SOLUTION BRIEF

Upgrade von Filialinfrastrukturen mit Fortinet Secure SD-WAN

Zusammenfassung

Da der Einsatz geschäftskritischer, cloudbasierter Anwendungen und Tools weiter zunimmt, wechseln dezentrale Unternehmen mit mehreren entfernten Standorten von Wide Area Networks (WANs) mit beschränkter Leistung zu softwaredefinierten WAN-Architekturen (SD-WAN). SD-WAN bietet schnellere Konnektivität, Kosteneinsparungen und Leistung für Software-as-a-Service (SaaS)-Anwendungen sowie digitale Sprach- und Video-Dienste. Aber SD-WAN kommt mit eigenen Schwächen – vor allem in Sachen Sicherheit.

Es wird erwartet, dass der globale SD-WAN-Markt mit einer durchschnittlichen jährlichen Wachstumsrate (CAGR) von über 40 % wächst und bis 2022 einen Umfang von 4,5 Milliarden USD erreicht.[4]

Fortinet FortiGate Next-Generation Firewalls (NGFWs) verfügen über Secure SD-WAN-Funktionen, die sicherheitsorientierte Netzwerke in einer einheitlichen Lösung bereitstellen. Die Fortinet-Lösung steigert die Anwendungsleistung durch sofortige Identifizierung und intelligentes Routing. Zusätzliche Funktionen erhöhen die Leistung des Filialnetzwerks und vereinfachen gleichzeitig die Workflows im Bereich Security und Compliance-Risikomanagement.

Verteilte Unternehmen setzen Technologien der digitalen Transformation (DX) wie SaaS-Anwendungen und IP-basierte Tools für Sprache und Video ein, um die Produktivität zu steigern, die Kommunikation zu verbessern und das schnelle Geschäftswachstum zu fördern. Diese cloudbasierten Tools und Services stellen jedoch hohe Anforderungen an ältere WAN-Infrastrukturen, insbesondere wenn man die Erwartungen der Unternehmensbenutzer an eine sehr hohe Leistungsqualität berücksichtigt.

Dieses Thema wird für wachsende Unternehmen immer wichtiger. Laut eines aktuellen Berichts haben 60 % der Unternehmen bereits mindestens einige SaaS-Anwendungen eingeführt.[1] Und die Einführungsraten werden an Geschwindigkeit zunehmen: Der weltweite SaaS-Markt wird voraussichtlich zwischen 2018 und 2023 mit einer durchschnittlichen jährlichen Wachstumsrate (CAGR) von 21,2 % weiter wachsen.[2] Gleichzeitig glauben 64 % der IT-Entscheider jedoch, dass die Einführung von SaaS-Technologien in ihrem Unternehmen schneller vorankommt als ihre Fähigkeit, diese zu sichern.[3]

Herkömmliche WANs nutzen private Multiprotocol Label Switching-(MPLS-)Verbindungen, die hohe Kosten für die Konnektivität mit sich bringen. Wichtiger als der Preis ist jedoch die Produktivität. Die meisten herkömmlichen WANs verfügen über eine „Hub-and-Spoke"-Architektur, die den Netzwerkverkehr der Filiale zurück zum Rechenzentrum des Unternehmens leitet, um ihn zu filtern und Sicherheitskontrollen zu unterziehen.

Dies bietet zwar einen zentralisierten Schutz, erhöht aber auch die Latenzzeiten und verlangsamt die Netzwerkleistung. Dies ist besonders für cloudbasierte Tools wie Voice over IP (VoIP) und Videokonferenztechnologien ein großes Problem. Sprache und Video stellen hohe Anforderungen an die Netzwerkressourcen, und Unternehmensbenutzer benötigen in der Regel eine qualitativ hohe Leistung dieser Dienste.

Viele Unternehmen mit verteilten Standorten, die sich inmitten von DX-Initiativen befinden, wollen daher ihre veralteten WAN-Infrastrukturen ersetzen. Sie benötigen eine Filialvernetzung mit signifikanter Vereinfachung, verbesserten Kostenstrukturen und besserer Unterstützung der Cloud-Breitstellung. Die SD-WAN-Technologie löst die genannten Probleme der Bandbreitenkosten und der Datenverkehrslatenz effektiv und ermöglicht es Unternehmen, über das MPLS hinauszugehen und öffentliche Breitbandverbindungen und selbst drahtlose 4G/LTE- und 5G-Verbindungen einzubeziehen. SD-WAN leitet den Netzwerkverkehr von den Niederlassungen in die Cloud, zur Zentrale oder zu anderen Niederlassungen, indem es den direkten Zugriff auf Cloud-Anwendungen und -Dienste ermöglicht – was es zu einer sehr beliebten Wahl für die Unternehmenstransformation macht.

