

Table of Contents

Executive Summary	3
Firewall Refreshes Represent Opportunity	3
High Availability Under Pressure	4
Contextual Security for Refined Access Control	4
Automated, Advanced Protection Against Evolving Tactics	5
Unified Software Platform	5
Demand More	6
About McAfee Network Security	6

Executive Summary

If application controls and intrusion prevention systems (IPS) are table stakes in the next-generation firewall (NGFW) competition, what else do you put on your requirements list?

This white paper will help network and cybersecurity teams understand the things they can and should demand from NGFWs:

- Built-in high availability and load balancing for operational resilience and handling growing data loads.
- Contextual security that provides fine-grained access control to reduce risk and manage usage.
- Automated, advanced evasion detection that can block and report on the unknown and evolving techniques enabling targeted and persistent threats.
- A unified software platform supporting adaptive network security and flexible deployment of next-generation features with visibility and operational efficiency.

These requirements go beyond specific features to encompass the long-term goal: securing the availability and integrity of critical networks as usage grows and threats evolve. Insisting on these capabilities will ensure that your NGFW can keep up with business requirements, clever cybercriminals, and budgetary realities.

“A next-generation firewall is not just a collection of the last generation’s answers. It takes security to the next level with its ability to detect advanced evasion techniques (AETs). Combining all the abilities in one solution allows it to see a more complete picture, providing enterprises with better security.”

—“2013 Next Generation Firewall Challenge,” Robin Layland, *Network World*¹

Firewall Refreshes Represent Opportunity

Firewalls are the first and most important line of defense against network threats. They serve diligently at every remote office, at the edge, and in the core/distribution network protecting data centers. And every few years, those legacy installations need an overhaul. Today, aging firewalls need to be retired, replaced by new designs with integrated and expanded features, deployment and control flexibility, and greater scalability and performance. These designs help future-proof your firewall to deal with changing business demands and the expanding threat landscape.

This firewall overhaul is a precious opportunity. For more than a decade, we have lived through the exasperation and cost of managing complex and disjointed firewall rule sets; deploying additional appliances for load balancing, intrusion prevention, VPNs, and threat analysis; and sifting through reams of logs. Now, we can use this experience to demand more intelligence and adaptability from network firewall vendors.

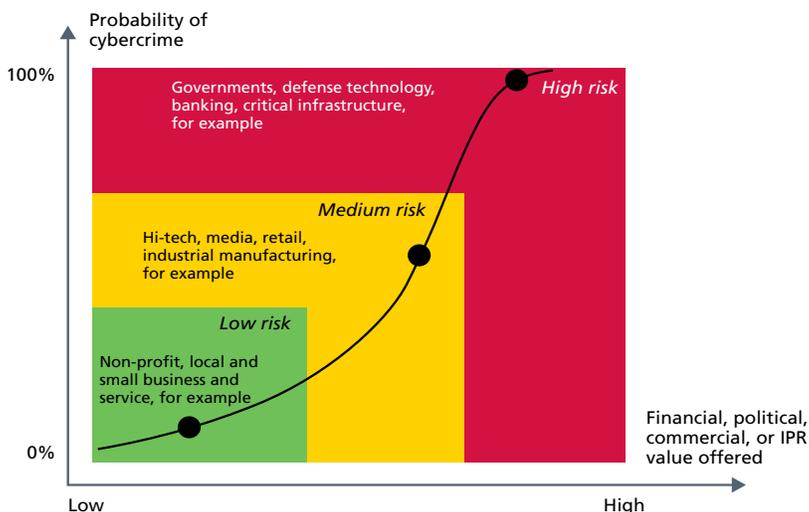


Figure 1. How the onslaught of advanced threats affects different industries.²

High Availability Under Pressure

Just about every business activity—even a phone call—now relies on the network. Network traffic volumes only have one direction: up. For IP-based security tools like NGFWs to do their job in this environment, they need to be continuously active—highly available and seamlessly scalable.

Some firewalls are designed to “fail open” (permit web traffic on failure) under pressure. If workloads pass a threshold, firewalls can drop traffic (standard firewalls) or stop performing inspections (NGFWs) to keep traffic flowing. This behavior keeps businesses operational, but sacrifices security. Why invest in application control and IPS rules that you can’t count on being enforced?

