SOLUTION BRIEF

SD-WAN-Betrieb mit einer zentralen Management-Konsole vereinfachen

Zusammenfassung

Herkömmliche WAN-Lösungen für Filialen und Remote-Standorte werden zunehmend durch softwaredefinierte SD-WANs (Software-Defined Wide-Area Networking) ersetzt. Zwar bietet SD-WANs Leistungsvorteile für neue digitale Innovationen, doch vielen SD-WAN-Lösungen fehlen konsolidierte Netzwerk- und Security-Funktionen. Netzwerk-Verantwortliche müssen deshalb eine komplexe Mischung aus Tools und Lösungen ergänzen, um SD-WAN-Implementierungen verwalten und schützen zu können. Sinnvoller wäre aber ein einfacherer Ansatz, der eine Kostenkontrolle, Effizienzsteigerung und Risikominimierung ermöglicht. Das FortiGate Secure SD-WAN erfüllt diese Anforderungen und kombiniert Next-Generation-Firewalls (NGFWs) mit integrierten Management- und Analytics-Lösungen, um SD-WAN-Vorgänge zu zentralisieren und zu vereinfachen.

Fortinet vereinfacht den SD-WAN-Betrieb (FortiGate, FortiManager, FortiAnalyzer)

- Zero-Touch-Bereitstellung
- Zentrales Management
- Reporting und Analytics
- Compliance Reporting
- Integration und Automatisierung

Unterstützung von Innovationen mit Security für wachsende Unternehmen

Immer mehr dezentrale Unternehmen führen digitale Innovationen wie SaaS-Anwendungen (Software-as-a-Service) und IP-basierte Tools für Sprache und Video ein, um die Produktivität zu steigern, die Kommunikation zu verbessern und ein schnelles Geschäftswachstum zu fördern. Herkömmliche WAN-Architekturen in vielen Filialen und entfernten Standorten erfüllen jedoch oft nicht die Bandbreiten-Anforderungen neuer Technologien. Viele Unternehmen entscheiden sich deshalb für SD-WAN-Architekturen, die günstigere Direktverbindungen zum Internet nutzen. Es wird erwartet, dass der globale SD-WAN-Markt mit einer durchschnittlichen jährlichen Wachstumsrate (CAGR) von über 40 % bis 2022 ein Marktvolumen von 4,5 Milliarden US-Dollar erreicht.[1]

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

Gartner

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

In zahlreichen Unternehmen hat die Notwendigkeit einer SD-WAN-Security dazu geführt, dass Netzwerk-Verantwortliche viele verschiedene Tools und Einzelprodukte integriert haben, um einzelne 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 erforderlich sind, wird die Komplexität der disaggregierten Filial-Infrastruktur beseitigt. Dies reduziert nicht nur die Angriffsfläche des Unternehmens und unterstützt zugleich digitale Innovationsinitiativen, sondern vereinfacht auch die Betriebsabläufe von Netzwerk-Teams.

Als integraler Bestandteil der Fortinet Security Fabric kann das **FortiGate Secure SD-WAN** die Funktionen des **FortiManager** und **FortiAnalyzer** (Appliances oder VMs) nutzen, um den SD-WAN-Betrieb in mehreren kritischen Bereichen zu vereinfachen.

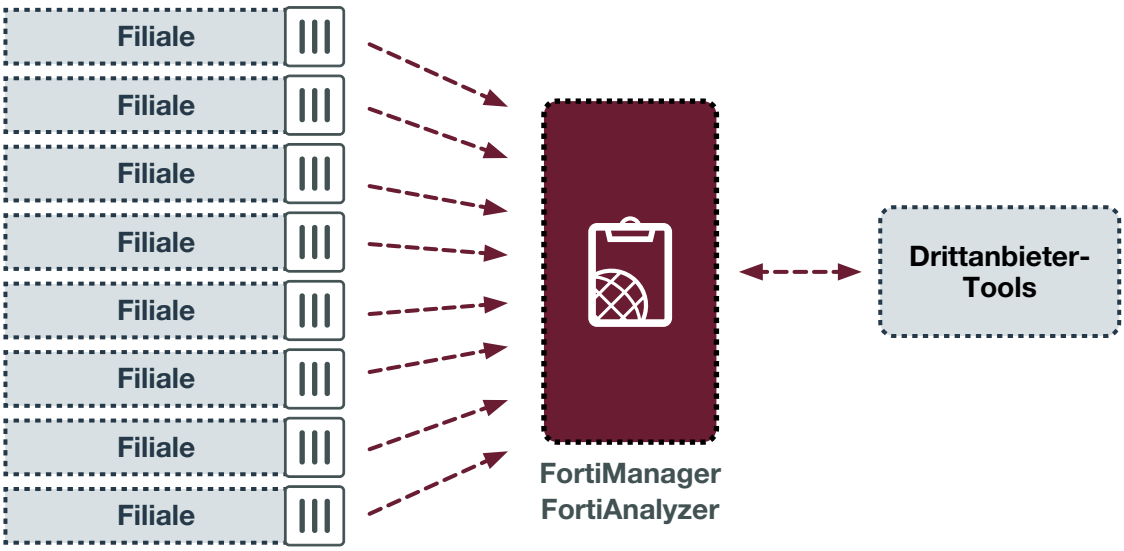

Abbildung 1: SD-WAN-Anwendungsfall mit FortiGate NGFWs, FortiManager und FortiAnalyzer

