FORTINET

Der SD-WAN-Leitfaden für Netzwerk-Betreiber

Sicherheitsorientierte Netzwerke für ein leistungsstarkes WAN-Edge

Inhaltsverzeichnis

FORTINET

Zusammenfassung

Viele Unternehmen, die sich inmitten von Maßnahmen zur digitalen Transformation (DX) für ihre dezentralen Unternehmen befinden, versuchen, ihre veralteten Wide Area Network-(WAN-)Infrastrukturen zu ersetzen. Die hohen Kosten und die Komplexität einer zuverlässigen Wide-Area-Konnektivität über traditionelle Netzbetreiber-basierte Netzwerke führen die meisten Entscheidungsträger zu einer Form von softwaredefiniertem Wide Area-Netzwerk (SD-WAN). Das Fortinet Secure SD-WAN bietet sowohl Netzwerk- als auch Security-Funktionen in einer einheitlichen Lösung. Es unterstützt Anwendungsleistung, konsolidierte Verwaltung und erweiterten Schutz vor Bedrohungen.

Einleitung

Die Auswahl der richtigen SD-WAN-Lösung für eine bestimmte Implementierung kann gewisse Kompromisse erfordern, die Sicherheit sollte jedoch nicht darunter fallen. Es gibt verschiedene Möglichkeiten, SD-WAN-Netzwerke und fortschrittliche Sicherheit zu kombinieren – aber nur eine Lösung kann wirklich als Secure SD-WAN bezeichnet werden. Fortinet, der vertrauenswürdigste Name im Bereich Netzwerk-Security, hat seine branchenführenden FortiGate Next-Generation Firewalls (NGFWs) um erstklassige SD-WAN-Funktionen erweitert. FortiGate NGFWs mit Secure SD-WAN bieten optimale Leistung für geschäftskritische Software-as-a-Service-(SaaS-)Anwendungen sowie digitale Sprach- und Video-Tools. Gleichzeitig helfen sie Unternehmen, sich vor den neuesten Risiken und sich entwickelnden komplexen Angriffen zu schützen.

IDC prognostiziert, dass der weltweite Umsatz mit SD-WAN-Infrastruktur und -Diensten eine durchschnittliche jährliche Wachstumsrate (Compound Annual Growth Rate, CAGR) von über 40 % aufweisen und bis 2022 4,5 Milliarden US-Dollar erreichen wird.[1]

Welcher Weg zum SD-WAN?

SD-WAN bietet die Möglichkeit, verfügbare WAN-Dienste effektiver und wirtschaftlicher zu nutzen und bietet den Benutzern in dezentralen Unternehmen die Freiheit, Kunden individueller anzusprechen, Geschäftsprozesse zu optimieren und Innovationen durchzuführen. Außerdem macht es die WAN-Verwaltung kostengünstiger, weshalb SD-WAN-Lösungen auf absehbare Zeit ein robuster Wachstumsmarkt bleiben werden.

Um dieser Nachfrage gerecht zu werden, wurden in den letzten Jahren viele SD-WAN-Lösungen vorgestellt. Aber nicht alle von ihnen bieten auch die gleichen Vorteile.

SD-WAN-Experten und Branchenanalysten sagen, dass das optimale SD-WAN für ein Unternehmen von den Anforderungen an die Anwendungsleistung, den Sicherheitsprioritäten und den IT-Fähigkeiten des Unternehmens abhängt. Es wird auch generell empfohlen, dass Unternehmen in Kombination mit SD-WAN eine NGFW-Lösung verwenden, um Security-Probleme zu lösen, da Niederlassungen mit SD-WAN über Breitbandverbindungen direkt mit dem Internet verbunden sind. Um diese Geschäftsanforderungen zu erfüllen, benötigen Unternehmen ein umfassendes SD-WAN-Angebot: Fortinet Secure SD-WAN, das einzige mit integrierter Security und den für eine SD-WAN-Implementierung erforderlichen Fähigkeiten.

Fortinet bietet das modernste SD-WAN

Fortinet Secure SD-WAN ersetzt separate WAN-Router, WAN-Optimierung und Security-Komponenten wie Firewalls und Secure Web Gateways (SWGs) durch eine einzige FortiGate NGFW. Diese bietet eine branchenweit unübertroffene Leistung mit Funktionen wie Anwendungserkennung, automatisierter Pfadintelligenz und WAN-Overlay-Unterstützung für VPN. Fortinet Secure SD-WAN bietet sicherheitsbasierte Netzwerke für Filialnetzwerke mit herausragender Leistung, die durch schnelle Anwendungsidentifikation und automatisierte Pfadintelligenz ermöglicht wird.

