FICHE SOLUTION

Simplifier les opérations SD-WAN au sein des environnements industriels pour une connectivité fiable

Synthèse

Le SD-WAN (software-defined wide-area networking) remplace progressivement le WAN traditionnel au service des sites distants industriels. Si le SD-WAN offre une connectivité fiable capable d'accompagner les innovations digitales, peu de solutions SD-WAN offrent des fonctions de sécurité et réseau consolidées et adaptées aux environnements hostiles. Les entreprises souhaitant déployer leur SD-WAN sur des usines, stations électriques ou forages pétroliers distants doivent souvent assembler des produits ciblés distincts. Les exploitants doivent simplifier leur approche métier pour maîtriser leurs coûts, doper leur efficacité et juguler les risques. C'est précisément ce que permet Fortinet FortiGate Rugged Secure SD-WAN. La solution associe des pare-feux de nouvelle génération et disposant d'une structure renforcée adaptée aux milieux hostiles avec des solutions intégrées de gestion et de traitement analytique. Ceci permet de simplifier et de centraliser les opérations SD-WAN.

Accompagner l'innovation au sein des infrastructures multisites de production

Les usines, stations électriques et forages pétroliers ont adopté l'innovation digitale, au travers d'applications SaaS ou de services temps-réel de voix et de vidéo par exemple, pour doper la productivité, améliorer les communications et encourager la croissance. Cependant, les architectures WAN traditionnelles, actives sur de nombreux sites distants peinent à supporter le trafic de ces applications et nouvelles technologies à un coût raisonnable. Ce constat aboutit à l'adoption d'une architecture SD-WAN capable d'utiliser des connexions internet directes et plus économiques. Le marché du SD-WAN a progressé de 110% entre 2018 ($841 millions) et 2019 ($1,77 milliards).[1]

Mais si le SD-WAN rend la connectivité plus fiable, il renforce également l'exposition au risque des entreprises. Selon une enquête de Gartner, « les clients s'investissent toujours pour améliorer la visibilité et les performances de WAN, mais la sécurité est aujourd'hui devenue la priorité absolue pour leur WAN ».[2]

Dans nombre d'entreprises, le besoin de sécuriser le SD-WAN a incité les professionnels de l'ingénierie et des opérations réseau à intégrer de nombreux outils différents et produits distincts pour répondre aux différents profils de menaces et assurer la conformité réglementaire. Cette approche induit néanmoins de la complexité en matière d'infrastructure, ce qui alourdit la charge de gestion, mais instaure également des failles au niveau de l'edge réseau.

Fortinet offre un SD-WAN adapté à l'OT, avec une appliance totalement intégrée et le module de gestion Fabric Management Center

- Pare-feu de nouvelle génération (NGFW)
- Fonctionnalité SD-WAN
- Design renforcé, adapté aux environnements hostiles (températures, vibrations, humidité, etc.)
- Déploiement « zero-touch »
- Gestion centralisée
- Reporting et traitement analytique
- Reporting de conformité
- Intégration et automatisation

Gartner indique dans une étude que « 72% des répondants indiquent que la sécurité constitue leur priorité en matière de WAN. »[3]

Gartner

Fortinet simplifie et sécurise le SD-WAN

La consolidation des outils réseau et de sécurité dans le cadre d'une solution SD-WAN orientée sécurité simplifie le déploiement sur des sites distants. Ceci restreint la surface d'attaque de l'entreprise, encourage les initiatives d'innovation digitale et simplifie les opérations pour équipes réseau.

En tant que partie intégrante du Fabric Management Center, FortiGate Rugged Secure SD-WAN bénéficie d'une console unifiée avec SD-WAN Orchestrator proposé dans le cadre de FortiManager et offrant un traitement analytique et un reporting pertinent via FortiAnalyzer. Ceci permet aux clients de simplifier et centraliser le déploiement de la solution, de gagner du temps avec l'automatisation et de définir des règles orientées métier.

