FORTINET

LIVRE BLANC

L'évolution du WAN offre des opportunités aux prestataires de services

Des services SD-WAN managés aux services SD-Branch managés

Synthèse

De nombreuses entreprises sont en phase de changer leurs attentes, préférences et modes d'utilisation des technologies numériques qu'elles choisissent pour leur activité. Ce changement étend la surface d'attaque du réseau, affectant ainsi l'ensemble du réseau, du datacenter à la périphérie du réseau. Comme les applications, les données et les ressources de calcul ne sont plus uniquement contenues dans le datacenter, l'évolution de la périphérie du réseau d'une entreprise distribuée moderne nécessite de repenser la gestion et la sécurité du trafic. Cela crée une opportunité pour les fournisseurs de services managés (MSP) et les fournisseurs de services de sécurité managés (MSSP) d'augmenter leur revenu annuel par utilisateur (ARPU) au fil du temps. Les déploiements SD-WAN et SD-Branch offrent un grand potentiel à cet égard, mais ils peuvent également accroître la complexité de l'infrastructure et la charge du personnel d'exploitation limité tout en exposant les clients à de nouveaux cyber-risques.

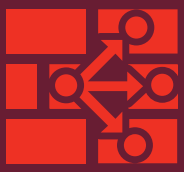
Augmenter les revenus des prestataires de services

Les fournisseurs de services managés et les fournisseurs de services de sécurité managés opèrent dans un domaine extrêmement compétitif. Leur défi constant est d'augmenter leur revenu annuel par utilisateur, leur rentabilité et leur part de marché. Au-delà de l'ajout de nouveaux clients, ils y parviennent généralement de deux manières :

- En augmentant les marges sur les services via une réduction des coûts d'investissement (CapEx) et des coûts d'exploitation (OpEx) ;
- En lançant de nouveaux services à valeur ajoutée (SVA).

Les offres de services managés basées sur le SD-WAN permettent aux bureaux distribués de remplacer leur WAN traditionnel. Mais le SD-WAN doit être considéré comme plus qu'un simple nouveau service de connectivité. Il peut fournir une plateforme pour des services à valeur ajoutée supplémentaires, tels que la sécurité SD-WAN et la consolidation SD-Branch (WAN/LAN). Mais actuellement, le plein potentiel de la plateforme SD-WAN est sous-utilisé par les prestataires de services.

Par conséquent, lorsque les prestataires de services choisissent une solution SD-WAN comme base pour leurs offres de services, ils doivent rechercher plus qu'un simple SD-WAN pur. Ils doivent prendre en compte d'autres fonctionnalités complètes et services supplémentaires que la plateforme SD-WAN peut offrir aujourd'hui et à l'avenir. C'est important, car une solution SD-WAN limitée peut avoir un impact négatif sur les coûts associés, la complexité et le temps de mise sur le marché des nouvelles offres de services, ainsi que sur les dépenses de gestion courantes après le déploiement.



Le marché SD-WAN devrait croître à un taux de 58% pour atteindre 17 milliards de dollars d'ici 2025.[1] L'une des principales raisons de cette croissance est que le SD-WAN devient de fait la rampe d'accès aux applications cloud, affectant considérablement l'expérience et la productivité des utilisateurs. Mais la complexité du déploiement, de la gestion et de la sécurisation de ces environnements dans une entreprise distribuée pousse de plus en plus les clients à s'adresser à des prestataires de services pour leurs projets SD-WAN.

Près de 80% des responsables d'infrastructures informatiques dans une enquête récente indiquent que leur solution SD-WAN est constituée de plusieurs éléments qui sont longs et difficiles à gérer. Dans le même temps, plus de la moitié d'entre eux (53%) déclarent s'associer à des prestataires de services pour une aide en matière de mise en œuvre et de gestion.[2]

Le choix de la bonne solution SD-WAN constitue un défi

Lorsque les entreprises adoptent des initiatives numériques, elles constatent souvent que les WAN traditionnels sont trop limités pour assurer la disponibilité et les performances des derniers services numériques, tels que les applications SaaS (Software-as-a-Service), la voix sur IP (VoIP) et la vidéoconférence.[3] En règle générale, la première étape consiste à remplacer les connexions WAN vieillissantes par une solution SD-WAN. Le SD-WAN permet une connectivité efficace, rentable et centrée sur les applications, qui favorise l'utilisation des innovations numériques par l'entreprise et son écosystème.

Pour faciliter cette transition, de nombreuses entreprises se tournent vers les prestataires de services SD-WAN pour combler les lacunes et le manque de compétences de leurs équipes existantes. Une nette majorité de chefs d'entreprise font appel avec un prestataire de services, notamment pour la mise en œuvre et la gestion de produits de sécurité spécifiques.[4] Mais malgré les nombreux avantages qu'offre le SD-WAN, toutes les solutions SD-WAN ne sont pas identiques. Le choix de la mauvaise solution SD-WAN comme base d'un service managé peut avoir des répercussions considérables.

