SOLUTION BRIEF

Upgrade Branch Infrastructures with Fortinet Secure SD-WAN

Executive Overview

As the use of business-critical, cloud-based applications and tools continues to increase, distributed organizations with multiple remote offices are switching from performance-inhibited wide-area networks (WANs) to software-defined WAN (SD-WAN) architectures. SD-WAN offers faster connectivity, cost savings, and performance for Software-as-a-Service (SaaS) applications as well as digital voice and video services. But SD-WAN has its own shortcomings—especially when it comes to security.

The global SD-WAN market is projected to grow at over 40% compound annual growth rate (CAGR) to reach $4.5 billion by 2022.[4]

Fortinet FortiGate next-generation firewalls (NGFWs) include Secure SD-WAN capabilities that deliver security-driven networking in a unified solution. The Fortinet solution boosts application performance through instant identification and intelligent routing. Additional features increase branch network performance while simplifying security and compliance risk management workflows.

Distributed enterprises are adopting digital transformation (DX) technologies—such as SaaS applications and IP-based tools for voice and video—to increase productivity, improve communications, and foster rapid business growth. But these cloud-based tools and services place a great deal of demand on legacy WAN infrastructures, especially considering enterprise user expectations for very high-quality performance.

This issue is becoming increasing important to growing businesses. According to one recent report, 60% of companies have already adopted at least some SaaS applications.[1] And adoption rates are going to increase in velocity: the worldwide SaaS market is projected to continue growing at a compound annual growth rate (CAGR) of 21.2% between 2018 and 2023.[2] But at the same time, 64% of IT decision-makers believe their organization's SaaS adoption is outpacing their ability to secure it.[3]

Traditional WANs utilize private multiprotocol label switching (MPLS) links, which carry a premium price for connectivity. But more important than cost, there is also productivity to consider. Most traditional WANs feature a "hub-and-spoke" architecture that funnels branch network traffic back to the organization's main data center for filtering and security checks.

While this provides centralized protection, it also increases latency and slows down network performance. This is an especially keen problem for cloud-based tools like Voice over IP (VoIP) and videoconferencing technologies. Voice and video place a great deal of demand on network resources, and enterprise users typically require high-quality performance from these services.

Thus, many organizations with distributed locations that are in the midst of DX initiatives are seeking to replace their outdated WAN infrastructures. They need branch networking with significant simplification, improved cost advantage, and better support for cloud adoption. SD-WAN technology effectively solves the aforementioned problems of bandwidth costs and traffic latency, allowing organizations to move beyond MPLS to include public broadband connections and even wireless 4G/LTE and 5G connections. SD-WAN routes network traffic from branches to the cloud, headquarters, or other branches by enabling direct access to cloud applications and services—which makes it a very popular choice for transforming enterprises.

SD-WAN Cannot Succeed Without Security

While SD-WAN offers connectivity options, performance gains, and a cost advantage over traditional WANs, it has several shortcomings:

- **Complexity.** SD-WAN architectures can be difficult to troubleshoot and hard to manage across all the branches. This adds to the burden on limited IT staff and often creates defensive gaps for threats to exploit.
- **Security.** Without the centralized protection provided by backhauling traffic through the data center, moving direct internet broadband links exposes organizations to new risks. Effective SD-WAN implementation requires additional security within the enterprise infrastructure to secure those connections and inspect high volumes of traffic—all without inhibiting network performance.
- **Encrypted traffic inspection.** Most SD-WAN solutions lack the ability to inspect secure sockets layer (SSL)/transport layer security (TLS) encrypted traffic, which comprises 72% of network traffic today.[5] Specifically, as cyber criminals are hiding malware to infiltrate networks and using it to exfiltrate data, organizations either put themselves at risk or must purchase additional appliances to inspect encrypted traffic at the edge of the network.

Advanced Networking and Security, Combined—Fortinet Secure SD-WAN

FortiGate next-generation firewalls (NGFWs) include Fortinet Secure SD-WAN capabilities, providing both networking and security for SD-WAN branch networks in a single solution. It provides efficient protection across all branch outposts by providing consistent policy enforcement with single-pane-of-glass management. It also allows enterprises to mitigate risks associated with DX.

In NSS Labs' first "Software-Defined Wide Area Networking Test Report," Fortinet was the only vendor with security capabilities to receive a "Recommended" rating.[6] FortiGate NGFWs also have the lead in total number of annual security unit shipments worldwide.[7] For SD-WAN capabilities, FortiGate combines NGFW and SD-WAN features in a single solution that improves WAN efficiency and security.

Fortinet Secure SD-WAN key capabilities include:

Application Awareness and Automated Path Intelligence

With traditional WAN, enterprises have a hard time maintaining the quality of user experience per application. Traditional WAN infrastructure relies on packet routing, which limits application visibility.