Alternatively, many enterprises increase capacity and availability through clustering, either using active-passive redundant configurations or using active-active load balancing to dole out traffic to several firewall nodes. Instead of a complex add-on, clustering should be designed in. Specifically, active-active clustering offers the best resource utilization, letting you make full use of your capital investments and add nodes as demand grows. Clustering can ensure that you have available compute resources for high-performance firewall inspections as well as capacity to accommodate expanding traffic.

Within this active-active model, three factors could affect your long-term satisfaction. First, look at the workload balancing model. If separate load balancing components are required, recognize that these extra components add capital expense and operational complexity—usually requiring at least an extra device, management server, and console to maintain and monitor.

Second, look for any limits to node counts. Some systems can only cluster a few nodes. That design forces you to size and pay now for a system that can meet your eventual peak loads, rather than adding nodes as your workloads increase. If all other features are equal, pick a design that can scale to 10 or more nodes.

Third, consider serviceability. What is the maintenance plan for the clustered firewall devices? Load balancing should permit individual nodes to be upgraded or serviced independently. This model means that you should be able to gradually upgrade nodes, effectively running multiple different versions of the firewall code, without degrading inspection quality or disrupting availability. If an individual firewall node fails, the load balancing model should ensure that no traffic has been dropped while redirecting the traffic to another node. This seamless and dynamic design provides for continuous inspection and policy enforcement.

Contextual Security for Refined Access Control

NGFWs include user and application controls as core features. They offer a great advance over block/allow firewall rules. But, once enterprises start experimenting with rules to drive these controls, many have found that user- and application-based rules are still simplistic. They work for major offender applications (such as free file sharing), but may not fit more intricate situations such as the use of LinkedIn. One challenge is that few IT teams have the visibility into users and applications to be completely confident about blocking. They don’t want to appear to be arbitrarily dictating access to applications and then have to deal with support calls from dissatisfied users.

Administrators prefer to apply thresholds, such as the number of times a specific situation occurs within a specific time window or the group or sequence of events. They want to correlate and aggregate events, including events that are collected on different NGFW sensors. This grouping of events and factors provides greater certainty and clarity about activities, from remote VPN use to Internet surfing. Once you start down this path, there’s a lot of value to be derived from this method. For example, the association of inbound and outbound IP addresses may be significant when administrators are concerned about a specific insider threat, botnet, or suspected attacker. All of these contextual control options empower IT to support business while keeping it secure.

“Security devices should do traffic normalization on each TCP/IP layer. But many network security devices favor speed over network security, and therefore they take short cuts. They don’t inspect all four layers of the TCP/IP model. In this way, the network security device might operate faster, but the network is susceptible to advanced evasions.”

—*Advanced Evasion Techniques for Dummies*³

Automated, Advanced Protection Against Evolving Tactics

NGFWs layered together reinforce and complement defenses, supporting defense-in-depth best practices. Anti-malware and intrusion prevention help identify and block known malware as well as zero-day threats targeting unpatched vulnerabilities. Generally, these systems use signatures or behavior to identify malicious code. In addition, application controls permit IT to shrink the attack surface by reducing use of risky applications and content. Together, these capabilities represent a significant step forward in edge protection compared to the legacy network firewall. It's an especially potent combination for protection at remote sites, where policies and protections work together to enhance the organization's network security strategy.

However, criminals continually invent ways to get past mainstream defenses. Where a few years ago attackers could succeed with investments in encryption and polymorphic malware, today's most determined and advanced hackers penetrate networks by distributing malicious code in a series of payloads, often obfuscated. Sometimes they send payloads using an assortment of protocols, such as FTP, HTTP, and HTTPS. This extra effort allows code to evade detection by standard signature-matching, protocol-specific, and pattern-detection defenses.

The way to combat these evasive tactics is to normalize the traffic across layers three to seven, tear down and examine the entire data stream, and assemble the parts into a unified whole. Once reassembled, the code can be inspected using signatures and patterns. Combined with the other defenses in a NGFW, this anti-evasion technique represents the leading edge of inline network defenses. If you can obtain these capabilities as part of your NGFW, you can incorporate tomorrow's mainstream defenses into today's network.

