SOLUTION BRIEF

Automate Network Management for the Fortinet Security Fabric

Executive Summary

The rapid embrace of digital innovation has made networks and network security much more complex—and vulnerable. While malicious cyberattacks remain a serious problem, 48% of all breaches last year came from benign sources that could have been prevented.[1] Moreover, 75% of network outages and performance issues are the result of misconfiguration error.[2] In this regard, a network security strategy that prioritizes network automation can help reduce one of the leading causes of cyber risk and downtime—human error and misconfigurations.

As a key part of the Security Fabric, the Fortinet Fabric Management Center (made up of FortiManager and FortiAnalyzer) simplifies operations by addressing this core challenge of network infrastructure teams across small, medium, or large enterprises.

Key Use Cases for the Fortinet Fabric Management Center

- Centralized management
- Network automation and orchestration
- Security Fabric analytics

Complexity of Network Operations

The challenges of increasingly complex and naturally fragmented infrastructures continue to enable a rise in cyber events and network outages. Too many point products deployed by most enterprises almost always operate in isolated silos with their own management consoles and automation frameworks that are narrow and only relevant for that one product. Subsequently, network operations teams rarely have clear and consistent insight into what controls and configurations are set up across the infrastructure. Even more importantly, they lack comprehensive visibility into the network to detect anomalies.

An integrated network security architecture with network automation capabilities can easily eliminate the complexity challenge for network operators. The Fortinet Fabric Management Center includes FortiManager combined with FortiAnalyzer to address three key use cases for effective network operations:

- Centralized management
- Network automation and orchestration
- Security Fabric analytics

Centralized Management

When it comes to network security, disparate products typically cannot share threat intelligence or coordinate responses across organizational infrastructure. This critical cybersecurity shortcoming is often compounded by a lack of skilled security personnel to manage a wide assortment of disconnected point products. But even large organizations with dedicated IT security staff still have difficulty monitoring the network to keep track of which devices are connected, who has access to the network, and which resources are needed by which applications and workflows.

A centralized management solution with a single-pane-of-glass view like the Fabric Management Center enables streamlined visibility that reduces complexity. It allows network operations teams to monitor data movement and identify anomalous activity, simplifies solution optimization, and centralizes the management of next-generation firewalls (NGFWs) and other security tools from a single location. It also streamlines operations for limited or under-resourced administrators and staff—requiring fewer man-hours while reducing total cost of ownership (TCO).

Figure 1: Fortinet Fabric Management Center.

Broad device management:

- Supports central management with a single console across NGFW, software-defined wired-area network (SD-WAN), software-defined branch (SD-Branch), and other use cases
- Scales to support management of 100,000-plus Fortinet devices

Enterprise configuration and change management:

- Supports geographically dispersed high availability with up to five units
- Enables creation of administrative domains for better segregation of networks

Visibility:

- Delivers advanced reporting and dashboards for operations and security
- Provides tools to enable scheduling of reports

Network Automation and Orchestration

Automation and orchestration are increasingly implemented, especially in enterprises that have complex infrastructures. These businesses are looking for ways to consolidate configuration and change management for security across complex, hybrid networks—and most importantly, across use cases like NGFW, SD-WAN, and many others.

Operations teams need to actively monitor for anomalies as enterprises increasingly embrace remote work. They also must identify irregularities with virtual private network (VPN) access in real time. This cannot be cohesively achieved if the tools in place are not integrated and automated. The Fabric Management Center enables automation and orchestration across complex infrastructures via connectors, automation hooks, and real-time alerts for any network abnormalities.

Figure 2: Fabric Management Center automation and orchestration dashboard.

Deployment and maintenance:

- Provides an application programming interface (API) that enables anyone to manage Fortinet deployments and integrate with external provisioning, monitoring, inventory, and change-management systems
- Includes command-line interface (CLI) support via sample scripts

Network integrations:

- Fortinet Fabric Connectors provide integration to manage policies in a single console across multiple software-defined network (SDN), cloud, and partner technology platforms
- Includes a Fortinet distribution service to act as the upgrade and threat-intelligence gateway for all deployed Fortinet devices

Workflow and orchestration:

- Enables fast and automated responses with FortiOS Automation Stitches—a simple way to define actions on triggers
- Provides interoperability with existing management and analytics tools

Security Fabric Analytics

Real-time network visibility is not easy—especially as enterprises add on an increasing number of point products to already complex infrastructures. As network teams consolidate point products and leverage FortiOS for intrusion prevention (IPS), VPN, NGFW, SD-WAN, SD-Branch, and other functions, they can easily share telemetry data between all deployments and enable real-time visibility of anomalies.