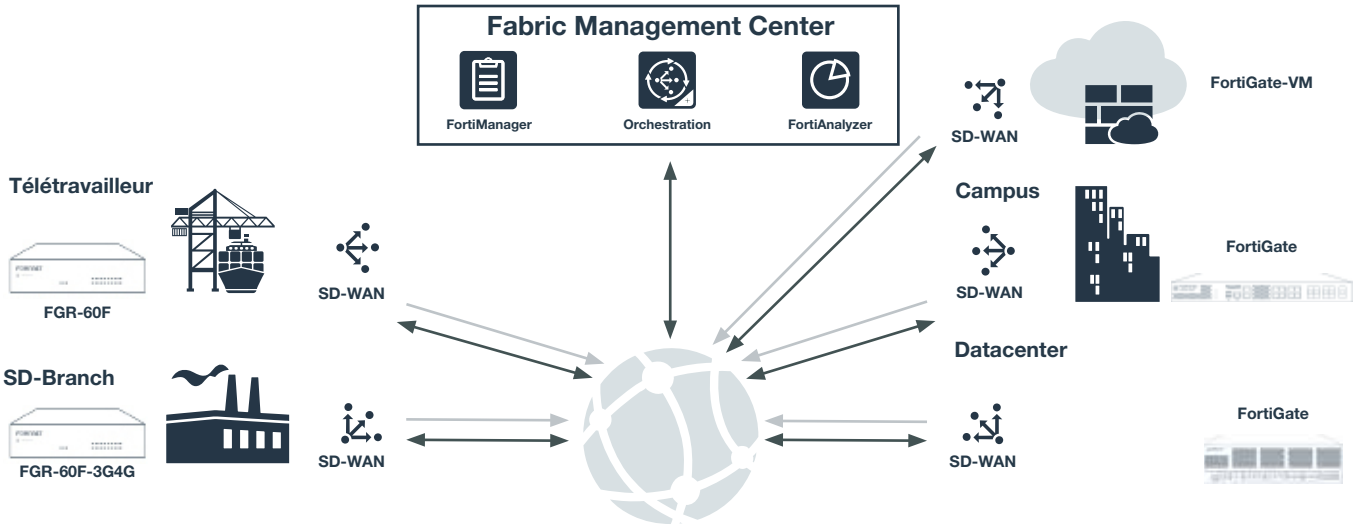

Schéma 1: les pare-feux FortiGate à structure renforcée permettent de piloter le SD-WAN à partir d'une interface unifiée.

Déploiement « zero-touch »

Les entreprises qui déploient FortiGate Rugged Secure SD-WAN peuvent tirer parti de Fabric Management Center pour accélérer le déploiement, de plusieurs jours à quelques minutes. L'automatisation des tâches de déploiement qu'offre Fabric Management Center permet aux dispositifs FortiGate sur site distant d'être interconnectés, puis d'être configurés automatiquement par FortiManager présent sur le site central : les gains de temps et les économies sont ainsi au rendez-vous. L'approche de Fortinet peut également tirer parti d'une configuration SD-WAN existante qui devient ainsi un modèle pour accélérer les déploiements sur de nombreux nouveaux sites.

Les tests de NSS Labs indiquent que FortiGate Rugged Secure SD-WAN permet d'interconnecter un site distant en moins de six minutes, grâce à un déploiement automatisé (zero-touch)[4]

Une gestion centralisée pour les entreprises multisites

La gestion centralisée des réseaux multisites sur l'ensemble d'un périmètre d'entreprise aide les professionnels réseau à mieux maîtriser le risque d'erreurs, celles qui renforcent l'exposition aux risques et favorisent des dysfonctionnements.

Secure SD-WAN Orchestrator est partie intégrante de Fabric Management Center. Ce module permet aux clients de simplifier leur environnement centralisé, de gagner du temps grâce à l'automatisation et de bénéficier de règles orientées métiers. Les outils de gestion de Fortinet prennent en charge des environnements bien plus larges que ceux de leurs concurrents, jusqu'à 100 000 appliances FortiGate. Certaines fonctionnalités, comme les modèles SD-WAN et NGFW, la gestion des configurations en environnement professionnel et le contrôle d'accès fondé sur les rôles aident les ingénieurs et équipes opérationnelles à garder la main sur le risque d'erreurs humaines.

