FORTINET

Seamless Security Unleashed: Empowering Your Organization with Hybrid Mesh Firewall

Table of Contents

Executive Overview

New business demands, including the need to enhance customer and user experience, have accelerated digital transformation, forcing organizations to adopt new digital technologies. According to Chris DePuy from 650 Group, "The rise of digital transformation and work-from-anywhere has made supporting and securing applications and employees at different locations critical for businesses."[1] The adoption of advanced networking technologies like SD-WAN, SD-Branch, IoT, multi-cloud, and zero-trust network access (ZTNA) has led to complex network infrastructures. Additionally, organizations face a shortage of skilled professionals and increasing compliance requirements.

To address this growing complexity, enterprises are embracing integrated architectures to consolidate solutions and streamline and optimize networks. These architectures offer benefits like zero-touch provisioning, centralized management, real-time security analytics, simplified compliance auditing, and the automation of manual workflows. By adopting integrated solutions such as new hybrid mesh firewalls (HMFs), businesses can mitigate challenges, enhance efficiency, and maintain robust security measures in the digital landscape.

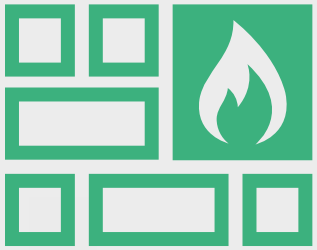
Gartner research shows that 94% of CEOs want to maintain or accelerate pandemic-driven digital transformation.[2]

Hybrid Mesh Firewalls Untangle Complexity Challenges

When it comes to protecting their infrastructures, network engineering and operations leaders face several challenges. First, visibility and control of network defenses are reduced due to an accumulation of isolated point network and security products. Compounding this issue, the continuing worldwide shortage of security talent means that most organizations lack the staff and skills to manage the growing number of individual tools. And because these tools aren't integrated, IT teams must manually correlate data to detect and respond to threats, deploy policies, and compile reports and audits for evolving compliance requirements—increasing the likelihood of human error while putting an escalating burden on already-strained teams.

Embracing an integrated network security infrastructure is the first step toward solving these critical problems. A network security architecture that connects all deployed solutions across the organization provides the foundation for critical capabilities.

An HMF is one such unified security platform. It provides coordinated protection across multiple areas of enterprise IT, including the branch, campus, data center, public and private clouds, and remote workers. To achieve this, HMFs come in various form factors, including appliances, virtual machines, cloud-native firewalls, and Firewall-as-a-Service (FWaaS) that are managed and orchestrated through a central, unified management system.



By 2026, more than 60% of organizations will have more than one type of firewall deployment, which will prompt the adoption of hybrid mesh firewalls.[3]

Simplified Provisioning

An HMF can enable advanced security orchestration capabilities for provisioning and configuration. This alleviates many of the complexity challenges being faced by organizations as they grow while improving operational efficiency and reducing the workflow burdens on limited staff resources. And as your business expands or adds new offices through mergers and acquisitions, automated onboarding capabilities enable fast and seamless security scalability to secure all areas of the network.

But to make this possible, an effective HMF must also support capabilities like zero-touch deployment to simplify and accelerate bringing new locations online. Zero-touch deployment enables a security device—such as a next-generation firewall (NGFW)—to be plugged in at a branch office or remote location and then be automatically configured at the main office via a broadband connection to avoid the time and cost of truck rolls. It should also use existing configurations as a template to accelerate deployment at new branches and remote sites at scale.

Centralized Management

Operations teams need to monitor data movement and identify anomalous activity across the network. But security complexity fragments this function. Siloed devices in a disaggregated security architecture do not communicate with one another or easily share threat intelligence. As a result, network engineering and operations teams must juggle multiple management consoles from different vendors, inhibiting clear, consistent, and timely insight into what is happening across the organization.

An HMF with centralized management capabilities, however, simplifies visibility and control by consolidating the multiple management consoles associated with an architecture made up of isolated point devices. An HMF provides a single-pane-of-glass view that allows IT to track all solutions protecting the network and apply policy-based controls with ease and consistency, even when applications and workflows move between different parts of the network.

But the biggest problem with decentralized solutions is human error, which is the primary culprit behind many cyber events. Stanford University researchers found that approximately 88% of all data breaches are caused by an employee mistake.[4] Centralizing management for the distributed solutions deployed across the organization helps network leaders drastically reduce the configuration errors that lead to security risks and outages.

“More organizations are coming to terms with embedding security in their cloud transformation battle plan. Many are looking to professionals, such as managed cloud security service providers, to get things done right.”[5]

Compliance Reporting

Virtually all compliance regulations require documentation. A strong audit trail that tracks every incident, action, and outcome can prove compliance with regulations. Collecting and compiling such management, however, is very often a heavily manual, labor-intensive process. Depending on the industry and organization, it can require months of work involving multiple full-time staff. This is most likely why 85% of IT compliance and risk management professionals plan to evaluate new tools to streamline and automate their compliance processes.[6]

For organizations with multiple point-security products deployed across their network, data must be assembled from each and then normalized to ensure that regulatory controls are reported accurately. To achieve so, network operations staff must monitor security controls using each individual vendor's audit tools and then normalize and correlate that information to prove compliance. Such complex and unwieldy auditing processes are inefficient and very often ineffective due to human errors and data inconsistencies.

Automating compliance tracking and reporting at the network operations layer can streamline these processes, allowing limited networking and security staff to focus on more critical operations activities. But that requires deploying tools like HMFs designed to operate as a unified system. In addition, an effective security management solution should provide compliance templates for both best practices and regulations to help reduce the cost and burdens of complexity. Specifically, the solution should provide real-time reports on industry regulations, such as the Payment Card Industry Data Security Standard. It should also support security standards, such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework and the Center for Internet Security (CIS) Security Controls.

