WHITE PAPER

Scaling for High-Performance Security

6 Criteria for Choosing Next-Generation Firewalls

Executive Summary

As the guardians of their enterprises' ever-expanding attack surfaces, security architects look for more effective ways to deliver threat protection and to coordinate it with threat detection and remediation. Next-generation firewalls (NGFWs), which typically anchor security architectures, are the linchpins of these capabilities, so architects should choose carefully.

Comprehensive threat protection includes firewalling, intrusion prevention, antivirus, and application control. Advanced NGFWs also inspect secure sockets layer (SSL)-encrypted traffic. In some NGFWs, though, the combination of these processes can severely hamper network throughput. That's why, as application counts and traffic volumes grow, security teams may resort to turning off some threatprotection controls to maintain acceptable levels of network service.

This is a compromise that organizations cannot afford. According to a recent report, the total average organizational cost of data breaches in the U.S. has already reached $7.35 million.[1] NGFWs must offer bestof-breed threat protection at the enterprise edge and in the data center without sacrificing performance. Operating within a broad, integrated, and automated security architecture, NGFWs must also satisfy the scalability, cost of ownership, and environmental concerns of the digitally transforming enterprise.

Evaluating Your NGFW Requirements

NGFWs play an important role in threat protection, from the network edge to the data center, between internal segments, and in the cloud. Security teams rely on their NGFWs to gain visibility into users, devices, applications, and threats on the network, and to apply advanced threat protection wherever it is needed.

Six key criteria should guide the evaluation and selection of enterprise edge or data-center NGFWs:

1. **Threat protection performance.** Threat protection performance is a measurement of how well an NGFW performs while running full threat protection (firewalling, intrusion prevention, antivirus, and application control). Ideally, the NGFW can sustain performance when full threat protection is turned on. In some cases, however, performance degradation is substantial. As an example, based on internal Fortinet research, signature-matching (a function of IPS) can reduce some NGFWs' speed by as much as 30%.

   Many NGFW providers are ambiguous in 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.

2. **SSL inspection across the entire enterprise.** An enterprise NGFW must also be able to perform well with SSL inspection engaged. Most enterprise network traffic is now encrypted.[2] Cyber criminals are taking advantage of the inherent trust and low inspection priority given to SSL traffic by some and are inserting malware into encrypted packets. Such malware can be ferreted out through SSL decryption and inspection. The penalty for SSL inspection, though, is reduced throughput. In some cases, the slowdown is significant enough to impact applications in ways that hamper business productivity and customer experience.

   While all NGFWs experience some impact on throughput with SSL turned on, the best will have predictable performance and see minimal speed degradation. When comparing data sheets, look for transparency in the vendor's SSL performance specifications. They should cite testing with industry-mandated ciphers (standardized algorithms used for encrypting and decrypting sensitive information) such as AES256-SHA and TLS 1.2 that have preferably been validated by objective third parties.

3. **Session capacity.** Session capacity for most NGFW appliances tops out at a few million sessions. As traffic volume and the number of devices connecting to the network continue to skyrocket, session capacity is critical to accommodate peak connectivity, which may exceed 100 million concurrent sessions in large enterprises.

   To deliver high-throughput performance, NGFWs designed for enterprise-scale traffic have a load-balancing architecture that supports high connection rates as well as offering failover for resiliency. This is a more cost-efficient alternative to routing trafficthrough several low-capacity firewalls.

1. **Price/performance and other operational considerations.** Some vendors scale performance by increasing the size, and consequently, the price of their NGFWs. This 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. This not only reduces total cost of ownership (TCO) but it also saves space and reduces energy consumption, both important objectives for environmentally conscious enterprises.

   Maintenance and support costs for the NGFW should be factored into TCO, too. 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 will support resiliency and accommodate migration to higher-capacity networks.

2. **Independent third-party validation.** Although network security is a rapidly evolving industry, no enterprise can afford the risk of untested security innovations. Architects should not rely on vendor claims alone but seek third-party evaluation from recognized bodies such as NSS Labs. The latter offers detailed test results and recommendations for NGFWs in a variety of use cases, such as data-center security gateway (DCSG), data-center firewall (DCFW), data-center intrusion prevention system (DCIPS), and next-generation intrusion prevention system (NGIPS).

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, but if it is limited to the NGFW, security teams will have to toggle between multiple dashboards to assess vulnerabilities and respond to threats. Endto-end visibility and control is 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 receives threat intelligence automatically.

   Single-pane-of-glass management is not only more effective from a security standpoint but it is also operationally more efficient, reducing administrative time and training costs.

Building Your NGFW Priority Checklist

As security architects evaluate NGFW solutions, potential trade-offs between security and performance may be top of mind. And it's true—the ability to provide full threat protection and SSL inspection with minimal performance impact is critical.

There are other considerations, however. Given power and space restrictions, preference should be given for compact NGFW solutions that minimize space requirements while being flexible enough to deploy in the data center or on the network edge.

Finally, security architects should consider the capability to integrate the NGFW into the overall security architecture, providing end-toend visibility and the ability to automatically share threat intelligence between devices.

The NGFW is at the heart of every enterprise security solution and plays a critical role in protecting corporate and customer data. Security architects reviewing their options will be pleased to learn that one NGFW stands out clearly from its peers.

[1] "2017 Cost of Data Breach Study: United States," Ponemon Institute LLC, June 2017.

[2] Siggi Stefnisson, "Private, But Not Secure: HTTPS is Hiding Cybercrime", SecurityWeek, September 22, 2017.

FORTINET

www.fortinet.com