FORTINET exaprobe

Assurez une sécurité périmétrique complète avec le Secure SD-WAN

Table des matières

FORTINET

Synthèse

L'innovation numérique, telle que la montée en puissance des applications SaaS (logiciel service) et IaaS (infrastructure service), contribue à accroître les revenus et l'efficacité des entreprises distribuées. Toutefois, les exigences accrues de ces technologies en matière de trafic augmentent considérablement les goulets d'étranglement en termes de coûts et de performances de la connectivité MPLS (Multiprotocol Label Switching – commutation multiprotocole par étiquette) sur les infrastructures de réseau étendu (WAN) traditionnelles. Par conséquent, la plupart des responsables de l'ingénierie et de l'exploitation des réseaux cherchent maintenant à remplacer leurs infrastructures WAN dépassées par une forme de réseau étendu défini par logiciel (SD-WAN). Des dizaines de milliers de clients choisissent FortiGate Secure SD-WAN, qui offre à la fois des fonctionnalités de réseau et de sécurité dans une solution unifiée. Il prend en charge les performances des applications, la gestion consolidée et la protection avancée contre les menaces.

Introduction

Même si choisir la solution SD-WAN adaptée à ses besoins nécessite de faire quelques compromis, la sécurité ne devrait pas en faire partie. Il existe plusieurs options pour combiner du SD-WAN et une sécurité avancée, mais une seule solution peut vraiment être qualifiée de Secure SD-WAN. Fortinet, le nom le plus réputé en matière de sécurité réseau, a ajouté les meilleures fonctionnalités SD-WAN à ses pare-feux de nouvelle génération (NGFW) FortiGate, leaders du marché. Les NGFW FortiGate et leurs fonctionnalités de Secure SD-WAN offrent des performances optimales pour les applications SaaS (logiciel service) critiques, ainsi que pour les outils numériques voix et vidéo. Ils permettent également de protéger les entreprises contre les dernières expositions aux risques et contre des attaques sophistiquées en constante évolution.

IDC prévoit que les revenus mondiaux provenant des infrastructures et des services de SD-WAN connaîtront un taux de croissance annuel composé (TCAC) de plus de 40% pour atteindre 4,5 milliards de dollars d'ici 2022.[1]

Quelle solution SD-WAN choisir ?

Le SD-WAN offre la possibilité d'utiliser les services WAN disponibles de manière plus efficace et économique, ce qui donne aux utilisateurs de l'ensemble des entreprises distribuées, la liberté de mieux impliquer les clients, d'optimiser les processus métier et d'innover. C'est pourquoi les solutions SD-WAN continueront d'être un marché en forte croissance dans un avenir proche.

Pour répondre à cette demande, de nombreuses solutions SD-WAN ont été introduites ces dernières années. Mais toutes ne se valent pas.

Les experts du SD-WAN et les analystes de l'industrie affirment que le SD-WAN optimal pour une entreprise dépend des exigences de performance des applications, des priorités de sécurité et des compétences informatiques de l'entreprise. Il est également largement recommandé aux entreprises d'utiliser une solution de pare-feu de nouvelle génération NGFW en combinaison avec le SD-WAN pour résoudre les problèmes de sécurité, car les succursales sont directement exposées à Internet via des connexions haut débit avec le SD-WAN.

Pour répondre à ces exigences professionnelles, les entreprises ont besoin d'une offre SD-WAN complète : FortiGate Secure SD-WAN est la seule à disposer d'une sécurité intégrée et des capacités de performance requises pour un déploiement SD-WAN.

Fortinet propose le meilleur SD-WAN du marché

FortiGate Secure SD-WAN remplace les routeurs WAN séparés, l'optimisation WAN et les dispositifs de sécurité tels que les firewalls et les passerelles Web sécurisées (SWG) par un seul pare-feu de nouvelle génération NGFW FortiGate. Cette solution offre les meilleures performances de l'industrie avec des fonctionnalités telles que la prise en compte des applications, l'intelligence automatisée des chemins d'accès et la prise en charge de la superposition WAN pour le VPN. FortiGate Secure SD-WAN offre une sécurité au cœur du réseau pour les réseaux des succursales avec des performances exceptionnelles grâce à l'identification rapide des applications et à l'intelligence automatisée des chemins d'accès.