SD-WAN kann ohne Security nicht erfolgreich sein

SD-WAN bietet zwar Konnektivitätsoptionen, Leistungssteigerungen und einen Kostenvorteil gegenüber herkömmlichen WANs, weist aber auch einige Schwächen auf:

- **Komplexität.** SD-WAN-Architekturen können Probleme bei der Fehlerbehebung verursacen und schwer zu verwalten sein. Dies erhöht die Belastung für das begrenzte IT-Personal und schafft oft Lücken in der Gefahrenabwehr, die für Angriffe ausgenutzt werden können.
- **Sicherheit.** Ohne den zentralisierten Schutz durch das Backhauling des Datenverkehrs über das Rechenzentrum bringt der Wechsel zu direkten Internet-Breitbandverbindungen neue Risiken mit sich – insbesondere wenn man bedenkt, dass Cyber-Angriffe sowohl an Volumen als auch an Komplexität zunehmen. Eine effektive SD-WAN-Implementierung setzt zusätzliche Security-Funktionen innerhalb der Unternehmensinfrastruktur voraus, um diese Verbindungen zu schützen und große Datenvolumen zu prüfen – und das alles, ohne die Netzwerkleistung zu beeinträchtigen.
- **Verschlüsselte Datenverkehrsprüfung.** Den meisten SD-WAN-Lösungen fehlt die Möglichkeit, den SSL-(Secure Sockets Layer-) bzw. TLS-(Transport Layer Security-) verschlüsselten Datenverkehr, der heute 72 % des Netzwerkverkehrs ausmacht, zu überprüfen.[5] Insbesondere da Cyber-Kriminelle Malware verbergen, um Netzwerke zu infiltrieren und Daten abzuschöpfen, setzen sich Unternehmen entweder selbst einem Risiko aus oder müssen zusätzliche Geräte kaufen, um verschlüsselten Datenverkehr am Netzwerkrand zu überprüfen.

Fortschrittliche Vernetzung und Security, kombiniert – Fortinet Secure SD-WAN

Die FortiGate Next-Generation Firewalls (NGFWs) beinhalten Fortinet Secure SD-WAN-Funktionen und bieten sowohl Vernetzung als auch Sicherheit für SD-WAN-Filialnetzwerke in einer einzigen Lösung. Sie bietet effizienten Schutz für alle Außenstellen, indem durch die Verwaltung über eine zentrale Konsole eine konsequente Richtliniendurchsetzung ermöglicht wird. Darüber hinaus können Unternehmen die mit DX verbundenen Risiken minimieren.

Im ersten „Software-Defined Wide Area Networking Test Report“ von NSS Labs war Fortinet der einzige Anbieter, dessen Sicherheitsfunktionen die Bewertung „Empfohlen“ erhielten.[6] FortiGate NGFWs haben auch den Spitzenplatz bei der Gesamtzahl der jährlich weltweit ausgelieferten Security-Komponenten.[7] Für SD-WAN-Fähigkeiten kombiniert FortiGate NGFW- und SD-WAN-Funktionen in einer einzigen Lösung, die die Effizienz und Sicherheit des WAN verbessert.

Zu den wichtigsten Funktionen von Fortinet Secure SD-WAN gehören:

Anwendungserkennung und automatisierte Pfadintelligenz

Mit traditionellem WAN haben Unternehmen Probleme, die Qualität der Benutzererfahrung pro Anwendung aufrechtzuerhalten. Die traditionelle WAN-Infrastruktur basiert auf Paket-Routing, was die Sichtbarkeit der Anwendung einschränkt.

Fortinet Secure SD-WAN verwendet die „First-Packet-Identifikation“, um Anwendungen bereits beim ersten Datenverkehrspaket intelligent zu identifizieren. Diese breite **Anwendungserkennung** hilft Netzwerk-Teams, zu erkennen, welche Anwendungen im gesamten Unternehmen verwendet werden, und ermöglicht es ihnen, fundierte Entscheidungen über SD-WAN-Richtlinien zu treffen. Fortinet Secure SD-WAN fragt eine Application Control-Datenbank mit über 5000 Anwendungen ab – eine Zahl, die mit der Entwicklung der Bedrohungslandschaft und des digitalen Netzwerks weiter wächst.

