Top SD-WAN-Features

Auf einen Blick

Policy Based Routing

Die Kontrolle darüber, welche Anwendungen in Unternehmensnetzwerken erlaubt oder blockiert sind, ist entscheidend. Dies kann im modernen SD-WAN-Netz leicht verwaltet werden: Durch Policy-Based Routing können Anwendungen beispielsweise umgeleitet oder blockiert werden. Für vertrauenswürdige Anwendungen ist es zudem empfehlenswert, an den einzelnen Standorten eine Priorisierung durch einen Local Internet Breakout vorzunehmen. Dadurch wird die Verbindung zur Zentrale entlastet und die Gesamtleistung des Netzwerks verbessert.

Load Balancing

Der Active / Active-Betrieb, bei dem mehrere Internetzugänge an einem Standort parallel genutzt und durch Load Balancing verteilt werden, steigert die verfügbare Gesamtbandbreite und ermöglicht eine dynamische Lastverteilung. Dieser Modus unterstützt die flexible und gleichzeitige Nutzung sämtlicher kabelgebundener Verbindungen – sei es Ethernet, Glasfaser, DSL / Kabel über externes Modem oder sogar Mobilfunk.

Advanced Routing & Forwarding

ARF, oder Advanced Routing and Forwarding, ist eine Technologie, die es ermöglicht, über ein zentrales Gateway getrennte Kommunikationskanäle für verschiedene Anwendergruppen (wie Buchhaltung, Entwicklung und Management) einzurichten. Jeder Kommunikationskanal oder IP-Kontext ist dabei isoliert, sodass unterschiedliche Teilnehmer je nach Bedarf Zugriff auf bestimmte IP-Kontexte erhalten können, während andere Bereiche gesperrt bleiben.

High Scalability VPN (HSVPN)

HSVPN verbessert die Skalierbarkeit und Effizienz einer SD-WAN-Architektur erheblich, insbesondere in Zeiten wachsender Digitalisierung, zunehmender Anwendungsvielfalt und steigender Datenmengen. Statt für jede Anwendung einen separaten VPN-Tunnel zu nutzen, ermöglicht HSVPN das Bündeln beliebig vieler Netzwerke in einem einzigen VPN-Tunnel (Secure Tunneling), der zur Gegenstelle transportiert wird. Dabei bleiben die einzelnen Netzwerke sicher und strikt voneinander getrennt. Der Vorteil liegt in der Reduzierung der benötigten VPN-Tunnel und schnelleren Wiederherstellungszeiten bei einem Failover.

Control & Data Plane

Ein entscheidendes Sicherheitsmerkmal moderner SD-WAN-Infrastrukturen ist die strikte Trennung zwischen Management- (Control Plane) und Datenverbindungen (Data Plane). Während die Datenverbindungen, wie VPN-Tunnel, direkt zwischen den VPN-Gateways hergestellt werden, kommuniziert jede Netzwerkkomponente über eine separate Managementverbindung mit einem Orchestrator. Das bedeutet, dass die Nutzdaten für das Managementsystem unsichtbar bleiben und das Management sowie Monitoring der Netzwerkkomponenten unabhängig von den Datenverbindungen erfolgt. Dieser Prozess wird vollautomatisch und ohne vorherige manuelle Konfiguration der Geräte (zero-touch Provisioning) durch einen gesicherten Verbindungsaufbau vom Gerät zum Management-System durchgeführt. Durch die Verlagerung der Control Plane in eine zentrale Cloud entsteht der Vorteil einer stets erreichbaren, standortunabhängigen, zentralen und webbasierten Administrationsoberfläche für alle Geräte und Anwendungen an allen Standorten.

Application Monitoring

In der heutigen Zeit ist es entscheidend zu wissen, welche Anwendungen im Netzwerk genutzt werden, um effektives Application Management betreiben zu können. Ein modernes SD-WAN überwacht kontinuierlich, welche Benutzer in welchem Umfang welche Anwendungen verwenden (Top-Benutzer / Top-Anwendungen). Historische Protokollierung und grafische Auswertungen liefern eine umfassende Übersicht, die als Grundlage für fundierte Netzwerkentscheidungen dient.

Dynamic Path Selection

Mit Dynamic Path Selection werden in einem SD-WAN geschäftskritische Anwendungen stets über die beste verfügbare Leitung geroutet. Dieses Feature überwacht kontinuierlich alle WAN-Verbindungen hinsichtlich Last, Paketverlust, Latenz und Jitter (Path Quality Monitoring) und wählt dynamisch die optimale Leitung für bestimmte Anwendungen basierend auf der aktuellen Verbindungs¬qualität aus. Der Algorithmus für Dynamic Path Selection entscheidet sich für die Leitung mit der besten Performance. Falls mehrere Leitungen die festgelegten Richtlinien erfüllen, erfolgt ein Load Balancing im Round-Robin-Verfahren. Dadurch profitieren Anwender in umfangreichen SD-WAN-Infrastrukturen mit mehreren WAN-Verbindungen im Active/Active-Modus von höchster Leistung und Ausfallsicherheit.

Advanced Mesh VPN

In klassischen, sternförmigen VPN-Standortvernetzungen, bei denen alle Filialen nur über die Zentrale und nicht direkt untereinander verbunden sind, wird die Internetleitung der Zentrale oft zum Engpass für die gesamte Kommunikation. Mit Advanced Mesh VPN können die Zweigstellen direkt miteinander kommunizieren, was den Traffic in der Zentrale reduziert und die Performance erhöht. Die VPN-Tunnel werden dynamisch aufgebaut, wenn Daten zwischen den Filialen übertragen werden, und ebenso dynamisch wieder abgebaut, wenn keine Kommunikation mehr stattfindet.

Firewall-Features

Die digitalisierte Gegenwart und ausgeklügelte Cyber-Angriffe erfordern neue Maßstäbe in der Netzwerksicherheit. Anwendungskontrolle, Blockierung, Angriffserkennung und -prävention sind unverzichtbar für sichere IT-Netzwerke. Im leistungsstarken Firewall-Betriebssystem LCOS FX integriert, bieten diese und weitere UTM-Sicherheitsfunktionen „engineered in Germany“ einen erheblichen Sicherheitsvorteil. Das Feature-Set der LANCOM R&S®Unified Firewalls und LANCOM vFirewalls wird regelmäßig erweitert, um professionelle Netzwerke gegen neuartige Risiken zu schützen.

LANCOM SYSTEMS