FortiGate Secure SD-WAN offre :

- Une identification rapide des applications
- L'amélioration de la précision et de la performance des applications
- Des mises à jour de la base de données des applications issues de la recherche de FortiGuard Labs

Prise en compte des applications pour améliorer les niveaux de service

FortiGate Secure SD-WAN est alimentée par le nouveau circuit intégré spécifique à l'application (ASIC) SOC4, qui permet un pilotage plus rapide des applications et offre des performances inégalées d'identification des applications. Cela inclut l'inspection approfondie de la couche de sockets sécurisés (SSL)/la sécurité de la couche de transport (TLS) avec la dégradation de performance la plus faible possible. Les capacités d'inspection du cryptage comprennent également la capacité d'inspecter le paquet afin que la solution SD-WAN puisse acheminer correctement le trafic.

D'un point de vue technique, une solution SD-WAN procède au routage des applications par l'intermédiaire des connexions WAN les plus efficaces à chaque instant. Pour garantir les performances optimales des applications, le système doit être capable d'identifier une large gamme d'applications et de mettre en œuvre les politiques de routage à un niveau très granulaire pour chacune d'entre elles. Sans ces capacités, les applications SaaS, vidéo et voix peuvent ralentir et limiter la productivité de l'utilisateur final.

Pour résoudre ces problèmes, FortiGate Secure SD-WAN utilise une base de données de contrôle des applications contenant les signatures de plus de 5000 applications (plus des mises à jour régulières des services de renseignements sur les menaces de FortiGuard Labs). FortiGate Secure SD-WAN identifie et classifie les applications, même le trafic d'applications cloud cryptées, dès le tout premier paquet.

FortiGate Secure SD-WAN reconnaît automatiquement et achemine de façon optimale plus de 5000 applications.

Les pare-feu NGFW FortiGate peuvent être configurés pour reconnaître les applications les plus critiques pour l'entreprise. Les applications critiques (Office 365, SalesForce, SAP), les applications générales de productivité (Dropbox) et les médias sociaux (Twitter, Instagram) peuvent se voir attribuer différentes priorités de routage. Des politiques uniques peuvent être appliquées à un niveau plus profond pour les sous-applications (par exemple, Word ou OneNote dans Office 365). Cette visibilité approfondie et étendue des applications, sur les modèles de trafic et d'utilisation, permet de mieux attribuer les ressources WAN en fonction des besoins de l'entreprise.

Un WAN simple et efficace

FortiGate Secure SD-WAN simplifie considérablement le processus de transformation des infrastructures WAN héritées afin d'améliorer les performances des applications, l'expérience utilisateur et la sécurité. Une fois que les politiques WAN sont définies en fonction de l'aspect critique des applications, des exigences de performance, des politiques de sécurité et d'autres considérations, la solution FortiGate Secure SD-WAN prend le relais. Les pare-feu NGFW FortiGate équipés de l'ASIC SOC4 offrent des performances de sécurité 10 fois supérieures à celles de la concurrence.[2]

Les fonctionnalités clés de FortiGate Secure SD-WAN incluent :

L'intelligence automatisée des chemins d'accès. L'identification des applications permet de hiérarchiser le routage des applications sur la bande passante du réseau en fonction de l'application et de l'utilisateur. Le nouvel ASIC SOC4 offre à FortiGate Secure SD-WAN le pilotage d'applications le plus rapide de l'industrie. Les accords de niveau de service (SLA) SD-WAN sont facilement définis en sélectionnant de façon dynamique la meilleure connexion WAN en fonction des circonstances spécifiques de l'entreprise. Pour les applications de faible à moyenne priorité, les entreprises peuvent spécifier des critères de qualité et FortiGate sélectionnera le lien correspondant. Pour les applications hautement prioritaires et critiques, les entreprises peuvent définir des SLA stricts, basés sur une combinaison de paramètres d'instabilité, de perte de paquets et de latence.

Superposition WAN. Les capacités d'un **VPN superposé** réactif permettent une meilleure expérience globale du WAN pour les utilisateurs des succursales. L'orchestration du **contrôleur de superposition sur le cloud**, optimisée par des services d'abonnement **360 Protection Bundle**, simplifie le déploiement du VPN par superposition avec un provisionnement automatisé basé sur le cloud.

Basculement automatique. La technologie de chemins multiples peut automatiquement basculer vers le meilleur lien disponible lorsque le chemin du WAN primaire se dégrade. Cette automatisation est intégrée dans le pare-feu nouvelle génération NGFW FortiGate, ce qui réduit la complexité pour les utilisateurs finaux tout en améliorant leur expérience et leur productivité.

