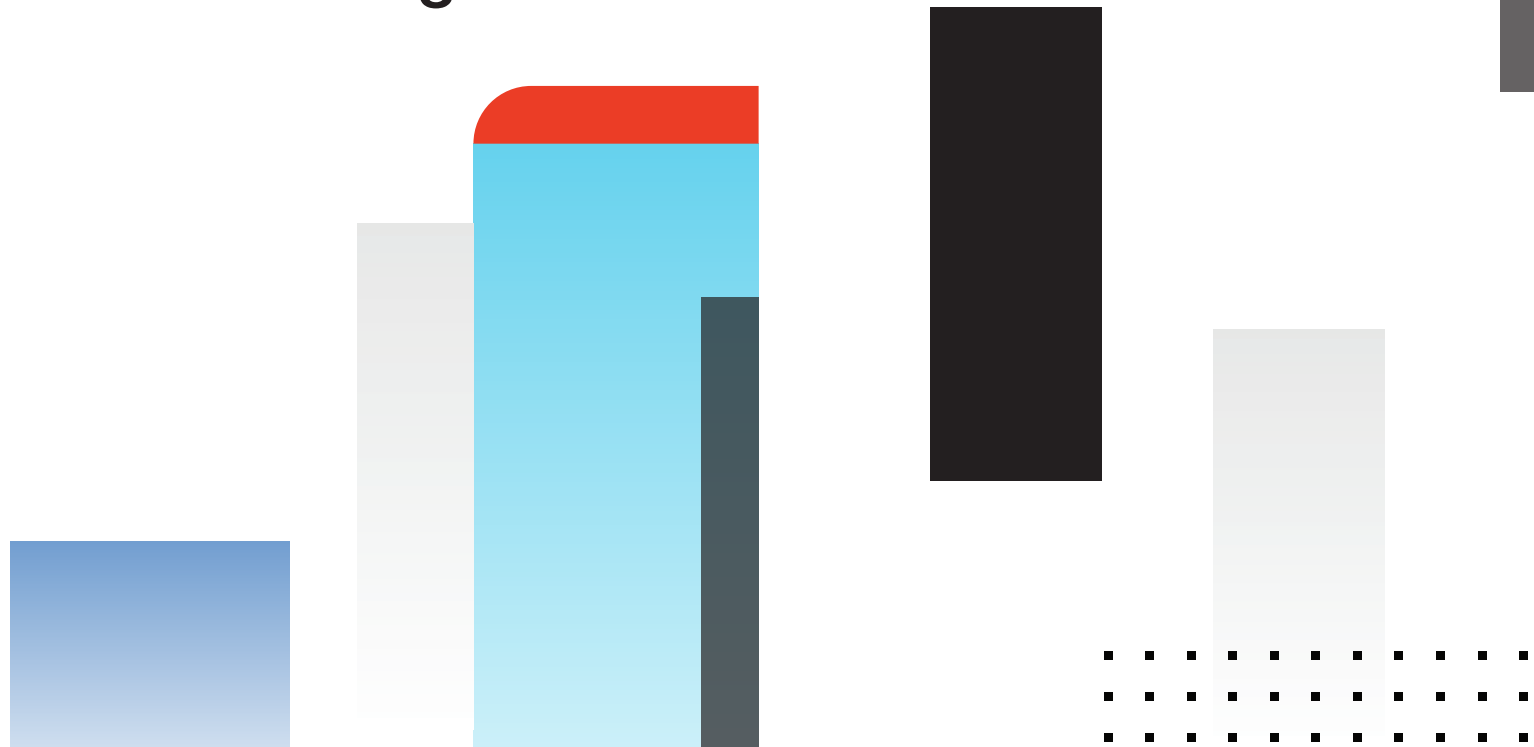


Sicheres SD-WAN: Leitfaden für Netzwerk-Verantwortliche

Sicherheitsorientierte Netzwerke für einen
leistungsstarken WAN-Edge



Inhaltsverzeichnis

Zusammenfassung	3
Einleitung	4
Welcher Weg zum SD-WAN?	6
Erstklassig und modern: Die SD-WAN-Lösung von Fortinet	7
Sicherheitsorientierte Netzwerke	14
In einem volatilen SD-WAN-Markt ist Fortinet die sichere Wahl	15