Unified Software Platform

This range of defenses should be part of a flexible and efficient operational architecture. Network security teams should assess the control and inspection features of NGFWs against their requirements for protection effectiveness and operational efficiency.

For effective security, you will want to be able to implement the most advanced analytics and make full use of all the controls you deploy. If you are hoping to deploy an all-in-one system, be wary of implementations that make you choose between defenses—such as trading off application control for IPS—or those that turn off inspections or other features under peak loads.

Even if you can live with these limitations today or like the flexibility of deploying a firewall/VPN, an NGFW, and an IPS wherever you see fit, a common software architecture for these solutions is desirable. A common platform allows policies and rules to work together to efficiently process traffic, stretching computing resources and teasing out the anomalies. Since your business requirements, network architecture, and risk posture may change quickly, a unified design can help you to respond immediately, adapting firewall configurations without paying the penalties of forklift upgrades.

A unified software platform provides a second benefit: operational efficiency. Years of legacy firewall maintenance has probably sensitized you to the issues of firewall operational complexity. Managing rules, swiveling between administration consoles, integrating data through spreadsheets—all of these day-to-day efforts add up to weeks over the course of a year. As you manage more firewalls in more places, you measure this operational burden in months—and this burden is often carried by a shrinking team.

As you add functionality to the firewall, including functions such as load balancing and VPN, you increase the importance of finding efficiencies. For instance, fine-grained policies should be reusable across firewalls. A centralized policy architecture provides practical ways to build fine-grained and consistent control into your firewall rules.

"Integrated security appliances have gained share every quarter since 4Q11, and Infonetics is forecasting quarterly share gains through 2Q14."

—*Network Security Appliances and Software*, Infonetics Research, September 2013⁴

Integration of your defenses architecturally enables integration of your defenses at a management level, boosting efficiency while opening up situational awareness of network events. The system can correlate and analyze logs for you, present events in a common console, and provide visualizations and analytics that help spotlight trending and breaking events.

Some businesses require IT to manage multiple or distributed domains: for example, for different organizational units or as a managed security service provider (MSSP). In these settings, be sure that you can share common tasks and monitor the situation from a single screen, while maintaining separate logical isolation for each domain. These capabilities are an NGFW benefit as you race to the cloud.

Integration and automation of policies, processes, and tools within a unified software base and architecture represent a critical success factor for harvesting the maximum security value from your next-generation firewalls. You improve the effectiveness of your controls and countermeasures while minimizing operational overhead.

Demand More

Your adoption of NGFWs should bring a substantial increase in the range of protections and controls you can apply to your network. Basic NGFW features such as crude application control provide a starting point for your checklist. However, basic features are just the beginning. You can demand other valuable features: intrusion prevention, contextual rules, advanced evasion analytics, secured access control, and high availability.

Beyond features, demand operational performance. Investigate the approach your vendors have taken to providing for present realities: limited skill sets and administrative resources faced with expanding demand and the need for visibility, defensive creativity, and situational awareness. Ask how they will help you adapt to future workloads, optimize resources, and detect and disable the next wave of threat techniques. By asking these questions now, you can protect your investment as well as your network and prevent disappointment, disruption, and unnecessary expenses down the road.

About McAfee Network Security

McAfee offers a complete line of network security solutions as part of its Security Connected framework. To learn more about the McAfee approach to next-generation firewalls, visit mcafee.com/NGFW.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ: INTC), empowers businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its visionary Security Connected strategy, innovative approach to hardware-enhanced security, and unique global threat intelligence network, McAfee is relentlessly focused on keeping its customers safe. <http://www.mcafee.com>



¹ http://resources.idgenterprise.com/original/AST-0088044_2013_NGFW_Challenge_document_FINAL.pdf

² <http://www.mcafee.com/uk/resources/reports/rp-advanced-evasion-techniques-for-dummies.pdf>

³ *Ibid.*

⁴ <http://www.infonetics.com/pr/2013/2Q13-Network-Security-Market-Highlights.asp>