournisseurs tiers ou des partenaires. Par exemple, les établissements d'enseignement primaire, secondaire et supérieur offrent aux élèves, étudiants et enseignants un accès sans fil à Internet pour travailler en collaboration localement et dans le monde entier.

Par conséquent, des fichiers sont constamment chargés ou partagés sur des ordinateurs portables ou des smartphones personnels (non gérés) par le biais de réseaux mobiles et sans fil. Dès que vous donnez la possibilité de partager des fichiers, des logiciels malveillants risquent d'être téléchargés. Cependant, lorsque les services informatiques adoptent des règles de partage de fichiers très restrictives pour des raisons de sécurité, les utilisateurs se mettent à utiliser leurs comptes personnels de partage de fichiers, comme Google Drive, pour transférer des documents et collaborer. Ces fichiers contournent les pare-feux quand les utilisateurs distants accèdent au réseau de l'entreprise par un accès VPN total. De plus, les organisations perdent le contrôle des données lorsqu'elles sortent du périmètre de sécurité avec les services Cloud publics comme Google Drive, les e-mails ou les clés USB. Cela représente un risque élevé en matière de sécurité et de conformité pour les organisations.

Performances réseau et productivité du personnel

Non seulement l'accès doit être possible partout, tout le temps et sur n'importe quel appareil, il doit aussi être rapide et sécurisé. La sécurité nécessaire face aux cybermenaces actuelles peut avoir un impact sur la productivité du personnel, accroître le budget informatique et augmenter le coût total de possession pour une entreprise.

Le volume croissant du trafic à lui seul affecte la bande passante disponible et les performances réseau. Le nombre d'appareils compatibles Wi-Fi, personnels ou mis à disposition par le service informatique, continue d'augmenter alors que la mobilité devient de plus en plus nécessaire et répandue. Selon Gartner, près de 1,5 milliard de smartphones ont été vendus rien qu'en 2016.[1] À la fin de la même année, la Wi-Fi Alliance prévoyait que les ventes de Wi-Fi dépasseraient les 15 milliards d'appareils.[2] La multiplication du nombre d'appareils Wi-Fi s'accompagne d'une augmentation de l'utilisation d'applications gourmandes en bande passante comme les applications multimédias HD, Cloud et mobile.

Le développement de l'IoT a favorisé l'augmentation du nombre d'appareils sans fil capables de prendre en charge les applications fortes consommatrices de bande passante. L'utilisation de la vidéo et des applications de collaboration comme Microsoft Lync, SharePoint et WebEx nécessite de larges volumes de bande passante pour fonctionner de manière optimale. De plus, le Cloud computing peut impliquer le transfert de fichiers volumineux sur le réseau sans fil, ce qui mobilise de la bande passante.

Par ailleurs, la multiplication des appareils a créé un environnement où les signaux sans fil interfèrent fréquemment entre eux en raison du grand nombre d'appareils partageant le même réseau. Cela comprend tous les appareils : ordinateurs portables, smartphones, tablettes et points d'accès, mais aussi micro-ondes, appareils Bluetooth, etc. Les performances médiocres qui en résultent sont un phénomène connu dans différents secteurs, dont la santé, l'éducation, les aéroports et les centres commerciaux. Le public s'attend désormais à bénéficier d'un réseau sans fil à l'extérieur dans les stades, les zones industrielles, sur les campus, les chantiers et autres espaces en plein air où le signal peut être affecté par l'environnement physique, dont les arbres et les autres bâtiments.

Les services de sécurité eux-mêmes ont un impact sur les performances réseau. La capacité à déchiffrer et analyser le trafic chiffré pour détecter les menaces, sans latence ou presque, revêt une importance critique. Tout retard ralentit le flux de données sur le réseau. Le déchiffrage et l'analyse simultanée de milliers de connexions Web chiffrées exigent une capacité de calcul considérable. Les pare-feux anciens peuvent déchiffrer le trafic et détecter les menaces dans une certaine mesure, mais sont incapables d'assurer la prévention. Ou alors ils peuvent effectuer toutes les tâches nécessaires, mais très lentement, en raison de la baisse des performances. Certaines organisations en arrivent même à désactiver des services de pare-feu essentiels afin de maintenir les performances.

Les organisations sont de plus en plus incitées à fournir à leurs clients, employés et étudiants une expérience améliorée sur toutes les plateformes. La technologie sans fil ultrarapide 802.11ac Wave 2 offre un débit de plusieurs gigabits. Cependant, pour exploiter son potentiel, le point d'accès et les appareils connectés doivent être compatibles avec le standard sans fil 802.11ac Wave 2. Pour permettre le débit sans fil requis, la plupart des pare-feux doivent également utiliser un port rétrocompatible 5 GbE ou 10 GbE nettement supérieur à la capacité nécessaire, ou ajouter un commutateur, ce qui augmente les coûts.

La plupart des organisations disposent d'un mélange d'applications sur site et dans le Cloud, d'où un environnement informatique hybride, ce qui complique encore les questions de performances et de sécurité. Le service informatique doit assumer les coûts liés au maintien de plusieurs répertoires utilisateurs pour les applications déployées sur leurs datacenters locaux ainsi que les applications Cloud SaaS tiers. Ces répertoires doivent être mis à jour en permanence pour garantir que les bonnes personnes ont bien accès aux bonnes applications au bon moment. Les utilisateurs sont obligés de garder et de se rappeler plusieurs URL et mots de passe, ce qui se traduit par de mauvaises pratiques de sécurité. Toute interruption de l'accès entraîne une perte de productivité, favorise le « shadow IT », ou informatique de l'ombre, et crée des brèches dans le système de sécurité de l'organisation.

Conclusion

Pour en savoir plus, découvrez comment détecter et prévenir les failles sur vos réseaux câblés, sans fil et mobiles. Lisez notre dossier, Meilleures pratiques de sécurisation des accès sans fil et mobiles, et rendez-vous sur notre page Web sans fil et mobilité.

[1] *http://www.gartner.com/newsroom/id/3609817*
[2] *http://www.wi-fi.org/news-events/newsroom/wi-fi-device-shipments-to-surpass-15-billion-by-end-of-2016*

À propos de nous

En 25 ans d'histoire, SonicWall a toujours été un partenaire industriel de confiance dans le domaine de la sécurité. De la sécurité réseau à celle des accès, en passant par la sécurisation de messagerie, SonicWall n'a cessé de développer son portefeuille de produits, permettant aux entreprises d'innover, d'aller plus vite et de croître. Avec plus d'un million d'appareils de sécurité en place dans près de 200 pays et territoires de par le monde, SonicWall permet à ses clients de dire en toute confiance oui à l'avenir.

Pour toute question concernant l'usage potentiel de ce document, contactez :

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Consultez notre site Internet pour de plus amples informations.
www.sonicwall.com

ExecBrief-NS-WhyYouNeed-US-IMAG-29144

SONICWALL®