Zusammenfassung

Digitale Innovationen wie das Cloud-on-Ramping von Software-as-a-Service-Anwendungen (SaaS) und Infrastructure-as-a-Service (IaaS) sind besonders für dezentrale Unternehmen der Schlüssel zu mehr Umsatz und Effizienz. Allerdings steigt durch diese Technologien der Datenverkehr auf eine Weise, dass es bei WAN-Infrastrukturen (Wide Area Network) mit MPLS-Verbindungen (Multiprotocol Label Switching) zu Netzwerk-Engpässen kommt und die Kosten explodieren. Viele Netzwerk-Verantwortliche möchten daher veraltete WAN-Infrastrukturen durch ein softwaredefiniertes Wide Area Networking (SD-WAN) ersetzen. Zehntausende Kunden haben sich bereits für das FortiGate Secure SD-WAN entschieden, das Netzwerk- und Security-Funktionen in einer einheitlichen Lösung vereint, die Anwendungsleistung unterstützt, das Management konsolidiert und einen erweiterten Bedrohungsschutz bietet.



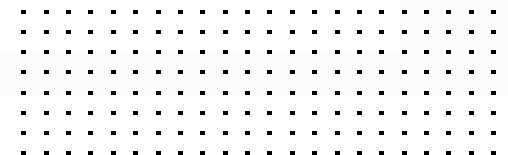
Einleitung

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, einer der renommiertesten Anbieter von Netzwerk-Security, hat seine branchenführenden FortiGate Next-Generation Firewalls (NGFWs) um erstklassige SD-WAN-Funktionen erweitert. FortiGate NGFWs mit Secure SD-WAN bieten eine optimale Leistung für geschäftskritische SaaS-Anwendungen (Software-as-a-Service) sowie digitale Sprach- und Video-Tools. Gleichzeitig helfen sie Unternehmen, sich vor den neuesten Risiken und sich weiterentwickelnden komplexen Angriffen zu schützen.





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



Welcher Weg zum SD-WAN?

Ein SD-WAN bietet die Möglichkeit, verfügbare WAN-Dienste effektiver und wirtschaftlicher zu nutzen. Mitarbeiter in dezentralen Unternehmen erhalten damit mehr Flexibilität bei der persönlichen Kundensprache, der Optimierung von Geschäftsprozessen und der Umsetzung von Innovationen. Zudem senkt ein softwaredefiniertes WAN die Kosten des WAN-Managements – einer der Hauptgründe, warum SD-WAN-Lösungen auf absehbare Zeit ein robuster Wachstumsmarkt bleiben dürften.

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

Laut SD-WAN-Experten und Branchenanalysten bestimmen die Anforderungen des Unternehmens – z. B. hinsichtlich Anwendungsleistung, Sicherheitsprioritäten und vorhandener IT-Kompetenz –, wie das optimale SD-WAN aussehen soll. Generell wird auch empfohlen, dass Unternehmen ihr SD-WAN mit einer NGFW-Lösung kombinieren, um die Security-Probleme zu lösen, die ein direkter Internetzugang in Filialen über Breitbandverbindungen mit sich bringt. Um diese Geschäftsanforderungen zu erfüllen, benötigen Unternehmen ein umfassendes SD-WAN-Angebot wie das FortiGate Secure SD-WAN – die einzige Lösung mit integrierter Security und dem für die SD-WAN-Implementierung notwendigen Funktionsumfang.



Erstklassig und modern: Die SD-WAN-Lösung von Fortinet

Das FortiGate Secure SD-WAN ersetzt separate WAN-Router, WAN-Optimierung und Security-Komponenten wie Firewalls und Secure Web Gateways (SWG) durch eine einzige FortiGate NGFW. Diese bietet eine branchenweit unübertroffene Leistung mit Funktionen wie Anwendungserkennung, automatisierter Pfadintelligenz und WAN-Overlay-Unterstützung für VPNs. Unternehmen erhalten damit sicherheitsorientierte Netzwerke für Filialen mit herausragender Leistung dank der schnellen Anwendungsidentifikation und dem automatisierten, intelligenten Routing.