Sélection intelligente des liens WAN. La sélection intelligente des liens WAN utilise la correction d'erreurs sans voie de retour (FEC) pour pallier les conditions défavorables du WAN telles que des liens de mauvaise qualité ou bruyants. Cela améliore la fiabilité des données et offre une meilleure expérience utilisateur pour des applications telles que les services vocaux et vidéo. La FEC ajoute des données de correction d'erreurs au trafic sortant, ce qui permet au destinataire de corriger la perte de paquets et d'autres erreurs survenant pendant la transmission. Ceci améliore la qualité des applications en temps réel.

Agrégation de la bande passante des tunnels. Pour les applications qui nécessitent une bande passante plus large, FortiGate Secure SD-WAN permet un équilibrage et une livraison de la charge par paquet en combinant deux tunnels superposés afin d'optimiser la capacité du réseau.

Gestion simplifiée et meilleur coût total de possession (CTP) de l'industrie

Les responsables de l'ingénierie et de l'exploitation des réseaux sont souvent confrontés à un dilemme lorsqu'il s'agit de déployer des périphériques de périmètre SD-WAN sur leurs nombreux sites distants et leurs succursales. Les interventions sur place coûtent cher et le personnel technique est souvent limité. D'un autre côté, l'expédition de dispositifs entièrement configurés est risquée. En outre, une fois que les périphériques de périmètre sont déployés, le personnel doit gérer à la fois les fonctions d'optimisation du WAN et les fonctions de sécurité, souvent à partir de deux interfaces différentes. FortiGate Secure SD-WAN résout ces problèmes de déploiement et de gestion afin de réduire le coût total de possession (CTP).

Dans les résultats des tests du groupe SD-WAN de NSS Labs pour 2019, FortiGate Secure SD-WAN a reçu pour la deuxième fois consécutive la mention « Recommandé », ce qui lui a permis d'obtenir le coût total de possession (CTP) le plus bas et de mettre en avant son provisionnement rapide sans contact pour des exploitations efficaces.[3]

Déploiement « zero-touch » (sans intervention). Grâce aux capacités de déploiement simplifiées de FortiGate Secure SD-WAN, les entreprises peuvent expédier de pare-feux nouvelle génération NGFW FortiGate non configurés sur chaque site distant. Une fois branché, le dispositif FortiGate se connecte automatiquement au service FortiDeploy dans FortiCloud. Il suffit de quelques secondes à FortiDeploy pour authentifier le dispositif à distance et le relier à votre système FortiManager central.

Une gestion à partir d'une console unique. FortiManager permet une visibilité centralisée de tous les pare-feux nouvelle génération NGFW FortiGate Secure SD-WAN déployés dans l'ensemble de l'organisation diffusée. Des visualisations très intuitives facilitent la surveillance des topologies physique et logique du réseau à un niveau élevé et permettent d'effectuer des recherches approfondies en cas de besoin pour étudier n'importe quel problème. Les administrateurs peuvent mettre à jour et diffuser les politiques WAN de l'entreprise à tous les sites ou reconfigurer des dispositifs individuels.

Il est possible, en un seul clic, de configurer des VPN pour les utilisateurs qui ont besoin de communications sécurisées sur les liens Internet publics. Tout cela permet de gagner du temps et simplifie l'administration SD-WAN (sur site ou via le cloud), allégeant ainsi la pression sur des équipes réseau réduites. Fortinet offre l'une des seules solutions permettant de gérer un réseau SD-WAN, la sécurité et le contrôle des couches d'accès à partir de la même console de gestion.

Coût total de possession (CTP). FortiGate Secure SD-WAN offre un CTP par Mbit/s à la pointe du secteur, ainsi qu'un approvisionnement sans contact des nouvelles agences en moins de six minutes.[4] Le passage au haut débit public signifie que les connexions MPLS coûteuses peuvent être remplacées par des options plus rentables. La solution Fortinet étant agnostique au transport, les entreprises peuvent utiliser toute la bande passante disponible en se servant des connexions en mode actif-actif.

