

SOLUTION BRIEF

Upgrade Branch Infrastructures and Accelerate Wireless WAN Deployments With Fortinet Secure SD-WAN

Executive Summary

Ubiquitous connectivity, migration to the cloud, and investment in modern networking technologies to enable digital acceleration have created a rapid expansion of attack surfaces and an explosion of new network edges. This has created a perfect storm of complexity, especially when coupled with the need to maintain high performance and optimal user experience while simplifying operational management.

As a result, 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 cloud applications as well as digital voice and video services.

Fortinet delivers Secure SD-WAN as an integrated capability of its industry-leading FortiGate Next-Generation Firewall (NGFW). Powered by the industry's first SD-WAN ASIC, Fortinet Secure SD-WAN enables superior quality of experience (QoE), accelerated network and security convergence, and improved operational efficiency. The Fortinet option also offers tight integration with LTE/5G connectivity options and enables a zero-trust edge architecture that brings networking and security together.

Fortinet Secure SD-WAN Addresses Common Shortcomings

While SD-WAN offers connectivity options, performance gains, and a cost advantage over traditional WANs, most solutions have shortcomings. Fortinet Secure SD-WAN solves these issues.

Complexity. SD-WAN architectures that do not include security and require more than one management console can be difficult to troubleshoot and hard to manage across all the branches. Fortinet reduces complexity with built-in security and centralized management, and therefore also reduces the burden on limited IT staff. Integrated security closes gaps introduced by "bolted-on security." Complexity is further decreased via tight integration with the LTE/5G wireless WAN.

Inadequate security. Without the centralized protection that was previously provided by backhauling traffic through the data center, organizations are exposed to new risks via direct internet connections. With the FortiGate NGFW's proven, comprehensive, high-performance security, effective SD-WAN implementation is achieved with protection for all connections, including LTE and 5G.

No integration with LTE/5G wireless. Without integrated SD-WAN and LTE/5G wireless WAN, organizations may run into problems fully achieving digital acceleration. Fortinet integration accelerates deployments and simplifies operation while ensuring reliable and secure connectivity. It delivers out-of-band management and active/active high availability via LTE/5G links.

Plus, enterprises can continue their digital acceleration efforts even in locations where cable/DSL can't reach. Ultra-fast LTE/5G WAN links, along with fast cellular failover means that cellular is more than just a backup. It could become the primary branch connection.

FROST & SULLIVAN

Global Alliance Partnership

"Though Fortinet is best known as a security company, they have shown their strength and innovation in networking as one of the top SD-WAN solutions on the market capable of supporting enterprise digital transformation."

– Roopa Honnachari, VP of Research, Network Services & Edge, Frost & Sullivan

Lack of encrypted traffic inspection. Most SD-WAN solutions lack the ability to inspect secure sockets layer (SSL)/transport layer security (TLS) encrypted traffic, which comprises the vast majority of network traffic today. Only with high-performance inspection can sophisticated malware hidden in encrypted traffic be detected and stopped. With Fortinet Secure SD-WAN, organizations do not need to choose between putting themselves at serious risk or purchasing additional appliances to inspect encrypted traffic at the edge of the network.

**95 percent of traffic
is encrypted as of
January 1, 2022.²**

Benefits of Converged Networking and Security With Fortinet Secure SD-WAN

Fortinet NGFWs with built-in SD-WAN capabilities provide both networking and security for branch networks in a single converged solution. The solution provides efficient protection across all branches by providing consistent policy enforcement with single-pane-of-glass management.

Our combination of SD-WAN, NGFW, advanced routing, and zero-trust network access (ZTNA) proxy features in a single solution improves WAN efficiency and security to enable a zero-trust edge architecture. In addition, tight LTE/5G gateway integration with Fortinet Secure SD-WAN accelerates deployments and simplifies operations while ensuring reliable and secure connectivity.

Key Fortinet Secure SD-WAN capabilities

Application awareness. 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, including encrypted traffic, 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.

Automated path intelligence. With application awareness, automated path intelligence—prioritizing routing across network bandwidth based on the specific application and user—is then possible. Offering per-application-level service-level agreement (SLA), Fortinet Secure SD-WAN automated path intelligence dynamically selects the best WAN link/connection, inclusive of LTE/5G, for the situation. Fortinet NGFWs that feature the new SoC4 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.

