FORTINET

LIVRE BLANC

Comprendre les obstacles à la transformation du WAN

La sécurité, la performance et le coût total de possession

Résumé

Les responsables réseaux se tournent vers le SD-WAN pour garantir l'afflux de trafic et d'applications entraîné par la transformation numérique (DX). Ces applications améliorent la productivité du personnel tout en créant de nouvelles opportunités commerciales. Elles façonnent également les besoins des entreprises en matière de réseaux et de sécurité.

En réponse, de nombreuses organisations commencent à repenser leur architecture WAN traditionnelle. Le SD-WAN a émergé comme une alternative, mais beaucoup de déploiements SD-WAN s'accompagnent également de sérieux défis, allant d'une sécurité inadéquate à un coût total de possession élevé. Comprendre ces enjeux est essentiel pour naviguer sur le marché de plus en plus complexe des technologies WAN de pointe.

IDC prévoit que le marché du SD-WAN connaîtra un taux de croissance annuel composé (TCAC) de plus de 40% d'ici 2022.[1]

«L'émergence de la technologie SD-WAN a été l'une des transformations les plus rapides que nous ayons vues depuis des années dans notre secteur. Les entreprises de toutes tailles modernisent leurs réseaux étendus afin d'offrir une meilleure expérience utilisateur pour toute une gamme d'applications cloud. »[2]

– Rohit Mehra
Vice-président, Infrastructure réseau IDC

Comment la DX impacte les réseaux d'entreprise

Les organisations sont de plus en plus nombreuses à adopter la DX. Les initiatives numériques touchent de nombreux domaines, plus particulièrement l'adoption croissante de la vidéo et de la voix sur IP (VoIP) pour la collaboration, la gestion de projets et même le développement commercial, de l'utilisation du DevOps pour accélérer le déploiement de nouvelles applications Web et de l'utilisation d'appareils IoT pour la collecte de données et la télémesure.

Cependant, ces initiatives DX présentent de nouveaux défis pour les succursales ou les bureaux distants. Les responsables réseaux sont chargés de maintenir les performances et la sécurité du réseau —du datacenter au réseau d'agence. Néanmoins, les réseaux étendus (WAN) traditionnels ne sont pas conçus pour prendre en charge le volume de trafic qui est acheminé vers les succursales et les bureaux distants. Plus précisément, ces solutions WAN utilisent un réseau basé sur la technologie MPLS qui assure le transit du trafic à travers le datacenter de l'entreprise à des fins de filtrage et de contrôles de sécurité. Cette architecture « hub-and-spoke » peut entraîner des goulets d'étranglement à la périphérie du réseau, ce qui se traduit par des performances médiocres pour les utilisateurs finaux.

Mais ce n'est pas le seul problème des solutions WAN traditionnelles. Les connexions MPLS ont un coût qui peut rapidement grimper, en particulier avec l'évolution rapide du volume de trafic des sites distants.

Répondre aux défis du WAN traditionnel

Ainsi, de nombreuses organisations adoptent les réseaux SD-WAN avec le postulat qu'ils offrent de meilleures performances. Pourtant, il existe un certain nombre de solutions SD-WAN différentes sur le marché avec des fonctionnalités variables, et il peut rapidement devenir difficile de déterminer laquelle répond aux besoins métiers. Avant que les responsables réseaux puissent évaluer les options disponibles, ils doivent examiner les raisons pour lesquelles c'est le cas avec de nombreux SD-WAN.

Une sécurité inadéquate : l'absence d'une protection complète contre les menaces

Malgré les faibles débits lorsqu'un WAN achemine tout le trafic vers le datacenter, les WAN basés sur MPLS sont généralement perçus comme suffisamment sécurisés. En revanche, pour de nombreuses solutions SD-WAN, la sécurité n'est pas intégrée ou elle est insuffisante. Plus précisément, les fonctionnalités de sécurité de la plupart des solutions SD-WAN n'adressent pas les couches 3 à 7, en raison de l'absence de système de sécurité avancé comme la prévention des intrusions (IPS), du filtrage Web, de l'inspection de la couche SSL (secure sockets layer) de transport (TSL) et d'autres types de protection.

