

Fortinet simplifie et optimise les services managés SD-Branch

Synthèse

Les réseaux de succursales distribués et les produits de sécurité individuels utilisés pour protéger l'infrastructure des succursales sont devenus difficiles et coûteux à gérer en raison de l'adoption rapide des appareils IoT (Internet of Things – Internet des objets), des applications SaaS (Software-as-a-Service) et des outils voix/vidéo numériques. Les fournisseurs de services managés (MSP) et les fournisseurs de services de sécurité managés (MSSP) peuvent étendre leurs offres et augmenter le revenu annuel par utilisateur (ARPU) en proposant aux clients actuels SD-WAN (software-defined wide area network), des services SD-Branch managés. En tant qu'extension des services basés sur la solution FortiGate Secure SD-WAN, Fortinet aide à consolider la couche d'accès réseau au sein d'une plateforme sécurisée qui offre visibilité et sécurité au réseau et à tous les appareils qui s'y connectent. Son coût total de possession (CTP), le meilleur du secteur, permet aux prestataires de services de fournir des services à valeur ajoutée (SVA) étendus tout en augmentant leurs revenus.

Le modèle IaaS (Infrastructure-as-a-Service) nécessite consolidation, contrôle des coûts et sécurité

Alors que les entreprises distribuées cherchent à consolider l'infrastructure des succursales sur l'ensemble de la périphérie du WAN, de la couche d'accès et des terminaux, les prestataires de services sont bien placés pour jouer un rôle pivot. Plus de la moitié (53%) des entreprises déclarent s'associer à des fournisseurs de services managés ou des fournisseurs de services de sécurité managés pour une aide en matière de mise en œuvre et de gestion.¹ Ici, les technologies SD-Branch peuvent consolider les fonctionnalités WAN et LAN pour simplifier l'infrastructure des bureaux distants et optimiser les opérations.

Alors qu'une offre SD-Branch managée commence par la fourniture d'un SD-WAN sous forme de service, les prestataires de services doivent tenir compte de facteurs essentiels, tels que l'intégration (pare-feu, commutateurs, points d'accès), la facilité de déploiement, la gestion centralisée, le coût total de possession et la sécurité, qui affectent tous le revenu annuel par utilisateur au fil du temps.

La solution Fortinet pour les déploiements SD-Branch

En tant qu'extension de FortiGate Secure SD-WAN, les fonctionnalités Fortinet SD-Branch dédiées permettent aux prestataires de services de fournir un service à valeur ajoutée SD-Branch avec des performances et une fiabilité réseau inégalées tout en offrant un contrôle et une visibilité centralisés sur l'ensemble de la surface d'attaque du réseau. La solution SD-Branch couvre toutes les expositions critiques des succursales, de la périphérie du WAN à la couche d'accès des succursales, en passant par toute une gamme de terminaux. Elle permet aux prestataires de services d'étendre les fonctionnalités de FortiGate Secure SD-WAN aux réseaux câblés et sans fil tout en simplifiant la gestion de l'infrastructure des succursales, ce qui augmente les capacités de service et les sources de revenus sans dépenses d'investissement supplémentaires (CapEx).

Extension de la sécurité jusqu'à la périphérie du réseau

En unifiant les environnements WAN et LAN, la solution Fortinet SD-Branch sécurise la périphérie étendue du réseau grâce à la combinaison du pare-feu NGFW, de la prévention des intrusions (IPS), du contrôle d'accès réseau (NAC), de la sécurité des commutateurs et des points d'accès, ainsi que d'autres fonctionnalités essentielles dans un seul appareil. Le fait qu'elle offre ces fonctionnalités de sécurité et réseau avancées dans le cadre d'une solution FortiGate Secure SD-WAN existante permet aux prestataires de services d'augmenter encore plus le revenu annuel par utilisateur des services managés existants grâce à une plus grande simplicité et une réduction des dépenses d'investissement (CapEx) et d'exploitation (OpEx).

Gestion et évolutivité simplifiées

La solution Fortinet SD-Branch aide les prestataires de services à centraliser les fonctionnalités d'orchestration et de gestion. Elle permet une gestion de la sécurité, de l'accès réseau et du SD-WAN via une interface unique. Cette interface combinée pour la sécurité et le réseau réduit la charge de gestion des prestataires de services tout en permettant une gestion proactive des risques. Fortinet permet également une évolutivité élastique des succursales grâce à des fonctions avancées telles que l'architecture mutualisée et le déploiement « zero-touch ». Le déploiement « zero-touch » réduit également les frais d'exploitation associés à l'installation initiale et à l'expansion des succursales au fil du temps.

