La consolidation des fonctionnalités réseau et sécurité peut réduire la vulnérabilité des sites distants

Synthèse

Au fur et à mesure que les entreprises adoptent des initiatives de transformation numérique (DX) (cloud, Internet des objets [IoT] et mobile), leur surface d'attaque s'étend rapidement et le risque de violation augmente. Par exemple, les organisations distribuées ayant un ou plusieurs sites distants se tournent vers le SD-WAN. Mais le SD-WAN à lui seul ne résout pas trois problèmes de sécurité connexes : 1) la protection des multiples périphéries du WAN, 2) le manque de visibilité sur les périphériques et 3) la complexité de l'infrastructure des sites distants. Cependant, une solution qui consolide les fonctionnalités réseau et sécurité peut aider les responsables de l'ingénierie et de l'exploitation réseau à simplifier l'infrastructure tout en améliorant la sécurité et la productivité dans les sites distants. Une approche SD-Branch intégrée peut améliorer la visibilité, le contrôle et la facilité de gestion, tout en réduisant le coût total de possession pour les entreprises distribuées.

Table des matières

FORTINET

01 L'expansion de la surface d'attaque des entreprises distribuées

L'adoption de nouvelles technologies dans le cadre de la DX crée des complications uniques pour les organisations distribuées disposant de réseaux de sites distants.

Sécurisation de multiples périphéries de WAN. Il devient de plus en plus difficile de protéger la périphérie du WAN dans le réseau des sites distants. Cela commence par des volumes de trafic en croissance rapide — résultat d'un afflux d'applications SaaS (Software-as-a-Service), d'outils basés sur le cloud, de services VoIP (Voice-over-IP) et vidéo. Cela inclut aussi une multiplication des points d'accès sans fil, ainsi que du nombre et des types de dispositifs qui y accèdent. Cette évolution de la périphérie du WAN expose des vulnérabilités qui doivent être sécurisées.

La visibilité. Les réseaux des sites distants doivent également prendre en charge un plus grand nombre de périphériques (câblés et sans fil). Il s'agit notamment des divers appareils mobiles personnels des employés, des fournisseurs et des visiteurs, ainsi que d'un nombre et d'une variété croissante d'appareils IoT.

Il se peut que certains ne disposent pas de logiciels système entièrement patchés et/ou mis à jour (dans le cas de l'IoT) et qu'un grand nombre d'entre eux ne disposent pas du tout de fonctionnalités de sécurité intégrées. D'autant plus que, parmi ces dispositifs, tous ne sont pas visibles par les équipes d'exploitation réseau ou sécurité.

La complexité. Dans la plupart des entreprises, l'approche de facto de l'infrastructure s'est attaquée aux nouvelles fonctions réseau et aux failles de sécurité, l'une après l'autre, en ajoutant à chaque fois un nouveau dispositif. Avec le temps, cela crée des environnements extrêmement complexes. En particulier, le grand nombre de produits de sécurité individuels isolés qui se sont accumulés, sont devenus difficiles à gérer — en termes de coût et de temps — tout en laissant des lacunes dans la protection. De même, l'intégration des technologies dans les sites distants peut aussi nécessiter beaucoup de temps et de ressources.

Ici, les responsables de l'ingénierie et de l'exploitation des réseaux ont besoin d'une solution capable d'assurer la sécurité, les performances, la fiabilité et la disponibilité au sein du site distant. Une approche efficace de la sécurité réseau doit offrir des performances puissantes et évolutives tout en intégrant plusieurs fonctionnalités réseau et sécurité au sein d'une même offre. Cela nécessite également une architecture de sécurité réseau qui fournit des contrôles centralisés des politiques et une visibilité transparente sur toute la surface d'attaque.

02 La sécurisation de la périphérie du WAN

Le WAN traditionnel est devenu trop cher en raison d'une connectivité MPLS coûteuse combinée à des besoins croissants en bande passante et en trafic (en raison, par exemple, de l'utilisation dominante d'applications SaaS).

Le SD-WAN peut permettre la transformation digitale (DX) des sites distants avec des économies de coûts et des améliorations de performance. Mais pour y parvenir, la solution SD-WAN doit assurer la sécurité du réseau, sans oublier la performance.
Une solution SD-WAN efficace devrait :

- Regrouper des fonctionnalités réseau et sécurité disparates en une seule solution
- Offrir un déploiement « zero-touch » des réseaux de succursales pour un faible coût total de possession
- Employer une sécurité robuste intégrée aux pare-feux SD-WAN (sans avoir à acheter et gérer des appliances de sécurité séparées)
- Optimiser la bande passante du réseau (prise en compte des applications et prise en charge de multiples connexions à haut débit)
- Inspecter le trafic SSL/TLS (Secure Sockets Layer/Transport Layer Security) chiffré sans goulets d'étranglement, pour une productivité optimale des utilisateurs

Les prévisions de croissance du marché SD-WAN mondial annoncent un taux de croissance annuel composé (TCAC) de plus de 40% et le marché devrait atteindre les 4,5 milliards de dollars d'ici 2022.[1]

03 La sécurisation des périphériques

La sécurité exige aussi la capacité de voir, de catégoriser et de sécuriser tous les périphériques connectés — en particulier les périphériques IoT invisibles qui peuvent être déployés sans autorisation officielle des équipes réseau ou du service informatique. L'établissement d'une plate-forme unifiée à l'échelle de l'organisation peut en outre fournir une vue transparente de tous les périphériques connectés sur le réseau des sites distants.

