SOLUTION BRIEF

Zuverlässigere Konnektivität mit einfacherem SD-WAN-Betrieb für Betriebstechnologie

Zusammenfassung

Das softwaredefinierte Wide Area Networking (SD-WAN) ersetzt zunehmend herkömmliche WANs an Remote-Standorten mit Betriebstechnologie (OT). Während ein SD-WAN zuverlässigere Verbindungen bietet und neue digitale Innovationen unterstützt, besitzen nur wenige SD-WAN-Lösungen konsolidierte Netzwerk- und Security-Funktionen, die für raue Umgebungen optimiert sind. Bislang mussten Unternehmen, die z. B. dezentrale Produktionsstätten, Umspannwerke oder Bohrinseln über ein SD-WAN verbinden wollten, auf isolierte Einzelprodukte zurückgreifen und daraus ein Netzwerk „zusammenschustern". Dezentrale Standorte benötigen jedoch einen simpleren Ansatz, um Kosten zu senken, die Produktivität zu steigern und Risiken zu minimieren – wie z. B. das Fortinet FortiGate Rugged Secure SD-WAN. Diese Lösung kombiniert integrierte Management- und Analyse-Lösungen mit Next Generation Firewalls (NGFWs), die speziell für anspruchsvolle Umgebungen gehärtet sind, und ermöglicht einen zentralisierteren, einfacheren SD-WAN-Betrieb.

Fortinet SD-WAN für Betriebstechnologie mit vollintegriertem Appliance- und Fabric Management Center

- Next Generation Firewall (NGFW)
- SD-WAN-Funktionalität
- Robustes Design für extreme Temperaturen, Vibrationen und elektromagnetische Interferenzen (EMI)
- Zero-Touch-Bereitstellung
- Zentrales Management
- Reporting und Analytics
- Compliance Reporting
- Integration und Automatisierung

Bei einer Gartner-Umfrage gaben 72 % der Befragten an, dass ihnen die WAN-Sicherheit die größten Sorgen bereitet.[3]

Gartner

Unterstützung von Innovationen in dezentralen Produktionsstätten

Immer mehr Fertigungsanlagen, Umspannwerke und Bohrinseln führen digitale Innovationen ein – wie SaaS-Anwendungen (Software-as-a-Service) und Echtzeit-Anwendungen für Sprach- und Video-Übertragungen –, um die Produktivität zu steigern, die Kommunikation zu verbessern und ein schnelles Geschäftswachstum zu fördern. Herkömmliche WAN-Architekturen in vielen Remote-Standorten erfüllen jedoch oft nicht die Bandbreiten-Anforderungen neuer Technologien zu angemessenen Kosten. Daher wird zunehmend auf SD-WAN-Architekturen umgestellt, die günstigere Direktverbindungen zum Internet nutzen. Allein von 2018 bis 2019 ist der SD-WAN-Markt mit einer durchschnittlichen jährlichen Wachstumsrate (CAGR) von über 110 % von 841 Mio. USD Marktvolumen auf 1,77 Mrd. USD gewachsen.[1]

Ein SD-WAN verbessert zwar die Zuverlässigkeit von Verbindungen, kann jedoch das Unternehmen neuen Risiken aussetzen. Laut einer Gartner-Umfrage wollen Kunden zwar weiterhin eine bessere WAN-Performance und mehr Transparenz, aber die Sicherheit steht mittlerweile beim WAN an erster Stelle.[2]

In vielen Unternehmen hat die Notwendigkeit einer SD-WAN-Security dazu geführt, dass Netzwerk-Verantwortliche viele verschiedene Tools und Einzelprodukte integriert haben, um bestimmte Funktionen, Bedrohungen und Compliance-Anforderungen zu erfüllen. Dieser Ansatz führt jedoch zu einer Infrastrukturkomplexität, die den Management-Aufwand erhöht und zugleich neue Verteidigungslücken am Netzwerk-Rand schafft.

