Advertorial

Sichere Standortvernetzung

SD-WAN ist preiswerter als MPLS, bietet höhere Bandbreiten, ermöglicht die Kombination mit umfassenden Sicherheitsfunktionen und erlaubt ein konsolidiertes Management des gesamten Standorts.

Für die Vernetzung verschiedener Firmenstandorte wurden bisher oft MPLS-Verbindungen genutzt. Dabei offerieren Telekom-Anbieter ihren Geschäftskunden über spezielle MPLS-Router sichere Verbindungen zwischen Hauptsitz, Filialen, Rechenzentren und anderen Standorten. MPLS hat allerdings diverse Nachteile. Der Service ist teuer, die Bandbreite begrenzt. Zudem wird der Verkehr mit dem Internet meist zentral über eine Breakout-Schnittstelle abgewickelt, was sich negativ auf die Performance auswirkt. Darüber hinaus werden die Datenpakete im MPLS-Netz häufig unverschlüsselt übertragen. Zudem erfolgt die Unterscheidung zwischen verschiedenen Kunden einzig über ein kundenspezifisches Tag in den Datenpaketen, was ein potenzielles Sicherheitsrisiko darstellt.

Um die Betriebskosten zu senken und gleichzeitig höhere Bandbreiten zu erreichen, steigen viele Unternehmen von MPLS auf SD-WAN um (Software-Defined Wide Area Network). Dabei dient das öffentliche Internet als Transportmedium. Es können je nach Kapazitäts- und Qualitätsbedarf mehrere Internet-Links per Software-Steuerung zu einer einheitlichen virtuell-privaten Vernetzung zusammengefasst werden – auch von verschiedenen Providern und über unterschiedliche Technologien wie Glasfaser, DSL oder 4G. Jede einzelne Verbindung wird dabei durch einen VPN-Tunnel gesichert.

SD-WAN mit Extras

SD-WAN per se bietet jedoch über die inhärente VPN-Sicherheit hinaus keine Sicherheitselemente. Deshalb werden für Firewall-, UTM- sowie Monitoring- und Steuerungs-Funktionen auf höheren Protokollebenen nebst dem SD-WAN-Gerät zusätzliche Systeme benötigt. Fortinet geht hier einen anderen Weg und vereint sämtliche für die sichere Vernetzung wichtigen Funktionen unter einem Dach.

Die Next-Generation-Firewalls der FortiGate-Familie kombinieren umfassende SD-WAN-Funktionalitäten mit Security-Aspekten zu einem integralen Ganzen.

So kombiniert Fortinet unter der Bezeichnung Secure SD-WAN weitreichende SD-WAN-Funktionalitäten mit der umfassenden Sicherheit der «Fortinet Security Fabric».

Zu den weitreichenden Funktionen gehört unter anderem Application Control auf Layer-7-Ebene. Dadurch lassen sich für bestimmte SaaS-Anwendungen und Anwendungsgruppen «Steering»-Strategien anhand von Kriterien wie Qualität, Bandbreite und Kostenfaktor festlegen. Die FortiGate-Appliance wählt dann automatisch die optimale Verbindung, überwacht den Datenverkehr und passt den Link bei Problemen per Load Balancing und Failover dynamisch an. So lassen sich für missionskritische und weniger wichtige Anwendungen SLAs mit konkreten Vorgaben definieren (zum Beispiel niedrige Latenzen für VoIP, hohe Bandbreite und Verfügbarkeit für Office 365 und geringere Priorität fürs Surfen im Web).

Mit dem eigens entwickelten «SD-WAN-Chip» SoC4 lanciert Fortinet als erster Hersteller ein hardwarebeschleunigtes Secure SD-WAN. Dabei wird die CPU der FortiGate-Appliance von SD-WAN- und Security-Operationen entlastet, was die Gesamtperformance des Systems um ein Mehrfaches erhöht. Als erste Appliance ist die FortiGate 100F mit dem neuen ASIC-Chip ausgestattet.

Von SD-WAN zu SD-Branch

Das FortiGate-Betriebssystem kontrolliert und unterstützt nicht nur die umfassenden Sicherheitsfunktionen, sondern erlaubt ohne zusätzliche Hardware, separate Software oder Mehrkosten das Management der lokal installierten Switches und Access Points – alles unter einer Oberfläche sowie mit einer konsolidierten Visualisierung des gesamten Netzwerks (bis hin zu einzelnen Nutzern, Geräten und Applikationen). Damit wird die Konfiguration, Überwachung und Verwaltung des Netzwerks wesentlich einfacher. Über die Fortinet-Cloud oder über die Management-Appliance FortiManager von Fortinet können überdies sämtliche Standorte zentral erfasst und gemanagt werden.

Fortinet Secure SD-WAN: die Highlights

- Kosteneinsparungen mit SD-WAN statt MPLS
- SD-WAN im Basis-Funktionsumfang von FortiGate enthalten
- SD-WAN und Next Generation Firewall in einer einzigen Appliance
- Unkomplizierte Einrichtung
- Hardwarebeschleunigung mittels SD-WAN-spezifischem ASIC
- Application Control mit Vorgaben für über 5000 Anwendungen
- Einheitliches Management von Sicherheit, SD-WAN, Switches und Access Points
- Dynamische Anpassung der Links anhand von SLAs mit Failover und Load Balancing

Kontakt

BOLL Engineering AG
Jurastrasse 58, 5430 Wettingen
Tel. 056 437 60 60, info@boll.ch, www.boll.ch