WHITE PAPER

Evolution of Next Generation Firewall

Choosing your first line of defense

Table of Contents

Executive Summary

Next generation firewalls (NGFWs) are a prime example of how cybersecurity controls continue to evolve. Enterprises need a strong first line of defense to protect their constantly changing attack surface. The number of attack vectors available to attackers is growing for several reasons, including a rise in the number of applications being used in the enterprise (and these must be constantly patched) and increased adoption of bring your own device (BYOD). Enterprises need to stop attackers at the perimeter.

The challenge is that the NGFW market is full of products that are being marketed as having seemingly endless features and configuration capabilities. This gives the enterprise buyer way too many products to evaluate, and since security is usually a major investment, enterprises could be stuck with the wrong choice for three years or longer.

As with any major purchase, buyers will progress through stages, beginning with educating themselves about products, then evaluating specific products, and finally deciding which product to purchase. Many buyers will start by listing all of the market leaders, but these lists need to be narrowed down to just the top contenders. Enterprise buyers must understand the following:

- Although vendors are trying to commoditize the NGFW market, it remains diverse—features, security capabilities, and inspected traffic performance vary greatly.
- Depending on vendor data sheets to narrow your list of vendors for proof of concept (POC) testing will only makes things confusing.
- Before conducting any POC, organizations should quantitatively assess products using common metrics, such as security effectiveness, performance, stability and reliability, and total cost of ownership.
- The POC is the time when evaluators should shortlist products based on traits specific to the organization's use case.
- Selecting products for a POC shortlist requires a disciplined approach that's based on facts rather than marketing hype.

Read on to find out what it takes to achieve that discipline, including specific details about the most productive quantitative measurement categories organizations should examine early in evaluation.

Buyers Must Keep Up with Constantly Evolving Products

NGFWs were initially built to merge traditional firewall functionality with intrusion prevention system (IPS) blocking capabilities and application awareness and control. The idea was to not only provide robust perimeter inspection to identify application-level threats that were evading traditional firewall filtering but also to provide deep packet inspection (DPI). This functionality was combined into a single product to simplify maintenance, configuration, and deployment.

However, threats have continued to evolve along with the growing enterprise attack surface, proliferation of applications, and lack of comprehensive vulnerability patch management—and some advanced threats can use evasion techniques to bypass network security controls. To combat these threats, NGFW vendors have added advanced features and capabilities, including:

- **Behavioral analysis and threat intelligence-fueled reputation services:** Attacks are detected and blocked based on identifying abnormal behavior through machine learning of what is considered "normal" activity and in conjunction with reputation services such as threat intelligence agents on endpoints.
- **Deeper forensics information:** This includes forensics portals with visibility into command & control traffic and indicators of compromise (IOCs) of how attacks occur so they can be prevented in the future by creating indicators of attack (IOAs) as early warning signals.
- **Alert prioritization per host:** Instead of having responders sift through a flood of alerts, the product scores and groups them, helping to avoid alert fatigue.
- **SSL inspection abilities:** Since SSL/TLS traffic can hide threats, NGFW products now integrate proxy services where they act as the "in-between" device establishing secure communications to both host and website so all traffic can be evaluated.
- **Sandboxed malware analysis:** Unverified or untrusted files are run in a virtual environment to see if they are malicious.

These features and capabilities are good news both for existing NGFW customers and for new market entrants who are looking to purchase their first—or second—cycle of product refreshes. Unfortunately, they also make product evaluation more difficult, since evaluators must decide which features can be objectively measured. Buyers can identify key measurable metrics early on during product evaluation by taking a step back from vendor claims and instead focusing on what their organizations require. Evaluators should start by listing their key requirements and from there, they can look for objective metrics that act as common measurements to quantitatively evaluate products across the board.

Security and Performance: NGFW Balancing Act

Further complicating the buying process is the fact that the maturation of the NGFW market has led to a wide spectrum of security and performance proficiency that's dependent not only on the vendor but also on how the NGFW is configured and deployed.

Security and performance almost always have an inverse relationship. An increase in security functionality usually causes a proportionate decrease in performance, and vice versa. This relationship between security and performance is particularly challenging in the NGFW market because of the mission-critical nature of network throughput and the growing need for threat prevention at the network perimeter. If organizations can stop threats without sacrificing performance and introducing latency, then they can prevent exploitation, installation of malware, and ongoing compromises of those systems, and they can do so with no impact to business continuity.

Security and performance almost always have an inverse relationship. An increase in security functionality usually causes a proportionate decrease in performance, and vice versa.

