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.

Fortinet, powered by industries first SD-WAN ASIC enable better application experience, higher performance, and better operational efficiency.[3]

Fortinet delivers Secure SD-WAN as an integrated feature of its industry-leading Fortinet next-generation firewall, powered by the industry's first SD-WAN ASIC to enable better application experience, higher performance, and better cost efficiency. The Fortinet solution boosts application performance through instant identification and intelligent routing. To help implement network changes that ensure business continuity with limited IT staff and infrastructure resources, Fortinet's broad product portfolio with built-in SD-WAN offers flexible business policies from a centralized Fabric Management Center console.

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, by 2024, to increase agility and enhance support for cloud applications, 60% of enterprises will have implemented SD-WAN, compared with less than 20% in 2019 to support increasing needs for SaaS application and cloud-on-ramp.[1]

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, as organizations digitally transform, the WAN edge market has continued to shift from the traditional hub-and-spoke architecture to a more distributed cloud connectivity and access to internet based resources in addition to other corporate locations. They need branch networking with significant simplification, improved applicaton performance, and faster Cloud-on-ramp for optimal access to SaaS and UCaaS applications. 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.[3]

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

Fortinet has traditionally supported advanced networking features including dynamic routing, ipv4/v6 and multicast support. Fortinet next-generation firewalls(NGFWs) with built-in SD-WAN capabilities provide both networking and security for branch networks in a single consolidated 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.

With over 21,550 customer deployments, Fortinet leads the market with Secure SD-WAN innovation with a integrated SD-WAN and security capabilities. For SD-WAN capabilities, Fortinet combines NGFW and SD-WAN features in a single solution that imporves WAN efficiency and security.[2]

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. Fortinet 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 Fortinet 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 Fortinet 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

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]

- **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

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.[2]

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. Fortinet Secure SD-WAN offers enhanced analytics and new SD-WAN reports with Fabric Management Center. Single console and rich SD-WAN analytics helps customers to fine-tune their business and security policies to improve quality of experience for all their users. Fortinet enables customers to focus on digital innovations and make network more agile.

Secure SD-WAN orchestrator: To help organizations overcome challenges associated with manually managing legacy routers, Fortinet introduced an intuitive Secure SD-WAN orchestrator as part of the Fortinet Fabric Management Center. This allows customers to significantly simplify centralized deployment and enable automation using intuitive workflows to save time and offer business centric policies.[3]

Enhanced analytics: To help organizations gain visibility into network and application performance (both real-time and historical statistics), Fortinet Secure SD-WAN offers enhanced analytics, as well as enhanced compliance, and delivers new SD-WAN reports via the Fabric Management Center. A single console and rich SD-WAN analytics help customers fine-tune their business and security policies to improve quality of experience for all users.[3]

Scalable and Flexible SD-WAN Solution

Home Office: Offered as a desktop appliance with built-in LTE, FortiGate 40F supports “super users” at home who require their applications to work without fail for business critical activities such as customer video demonstrations. With the minimal footprint of Fortinet’s desktop appliance, remote workers can procure and install a solution at their home offices to handle routing, security, and wireless needs in a single, integrated platform. The critical advantage of extending SD-WAN functionality to individual teleworkers, especially super users, is that they can enjoy on-demand remote access as well as dynamically scalable performance regardless of their local network availability. And when others in the organization rely on these individuals to do their jobs quickly and efficiently, SD-WAN functionality can make all the difference.

Branch: Fortinet Secure SD-WAN is perhaps the most well-known for supporting complex branch deployments with advanced routing and cloud on-ramp capabilities, which has helped thousands of customers to reduce their use of point products such as legacy routers, while improving business application experience.

Distributed Cloud: For organizations with applications in distributed clouds, Fortinet Secure SD-WAN offers the most comprehensive technology building blocks for interconnecting clouds for better user experience. Fortinet Secure SD-WAN is available in every cloud provider and enables the industry's highest IPsec throughput at 20Gbps to interconnect clouds. With native application steering and cloud integration framework, as well as fully programmable API, Fortinet Secure SD-WAN helps customers to connect hundreds of cloud environments.

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] "SD-WAN Infrastructure Market Poised to Reach $5.25 Billion in 2023," IDC, July 2019.

[2] "SD-WAN Should be a Feature, Not a Stand-Alone Solution," NetworkWorld, May 2020.

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

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

[5] "Fortinet Secure SD-WAN receives a second consecutive "Recommended" rating in NSS Labs report," Fortinet, July 2019.

FORTINET

www.fortinet.com

May 27, 2020 8:16 AM

372029-0-0-EN

Macintosh HD:Users:spedersen:Desktop:sb-fortinet-sd-wan Folder:sb-fortinet-sd-wan