Report

Network Performance and Security

CIOs and CISOs can avoid risky tradeoffs and boost threat defenses by deploying next-generation firewalls built for both security and network performance now.

intel Security

Table of Contents

Executive Summary

In recent years, the network firewall has evolved from a relatively simple security appliance to assume a prominent role in the enterprise's cybercrime defenses. Next-generation firewalls (NGFWs) represent the state of the art, incorporating features such as intrusion prevention, anti-malware, and deep packet inspection (DPI), technologies formerly implemented as separate point solutions.

These capabilities are essential tools in the fight against increasingly sophisticated attacks known as advanced persistent threats (APTs). As security experts were developing ways to defend against APTs, cybercriminals came up with new ways to defeat those defenses, the so-called advanced evasion techniques (AETs).

Though essential in the fight against APTs and AETs, enabling advanced protections on NGFWs can adversely affect network performance—sometimes dramatically. In response to users' complaints about poor application responsiveness, system administrators often disable key NGFW features such as DPI to restore performance levels. This action creates an existential tug-of-war between security administration's mandate to keep the business safe from intruders and network operation's requirement to ensure employee and customer usability and productivity. Compounding the problem, most CIOs and CISOs don't even know that tradeoffs are being made by their operations staff—until it's too late.

Faced with this troubling situation, IT executives must act. For starters, they need to institute internal training programs and awareness campaigns to ensure that every person in the IT organization understands the nature of advanced threats and the security implications of their actions. Fostering collaboration between operations and security leads to a more proactive stance and coordinated response to security incidents. Most importantly, CIOs and CISOs should aggressively push to deploy NGFWs that eliminate the performance-security tradeoff, boost proactive defenses against advanced threats, and improve IT staff efficiency.

Upgrading firewalls can meet with resistance from budget-conscious executive staffs, particularly when the proposed firewall replacement is ahead of a planned refresh cycle. In this event, the CIO or CISO must build a convincing financial case, documenting benefits such as risk mitigation, productivity increases, and infrastructure cost reductions from real-world deployments.

The evaluation process must include internal testing of candidate offerings based on the organization's individual performance and scalability needs. Testing should also verify that the NGFW is effective in detecting APTs, especially those employing AETs.

CIOs and CISOs who follow these recommendations will not only improve the effectiveness of both users and IT staff, but they will be successful in their most important job—protecting their organization's invaluable data assets and customer information.

Trading Security for Speed is Risky—and Common Practice

The importance of security is clear to most IT professionals. A recent survey of 504 IT professionals found that 60% prioritize security as the primary driver of network design[1]. In light of recent high-profile data breaches, this finding is hardly surprising.

Operationally, the picture is somewhat different. System administrators under pressure to improve network performance often point their fingers at the firewall. In about one-third of the organizations surveyed, operators routinely disable firewall security features in an attempt to increase performance—in essence, they prioritize performance over security (see Figure 1).

Disabling features may speed up the network, but it also compromises security. Why? Because the features that are routinely disabled—deep packet inspection, antispam, antivirus, and VPN access—are essential for robust threat defenses. Whether operators realize it or not, disabling firewall features is mortgaging security to pay for performance. Eventually the bill comes due with interest—in the form of a costly, embarrassing data breach.