Fortinet Secure SD-WAN uses "first-packet identification" to intelligently identify applications on the very first packet of data traffic. This broad **application awareness** helps network teams see which applications are being used across the enterprise, enabling them to make well-informed decisions regarding SD-WAN policies. Fortinet Secure SD-WAN references an application control database of over 5,000 applications, a number that continues to grow as both the threat landscape and digital network evolve.

Being application aware opens the doors to **automated path intelligence**—prioritizing routing across network bandwidth based on the specific application and user. Offering a per-application-level SLA, Fortinet Secure SD-WAN automated path intelligence dynamically selects the best WAN link/connection for the situation. FortiGate NGFWs that feature the new SOC4 application-specific integrated circuit (ASIC) enable the fastest application steering in the industry, including unrivaled application identification performance. This includes deep SSL/TLS inspection with the lowest possible performance degradation. Related features include:

- **WAN path remediation**, which 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**, 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.

NGFW Security and Compliance

Fortinet Secure SD-WAN delivers enterprise-class security and branch networking capabilities with a single-box solution—the FortiGate NGFW. Critical security features include:

- **SSL/TLS inspection and threat protection** to provide visibility and prevention against malware that obviates the need for separate encryption inspection appliances
- **Web filtering service** to enforce internet security and reduce complexity, eliminating the need for a separate Secure Web Gateway device
- **Complete threat protection**, including sandboxing, anti-malware, and intrusion prevention system (IPS)
- **Highly scalable overlay VPN tunnels** with high throughput for ensuring that traffic is always encrypted and stays confidential
- **Granular SLA analytics**, including application transactions for quick remediation

A key feature of SD-WAN is its ability to deliver the cost-performance benefits of internet-based VPNs with the performance and agility of MPLS VPNs.[8]

Fortinet Secure SD-WAN-enabled tracking and reporting help ensure adherence to privacy laws, security standards, and industry regulations while reducing collateral risks of fines and legal costs in the event of a breach. These features track real-time threat activity, facilitate risk assessment, detect potential issues, and mitigate problems. They also monitor firewall policies and help automate compliance audits.

Fortinet **Security Rating Service** provides best practices for regulations such as the Payment Card Industry Data Security Standard (PCI DSS) and real-time tracking and reporting against security standards such as the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS). As part of the service, organizations receive their own security posture score and are then able to compare that to the scores of their peers.

Simplified Management, Orchestration, and Overlay Control

As enterprises adopt SD-WAN, they need the right tools to seamlessly deploy and manage it across widely distributed infrastructures. Fortinet Secure SD-WAN can be administered through FortiManager, a single intuitive and unified management console. It includes options for a cloud-based or hosted solution for remote control and orchestration across thousands of locations. With FortiManager, FortiGate devices are true plug and play. Centralized policies and device information can be configured with FortiManager, and the FortiGate devices are automatically updated to the latest policy configuration.

FortiGate NGFWs featuring the SOC4 ASIC deliver the fastest SD-WAN security performance in the industry. This includes acceleration for responsive **overlay VPN** and a better overall WAN user experience across the enterprise. **Cloud overlay controller** orchestration, powered by the 360 Protection Bundle subscription services, simplifies overlay VPN deployment with cloud-based automated provisioning. The flexibility of single-pane-of-glass management includes scalable remote security and network control via the cloud for all branches and locations.

Total Cost of Ownership

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 Secure SD-WAN delivers the industry's best total cost of ownership (TCO)—10x better than the competition.[9]

Security-Driven Networking

There are many different SD-WANs on the market today, and VPs of IT should carefully review their options. Fortinet Secure SD-WAN integrates enhanced SD-WAN features with proven security capabilities, delivering security-driven networking that improves branch efficiency without compromising protection.

[1] "SaaS Adoption Rising," Computer Economics, November 2018.

[2] "Global Software-as-a-Service (SaaS) Market Outlook (2018-2023)," Business Wire, November 14, 2018.

[3] Conner Forrest, "Businesses are adopting SaaS too fast to properly secure it," TechRepublic, April 10, 2018.

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

[5] John Maddison, "More Encrypted Traffic Than Ever," Fortinet, December 10, 2018.

[6] "Fortinet SD-WAN gives the performance of a lifetime," Fortinet, August 9, 2018.

[7] "IDC Worldwide Security Appliances Tracker," April 2018 (based on annual unit shipments).

[8] Zeus Kerravala, "Understanding Virtual Private Networks (and why VPNs are important to SD-WAN)," Network World, April 13, 2018.

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

March 22, 2019 7:49 PM

372029-0-0-EN

D:\Fortinet\Work\March\032219\Task 2\sb-fortinet-sd-wan