

TIPPS VON FORTINET

# Abschied von Routern in Filialen

4 Hauptvorteile eines sicheren SD-WANs.



Immer mehr Unternehmen ersetzen Filial-Router durch ein Secure SD-WAN, um Cloud-Lösungen zu unterstützen und die Benutzererfahrung zu verbessern. Solche sicheren SD-WAN-Lösungen sind nicht nur leicht zu verwalten, sondern vereinfachen auch den gesamten WAN-Betrieb.

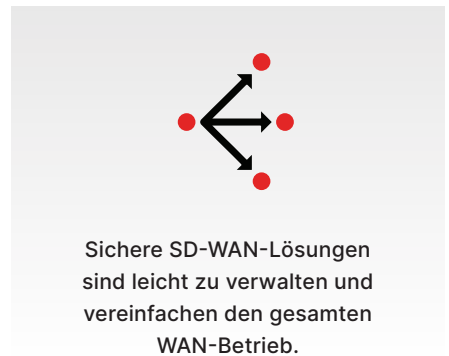
Unternehmen sollten auf sichere SD-WAN-Lösungen umstellen, damit Benutzer in Filialen stärker von Unified Communications, einer besseren Zusammenarbeit, wichtigen SaaS-Anwendungen und einem einfachen Zugriff auf Cloud-Ressourcen profitieren. Gegenüber älteren Routing-Architekturen bietet ein Secure SD-WAN vier wesentliche Vorteile:

## 1. Mehr Agilität für Anwendungen

Router übertragen Pakete und lassen sich deshalb nicht auf bestimmte Applikationen abstimmen. Da aber die meisten Unternehmen in Cloud-Anwendungen und Cloud-Dienste investieren, kann die Benutzererfahrung darunter leiden, wenn geschäftskritische Anwendungen nicht erkannt und Protokolle ignoriert werden, die für spezielle Bandbreiten- und Konnektivitätsanforderungen notwendig sind.

SD-WAN-Lösungen können alles, was ein herkömmlicher Router kann (z. B. erweitertes Routing und Bereitstellen der WAN-Konnektivität), bieten darüber hinaus aber noch zusätzliche Möglichkeiten, die über die üblichen Routing-Funktionen hinausgehen:

- Identifizieren und Steuern von Anwendungen mit dynamischer Pfadauswahl für eine gleichbleibend hohe Quality of Experience (QoE)
- Identifizieren von Anwendungen und Service-Vereinbarungen (SLA) für Tausende von Anwendungen wie Office 365, Salesforce und Unified Communications
- Tägliche Aktualisierung von Geschäftsanwendungen, damit Applikationen korrekt identifiziert werden und den optimalen Pfad verwenden



## 2. Einfache Skalierung mit erheblichen Einsparungen bei Investitions- und Betriebskosten

Bei MPLS-Verbindungen sind Geschwindigkeit und Datenvolumen fix – und kostspielig. Das bedeutet, dass bei einem plötzlichen Anstieg des Datenverkehrs – wie z. B. mehrere High-Speed-Verbindungen für Unified Communications oder die Verarbeitung großer Datenmengen – alle Benutzer von einem langsameren Durchsatz betroffen sein können. Zudem ist die Einbindung neuer Standorte mit Filial-Routern ein kostspieliger, zeitaufwändiger Prozess.

SD-WAN-Lösungen vereinfachen die Umstellung von MPLS auf Breitband (DSL, 4G/5G, Ethernet) und eröffnen in vielen Fällen ein Einsparpotenzial bei den Betriebskosten um bis zu 40 %. Mit einem SD-WAN können Unternehmen dynamisch und sicher auf Zehntausende Filialen skalieren, nahtlos mit vorhandenen physischen und Cloud-Infrastrukturen zusammenarbeiten und Fehler per Fernzugriff beheben, um kostspielige Technikereinsätze vor Ort zu vermeiden. Ein sicheres SD-WAN konsolidiert zudem mehrere Einzelprodukte – wie Router, Firewalls und WAN-Optimierungs-Tools – in einem einzigen Produkt, wodurch die Investitionskosten deutlich sinken.

