FICHE SOLUTION

Fortinet SD-Branch sécurise la périphérie des réseaux en succursale

Résumé

La transformation numérique (DX) a rendu les réseaux de succursales beaucoup plus complexes, et donc plus vulnérables. De nombreux fournisseurs en cybersécurité développent des produits spécifiques aux nouvelles menaces, à mesure qu'elles apparaissent. Mais cette approche complique les infrastructures des succursales, ce qui les fragilise et augmente les coûts. Pour résoudre ces problèmes, les succursales doivent veiller à l'intégration du réseau et de la sécurité au niveau de la périphérie WAN, de la couche d'accès et des endpoints. Fortinet SD-Branch consolide la couche d'accès au réseau en s'appuyant sur une plateforme offrant sécurité et visibilité sur le réseau et sur tous les appareils qui s'y connectent.

Gérer une surface d'attaque en expansion

L'adoption rapide des technologies DX (équipements connectés IoT, applications SaaS, outils vocaux/vidéo numériques et BYOD « bring-your-own-device ») a entraîné une expansion de la périphérie réseau, qui doit être sécurisée pour chaque succursale. À une heure où les réseaux se complexifient et impliquent des coûts plus importants, les produits de sécurité utilisés pour protéger l'infrastructure des succursales impliquent eux-aussi un certain nombre de complexifications et de surcoûts. Avec l'essor des équipements connectés IoT (appliances de bureau connectées, systèmes d'éclairage, climatisation et même produits de fitness personnels appartenant aux employés), de plus en plus d'appareils se connectent au réseau, souvent sans que la sécurité et la visibilité soient suffisantes.

64 % des décideurs informatiques estiment que leur entreprise déploient le SaaS plus rapidement qu'elles ne le sécurise.[1]

En 2020, plus de 25 % des cyberattaques devraient cibler les équipements connectés (IoT). Pourtant, moins de 10 % des budgets de sécurité informatique sont consacrés à la protection de ces appareils.[2]

Fortinet SD-Branch

Fortinet propose une approche globale, intégrée et automatisée de la sécurité réseau, à un rapport qualité-prix inégalé. Fortinet SD-Branch se déploie sans difficultés jusqu'aux nouvelles périphéries réseau. Cette solution offre des performances et une fiabilité incomparabes, tout en fournissant un contrôle et une visibilité centralisés sur toute la surface d'attaque de la succursale.
SD-Branch regroupe les fonctionnalités réseau et sécurité au sein d'une seule solution offrant une protection complète aux environnements distribués. SD-Branch couvre toutes les zones critiques exposées des succursales, de la périphérie WAN jusqu'à la couche d'accès des succursales, en passant par l'ensemble des endpoints. Cette solution déploie les capacités de Fortinet Secure SD-WAN jusqu'aux réseaux câblés et sans fil, tout en simplifiant la gestion de l'infrastructure des succursales.

NGFW FortiGate avec SD-WAN sécurisé, recommandé par NSS Labs[3]:

- Blocage de 100 % des évasions et sécurité efficace à 99,9 %
- Meilleur coût total de possession (TCO) du secteur : 10 fois inférieur à la concurrence
- Meilleures performances des applications VoIP et vidéo parmi toutes les solutions testées

Comparés aux offres concurentes, Fortinet SD-Branch dispose de plusieurs atouts. Cette solution se distingue en proposant une mise en réseau axée sur la sécurité. Elle repose sur un firewall nouvelle-génération FortiGate (NGFW) et sur l'infrastructure Fortinet Security Fabric. Les entreprises peuvent ainsi sécuriser toute la couche d'accès réseau. Fortinet Security Fabric inclut notamment les solutions Fortinet FortiAP (points d'accès sans fil sécurisés) et FortiSwitch-FortiLink (Ethernet sécurisé). FortiNAC, outil de contrôle d'accès au réseau (NAC), assure visibilité, détection et contrôle des équipements connectés (IoT), pour suivre la détection des anomalies via l'analyse du trafic.[4]

Fortinet SD-Branch intègre également la gestion de la sécurité, du SD-WAN et de l'accès au réseau, via un unique panneau de contrôle. Notre solution FortiManager permet une gestion étendue, avec un déploiement sans contact. L'interface, qui unifie sécurité et mise en réseau, contribue à alléger le travail des équipes informatiques, tout en minimisant le coût total de possession..