Das Erkennen von Anwendungen öffnet die Tür zu **automatisierter Pfadintelligenz** – und für das priorisierte Routing über die Netzwerkbandbreite, basierend auf der spezifischen Anwendung und dem Benutzer. Fortinet Secure SD-WAN bietet einen SLA auf Anwendungsebene mit automatisierter Pfadintelligenz für die dynamische Auswahl der für die jeweilige Situation besten WAN-Verbindung. FortiGate NGFWs mit der neuen SOC4 ASIC (Application Specific Integrated Circuit, anwendungsspezifische integrierte Schaltung) ermöglichen die branchenweit schnellste Anwendungssteuerung mit einer konkurrenzlosen Anwendungserkennungsleistung. Diese umfasst auch eine tiefgehende SSL/TLS-Prüfung mit dem geringsten möglichen Leistungsabfall und folgenden zugehörigen Funktionen:

- **WAN-Pfadkorrektur**, bei der mittels Vorwärtsfehlerkorrektur (FEC, Forward Error Correction) widrige WAN-Bedingungen wie schlechte oder verrauschte Verbindungen überwunden werden. Dies erhöht die Datenzuverlässigkeit und sorgt für eine bessere Benutzererfahrung bei Anwendungen wie Sprach- und Videodiensten. FEC fügt dem ausgehenden Datenverkehr Fehlerkorrekturdaten hinzu, sodass die Empfängerseite nach Paketverlust und anderen während der Übertragung aufgetretenen Problemen die Fehler beheben kann, wodurch die Qualität von Echtzeitanwendungen verbessert wird.
- **Tunnelbandbreiten-Aggregation**, die eine paketweise Lastverteilung und eine Zustellung durch die Kombination von zwei Overlay-Tunneln ermöglicht, um die Netzwerkkapazität zu maximieren, wenn eine Anwendung eine größere Bandbreite benötigt.

- **Automatische Failover-Funktionen**, die bei einer Verschlechterung des primären WAN-Pfades auf die beste verfügbare Verbindung wechseln. Diese Automatisierung ist in FortiGate NGFWs integriert, wodurch die Komplexität für den Endbenutzer reduziert und gleichzeitig seine Erfahrung und Produktivität verbessert wird.

Ein wesentliches Merkmal von SD-WAN ist seine Fähigkeit, die Kosten-Nutzen-Vorteile von internetbasierten VPNs mit der Leistung und Agilität von MPLS-VPNs zu bieten.[8]

NGFW-Sicherheit und Compliance

Fortinet Secure SD-WAN bietet unternehmenstaugliche Sicherheits- und Filialnetzwerkfunktionen mit einer Single-Box-Lösung – der FortiGate NGFW. Zu ihren wichtigsten Security-Funktionen gehören:

- **SSL/TLS-Prüfung und Schutz vor Bedrohungen**, um Transparenz und Schutz vor Malware zu gewährleisten, wodurch separate Appliances zur Verschlüsselungsprüfung überflüssig werden
- **Web Filtering-Dienst** zur Durchsetzung der Internetsicherheit und Reduzierung der Komplexität, wodurch die Notwendigkeit einer separaten Secure Web Gateway-Vorrichtung entfällt
- **Umfassender Schutz vor Bedrohungen**, einschließlich Sandboxing, Anti-Malware und Intrusion Prevention System (IPS)
- **Hochskalierbare Overlay-VPN-Tunnel** mit hohem Durchsatz, um sicherzustellen, dass der Datenverkehr immer verschlüsselt ist und vertraulich bleibt
- **Granulare SLA-Analysen**, einschließlich Anwendungstransaktionen für eine schnelle Problembehandlung

Fortinet Secure SD-WAN-fähige Tracking- und Berichterstellungsfunktionen tragen dazu bei, die Einhaltung von Datenschutzgesetzen, Sicherheitsstandards und Branchenvorschriften sicherzustellen und gleichzeitig das zusätzliche Risiko von Geldbußen und Rechtskosten im Falle eines Verstoßes zu reduzieren. Diese Funktionen verfolgen Bedrohungsaktivitäten in Echtzeit, erleichtern die Risikobewertung, erkennen potenzielle Probleme und wehren Gefahren ab. Sie überwachen außerdem Firewall-Richtlinien und helfen bei der Automatisierung von Compliance-Audits.

