FORTINET®

The Network Leader's Guide to Secure SD-WAN

Security-driven Networking Delivers Comprehensive WAN Edge

Table of Contents

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 Most network engineering and operations leaders, as a result, are now looking to replace their outdated WAN infrastructures with some form of software-defined wide area networking (SD-WAN).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 Fortinet 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

With Digital Innovations placing increased demands on bandwidth requirement to deliver best user experience, SD-WAN requirements are maturing but many solutions are incomplete. Issues like limited scalability, the lack of automation to simplify operations, and lackluster cloud on-ramp and cloud and SaaS integrations can result in a poor user experience that can undermine the value of an SD-WAN deployment. Instead, SD-WAN solutions need to provide a robust set of networking and connectivity tools that can meet and adapt to the dynamic nature of digital innovation, especially as organizations move more aggressively to the cloud, transition from regional to global deployments, or expand the number of their regional offices.

Fortinet delivers Secure SD-WAN, powered by the industry's first SD-WAN ASIC to enable better application experience, higher performance, and better cost efficiency.
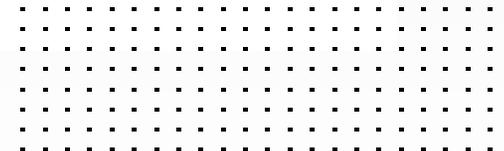
Which Way to SD-WAN?

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. WAN innovation with additional carrier links can be leveraged to provide redundancy, load-balancing and optimization of applciation traffic. 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, faster cloud-on-ramp to multi-cloud access and simplified operations with centralized management to reduce complexity. 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—Fortinet Secure SD-WAN, the only one with built-in security and the performance capabilities flexible to deploy at scale across any size enterprise.

Fortinet Delivers Best-of-Breed SD-WAN

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

Application Awareness for Improved Service Levels

Fortinet 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, SDWAN 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, Fortinet 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). Fortinet Secure SD-WAN identifies and classifies applications—even encrypted cloud application traffic—from the very first packet.
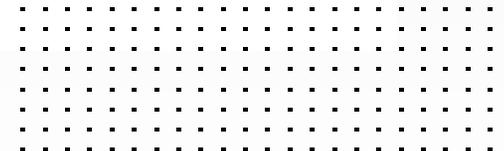
Fortinet Secure SD-WAN Delivers:

- Optimal application experience with accurate detection
- Effective business policies based on application signature
- Constant Application database updates from FortiGuard Labs research

Fortinet Secure SD-WAN accurately recognizes and optimally routes over 5,000 applications.

Fortinet 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 subapplications (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

Fortinet 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 Fortinet Secure SD-WAN solution takes over from there. Fortinet NGFWs featuring the SOC4 ASIC deliver 10 times faster security performance than the competition.[1]

When it comes to WAN efficiencies, key capabilities in Fortinet 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 Fortinet 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.

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 Fortinet NGFW, which reduces complexity for endusers 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.

Prioritize applications. With Fortinet Secure SD-WAN's ability to define application-specific business policies, the best possible utilization of bandwidth can be ensured by adding precise QoS prioritization for critical applications, while rate-limiting non-critical applications that can impact performance and end user experience.

Tunnel bandwidth aggregation. For applications that require greater bandwidth, Fortinet 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. Fortinet Secure SD-WAN solves both deployment and the management problems to reduce total cost of ownership (TCO).
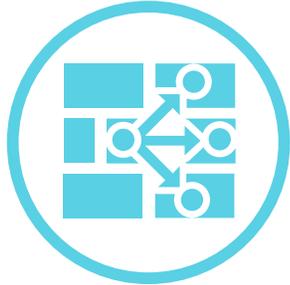
Fabric Management Center allows for effective network operations and agile network management for customers across SD-WAN and security projects.[2]
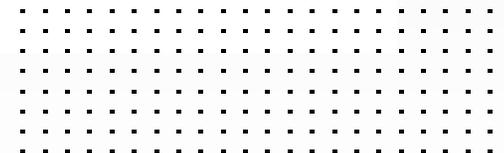
Zero-touch deployment. Fortinet Secure SD-WAN's simplified deployment capabilities allow enterprises to ship unconfigured Fortinet NGFW appliances to each remote site. When plugged in, the FortiGate automatically connects to the FortiDeploy service in FortiCloud. Within seconds, FortiDeploy authenticates the remote device and connects it to a central FortiManager system.

Single-pane-of-glass management. Fortinet Fabric Management Center enables centralized visibility of all deployed Secure SD-WAN-enabled Fortinet NGFWs across the distributed organization. Fortinet secure SDWAN orchestrator offers simplified work flow to deploy and update policies with few easy clicks/steps.

SD-WAN orchestrator automatically builds and manages full mesh overlay links for secure connectivity between sites. With guided work flows, automated overlay bring up and simplified business policies SD-WAN orchestrator reduces the IT staff hours spent on infrastructure deployment and changes from months to minutes.