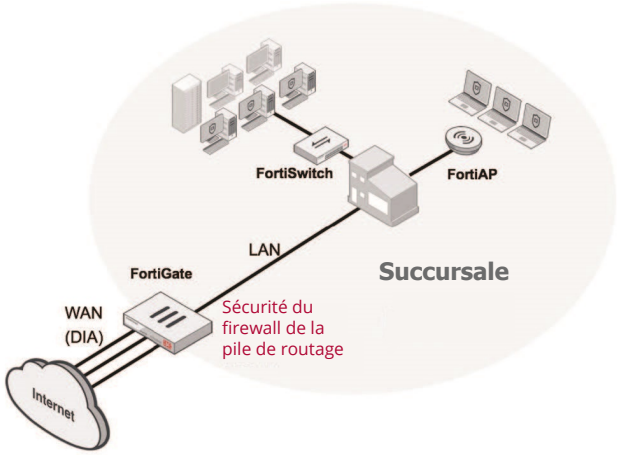

Figure 1 : Fortinet SD-Branch consolide les infrastructures WAN et LAN.

Mise en réseau axée sur la sécurité

- Sécurisation dès la conception
- Sécurité intégrée d'emblée au réseau
- Intégration native à une plateforme unifiée

Le marché mondial SD-Branch est estimé à 3,27 milliards de dollars d'ici 2023.[5]

« L'argument le plus convaincant en faveur du SD-Branch est l'efficacité opérationnelle. Les entreprises peuvent rapidement déployer et fournir à chaque nouvelle succursale une solution réseau prête-à-l'emploi ».[6]

Avantages de Fortinet SD-Branch pour les experts en ingénierie et exploitation réseau

La solution Fortinet SD-Branch permet une amélioration significative de la sécurité en succursale. Les politiques globales sont appliquées à toute la périphérie WAN, à la couche d'accès de la succursale et à tous les endpoints. Cette solution étend à la fois la protection et les performances du réseau à la couche d'accès, en unifiant les environnements WAN et LAN. Elle automatise l'identification, la classification et la sécurisation des équipements IoT lorsqu'ils cherchent à accéder au réseau. Elle fournit des processus automatisés de détection et de correction des anomalies basés sur la logique définie par l'entreprise. Enfin, elle permet aux entreprises distribuées d'élargir rapidement leurs activités à de nouveaux bureaux et à de nouveaux emplacements géographiques.
Fortinet SD-Branch contribue à réduire les besoins en ressources on-site, de manière à réduire le coût total de possession. SD-Branch intègre les firewalls, les commutateurs et les points d'accès au sein d'une solution unique et consolidée.

Son panneau de contrôle unifié permet de gérer la sécurité et la visibilité de la couche réseau pour optimiser l'efficacité des équipes tout en permettant une gestion proactive des risques. Les fonctions de déploiement zero-touch réduisent les dépenses liées à l'installation initiale et au développement ultérieur de l'entreprise.

Définir une approche réseau des succursales axée sur la sécurité

Du point de la sécurité, l'évolution constante des réseaux pose de nombreux défis. Les sites éloignés requièrent des défenses propres, adaptées aux risques uniques qu'ils encourent. SD-Branch, véritable prolongement de Fortinet Security Fabric, consolide la couche d'accès au réseau en s'appuyant sur une plateforme sécurisée qui offre visibilité et sécurité sur le réseau et sur tous les appareils qui s'y connectent.

[1] Conner Forrest, « Businesses are adopting SaaS too fast to properly secure it », TechRepublic, 10 avril 2018.
[2] « 25% Of Cyberattacks Will Target IoT In 2020 », Retail TouchPoints, dernière accès : 21 mars 2019.
[3] Nirav Shah, « Fortinet Secure SD-WAN Gives the Performance of a Lifetime, Recommended by NSS Labs » Fortinet, 9 août 2018.
[4] Disponible avec FortiNAC version 8.6.
[5] « Worldwide SD-Branch (Fixed Site, Mobile Office) Market 2018-2023 - Market is Estimated to Reach $3.27 Billion », PR Newswire, 21 août 2018.
[6] Lee Doyle, « SD-Branch: What it is and why you'll need it » Network World, 23 janvier 2018.

FORTINET

www.fortinet.com

12 juin 2019 11:48 AM

431530-0-0-EN