

FortiGate Secure SD-WAN Helps Service Providers Boost Revenue

Executive Overview

As distributed enterprises and small and midsize businesses (SMBs) adopt digital innovations (DI) throughout their distributed environments, their attack surface expands. Dealing with associated network and security challenges often stretches their overburdened teams to a breaking point. This is where managed service providers (MSPs) and managed security service providers (MSSPs) can help, offering managed SD-WAN value-added service (VAS) offerings. FortiGate Secure SD-WAN is a critical linchpin, enabling them to consolidate networking, routing, WAN optimization, and security infrastructure in an integrated, best-in-class solution. With Secure SD-WAN, service providers can offer their customers robust branch WAN networking capabilities that support the latest high-performance digital applications while ensuring security for direct internet access at branch deployments. At the same time, they can elevate their revenue streams per individual user.

Managed SD-WAN Services Need Solution-level Simplicity and Security

Managed services solutions that replace traditional approaches to WAN edge infrastructure at remote sites and branch offices have great potential for addressing the problems of distributed organizations. SD-WAN can help reduce connectivity costs while improving network support for the latest digital tools—such as Software-as-a-Service (SaaS), Voice over IP (VoIP), and video communications. But for any managed SD-WAN service to be effective, the underlying technology that drives it must also fully address the expanded attack surface that comes with DI adoption at the network edge. The SD-WAN solution itself must secure connections and inspect high volumes of traffic without inhibiting network performance. Choosing the right foundational SD-WAN solution is also critical for establishing a managed service's scope, addressable markets, potential revenue, and size of margins.

FortiGate Secure SD-WAN from Fortinet helps service providers deliver best-of-breed SD-WAN performance and Security-as-a-Service (SECaaS) for their customers. At the same time, it helps providers reduce costs by consolidating multiple point solutions while establishing a secure foundation for new VAS offerings. This, over time, increases annual revenue per user (ARPU) as well as depth of penetration and customer loyalty.

Fortinet Delivers Best-of-Breed Secure SD-WAN for Managed Services

FortiGate Secure SD-WAN to SD-WAN improves WAN efficiency without compromising performance, thanks to purpose-built SOC4 integrated circuits (ASICs). At the same time, Fortinet's integrated approach provides consistent policy enforcement and single-pane-of-glass management in a solution that supports managed services with multi-tenancy, interoperability, and automation.

Consolidated CapEx: Integrated security and networking

FortiGate Secure SD-WAN integrates multiple networking and security capabilities into a single-box-solution—including network firewalls, intrusion prevention (IPS), anti-malware, and WAN optimizers. This allows service providers to consolidate the equipment required to deliver a fully featured and secure SD-WAN service that greatly decreases capital expenditure (CapEx) investments and thereby elevates ARPU for service providers.

Optimized OpEx: Simplified orchestration and operations

Eliminating infrastructure complexity not only lowers CapEx costs but also streamlines deployment and operations for reduced management expenses. Other solutions require multiple tools and devices for comprehensive functionality—which increases management burdens and operational costs for service providers. FortiGate Secure SD-WAN improves efficiency for solution deployment and implementation, which, in turn, reduces the time, resources, and costs associated with onboarding new customers.

More than half (53%) of organizations report that they partner with MSPs or MSSPs for implementation and management support.¹

FortiGate Secure SD-WAN also provides automation that simplifies ongoing management workflows for service provider staff. Fortinet's solution provides historical data and comprehensive analytics to help to troubleshoot and quickly address performance issues. These features directly reduce the management time, labor, and costs for customer deployments.

FortiGate Secure SD-WAN-enabled tracking and reporting also help service providers ensure adherence to privacy laws, security standards, and industry regulations, while reducing collateral risks and liability in the event of a breach. These features track real-time threat activity, facilitate risk assessment, detect potential issues, and mitigate problems. Further, they monitor firewall policies and help automate compliance audits that reduce the operational churn on service provider staff.

SD-WAN performance for elastic and efficient managed services

FortiGate Secure SD-WAN is an ideal foundation for managed SD-WAN services, reducing risks along with lowering CapEx and operational expenditure (OpEx) costs. It provides enterprise-grade reliability and high IPsec VPN performance needed for secure direct internet connectivity in order to help service providers meet aggressive service-level agreements (SLAs) without adding more CapEx costs in requisite hardware, which often is required in other SD-WAN solution scenarios.

