SOLUTION BRIEF

Simplifying SD-WAN Operations in Operational Technology Environments for Reliable Connectivity

Executive Summary

Software-defined wide-area networking (SD-WAN) is starting to replace traditional WAN in remote operational technology (OT) sites. While SD-WAN offers connection reliability benefits that support new digital innovations, few SD-WAN solutions offer consolidated networking and security features optimized for harsh environments. Companies looking to provision SD-WAN to remote factories, substations, or oil rigs have had to cobble together separate point products. Asset operators need a simplified approach to contain costs, improve efficiency, and reduce risks. Fortinet FortiGate Rugged Secure SD-WAN delivers just this, combining next-generation firewalls (NGFWs) hardened for harsh environments with integrated solutions for management and analytics. This centralizes and simplifies SD-WAN operations.

Supporting Innovation in Distributed Production Sites

Factories, electrical substations, and oil rigs are adopting digital innovations—such as Software-as-a-Service (SaaS) applications and real-time applications such as voice and video—to increase productivity, improve communications, and foster rapid business growth. However, traditional WAN architectures at many remote locations struggle to support the traffic demands of these new technologies at reasonable costs. This has led to increasing adoption of SD-WAN architectures that utilize more affordable direct internet connections. The SD-WAN market has grown at a CAGR of 110% from $841M in 2018 to $1.77B in 2019.[1]

But while SD-WAN improves connectivity reliability, it can also increase the organization's risk exposure. According to Gartner survey analysis, "Customers continue to strive for better WAN performance and visibility, but security now tops their priorities when it comes to the challenges with their WAN.[2]

In many organizations, the need for SD-WAN security has led network engineering and operations leaders to incorporate many different tools and point products to address individual functions, threat exposures, or compliance requirements. But this approach leads to infrastructure complexity, which increases manageability burdens while creating new defensive gaps at the network edge.

Fortinet Enables SD-WAN for OT with Fully Integrated Appliance and Fabric Management Center

- Next-generation firewall (NGFW)
- SD-WAN functionality
- Rugged design for temperature, vibration, and EMI
- Zero-touch deployment
- Centralized management
- Reporting and analytics
- Compliance reporting
- Integration and automation

Gartner notes that "72% of the respondents said that security was their topmost concern when it comes to their WAN."[3]

Gartner

Fortinet Simplifies and Secures SD-WAN Deployments

Consolidation of the networking and security tools required for a security-driven SD-WAN solution eliminates the complexity of deploying across many remote, non-environmentally controlled sites. This not only reduces the organization's attack surface while enabling digital innovation initiatives but it also simplifies operations for networking teams.

As an integrated part of Fabric Management Center, FortiGate Rugged Secure SD-WAN can leverage a single-pane-of-glass console with SD-WAN Orchestrator offered as part of FortiManager and provide enhanced analytics and improved reporting with FortiAnalyzer. This allows customers to significantly simplify centralized deployment, enable automation to save time, and offer business-centric policies.