Anwendungserkennung für verbesserte Service Levels

Das FortiGate Secure SD-WAN wird durch die neue anwendungsspezifische integrierte SOC4-Schaltung (ASIC) unterstützt, die eine schnellere Anwendungssteuerung und eine konkurrenzlose Anwendungsidentifizierung bietet – einschließlich tiefgehender SSL/TLS-Prüfung (Deep Secure Sockets Layer/Transport Layer Security) mit geringstmöglichem Leistungsabfall. Zu den Funktionen zur Verschlüsselungsprüfung gehört auch die Möglichkeit, das Paket zu prüfen, damit die SD-WAN-Lösung den Datenverkehr korrekt weiterleitet.



Technisch gesehen sorgt ein SD-WAN dafür, dass für Anwendungen zu jedem Zeitpunkt die effizienteste WAN-Verbindung gewählt wird. 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 ausbremsen und beeinträchtigen.

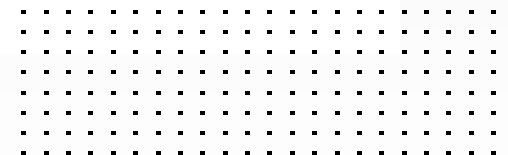
Um diesen Problemen zu begegnen, verwendet das FortiGate Secure SD-WAN eine Application-Control-Datenbank mit den Signaturen von mehr als 5000 Anwendungen (mit regelmäßigen Updates von den FortiGuard Labs Threat Intelligence Services). Das FortiGate Secure SD-WAN identifiziert und klassifiziert Anwendungen – auch verschlüsselten Datenverkehr von Cloud-Anwendungen – vom ersten Paket an.

Das FortiGate Secure SD-WAN bietet:

- **Schnelle Anwendungsidentifikation**
- **Verbesserte Anwendungsgenauigkeit und -leistung**
- **Aktualisierungen der Anwendungsdatenbank anhand neuer Research-Daten der FortiGuard Labs**



**Das FortiGate Secure
SD-WAN erkennt über 5000
Anwendungen automatisch
und leitet sie optimal weiter.**



FortiGate NGFWs können so eingestellt werden, dass sie die Kritikalität von Geschäftsanwendungen erkennen. Geschäftskritische Anwendungen (z. B. Office 365, Salesforce, SAP), allgemeine Produktivitätsanwendungen (wie Dropbox) und Social Media (z. B. Twitter, Instagram) können unterschiedliche Routing-Prioritäten erhalten. Auf tieferer Ebene lassen sich einzigartige Richtlinien für Unteranwendungen einrichten (z. B. Word oder OneNote in Office 365). Diese tiefgehende, umfassende Transparenz auf Anwendungsebene hinsichtlich Verkehrsmustern und Auslastung ermöglicht eine bessere Zuordnung der WAN-Ressourcen je nach Geschäftsanforderungen.

Müheleose WAN-Effizienz

Das FortiGate Secure SD-WAN vereinfacht den Transformationsprozess älterer WAN-Edge-Infrastrukturen erheblich und bietet eine stärkere Anwendungsleistung, bessere Benutzererfahrung und höhere Sicherheit. Sobald die WAN-Richtlinien auf der Grundlage von Anwendungskritikalität, Leistungsanforderungen, Sicherheitsrichtlinien und anderen Kriterien festgelegt wurden, übernimmt die FortiGate Secure SD-WAN-Lösung die restliche Arbeit. Dank spezieller Sicherheitsprozessen (den SOC4 ASICs) bieten FortiGate NGFWs eine 10-mal schnellere Security-Leistung als vergleichbare Firewalls.²

Das FortiGate Secure SD-WAN bietet alle wichtigen Funktionen für ein effizientes WAN:

Automatisierte Pfadintelligenz: Die Anwendungserkennung ermöglicht ein priorisiertes Anwendungs-Routing über die gesamte Netzwerk-Bandbreite, abgestimmt auf die jeweilige Anwendung und den Benutzer. Mit dem neuen SOC4 ASIC verfügt das FortiGate Secure SD-WAN über die schnellste Anwendungssteuerung der Branche. Service-Vereinbarungen (SLAs) für das SD-WAN lassen sich leicht definieren, indem man dynamisch die beste WAN-Verbindung für die spezifischen Geschäftsumstände auswählt. Für Anwendungen mit geringer bis mittlerer Priorität können Unternehmen die Qualitätskriterien vorgeben, und die FortiGate wählt dann eine passende Verbindung aus. Für Anwendungen mit hoher Priorität und geschäftskritische Anwendungen können strenge SLAs definiert werden, die kombinierte Faktoren