Effective security management should also include tools to help networking leaders evaluate their environments against industry best practices. Part of this process includes the aggregation and reconciliation of threat data from multiple sources and the application of recommendations to protect against threat exposures.

Worldwide spending on security and risk management is forecast to grow 11.3% in 2023.[7]

Network Automation and Real-Time Security Analytics

As the number of branches within an organization grows and the network-edge attack surface expands, network engineering and operations leaders must increasingly rely on real-time analytics to instantly measure and identify network and security risks. To enable this, an HMF can coordinate data across all deployed parts of the infrastructure and provide comprehensive, real-time reports that combine network traffic, applications, and overall network health.

Features such as enterprise-grade configuration management and role-based access controls can help network operations and engineering leaders easily track changes and mitigate human errors. Hybrid mesh firewalls can also provide service level agreement (SLA) logging and history monitoring, as well as customizable SLA alerting. Additional capabilities include network bandwidth monitoring reports and adaptive response handlers for network events.

“82% of breaches involved the human element. Misconfiguration is responsible for 13% of breaches.”[8]

Cybersecurity Staff Shortages

According to the International Information System Security Certification Consortium (ISC[2]), the size of the global cybersecurity workforce gap in 2022 was around 4.3 million. And despite adding more than 464,000 workers in the past year, the cybersecurity workforce gap has grown more than twice as fast as the workforce.[9] And more than half of those organizations with workforce shortages feel that staff deficits put their organization at a "moderate" or "extreme" risk of cyberattack. It jeopardizes the most foundational functions of their profession, like risk assessment, incident handling, and remediation follow-ups.

The longer it takes to remediate a breach, the more damage and expense to the organization. According to IBM, both the length of time to contain a breach and total cost have increased. And from that same report, it now takes an average of 277 days to identify and contain a breach. And "data breach costs rose from $4.24 million to $4.35 million, the highest average total cost in the 18-year history of the report."[10]

Hybrid mesh firewalls use automation to enhance network protection and compensate for limited staff. By coordinating threat responses, an HMF can streamline processes across the entire organization and reduce the reliance on manual steps that require human intervention, such as alert correlation and research. This automation significantly shortens the time between threat detection and response while also minimizing operational anomalies caused by human errors. In addition, intelligence sharing and automation capabilities have become vital for safeguarding data and operations. With an HMF, this automation extends across the entire network, encompassing both the data center and remote users.

“(ISC)² estimates a worldwide gap of 3.4 million cybersecurity workers. Nearly 70% of respondents feel their organization does not have enough cybersecurity staff to be effective.”[11]

Evolving to Automation-Driven Network Management with HMF

An HMF can help detangle complex challenges and reduce risk around the primary causes of cyber breaches (such as system glitches, misconfigurations, and human errors) through what is sometimes called "automation-driven network management." An HMF can simplify and expand provisioning capabilities, enable single-pane-of-glass management and integrated analytics, deliver advanced compliance reporting tools, and ensure network-aware rapid responses across all parts of the network (on-premises, cloud, and hybrid environments).

The Fortinet Network Operations solution, which includes FortiManager and FortiAnalyzer, provides these capabilities to help support network administrators improve operational efficiency with a centralized and simplified view for overseeing their entire Fortinet Security Fabric infrastructure. When evaluating solutions, all teams should examine how best to invest to improve efficiency, reduce risk, and reduce their total cost of ownership. An HMF that prioritizes network automation capabilities can solve the persistent challenges of infrastructure complexity.

"We could not have managed different devices in every office for intrusion detection system, intrusion prevention system, application control, and load balancing—with everything configured differently. Fortinet provided consistency for our security nationwide and a single pane of glass for management by our central security team."

- Sonu Singh VP, IT, and National Security Officer, Seasons Healthcare Management, Seasons Healthcare Management

[1] Chris DePuy, "Secure Access Service Edge (SASE) Market Surges over 40% Y/Y in 2022; According to 650 Group," 650 Group, March 27, 2023.

[2] Gartner®, "Top Strategic Technology Trends 2023," David Groombridge, October, 2022.

[3] Gartner®, "2022 Gartner® Magic Quadrant™ for Network Firewalls," Rajpreet Kaur, Adam Hils, Thomas Lintemuth, December 19, 2022.

[4] "Psychology of Human Error 2022: Understand the Mistakes That Compromise Your Company's Cybersecurity," Tessian, 2022.

[5] Cathy Huang, "IDC MarketScape: Worldwide Managed Cloud Security Services in the Multicloud Era 2022 Vendor Assessment," 2022.

[6] Jingcong Zhao and Cat Hausler, "2022 IT Compliance Benchmark Report," Hyperproof, 2022.

[7] Gartner®, "Gartner Identifies Three Factors Influencing Growth in Security Spending," Gartner, October 13, 2022.

[8] "2022 Data Breach Investigation Report (DBIR)," Verizon, 2022.

[9] "2022 Cybersecurity Workforce Study: A Resilient Cybersecurity Profession Charts the Path Forward," (ISC)², 2022.

[10] "Cost of a Data Breach Report 2022," IBM, July 2022.

[11] "2022 Cybersecurity Workforce Study: A Resilient Cybersecurity Profession Charts the Path Forward," (ISC)², 2022.

FORTINET

www.fortinet.com

Copyright © 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. 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.

June 22, 2023 11:53 PM

667870-B-0-EN