Fortinet **Security Rating Service** bietet Best Practices für Vorschriften wie den Payment Card Industry Data Security Standard (PCI DSS) und Echtzeit-Tracking und Berichterstellung gemäß Sicherheitsstandards des National Institute of Standards and Technology (NIST) und des Center for Internet Security (CIS). Als Teil des Diensts erhalten Unternehmen eine Bewertung ihres eigenen Sicherheitsprofils, die sie dann mit den Bewertungen ihrer Marktbegleiter vergleichen können.

Vereinfachte Verwaltung, Orchestrierung und Overlay-Steuerung

Wenn Unternehmen SD-WAN einführen, benötigen sie die richtigen Tools, um es nahtlos in weit verteilten Infrastrukturen zu implementieren und zu verwalten. Fortinet Secure SD-WAN kann über FortiManager, eine intuitive und einheitliche Verwaltungskonsole, administriert werden. Es umfasst Optionen für eine cloudbasierte oder gehostete Lösung zur Remote-Steuerung und Orchestrierung über Tausende Standorte hinweg. Mit FortiManager sind FortiGate-Geräte echte Plug-and-Play-Komponenten. Zentralisierte Richtlinien und Geräteinformationen können mit FortiManager konfiguriert werden, und die FortiGate-Geräte werden automatisch auf die neueste Richtlinienkonfiguration aktualisiert.

FortiGate NGFWs mit dem SOC4 ASIC bieten die branchenweit schnellste SD-WAN-Security-Leistung. Dazu gehören die Beschleunigung für reaktives **Overlay-VPN** und eine bessere allgemeine WAN-Benutzererfahrung über das gesamte Unternehmen hinweg. Die Orchestrierung von **Cloud Overlay-Controllern**, die auf Abonnementdiensten des 360 Protection Bundle basieren, vereinfacht die Overlay-VPN-Implementierung mit cloudbasiertem automatisiertem Provisioning. Die Flexibilität der Verwaltung über eine zentrale Konsole umfasst skalierbare entfernte Security- und Netzwerksteuerung über die Cloud für alle Niederlassungen und Standorte.

Gesamtbetriebskosten (TCO)

Durch den Umstieg auf das öffentliche Breitband können teure MPLS-Verbindungen durch kostengünstigere Optionen ersetzt werden. Mit der transportunabhängigen Lösung von Fortinet können Unternehmen die gesamte verfügbare Bandbreite verwenden, indem sie die Verbindungen im Aktiv/Aktiv-Modus nutzen. Fortinet Secure SD-WAN bietet die branchenweit besten Gesamtbetriebskosten (TCO) – 10-mal günstiger als der Wettbewerb.[9]

Sicherheitsbasierte Netzwerke

Es gibt heute viele verschiedene SD-WANs auf dem Markt, und die VPs der IT-Abteilungen sollten ihre Optionen sorgfältig prüfen. Fortinet Secure SD-WAN integriert erweiterte SD-WAN-Funktionen mit bewährten Security-Funktionen und bietet sicherheitsorientierte Netzwerke, die die Effizienz der Filialen verbessern, ohne Abstriche beim Schutz zu machen.

[1] „SaaS Adoption Rising“, Computer Economics, November 2018.

[2] „Global Software-as-a-Service (SaaS) Market Outlook (2018-2023)“, Business Wire, 14. November 2018.

[3] Conner Forrest, „Businesses are adopting SaaS too fast to properly secure it“, TechRepublic, 10. April 2018.

[4] „SD-WAN Infrastructure Market Poised to Reach $4.5 Billion in 2022“, IDC, 7. August 2018.

[5] John Maddison, „More Encrypted Traffic Than Ever“, Fortinet, 10. Dezember 2018.

[6] „Fortinet SD-WAN gives the performance of a lifetime“, Fortinet, 9. August 2018.

[7] „IDC Worldwide Security Appliances Tracker“, April 2018 (basierend auf jährlich ausgelieferten Stückzahlen).

[8] Zeus Kerravala, „Understanding Virtual Private Networks (and why VPNs are important to SD-WAN)“, Network World, 13. April 2018.

[9] „Fortinet SD-WAN gives the performance of a lifetime“, Fortinet, 9. August 2018.

September 10, 2019 12:47 nachm.

372029-0-0-DE

E:\PRACE\ARGOS\2019\09 2019\A-344888-924139\de-DE\SD-WAN\sb-fortinet-sd-wan-A4_de-DE\sb-fortinet-sd-wan-A4_de-DE