Zero-Touch-Bereitstellung

Unternehmen, die auf ein Secure SD-WAN umstellen, können mit dem FortiManager die Implementierungszeit von Tagen auf Minuten verkürzen. Mit den Zero-Touch-Bereitstellungsfunktionen des FortiManagers lassen sich FortiGate-Geräte an einem Filialstandort 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 Filialen und Remote-Standorten zu beschleunigen.

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

Zentrales Management für dezentrale Unternehmen

Über die Hälfte (52 %) aller Sicherheitsverletzungen gehen auf menschliche Fehler oder Systemfehler (und nicht auf bösartige oder kriminelle Absichten) zurück.[5] Ein zentrales Management aller Unternehmensnetzwerke unterstützt Netzwerk-Verantwortliche dabei, sicherheitsrelevante Konfigurationsfehler – und damit die Gefahr von Schwachstellen und Netzwerk-Ausfällen – drastisch zu reduzieren.

Der FortiManager und FortiAnalyzer verwenden eine **zentrale Konsole für das Management**, über die sich das gesamte dezentrale Unternehmen verwalten lässt. Fortinet-Management-Tools können viel größere Implementierungen unterstützen 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

Steigt die Anzahl der Unternehmensfilialen, wächst auch die Angriffsfläche am Netzwerk-Rand. Netzwerk-Verantwortliche müssen sich daher zunehmend auf Echtzeit-Analysen verlassen, um Netzwerk- und Sicherheitsrisiken umgehend bewerten und identifizieren zu können. Der FortiAnalyzer liefert umfassende Messwerte, die u. a. über den Netzwerkverkehr, Anwendungen und den allgemeinen Zustand des Netzwerks Aufschluss geben.

Diese Funktionen umfassen **Berichte zur Bandbreiten-Überwachung** und Datensätze zum SD-WAN, eine **SLA-Protokollierung für Service-Level-Vereinbarungen 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. Der FortiAnalyzer umfasst z. B. anpassbare **Vorlagen für regulatorische Anforderungen** und **vorkonfigurierte Berichte** für Standards wie PCI DSS (Payment Card Industry Data Security Standard), SAR (Security Activity Report), CIS (Center for Internet Security) und NIST (National Institute of Standards and Technology). Zudem bietet der FortiAnalyzer 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 FortiAnalyzer-Funktionen 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.[6]

Compliance und Security ergänzen sich: Cyber-Angriffe können Unternehmen dann am wenigsten anhaben, wenn Netzwerke auf Compliance-Vorgaben aufbauen.[7]

Integration und Automatisierung

Um effektiv zu sein, muss die Security nahtlos in jeden Teil des dezentralen Unternehmens integriert werden – in jede Filiale und 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 FortiManager 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 Filial-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 FortiManager 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 Event 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

Die Kombination aus FortiGate Secure SD-WAN, FortiManager und FortiAnalyzer bietet Security- und Filialnetzwerk-Funktionen der Enterprise-Klasse 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.[8]

Effizienzsteigerung: Gleichzeitig schafft Fortinet eine vereinfachte SD-WAN-Infrastruktur, die die betriebliche Komplexität sowohl in der Filiale als auch im gesamten dezentralen Unternehmen verringert. Das FortiGate 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 Single-Pane-of-Glass-Managements umfasst skalierbare Remote-Sicherheit und die Netzwerk-Steuerung über die Cloud für alle Filialen und Standorte.

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 Secure SD-WAN ermöglicht die Überwachung von Firewall-Richtlinien und die Automatisierung von Compliance-Audits in dezentralen Unternehmensinfrastrukturen.

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.[9]

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. FortiGate Secure SD-WAN, FortiManager und FortiAnalyzer bieten erstklassige SD-WAN-Management- und Analysefunktionen, mit denen Netzwerk-Verantwortliche Betriebskosten und Risiken am Netzwerk-Rand reduzieren können.

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

[2] Naresh Singh: „Survey Analysis: Address Security and Digital Concerns to Maintain Rapid SD-WAN Growth“. Gartner, 12. November 2018.

[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] „2018 Cost of a Data Breach Study“. Ponemon Institute, Juli 2018.

[6] „Proactive, Actionable Risk Management with the Fortinet Security Rating Service“. Fortinet, 5. April 2019.

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

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

[9] „2019 Cost of a Data Breach Report“. Ponemon Institute und IBM, Juli 2019.

FORTINET®

www.fortinet.com/de

31. August 2020, 8:43 Uhr

476710-0-1-DE