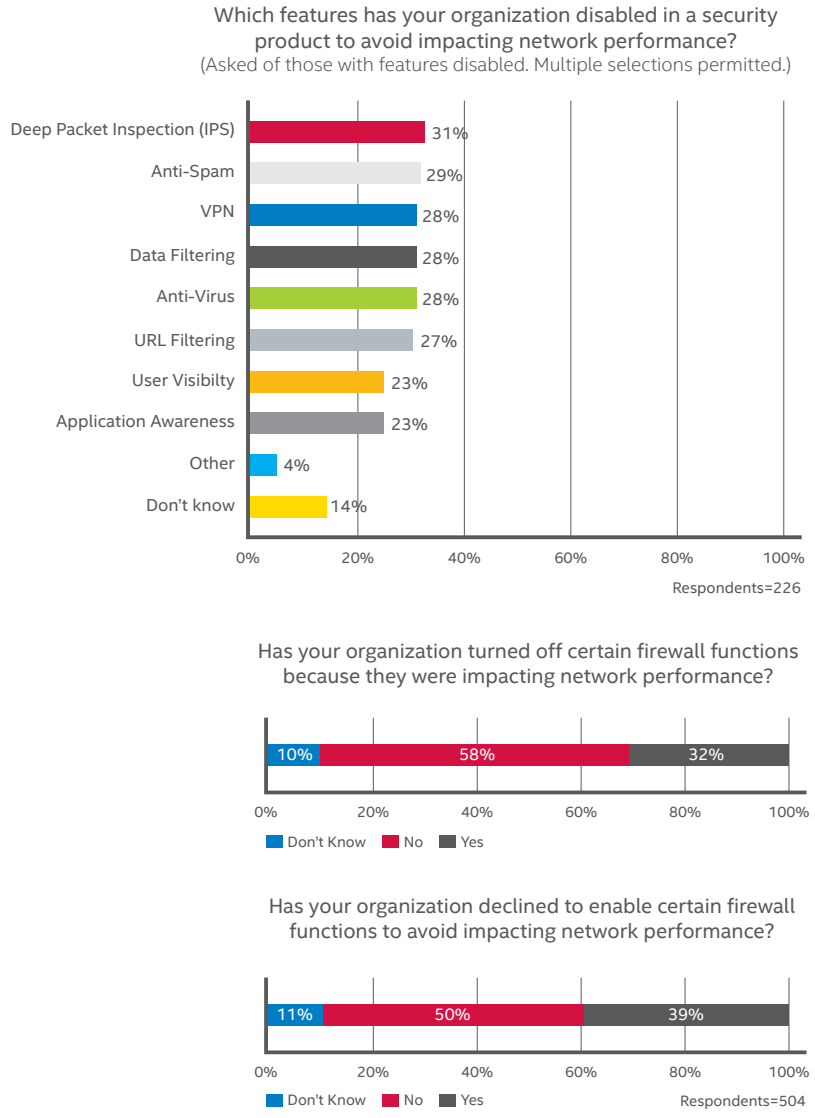

Figure 1. Survey responses regarding firewall features. At least one-third of organizations are compromising security by either declining to enable certain firewall features in the initial deployment perceived to impact network performance, or disabling features later in response to performance issues.

Networks Under Increased Pressure from Advanced Threats

A recent troubling escalation in cybercrime technology involves the use of AETs. In simplest terms, AETs are delivery mechanisms used to disguise APTs and permit them to slip through network security undetected (see Figure 2). AETs are having a profound impact: 40% of IT experts who have experienced a significant breach believe that AETs played a key role. Furthermore, AETs are proliferating at an almost incomprehensible rate—experts estimate that the number of AETs in existence today is approaching one billion.[2]

Many IT professionals have a false sense of security about their AET defenses. In a recent survey, 61% said that they were protected. However, when AET security experts closely examined those defenses, they determined that at least half were unable to detect AETs.[3] The risks associated with inadequate AET defense must drive CIO and CISO decision-making as will be discussed later in this report.

Figure 2. Relationship between AETs and APTs. AETs disguise APTs to bypass network defenses such as intrusion prevention systems and firewalls.

Upper Management Is Often in the Dark

As discussed earlier, seemingly minor decisions made by front-line IT operations staff can have huge implications on network security. IT executives certainly need to be aware of these potential dangers—but are they?

Sadly, the answer is usually no. CIOs and CISOs rarely find out until it's too late that their staff has been compromising security by disabling firewall features. It's not hard to understand why. IT executives spend most of their time interacting with other C-level executives on strategic issues and often delegate other decisions—even the management of critical security defenses—to subordinates. In addition, firewall configuration is considered a tactical decision and rarely rolls up beyond the IT-manager level. For their part, system administrators sometimes underestimate the risks involved and therefore don't include detailed firewall information in their status reports.

Remedying the situation begins with awareness. CIOs and CISOs should ask their staffs more detailed questions about how they are responding to performance problems. As executives become informed about what is really happening in their network, they can take more concrete actions discussed later in this report.