Reporting et traitement analytique sur le SD-WAN

Les traitements analytiques sophistiqués (garants de la haute disponibilité du lien WAN), les accords de niveau de service (SLA) sur les performances et le trafic applicatif, ainsi que les statistiques historiques permettent à l'équipe d'infrastructure de traiter rapidement les problématiques réseau. Fabric Management Center offre des indicateurs évolués sur les performances réseau et applicatives pour accélérer la résolution des problématiques et réduire le nombre de tickets de support. Des rapports d'activité sur le SD-WAN, édités à la demande, offrent davantage de visibilité sur l'univers des menaces, les niveaux de confiance et l'accès aux ressources, ce qui permet d'évaluer le niveau de conformité.

Ces rapports portent sur **le monitoring de la bande passante** et des données du SD-WAN, **le monitoring des logs et de l'historique des SLA** via des tableaux et graphiques, des alertes personnalisables sur les SLA, ainsi que des tableaux de bord et rapports sur les usages applicatifs. D'autre part, ce sont des **scénarios de prise en charge** qui sont proposés pour les évènements SD-WAN, ainsi que des fonctions de logs et d'archivage sur les SLA, sur l'ensemble des applications et interfaces.

Reporting de conformité

Les clients ont besoin de rapport et d'outils pour démontrer leur conformité réglementaire lors d'audit. Cependant, la gestion de la conformité est généralement une opération coûteuse et qui mobilise fortement les équipes réseau : l'agrégation des données et leur standardisation à partir de différents produits de sécurité distincts peuvent mobiliser plusieurs collaborateurs à temps plein pendant des semaines, si ce n'est des mois.

Fortinet accélère le reporting de conformité en simplifiant l'infrastructure de sécurité et en éliminant les processus manuels. Fabric Management Center propose des **modèles réglementaires personnalisés**, ainsi que des **rapports prêts à l'emploi** pour des normes telles que Security Activity Report (SAR), Center for Internet Security (CIS) et National Institute of Standards and Technology (NIST). Enfin, ce module offre la **mise en log de données d'audit** et **un contrôle d'accès fondé sur les rôles** pour s'assurer que les collaborateurs n'ont accès qu'aux informations dont ils ont réellement besoin pour mener leurs tâches.

En complément de Fabric Management Center, **FortiGuard Security Rating Service** mène des audits qui permettent aux équipes réseau et de sécurité d'identifier des vulnérabilités critiques et des configurations à risque au sein de leur Security Fabric, pour ensuite bénéficier de recommandations en matière de bonnes pratiques. Dans le cadre de ce service les professionnels du réseau peuvent comparer leur score de posture de sécurité à celui de leur pairs.[5]

Intégration et automatisation

Pour être efficace, la sécurité se doit d'être transparente sur l'ensemble des segments d'une entreprise multisite, sur chaque site distant. Les équipes d'ingénierie et d'exploitation doivent disposer d'une visibilité totale sur la surface d'attaque, et ce, à partir d'un seul lieu. Elles ont également besoin d'automatisation pour accélérer la prise en charge des incidents et leur remédiation, et pour réduire le nombre de tâches manuelles.

La conformité n'est pas la sécurité. Les entreprises les plus résilientes sont celles qui font de la conformité un socle de leur sécurité.[6]

Fabric Management Center accélère les délais de remédiation, grâce à une coordination des **actions de remédiation automatisées et basées sur des règles** sur l'ensemble de la Security Fabric, une architecture de sécurité intégrée qui facilite l'automatisation des workflows de sécurité et de veille sur les menaces. En cas d'incident, une alerte est envoyée avec des données contextuelles sur le lieu de l'incident, permettant à l'administrateur réseau de déterminer rapidement les actions à mener pour protéger l'entreprise dans son intégralité contre des attaques coordonnées. Certains évènements peuvent également déclencher des changements automatiques aux configurations des équipements, pour initier automatiquement la phase de remédiation post incident.

FortiAnalyzer et Fabric Management Center permettent également d'automatiser nombre de tâches associées au SD-WAN pour aider les équipes réseau à alléger la charge de travail de leurs équipes. Les deux produits **s'intègrent avec des outils tiers**, qu'il s'agisse d'un SIEM (security information and event management), d'une plateforme de gestion des servies IT, ou encore de DevOps (Ansible, Terraform), pour préserver les workflows existants et les investissements réalisés dans d'autres outils de sécurité et réseau.

