FORTINET

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. Fortinet 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.

Supporting Innovation While Securing Growing Businesses

Distributed enterprises 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 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 SD-WAN market is expected to grow to over $30 billion in 2030, from $3.5 billion in 2022, with a CAGR of 31.2% from 2022 to 2030.[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]

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

Consolidating networking and security tools requires a secure SD-WAN solution that eliminates the complexity of disaggregated branch infrastructures. This not only reduces the organization's attack surface while enabling digital innovation initiatives, but it also simplifies operations for networking teams.

Fortinet simplifies SD-WAN operations with network operations center solutions

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

Fortinet named a Leader for the third year in a row and highest in Ability to Execute for the second year in a row in the 2022 Gartner® Magic Quadrant™ for SD-WAN.[3]

Gartner.

Fortinet enables the convergence of networking and security to simplify network operations, ensuring a secure and optimized user experience across all network edges with the hybrid mesh firewall (HMF). Hybrid mesh firewall is a new concept bringing all firewall deployments together in an integrated mesh to manage, monitor, and secure all firewall deployments. It unifies network management and security policies for all firewall deployments, whether on-premises for branch, campus, and data center deployments or virtual firewalls for cloud and cloud-native environments. It also uses artificial intelligence and machine learning to provide advanced threat protection. FortiManager is the foundation of HMF, offering unified, centralized management of all FortiGate deployments.

Fortinet Secure SD-WAN can leverage a single-pane-of-glass console with an SD-WAN orchestrator offered as part of FortiManager and provide enhanced analytics and improved reporting with FortiAnalyzer. This allows organizations to significantly simplify centralized deployment, enable automation to save time, and offer business-centric policies.

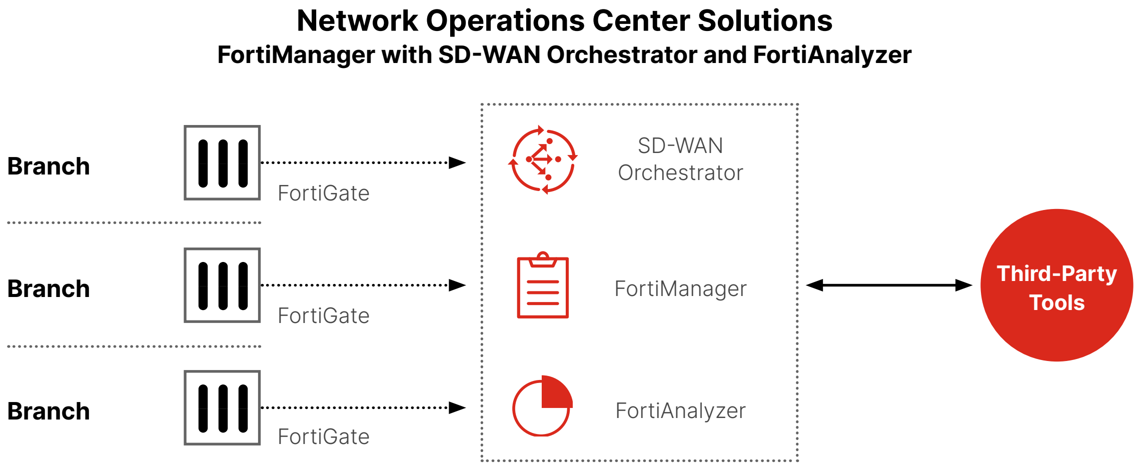


Figure 1: SD-WAN use case featuring network operations center solutions

Zero-touch deployment

Organizations implementing Fortinet Secure SD-WAN can leverage FortiManager to accelerate deployment, reducing the time from days 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 a broadband connection, thereby avoiding the time and cost of truck rolls. Fortinet's approach can also leverage an existing SD-WAN configuration as a template to accelerate the deployment of new branches and remote sites at scale.

