

PRÉSENTATION DE LA SOLUTION

Fortinet SD-Branch sécurise le réseau étendu des sites distants

Synthèse

La transformation numérique (DX) a rendu les réseaux des sites distants beaucoup plus complexes et, donc, vulnérables aux attaques. En réponse, de nombreuses organisations ont déployé des produits multipoints pour faire face aux nouvelles expositions aux menaces, au fur et à mesure de leur apparition. Mais cette approche complique encore davantage les infrastructures des sites distants, ce qui accroît les coûts, la complexité et la vulnérabilité. Pour résoudre ces problèmes, les sites distants devraient intégrer des fonctionnalités de réseau et sécurité au niveau de la couche d'accès et des périphériques réseau WAN. La solution Fortinet SD-Branch consolide la couche d'accès réseau au sein d'une plate-forme sécurisée qui offre visibilité et sécurité au réseau et à tous les périphériques qui s'y connectent.

Réponse face à une surface d'attaque en expansion

L'adoption rapide des technologies de la DX — y compris les appareils de l'Internet des objets (IoT), les applications SaaS (Software-as-a-Service), les outils numériques voix/vidéo et les terminaux BYOD (Bring your own-device) — a entraîné une augmentation du nombre de périphéries réseau à protéger dans une succursale donnée. Les réseaux comme les produits de sécurité des solutions ponctuelles utilisés pour protéger l'infrastructure des succursales sont devenus difficiles et coûteux à gérer.

L'essor de l'IoT en particulier — des appliances connectées, aux appareils d'éclairage et de climatisation efficaces, en passant par les appareils de conditionnement physique personnels appartenant aux employés — se traduit par l'arrivée de nombreux appareils sur le réseau, souvent avec une sécurité douteuse et une visibilité peu fiable.

Solution Fortinet SD-Branch

Fortinet offre une approche large, intégrée et automatisée de la sécurité réseau, avec un rapport qualité-prix inégalé. Fortinet SD-Branch s'étend en toute transparence sur les nouvelles périphéries du réseau et offre des performances et une fiabilité inégalées, tout en permettant un contrôle et une visibilité centralisés sur toute la surface d'attaque de la succursale.

La solution SD-Branch consolide les fonctionnalités réseau et sécurité en une solution unique qui assure une protection transparente des environnements distribués. Elle couvre toutes les expositions critiques des sites distants, de la périphérie du WAN à sa couche d'accès, en passant par une gamme complète de périphériques. Elle étend les fonctionnalités de Fortinet Secure SD-WAN aux réseaux câblés et sans fil tout en simplifiant la gestion de l'infrastructure des sites distants.

La solution Fortinet SD-Branch offre plusieurs éléments différenciateurs clés par rapport aux options concurrentes. Tout d'abord, elle permet de mettre en place **un réseau sécurisé** en utilisant le pare-feu de nouvelle génération FortiGate (NGFW) et une architecture Fortinet Security Fabric plus large pour étendre la sécurité à travers la couche d'accès réseau. Cela inclut des solutions Fortinet comme FortiAP (points d'accès sans fil sécurisés) et FortiSwitch avec FortiLink (Ethernet sécurisé). Le contrôle d'accès au réseau FortiNAC (NAC) ajoute la visibilité, la détection et le contrôle des appareils IoT, ainsi que la possibilité supplémentaire de suivre la détection des anomalies via l'analyse du trafic.⁴

Fortinet SD-Branch comprend également la gestion de la sécurité, de l'accès au réseau et du SD-WAN via un tableau de bord unique. Notre solution FortiManager permet une gestion extensible à grande échelle avec un déploiement « zero-touch ». Son interface combinée pour la sécurité et le réseau permet d'alléger la charge d'une équipe informatique restreinte, tout en minimisant le coût total de possession.