Création de valeur, simplicité et sécurité

Fabric Management Center déploie une sécurité et des fonctionnalités réseau à l'intention des sites distants, avec de réels avantages :

Maîtrise du TCO. L'approche intégrée de Fortinet au SD-WAN orienté sécurité est un levier de maîtrise du coût total de possession (TCO) qui résulte de la consolidation des nombreux outils réseau et de sécurité. Les investissements financiers sont ainsi moins élevés, tout comme les charges d'exploitation grâce à une gestion simplifiée et une automatisation des workflows. La migration vers l'Internet haut-débit public permet de remplacer les liens MPLS coûteux par des liaisons plus économiques. Dans ce contexte, FortiGate Rugged Secure SD-WAN offre le TCO le plus optimisé du marché, jusqu'à 10 fois moindre par rapport aux concurrents.[7]

Efficacité renforcée. Simultanément, Fortinet institue une infrastructure de SD-WAN qui simplifie l'opérationnel sur les sites distants et sur la totalité du périmètre organisationnel multisite. FortiGate Rugged Secure SD-WAN se gère à partir d'une console de gestion unique et intuitive. Avec FortiManager, les dispositifs FortiGate se déploient en mode plug and play. Les règles centralisées et les paramètres des appliances peuvent être configurés avec FortiManager, tandis que les appliances FortiGate sont mises à jour automatiquement à l'aide de configuration actualisées de règles. La flexibilité d'une gestion à partir d'une interface unique permet une sécurité distante évolutive et un contrôle réseau via le cloud, pour tous les sites distants.

Le coût moyen d'un piratage de données ($3,92 millions) progresse compte tenu de la complexité système (+$290,000). L'utilisation d'une veille sur les menaces partagée (-$240,000) et le traitement analytique des données de sécurité (-$200,000) contribuent tous deux à alléger ce coût.[8]

Maîtrise des risques Les fonctions de tracking et de reporting de Fortinet aident les entreprises à assurer leur conformité aux réglementations en matière de confidentialité, de normes de sécurité et des cadres réglementaires sectoriels, tout en réduisant les risques de pénalités et de coûts légaux associés à un piratage. FortiAnalyzer suit l'activité en temps réel, simplifie l'évaluation des risques, détecte les menaces potentielles et aide à maîtriser toute défaillance. Son intégration étroite avec FortiGate Rugged Secure SD-WAN permet d'assurer le monitoring des règles de pare-feu et automatise les audits de conformité sur des infrastructures multisites.

Fortinet concrétise un SD-WAN orienté sécurité

Si un SD-WAN orienté sécurité concrétise de nombreux cas d'utilisation, l'approche de Fortinet constitue le levier le plus efficace pour tous les types de projets SD-WAN. La simplification des opérations de SD-WAN est essentielle pour assurer sa mise en œuvre et son expansion, en support des projets d'innovation digitale. FortiGate Secure SD-WAN with Fabric Management Center constitue la meilleure alternative en termes de gestion du SD-WAN et de traitement analytique, pour aider les équipes réseau à réduire leurs charges d'exploitation et à maîtriser leurs risques sur l'edge réseau.

[1] « Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 4Q19 et 2019, tableau 16.1 », Gartner, mars 2020.

[2] « Fortinet Recognized as a 2020 Gartner Peer Insights Customers' Choice for WAN Edge Infrastructure, » Fortinet, 26 mars 2020.

[3] « Fortinet Secure SD-WAN: Best-of-Breed NGFW and SD-WAN in a Single Offering, » Gartner, novembre 2018.

[4] Ahmed Basheer, « Software-Defined Wide Area Network Test Report: Fortinet FortiGate 61E, » NSS Labs, 19 juin 2019.

[5] « Proactive, Actionable Risk Management with the Fortinet Security Rating Service, » Fortinet, 8 juillet 2020.

[6] Frances Dewing, « Compliance Is Not Security: Why You Need Cybersecurity Chops In The Boardroom, » Forbes, 15 août 2019.

[7] « Fortinet Placed Highest in Ability to Execute in the Challengers Quadrant of the 2019 Gartner Magic Quadrant for WAN Edge Infrastructure, » Fortinet, 4 décembre 2019.

[8] « 2019 Cost of a Data Breach Report, » Ponemon Institute et IBM, 23 juillet 2019.

FORTINET

www.fortinet.fr

mars 2, 2021 11:06 AM

476710-B-1-FR