

Fortinet Secure SD-Branch

Opportunités

- Secure SD-Branch constitue un cas d'utilisation spécifique de Secure SD-WAN. Secure SD-WAN est une fonctionnalité incluse, sans frais supplémentaires, avec chaque NGFW FortiGate. SD-Branch, en revanche, propose des dispositifs hardware et des services supplémentaires, pour aller au-delà de FortiGate. Il s'agit d'une opportunité commerciale pouvant multiplier par trois les montants en jeu.
- Le SD-WAN opère un remodelage spectaculaire du marché du routage professionnel. Selon Gartner, le SD-WAN devrait connaître un taux de croissance annuel composé (TCAC) de 59 % jusqu'en 2021 pour atteindre cette même année 1,3 milliard de dollars.¹
- IDC prévoit un taux de croissance annuel composé de plus de 40 % pour le SD-WAN et estime que le marché global atteindra 4,5 milliards de dollars d'ici 2022.²
- À titre de comparaison, les opportunités du marché du sans-fil représentent, en 2020, 5,84 milliards de dollars, avec un TCAC moyen de 7,9 % entre 2018 et 2023. Le marché de la commutation en campus affiche, quant à lui, 14,6 milliards de dollars avec un TCAC de 1 %. Le marché SD-WAN constitue donc une opportunité particulièrement intéressante.

Pourquoi Fortinet ?

La solution Fortinet Secure SD-Branch regroupe la gestion du SD-WAN, des firewalls, des switchs et des points d'accès en une seule solution. Les entreprises multi-sites peuvent ainsi simplifier leur infrastructure, optimiser les coûts et assurer une protection optimale au niveau du WAN et des accès.

Avec la solution Fortinet Secure SD-Branch :

- La protection et les performances sont assurées au niveau de la couche d'accès, avec l'unification des environnements WAN et LAN.
- Les politiques unifiées sont appliquées à la périphérie du WAN, à la périphérie de l'accès à la succursale, et sur tous les endpoints (y compris les objets connectés).
- Secure SD-Branch permet la détection, la classification et la sécurité automatisées des objets connectés, ainsi que la détection et la correction des anomalies.
- Le déploiement Zero-touch permet aux entreprises multi-sites de s'adapter rapidement. Les nouveaux bureaux gagnent en adaptabilité. Il n'est plus nécessaire de recruter des experts IoT sur chaque site.
- La gestion centralisée réduit les besoins en ressources sur site, ce qui diminue le coût total de possession.

Défis des entreprises

Sociétés et professionnels cibles

Taille de l'entreprise

- Moyennes et grandes entreprises dont le portefeuille est de 249 millions de dollars et plus
- Toute organisation établie en plusieurs endroits : siège social, succursales, centres de données d'entreprise, sites de co-location ou d'hébergement, fournisseurs de services cloud, etc.

Professionnels

- Cibles principales. VP/directeur de l'ingénierie réseau
- Acheteurs techniques/influenceurs. Vice-président IT, administrateur/architecte de la sécurité, ingénieur réseau
- Acheteurs commerciaux/influenceurs. Directeur d'agence/de magasin, directeur financier, finances/approvisionnement

Défis	Solutions Fortinet
Opérations complexes	Fortinet Secure SD-Branch simplifie les opérations et élimine les silos. La convergence du WAN, de la sécurité et de la couche d'accès (avec et sans fil) consolide la gestion, réduit les risques et offre plus de précision.
Conflits réseau/sécurité	Avec Fortinet, les capacités de réseau et de sécurité sont gérées ensemble, via une seule interface. Il devient possible de visualiser et de contrôler toutes les succursales et tous les sites distants, depuis la périphérie d'accès jusqu'à la périphérie du WAN. L'ensemble des succursales disposent d'une protection et d'une surveillance simplifiées, pour une sécurité sans faille.
Contraintes budgétaires	Fortinet réduit le coût de gestion des succursales en réduisant le nombre de produits disparates provenant de différents fournisseurs. Cette optimisation permet des économies importantes avec, notamment, une réduction des coûts de licence et d'assistance, et donc une baisse des frais d'exploitation et du coût total de possession (TCO).

Facteurs-clés de différenciation

Face à la croissance du marché SD-WAN, beaucoup de vendors tentent de se positionner également comme fournisseurs de solutions SD-Branch. Toutefois, peu d'entre eux proposent une solution complète. Fortinet, à l'inverse :

- Est l'un des seuls fournisseurs représentés dans les trois Gartner Magic Quadrants concernés :
 - Gartner Magic Quadrant 2019 Infrastructures de périphérie WAN
 - Gartner Magic Quadrant 2019 Firewalls réseau
 - Gartner Magic Quadrant 2019 Infrastructures d'accès aux réseaux locaux câblés et sans fil
- Arrive en tête pour la vision globale (completeness of vision) et les capacités d'exécution dans le Magic Quadrant 2019 Infrastructures de périphérie WAN.³
- Se différencie de tous les autres fournisseurs par l'intégration de services (SD-WAN, accès et sécurité) au sein d'un cadre commun (la Fortinet Security Fabric).
- N'exige pas de licence pour Secure SD-Branch. Comme Secure SD-WAN, la gestion des accès est incluse dans FortiOS.
- Offre une sécurité NGFW entièrement intégrée, contrairement à la plupart des fournisseurs SD-Branch.