The Fabric Management Center's FortiAnalyzer solution enables organizations to apply FortiGuard Labs threat intelligence to identify problems in real time. FortiAnalyzer helps correlate threat intelligence across the Security Fabric, leveraging its built-in analytics engine. It applies risk scoring to prioritize anomalies and shares findings across the infrastructure. These core analytics capabilities are managed via FortiManager's unified console view.

Additionally, the analytics engine powers visualization of the Security Fabric in real time. These visualizations enable operations teams to identify and investigate any network risks in real time. FortiAnalyzer also comes with built-in dashboards and reports that can easily be customized. These functions include over 700 datasets for easy onboarding—advanced queries that are optimized for real-time responses.

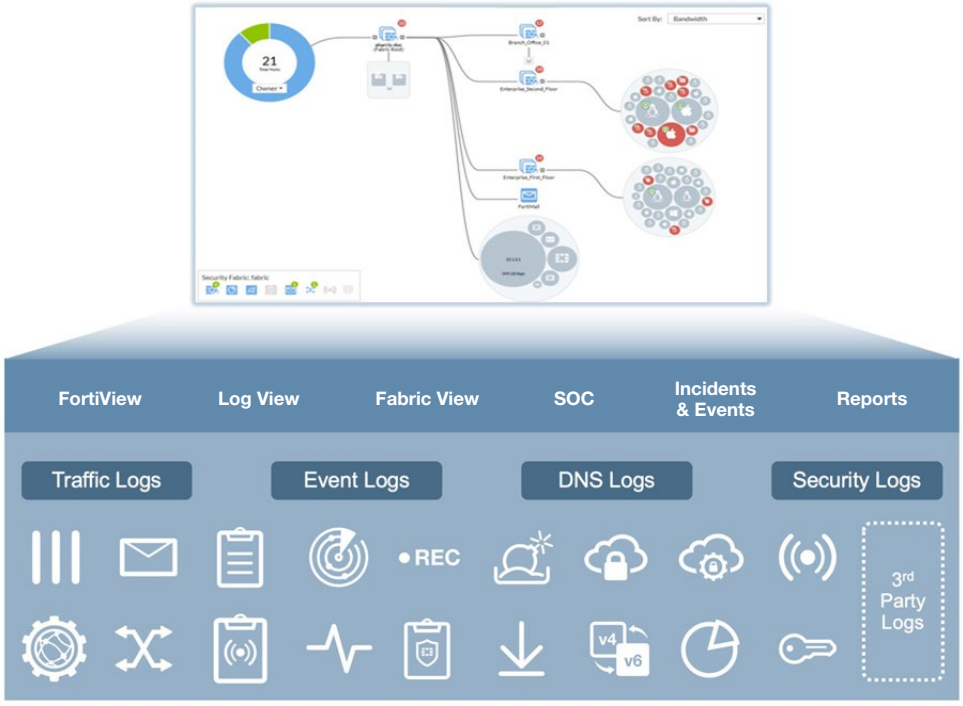

Figure 3: Fabric Management Center analytics view.

Advanced reporting:

- Supports security standards such as National Institute of Standards and Technology (NIST) and Center for Internet Security (CIS)
- Includes a security rating report based on hundreds of Fortinet security best practices

Role-based visibility:

- Offers targeted dashboards for key enterprise stakeholders, including CIO, CISO, network architect, and security architect
- Includes a security assessment dashboard for security operations (SecOps)

Security Fabric back end:

- Integrates into the FortiOS operating system, and can be leveraged for topology and other views
- Uses automation hooks in FortiAnalyzer and orchestrates responses in FortiOS

Elevating the Total Value of Security Across the Enterprise

The Fortinet Fabric Management Center enables enterprise-class security capabilities while helping network leaders actualize industry-leading benefits:

Improves Efficiency. With its single-pane view, FortiManager helps enterprises simplify oversight of security infrastructure and automate responses to potential problems.

Reduces Risk. The Fortinet 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.

Reduces TCO. As part of the Fortinet Security Fabric architecture, the Fabric Management Center helps lower TCO by consolidating disparate security management functions. FortiAnalyzer delivers the advantages of advanced analytics and automation capabilities without having to add on expensive, third-party point solutions.

[1] "2019 Cost of a Data Breach Report," Ponemon Institute and IBM Security, July 2019.

[2] Jeff Edwards, "Managing Network Configuration Changes: Five Best Practices," WhatsUp Gold, July 19, 2018.

May 11, 2020 10:33 PM

D:\Fortinet\Solution Briefs\grey solution briefs\BOFA Asset\sb-FA-automate-network-management-for-the-fortinet-security-fabric-5112020

666918-0-0-EN