Pour répondre à ces exigences de sécurité dans les réseaux de succursales et de bureaux distants, les responsables réseaux doivent coupler des équipements de sécurité dédiés à leur SD-WAN. À minima, cela implique l'ajout d'un pare-feu à chaque emplacement, mais parfois plus (p. ex. l'inspection SSL/TLS n'est pas disponible dans tous les pare-feux sur le marché). L'hétérogénéité de la solution crée de la complexité, ce qui augmente le coût total de possession, depuis les dépenses d'investissement (CapEx) pour l'équipement supplémentaire jusqu'au temps du personnel (dépenses opérationnelles [OpEx]) consacré à la gestion du pare-feu supplémentaire et autres équipements.

Même parmi les solutions SD-WAN qui comprennent des technologies plus avancées, il existe encore des lacunes. Par exemple, toutes les solutions SD-WAN ne disposent pas d'options de sécurité minutieusement examinées par des experts tiers tels que NSS Labs. Cette comparaison et analyse objective des solutions SD-WAN permet aux responsables réseaux de déterminer quelles solutions SD-WAN répondent le mieux aux besoins réels de l'entreprise.

La performance : un compromis avec la sécurité

La connectivité directe et le load balancing des solutions SD-WAN améliorent les performances par rapport au WAN traditionnel. A l'instar des solutions de sécurité, les solutions SD-WAN ne se valent pas toutes. En particulier, toutes les solutions SD-WAN ne sont pas capables d'identifier et de classifier le trafic applicatif et de mettre en œuvre des stratégies de routage granulaire. Ainsi la priorité des applications métiers n'est pas respectée. Sans discrimination des flux, les applications critiques, les appels VoIP et vidéo peuvent ralentir, ce qui entrave la productivité des utilisateurs finaux.

De plus, parmi le sous-ensemble des solutions SD-WAN avec sécurité intégrée, certains paramètres de sécurité peuvent dégrader les performances du réseau. Par exemple, l'activation de l'inspection des flux cryptés SSL/TLS peut avoir un impact important sur les performances de débit. Les organisations qui choisissent de ne pas déchiffrer les flux s'exposent à un risque accru : 72% du trafic réseau est crypté et 60% des attaques utilisent le cryptage pour masquer les logiciels malveillants avec cryptage SSL et TLS.[4]

Les coûts et les ressources : le coût total de possession reste élevé

Le volume du trafic réseau des applications VoIP, vidéo et SaaS est en croissance alarmante, ce qui augmente les coûts de bande passante du réseau pour de nombreuses entreprises. Si l'on considère que les coûts MPLS sont multipliés par quatre ou cinq, les économies de coûts du SD-WAN qui utilise l'Internet public sont significatives.

Pourtant, les responsables réseaux qui déploient des solutions SD-WAN sont souvent surpris de constater un coût total de possession plus élevé que prévu. Plus précisément, l'ajout de multiples équipements pour différentes fonctionnalités augmente les dépenses d'investissement (CapEx) ainsi que le temps que le personnel doit consacrer à leur gestion (OpEx). Le personnel réseau doit surveiller et compiler manuellement les logs pour la gestion des menaces. Cela prend du temps et est inefficace.

De plus, la nécessité de déployer plusieurs produits ponctuels pour chaque bureau distant et chaque succursale — qu'il s'agisse de routeurs, de pare-feux, de passerelles Web sécurisées ou d'optimisation WAN —, demande beaucoup de temps de gestion au personnel. Chaque solution a ses propres protocoles et interfaces utilisateur. Pour obtenir une visibilité et un contrôle centralisé et démontrer la conformité aux diverses réglementations et normes de sécurité de l'industrie et du gouvernement, le personnel réseau doit consacrer du temps à l'agrégation et au rapprochement manuels des données de chaque silo technologique spécifique. Face à une pénurie de compétences, cette dépense de temps peut devenir très coûteuse, car les équipes réseau ont des difficultés à s'adapter à ces exigences.

