LE POINT DE VUE DE FORTINET

Le SD-WAN peut présenter des risques

Il y a quelques années seulement, ces cinq lettres se sont fait une solide réputation dans le monde de l'informatique. Cependant, avec l'explosion du trafic à la périphérie, tous les SD-WAN ne sont pas créés égaux.

Peut-être l'acronyme le plus populaire dans le monde du réseau...

Il n'est pas nécessaire d'être un architecte réseau pour connaître la terminologie. En fait, ceux qui ont rendu le SD-WAN si populaire sont ceux qui cherchent une meilleure façon de construire et de gérer une infrastructure multisite, ou ceux dont la capacité à extrapoler les coûts MPLS a presque provoqué une crise cardiaque car ils ont pris en compte le nombre de sites et la croissance du trafic dans l'équation.

Comme certains autres concepts informatiques, celui-ci est devenu célèbre parce qu'il semblait être une meilleure façon de construire un réseau et qu'il permettait en même temps de réaliser des économies.

Et à juste titre. Pourquoi continueriez-vous à dépenser une fortune en lignes louées alors qu'en plus des applications essentielles, l'ensemble de votre trafic pourrait également être transporté sur Internet ? Le SD-WAN offre des systèmes de retour sur investissement particulièrement attrayants et améliorant les performances des applications.

Rend le directeur des systèmes d'information (DSI) et le directeur financier heureux

En fait, le SD-WAN est devenu le terrain d'entente sur lequel le directeur des systèmes d'information (DSI) et le directeur financier peuvent réellement se parler et sourire. Et il n'y a pas beaucoup de sujets de ce genre. Après tout, si une technologie plaît à la fois à l'informatique et aux finances, pourquoi chercher plus loin ?

Puis une nouvelle espèce est arrivée dans la salle du conseil : le responsable de la sécurité des systèmes d'information (RSSI) dont le mandat et la position dans l'organigramme étaient beaucoup plus larges que le simple fait de s'assurer que la base de données antivirus était à jour.

Points clés

- Toutes les solutions SD-WAN ne sont pas créées égales. Ce qui était au départ un simple concept réseau doit évoluer vers une solution réseau axée sur la sécurité.
- Les fonctionnalités de base d'un pare-feu ne suffisent pas. Comme la menace devient plus sophistiquée et que la vitesse augmente considérablement, il est essentiel que la solution SD-WAN s'intègre nativement à l'ensemble de l'écosystème de sécurité.
- Le déploiement automatisé est la clé. Lors de la configuration manuelle, les retards, les erreurs et les problèmes d'évolutivité sont très susceptibles d'affecter le projet.
- La visibilité est primordiale. Comme le nombre de sites distants et le nombre d'appareils par site augmentent régulièrement, le maintien d'une vue centralisée de la surface d'attaque devient une nécessité absolue.

Le MPLS ne suffit pas

Malgré tous les avantages que présentent les lignes louées et le MPLS en termes de sécurité, il serait erroné de supposer que le niveau de protection dont vous bénéficiez dans votre datacenter se répercute automatiquement sur les sites distants. Comme les applications se multiplient et que le trafic augmente progressivement, la sécurisation des sites distants nécessite une protection de nouvelle génération. Un autre point important est que le déploiement SD-WAN repose sur des appliances qui se trouvent à la périphérie du réseau, une zone nettement plus exposée aux menaces.

Afin d'effectuer le bon investissement, voici quelques considérations importantes que les RSSI doivent garder à l'esprit :

Les règles d'or pour choisir un SD-WAN

- Un simple pare-feu ne suffira pas à vous protéger, d'autant plus que les menaces ne cessent de croître en volume et en sophistication. Choisissez une solution qui prend en charge toute la gamme des fonctionnalités de pare-feu de nouvelle génération (NGFW), telles que l'antivirus, le système de prévention des intrusions, le contrôle des applications et le filtrage des URL. Vérifiez également les performances globales avec les fonctions de sécurité activées pour évaluer correctement l'impact de la sécurité avancée sur les performances réseau.
- Exigez un déploiement automatisé. À mesure que le nombre de sites distants augmente, ainsi que le nombre d'appareils connectés par site, le déploiement manuel devient une charge et une source d'erreur. Associé à un contrôleur centralisé, le déploiement automatisé est la clé de l'évolutivité, minimise l'erreur humaine et garantit une sécurité renforcée.
- Profitez de la diversification de l'offre de transport pour réduire vos coûts et renforcer la continuité des activités. L'ajout d'un ou de deux prestataires de services vous offre plus d'options en cas de défaillances techniques ou d'attaques.

De la sécurité à la mise en réseau, et non l'inverse

Aussi puissante que puisse être la technologie SD-WAN, il n'est tout simplement pas sûr de la déployer massivement et de considérer la sécurité comme la deuxième étape. Cela conduit généralement à une multiplicité de technologies de sécurité dont l'intégration ultérieure est inévitablement longue, coûteuse et sujette aux erreurs. En fait, alors que la fusion de la mise en réseau et de la sécurité devient une réalité mondiale, il est beaucoup plus rentable et sûr d'adopter une solution SD-WAN dont les fonctions de sécurité avancées sont intégrées nativement aux fonctions réseau. L'alliance du DSI et du directeur financier basée sur les performances et le coût n'est durable que si elle prend en compte le programme de sécurité du RSSI comme un élément clé du processus de sélection et de mise en oeuvre du SD-WAN.

June 14, 2021 11:12 AM

fortinet:Shared:CREATIVE SERVICES:EMEA Creative Server:03_DOCUMENTS:22_PointOfView-POV:2021:POV-sdwan-can-hurt:French:pov-sdwan-can-hurt-A4-FR

1006801-0-1-FR