Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 9, Issue 6

Next Generation Firewalls: Protection and Performance

By Patrick Sweeney

Protection and performance should go hand in hand in terms of data and network security. However, until the introduction of Next-Generation Firewalls (NGFWs) organizations often had to compromise data throughput and productivity for security. But while NGFWs are good news for business, many organizations are unaware that they have "old" firewalls, ones that are barriers to productivity but not, unfortunately, barriers to the latest security threats.

A Quick History of Firewalls

First-generation firewalls of the 1980s provided packet filtering based upon criteria such as port, protocol and MAC/IP address, and operated at layers 2 and 3 of the OSI model. Second-generation firewalls of the '90s incorporated stateful packet inspection (SPI), which verified the state of inbound and outbound traffic based upon state tables, and operated at layers 2, 3 and 4. Then, third-generation firewalls of the past decade delivered processing power and broader capabilities, including deep packet inspection (DPI) of the entire packet payload, intrusion prevention, malware detection, traffic analytics, application control, and IPSec and SSL VPNs. Another development during the evolution of third-generation firewalls was Unified Threat Management (UTM), which extended the role of the traditional firewall into a product that not only guards against intrusion but performs content filtering, data leakage protection, intrusion detection, and anti-malware duties typically handled by multiple systems.

This worked well until the advent and mass adoption of Web 2.0 applications, mobile devices and mobile apps, all of which combined to create entirely new challenges for network security and productivity. Suddenly, bandwidth was being gobbled up by greedy Web applications and multimedia files. Simultaneously, the Web 2.0 and multimedia files became new and difficult to detect for existing and new malware and viruses. Enter the need for Next-Generation Firewalls.

Defining Next-Generation Firewall

An NGFW includes all standard capabilities found in a first-generation firewall, i.e., packet filtering, stateful packet inspection (SPI), network address translation (NAT), and high availability (HA). But it takes network security and performance to the next level through the combination and integration of innovations such as deep packet inspection (DPI), intrusion prevention systems (IPS) and application intelligence and control.

Gartner defines an NGFW as "an inline security control that implements network security policy between networks or different trust levels" as well as "a wire-speed integrated network platform that performs deep inspection of traffic and blocking of attacks."

At the minimum, an NGFW should include the following:

1. **Gateway Anti-Malware and Anti-Spyware Service.** This type of software inspects all email file attachments, FTP downloads and real-time applications such as IM and P2P for total file-based threat control. As a result, zero-day attacks are prevented with dynamically updated

databases and an extensive list of malware and virus signatures. And, because all threats are blocked at the gateway, users are completely prevented from downloading malware in the first place.

2. **Intrusion Prevention.** Application vulnerabilities, buffer overflows and blended threats can open up your network to exploits, making intrusion prevention a necessary technology. An NGFW can scan all network traffic for worms, Trojan horses, software vulnerabilities, backdoor exploits, and other types of malicious attacks. Utilizing a comprehensive signature database, the Intrusion Prevention Service (IPS) engine protects against an array of network-based application vulnerabilities and exploits. Deployed to protect against both internal and external threats, it can monitor the network for malicious or anomalous traffic, then block or log traffic based on predefined and automatically updated conditions. By focusing on known malicious traffic, Dell SonicWALL IPS decreases false positives while increasing network reliability and performance.

3. **Application Intelligence, Control and Visualization/Deep Packet Inspection.** Application intelligence is a foundational component of a Next-Generation Firewall. It is what enables the identification of individual applications within network traffic, ideally irrespective of port, protocol or evasive tactic. Coverage should be both broad and deep in terms of the variety of applications and the specific functions within them that can be distinguished, and is typically based on the presence of an extensive application-signature library and the resources to maintain it. The Application Control is a critical tool in determining who gets access to which applications and by which priority; this control and load-balancing tool is instrumental in maintaining network performance and ensuring that business-critical apps and data aren't playing second fiddle to the latest viral YouTube video. One of the most impactful advances on the security side that NGFWs provide concerns the deep packet inspection; it is also one that should be investigated with extra care when upgrading. Our approach is through patented Reassembly-Free Deep Packet Inspection™ (RFDPI), which scans every packet, across every protocol and interface, to identify and control over 3,500 applications and individual application functions. This approach has no reliance, dependence or limitation relative to the ports and protocols being used, and can optionally be extended to SSL-encrypted traffic as well. The productivity as well as the security advantages are compelling here because RFDPI can maintain granular control over applications, prioritize or throttle bandwidth and deny website access through its constantly expanding signature database, which currently recognizes over 3,500 applications and millions of malware threats.

A key consideration when upgrading to NGFWs is performance.

A key consideration when upgrading to NGFWs is performance. While the increased levels of inspection and protection are critical, so is the expectation of multigigabit-speed throughput performance; NGFWs must deliver massively scalable throughput if they are to enable the highest-performance networks. Dell SonicWALL, for example, has implemented a multicore architecture to accelerate the processing of network traffic. Businesses should not — and cannot — be willing to compromise protection and visibility for performance.

NGFW Adoption

Given the threat environment out there, Gartner and other experts predict that the enterprise will certainly be the first to adopt the NGFW, as part of their existing refresh cycles. But the fact remains that organizations large and small should not tolerate older firewalls that may be vulnerable to malware that could inflict great harm on their business. If that sounds alarmist, then take a look at these recent statistics:

A 2012 Cost of Cyber Crime Study conducted by the Ponemon Institute found that the average annual cost of cybercrime for U.S. organizations was $8.9 million in 2012. That amount is 6 percent higher than the average cost in 2011 — $8.4 million — and a 38 percent increase over the 2010 average of $6.5 million. The report also shows a 42 percent increase in the number of cyberattacks in 2012; this year organizations have experienced an average of 102 successful attacks per week, compared to 72 per week last year and 50 per week in 2010.

The most costly cybercrimes continue to be those caused by malicious code, denial of service, stolen or hijacked devices, and malevolent insiders. When

combined, these account for more than 78 percent of annual cybercrime costs per organization.

IT organizations have many options these days in selecting an NGFW, as one size doesn't fit all. That said, the first step is to know how an NGFW differs from its predecessors and to ascertain how you can use one to your organization's advantage. The next is to choose an NGFW that will scale to your business or institution's size as well as provide ease of use and implementation so that it does the job you need it to — without compromise.

The most costly cybercrimes continue to be those caused by malicious code, denial of service, stolen or hijacked devices, and malevolent insiders.