64% des décideurs informatiques estiment que l'adoption du SaaS dans leur entreprise dépasse leurs capacités à le sécuriser.¹

Alors que plus de 25% des cyberattaques viseront l'IoT d'ici 2020, moins de 10% des budgets de sécurité informatique seront consacrés à la protection de ces dispositifs.²

FortiGate NGFW intégrant le Secure SD-WAN — Recommandé par NSS Labs³ :

- A bloqué 100% des évasions et atteint une efficacité de sécurité de 99,9%
- Meilleur coût total de possession de l'industrie — 10 fois supérieur à celui de la concurrence
- La meilleure qualité d'expérience pour les applications VoIP et vidéo, parmi toutes les solutions testées

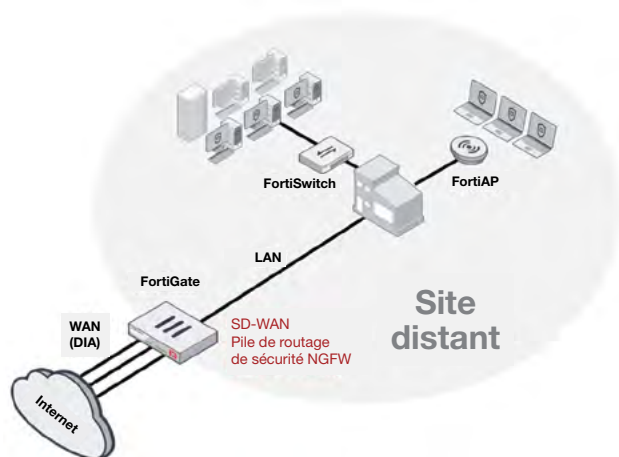


Schéma 1 : Fortinet SD-Branch consolide les infrastructures WAN et LAN.

Les avantages de la solution Fortinet SD-Branch pour les responsables réseau et les responsables d'exploitation

Les principaux avantages de la solution Fortinet SD-Branch sont liés à l'amélioration de la sécurité au niveau du site distant. Les stratégies globales sont appliquées à toutes les périphéries WAN, à la couche d'accès du site distant et à tous les périphériques. Elle étend à la fois la sécurité et les performances réseau à la couche d'accès en unifiant les environnements WAN et LAN. Elle automatise la découverte, la classification et la sécurité des appareils IoT lorsqu'ils cherchent à accéder au réseau. Elle fournit aussi automatiquement des processus de détection et de correction d'anomalies basés sur une logique métier définie. Enfin, elle permet aux organisations distribuées d'étendre rapidement leurs activités à de nouveaux bureaux et à de nouveaux emplacements géographiques.

Fortinet SD-Branch contribue également à réduire le besoin de ressources sur place, ce qui réduit le coût total de possession. SD-Branch intègre les pare-feux, les commutateurs et les points d'accès dans une solution unique et consolidée. Ses fonctionnalités de gestion à partir d'un tableau de bord unique combinent la sécurité et la visibilité de la couche réseau pour optimiser l'efficacité du personnel tout en permettant une gestion proactive des risques. Les fonctions de déploiement « zero-touch » réduisent les charges associées à l'installation initiale et à la croissance de l'entreprise au fil du temps.

Définition d'une approche axée sur la sécurité pour le réseau des sites distants

L'évolution constante des réseaux des sites distants en fait un défi en matière de sécurité. Les sites éloignés ont besoin de leurs propres moyens de défense, qui soient conformes aux risques uniques qu'ils présentent. En tant qu'extension naturelle de la Fortinet Security Fabric, le SD-Branch offre un réseau sécurisé. Ce faisant, SD-Branch consolide la couche d'accès réseau au sein d'une plate-forme sécurisée qui fournit visibilité et sécurité au réseau et à tous les dispositifs 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, consulté le 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 la 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.

La sécurité au cœur du réseau

- Une sécurité mûrement réfléchie
- Intégrée au réseau dès le départ
- Élément d'une solution de plate-forme intégrée

Le marché mondial de la solution SD-Branch est estimé à 3,27 milliards de dollars d'ici 2023.⁵

« L'argument le plus convaincant en faveur de la solution SD-Branch est l'agilité opérationnelle. Les services informatiques peuvent rapidement déployer et fournir une solution clé en main réseau pour de nouveaux sites. »⁶