WAN-Overlay: Reaktive **Overlay-VPN**-Funktionen verbessern die WAN-Nutzung für Benutzer in Filialen. Die Orchestrierung von **Cloud-Overlay-Controllern**, die auf Abonnementdiensten des **360 Protection Bundle** basieren, vereinfacht die Overlay-VPN-Implementierung mit einer cloudbasierten, automatisierten 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 NGFW integriert, wodurch sich die Komplexität für den Endbenutzer reduziert und gleichzeitig seine Anwendungserfahrung und Produktivität verbessert werden.

WAN-Pfadkorrektur: Die WAN-Pfadkorrektur nutzt die Vorwärtsfehlerkorrektur (Forward Error Correction, FEC), um widrige WAN-Bedingungen, wie schlechte Verbindungen oder Leitungsrauschen zu kompensieren. 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.

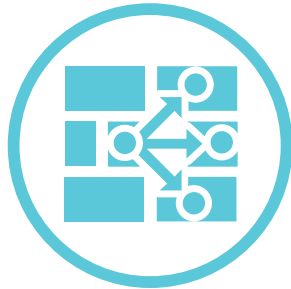
Aggregation der Tunnelbandbreite:

Für Anwendungen, die eine größere Bandbreite erfordern, ermöglicht das FortiGate Secure SD-WAN eine Lastverteilung und Lieferung pro Paket. Hierzu werden zwei Overlay-Tunnel zur Maximierung der Netzwerk-Kapazität kombiniert.

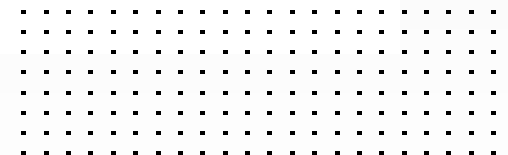
Einfacheres Management und branchenweit geringste Gesamtbetriebskosten (TCO)

Netzwerk-Verantwortliche haben oft Probleme bei der Bereitstellung von SD-WAN-Edge-Geräten in ihren zahlreichen Remote-Standorten und Niederlassungen. Der Einsatz von IT-Experten vor Ort ist teuer und mit personell begrenzten Teams schwer realisierbar. Andererseits ist der Versand von komplett vorkonfigurierten Geräten nicht sicher. Außerdem müssen Mitarbeiter nach der Implementierung der Edge-Geräte sowohl die WAN-Optimierung als auch die Security-Funktionen verwalten können – häufig über zwei verschiedene Schnittstellen. Das FortiGate Secure SD-WAN löst diese Implementierungs- und Management-Probleme und senkt so die Gesamtbetriebskosten (TCO).





Im SD-WAN-Gruppentest der NSS Labs von 2019 wird das FortiGate Secure SD-WAN das zweite Mal in Folge als empfehlenswert bewertet – mit den niedrigsten Gesamtbetriebskosten (TCO) und besonderer Betonung auf den effizienten Netzwerk-Betrieb dank Zero-Touch-Bereitstellung.³



Zero-Touch-Bereitstellung: Dank der vereinfachten Implementierungsfunktionen des FortiGate Secure SD-WAN können Unternehmen einfach FortiGate NGFW-Appliances an alle Remote-Standorte 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 vernetzt es dann mit einem zentralen FortiManager-System.

Management über eine zentrale Konsole: Der FortiManager ermöglicht eine zentrale Transparenz über alle implementierten FortiGate NGFWs im gesamten dezentralen Unternehmen, die ein SD-WAN unterstützen können. Intuitive Visualisierungen machen es einfach, sowohl die physischen als auch die logischen Netzwerk-Topologien 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.

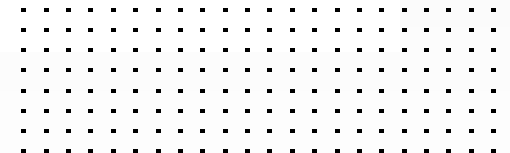
Für Benutzer, die eine sichere Kommunikation über öffentliche Internetverbindungen benötigen, können mit nur einem Klick VPNs eingerichtet werden. All dies spart Zeit, vereinfacht die SD-WAN-Administration (On-Premises oder über die Cloud) und entlastet personell begrenzte Netzwerk-Teams. Fortinet bietet eine der wenigen Lösungen, mit der man das SD-WAN-Netzwerk, die Security und den Access Layer von derselben Management-Konsole aus verwalten kann.

