SOLUTION BRIEF

Simplifying SD-WAN Operations with Single-pane Management

Executive Summary

Software-defined wide-area networking (SD-WAN) is rapidly replacing traditional WAN for remote office and branch deployments. While SD-WAN offers performance benefits that support new digital innovations, many SD-WAN solutions lack consolidated networking and security features. In response, many network leaders have had to add a complex assortment of tools and solutions to manage and protect their SD-WAN deployments. Instead, they need a simplified approach to contain costs, improve efficiency, and reduce risks. FortiGate Secure SD-WAN addresses each of these requirements, combining next-generation firewalls (NGFWs) with integrated solutions for management and analytics to centralize and simplify SD-WAN operations.

Fortinet Simplifies SD-WAN Operations (FortiGate, FortiManager, FortiAnalyzer)

- Zero-touch deployment
- Centralized management
- Reporting and analytics
- Compliance reporting
- Integration and automation

Supporting Innovation While Securing Growing Businesses

Distributed enterprises are adopting digital innovations—such as Software-as-a-Service (SaaS) applications and IP-based tools for voice and video—to increase productivity, improve communications, and foster rapid business growth. However, traditional WAN architectures at many branch and remote office locations struggle to support the traffic demands of these new technologies. This has led to increasing adoption of SD-WAN architectures that utilize more affordable direct internet connections. The global SD-WAN market is projected to grow at over 40% compound annual growth rate (CAGR) to reach $4.5 billion by 2022.[1]

But while SD-WAN improves networking bandwidth, 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]

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

Gartner

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 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 disaggregated branch infrastructure. 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 the Fortinet Security Fabric, **FortiGate Secure SD-WAN** can leverage the capabilities of **FortiManager** and **FortiAnalyzer** (appliances or VMs) to help simplify SD-WAN operations in several critical areas.

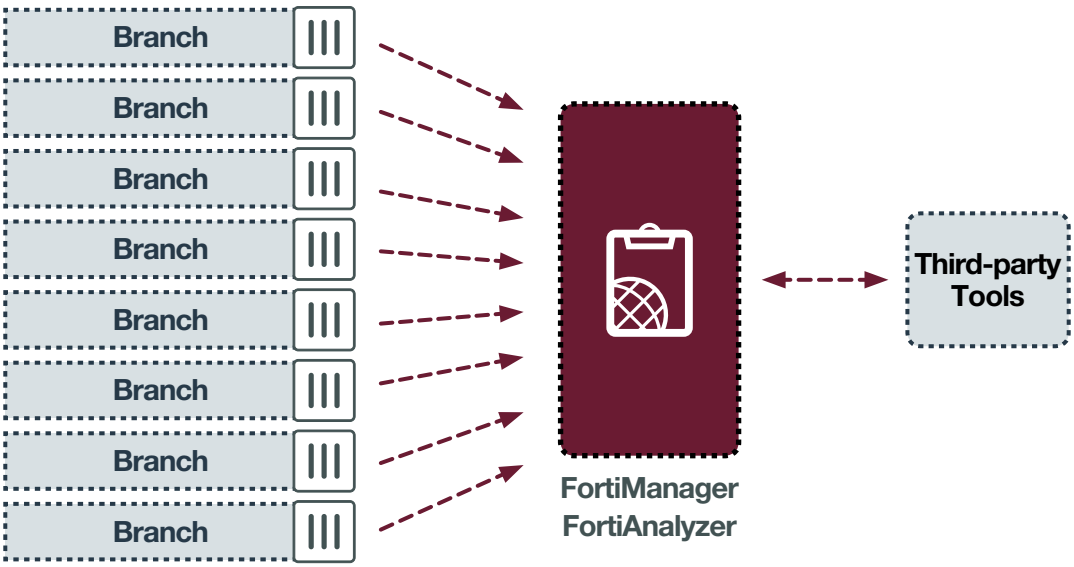

Figure 1: SD-WAN use case featuring FortiGate NGFWs, FortiManager, and FortiAnalyzer.

Zero-touch deployment

Organizations implementing Secure SD-WAN can leverage FortiManager to accelerate deployment, reducing the time it takes from days down to minutes. FortiManager zero-touch deployment capabilities enable FortiGate devices to be plugged in at a branch 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 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

More than half (52%) of all breaches are caused by human errors or system glitches (as opposed to malicious or criminal attacks).[5] 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.

FortiManager and FortiAnalyzer utilize a **single pane of glass** for centrally managing distributed enterprises at scale. 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

As the number of branches grows within an organization and the network-edge attack surface grows, the more network leaders need to rely on real-time analytics to instantly measure and identify network and security risks. FortiAnalyzer offers comprehensive readings that include network traffic, applications, and overall network health.

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.

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. FortiAnalyzer includes **customizable regulatory templates** as well as **canned reports** for standards such as Payment Card Industry Data Security Standard (PCI DSS), Security Activity Report (SAR), Center for Internet Security (CIS), and National Institute of Standards and Technology (NIST). FortiAnalyzer 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 FortiAnalyzer 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.[6]

Compliance is not security. The most cyber-resilient organizations are those that treat compliance as a baseline.[7]

Integration and automation

To be effective, security must become seamlessly integrated across every part of the distributed organization—every branch and 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.

FortiManager 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 branch 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 FortiManager 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 events management (SIEM), IT service management (ITSM), DevOps (e.g., Ansible, Terraform), to preserve existing workflows and preserve previous investments in other security and networking tools.

Delivering Value, Simplicity, and Security

The combination of FortiGate Secure SD-WAN, FortiManager, and FortiAnalyzer 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 Secure SD-WAN delivers the industry's best TCO—10x better than the competition.[8]

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 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.

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 Secure SD-WAN allows it to monitor firewall policies and help automate compliance audits across distributed business infrastructures.

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.[9]

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 Secure SD-WAN, FortiManager, and FortiAnalyzer offer best-of-breed SD-WAN management and analytics capabilities that help network leaders reduce operational costs and risks at the network edge.

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

[2] Naresh Singh, "Survey Analysis: Address Security and Digital Concerns to Maintain Rapid SD-WAN Growth," Gartner, November 12, 2018.

[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] "2018 Cost of a Data Breach Study," Ponemon Institute, July 2018.

[6] "Proactive, Actionable Risk Management with the Fortinet Security Rating Service," Fortinet, April 5, 2019.

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

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

[9] "2019 Cost of a Data Breach Report," Ponemon Institute and IBM, July 2019.

FORTINET

www.fortinet.com

September26,201911:22AM

476710-0-0-EN