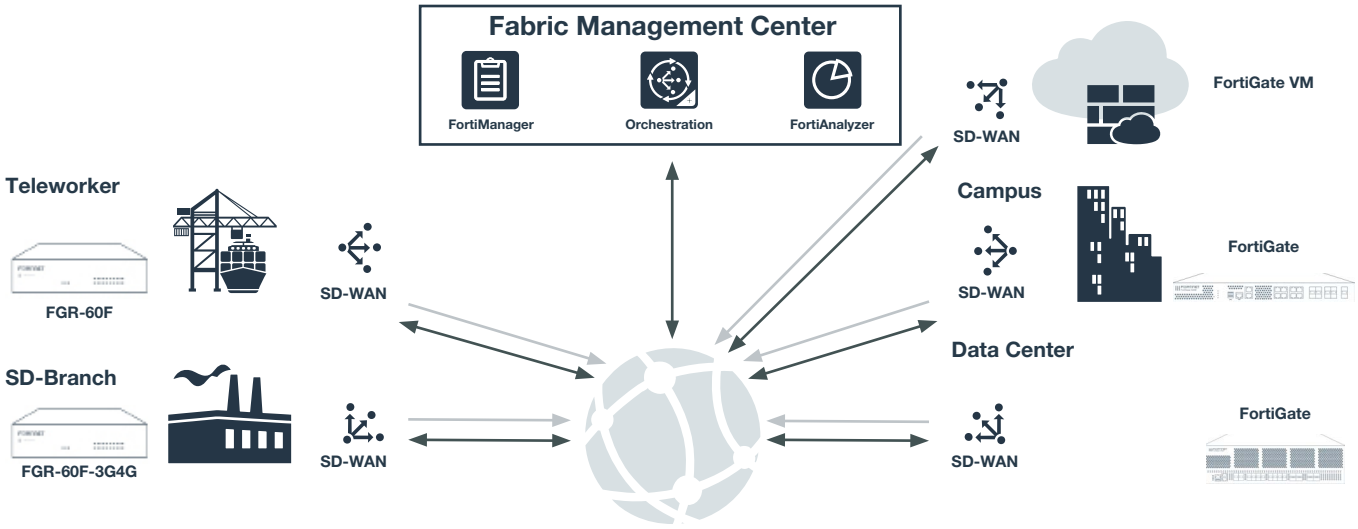


Figure 1: Rugged FortiGate firewalls enable SD-WAN operations with single-pane-of-glass management.

Zero-touch deployment

Organizations implementing FortiGate Rugged Secure SD-WAN can leverage Fabric Management Center to accelerate deployment, reducing the time it takes from days down to minutes. Fabric Management Center zero-touch deployment capabilities enable FortiGate devices to be plugged in at a remote location and then automatically configured by FortiManager at the main office via broadband connection, thereby avoiding time and cost of truck rolls. Fortinet's approach can also leverage an existing SD-WAN configuration as a template to accelerate deployment of new branches and remote sites at scale.

NSS Labs testing shows that FortiGate Rugged Secure SD-WAN can bring a branch online in less than six minutes as a result of its zero-touch deployment capabilities.[4]

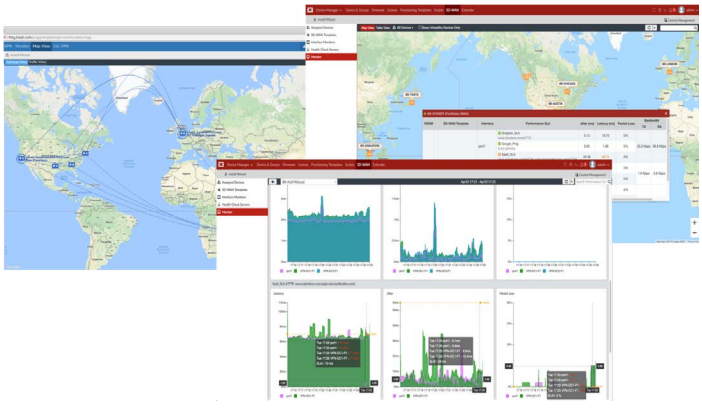
Centralized management for distributed organizations

Centralized management of all distributed networks across the organization helps network leaders drastically reduce the opportunities for configuration errors that lead to cyber-risk exposures and network outages.

Secure SD-WAN Orchestrator is part of its Fabric Management Center. This allows customers to significantly simplify centralized deployment, enable automation to save time, and offer business-centric policies. Fortinet management tools can support much larger deployments than competing solutions—up to 100,000 FortiGate devices. Features such as SD-WAN and NGFW templating, enterprise-grade configuration management, and role-based access controls help network engineering and operations leaders easily mitigate human errors.

SD-WAN reporting and analytics

Enhanced analytics for WAN link availability, performance service-level agreement (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; **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.

Compliance reporting

Customers need reports and tools for customization to help prove compliance to their auditors. However, compliance management has traditionally been a costly, labor-intensive process for networking teams—often requiring multiple full-time staff and months of work to aggregate and normalize data from multiple point security products.

Fortinet accelerates the compliance reporting process by simplifying security infrastructure and eliminating the need for many manual processes. Fabric Management Center includes **customizable regulatory templates** as well as **canned reports** for standards such as Security Activity Report (SAR), Center for Internet Security (CIS), and National Institute of Standards and Technology (NIST). Fabric Management Center also provides **audit logging** and **role-based access control (RBAC)** to ensure that employees can only access the information they need to perform their jobs.

As an extension of Fabric Management Center capabilities, the **FortiGuard Security Rating Service** runs audit checks to help security and networking teams identify critical vulnerabilities and configuration weaknesses in their Security Fabric setup, and implement best-practice recommendations. As part of the service, network leaders can compare their organization's security posture score against those of other industry peers.[5]

Integration and automation

To be effective, security must become seamlessly integrated across every part of the distributed organization—every remote office location. Network engineering and operations leaders need full visibility of the entire attack surface from a single location. Then, they need automated responses to reduce the window of time from detection to remediation and to alleviate the burdens of manual tasks from their staff.