Fortinet vereinfacht und schützt SD-WAN-Implementierungen

Durch die Konsolidierung der Netzwerk- und Security-Tools, die für eine sicherheitsorientierte SD-WAN-Lösung notwendig sind, wird die Komplexität einer Implementierung in vielen unkontrollierten Remote-Umgebungen beseitigt. Dies reduziert nicht nur die Angriffsfläche des Unternehmens und unterstützt zugleich digitale Innovationen, sondern vereinfacht auch die Betriebsabläufe für Netzwerk-Teams.

Als integraler Bestandteil des Fabric Management Centers lassen sich das FortiGate Rugged Secure SD-WAN und der SD-WAN Orchestrator (erhältlich mit dem FortiManager) über eine zentrale Konsole gemeinsam verwalten. Kunden profitieren so nicht nur von besseren Analysen und Berichten mit dem FortiAnalyzer, sondern können auch zentralisierte Implementierungen erheblich vereinfachen, Zeit durch Automatisierung sparen und geschäftsorientierte Richtlinien bereitstellen.

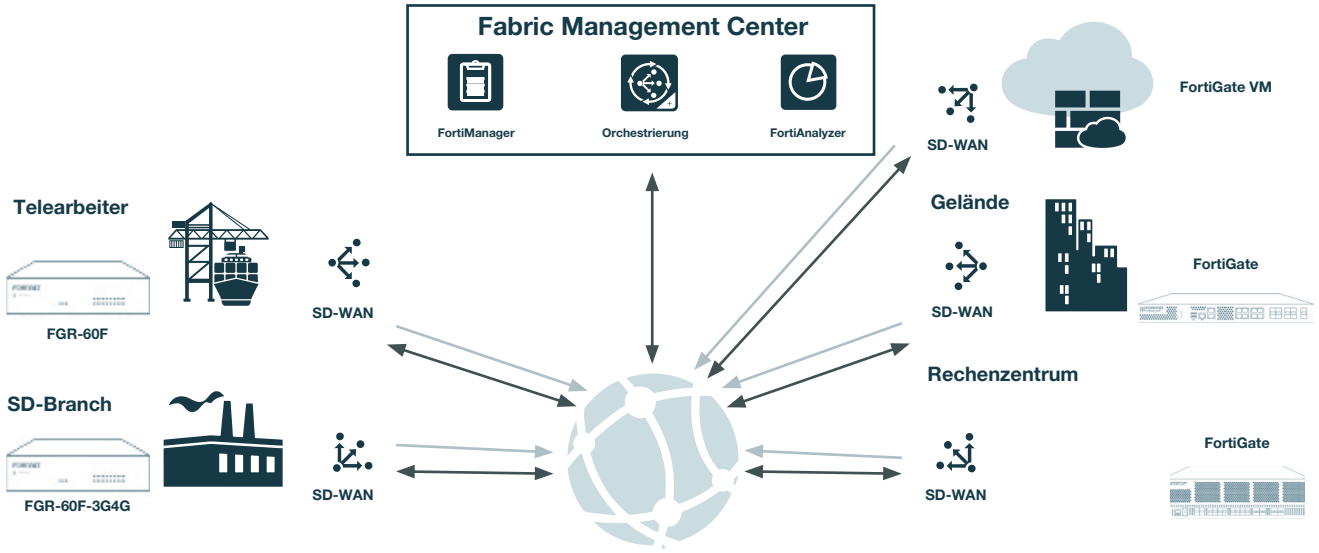


Abbildung 1: Robuste FortiGate-Firewalls ermöglichen einen SD-WAN-Betrieb mit zentralem Management.

