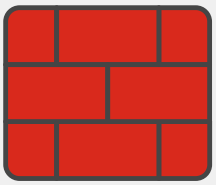
INDUSTRY INSIGHTS

Integrated Network Firewalls: An Essential Solution for Today's Distributed Enterprise

What Is an Integrated Network Firewall Solution?

Most organizations lack consistent security and visibility across various segments of their distributed networks, and cybercriminals are using that to their advantage. Because the data center, campus, cloud, and branch environments are interconnected, east-west traffic has increased, allowing a successful breach in one part of the network to quickly spread to others. The most effective way to address this challenge is to deploy the same security in every part of the network, thereby enabling centralized threat correlation and coordinated protection for multiple areas of the enterprise simultaneously. However, the complexities and differences between various network ecosystems can make that difficult.

Network firewalls can be deployed to provide critical NGFW functions anywhere across your network—campus, data center, cloud, FWaaS, and SASE environments—with remote unified management. Using the same operating system creates a single, integrated platform that can span, scale, and adapt to today's dynamic and distributed networks. A unified management console can coordinate protection across IT domains, including corporate sites, public and private clouds, and remote workers. This integrated approach allows IT teams to automate threat detection and response, orchestrate configurations, and enforce policies without investing needless manual hours—especially when the cybersecurity skills gap is already constraining resources.



Fortinet has been recognized as a Leader in the Gartner® Magic Quadrant™ for Network Firewalls for 13 consecutive years and is positioned highest in Ability to Execute in the latest report.[1]

The Need for Integrated Network Firewalls

Network firewalls are essential for safeguarding networks from unauthorized access and malicious attacks. They act as digital gatekeepers, monitoring and controlling network traffic to prevent unauthorized access, data breaches, and other security threats. These solutions are designed to address four critical challenges today's IT organizations face:

1. IT complexity

Many of today's NGFWs cannot support key capabilities, forcing enterprise IT to purchase separate security solutions for corporate sites, public and private cloud environments, and remote workers. This creates operational inconsistencies, including misconfigurations that can lead to network breaches.

2. The cybersecurity skills gap

In addition to complexity, point products add to organizational risk due to their long ramp-up times. Multiple point products increase your cybersecurity IT staff's time learning new features and dashboards. This puts enterprises at even greater risk, as many cybersecurity roles remain unfilled due to the global talent gap.

3. The rise of advanced threats

Complexity and cybersecurity skills shortages aren't the only factors driving the need for integrated network firewalls. Advanced, sophisticated cyberthreats are rapidly increasing, in many cases thanks to artificial intelligence. These advanced threats are becoming more difficult to detect and are increasingly devastating to businesses. Their attack vectors span the web, applications, content, and devices. Ransomware, for example, continues to disrupt industries across verticals, including operational technology (OT), state and local governments, manufacturing, and healthcare organizations.

4. The role of AI/ML and threat intelligence

Complexity, manual oversight, and an expanding threat landscape require coordinated protection. It's not enough that your firewall can span the different areas of your network. They must also contain the artificial intelligence and machine learning (AI/ML) capabilities required to protect against known and unknown threats. Adding AI/ML-powered security to network firewalls enables them to identify and classify applications, web URLs, users, devices, malware, and more, all while automating policy enforcement across domains. AI/ML is at the heart of network firewall automation and can significantly reduce the amount of manual work involved in protecting enterprise IT.

What to Look for in a Network Firewall Solution for Hybrid Environments

Centralized and unified management

The most vital benefits of network firewalls are seeing threats, managing policies, and automatically orchestrating responses to threats anywhere across your network using every tool at your disposal.

Unified management coordinates and unifies your domains into a single enterprise IT security solution, enabling simple, automated protection that extends from corporate sites to the cloud and remote workers. Because different organizations have different requirements for managing disparate network firewalls, all form factors must be supported, including appliances, VMs, SaaS, and managed firewall services.

Your network firewall must also bring your network operations center (NOC) and security operations center (SOC) teams together through a single pane of glass to manage and monitor your entire attack surface.

ASIC-based appliances

Every environment in your network has unique security challenges. Corporate sites require appliances that can scale security functions, ensuring consistent protection without impacting user experience.

Today's performance-hungry organizations need appliances that include enhanced application-specific integrated circuits (ASICs) to increase the speed of critical security services. A security appliance built with a custom ASIC can offload numerous resource-intensive functions, like firewalling, VPN, IPS, and even SSL/TLS or deep packet inspection (DPI). ASICs can significantly enhance the performance of security functions compared to general-purpose processors.

Cloud-native firewall

Cloud-native firewalls protect public cloud application workloads deployed in IaaS environments as Infrastructure-as-Code. Adding a cloud-native network firewall to your cloud environment also reduces your network security operations workload by expanding visibility while eliminating the need to configure, provision, and maintain a firewall software infrastructure, allowing security teams to focus on policy management.

Virtual firewall

Virtual firewalls are commonly used to protect virtualized environments in software-defined data centers and multi-cloud environments. Because they are the least expensive and the most portable solution, IT staff can quickly move a virtual firewall from cloud to cloud. The virtual firewalls within a network firewall solution further enable a comprehensive security ecosystem for your software-defined data center, aiding your consolidation process while protecting your environment from threats, using a variety of cybersecurity services beyond stateful firewalling.

Firewall-as-a-Service

Firewall-as-a-Service (FWaaS) is a firewall solution delivered as a cloud-based service. This allows companies to simplify and scale their IT infrastructure. In many ways, FWaaS is much like the hardware firewall you deploy on-premises, providing the full range of NGFW capabilities, like web filtering, advanced threat protection, IPS, and DNS security. A network firewall deployed as an FWaaS solution extends its unique capabilities to distributed users and devices, combining nearly instantaneous scalability with centralized control.

A single operating system

The rapid expansion of network edges has compounded the challenges of vendor and point solution sprawl. Disparate point solutions cannot work together or share information, making consistent security policy, end-to-end visibility, and automation impossible. Trying to maintain and monitor numerous hybrid, hardware, software, and X-as-a-Service solutions also overburdens security teams.

A single operating system consolidates numerous technologies and use cases into a simplified, single policy and management framework. While its unified management console unifies its front-end operations, a single operating system ensures that various deployments, such as appliances, virtual and cloud-native firewalls, and FWaaS agents, can all interoperate on the back end.

The Value of Integrated Network Firewalls

Integrated network firewalls bring enormous benefits to enterprise IT. These include increased IT operational efficiency, simplified cybersecurity operations, reduced organizational risk, relief from the cybersecurity skills gap, resilient protection against known and unknown cyberthreats, automation and coordination via AI/ML, and a lower total cost of ownership.

[1] A Leader Positioned Highest in Ability to Execute, Fortinet, accessed September 13, 2024.

September 19, 2024 1:58 PM / 2133550-A-0-EN