Compliance is not security. The most cyber-resilient organizations are those that treat compliance as a baseline.[6]

Fabric Management Center helps decrease threat remediation time from months to minutes by coordinating **policy-based automated response actions** across the Fortinet Security Fabric, an integrated security architecture that unlocks security workflows and threat-intelligence automation. A detected incident alert sent with contextual awareness data from one location allows a network administrator to quickly determine a course of action to protect the entire enterprise against a potential coordinated attack. Certain events can also trigger automatic changes to device configurations to close the loop on attack mitigation in an instant.

FortiAnalyzer and Fabric Management Center also automate many required SD-WAN tasks to help network leaders reduce the burden on their staff resources. Both products **integrate with third-party tools**, such as security information and event management (SIEM), IT service management (ITSM), and DevOps (e.g., Ansible, Terraform), to preserve existing workflows and preserve previous investments in other security and networking tools.

Delivering Value, Simplicity, and Security

Fabric Management Center delivers enterprise-class security and branch networking capabilities with industry-leading benefits:

Lowers TCO. Fortinet's integrated approach to security-driven SD-WAN improves total cost of ownership (TCO) by consolidating the number of networking and security tools required via capital expenditure (CapEx), while also reducing operating expenses (OpEx) through simplified management and workflow automation. The move to public broadband means that expensive multiprotocol label switching (MPLS) connections can be replaced with more cost-effective options. Here, FortiGate Rugged Secure SD-WAN delivers the industry's best TCO—10x better than the competition.[7]

Improves efficiency. Simultaneously, Fortinet institutes a simplified infrastructure for SD-WAN that reduces operational complexity both at the branch and across the entire distributed organization. FortiGate Rugged Secure SD-WAN can be administered through a single, intuitive management console. 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. The flexibility of single-pane-of-glass management includes scalable remote security and network control via the cloud for all branches and locations.

The average cost of a data breach ($3.92 million) is increased by system complexity (+$290,000). Use of threat-intelligence sharing (-$240,000) and security analytics (-$200,000) both decrease that cost.[8]

Contains risks. Fortinet's tracking and reporting features help organizations ensure compliance with privacy laws, security standards, and industry regulations while reducing risks associated with fines and legal costs in the event of a breach. FortiAnalyzer tracks real-time threat activity, facilitates risk assessment, detects potential issues, and helps mitigate problems. Its close integration with FortiGate Rugged Secure SD-WAN allows it to monitor firewall policies and help automate compliance audits across distributed business infrastructures.

Fortinet Realizes Security-driven SD-WAN

While there are many use cases for security-driven SD-WAN, Fortinet's approach enables this in the most effective way for all types of SD-WAN projects. Simplifying SD-WAN operations is core to making its implementation and expansion successful in support of digital innovation initiatives. FortiGate Rugged Secure SD-WAN with Fabric Management Center offers best-of-breed SD-WAN management and analytics capabilities that help network leaders reduce operational costs and risks at the network edge.

[1] "Market Share: Enterprise Network Equipment by Market Segment, Worldwide, 4Q19 and 2019, Table 16.1, Gartner, March 2020.

[2] "Fortinet Recognized as a 2020 Gartner Peer Insights Customers' Choice for WAN Edge Infrastructure," Fortinet, March 26, 2020..

[3] "Fortinet Secure SD-WAN: Best-of-Breed NGFW and SD-WAN in a Single Offering," Gartner, November 2018.

[4] Ahmed Basheer, "Software-Defined Wide Area Network Test Report: Fortinet FortiGate 61E," NSS Labs, June 19, 2019.

[5] "Proactive, Actionable Risk Management with the Fortinet Security Rating Service," Fortinet, July 8, 2020.

[6] Frances Dewing, "Compliance Is Not Security: Why You Need Cybersecurity Chops In The Boardroom," Forbes, August 15, 2019.

[7] "Fortinet Placed Highest in Ability to Execute in the Challengers Quadrant of the 2019 Gartner Magic Quadrant for WAN Edge Infrastructure," Fortinet, December 4, 2019.

[8] "2019 Cost of a Data Breach Report," Ponemon Institute and IBM, July 23, 2019.

FORTINET

www.fortinet.com

November 11, 2020 5:18 AM

476710-B-1-EN