Fabric Management Center offers advanced telemetry for application visibility and network performance to achieve faster resolution and reduce
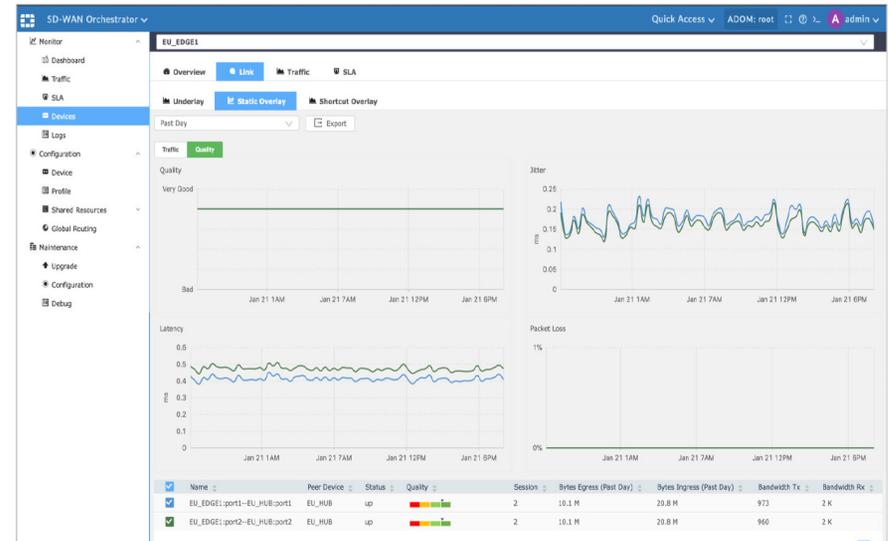
the number of IT support tickets. On-demand SD-WAN reports provides further insight into threat landscape, trust level and asset access which are mandated for compliance purposes.

SD-WAN reporting and analytics. Enhanced analytics for WAN link availability, performance SLA and application traffic in runtime, and historical stats allow the infrastructure team to troubleshoot and quickly resolve network issues. Fabric Management Center offers advanced telemetry for application visibility and network performance to achieve faster resolution and reduce the number of IT support tickets. On-demand SD-WAN reports provide further insight into the threat landscape, trust level, and asset access, which are mandated for compliance purposes.

These features include SD-WAN bandwidth monitoring reports and datasets; service-level agreement (SLA) logging and history monitoring via datasets, charts, and reports plus customizable SLA alerting; and application usage reports and dashboards. It also provides adaptive response handlers for SD-WAN events as well as event logging and archiving around SLAs across applications and interfaces.

Low Latency access to distributed cloud. Provide Low Latency Cloud Access for Easy Collaboration Fortinet Secure SD-WAN not only provides instant multicloud access for the rapid adoption of shared applications such as Office365. Its built-in security adds another layer of secure access to these applications, while providing a low latency connection through public internet links so they can become part of the trusted and reliable WAN infrastructure.

This is especially critical as remote workers and their families use advanced, feature-rich cloud-hosted applications for voice and video conferencing. While these applications provide enhanced voice and video capabilities, they also demand more bandwidth availability. And in most cases, that traffic can also be encrypted, which puts even more pressure on things like traffic inspection. With the intelligence to detect subapplications and provide encrypted applications with SSL inspection capability at line rates, Fortinet Secure SDWAN ensures these applications are steered to the best performing WAN link to provide optimal performance.

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. Fortinet Secure SD-WAN delivers industry-leading TCO per Mbps—along with zero-touch provisioning of new branches under six minutes.[3] 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.

Fortinet leads the market with Secure SD-WAN innovation, able to scale from home office to branch to distributed cloud.[4]
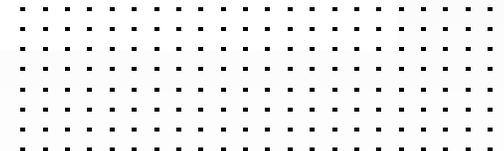
Security-driven Networking

Fortinet enables best-of-breed, certified SD-WAN that is both high-performance and protected. Fortinet 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.[5]

Specifically, Fortinet Secure SD-WAN has robust SD-WAN threat protection, including Layer 3 through Layer 7 security 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[6]

Secure SD-WAN-enabled Fortinet 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, Fortinet 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, Fortinet 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.

Fortinet 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.

Fortinet 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, Fortinet Secure SD-WAN customers are each achieving their own optimal mix of best-of-breed security and SD-WAN functionality.

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

[2] "Fortinet Leads the Market with Secure SD-WAN Innovation," Fortinet, May 2020.

[3] "SD-WAN Infrastructure Market Posied to Reach $5.25 Billion in 2023," July 2019.

[4] "Learn more about a Fortune 500 customer that achieved a 65% cost reduction," Fortinet, April 24, 2020.

[5] Ibid.

F:RTINET

www.fortinet.com