Des coûts plus élevés. Les services managés basés sur une solution SD-WAN sans fonctionnalités de sécurité intégrées exposent les clients à un risque accru, qui, à son tour, augmente les frais généraux de gestion des prestataires de services (par exemple, le temps consacré par le personnel au nettoyage des systèmes infectés dans les succursales). Les solutions SD-WAN pures (qui ne disposent pas de puissantes fonctions de sécurité intégrées) nécessitent également l'achat d'appareils et d'appliances de sécurité (ou d'appliances virtuelles) complémentaires, ainsi que davantage de temps passé à assembler et à gérer les différents éléments, et (en fin de compte) réduisent le revenu annuel par utilisateur.

Une visibilité et une gestion médiocres. Les services SD-WAN managés, assemblés à partir de plusieurs solutions de sécurité et réseau, entraînent une vision désagrégée et des contrôles de politiques déconnectés. L'investissement supplémentaire dans des produits cloisonnés et dans du personnel d'exploitation réduit le revenu annuel par utilisateur tout en augmentant les risques en raison des lacunes potentielles d'une infrastructure trop complexe. Une solution SD-WAN sans ces fonctionnalités intégrées complique également les opérations d'intégration et de gestion des services pour les prestataires de services.

Une connaissance des applications. Le routage en fonction des applications peut être particulièrement problématique. De nombreuses solutions SD-WAN ne sont pas en mesure de hiérarchiser le trafic en fonction de l'utilisateur, des appareils et des applications. Cela dégrade non seulement les performances des utilisateurs finaux mais peut également affecter les contrats de niveau de service (SLA) des prestataires de services. Certains devront même acheter des optimiseurs WAN (ce qui augmente les coûts d'investissement et d'exploitation).

Des appareils de sécurité sous-équipés. Même lorsque la sécurité est intégrée dans un service SD-WAN, elle peut être déficiente. Les produits et/ou services de sécurité individuels, lorsqu'ils sont utilisés en tandem avec une solution réseau SD-WAN autonome, peuvent donner lieu à des défenses fragmentées et réactives. Cela augmente les risques pour les clients et crée des problèmes supplémentaires avec les contrats de niveau de service, sans parler de la complexité d'intégration et d'exploitation supplémentaire pour les fournisseurs de services managés.

L'inspection du chiffrement. La plupart des solutions SD-WAN ne sont pas évolutives lorsque l'inspection SSL/TLS (Secure Sockets Layer/Transport Layer Security) est activée. Au lieu de cela, l'inspection du chiffrement entraîne une dégradation des performances à grande échelle de nombreux pare-feux réseau. Et si l'inspection SSL/TLS n'est pas activée, les entreprises courent un risque beaucoup plus élevé; jusqu'à 60% du trafic chiffré contient des logiciels malveillants cachés.[9] Les prestataires de services doivent ainsi acquérir davantage de pare-feux SD-WAN ou acheter des équipements d'inspection du chiffrement distincts, tous deux augmentant les coûts d'investissement et d'exploitation et réduisant le revenu annuel par utilisateur.

Adopter rapidement une solution SD-Branch

Le SD-WAN est à la fois un précurseur et une voie essentielle vers une solution SD-Branch. Il s'agit d'une solution clé en main dotée de l'agilité opérationnelle nécessaire pour déployer et fournir rapidement des services réseau et de sécurité sur de nouveaux sites.[10] Une solution SD-Branch consolide à la fois les infrastructures WAN et LAN pour simplifier l'infrastructure des succursales tout en étendant les fonctionnalités SD-WAN à la couche d'accès dans les succursales.

La transformation des clients en un modèle as-a-service pour favoriser l'expansion des succursales simplifie le déploiement et l'orchestration pour les entreprises en sous-effectif, tout en permettant aux prestataires de services d'étendre leur présence au sein de chaque compte et d'augmenter potentiellement leur revenu annuel par utilisateur. Mais là encore, les solutions SD-WAN pures manquent de plusieurs fonctionnalités essentielles pour fournir un service SD-Branch géré qui accroît efficacement la rentabilité.

La sécurité. Les solutions SD-WAN qui ne disposent pas de fonctionnalités de sécurité puissantes et intégrées ne peuvent pas répondre aux besoins SD-Branch essentiels, tels que :

- Le contrôle d'accès réseau
- L'identification, le suivi et la surveillance des appareils en réseau
- L'analyse du trafic des succursales
- La détection des logiciels malveillants avancés des pirates informatiques qui cherchent à lancer une attaque via la succursale généralement moins sécurisée.

Comme pour le SD-WAN, une solution avec peu ou pas de sécurité entraîne des coûts d'investissement et d'exploitation supplémentaires, ainsi qu'une plus grande exposition aux risques pour les clients (et plus de temps passé à nettoyer les infections dans les succursales), qui réduisent tout le revenu annuel par utilisateur.