Zero-Touch-Bereitstellung

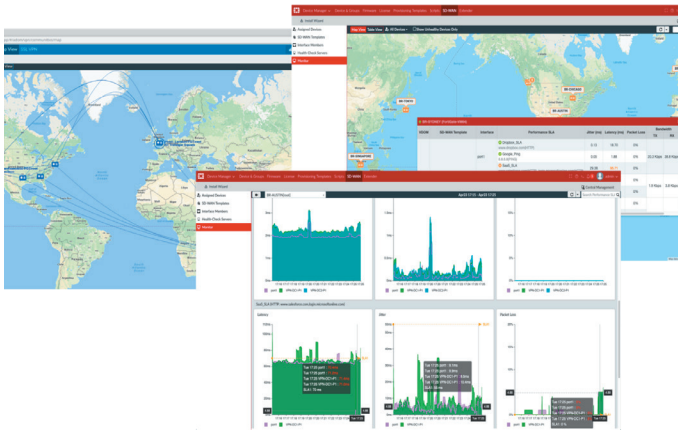
Unternehmen, die auf ein FortiGate Rugged Secure SD-WAN umstellen, können mit dem Fabric Management Center die Implementierungszeit von Tagen auf Minuten verkürzen. Mit den Zero-Touch-Bereitstellungsfunktionen des Fabric Management Center lassen sich FortiGate-Geräte an einem Remote-Standort anschließen und dann automatisch mit dem FortiManager von der Zentrale aus über eine Breitbandverbindung konfigurieren, ohne dass extra ein IT-Team vor Ort sein muss. Mit der Fortinet-Lösung kann auch eine vorhandene SD-WAN-Konfiguration als Vorlage verwendet werden, um umfassende Implementierungen in neuen Niederlassungen und Remote-Standorten zu beschleunigen.

Tests der NSS Labs zeigen, dass mit der Zero-Touch-Bereitstellung des FortiGate Rugged Secure SD-WANs eine Niederlassung in unter 6 Minuten online ist.[4]

Zentrales Management für dezentrale Unternehmen

Durch das zentrale, unternehmensweite Management aller verteilten Netzwerke können Netzwerk-Verantwortliche Konfigurationsfehler, die zu Cyber-Risiken und Netzwerk-Ausfällen führen, drastisch reduzieren.

Der Secure SD-WAN Orchestrator gehört zum Fabric Management Center. Kunden können so zentralisierte Implementierungen stark vereinfachen, durch Automatisierung Zeit sparen und geschäftsorientierte Richtlinien bereitstellen. Fortinet-Management-Tools unterstützen weitaus größere Implementierungen als Lösungen anderer Anbieter: Bis zu 100 000 FortiGate-Geräte lassen sich damit verwalten. Features wie SD-WAN- und NGFW-Vorlagen, ein unternehmensweites Konfigurationsmanagement und rollenbasierte Zugriffskontrollen helfen Netzwerk-Verantwortlichen dabei, menschliche Fehler auf einfache Weise zu minimieren.



SD-WAN-Reporting und -Analytics

Dank verbesserter Analysen der Verfügbarkeit von WAN-Verbindungen, der Erfüllung von Service-Vereinbarungen (SLA), des Anwendungsverkehrs zur Laufzeit sowie rückblickender Statistiken kann das Infrastruktur-Team Fehler schnell eingrenzen und Netzwerk-Probleme beheben. Das Fabric Management Center bietet erweiterte Telemetrie-Daten für mehr Transparenz über Anwendungen und die Netzwerk-Leistung, um schneller eine Lösung zu finden und IT-

Support-Anfragen zu reduzieren. SD-WAN-Berichte liefern bei Bedarf weitere Informationen über die Bedrohungslage, die Vertrauensstufe und den Zugriff auf Ressourcen, die für Compliance-Zwecke vorgeschrieben sind.

Diese Funktionen umfassen **Berichte zur Bandbreiten-Überwachung** und Datensätze zum SD-WAN, eine **SLA-Protokollierung und eine rückblickende Vorgangsüberwachung (History Monitoring)** anhand von Datensätzen, Diagrammen und Berichten. Anpassbare SLA-Warnungen, Berichte zur Anwendungsnutzung und Dashboards gehören ebenfalls zum Funktionsumfang. Außerdem gibt es **adaptive Response Handler** für SD-WAN-Ereignisse, eine Ereignis-Protokollierung (Event Logging) und eine Archivierung von Vorfällen bei Anwendungen und Schnittstellen im Zusammenhang mit SLAs.

Compliance Reporting

Kunden benötigen anpassbare Berichte und Tools, um die Erfüllung gesetzlicher Vorgaben bei Audits nachzuweisen. Bislang war das Compliance-Management für Netzwerk-Teams ein kostspieliger, arbeitsintensiver Prozess: Oft waren mehrere Vollzeitmitarbeiter und monatelange Arbeit notwendig, um Daten aus unterschiedlichsten Security-Einzelprodukten zu aggregieren und zu normalisieren.

