FORTINET

The Network Leader's Guide to Secure SD-WAN

Security-driven Networking Delivers Comprehensive WAN Edge

Table of Contents

FORTINET

Executive Overview

Digital innovation, such as cloud on-ramping of Software-as-a-Service (SaaS) applications and Infrastructure-as-a-Service (IaaS), is helping to propel revenues and efficiencies for distributed businesses. However, the increased traffic demands of these technologies greatly increase the cost and performance bottlenecks of multiprotocol label switching (MPLS) connectivity over traditional wide area network (WAN) infrastructures. Most network engineering and operations leaders, as a result, are now looking to replace their outdated WAN infrastructures with some form of software-defined wide area networking (SD-WAN). Tens of thousands of customers are choosing FortiGate Secure SD-WAN, which delivers both networking and security capabilities in a unified solution. It supports application performance, consolidated management, and advanced protection against threats.

Introduction

While selecting the right SD-WAN solution for a specific implementation may require a few compromises, security should not be one of them. There are several options for combining SD-WAN networking and advanced security—but only one solution can truly be called Secure SD-WAN. Fortinet, the most trusted name in network security, has added best-of-breed SD-WAN capabilities to its industry-leading FortiGate next-generation firewalls (NGFWs). FortiGate NGFWs featuring Secure SD-WAN provide optimal performance for business-critical Software-as-a-Service (SaaS) applications as well as digital voice and video tools. At the same time, they help protect organizations against the latest risk exposures and evolving sophisticated attacks.

IDC predicts that worldwide SD-WAN infrastructure and services revenue will see a compound annual growth rate (CAGR) of over 40% to reach $4.5 billion by 2022.[1]

Which Way to SD-WAN?

SD-WAN offers the ability to use available WAN services more effectively and economically—giving users across distributed organizations the freedom to better engage customers, optimize business processes, and innovate. It also makes WAN management more cost-effective, which is why SD-WAN solutions will continue to be a robust growth market for the foreseeable future.

To answer this demand, there have been many SD-WAN solutions introduced in the last few years. But not all of them are created equal.

SD-WAN experts and industry analysts say that the optimal SD-WAN for an enterprise depends on the organization's application performance requirements, security priorities, and IT skill sets. It is also widely recommended that companies use an NGFW solution in combination with SD-WAN to address security issues, as branches are directly exposed to the internet via broadband connections with SD-WAN. To address these business requirements, organizations need a comprehensive SD-WAN offering—FortiGate Secure SD-WAN, the only one with built-in security and the performance capabilities an SD-WAN deployment requires.

Fortinet Delivers Best-of-Breed SD-WAN

FortiGate Secure SD-WAN replaces separate WAN routers, WAN optimization, and security devices such as firewalls and secure web gateways (SWGs) with a single FortiGate NGFW. This provides industry-best performance with capabilities that include application awareness, automated path intelligence, and WAN overlay support for VPN. FortiGate Secure SD-WAN delivers security-driven networking for branch networks with outstanding performance enabled by fast application identification and automated path intelligence.

FortiGate Secure SD-WAN Delivers:

- Fast application identification
- Enhanced application accuracy and performance
- Application database updates from FortiGuard Labs research

Application Awareness for Improved Service Levels

FortiGate Secure SD-WAN is powered by the new SOC4 application-specific integrated circuit (ASIC), which provides faster application steering and unrivaled application identification performance). This includes deep secure sockets layer (SSL)/ transport layer security (TLS) inspection with the lowest possible performance degradation. Encryption inspection capabilities also include the ability to inspect the packet in order for the SD-WAN solution to correctly route the traffic.

Technically, SD-WAN works by routing applications over the most efficient WAN connection at any point in time. To ensure optimal application performance, SD-WAN solutions must be able to identify a broad range of applications and apply routing policies at a very granular level. Without these capabilities, SaaS applications, video, and voice can slow and impede end-user productivity.

To address these issues, FortiGate Secure SD-WAN uses an application control database with the signatures of more than 5,000 applications (plus regular updates from FortiGuard Labs threat intelligence services). FortiGate Secure SD-WAN identifies and classifies applications—even encrypted cloud application traffic—from the very first packet.