Ressources complémentaires

- [Secure Access et SD-Branch sur le portail partenaires Fortinet](#)
- [Webinaire à la demande](#)
- [Guide de ventes Secure SD-Branch](#)

Questions préliminaires

REMARQUE : La plupart des questions visant à qualifier les opportunités SD-WAN fonctionnent également pour SD-Branch. Les questions ci-dessous sont spécifiques ou particulièrement importantes :

- Comment sécurisez-vous actuellement les réseaux distants des succursales, notamment pour les objets connectés (IoT) ?
- Comment gérez-vous actuellement vos succursales ? La complexité pose-t-elle problème ? Manquez-vous de ressources/ d'expertise pour gérer plusieurs produits ?
- Disposez-vous d'une politique de sécurité globale ? Comment est-elle mise en œuvre ?
- Le respect des réglementations telles que le RGPD, l'HIPAA, le GLBA, le PCI vous pose-t-il des difficultés ? Avez-vous besoin de sécuriser des données au repos ou en mouvement ?

Surmonter les objections

Je recours à une approche best-of-breed OU je ne vois en Fortinet qu'un simple fournisseur de sécurité.

Fortinet est reconnu dans sept Magic Quadrant de Gartner. En plus d'être Leader dans la catégorie Firewall, Fortinet est challenger dans la catégorie Périphérie WAN, et seuls quatre fournisseurs sont classés plus haut dans la catégorie Infrastructures d'accès aux réseaux locaux câblés et sans fil.

Notre projet concerne uniquement (SD-WAN, sécurité, sans fil, etc.).

De nombreuses entreprises cherchent à réduire la complexité globale des succursales. Le fait de recourir à un fournisseur unique permet de réduire le nombre de contrats, de raccourcir les délais de résolution des problèmes, etc.

Nous souhaitons nous focaliser uniquement sur le cloud. Nous ne voulons pas installer de matériel hardware sur site.

Certains équipements resteront nécessaires, comme la rampe d'accès cloud et vos utilisateurs devront se connecter à votre réseau par un accès câblé ou sans fil. Puisque vous devrez de toute façon déployer ce matériel, pourquoi ne pas le faire de manière sécurisée ?

Nous manquons de ressources humaines et d'expertise pour utiliser ou gérer ce type de solution, surtout si elle nécessite plusieurs consoles de gestion.

Fortinet simplifie le déploiement et la gestion, pour vous permettre de connecter plus rapidement et plus facilement de nouvelles succursales. Fortinet Secure SD-Branch est facile à installer et à gérer. Vous pouvez tout administrer, tout contrôler, via un unique panneau de contrôle.

Environnement concurrentiel

REMARQUE : Peu de fournisseurs proposent une solution complète SD-WAN, câblée, sans fil et NAC. De nombreux fournisseurs SD-WAN qui ne proposent pas la gestion des objets connectés ou de la couche d'accès tenteront de proposer un modèle SASE. Cette approche concentre les opérations de sécurité vers le cloud. Elle laisse les couches d'accès et d'appareils sur site non-protégées. Chez Fortinet, nous jugeons cette approche insatisfaisante. Notre architecture Secure SD-Branch assure la sécurité du WAN, de l'accès et de la périphérie, tout en offrant des modèles de sécurité cloud.

Fonctionnalités	Fortinet	Cisco Meraki	HPE / Aruba	Cisco ISR / Viptela	Juniper / Mist	Forcepoint	VeloCloud	Palo Alto Networks	Versa Networks
Inspection NGFW incl. SSL	Oui	Limité	Non	Oui	Limité	Oui	Non	Oui (mais lent)	Limité
Prise en compte des applications	Oui	Limité	Oui	Oui	Oui	Oui	Oui	Basique	Partielle
Offre fil et sans fil	Oui	Oui	Oui	Oui	Oui	Non	Non	Non	Non
Unique console de gestion (fil, sans fil,, sécurité, SD-WAN)	Oui	Oui	Oui	Non	Limité (en développement)	Non	Non	Non	Non
Visibilité et contrôles des objets connectés (IoT)	Oui	Limité	Oui	Oui	Oui	Non	Non	Non	Non
Provisionnement Zero Touch	Oui	Oui	Oui	No	Oui	Oui	Oui	Non	Oui
CTO	Faible	Modéré	Modéré	Élevé	Modéré	Modéré	Élevé	Modéré	Modéré

¹ Danielle Young, Ted Corbett, Lisa Pierce, "[Gartner Group: SD-WAN Survey Yields Surprises](#)," Technology Blog, November 19, 2017.

² "[SD-WAN Infrastructure Market Poised to Reach \\$4.5 Billion in 2022](#)," IDC, August 8, 2018.

³ "[2019 Gartner Magic Quadrant for WAN Edge Infrastructure](#)," Gartner, 2019.