Une fois que tous les périphériques du réseau sont découverts et visibles, les fonctionnalités de gestion centralisée de la solution SD-Branch devraient gérer de façon dynamique l'accès au réseau et appliquer des contrôles basés sur des règles, pour une sécurité cohérente pour tous les utilisateurs, applications et périphériques, y compris les périphériques IoT vulnérables. La solution devrait comprendre des contrôles d'accès automatisés (p. ex. pour mettre en quarantaine les dispositifs vulnérables ou suspects), ainsi que des capacités de détection des anomalies et d'intervention en cas d'incident, pour une correction rapide qui allège le fardeau du personnel informatique.

Les cybercriminels ont en ligne de mire les appareils IoT en périphérie de réseau des sites distants. On estime que 25% des attaques viseront des appareils IoT d'ici 2020.[2]

04 La sécurisation de la couche d'accès des sites distants

L'intégration de plates-formes WAN et LAN peut améliorer encore les performances et la sécurité du réseau. Pour simplifier l'infrastructure des sites distants, les responsables réseau peuvent regrouper de multiples appliances spécialement conçues pour les fonctions réseau (p. ex., routeurs, load balancers) et des fonctionnalités de sécurité spécifiques (p. ex., prévention et détection des intrusions).

La convergence des réseaux câblés et sans fil au sein d'un Next-Generation Firewall (NGFW) étend les fonctionnalités d'une solution SD-WAN sécurisée à la couche d'accès du site distant — combinant la sécurité NGFW, les commutateurs, les extensions de réseau et les points d'accès en une seule solution interopérable. Cette intégration réduit la complexité de l'infrastructure en simplifiant la gestion de la sécurité, de l'accès au réseau et du SD-WAN des sites distants. Elle élimine la multiplicité des fournisseurs, des interfaces et des systèmes d'exploitation, ce qui peut peser sur des ressources en personnel limitées, tout en effaçant les failles dans la défense sur les jonctions entre les différentes solutions.

Une solution efficace devrait permettre d'accroître l'agilité grâce à une interface à tableau de bord unique, ce qui améliore la visibilité et le contrôle du site distant. Elle devrait également prendre en charge le déploiement d'une solution « zero-touch » pour un meilleur coût total de possession.

Une entreprise utilise en moyenne plus de 75 solutions de sécurité différentes, dont beaucoup ne répondent qu'à une seule fonction ou exigence de conformité.[3]

05 La sécurité globale des sites distants

Les filiales d'entreprises accédant directement aux connexions Internet (via le SD-WAN), les responsables réseau doivent mettre en œuvre une sécurité nouvelle génération tout en permettant aux réseaux étendus à chemins multiples d'améliorer les performances des applications. Pour être efficace, le déploiement d'un site distant doit intégrer de manière transparente des fonctionnalités réseau et sécurité dans les domaines susmentionnés — périphérie du WAN, couche d'accès et périphériques.

Lors de l'évaluation d'une solution visant à optimiser la fonctionnalité globale du réseau d'un site distant et à améliorer la sécurité, les questions suivantes peuvent s'avérer utiles :

- La solution consolide-t-elle efficacement la sécurité et le réseau sur l'ensemble du site distant ?
- La solution offre-t-elle une visibilité transparente et un contrôle granulaire des appareils et des utilisateurs ?
- La solution propose-t-elle une console de gestion centralisée (tableau de bord unique) avec la possibilité d'appliquer des politiques globales ?
- Existe-t-il des certifications ou des essais tiers pour valider la performance, la fiabilité ou la valeur (coût total de possession) de la solution ?
- Les tests comprennent-ils une évaluation des performances pour des besoins spécifiques tels que les applications SaaS ou les performances VoIP/vidéo ?

[1] « SD-WAN Infrastructure Market Poised to Reach $4.5 Billion in 2022 », IDC, 7 août 2018.

[2] « 25% Of Cyberattacks Will Target IoT In 2020 », Retail TouchPoints, consulté le 21 mars 2019.

[3] Kacy Zurkus, « Defense in depth: Stop spending, start consolidating », CSO Online, 14 mars 2016.

FORTINET

www.fortinet.fr

419872-0-0-FR

novembre 14, 2019 12:41 PM

eb-branch-solution-research-FR