Fortinet Secure SD-WAN liefert:

- Schnelle Anwendungsidentifikation
- Verbesserte Anwendungsgenauigkeit und -leistung
- Aktualisierungen der Anwendungsdatenbank anhand der FortiGuard Labs-Forschung

Anwendungserkennung für verbesserte Service Levels

Fortinet Secure SD-WAN wird durch die neue anwendungsspezifische integrierte SOC4-Schaltung (ASIC) unterstützt, die schnellere Anwendungssteuerung und konkurrenzlose Anwendungsidentifizierung bietet. Dazu gehört die Deep Secure Sockets Layer-(SSL-) / Transport Layer Security-(TLS-)Prüfung mit geringstmöglichem Leistungsabfall.

Technisch gesehen funktioniert SD-WAN, indem es Anwendungen zu jedem Zeitpunkt über die effizienteste WAN-Verbindung weiterleitet. Um eine optimale Anwendungsleistung zu gewährleisten, müssen SD-WAN-Lösungen in der Lage sein, ein breites Anwendungsspektrum zu identifizieren und Routing-Richtlinien auf einer sehr granularen Ebene anzuwenden. Ohne diese Funktionen können SaaS-, Video- und Sprach-Anwendungen die Produktivität der Endanwender verlangsamen und beeinträchtigen.

Um diesen Problemen zu begegnen, verwendet Fortinet Secure SD-WAN eine Application Control-Datenbank mit den Signaturen von mehr als 5.000 Anwendungen (mit regelmäßigen Updates von den FortiGuard Labs Threat Intelligence Services). Fortinet Secure SD-WAN identifiziert und klassifiziert Anwendungen – auch verschlüsselten Datenverkehr von Cloud-Anwendungen – vom ersten Paket an.

Fortinet Secure SD-WAN erkennt über 5000 Anwendungen automatisch und leitet sie optimal weiter.

FortiGate kann so eingestellt werden, dass es die Kritikalität von Geschäftsanwendungen erkennt. Geschäftskritische Anwendungen (z. B. Office 365, Salesforce, SAP), allgemeine Produktivitätsanwendungen (z. B. Dropbox) und Social Media (z. B. Twitter, Instagram) können mit unterschiedlichen Routing-Prioritäten versehen werden. Einzigartige Richtlinien können auf einer tieferen Ebene für Unteranwendungen angewendet werden (z. B. Word oder OneNote in Office 365). Diese tiefgehende und umfassende Transparenz auf Anwendungsebene hinsichtlich Verkehrsmustern und Auslastung ermöglicht eine bessere Zuordnung der WAN-Ressourcen entsprechend den Geschäftsanforderungen.

Mühelose WAN-Effizienz

Fortinet Secure SD-WAN vereinfacht den Transformationsprozess älterer WAN-Edge-Infrastrukturen erheblich und bietet eine verbesserte Anwendungsleistung, bessere Benutzerfreundlichkeit und höhere Sicherheit. Sobald die WAN-Richtlinien auf der Grundlage von Anwendungskritikalität, Leistungsanforderungen, Sicherheitsrichtlinien und anderen Aspekten festgelegt wurden, übernimmt die Fortinet Secure SD-WAN-Lösung den Rest der Arbeit. FortiGate NGFWs mit dem SOC4 ASIC bieten eine 10-mal schnellere Security-Leistung als die Konkurrenz.[2]

Im Bereich der WAN-Effizienz stellt Fortinet Secure SD-WAN alle wichtigen Funktionen bereit:

Automatisierte Pfadintelligenz. Die Anwendungserkennung ermöglicht ein priorisiertes Anwendungs-Routing über die Netzwerkbandbreite abhängig von der spezifischen Anwendung und dem Benutzer. Mit dem neuen SOC4 ASIC verfügt Fortinet Secure SD-WAN über die schnellste Anwendungssteuerung der Branche. SD-WAN Service Level Agreements (SLAs) lassen sich leicht definieren, indem man dynamisch die beste WAN-Verbindung für die spezifischen Geschäftsumstände auswählt. Für Anwendungen mit niedriger bis mittlerer Priorität können Unternehmen die Qualitätskriterien angeben, und die FortiGate wählt den entsprechenden Link aus. Für Anwendungen mit hoher Priorität und geschäftskritische Anwendungen können strenge SLAs definiert werden, die auf einer Kombination aus Jitter, Paketverlust und Latenzmetriken basieren.

WAN-Overlay. Reaktive **Overlay-VPN**-Funktionen ermöglichen ein besseres WAN-Erlebnis für Benutzer in Filialen. Die Orchestrierung von **Cloud Overlay-Controllern**, die auf Abonnementdiensten des **360 Protection Bundle** basieren, vereinfacht die Overlay VPN-Implementierung mit cloudbasierter automatisierter Bereitstellung.