FortiGate Secure SD-WAN automatically recognizes and optimally routes over 5,000 applications.

FortiGate NGFWs can be set to recognize applications by business criticality. Business-critical applications (e.g., Office 365, Salesforce, SAP), general productivity applications (e.g., Dropbox), and social media (e.g., Twitter, Instagram) can be given different routing priorities. Unique policies can be applied at a deeper level for sub-applications (e.g., Word or OneNote within Office 365). This deep and broad application-level visibility into traffic patterns and utilization offers a better position to allocate WAN resources according to business needs.

Effortless WAN Efficiency

FortiGate Secure SD-WAN greatly simplifies the process of transforming legacy WAN edge infrastructures to provide enhanced application performance, a better user experience, and improved security. Once WAN policies are set based on application criticality, performance requirements, security policies, and other considerations, the FortiGate Secure SD-WAN solution takes over from there. FortiGate NGFWs featuring the SOC4 ASIC deliver 10 times faster security performance than the competition.[2]

When it comes to WAN efficiencies, key capabilities in FortiGate Secure SD-WAN include:

Automated path intelligence. Application awareness enables prioritized application routing across network bandwidth based on the specific application and user. The new SOC4 ASIC gives FortiGate Secure SD-WAN the fastest application steering in the industry. SD-WAN service-level agreements (SLAs) are easily defined by dynamically selecting the best WAN connection for the specific business circumstances. For low- to medium-priority applications, organizations can specify the quality criteria, and the FortiGate will select the corresponding link. For high-priority and business-critical applications, organizations can define strict SLAs based on a combination of jitter, packet loss, and latency metrics

WAN overlay. Responsive **overlay VPN** capabilities enable a better overall WAN experience for branch users. **Cloud overlay controller** orchestration, powered by **360 Protection Bundle** subscription services, simplifies overlay VPN deployment with cloud-based automated provisioning.

Automatic failover. Multi-path technology can automatically fail over to the best available link when the primary WAN path degrades. This automation is built into the FortiGate NGFW, which reduces complexity for end-users while improving their experience and productivity.

WAN path remediation. WAN path remediation utilizes forward error correction (FEC) to overcome adverse WAN conditions such as poor or noisy links. This enhances data reliability and delivers a better user experience for applications like voice and video services. FEC adds error correction data to the outbound traffic, allowing the receiving end to recover from packet loss and other errors that occur during transmission. This improves the quality of real-time applications.

Tunnel bandwidth aggregation. For applications that require greater bandwidth, FortiGate Secure SD-WAN enables per-packet load balancing and delivery by combining two overlay tunnels to maximize network capacity.

Simplified Management and Industry-Best TCO

Network engineering and operations leaders are often in a quandary when it comes to deploying SD-WAN edge devices to their numerous remote sites and branch offices. Truck rolls are expensive, and technical staff is often limited. On the other hand, shipping fully configured devices is not secure. Also, once edge devices are deployed, staff must manage both the WAN optimization functions and security functions, often from two different interfaces. FortiGate Secure SD-WAN solves both deployment and the management problems to reduce total cost of ownership (TCO).

In NSS Labs' 2019 SD-WAN Group Test Results, FortiGate Secure SD-WAN received a second straight "Recommended" rating—earning the lowest total cost of ownership (TCO) rating and highlighting its quick zero-touch provisioning for efficient operations.[3]

Zero-touch deployment. FortiGate Secure SD-WAN's simplified deployment capabilities allow enterprises to ship unconfigured FortiGate NGFW appliances to each remote site. When plugged in, the FortiGate automatically connects to the FortiDeploy service in FortiCloud. Within seconds, FortiDeploy authenticates the remote device and connects it to a central FortiManager system.

Single-pane-of-glass management. FortiManager enables centralized visibility of all deployed Secure SD-WAN-enabled FortiGate NGFWs across the distributed organization. Highly intuitive visualizations make it easy to monitor both the physical and logical network topologies at a high level and drill down when needed to investigate any issues. Administrators can update and disseminate corporate WAN policies to all locations or reconfigure individual devices.