NGFWs Boost Throughput and Enhance Defenses

Despite the name, the next-generation firewall (NGFW) is not a new technology. First introduced in the mid-2000s, the first NGFWs combined the functionality of traditional firewalls—packet filtering, network address translation, URL blocking, and VPNs—with deep packet inspection (DPI), intrusion prevention (IPS), SSL and SSH inspection, reputation-based malware detection, and most importantly, application awareness.[4]

In recent years, the NGFW has evolved in several ways. Multi-core processor technology has pushed the performance bar ever higher, above 100 Gbps for top-of-the-line models. The practical impact of 100-Gpbs+ throughput is to eliminate the tradeoffs between security and network performance that plagued the earlier generation of NGFWs. Today's NGFWs also provide better protection against advanced threats, support high availability, and feature centralized management (see Figure 3).

Given these advances, it's hardly a surprise that CIOs and CISOs have wholeheartedly embraced the NGFW to the point that they represent 70% of all new firewalls purchases.[5] However, all NGFWs are not created equal, which puts more pressure on IT decision-makers to carefully evaluate vendor offerings against the organization's specific requirements and constraints. The following section presents recommendations for NGFW evaluation.

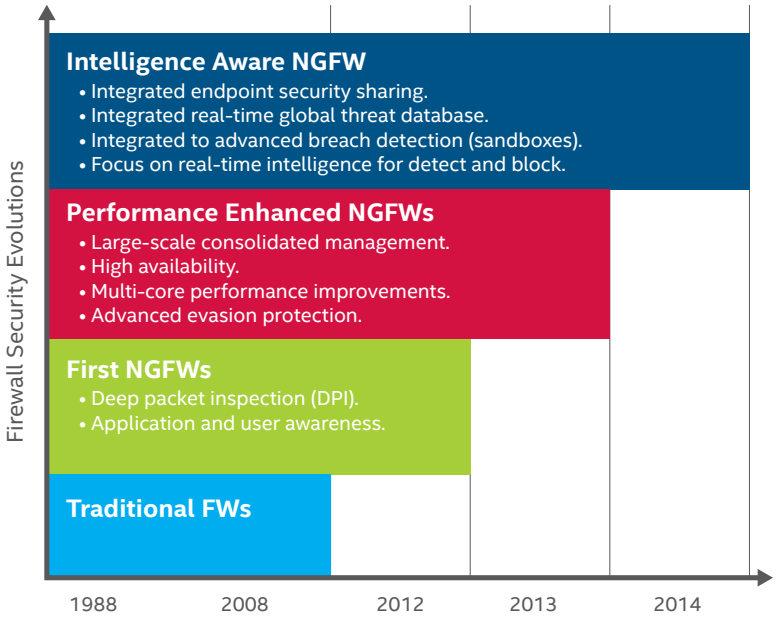

Figure 3. Evolution of the NGFW. Performance-enhanced NGFWs offer better protection against advanced threats, high availability, and centralized management. They also pave the way for intelligence-aware NGFWs, the next evolutionary step towards a fully connected security infrastructure. (Figure courtesy Gartner, Inc. 2014.)

Evaluate NGFWs under Real-World Conditions

When evaluating commercial NGFWs, CIOs and CISOs should mandate in-house testing under conditions that closely match their network's traffic volume and patterns, key protocols, and other parameters. While a comprehensive test plan is beyond the scope of this report, these tests should be included in every NGFW evaluation plan.

Throughput testing

Top-of-the-line NGFWs have maximum throughputs well above 100 Gbps, but that figure can dip to as low as 4 Gbps at peak loading. Establish a minimum threshold throughput value, with all the desired NGFW features enabled, that ensures acceptable application performance for your users.

Scalability testing

Deploying NGFWs in clusters for high availability is an increasingly common practice that is supported by most firewall manufacturers. However, NGFW models vary widely in the efficiency of their clustering models. Scalability testing should be performed on clusters of two, three, and four NGFWs. As a general guideline, adding another NGFW to the cluster should boost overall performance at least 75%.

Deep packet inspection testing

As the number-one cause of performance degradation in firewalls, DPI must remain operational at all times—turning it off even for occasional bursts of traffic is unacceptable. As a general rule of thumb, NGFWs should provide at least 10 Gbps throughput with DPI enabled.

Protocol-specific testing

Virtually every company is connected to the Internet and therefore susceptible to attack strategies targeting TCP and HTTP protocols. The NGFW should be able to process a high level of TCP and HTTP connections. A reasonable target value is at least 50,000 TCP/HTTP connections per second.