Pour la deuxième année consécutive, FortiGate Secure SD-WAN offre le meilleur CTP du secteur, selon les tests de NSS Labs.[5]

Un réseau WAN sécurisé

Fortinet vous propose le meilleur SD-WAN certifié performant et sécurisé de son genre. Les NGFW FortiGate équipés de l'ASIC SOC4 offrent les performances de sécurité SD-WAN les plus rapides de l'industrie. Dans le « Rapport 2019 d'essai sur les réseaux étendus définis par logiciel » (Software-Defined Wide Area Networking Test Report) du NSS Labs, Fortinet a reçu pour la deuxième fois consécutive la mention « Recommandé ».[6]

Plus précisément, FortiGate Secure SD-WAN est doté d'une protection robuste contre les menaces SD-WAN, y compris des contrôles de sécurité de la couche 3 à la couche 7 que l'on ne trouve généralement pas dans les autres solutions SD-WAN qui incluent un pare-feu :

- Une protection complète contre les menaces, incluant un pare-feu, un antivirus, un système de prévention des intrusions (IPS) et Application Control
- Inspection du cryptage des paquets à haut débit par le protocole SSL/protocole TLS avec une dégradation minimale des performances, garantissant que les organisations ne sacrifient pas le débit pour une protection complète contre les menaces
- Web filtering pour renforcer la sécurité Internet sans avoir besoin d'un dispositif distinct de Secure Web Gateway (SWG)
- Des performances WAN élevées pour les applications de cloud, avec des performances exceptionnelles de superposition du VPN pour une expérience utilisateur supérieure et une faible latence[7]

Les pare-feux nouvelle génération FortiGate qui englobent les fonctionnalités de Secure SD-WAN surveillent également les règles et politiques du pare-feu et mettent en évidence les meilleures pratiques pour améliorer la sécurité globale de l'entreprise. Cela permet de simplifier la conformité aux normes de sécurité ainsi qu'aux lois sur la protection des données personnelles et aux règlements de l'industrie. L'automatisation des processus de vérification et de signalement permet au personnel d'économiser des heures de travail tout en réduisant le risque d'omissions et d'erreurs.

L'activation du SD-Branch

Il arrive souvent que des succursales d'entreprise décident de remplacer simultanément leurs périphériques WAN et LAN au profit d'une solution mieux intégrée et simplifiant la gestion de leurs opérations. L'utilisation d'infrastructures WAN et LAN séparées augmente la complexité au sein des succursales ; il y a plus de dispositifs à déployer et à mettre à jour avec plusieurs consoles de gestion, mais ce n'est pas tout. Elle réduit également la visibilité et le contrôle des opérations, tout en augmentant les possibilités de failles de sécurité que les pirates informatiques peuvent exploiter. Pour résoudre ces difficultés, FortiGate Secure SD-WAN inclut une extension de sécurité accélérée à la couche d'accès qui permet la transformation du SD-Branch.

Sur le marché changeant du SD-WAN, Fortinet est un pari sûr

Alors que les applications basées sur le cloud et les outils comme la voix et la vidéo deviennent de plus en plus critiques pour les entreprises diffusées, FortiGate Secure SD-WAN peut aider les entreprises à profiter des avantages de l'innovation numérique sans entraver les performances des applications, affecter la productivité des utilisateurs finaux ou exposer les données à des risques.

FortiGate Secure SD-WAN est une solution évolutive qui aide les entreprises à prendre en charge en toute confiance davantage de sites distants, d'applications critiques sensibles à la bande passante, de services cloud et tout ce dont le réseau de succursales a besoin.

FortiGate Secure SD-WAN a déjà été adoptée dans le monde entier par des secteurs aussi divers que la finance, le commerce de détail, la production et les services clients. Qu'ils aient besoin de prendre en charge quelques centaines de points d'extrémité mobiles ou des dizaines de milliers de succursales, les clients qui ont choisi FortiGate Secure SD-WAN ont trouvé une combinaison optimale entre une sécurité de pointe et une fonctionnalité SD-WAN.

[1] « SD-WAN Infrastructure Market Poised to Reach $4.5 Billion in 2022 (Le marché des infrastructures SD-WAN devrait atteindre 4,5 milliards de dollars en 2022) », IDC, 8 août 2018.

[2] D'après des essais internes effectués par Fortinet.

[3] « Fortinet Receives Second Consecutive NSS Labs Recommended Rating in SD-WAN Group Test Report (Fortinet reçoit pour la deuxième fois consécutive la mention « Recommandé » des laboratoires NSS dans le rapport des résultats des tests du groupe SD-WAN) », Fortinet, 19 juin 2019.

[4] Idem.

[5] Idem.

[6] Idem.

[7] Idem.

FORTINET

www.fortinet.fr

372656-0-0-FR

septembre 29, 2020 4:19 PM

eb-FA-the-network-leaders-guide-to-secure-sd-wan