The market has responded with NGFW products that offer both high security and high performance, which in turn could impact the overall cost of the product. Product evaluation teams must not only understand these trade-offs, but they must also decide how they will evaluate products against each other. For example, certain vendors may tout performance numbers in their marketing literature that can only be achieved when application-level control is off, while others may promote performance numbers with application-level control enabled. It is critical for buyers to take such information into account when evaluating NGFW products.

Enterprises seeking to purchase NGFW products must perform due diligence to sift through potential contenders and level the playing field. With dozens of vendors competing for market share, it is essential for enterprise buyers to conduct in-depth POCs in order to establish which products are the best fit for their organizations.

Marketing Hype vs. Facts

Even before getting to the POC stage, enterprises need to compare NGFW products based on facts, not just vendor claims. Buyers who can't establish their own quantitative metrics for comparison are forced to rely on marketing data sheets to narrow down the field, and these claims can often distract enterprises from finding the products they truly need.

Some vendors promote capabilities such as breach detection functionality and advanced malware protection, while others focus on application ID firewalls and threat prevention. Buzzwords like "visibility," and "management" only add to the confusion. And because vendors use different metrics to promote their product capabilities, there is no common denominator to use to quickly compare security and performance metrics. Marketing material is simply too subjective.

Even before getting to the POC stage, enterprises need to compare NGFW products based on facts, not just vendor claims.

So how does an enterprise choose? It needs common metrics against which all products can be evaluated. At NSS Labs, we believe that to enable meaningful comparisons, security products should be tested in the following four areas:

- Security effectiveness
- Performance
- Stability and reliability
- Total cost of ownership (TCO)

Security Effectiveness

NGFWs should be evaluated for their ability to protect against known and unknown threats entering from both north-south and east-west (lateral movement) entry points in an enterprise network.

- Firewall policy enforcement: How well does the firewall enforce policy between trusted to untrusted, untrusted to DMZ, and trusted to DMZ connections?
- Application control: Can the product correctly identify and block policy-named applications, and can it block specific actions depending on the application?
- Intrusion prevention: Based on recommended security profiles, how well does the IPS function handle a standardized set of exploits? Does it report on false positive events, and is it able to handle different attack vectors from network exploits?
- Evasions: How well does the product handle common evasion tactics, including HTML and URL obfuscation, packet fragmentation, Hyper Text Transfer Protocol "HTTP" compression, and payload encoding?
- SSL inspection: Can the NGFW intercept, decrypt, and inspect SSL/TLS-based traffic?

Performance

NGFWs must not only deliver high performance and throughput, but they must also be scalable, so that security functions can be consolidated without causing disruption to applications and services. Medium-to-large enterprises demand highly flexible architectures that can quickly inspect content for threats while also performing basic firewall tasks.

Enterprise buyers should ask the following questions during evaluation of an NGFW product:

- UDP throughput: What is the device's UDP throughput for packets of varying sizes with variable source and destination IP addresses transmitted bi-directionally through each port pair of the tested device?
- Latency: How does the device affect traffic passing through it under various load conditions?
- Maximum capacity: How does the engine handle high volumes of TCP connections per second, application layer transactions per second, and concurrent open connections?
- HTTP capacity: How does the inspection engine handle HTTP capacity with and without transaction delays or persistent connections?
- Real-world traffic mixes: How is device performance affected by the addition of protocols and real-world content beyond HTTP traffic?
- IPsec site-to-site VPN: How well does the device's default "out-of-the-box" policy account for inspection over the VPN tunnel?

Stability and Reliability

NGFWs should be able to perform well even under extraordinary circumstances, including accounting for power failure and extended attacks, such as distributed denial-of-service (DDoS) attacks. The following capabilities should also be considered:

- Blocking under extended attack: How does the device perform blocking when submitted to a continuous stream of security policy violations mixed with legitimate traffic for an extended period of time?
- Passing legitimate traffic under extended attack: When submitted to that same extended attack, how well does the device pass legitimate traffic?
- Behavior of the state engine under load: Can the device preserve state across a large number of open connections over an extended period of time?
- Protocol fuzzing and mutation: How well does the device handle traffic from protocol

randomizer and mutation tools?

- Power fail: Does the device fail closed, i.e., on failure, or does it continue to pass traffic?
- Persistence of data: Is all configuration data, policy data and locally logged data retained following power failure?

