Enterprises today rely on an ever-expanding array of advanced technology options to heighten productivity, taking advantage of Web 2.0, real-time collaboration, instant messaging, voice over IP (VoIP), streaming media, teleconferencing, and mission-critical cloud-based applications. These technologies play a significant role in advancing business and organizational outcomes, but employees may also run unknown and untrusted applications during the course of the workday. As a result, IT leaders must continue to find ways to increase productivity, security, and compliance while containing costs.

Mission-critical applications need bandwidth prioritization while other applications must be throttled or completely blocked. Moreover, enterprises cannot rely on the low level of security provided by legacy stateful packet inspection (SPI) firewalls, nor can they tolerate the network bottlenecks associated with some next-generation firewalls.

Protection and performance can go hand-in-hand for next-generation firewalls. Real-time deep packet inspection helps Dell™ SonicWALL™ SuperMassive™ firewalls meet security demands in a fast-paced world of constant Web access and cloud-based computing.

Advancing network security and performance

By Patrick Sweeney
Performance is an essential consideration when determining how to address security challenges.

Securing the network
Technology analyst firm Gartner defines an NGFW as “a wire-speed integrated network platform that performs deep inspection of traffic and blocking of attacks.” In basic terms, an NGFW integrates deep packet inspection (DPI) firewall technology with intrusion prevention service (IPS) and application intelligence and control.

Outdated NGFWs pose a serious security risk to organizations because they may fail to fully inspect the data payload of network packets. In addition, some firewalls buffer downloaded files and then inspect them for malware. This proxy or assembly method may introduce significant latency. With this type of approach, memory is consumed until it runs out, resulting in the firewall either passing traffic through unscanned—which can compromise security—or blocking all traffic until memory is freed.

One alternative is real-time inspection over an NGFW. By effectively combining real-time DPI technology with high-performance multicore architecture, NGFWs are now capable of delivering exceptional application intelligence and control, intrusion prevention, malware protection, and Secure Sockets Layer (SSL) inspection at multigigabit speeds.

Achieving effective protection
By combining a multicore architecture with Dell SonicWALL Reassembly-Free Deep Packet Inspection™ (RFDPI) technology, the SonicWALL SuperMassive E10000 Series NGFW enables effective security and control with tightly integrated intrusion prevention, malware protection, and application intelligence. RFDPI is designed to scan any number of simultaneous files of unlimited size in real time across any port, without security or performance degradation—as a result, minimizing the chance that infected files will slip through undetected when the firewall is under heavy load. In addition, it can apply security and application-control technologies to SSL-encrypted traffic to help ensure that it does not become a malware vector in the network.

RFDPI is designed to match within files, attachments, and certain compressed archives, regardless of size, and to transform as needed to perform normalization pattern matching. RFDPI also helps identify malicious code within parts of files and emerging variant mutations, as well as block compressed files that have been password protected or contain embedded macros. Moreover, RFDPI is designed to scan all ports and protocols to detect and block known viruses and malware, regardless of the transmitting protocol.

Validating firewall performance
To select a suitable NGFW, best practices suggest obtaining verification of its protection and performance from independent security product testing or certification sources, such as NSS Labs. Recent NSS Labs tests on NGFWs provided detailed performance and security effectiveness data across a broad spectrum of devices. According to the lab’s 2012 Next Generation Firewall Security Value Map, the Dell SonicWALL SuperMassive E10800 appliance was one of three NGFWs—out of seven evaluated—to earn NSS Labs’ highest rating of “Recommend.”

NSS Labs rated the SuperMassive E10800 appliance’s stability and reliability to be excellent, with 100 percent scores in firewall enforcement, application control, and identity awareness. The SuperMassive E10800 successfully passed 18.9 Gbps of inspected traffic. Findings stated that the firewall “offers some highly evolved features suitable for large enterprise and multitenant service providers.”

Network World magazine also evaluated NGFWs in a Clear Choice Test. Out of four tested, the SuperMassive E10800 topped the performance test; it “moved traffic the fastest, even when forwarding SSL traffic. In multiple cases, it maxed out the capabilities of our test bed. For example, when doing application of clear text traffic, it moved traffic at or near 20 Gbps.”

Defending against threats
Critical Web- and cloud-based applications help boost productivity but can also introduce security challenges. Organizations can defend their networks against emerging threats while optimizing network performance by using NGFWs. As verified by independent testing, Dell SonicWALL SuperMassive NGFWs provide in-depth protection and enterprise performance levels that help overcome the limitations of traditional firewall solutions.

Author
Patrick Sweeney is executive director at Dell, where he oversees the Dell SonicWALL network security, content security, business continuity, and policy and management product lines.

Learn more
NSS Labs Next Generation Firewall Security Value Map:
sonicwall.com/nss

Dell SonicWALL SuperMassive E10000 Series:
sonicwall.com/supermassive

1 “Defining the next-generation firewall,” by John Pesceatore and Greg Young, Gartner RAS Core Research Note G00171540, R3210 04102010, Gartner, Inc., October 12, 2009.
