Les firewalls de nouvelle génération de la famille FortiGate combinent des fonctionnalités SD-WAN complètes avec des aspects de sécurité pour former un tout.

Bild: Laurence Dutton/iStock.com

Secure SD-WAN

WAN edge transformation with security-driven networking

Réseau sécurisé pour tous les sites

La technologie MPLS a fait son temps dans les réseaux de sites. L'alternative SD-WAN est moins chère et offre des bandes passantes plus élevées. D'autres avantages incluent la combinaison du SD-WAN avec des fonctions de sécurité complètes et la gestion consolidée de l'ensemble du site.

Par le passé, les connexions MPLS étaient souvent utilisées pour mettre en réseau différents sites de l'entreprise. Dans ce type de déploiement, les fournisseurs de télécommunications offrent à leurs clients professionnels des connexions sécurisées entre le siège, les succursales, les centres de données et d'autres sites via des routeurs MPLS spéciaux. Toutefois, le MPLS présente plusieurs inconvénients. Le service est coûteux et la bande passante est limitée. En outre, le trafic Internet est généralement géré de manière centralisée avec un impact négatif sur les performances. De plus, les paquets de données du réseau MPLS sont souvent transmis en clair. En outre, la distinction entre différents clients n'est faite que sur la base d'une balise spécifique au client dans les paquets de données, ce qui représente un risque potentiel pour la sécurité.

Pour réduire les coûts d'exploitation tout en augmentant la bande passante, de nombreuses entreprises passent du MPLS au SD-WAN (Software-Defined Wide Area Network). L'Internet public sert alors de moyen de transport. En fonction de la capacité et des exigences de qualité, plusieurs liaisons Internet peuvent être combinées via un contrôle logiciel pour former un seul réseau virtuel privé – même provenant de différents fournisseurs et utilisant différentes technologies telles que la fibre optique, DSL ou 4G. Chaque connexion individuelle est sécurisée par un tunnel VPN.

SD-WAN avec des extras

La technologie SD-WAN n'offre cependant aucun élément de sécurité en dehors de la sécurité VPN inhérente. Par conséquent, les fonctions de firewall, UTM, surveillance et contrôle à des niveaux de protocole plus élevés nécessitent des systèmes supplémentaires en plus de l'appareil SD-WAN. Fortinet adopte une approche différente et combine sous un même toit toutes les fonctions importantes pour un réseau sécurisé. Sous le nom de Secure SD-WAN, Fortinet combine des fonctionnalités SD-WAN étendues avec la sécurité complète de Fortinet Security Fabric.

Les fonctions étendues comprennent notamment le contrôle des applications au niveau de la couche 7. On peut ainsi définir des stratégies de «pilotage» pour des applications SaaS et des groupes d'applications spécifiques sur la base de critères tels que la qualité de la connexion, la bande passante et le coût. L'appliance FortiGate sélectionne alors automatiquement la connexion optimale, surveille le trafic et ajuste dynamiquement le lien pour répondre aux problèmes d'équilibrage de charge et de basculement. Pour les applications critiques, des SLA peuvent être définis avec des objectifs spécifiques (par exemple, de faibles temps de latence pour la VoIP, une bande passante et une disponibilité élevée pour Office 365, ou encore une priorité moindre pour la navigation Web).

Fortinet est le premier fabricant à lancer un Secure SD-WAN accéléré au niveau matériel avec la puce «SD-WAN» SoC4 développée spécialement. Le CPU de l'appliance FortiGate est ainsi libéré des opérations SD-WAN et de sécurité, ce qui augmente les performances globales du système. Le FortiGate 100F est le premier appareil à être équipé de la nouvelle puce ASIC.

De SD-WAN à SD-Branch

Le système d'exploitation du FortiGate contrôle et supporte non seulement les fonctions de sécurité complètes mais permet également de gérer les switches et les access points installés localement sans avoir besoin de matériel additionnel, logiciel séparé ou d'autres coûts supplémentaires – le tout dans une seule interface et avec une visualisation consolidée de l'ensemble du réseau (jusqu'aux utilisateurs, appareils et applications individuelles). La configuration, la surveillance et la gestion du réseau s'en trouvent grandement facilitées. Le Cloud Fortinet ou l'appliance de gestion FortiManager peuvent également être utilisés pour collecter et gérer de manière centralisée tous les sites.

Fortinet Secure SD-WAN: les points forts

- Réduction des coûts avec SD-WAN au lieu de MPLS
- SD-WAN inclus dans les fonctionnalités de base de FortiGate
- SD-WAN et firewall nouvelle génération dans une même appliance
- Configuration simple
- Accélération matérielle via un ASIC spécifique au SD-WAN
- Contrôle des applications avec des spécifications pour plus de 5000 applications
- Gestion unifiée de la sécurité, du SD-WAN, des switches et des access points
- Ajustement dynamique des liaisons sur la base de SLAs avec basculement et équilibrage de charge

BOLL
IT Security Distribution

BOLL Engineering SA

En Budron H15
1052 Le Mont-sur-Lausanne
Tél. 021 533 01 60
vente@boll.ch
www.boll.ch