Automatisches Failover. Die Multi-Path-Technologie kann automatisch auf die beste verfügbare Verbindung umschalten, wenn sich der primäre WAN-Pfad verschlechtert. Diese Automatisierung ist in die FortiGate integriert, wodurch die Komplexität für den Endbenutzer reduziert und gleichzeitig seine Anwendungserfahrung und seine Produktivität verbessert werden.

WAN-Pfadkorrektur. Die WAN-Pfadkorrektur nutzt die Vorwärtsfehlerkorrektur (Forward Error Correction, FEC), um widrige WAN-Bedingungen, wie schlechte oder verrauschte Verbindungen, zu überwinden. Dies erhöht die Datenzuverlässigkeit und bietet eine bessere Benutzererfahrung für Anwendungen wie Sprach- und Videodienste. FEC fügt dem ausgehenden Datenverkehr Fehlerkorrekturdaten hinzu, sodass die Empfängerseite Paketverluste und andere Fehler, die während der Übertragung auftreten, beheben kann. Dies verbessert die Qualität von Echtzeitanwendungen.

Aggregation der Tunnelbandbreite. Für Anwendungen, die eine größere Bandbreite erfordern, ermöglicht Fortinet Secure SD-WAN Lastverteilung und Lieferung pro Paket. Hierzu werden zwei Overlay-Tunnel zur Maximierung der Netzwerkkapazität kombiniert.

Vereinfachte Verwaltung und branchenweit niedrigste Gesamtbetriebskosten (TCO)

WAN-Manager haben oft Probleme, wenn es darum geht, SD-WAN-Edge-Geräte an ihren zahlreichen Remote-Standorten und Niederlassungen bereitzustellen. LKW-Transporte sind teuer und häufig steht nicht genügend technisches Personal zur Verfügung. Andererseits ist der Versand von vollständig konfigurierten Geräten nicht sicher. Außerdem müssen, sobald Edge-Geräte bereitgestellt sind, die Mitarbeiter sowohl die WAN-Optimierungsfunktionen als auch die Security-Funktionen verwalten, und das häufig über zwei verschiedene Schnittstellen. Fortinet Secure SD-WAN löst sowohl das Implementierungs- als auch das Verwaltungsproblem und senkt so die Gesamtbetriebskosten (TCO).

In den SD-WAN-Gruppentestergebnissen der NSS Labs für 2018 erhielt Fortinet Secure SD-WAN Bestnoten sowohl für VoIP (höchste Punktzahl) als auch für Video Quality of Experience (QoE).[3]

Zero-Touch-Implementierung. Die vereinfachten Implementierungsfunktionen von Fortinet Secure SD-WAN ermöglichen es Unternehmen, an alle Remote- Standorte unkonfigurierte FortiGate NGFW-Appliances zu liefern. Wenn die FortiGate angeschlossen ist, verbindet sie sich automatisch mit dem FortiDeploy-Dienst in FortiCloud. FortiDeploy authentifiziert das Remote-Gerät innerhalb von Sekunden und verbindet es mit einem zentralen FortiManager-System.

Verwaltung über eine zentrale Konsole. FortiManager ermöglicht eine zentrale Sicht auf alle implementierten Secure SD-WAN-fähigen FortiGate NGFWs im gesamten dezentralen Unternehmen. Intuitive Visualisierungen machen es einfach, sowohl die physischen als auch die logischen Netzwerktopologien auf hohem Niveau zu überwachen und bei Bedarf im Detail zu analysieren, um eventuelle Probleme zu untersuchen. Administratoren können unternehmensweite WAN-Richtlinien aktualisieren und an alle Standorte verteilen oder einzelne Geräte neu konfigurieren.

Für Benutzer, die eine sichere Kommunikation über die öffentlichen Internetverbindungen benötigen, können mit nur einem Klick VPNs eingerichtet werden. All dies spart Zeit und vereinfacht die SD-WAN-Administration (lokal oder über die Cloud) und entlastet zudem die schlanken Netzwerkteams. Fortinet bietet eine der wenigen Lösungen, die SD-WAN-Netzwerk-, Security- und Access Layer-Kontrollen von derselben Verwaltungskonsole aus verwalten kann.

Gesamtbetriebskosten (TCO). Fortinet Secure SD-WAN bietet die branchenweit niedrigsten Gesamtbetriebskosten mit dem besten Preis-Leistungs-Verhältnis für den Schutz vor Bedrohungen bei einem Durchsatz von 1 GBit/s.[4] 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 nutzen, indem sie die Verbindungen im Aktiv/Aktiv-Modus nutzen.