Une solution SD-Branch efficace devrait inclure une gestion intelligente et centralisée du SD-WAN, du routage, de la sécurité intégrée, des commutateurs réseau (câblés) et des points d'accès (sans fil).²

Visibilité, contrôle et conformité

Dans le cadre de l'architecture Security Fabric intégrée, Fortinet offre aux prestataires de services une interface de gestion commune via des interfaces de programmation d'applications (API) libres afin de fournir une visibilité et un contrôle complets de l'infrastructure des succursales. La solution Fortinet SD-Branch automatise la découverte, la classification et la sécurité de tous les terminaux (y compris les appareils IoT non sécurisés) lorsqu'ils cherchent à accéder au réseau.

Lors du dernier test du groupe NSS Labs NGFW, FortiGate a offert une efficacité de sécurité de 99,3% et un blocage des évasions de 100%.³

Pour minimiser encore plus les dépenses d'exploitation des services managés, la solution Fortinet SD-Branch automatise également les processus de détection et de correction des anomalies en fonction d'une logique métier définie. Elle assure le contrôle d'accès réseau dynamique et automatisé en fonction du type de connexion, du terminal, de l'utilisateur et de l'application. Cette solution permet d'améliorer la protection de la périphérie du réseau tout en réduisant la charge de gestion des prestataires de services.

Sans les bons outils, les processus de génération de rapports de conformité peuvent être longs et coûteux (en termes de ressources humaines) pour les prestataires de services. La solution Fortinet offre des fonctionnalités de suivi et de génération de rapports automatisés qui contribuent à garantir le respect des lois sur la confidentialité des données, des normes de sécurité et des réglementations du secteur tout en réduisant les risques collatéraux d'amendes et de frais juridiques en cas de violation. Ces fonctions permettent de suivre l'activité des menaces en temps réel, de faciliter l'évaluation des risques, de détecter les problèmes potentiels et de les atténuer. Elles permettent également de surveiller les politiques de pare-feu et de faciliter les audits de conformité, réduisant ainsi le temps consacré par le personnel à ces tâches tout en éliminant les erreurs humaines potentielles et les coûts d'exploitation associés.

Réduction du coût total de possession

Fortinet réduit considérablement les dépenses d'investissement des prestataires de services et le coût total de possession en diminuant considérablement le nombre d'outils et d'appareils nécessaires pour fournir aux clients une infrastructure de succursale sécurisée et fonctionnelle. La solution Fortinet consolidée intègre des commutateurs, des pare-feux, des modules d'extension et des points d'accès sans fil. Dans le même temps, la gestion centralisée et les flux de travail automatisés de Fortinet permettent de réduire les coûts d'exploitation. Avec moins de fournisseurs de technologies à gérer, accompagner et former, les prestataires de services augmentent leurs marges, améliorent la satisfaction des clients et renforcent la confiance des vendeurs. À titre de confirmation, Fortinet a offert le plus faible coût total de possession par Mbit/s selon des scénarios réels lors des derniers tests de NSS Labs.⁴

Extension de l'offre de services à valeur ajoutée avec des réseaux de succursales sécurisés

Les succursales distantes ont besoin de leurs propres moyens de défense, qui soient conformes aux risques uniques qu'ils présentent. La solution Fortinet SD-Branch consolide la couche d'accès au réseau au sein d'une plateforme sécurisée qui offre visibilité et sécurité au réseau et à tous les appareils qui s'y connectent.

Les services managés basés sur FortiGate Secure SD-WAN permettent une migration transparente de façon à ce que les clients puissent profiter des avantages d'une offre de services à valeur ajoutée SD-Branch. Les prestataires de services peuvent ainsi développer de nouvelles sources de revenus avec leurs clients existants sans complexité, coût ou perte de déploiement d'infrastructure supplémentaire.

¹ Enquête menée par Fortinet auprès des responsables des infrastructures informatiques. Conclusions générales de l'enquête dans « [The IT Infrastructure Leader and Cybersecurity: A Report on Current Priorities and Challenges](#) », Fortinet, 18 août 2019.

² Kelly Ahuja, « [SD-Branch: The Next Destination On The Digital Transformation Journey](#) », Forbes, 9 novembre 2018.

³ « [Fortinet Receives Second Consecutive NSS Labs Recommended Rating in SD-WAN Group Test Report](#) », Fortinet, 19 juin 2019.

⁴ Ibid.