Centralized management for distributed organizations

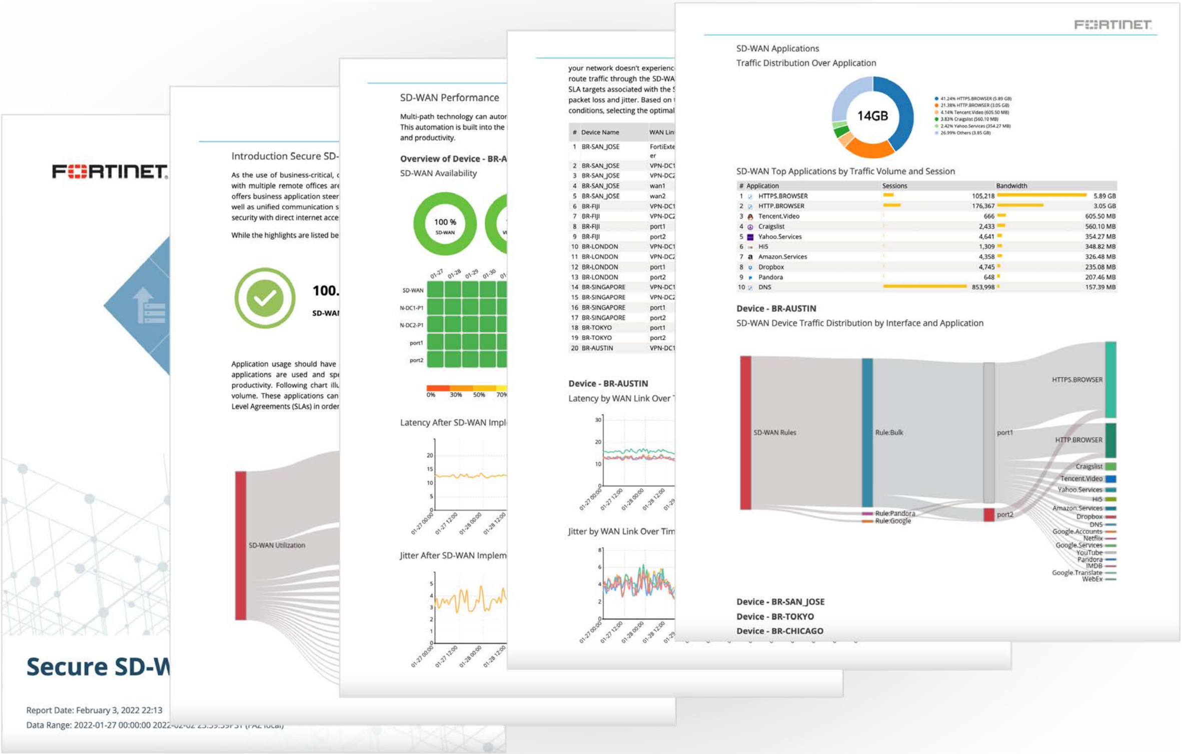
Centralized management through the FortiManager of all distributed networks across the organization helps network leaders drastically reduce the opportunities for configuration errors that lead to cyber-risk exposures and network outages.

Secure SD-WAN orchestrator is part of the FortiManager. 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 quickly mitigate human errors.

SD-WAN reporting and analytics

Enhanced analytics for WAN link availability, performance service-level agreements (SLAs) and application traffic in runtime, and historical stats allow the infrastructure team to troubleshoot and quickly resolve network issues. FortiManager, integrated with FortiAnalyzer, 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.

These features include SD-WAN bandwidth monitoring reports and datasets, SLAs 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, event logging, and archiving around SLAs across applications and interfaces.



