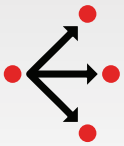
LE POINT DE VUE DE FORTINET

Il est temps de remplacer les routeurs de succursales

Les quatre grands avantages d'un SD-WAN sécurisé.

De plus en plus d'organisations abandonnent les routeurs des succursales au profit d'un SD-WAN sécurisé pour se préparer au cloud et améliorer l'expérience de l'utilisateur. Les solutions de SD-WAN sécurisé sont non seulement simples à gérer, mais elles simplifient également les opérations du WAN en général.

Les organisations doivent adopter des solutions SD-WAN sécurisées pour aider les utilisateurs des succursales à mieux tirer parti des communications unifiées et de la collaboration, à utiliser des applications SaaS essentielles et à accéder facilement aux ressources stockées dans le cloud. Voici quatre avantages clés que le SD-WAN sécurisé offre par rapport aux architectures de routage des succursales existantes :



Les solutions SD-WAN sécurisées sont faciles à gérer et simplifient les opérations du WAN en général.

1. Une plus grande agilité des applications

Les routeurs fonctionnent sur la base de paquets et ne sont donc pas en mesure de fournir une visibilité approfondie des applications. La majorité des organisations ayant investi dans les applications et les services cloud, l'incapacité d'identifier ces applications critiques pour les entreprises et d'appliquer des protocoles afin de répondre à leurs besoins uniques en matière de bande passante et de connectivité peut dégrader l'expérience de l'utilisateur. Les solutions SD-WAN peuvent faire tout ce qu'un routeur traditionnel peut faire, comme fournir un routage avancé et une connectivité WAN. Au-delà des fonctions de routage traditionnelles, toutefois, les solutions SD-WAN :

- Identifient et orientent les applications en utilisant la sélection dynamique des chemins d'accès pour une qualité d'expérience constante;
- Peuvent identifier les applications et créer des SLA pour des milliers d'applications telles que O365, Salesforce.com et des communications unifiées ;
- Ont la capacité de mettre à jour les applications commerciales au quotidien pour s'assurer que les applications sont identifiées avec précision et qu'elles prennent le meilleur chemin d'accès.

2. Une évolutivité simple, avec des économies en capex (économies d'investissement) et en opex (économies d'exploitation) considérables

Les vitesses et les volumes des connexions MPLS sont prédéterminés et coûteux, ce qui signifie qu'une soudaine augmentation du trafic — comme de multiples connexions de communications unifiées à haut débit ou la nécessité de traiter une grande quantité de données — peut affecter tout le monde. L'ajout de nouveaux sites de routage pour les succursales est également un processus long et coûteux.

Les solutions SD-WAN peuvent toutefois aider les clients à migrer de MPLS vers le haut débit (DSL, 4G/5G, Ethernet) et à réaliser des économies en opex (économies d'exploitation) de 40 % dans de nombreux cas. Le SD-WAN permet aux entreprises d'évoluer de manière dynamique et sécurisée vers des dizaines de milliers de succursales, d'interagir de manière transparente avec les infrastructures physiques et cloud existantes, et fournir un service de dépannage à distance afin d'éliminer les interventions physiques coûteuses des techniciens qualifiés. Le SD-WAN sécurisé regroupe également une gamme de produits ponctuels, notamment des routeurs, des firewalls et des outils d'optimisation WAN, en un seul produit, ce qui permet de réaliser des économies en capex (économies d'investissement) considérables.

3. Une gestion et une orchestration simplifiées

Les routeurs de succursales sont souvent complexes à installer, à mettre à niveau et à entretenir, même lorsqu'ils sont censés être une solution « à faible coût ». La configuration nécessite une expertise de l'interface en ligne de commande (CLI) d'un routeur et, en raison de sa complexité, elle peut rarement être effectuée par une ressource locale d'une succursale.

La gestion centralisée et sécurisée du SD-WAN garantit que les nouveaux services et les nouvelles politiques sont axés sur les applications et que les configurations de connectivité et de sécurité ainsi que les changements de politiques peuvent être propagés de manière transparente sur l'ensemble du WAN étendu, éliminant ainsi la nécessité de configurer ou de gérer chaque appareil ou service sur le plan individuel.
Un SD-WAN sécurisé et centralisé fournit également des analyses complètent qui montrent l'historique et les performances des applications en temps réel, ce qui permet aux équipes de dépanner rapidement et d'améliorer les mesures de performances clés, telles que le délai moyen de réponse des applications.

4. Un réseau et une sécurité intégrés

Les routeurs de succursales ne sont en aucun cas des solutions réseau et de sécurité totalement intégrées.

Lorsque le système MPLS est complété par un tunnel divisé pour permettre un accès direct à Internet, les routeurs de succursales ne permettent que peu ou pas de gestion des liens ou des connexions. Même lorsque le trafic est interrompu ou déplacé vers un autre chemin, ils ne disposent pas de la direction proactive de la sous-seconde nécessaire pour éviter les interruptions de connexion, et n'ont pas la capacité d'atténuer les problèmes de transport ou de fournir des éléments tels que la mise en mémoire tampon dynamique de la gigue. Ils ne sont pas non plus en mesure de réguler activement le trafic avant que la saturation ne devienne problématique. Pire encore, comme les routeurs manquent de sécurité efficace, ces connexions non MPLS exposent votre organisation à un risque supplémentaire.

Mais il est important de noter que la plupart des solutions SD-WAN ne sont pas sans poser de problèmes de sécurité. En effet, l'une des exigences essentielles pour le succès du SD-WAN est une sécurité totalement intégrée. Les pare-feux de nouvelle génération (NGFW), dont les principaux composants sont l'IPS, le filtrage Web, l'inspection SSL et l'anti-malware, sont un exemple de solution intégrée. Sans une sécurité totalement intégrée, le SD-WAN devient un canal de plus pour les logiciels malveillants et les cybercriminels qui s'attaquent à votre réseau.

Une véritable plate-forme a besoin d'outils explicitement conçus pour interagir comme un système unique, idéalement avec chaque élément fonctionnant sur le même système d'exploitation et géré à l'aide d'une interface à écran unique. Cela garantit que toutes les transactions sont vues et inspectées, et que toute menace ou comportement anormal est partagé entre chaque solution pour une protection optimale.

Dans le cadre d'un tel système intégré, les fonctionnalités réseau et de connectivité d'un SD-WAN ne sont pas seulement plus étroitement associées aux solutions de sécurité installées sur la plate-forme ; elles sont identiques.

Autres éléments à prendre en compte pour passer à l'étape suivante

Il est essentiel de reconnaître non seulement la nécessité de s'éloigner d'une stratégie WAN traditionnelle basée sur les routeurs, mais aussi de choisir avec soin une solution SD-WAN sécurisée, conçue pour offrir tout le spectre des fonctionnalités et le plus grand nombre possible de cas d'utilisation. Cela permet de s'assurer que votre nouveau déploiement SD-WAN répond non seulement aux besoins actuels de votre organisation, mais qu'il peut également s'adapter à l'évolution rapide de vos exigences.

FORTINET

www.fortinet.fr

June 1, 2021 3:30 PM

Sheldon:Fortinet:2021-04-1006801-Updating-branding-SD-WAN-assets:pov-sdwan-branch-routers:French:pov-sdwan-branch-routers-FR

1006801-0-1-FR