FORTINET

WHITE PAPER

Scaling for High-Performance Security

6 Criteria for Choosing Next-Generation Firewalls

Executive Summary

The shift to a hybrid workforce and the rapid adoption of cloud services have allowed today's users to connect to any resource from any location using any device. Although this flexibility is necessary, it also expands the attack surface, which opens the door to new threats. Organizations need to be sure their network security enables complete visibility across the entire distributed infrastructure. Otherwise, it will be impossible to effectively deliver and coordinate security protection with fast enough threat detection and remediation.

Combining next-generation firewalls (NGFWs) with AI-powered security services provides real-time threat intelligence, giving users multilayered security with intrusion prevention, malware scanning, and web filtering for comprehensive protection. This combination reduces downtime and data breach risks, minimizing costly recovery efforts and reputational damage. Ideally, the security services are tightly integrated into the firewall to offer a valuable approach to bolstering network security.

$4.45 M

According to a recent report, the global average cost of a data breach reached a record high of $4.45 million in 2023. This represents a 2.25% increase from the previous year.[1]

NGFWs should provide threat protection at every edge across the branch, campus, and the data center without sacrificing performance. To be effective across the organization, they must also be part of a broad, integrated, and automated security architecture and address scalability, cost of ownership, and environmental concerns.

Requirements for Evaluating NGFWs

NGFWs play an important role in threat protection, providing security that extends from the network edge to the data center, between internal segments, and in the cloud. Security teams rely on NGFWs to gain visibility into the users, devices, applications, and network threats and apply advanced threat protection wherever needed. Organizations should consider six key criteria when selecting NGFW for enterprise edges or data centers.

1. **Integrated AI-powered security services.** Security services powered by artificial intelligence (AI) complement traditional firewall capabilities by providing proactive threat detection against evolving threats. The services help reduce the workload for security teams, improve security efficiency and resource allocation, and streamline security management for better decision-making.

   NGFWs with integrated AI-powered security services go beyond traditional firewalls because they include machine learning that can analyze vast amounts of data to identify anomalous patterns that might indicate malicious activity. Using AI, the firewall can dynamically adapt security policies based on real-time network traffic analysis, which ensures that relevant and effective security measures are applied, reducing the risk of breaches and optimizing resource allocation.

2. **Threat protection performance.** Threat protection performance measures how well an NGFW performs while running full threat protection, including firewalling, intrusion prevention, antivirus, and application control. It is critical for the NGFW to sustain high performance when full threat protection is turned on. Many NGFW providers are ambiguous about how they represent their threat protection performance claims. Documented performance claims should be examined carefully to ensure they reflect testing under load with threat protection fully engaged.

3. **Single-pane-of-glass management.** The management interface is where many security architects are stymied in their selection process. Careful attention may have been paid to the management system's user interface and functionality. Still, if it is limited to the NGFW, security teams must toggle between multiple dashboards to assess vulnerabilities and respond to threats. End-to-end visibility and control are possible only if the NGFW is part of a broad, integrated security architecture, across which it can share threat information with other network devices and receive threat intelligence automatically. From a security standpoint, single-pane-of-glass management is more effective. It is also operationally more efficient, reducing administrative time and training costs.

4. **Ensure a broader security strategy.** The hybrid workforce has forever changed the cybersecurity landscape. Organizations also often have distributed offices that depend on redundant WAN connections. In many cases, they require additional security solutions like SD-WAN, zero-trust network access (ZTNA), and secure access service edge (SASE).

   Many NGFW vendors have add-on SD-WAN, SASE, and ZTNA features that allow organizations with branch offices to build highly available and high-performance networks. However, these offers are not ideal. Look for a vendor that offers fully integrated secure SD-WAN, SASE, and ZTNA capabilities in its NGFWs that help consolidate their point products and enforce centralized control. Consolidation helps reduce overall investment costs and eliminate security gaps.

5. **Price/performance and other operational considerations.** Some vendors scale performance by increasing the size and price of their NGFWs, which may not align with enterprise trends toward shrinking technology footprints. Aim for an NGFW that delivers the required performance in the most compact form factor. Opting for a smaller NGFW can reduce total cost of ownership (TCO), save space, and reduce energy consumption, which can be important objectives for environmentally conscious enterprises. Maintenance and support costs for the NGFW should also be factored into the TCO. Mature technology has an edge in this respect, as does an offering from a vendor with deep investments in research and design. Owners of NGFWs that fall into this category can expect smoother deployments and fewer support calls. When considering the NGFW hardware, pay attention to power redundancy and support for 40 GbE and 100 GbE network interfaces. These options support resiliency and accommodate migration to higher-capacity networks.

6. **Independent third-party validation.** Although network security is a rapidly evolving industry, no enterprise can afford the risk of untested security solutions. Architects should not rely on vendor claims alone but seek third-party evaluation from recognized testing houses such as cyberratings.org.

Top NGFW Priorities

Because the NGFW plays a critical role in protecting the entire enterprise, including corporate and customer data, security architects should be diligent in reviewing their options. When evaluating NGFW solutions, potential trade-offs between security and performance may be top of mind. The ability to provide consistent and consolidated security protection across all distributed edges with minimal performance impact is critical.

However, organizations need to take other considerations into account. Given power and space restrictions, preference should be given to compact NGFW solutions that minimize space requirements while being flexible enough to deploy in the data center or on the network edge. Security architects also should make sure the NGFW is integrated into the overall security architecture and that it provides end-to-end visibility and the ability to automatically share threat intelligence between devices.

[1] IBM Security and the Ponemon Institute, The Cost of a Data Breach Report 2023.

March 19, 2024 1:42 PM

2155416-A-0-EN