INDUSTRY INSIGHTS

Three Ways Fortinet Hybrid Mesh Firewalls Secure Edge Networks

Enterprise IT is changing. Applications are shifting to hybrid deployments across on-premises data centers and the cloud. Corporate campuses and branches are migrating from MPLS to low-cost broadband in Direct Internet Access (DIA) models. Employees no longer work exclusively at offices but can access company resources anywhere and with any device, often at home. Egress points multiply from a few to hundreds and even thousands, creating complex edge networks. The internet ties these changes together as the new corporate backbone.

Despite the wonders of edge networks, challenges remain. Management is complex with siloed domains across data centers, public clouds, distributed sites, and remote locations. In fact, according to Gartner, 99% of all firewall breaches through 2025 will be the result of user errors borne from complexity.[1]

In 2022, Fortinet surveyed global enterprises and found that 78% felt they were "very" or "extremely" prepared to thwart a ransomware breach, yet half of those respondents still fell victim to an attack.[2] In addition, enterprises struggle to manage edge networks as most internet traffic is encrypted, with the latest estimate by Google at 95%.[3] For enterprises relying on the internet to conduct business, that means IT teams are blind to everything being sent to and from the network, including cyberattacks.

To address these challenges, Fortinet Hybrid Mesh Firewalls (HMFs) provide unified and centralized visibility, management, and protection for data centers, branches and campuses, public clouds, and remote sites. With FortiManager centralized management, Fortinet offers simple management for unified protection. Fortinet HMFs leverage FortiGuard AI-Powered Security Services to protect edge networks and devices against known and unknown cyberthreats. Proprietary security processing units (SPUs) deliver unparalleled performance at the network edge, even when decrypting traffic, ensuring malware hiding in encrypted traffic does not slip through.

Centralized and Unified Management

The most important aspect of an HMF is unified management. Hybrid mesh firewall solutions cannot be disjointed solutions where different areas of IT require their own individual management consoles. Centralized and unified management integrates traditionally separate IT domains—data centers, distributed sites, public clouds, and remote workers—into one platform.

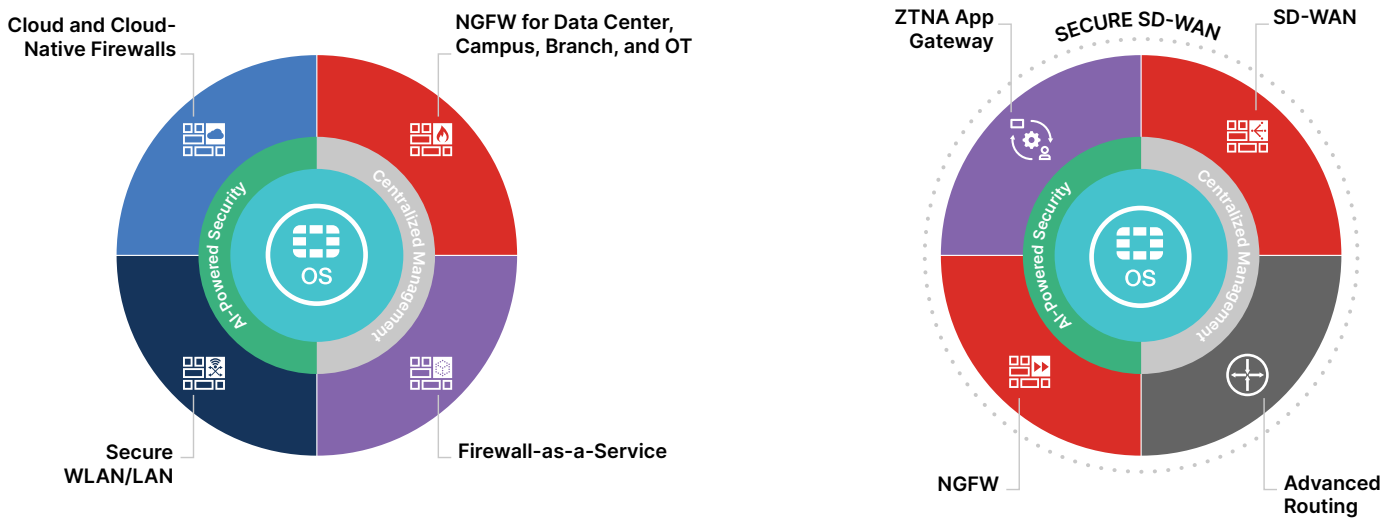

Figure 1: Example of a hybrid mesh firewall deployment

FortiManager allows for consistent policies across the entire HMF deployment. Policies are entered once, automated, and enforced wherever needed across the enterprise. Efficient management and automation reduce manual work, filling workplace shortages. Our easy-to-use centralized management shortens new-hire ramp times and reduces churn, allowing IT professionals to focus on strategic tasks.

AI-Powered Security Services

FortiGuard AI-Powered Security Services integrate critical capabilities into Fortinet HMFs (FortiGate Next-Generation Firewalls) to protect against threats in real time. These services include URL and DNS filtering, application control, anti-malware, and sandboxing, as well as hardware-accelerated IPS for high-performance SSL inspection and virtual patching. Fortinet also has a proven track record protecting IoT and OT environments and devices.

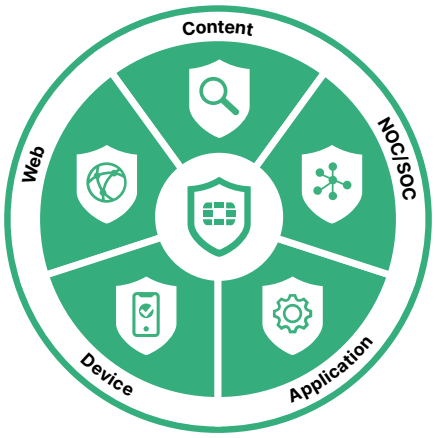

Figure 2: FortiGuard AI-Powered Security Services

With over 660,000 customers and 8 million sensors deployed, Fortinet leverages industry-leading telemetry, along with trusted partnerships, open-source intelligence (OSINT), Cyber Threat Alliance (CTA) feeds, and more to keep customers safe.

Custom-Built SPUs

Traditional network security vendors rely on general-purpose CPUs to deliver networking and security capabilities. Their products cause poor experiences when resource-intensive functions like decryption, IPsec, or IPS are enabled. Fortinet HMFs leverage proprietary SPUs to offload resource-intensive functions from device CPUs and improve user experiences. Our SPUs provide performance advantages so edge traffic can be inspected with no network slowdowns. Fortinet SPUs also provide the highest ROI for businesses while offering lower power consumption, thereby reducing TCO while adhering to environmental, social, and governance (ESG) goals.

The Fortinet Hybrid Mesh Firewall for Edge Networks

As enterprise networks transform into edge networks with multiple domains across data centers, distributed sites, public clouds, and remote locations, a unified security solution is needed to address the associated challenges and complexity. Fortinet HMFs can help enterprises overcome transformational challenges, offering unified, centralized management and protection and operational simplicity.

[1] Gartner, Control Network Security Complexity, Inefficiencies and Security Failures by Minimizing Firewall Diversity, Accessed May 31, 2023.

[2] Fortinet, The 2023 Global Ransomware Report, April 20, 2023.

[3] Google, HTTPS Transparency Report, Accessed May 22, 2023.

June 8, 2023 2:37 PM

2195473-0-0-EN