« 72% des répondants [d'après une enquête Gartner] ont indiqué que la sécurité était leur principale préoccupation lorsqu'il s'agit de leur WAN. »[3]

De nombreuses entreprises qui passent au SD-WAN réalisent des économies substantielles sur la connectivité de la bande passante — pouvant aller jusqu'à 40% dans certains cas.[5]

72% du trafic réseau est crypté, et 60% des attaques utilisent aujourd'hui le cryptage.

Le coût total de possession des solutions SD-WAN varie de 5$ à 496$ le mégabit par seconde (Mbps). Les organisations devraient évaluer méticuleusement le coût total de possession à court et à long terme de la solution SD-WAN qu'elles envisagent, afin de déterminer laquelle offre le plus de fonctionnalités pour le coût total de possession le plus bas.[6]

Les inefficacités s'accumulent dans les réseaux distribués. La gestion des solutions réseau et de sécurité oblige le personnel à se déplacer vers des sites éloignés. Plus précisément, lorsque les solutions SD-WAN n'offrent pas d'alternative virtuelle ou de fonctionnalités de déploiement « zero-touch », le temps consacré au déploiement initial et à la maintenance continue peut s'accumuler rapidement.

Conclusion : ce qu'il faut rechercher dans une solution SD-WAN

Lors de l'évaluation des nombreuses solutions SD-WAN disponibles, les responsables réseaux devraient se poser les questions suivantes :

- Quels résultats réels ont été documentés dans le monde par des tests indépendants réalisés par des tiers, comme ceux effectués par NSS Labs ?
- Comment la solution a-t-elle été évaluée dans les rapports d'analystes tiers tels, que les Magic Quadrants de Gartner ?
- En supposant que la solution dispose d'une sécurité intégrée, inclut-elle des fonctionnalités avancées — contrôles de sécurité des couches 3 à 7 : 1) IPS, 2) filtrage Web et 3) inspection approfondie du trafic crypté SSL/TLS ?
- En supposant que la solution dispose d'une fonctionnalité d'inspection SSL/TLS, quel est l'impact sur les performances lorsqu'elle est activée ?
- La solution est-elle sensible aux applications et utilise-t-elle la sélection dynamique de liens pour optimiser le routage et la hiérarchisation des applications SaaS, des appels VoIP et de la vidéo critiques pour l'entreprise ? La solution s'intègre-t-elle aux éléments de sécurité à l'échelle de l'entreprise et aux différents domaines de sécurité (p. ex., courrier, cloud, périphériques, entre autres) pour un partage intégré et automatisé des renseignements sur les menaces ?

[1] « SD-WAN Infrastructure Market Poised to Reach $4.5 Billion in 2022 », IDC, 7 août 2018.

[2] Ibid.

[3] Naresh Singh, « Survey Analysis: Address Security and Digital Concerns to Maintain Rapid SD-WAN Growth », Gartner, 12 novembre 2018.

[4] John Maddison, « More Encrypted Traffic Than Ever », Fortinet Blog, 10 décembre 2018 ; Omar Yaacoubi, « The hidden threat in GDPR's encryption push », PrivSec Report, 8 janvier 2019.

[5] Paul Ruelas, « Catching the SD-WAN wave: the cost savings hype and MPLS misconceptions need more explanation », Network World, 18 avril 2018.

[6] Thomas Skybakmoen, « SD-WAN Comparative Report », NSS Labs, 8 août 2018.

novembre 14, 2019 1:22 PM

376872-0-1-FR

wp-understanding-the-obstacles-to-wan-transformation-A4-FR