Gesamtbetriebskosten (TCO): Das FortiGate Secure SD-WAN bietet die branchenweit niedrigsten Gesamtbetriebskosten pro Mbit/s – und eine Zero-Touch- Bereitstellung von neuen Filialen und Niederlassungen in weniger als sechs Minuten.⁴ Durch den Umstieg auf das öffentliche Breitband lassen sich teure MPLS-Verbindungen durch kostengünstigere Optionen ersetzen. Mit der transportunabhängigen Lösung von Fortinet können Unternehmen die gesamte verfügbare Bandbreite nutzen, indem sie Verbindungen im Aktiv/Aktiv-Modus laufen lassen.





Das FortiGate Secure SD-WAN erzielt bei Tests der NSS Labs das zweite Jahr in Folge die branchenweit besten Werte bei den Gesamtbetriebskosten (TCO).⁵



Sicherheitsorientierte Netzwerke

Fortinet bietet ein erstklassiges, zertifiziertes SD-WAN, das sowohl leistungsstark als auch geschützt ist. FortiGate NGFWs mit dem SOC4 ASIC liefern die branchenweit schnellste SD-WAN-Security-Leistung. Im „Software-Defined Wide Area Networking Test Report“ der NSS Labs von 2019 erhielt Fortinet das zweite Mal in Folge die Bewertung „Empfohlen“.⁶

Besonders am FortiGate Secure SD-WAN ist auch der robuste SD-WAN-Bedrohungsschutz mit Layer-3- bis Layer-7-Security-Kontrollen – etwas, das man bei anderen SD-WAN-Lösungen mit Firewall selten findet. Unternehmen profitieren dadurch von Vorteilen wie:

- Umfassender Schutz vor Bedrohungen, einschließlich Firewall, Antivirus, Intrusion Prevention System (IPS) und Application Control
- Überprüfung von Deep-Packet-Verschlüsselungen für SSL/TLS (Secure Sockets Layer/Transport Layer Security) mit hohem Durchsatz und minimalen Leistungseinbußen, damit der Komplettschutz vor Bedrohungen nicht zu Lasten der Bandbreite geht
- Web-Filter zur Durchsetzung einer sicheren Internet-Nutzung, ohne dass ein separates Secure Web Gateway (SWG) erforderlich ist
- Hohe WAN-Leistung für Cloud-Anwendungen mit erstklassiger VPN-Overlay-Leistung für eine überlegene Benutzererfahrung und geringe Latenz⁷

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.

Erfolgreiche SD-Branch-Transformation

Viele Filialen entscheiden, sowohl ihre WAN- als auch ihre LAN-Geräte durch eine Lösung mit tiefergehender Integration und vereinfachter Verwaltung zu ersetzen. Getrennte WAN- und LAN-Infrastrukturen verschlimmern nicht nur die Komplexität (mehr Geräte-Implementierungen und Updates mit verschiedenen Management-Konsolen), sondern verringern auch die Transparenz und Kontrolle über Betriebsabläufe – und erhöhen gleichzeitig das Risiko von Sicherheitslücken, die Hacker ausnutzen können. Um diesen Herausforderung zu begegnen, umfasst das FortiGate Secure SD-WAN eine schnellere Security-Erweiterung bis zum Access Layer, die eine 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, können Unternehmen mit dem FortiGate Secure SD-WAN von den Vorteilen digitaler Innovationen profitieren, ohne die Anwendungsleistung zu verlangsamen, die Produktivität der Endanwender zu beeinträchtigen oder Daten zu gefährden.

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

Das FortiGate 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, FortiGate 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, 8. August 2018.

² Basierend auf internen Tests von Fortinet.

³ „[Fortinet wird im SD-WAN-Gruppentest der NSS Labs das zweite Mal als empfehlenswert bewertet](#)“. Fortinet, 19. Juni 2019.

⁴ Ebd.

⁵ Ebd.

⁶ Ebd.

⁷ Ebd.



www.fortinet.com/de

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

May 20, 2021 4:37 PM

eb-network-leaders-guide-to-secure-sd-wan-DE

1006801-C-0-DE