Total Cost of Ownership

An enterprise-class NGFW is a significant investment that is expected to provide value for a minimum of three years. Costs should be considered for the entire life cycle of the product and not just the first year. The following factors should be considered:

- Product purchase: How much does it cost to acquire the product?
- Product maintenance: What fees does the vendor charge for support, maintenance, and updates to the product after acquisition?
- Installation: What resources does the buyer require to deploy the product?
- Upkeep: What ongoing resources are required to apply updates and patches from the vendor?

If evaluating many NGFW products in each of these areas sounds like a lot of work, that's because it is. It requires a significant test bench, a comprehensive exploit library, and knowledgeable testers. But establishing these metrics early on during product evaluation is crucial to rightsizing a POC, since it allows for more stringent testing of products. Organizations that wait until POC evaluations to submit products to this level of testing risk choosing the wrong products.

Ensuring NGFW POC Success

NSS provides organizations with the results of its own hands-on testing, and this data can greatly accelerate the buying process. Armed with the quantitative data provided by NSS' NGFW reports, an organization can choose its POC shortlist quickly and confidently. There is no need for risky guesswork about products' real-world technical capabilities and no need to make purchasing decisions based on self-serving data sheets.

Additionally, organizations can leverage NSS testing results to focus their POC evaluations on areas that require further in-depth analysis. For NGFW products, this means spending time testing visibility and management. If a product's core engines have already been stress tested, evaluators can focus on the dashboard and integration points, and on how processes would need to be changed to integrate with existing products.

Similarly, if evaluators have core security, performance, and stability metrics in hand, they can spend more time looking at advanced features such as reputation services and SSL inspection to determine if these capabilities give one product the edge over another.

In terms of visibility, this means delving into the product's unified management console and ensuring that it is capable of coordinating with the organization's threat management tools and other security solutions. NGFW products must also be capable of merging with endpoint, sandbox, and breach detection tools that focus on detecting, investigating, and mitigating suspicious activities, known threats, and other issues on an enterprise's hosts and endpoints. NGFWs should also be able to provide security information and event-based incident response-based workflows that are reliable and scalable, and they should be able to integrate with threat analytics platforms and take preventative action in real time.

There is no need for risky guesswork about products' real-world technical capabilities and no need to make purchasing decisions based on self-serving data sheets.

During a POC, organizations should ensure that the visibility afforded by greater integration into a layered security ecosystem doesn't come at the cost of management overhead. Deployment of these security controls often inadvertently introduces complexity. As a core component of an enterprise's security architecture, the NGFW's central management capabilities are critical. This includes the ability to view, manage, and configure multiple security controls from one central location.

Make Informed Decisions Based on Facts

NGFW products are key components of modern security strategies. As such, organizations can't afford to take product selection lightly. While POC evaluations play a critical role in analyzing product fit, the findings are moot if the products chosen for the bake-off are not well-suited for an organization's needs. Unfortunately, many organizations choose POC candidates based on marketing hyperbole, assuming they can sort through the hype at a later stage in the evaluation. This puts the organization at risk of a failed POC, or worse, a poorly chosen product.

NSS Labs allows organizations to evaluate a broad field of NGFW contenders based on quantitative facts rather than marketing hype. With this data in hand, enterprises can conduct POCs with confidence. To learn more about the NSS Labs NGFW Test Methodology, examine comparative data about NGFW vendor capabilities, or download reports on individual NGFW products, visit www.nsslabs.com/ngfw.

About NSS Labs

NSS Labs, Inc. is the global leader in operationalizing cybersecurity. Through continuous security validation and global threat discovery and automation, NSS Labs empowers enterprises to reduce the operational burden of cybersecurity and address crucial gaps in their cybersecurity efforts.

Informed by our experience and strong foundation of security product validation, NSS Labs offers CAWS, a cyber threat protection platform that provides businesses with visibility into the cyber kill chain and automated insights into active threats. With global visibility into active threats and vulnerabilities, CAWS delivers a unique cyber risk rating that makes cybersecurity measurable and helps enterprises focus their resources in the areas that make the most difference.

Combined, this information enables businesses to continuously monitor and respond to threats, strengthen their cybersecurity posture, and have confidence that they are appropriately securing the enterprise. CISOs, security operations teams, threat researchers, and information security professionals from many of the world's largest and most demanding enterprises rely on trusted insights from NSS Labs.

For more information, visit www.nsslabs.com.

NSS Labs
206 Wild Basin Road
Building A, Suite 200
Austin, TX 78746

+1 (844) NSS-LABS
www.nsslabs.com
advisor@nsslabs.com
@nsslabs