SOLUTION BRIEF

Supercharge Your Network: Unleash Network Management Automation

Executive Summary

The rapid adoption of digital transformation pushes business networks to adopt a hybrid strategy. As a result, the network infrastructure is getting more distributed, making it hard to manage and secure. And not surprisingly, among all causes leading to cyber incidents and network downtime, human error and misconfigurations are at the top. A recent Data Breach Investigation Report showed that misconfiguration errors were the most common, representing approximately 15% of breaches. Human error is another dominant trend responsible for 13% of breaches.[1]

Complexity is the primary culprit here, as most IT teams do not have a single source of truth for real-time information on the state of the network and network security. They also need a unified solution to ensure consistent configuration and policy enforcement across the network. Such challenges require a unified network management solution with single-pane-of-glass visibility and process automation for consistency and efficiency.

Gartner survey shows 75% of organizations are pursuing security vendor consolidation in 2022.[2]

Modern-Day Network Operations

Companies are expanding and adopting hybrid and distributed strategies to be close to their customers and suppliers. Subsequently, their networks have spread widely, including hybrid data centers to remote sites. And business data and applications are now being hosted on-premises and in the cloud, making secure access to critical resources from a hybrid workforce increasingly challenging. But to address this rapidly evolving scenario, many businesses now find themselves with too many point products operating in silos, each with its own management console and automation framework. As a result, many network operations teams lack comprehensive visibility into the network to detect anomalies, and they rarely have clear and consistent insight into configurations and controls across the infrastructure.

Hybrid Mesh Firewall with Network Automation and Orchestration

Businesses are looking for ways to consolidate configurations and simplify change management for security across their increasingly complex and hybrid networks and use cases, including next-generation firewalls (NGFWs), SD-WAN, and others. But this cannot be achieved without their solutions being integrated and automated.

A hybrid mesh firewall (HMF) with network automation capabilities is the right approach. It provides a unified security platform that offers coordinated protection across enterprise IT, including the branch, campus, data center, public and private clouds, and remote workers. A hybrid mesh firewall is designed to address the evolving needs of network security, especially in hybrid-cloud environments.

Fortinet's Hybrid Mesh Firewall solution, FortiManager, manages and orchestrates NGFWs in any form factor deployed in any location, all through a single-pane-of-glass console. FortiManager also includes automation capabilities to streamline the management of security policies, firmware revisions, and configurations across complex infrastructures—all done via connectors, automation hooks, and real-time alerts for detected network abnormalities.

Zero-trust provisioning

FortiManager Zero-Touch Provisioning (ZTP) enables the automatic provisioning and configuration of FortiGate devices without manual intervention. FortiManager ZTP achieves this using DHCP options 240 and 241, helping organizations save time and resources by automating repetitive configuration tasks and reducing human errors.

FortiManager ZTP can also expedite troubleshooting at the maintenance stage by checking and ensuring consistent configuration across devices, further reducing the risk of human error.

Administrative domain

Administrative domain (ADOM) is a key FortiManager feature that allows administrators to manage multiple Fortinet devices efficiently. The ADOM feature divides the management of devices into logical groups, making it easier to manage them separately while applying consistent policies.

Administrative domain also allows administrators to manage devices based on their roles in the network. For instance, administrators can create different ADOMs for different departments, each with its own set of policies. Administrative domain can also delegate management tasks, streamline firmware upgrades, and apply policies consistently across multiple devices.

Security policy automation

FortiManager automates security policy enforcement by providing a unified platform for defining and managing security policies across multiple devices and locations. It allows administrators to create and deploy policies to FortiGate firewalls, FortiAnalyzer, and other security devices consistently and efficiently. FortiManager also integrates with ITSM to seamlessly mitigate security incidents and events, apply configuration changes, and update policies. Integration with FortiAnalyzer provides in-depth discovery, analysis, prioritization, and reporting of network security events. It also allows administrators to create and manage policies in policy packages and sync to the FortiGates by installing policy package changes. Organizations can also use FortiManager to automate security policy enforcement by checking their security configuration to ensure it's consistent with their security policy.

> *"FortiManager is easy for us to use. It provides single-pane-of-glass management, which helps ensure that our firewalls have the same configuration everywhere around the world. The Fortinet solutions are well-integrated, which means we have more visibility across the network. And we can push out code to our firewalls from a centralized portal, so we can quickly and easily distribute fixes to remediate any issues."*
>
> **- Jonathan Martin**
> Director, Global IT
> Infrastructure, QIAGEN

Automation enables a hybrid mesh firewall architecture

FortiManager automation is also essential for enhancing the management and operation of an HMF. It allows IT personnel to centrally manage network and security policies for thousands of FortiGate NGFWs, Secure SD-WAN devices, and FortiSwitch, FortiAP, and FortiExtender solutions through its single console management system. This level of automation simplifies management tasks, accelerates responses to potential problems, ensures consistency in security policies, and facilitates integration with external automation tools. They also contribute to improved operational efficiency, enhanced security, and streamlined management of HMF deployments.

Automation through APIs

FortiManager provides an HTTPS API based on the JSON-RPC protocol that can be used for automation and to support DevOps. This API offers complete management and monitoring capabilities, allowing users to automate tasks such as configuring devices, creating backups, and retrieving device information. One specific automation implementation example that can save time and improve recovery is scheduled configuration backup. FortiManager also provides JSON API access permission that can be configured from the administrator's configuration page.

Automation with connectors

FortiManager uses connectors to enable automation by providing integration and orchestration capabilities with the various security and network devices in an organization's environment. The connectors allow FortiManager to communicate with these devices, collect information, and automate configuration and management tasks. For example, by creating FSSO connectors, FortiManager can connect with Fortinet Single Sign-On agents for identity-based access control and policy enforcement.

FortiManager enables automation through these connectors by providing APIs to collect and share network information, query FortiGate NGFWs, and optimize network operations through orchestration. This approach broadens end-to-end visibility and response across the security fabric and provides interoperability with existing management and analytics tools.

Automation stitches

FortiManager also enables automation using automation stitches. Automation stitches are a simple way to define actions on triggers. It automates tasks across the Fortinet Security Fabric by defining triggers and actions and can be configured to run on a schedule, such as daily or weekly. For example, it can block traffic from a specific subnet when a particular event occurs, such as when a WAN link goes down. It can also be used to send alert emails based on event logs. Automation stitches automate security responses so DevOps processes are not obstructed or slowed.

FortiManager provides centralized and unified management for HMFs, ensuring consistent security policies across the hybrid environment. It simplifies configuration and provisioning processes, offers granular control, and integrates with FortiAnalyzer for threat detection and risk assessment.

[1] DBIR (Data Breach Investigations Report), Verizon, 2022.

[2] 2023 Leadership Vision for Security and Risk Management Leaders, Gartner, 2022.

June 14, 2023 1:10 PM

2172906-0-0-EN