Fortinet beschleunigt den Compliance-Berichtsprozess dank einer einfacheren Security-Infrastruktur, die viele manuelle Prozesse überflüssig macht. Das Fabric Management Center umfasst z. B. anpassbare **Vorlagen für regulatorische Anforderungen** und **vorkonfigurierte Berichte** für Standards wie SAR (Security Activity Report), CIS (Center for Internet Security) und NIST (National Institute of Standards and Technology). Zudem bietet das Fabric Management Center ein **Audit Logging** und eine **rollenbasierte Zugriffskontrolle (RBAC)**, damit Mitarbeiter nur auf die Informationen zugreifen können, die sie für ihre Arbeit wirklich brauchen.

Als Erweiterung der Funktionalität des Fabric Management Center führt der **FortiGuard Security Rating Service** Audit-Überprüfungen durch. Security- und Netzwerk-Teams können so leichter kritische Sicherheitslücken und Konfigurationsschwächen im Security-Fabric-Setup identifizieren und Best-Practice-Empfehlungen umsetzen. Das Sicherheitsprofil des eigenen Unternehmens kann zudem mit ähnlichen Firmen aus der Branche verglichen werden.[5]

Compliance und Security ergänzen sich: Cyber-Angriffe können Unternehmen dann am wenigsten anhaben, wenn Netzwerke auf Compliance-Vorgaben aufbauen.[6]

Integration und Automatisierung

Um effektiv zu sein, muss die Security nahtlos in alle Bereiche des dezentralen Unternehmens integriert werden – also in jeden entfernten Standort. Netzwerk-Verantwortliche brauchen eine einzige „Schaltzentrale“, die vollständige Transparenz über die gesamte Angriffsfläche bietet. Weiter benötigen sie eine automatisierte Bedrohungsabwehr, um das Zeitfenster von der Erkennung bis zur Korrektur zu verkürzen und Mitarbeiter von manuellen Aufgaben zu entlasten.

Mit dem Fabric Management Center lassen sich Bedrohungen in Minuten statt in Monaten beseitigen: Die **richtlinienbasierte, automatisierte Bedrohungsabwehr** erfolgt koordiniert innerhalb der gesamten Fortinet Security Fabric – einer integrierten Sicherheitsarchitektur, die Security-Workflows und die Automatisierung von Bedrohungsinformationen ermöglicht. Anhand der Warnung mit kontextbezogenen Daten, die bei einem Sicherheitsvorfall von einem Standort gesendet wird, kann ein Netzwerk-Administrator schnell die Vorgehensweise bestimmen, um das gesamte Unternehmen vor einem möglichen koordinierten Angriff zu schützen. Bestimmte Ereignisse können zudem automatische Änderungen der Gerätekonfigurationen auslösen, um die Verbreitung von Angriffen im Keim zu ersticken.

Der FortiAnalyzer und das Fabric Management Center automatisieren viele notwendige SD-WAN-Aufgaben, wodurch Netzwerk-Teams deutlich entlastet werden. Beide Produkte sind **mit Drittanbieter-Tools integrierbar**, z. B. mit einem Security Information und Events Management (SIEM), IT-Service-Management (ITSM) und DevOps-Lösungen wie Ansible oder Terraform. So lassen sich gewohnte Workflows beibehalten und bisherige Investitionen in andere Security- und Netzwerk-Tools weiterhin nutzen.

Mehrwert, Einfachheit und Security

Das Fabric Management Center bietet eine Security der Enterprise-Klasse und Netzwerk-Funktionen für Filialen mit marktführenden Vorteilen:

Geringere Gesamtbetriebskosten (TCO): Fortinets integrierter Ansatz für ein sicherheitsorientiertes SD-WAN reduziert die Gesamtbetriebskosten (TCO). Da weniger Netzwerk- und Security-Tools angeschafft werden müssen, verringern sich die Investitionskosten. Gleichzeitig sinken die Betriebskosten dank des einfacheren Managements und der Workflow-Automatisierung. Durch die Umstellung auf öffentliches Breitband können teure MPLS-Verbindungen (Multiprotocol Label Switching) durch kostengünstigere Optionen ersetzt werden. Hier

liefert das FortiGate Secure SD-WAN die branchenweit besten TCO-Werte – zehnmal besser als die Konkurrenz.[7]