Application awareness and bandwidth management

FortiGate Secure SD-WAN uses "first-packet identification" to intelligently identify applications on the very first packet of data traffic. As part of this process, it references an application control database of over 5,000 applications—even in encrypted traffic instances. This broad **application awareness** gives service providers comprehensive visibility into which applications are being used across the enterprise to help administrators monitor and manage traffic patterns and make well-informed decisions regarding SD-WAN policy implementation.

Being application aware opens the doors to **automated path intelligence**—namely, the ability to prioritize routing across network bandwidth based on the specific application and user. Here, FortiGate Secure SD-WAN automated path intelligence dynamically selects the best WAN link/connection for the situation. FortiGate NGFWs that feature the new SOC4 ASIC enable the fastest application steering in the industry, including unrivaled application identification performance. Fortinet offers a per-application-level SLA, which helps service providers better meet client SLAs while avoiding higher CapEx and OpEx costs (associated with adding more equipment) as well as SLA penalties.

Other related features in FortiGate SD-WAN include:

- **WAN path remediation**, which utilizes forward error correction (FEC) to overcome the most adverse WAN conditions. This delivers a better user experience for business-critical applications like voice and video services.
- **Tunnel bandwidth aggregation**, which provides per-packet load balancing and delivery by combining two overlay tunnels to maximize network capacity if an application requires greater bandwidth.
- **Automatic failover** capabilities, which change to the best available link when the primary WAN path degrades. This automation is built into FortiGate NGFWs, reducing complexity for end-users while improving their experience and productivity.

In combination, these features help service providers deliver high application availability to customers based on criticality of applications and users, while also optimizing network costs for lower total cost of ownership (TCO).

In NSS Labs testing, FortiGate Secure SD-WAN delivered best user experience with high availability in extreme WAN impairment conditions.² The SD-WAN capabilities that were assessed included zero-touch provisioning, WAN performance, application-aware traffic steering, dynamic path selection with service-level agreement (SLA) measurements, and high availability with WAN impairments.

In the latest NSS Labs NGFW group test, FortiGate delivered 99.3% security effectiveness and 100% evasions blocking.³

Scalable encryption inspection

Organizations need scalable secure sockets layer (SSL)/transport layer security (TLS) inspection to verify the ever-increasing volume of network traffic that is encrypted. Indeed, as much as 60% of encrypted traffic contains hidden malware.⁴ To address this issue, FortiGate Secure SD-WAN includes deep SSL/TLS inspection with the lowest possible performance degradation. This provides visibility and prevention against malware while eliminating the need (plus associated CapEx and OpEx costs) for more firewalls and separate encryption inspection appliances. This further improves Fortinet solution TCO while helping service providers elevate their customer revenue streams.

FortiGate Secure SD-WAN delivered the lowest TCO per Mbps based on real-life scenarios in the latest NSS Labs testing.⁵

A Secure SD-WAN Managed Service Starts with Fortinet

As the basis for a truly effective managed service, FortiGate Secure SD-WAN integrates enhanced SD-WAN networking features with proven NGFW security to improve branch efficiency without compromising protection. Best of all, Fortinet delivers industry-best TCO which reduces both the upfront costs and management overhead of maintaining an SD-WAN solution over time. This helps service providers immediately boost ARPU while increasing customer stickiness for expanded SD-WAN-based services in the future—such as WLAN/LAN services and SD-Branch services—which can expand revenue streams even further.

¹ Survey of IT infrastructure leaders conducted by Fortinet. Broader findings of the survey found in [“The IT Infrastructure Leader and Cybersecurity: A Report on Current Priorities and Challenges,”](#) Fortinet, August 18, 2019.

² Ahmed Basheer, [“Software-defined Wide Area Network Test Report: Fortinet FortiGate 61E,”](#) NSS Labs, June 19, 2019.

³ [“Fortinet Receives Second Consecutive NSS Labs Recommended Rating in SD-WAN Group Test Report,”](#) Fortinet, June 19, 2019.

⁴ Omar Yaacoubi, [“The hidden threat in GDPR’s encryption push,”](#) PrivSec Report, January 8, 2019.

⁵ [“Fortinet Receives Second Consecutive NSS Labs Recommended Rating in SD-WAN Group Test Report,”](#) Fortinet, June 19, 2019.



www.fortinet.com