CHECKLIST

# 10 Considerations for Building a Hybrid Mesh Firewall

## Today's Threats Require a New Approach to Network Security

**Today's attackers, whether individuals, organized crime rings, or even hostile nation-states, are more sophisticated, better organized, and better financed than ever.[1] This can be seen in the growing number of threats, such as advanced persistent attacks, ransomware, and wiper threats—often facilitated by the rise of Crime-as-a-Service (CaaS), new attacks targeting nontraditional devices, and the increase in multifaceted attack strategies. And new concerns are looming, such as the weaponization of artificial intelligence (AI) and the fear that quantum computing will degrade the effectiveness of the encryption tools that are the basis for much of modern cybersecurity.**

However, it's not just the threat landscape that is changing. Broader economic and social trends are leading many organizations to rethink their approaches to network security as part of new digital transformation projects. The Internet of Things (IoT), the rise of hybrid-cloud computing, the vast increase in remote work demands, the distribution of data center and application resources, the convergence of IT and operational technology (OT), and the continued shortage of skilled security professionals are just a few of the realities driving organizations to reassess their security strategies.

One outcome of these changes is the realization that network security tools, especially firewalls, can't work in isolation. Instead, they must work together, forming what is being called a hybrid mesh firewall (HMF).[2] This unified security platform provides coordinated protection to multiple areas of enterprise IT, including corporate sites, such as branches, campuses, data centers, public and private clouds, and remote workers. This, then, can form the core of a broader security framework.

To achieve this, HMFs must be available in a variety of form factors, including chassis, appliances for large and small sites, virtual machines, cloud-native firewalls, and Firewall-as-a-Service (FWaaS). This allows them to be deployed anywhere across the distributed network, scale and adapt as the network evolves, and seamlessly integrate with other technologies to share security context signals and enable automation.

One of the most essential components of an HMF is its ability to traverse today's multi-cloud and hybrid data center environments. Using a unified management console, HMFs can coordinate protection across every IT domain (corporate sites, public and private clouds, and remote workers). This allows enterprise IT to automate its protection capabilities, such as collecting and correlating data, performing AI-assisted deep analysis, and coordinating a unified response across the network without duplicating efforts, re-creating policies, or investing needless manual hours when a cybersecurity skills gap already constrains resources.

The challenge is that building an HMF strategy can be daunting. There are too many options, misleading claims, and incomplete information for many organizations to design, build, and deploy a complete solution without assistance. The following checklist is designed to help security professionals evaluate HMF solutions and the vendors who offer them.

## The Top 10 Considerations for Building a Hybrid Mesh Firewall

### ☑ Assess Your NGFW's Capabilities

An HMF is an integrated collection of next-generation firewalls (NGFWs) deployed across the network and working together as a unified solution. The features of NGFWs typically include inline deep packet inspection, IDS/IPS, application inspection and control, SSL/SSH offloading and inspection, website filtering, QoS/bandwidth management, malware detection, botnet detection, and malware detection. Additionally, most NGFWs offer threat intelligence, mobile device security, data loss prevention (DLP), Active Directory (AD) integration, sandboxing, and an open architecture that allows organizations to tailor application control and integrate with a broad ecosystem of related tools and technologies.

But given today's transition to a highly mobile hybrid workforce, the most advanced NGFWs must also offer zero-trust enforcement, secure SD-WAN functionality, and, most importantly, the innate ability to function as an active component of an HMF infrastructure.

### ☑ Centralized and Unified Management

Integral to any HMF is a well-designed system of central management that efficiently manages a distributed and integrated security architecture through a single-pane-of-glass management console. Ideally, this management tool should include advanced analytics and easily integrate with third-party tools like Ansible (Automation), Terraform (Automation), ServiceNow (ITSM), Splunk (SIEM), Tufin (NSPM), and others across large-scale, multivendor deployments. Other key functionalities should include centralized security content and signatures distribution, SD-WAN overlay orchestration, administrative domains, and cross-firewall automation.

### ☑ Efficacy

A security system is only as good as its ability to detect threats. However, the effectiveness of NGFW solutions is difficult to determine on your own. In this scenario, third-party testing is invaluable. One excellent source for efficacy data is CyberRatings.org, a nonprofit member organization dedicated to providing visibility and transparency on the effectiveness of cybersecurity products and services. While not all firewall vendors have agreed to be tested, those that do—like Fortinet—often offer the report on their website. See the latest report here or scan the QR code.

### ☑ Automation

Network automation is essential to keep up with the speed and sophistication of today's threats. But it is impossible to implement when your various point security tools, including your NGFW deployments, operate in a silo. Automation must combine software and processes to provision, configure, manage, and optimize all physical and virtual devices within your network. With everyday functions automated and repetitive processes streamlined and controlled, network service availability and overall user experience improve.