Effizienzsteigerung: Gleichzeitig schafft Fortinet eine vereinfachte SD-WAN-Infrastruktur, die die betriebliche Komplexität sowohl in der Niederlassung als auch im gesamten dezentralen Unternehmen verringert. Das FortiGate Rugged Secure SD-WAN kann über eine einzige intuitive Management-Konsole verwaltet werden. Mit dem FortiManager lassen sich FortiGate-Geräte einfach per Plug-and-Play installieren. Zentralisierte Richtlinien und Geräteinformationen können mit dem FortiManager konfiguriert werden. Zudem werden FortiGate-Geräte automatisch auf die neueste Richtlinienkonfiguration aktualisiert. Die Flexibilität des zentralen Managements umfasst skalierbare Remote-Sicherheit und die Netzwerk-Steuerung über die Cloud für alle Niederlassungen und Standorte.

Die durchschnittlichen Kosten einer Datenpanne (3,92 Mio. USD) steigen durch die Systemkomplexität (+290 000 USD). Mit Bedrohungsdaten (-240 000 USD) und Security-Analysen (-200 000 USD) lassen sich diese Kosten dagegen senken.[8]

Risikominimierung: Die Tracking- und Reporting-Funktionen von Fortinet unterstützen Unternehmen bei der Einhaltung von Datenschutzgesetzen, Sicherheitsstandards und Branchenvorschriften. Gleichzeitig werden die mit Verstößen verbundenen Risiken von Bußgeldern und Rechtskosten reduziert. Der FortiAnalyzer verfolgt Bedrohungsaktivitäten in Echtzeit, erleichtert die Risikobewertung, erkennt potenzielle Probleme und wehrt Gefahren ab. Die enge Integration mit dem FortiGate Rugged Secure SD-WAN ermöglicht die Überwachung von Firewall-Richtlinien und die Automatisierung von Compliance-Audits in dezentralen Unternehmensinfrastrukturen.

Fortinet ermöglicht ein sicherheitsorientiertes SD-WAN

Während es viele Anwendungsfälle für ein sicherheitsorientiertes SD-WAN gibt, ermöglicht der Fortinet-Ansatz dies auf die effektivste Weise für alle Arten von SD-WAN-Projekten. Die Vereinfachung des SD-WAN-Betriebs ist von zentraler Bedeutung für die erfolgreiche Implementierung und Erweiterung zur Unterstützung digitaler Innovationsinitiativen. Das FortiGate Secure SD-WAN bietet mit dem Fabric Management Center erstklassige SD-WAN-Management- und Analysefunktionen, mit denen Netzwerk-Verantwortliche Betriebskosten und Risiken am Netzwerk-Rand reduzieren können.

[1] „Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 4Q19 and 2019, Table 16.1“. Gartner, März 2020.

[2] „Fortinet Recognized as a 2020 Gartner Peer Insights Customers' Choice for WAN Edge Infrastructure“. Fortinet, 26. März 2020.

[3] „Fortinet Secure SD-WAN: Best-of-Breed NGFW and SD-WAN in a Single Offering“. Gartner, November 2018.

[4] Ahmed Basheer: „Software-Defined Wide Area Network Test Report: Fortinet FortiGate 61E“. NSS Labs, 19. Juni 2019.

[5] „Proactive, Actionable Risk Management with the Fortinet Security Rating Service“. Fortinet, Mittwoch, 8. Juli 2020.

[6] Frances Dewing: „Compliance Is Not Security: Why You Need Cybersecurity Chops In The Boardroom“. Forbes, 15. August 2019.

[7] „Fortinet Placed Highest in Ability to Execute in the Challengers Quadrant of the 2019 Gartner Magic Quadrant for WAN Edge Infrastructure“. Fortinet, 4. Dezember 2019.

[8] „2019 Cost of a Data Breach Report“. Ponemon Institute und IBM, 23. Juli 2019.

FORTINET®

www.fortinet.com/de

April 26, 2021 12:51 PM

476710-B-1-DE