WAN path remediation. Packet duplication and forward error correction (FEC) are used to overcome adverse WAN conditions such as poor or noisy links, including wireless WAN LTE/5G. 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. Per-packet load balancing and delivery is provided by combining two overlay tunnels to maximize network capacity if an application requires greater bandwidth.

Automatic failover. If the primary link goes down, the other link will be switched to in sub-seconds (including LTE/5G wireless WAN options). This automation is built into the FortiGate, reducing complexity for end-users while improving their experience and productivity.

FortiGate NGFW security

Fortinet Secure SD-WAN delivers enterprise-class security and branch networking capabilities in one solution. FortiGate NGFWs are updated in near real time by FortiGuard Security Services, protecting customers from the evolving threat landscape by leveraging the most effective artificial intelligence and machine learning systems. These systems gather and analyze over 100 billion security events every day.



Critical security features include:

SSL/TLS inspection and threat protection provides visibility and prevention against malware that obviates the need for separate encryption inspection appliances.

Web filtering enforces internet security, eliminating the need for a separate secure web gateway device.

Complete threat protection includes sandboxing, anti-malware, and intrusion prevention system (IPS).

Virtual private network (VPN) tunnels with high throughput ensure that traffic is always encrypted and stays confidential.

Simplified management and overlay control

As enterprises adopt SD-WAN and LTE/5G, they need the right tools to seamlessly deploy and manage it across widely distributed infrastructures with wired and wireless connections. Fortinet Secure SD-WAN can be administered through FortiManager, an intuitive, unified management console. It includes options for a cloud-based or hosted solution for remote control and orchestration across thousands of locations.

Fortinet enables customers to focus on digital acceleration and increase network agility. In addition, the deployment of an LTE/5G gateway is simplified and accelerated with single centralized management, resulting in reduced operational cost and significantly reduced support tickets.

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. Rich SD-WAN analytics help customers fine-tune their business and security policies to improve QoE for all users.

Top Use Cases

Our scalable and flexible SD-WAN and LTE/5G solution is ideal for the following locations:

Home office. Offered as a desktop appliance, remote workers can implement SD-WAN with embedded wireless WAN solution to ensure their applications will work without fail for business-critical activities such as customer video demonstrations.

The critical advantage of extending SD-WAN functionality to individual teleworkers, especially “super users,” is that they can count on access, as well as dynamically scalable performance, regardless of their local network availability.

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

Distributed cloud. For applications across clouds, we offer the most comprehensive technology building blocks for interconnecting multiple clouds to enable a better user experience. Fortinet Secure SD-WAN is available for every cloud provider and enables the industry's highest IPsec throughput at 20 Gbps to interconnect clouds.

Only Fortinet Security-Driven Networking Solves Today's SD-WAN Challenges

Fortinet Secure SD-WAN integrates enhanced SD-WAN features with proven security capabilities, as well as tight integration with wireless WAN. This convergence of enterprise-class security and networking, known as Security-Driven Networking—part of the Fortinet Security Fabric—fully enables the deployment of an authentic cybersecurity mesh platform architecture. Its innovative approach empowers CIOs to deploy, integrate, and secure the modern technologies required for digital acceleration. Security-Driven Networking improves branch efficiency without compromising protection. It also enables organizations to build a zero-trust edge architecture. Further, to help implement network changes that ensure business continuity with limited IT staff and infrastructure resources, Fortinet's broad product portfolio offers flexible business policies from a centralized fabric management center console.



Summary

There is a wide variety of SD-WAN solutions on the market today with varying capabilities and effectiveness. Security leaders should carefully evaluate their options to ensure the best fit for their needs. Fortinet offers a unique solution for many reasons noted above, arguably the most important differentiator being built-in, high-performance security.

With near 35,000 customer deployments, Fortinet leads the market with Secure SD-WAN innovation. Fortinet is recognized as a Leader in both the 2021 Gartner® Magic Quadrant™ for WAN Edge Infrastructure and the 2021 Gartner® Magic Quadrant™ for Network Firewalls. We also consistently receive accolades from other top industry analysts including IDC and Frost & Sullivan.

Gartner is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

¹ ["Fortinet Receives Frost & Sullivan's 2021 Global SD-WAN Vendor Product Leadership Award,"](#) Frost & Sullivan, December 9, 2021.

² ["Google Transparency Report,"](#) Google, accessed January 12, 2022.



www.fortinet.com