La complexité et le coût. Par le passé, les infrastructures complexes des succursales comprenaient plusieurs ensembles d'outils réseau et de sécurité, chacun d'entre eux devant être acheté et géré séparément. Ce type de frais généraux réduit le revenu annuel par

Le manque de compétences en matière de cybersécurité exacerbe les problèmes de sécurité dans de nombreuses entreprises, et une majorité de chefs d'entreprise sont favorables à un partenariat avec des prestataires de services pour combler les lacunes de leurs équipes existantes.

- **58% des DSI[5]**
- **59% des RSSI[6]**
- **66% des architectes sécurité[7]**
- **74% des responsables réseaux[8]**

Dans une enquête récente, la sécurité (50%) a été classée comme le plus grand défi du WAN et le principal facteur (81%) guidant les entreprises dans le processus de sélection du SD-WAN.[11]

Selon un rapport, 41% des entreprises souhaitent que leur environnement de gestion WAN couvre l'infrastructure LAN des succursales (notamment, le Wi-Fi, la commutation).[12]

utilisateur des prestataires de services chargés de les gérer. Plus le nombre de succursales (et de solutions individuelles) augmente, plus les problèmes de coût et de complexité ne font que s'intensifier pour les prestataires de services.

Les contrats de niveau de service (SLA). Les prestataires de services peuvent également avoir du mal à respecter les contrats de niveau de service sans visibilité et intégration transparentes à toutes les couches d'accès. Par exemple, dans les configurations réseau traditionnelles des succursales, les prestataires de services sont incapables d'étendre l'application de la sécurité et la réduction des risques à tous les terminaux, y compris les appareils IoT (Internet-of-Things).

Le marché SD-Branch est actuellement à un stade embryonnaire et devrait représenter 3 milliards de dollars d'ici 2022.[13]

Le défi à venir pour les prestataires de services

Bien que toutes les technologies SD-WAN n'offrent pas de solides capacités de service, le choix de la bonne solution permet aux prestataires de services d'offrir plus qu'une simple connectivité agile à la périphérie. Il leur permet également d'ajouter des services d'accès au LAN (câblé et sans fil), de visibilité et de contrôle IoT, de rampe d'accès au cloud public et (surtout) de sécurité. Le SD-WAN peut servir de base à une plateforme de services à valeur ajoutée tout-en-un qui permet aux prestataires de services de renforcer leur présence stratégique et d'augmenter leurs revenus tout en réduisant leurs efforts d'intégration.

Le contrôle des coûts d'investissement et d'exploitation est un facteur essentiel qui doit être pris en compte pour le coût total de possession et la maximisation des profits. Une offre de services efficace doit reposer sur des technologies qui consolident et intègrent l'infrastructure réseau. Les prestataires de services peuvent ainsi limiter l'investissement initial tout en établissant une plateforme technologique qui offre des avantages essentiels, tels qu'une grande visibilité, une gestion transparente, une facilité de déploiement à grande échelle, un partage des renseignements et des réponses automatisées en matière de cybersécurité.

1 « SD-WAN Market to grow at over 58% CAGR from 2019 to 2025: Global Market Insights, Inc. », Globe Newswire, 10 mai 2019.

2 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.

3 « L'architecte Sécurité et la Cybersécurité : Un rapport sur les priorités et défis actuels », Fortinet, 29 juin 2019.

4 « Cybersécurité et le responsible de l'Ingénierie réseau et des Opérations », Fortinet, 4 septembre 2019.

5 Jason Pappalexis, « Security Controls in the US Enterprise: Software-Defined Wide Area Network (SD-WAN) », NSS Labs, consulté le 2 septembre 2019.

6 « Le DSI et la Cybersécuité : Un rapport sur les priorités et les défis actuels », Fortinet, 23 mai 2019.

7 Ibid.

8 « Le RSSI et la Cybersécurité : Un rapport sur les priorités et défis actuels », Fortinet, 26 avril 2019.

9 Omar Yaacoubi, « Les menaces cachées de la poussée du chiffrement des données liée au RGPD », Rapport PrivSec, 8 janvier 2019.

10 Lee Doyle, « SD-Branch: Qu'est ce que c'est et pourquoi vous en aurez besoin ? », Network World, 23 janvier 2018.

11 « Skills gap remains a Les principaux freins à l'adoption du SD-WAN », Help Net Security, 18 juillet 2019.

12 Shamus McGillicuddy, « Enquête: Les entreprises veulent une gestion de bout-en-bout du SD-WAN », Network World, 9 janvier 2019.

13 Cynthia Harvey, « SD-Branch: Les 4 points principaux à connaître », Network Computing, 11 juillet 2018.

FORTINET

www.fortinet.fr

13 mai, 2020 3:47 PM

281094-0-1-FR

wp-wan-evolution-presents-opportunities_A4_FR