Network automation can reduce human error, improve efficiency, and ultimately lower costs. Employees can be dynamically authenticated and connected to the network to improve an organization's overall productivity levels. And with zero-touch provisioning, new devices can be configured and made ready for use by employees right out of the box, enabling them to start work faster without downtime.

But network automation isn't enough. An HMF infrastructure must also automate its security functions. Security automation enables the coordination of activities between different firewall mesh components to accelerate detection and decrease response times to security events. Events occurring anywhere across the firewall mesh should be monitored, and action responses should be able to defend any destination.

## ☑ ASIC-Based Appliances

Corporate sites and on-premises hardware should never be the reason for network bottlenecks. But to ensure that devices and users can operate at business speeds, the corporate networks and data centers in your HMF deployment must use appliances designed to scale security functions. This is especially crucial when performing processor-intensive tasks, such as inspecting encrypted data or streaming video, which drives most security appliances to their knees.

Avoiding these bottlenecks requires deploying on-premises appliances enhanced with application-specific integrated circuits, or ASICs. A security appliance containing a custom security or networking ASIC can offload many resource-intensive functions, like firewalling, VPN, IPS, and even SSL or deep packet inspection (DPI). That means your corporate sites are protected with multi-layered security controls without impacting network performance or user experience.

## ☑ Artificial Intelligence, Machine Learning, and Threat Intelligence

Complex networks and an expanding threat landscape require coordinated protection. It's not enough that firewalls span different areas of the network. They must also utilize artificial intelligence and machine learning (AI/ML) capabilities to effectively detect and protect against known and unknown threats.

AI/ML-powered security enables HMFs to identify and classify applications, web URLs, users, devices, malware, and more—all while automating policy enforcement across domains. Artificial intelligence and machine learning are at the heart of HMF automation and can significantly reduce the amount of manual work involved in protecting enterprise IT and OT.

## ☑ Full Range of Form Factors on a Single OS

Modern enterprises require a wide variety of types and sizes of firewalls, ranging from expandable chassis for large data centers and corporate headquarters to midsized appliances for regional offices, smaller appliances for branch offices, and virtual appliances for private and public cloud deployments. Depending on specific use cases, they may also require access to cloud-native firewalls and FWaaS. An HMF must incorporate all of these form factors. This requirement is easier to meet and maintain when every solution runs on the same operating system and can be managed using the same management platform.

## ☑ Flexible Firewall Pricing Options

As business needs change, organizations require the flexibility to deploy a broad range of firewall types without being locked into a single form factor. And they need to be able to move assets from place to place as the network continues to evolve. Flexible pricing models enable organizations to adapt to changing network requirements, pay for what they use, customize their security services, and manage their budgets effectively. These pricing models offer greater flexibility and cost control, which is crucial given network security's dynamic and evolving landscape.

## ☑ Security Fabric

An HMF, however robust, is only part of your broader security infrastructure. Today's security also requires a comprehensive and integrated cybersecurity architecture that provides advanced protection and visibility across the entire network infrastructure. This approach must combine a full range of security solutions, including firewalls, endpoint protection, secure access, and cloud security, into a unified framework and tools that can also enable and support a modern security operations center (SOC). This security fabric enables organizations to detect and respond to threats in real time, automate security policies, centralize configurations, and share threat intelligence across different security components, creating a cohesive and effective defense against cyberattacks.

## ☑ Start with a Partner You Can Trust

Security purchasing decisions are about more than just technology. They are about building a partnership that may go on long after the products have reached the end of their life. It is vital to work with a vendor with a long history of innovation and investment not just in technology but in service, support, and above all else, security research, so you can remain ahead of your cyber adversaries even as networking and security solutions and strategies continue to evolve. Metrics worth considering include R&D budget, global presence, analyst validation, number of patents filed, breadth of an integrated portfolio, and a history of uncovering zero-day threats.

## Conclusion

Today's best practice is to build a security infrastructure composed of components that can work together to create an HMF and, beyond that, a completely integrated security fabric that combines security and networking into a single solution. Fortinet FortiGate NGFWs are designed from the ground up to support an HMF infrastructure, and that, in turn, can serve as the core of your broader security fabric that embraces a wide range of security and networking tools from Fortinet and our many partners.

[1] Cyber Threat Predictions for 2023, FortiGuard Labs, 2022.

[2] Fortinet, "Hybrid Mesh Firewall," March 2023.

June 12, 2023 3:41 PM

2197076-0-0-EN