Fortinet Secure SD-WAN bietet branchenweit niedrigste Gesamtbetriebskosten – 10-mal besser als die Wettbewerber.[5]

Sicherheitsorientierte Netzwerke

Fortinet bietet ein erstklassiges, zertifiziertes SD-WAN, das sowohl leistungsstark als auch geschützt ist. FortiGate NGFWs mit dem SOC4 ASIC bieten die branchenweit schnellste SD-WAN-Security-Leistung. Im ersten „Software-Defined Wide Area Networking Test Report“ von NSS Labs war Fortinet der einzige Anbieter mit Security-Funktionen, die die Bewertung „Empfohlen“ erhielten.[6]

Insbesondere verfügt Fortinet Secure SD-WAN über einen robusten SD-WAN-Bedrohungsschutz, einschließlich Layer 3- bis Layer 7-Security-Kontrollen, die in anderen SD-WAN-plus-Firewall-Lösungen gewöhnlich nicht verfügbar sind:

- Umfassender Schutz vor Bedrohungen, einschließlich Firewall, Antivirus, Intrusion PreventionSystem (IPS) und Application Control
- SSL-Inspektion mit hohem Durchsatz und minimalen Leistungseinbußen, um sicherzustellen, dass Unternehmen für den umfassenden Schutz vor Bedrohungen nicht den Durchsatz opfern[7]
- Web Filtering zur Durchsetzung der Internet-Sicherheit, ohne dass ein separates SWG-Gerät erforderlich ist
- Hochskalierbare Overlay-VPN-Tunnel mit hohem Durchsatz, die sicherstellen, dass vertraulicher Datenverkehr immer verschlüsselt ist

Secure SD-WAN-fähige FortiGate NGFWs überwachen auch Firewall-Regeln und Richtlinien und nutzen Best Practices, um das allgemeine Sicherheitsprofil des Unternehmens zu verbessern. Dies trägt dazu bei, die Compliance mit Security-Standards sowie Datenschutzgesetzen und Branchenvorschriften zu vereinfachen. Automatisierte Audit- und Berichts-Workflows sparen den Mitarbeitern viele Stunden Arbeit und reduzieren das Risiko von Pflichtverletzungen und Fehlern.

SD-Branch möglich machen

Viele Filialen entscheiden, sowohl ihre WAN- als auch ihre LAN-Geräte durch eine Lösung mit tiefergehender Integration und vereinfachter Verwaltung zu ersetzen. Die Verwendung getrennter WAN- und LAN-Infrastrukturen erhöht nicht nur die Komplexität (mehr Geräte für Bereitstellung und Updates mit mehreren Management-Konsolen), sondern reduziert auch die Transparenz und Kontrolle der Betriebsabläufe und erhöht gleichzeitig das Risiko von Sicherheitslücken, die Hacker ausnutzen können. Um diesen Herausforderung zu begegnen, umfasst Fortinet Secure SD-WAN eine schnellere Security-Erweiterung auf das Access Layer, die die SD-Branch-Transformation ermöglicht.

In einem volatilen SD-WAN-Markt ist Fortinet die sichere Wahl

Da cloudbasierte Anwendungen und Tools wie Sprache und Video für dezentrale Unternehmen immer wichtiger werden, kann Fortinet Secure SD-WAN Unternehmen helfen, die Vorteile von DX zu nutzen, ohne die Anwendungsleistung zu verlangsamen, die Produktivität der Endanwenders zu beeinträchtigen oder Daten zu gefährden.

Fortinet Secure SD-WAN ist skalierbar und hilft Unternehmen dabei, mehr Remote- Standorte, bandbreitenempfindlichere geschäftskritische Anwendungen, mehr Cloud-Services und alles, was das Filialnetz benötigt, zuverlässig zu unterstützen.

Fortinet Secure SD-WAN wird weltweit in den verschiedensten Branchen eingesetzt – von der Finanzwirtschaft über den Einzelhandel bis hin zu Fertigung und im Bereich Customer Service. Unabhängig davon, ob sie einige Hundert mobile Endgeräte oder Zehntausende Niederlassungen unterstützen müssen, Fortinet Secure SD-WAN-Kunden erreichen ihre eigene optimale Mischung aus erstklassiger Security und SD-WAN-Funktionalität.

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

[2] Basierend auf internen Tests von Fortinet.

[3] Nirav Shah, „Fortinet Secure SD-WAN Gives the Performance of a Lifetime, Recommended by NSS Labs“, Fortinet, 9. August 2018.

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] Ibid.

www.fortinet.de

372656-0-0-DE

September 10, 2019 12:26 nachm.

eb-network-leaders-guide-to-SD-WAN_de-DE