## 3. Einfacheres Management, einfachere Orchestrierung

Filial-Router sind häufig komplex zu installieren, zu aktualisieren und zu warten – selbst wenn es sich um eine vermeintliche „Low-Touch“- Lösung handelt. Die Konfiguration erfordert Kenntnisse über die Befehlszeilen-Schnittstelle (CLI) eines Routers und kann aufgrund ihrer Komplexität nur selten von einem Mitarbeiter in der Filiale vorgenommen werden.

Durch das zentralisierte Management eines Secure SD-WANs wird sichergestellt, dass neue Dienste und Richtlinien anwendungsorientiert sind und Konnektivitäts- und Sicherheitskonfigurationen sowie Richtlinienänderungen nahtlos im erweiterten WAN übernommen werden. Das bedeutet: Ihr Team muss nicht jedes Gerät und jeden Dienst einzeln konfigurieren und verwalten. Ein zentralisiertes Secure SD-WAN bietet außerdem umfassende Analysen, die die bisherige Leistung von Anwendungen in Echtzeit anzeigen. So können Teams Fehler schnell beheben und wichtige Performance-Kennzahlen wie die durchschnittliche Reaktionszeit umgehend verbessern.

## 4. Integrierte Security- und Netzwerk-Dienste

Filial-Router sind bei weitem keine vollintegrierten Sicherheits- und Netzwerk-Lösungen. Wird die MPLS-Verbindung durch Split-Tunneling für einen direkten Internetzugang ergänzt, lassen sich Links oder Verbindungen mit einem Filial-Router kaum oder gar nicht verwalten. Bei einem Traffic-Failover oder der Verlagerung von Datenverkehr auf einen alternativen Pfad bietet ein Filial-Router keine proaktive Umleitung in Sekundenbruchteilen, um Verbindungsabbrüche zu vermeiden. Auch kann ein Router weder Übertragungsprobleme abmildern noch eine dynamische Jitter-Pufferung bereitstellen oder den Datenverkehr aktiv regulieren, bevor Engpässe zum Problem werden. Schlimmer noch: Da Routern eine effektive Security fehlt, setzen Backup-Verbindungen bei einem MPLS-Ausfall Ihr Unternehmen einem zusätzlichen Risiko aus.

Es muss jedoch darauf hingewiesen werden, dass die meisten SD-WAN-Lösungen bei der Sicherheit schlecht abschneiden. Eine entscheidende Voraussetzung für den Erfolg eines SD-WANs ist daher eine vollständig integrierte Security – ansonsten wird das SD-WAN zu einem weiteren „Zugangstor“ für Malware- und Cyber-Kriminelle, um Ihr Netzwerk anzugreifen. Ein Beispiel für eine integrierte Security-Lösung sind Next-Generation-Firewalls (NGFWs) mit Kernfunktionen wie IPS, Web-Filter, SSL-Inspektion und Malware-Schutz.

Eine gut funktionierende Plattform sollte Tools bieten, die explizit für die Zusammenarbeit konzipiert sind und wie ein einziges System funktionieren. Idealerweise arbeitet jedes Element mit dem gleichen Betriebssystem und wird über eine einzige „Schaltzentrale“ verwaltet. Das gewährleistet, dass sämtliche Transaktionen sichtbar sind und überprüft werden. Alle Sicherheitskomponenten können so Informationen über Bedrohungen und anomale Verhaltensweisen austauschen, um einen maximalen Schutz sicherzustellen. Das SD-WAN ist damit Teil eines integrierten Systems und verwendet für seine Netzwerk- und Konnektivitätsfunktionen die gleichen Sicherheitslösungen wie die gesamte Plattform.

## Überlegungen für die nächste Phase

Es ist wichtig, nicht nur die Notwendigkeit einer Umstellung von einer herkömmlichen routerbasierten WAN-Strategie zu erkennen, sondern auch sorgfältig eine sichere SD-WAN-Lösung auszuwählen, die das gesamte Funktionsspektrum und die größtmögliche Anzahl von Anwendungsfällen bietet. So stellen Sie sicher, dass Ihre neue SD-WAN-Implementierung nicht nur den heutigen Anforderungen Ihres Unternehmens entspricht, sondern sich auch an schnell wechselnde Erfordernisse anpassen lässt.