SD-WAN Applications

Traffic Distribution Over Application

14GB
41.24% HTTPS.BROWSER (5.89 GB)
21.38% HTTP.BROWSER (3.05 GB)
4.14% Tencent.Video (605.50 MB)
3.83% Craigslist (560.10 MB)
2.42% Yahoo.Services (354.27 MB)
26.99% Others (3.85 GB)

SD-WAN Top Applications by Traffic Volume and Session

#	Application	Sessions	Bandwidth
1	HTTPS.BROWSER	105,218	5.89 GB
2	HTTP.BROWSER	176,367	3.05 GB
3	Tencent.Video	666	605.50 MB
4	Craigslist	2,433	560.10 MB
5	Yahoo.Services	4,641	354.27 MB
6	Hi5	1,309	348.82 MB
7	Amazon.Services	4,358	326.48 MB
8	Dropbox	4,745	235.08 MB
9	Pandora	648	207.46 MB
10	DNS	853,998	157.39 MB

Device - BR-AUSTIN

SD-WAN Device Traffic Distribution by Interface and Application

Device - BR-SAN_JOSE

Device - BR-TOKYO

Device - BR-CHICAGO

Secure SD-W
Report Date: February 3, 2022 22:13
Data Range: 2022-01-27 00:00:00
SD-WAN Performance
SD-WAN Utilization

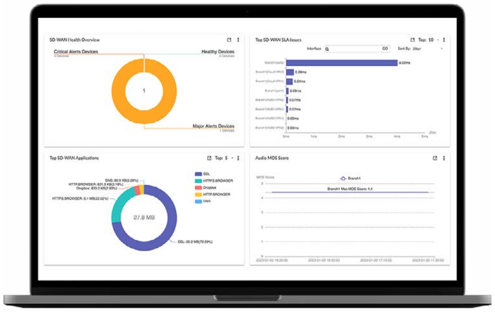
Figure 2: Detailed and highly configurable SD-WAN reports save the IT team valuable time

Compliance reporting

Organizations 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 compliance reporting by simplifying security infrastructure and eliminating the need for many manual processes. FortiManager and FortiAnalyzer include 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). They also provide 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 FortiManager and 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.[5]



Security Compliance: Hurdle Or Critical Growth Strategy?[4]

Integration and automation

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

FortiManager and FortiAnalyzer help 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 instantly close the loop on attack mitigation.

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 event management (SIEM), IT service management (ITSM), and DevOps (for example, Ansible, Terraform), to preserve existing workflows and previous investments in other security and networking tools.

Delivering Value, Simplicity, and Security

FortiManager and FortiAnalyzer deliver enterprise-class security and branch networking capabilities with industry-leading benefits:

Increases ROI: Fortinet's integrated approach to secure SD-WAN improves return on investment (ROI) 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 expensive multiprotocol label switching (MPLS) connections can be replaced with more cost-effective options. Here, Fortinet Secure SD-WAN delivers 300% ROI over three years, eight months payback, a 65% reduction in the number of network disruptions, and a 50% increase in the productivity of security and network teams.[6]

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

The average total cost of a data breach ($4.35 million) in 2022, a 2.6% increase from last year.[7]

Fortinet Realizes Secure SD-WAN

There are many use cases for secure SD-WAN, and Fortinet's unique approach enables them in the most effective way for all types of SD-WAN projects. Simplifying SD-WAN operations is core to successful implementation and expansion in support of digital innovation initiatives. Fortinet Secure SD-WAN with FortiManager and FortiAnalyzer offers 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 Market," Prescient & Strategic Intelligence, Dec. 2022.

[2] "Fortinet Named a 2023 Gartner® Peer Insights™ Customers' Choice for SD-WAN for the Fourth Year in a Row," Fortinet, March 23, 2023.

[3] "2022 Gartner® Magic Quadrant™ for SD-WAN," Gartner, September 2022.

[4] Meiran Galis, "Security Compliance: Hurdle or Critical Growth Strategy," Forbes, June 13, 2023.

[5] "FortiGuard Security Rating Service," Fortinet, accessed July 20, 2023.

[6] "The Total Economic Impact™ Of Fortinet Secure SD-WAN," Forrester, Dec. 2022.

[7] "Cost of a Data Breach Report 2022," Ponemon Institute and IBM, July 2022.

FORTINET

www.fortinet.com

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 organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

July 21, 2023 3:10 PM

2263219-0-0-EN