For users who need secure communications over the public internet links, VPNs can be set up with just one click. All this saves time and simplifies SD-WAN administration (on-premises or via the cloud), alleviating pressure on lean network teams. Fortinet offers one of the only solutions that can manage SD-WAN networking, security, and access layer controls from the same management console.

TCO. FortiGate Secure SD-WAN delivers industry-leading TCO per Mbps—along with zero-touch provisioning of new branches under six minutes.[4] The move to public broadband means that expensive MPLS connections can be replaced with more cost-effective options. With the Fortinet transport-agnostic solution, enterprises can utilize the entire available bandwidth by using the connections in active-active mode.

For the second year in a row, FortiGate Secure SD-WAN delivers industry-best TCO, according to NSS Labs testing.[5]

Security-driven Networking

Fortinet enables best-of-breed, certified SD-WAN that is both high-performance and protected. FortiGate NGFWs featuring the SOC4 ASIC deliver the fastest SD-WAN security performance in the industry. In NSS Labs' 2019 "Software-Defined Wide Area Networking Test Report," Fortinet received a second straight "Recommended" rating.[6]

Specifically, FortiGate Secure SD-WAN has robust SD-WAN threat protection, including Layer 3 through Layer 7security controls not commonly found in other SD-WAN-plus-firewall solutions:

- Complete threat protection, including firewall, antivirus, intrusion prevention system (IPS), and application control
- High-throughput secure sockets layer (SSL)/transport layer security (TLS) deep-packet encryption inspection with minimal performance degradation, ensuring that organizations do not sacrifice throughput for complete threat protection
- Web filtering to enforce internet security without requiring a separate secure web gateway (SWG) device
- High WAN performance for cloud applications, featuring exceptional VPN overlay performance for superior user experience and low latency[7]

Secure SD-WAN-enabled FortiGate NGFWs also monitor firewall rules and policies and highlight best practices to improve the organization's overall security posture. This helps to simplify compliance with security standards as well as privacy laws and industry regulations. Automated auditing and reporting workflows save staff hours while reducing the risk of omissions and errors.

Enabling the SD-Branch

Many enterprise branches are deciding to simultaneously replace both their WAN and LAN devices in favor of a solution with deeper integration and simplified branch operations management. Using separate WAN and LAN infrastructures increases branch complexity; there are more devices to deploy and update with multiple management consoles. It also reduces visibility and control of operations while increasing the opportunities for security gaps that hackers can exploit. To solve these challenges, FortiGate Secure SD-WAN includes an accelerated security extension to the access layer that enables SD-Branch transformation.

In a Volatile SD-WAN Market, Fortinet Is the Safe Bet

As cloud-based applications and tools like voice and video become increasingly critical to distributed businesses, FortiGate Secure SD-WAN can help organizations embrace the benefits of digital innovation without bottlenecking application performance, impacting end-user productivity, or putting data at risk.

FortiGate Secure SD-WAN is scalable, helping organizations confidently support more remote sites, more bandwidth-sensitive, business-critical applications, more cloud services, and whatever else the branch network requires.

FortiGate Secure SD-WAN has been adopted worldwide in wide-ranging industries—from finance, to retail, to manufacturing, to customer service. Whether they need to support a few hundred mobile endpoints or tens of thousands of branch offices, FortiGate Secure SD-WAN customers are each achieving their own optimal mix of best-of-breed security and SD-WAN functionality.

[1] "SD-WAN Infrastructure Market Poised to Reach $4.5 Billion in 2022," IDC, August 8, 2018.

[2] Based on internal testing by Fortinet.

[3] "Fortinet Receives Second Consecutive NSS Labs Recommended Rating in SD-WAN Group Test Report," Fortinet, June 19, 2019.

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] Ibid.

FORTINET

www.fortinet.com

372656-0-0-EN

October 3, 2019 5:21 AM

eb-the-network-leaders-guide-to-secure-sd-wan-v2.1