AET effectiveness testing

Most IT organizations lack the in-depth knowledge to design an effective AET test, so you should either require the vendor to provide AET expertise or rely on a professional AET testing tool (see Figure 4). While testing AET effectiveness may be a daunting task, skipping the test or relying on the manufacturer's data sheet can lead to an unwelcome surprise when the NGFW is actually deployed.

Figure 4. McAfee® Evader, a free software-based AET testing environment, can be downloaded at **http://evader.mcafee.com/**.

What CIOs/CISOs Can (and Should) Do Now

1: Focus staff attention on advanced threat defenses

As a crucial first step, CIOs and CISOs should push their direct reports to certify the adequacy of AET defenses using testing best practices and, if necessary, independent verification. They should also beef-up internal training programs to ensure that everyone in their IT organization understands advanced threats—including AETs—and knows how they can contribute to an effective defense.

At the strategic level, CIOs and CISOs need to include network resilience when they develop corporate and operational risk profiles. Where risk analyses identify vulnerabilities, those findings should inform investment decisions, in particular, procuring firewalls with demonstrated ability to detect AETs.

When evaluating firewalls, CIOs and CISOs should also consider the emerging class of NGFWs that Gartner calls "intelligence-aware," and are discussed later in this report.

2: Foster collaboration between operations and security

There is a common perception that network operations and security teams have conflicting priorities. Network administrators are expected to ensure access to applications—performance is their top priority. Security professionals must prevent data breaches and neutralize malicious activity, so they naturally favor tight security.

This way of thinking ignores the fact that everyone in IT—operations and security—have a common goal: helping the organization achieve its strategic goals. Meeting this goal requires both a high-performance network and security for vital information assets—any tradeoff between the two is detrimental.

CIOs and CISOs should foster collaboration between operations and security teams. When security experts and system administrators work together, they find solutions that do not compromise security. Our survey confirms that IT executives are moving in this direction. A full 89% of respondents have taken steps to integrate network and IT security staffs.

3: Upgrade to next-generation firewalls that can provide all the security you need without a performance penalty

Since the typical refresh cycle for security components is three years or more, accelerating NGFW upgrades may result in pushback from CFOs and other executives. Therefore, CIOs and CISOs must carefully build their case for upgrading with benefits such as mitigating risk, increasing IT staff and business productivity, and reducing infrastructure costs.

On the Horizon—the Intelligence-Aware NGFW

Just as application awareness has been a defining characteristic of NGFWs to date, intelligence awareness will be the hallmark of the emerging generation of NGFWs. Overcoming the limitations of siloed security information, intelligence-aware NGFWs integrate and share information with other security solutions such as endpoint clients, breach detection solutions (sandboxes), and global threat databases. The result? Real-time intelligence to detect advanced threats more effectively and block them before they result in a disastrous data breach.

Conclusion

The stakes have never been higher for CIOs and CISOs who are charged with protecting the organization's information assets. The combination of more elusive threats, overworked staff, risky operating procedures, and legacy tools has become a significant risk factor for a major data breach—something that executive staffs cannot afford to ignore. Technology advances in next-generation firewalls present an opportunity for CIOs and CISOs to get out in front of these challenges by aggressively advocating for next-generation firewalls that don't impact network performance and taking steps to transform their staffs into effective and efficient threat hunters. The security benefits alone justify upgrading to NGFWs, and when the financial benefits are added to the mix—it's really an easy decision. For more information on McAfee Next Generation Firewall, visit **www.mcafee.com/ngfw-hub**.

1. McAfee, unpublished research study
2. McAfee report, "Industry Experts Speak Out on Advanced Evasion Techniques," 2014. **http://www.mcafee.com/us/resources/reports/rp-whats-next-aet.pdf**
3. Ibid.
4. Margaret Rouse, "Next-generation firewall," January 2014. **http://searchsecurity.techtarget.com/definition/next-generation-firewall-NGFW**.
5. Gartner finding cited in "Next Generation Firewalls and Employee Privacy in the Global Enterprise," SANS Institute, September 21, 2014. **http://www.sans.org/reading-room/whitepapers/legal/generation-firewalls-employee-privacy-global-enterprise-35467**

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com