Executive Summary

Enterprises must constantly balance network and data vulnerability against deployment of new apps and new equipment. And with the rise of mobility, remote access, and cloud-based resources, they've got their hands full securing everything and everyone who's connected from inside and outside their corporate environment.

Outdated firewalls pose a serious security risk to organizations since they fail to inspect the data payload of network packets in multi-application environments. Next-Generation Firewalls (NGFWs) combine multi-core architecture with real-time Deep Packet Inspection (DPI) to fulfill the protection and performance demands of today's enterprise networks.

With NGFWs, organizations should not have to sacrifice throughput and productivity for security. Many vendors tout Stateful Packet Inspection (SPI) speeds only, but the real measure of security and performance is deep packet inspection throughput and effectiveness.
Table of Contents

Introduction .................................................................................................................. 3
Packet Inspection and the Evolution of Firewalls ......................................................... 4
NGFW: Industry Definition and Feature Requirements .................................................. 5
How to Achieve Maximum Protection and Minimum Latency with NGFW Hardware ...... 6
Dell SonicWALL NGFWs: Hardware overview ............................................................... 7
NSS Labs Independent Testing Results ......................................................................... 11
Conclusion .................................................................................................................... 12
Introduction

Organizations are suffering from application chaos. Network communications have expanded to include real-time collaboration tools, Web 2.0 applications, instant messenger (IM) and peer-to-peer applications, Voice over IP (VoIP), streaming media, and teleconferencing, each presenting conduits for potential attack. Many organizations cannot differentiate applications in use on their networks or those with legitimate business purposes from those that are potentially wasteful or dangerous.

Today, organizations need to deliver critical business solutions, while also contending with employee use of wasteful and often dangerous web-based applications. Critical applications need bandwidth prioritization while social media and gaming applications need to be throttled or completely blocked. Moreover, organizations can face fines, penalties and loss of business if they are in noncompliance with security mandates and regulations.

In addition to these challenges, IT needs to make sure that traffic is thoroughly scanned with minimal latency for optimal throughput.

To meet these requirements, multi-gigabit throughput rates have become standard for NGFWs.

The question that arises is this, what does it take for security hardware to meet the demands for deep packet inspection and low latency?
Packet Inspection and the Evolution of Firewalls

First generation firewalls provided packet filtering based upon criteria such as port, protocol, and MAC/IP address, and operated at layer 2 and 3 of the Open Systems Interconnection OSI model.

Second generation firewalls added 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 of the OSI model.

Third-generation firewalls provided more processing power and broader capabilities, including deep packet inspection (DPI) of the entire packet payload, intrusion prevention, malware detection, gateway antivirus, traffic analytics, application control, IPSec and SSL VPN.

Unified Threat Management (UTM) represented the next trend in the evolution of the traditional firewall into a product that not only guards against intrusion, but also performs content filtering, data leakage protection, intrusion detection and anti-malware duties typically handled by multiple systems.

Next Generation Firewalls (NGFWs) inspect the payload of packets and match signatures for nefarious activities, all on the fly. Administrators can create very granular permit and deny rules for controlling specific applications and web sites, and mine the traffic analytics to perform capacity planning, troubleshoot problems, or monitor what individual employees are doing throughout the day. Today’s firewalls operate at layers, 2, 3, 4, 5, 6 and 7 of the OSI model.
NGFW: Industry Definition and Feature Requirements

Gartner defines an NGFW as “a wire-speed integrated network platform that performs deep inspection of traffic and blocking of attacks.” At minimum, Gartner states that an NGFW should provide:

- Non-disruptive in-line bump-in-the-wire configuration
- Standard first-generation firewall capabilities, e.g., network address translation (NAT), stateful protocol inspection (SPI), virtual private networking (VPN), etc.
- Integrated signature based IPS engine
- Application awareness, full stack visibility, and granular control
- Capability to incorporate information from outside the firewall, e.g., directory-based policy, blacklists, white lists, etc.
- Upgrade path to include future information feeds and security threats
- SSL decryption to enable identifying undesirable encrypted applications

Next Generation Firewalls should also provide the following features.

**Legacy compatibility**

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).

**Integrated intrusion prevention systems (IPS)**

Organizations need best-in-class intrusion prevention without the complexity of managing separate appliances, GUIs, and deployments. NGFWs with IPS capabilities deliver enterprise class resistance to evasion, powerful context and content protection capabilities as well as comprehensive threat protection and application control in a single integrated device.

**Application intelligence and control**

Application awareness and control includes protocol-level enforcement, full-stack visibility with granular application control, and the ability to identify applications regardless of port or protocol being utilized.

**Extra firewall input**

User-ID awareness enables administrators to enforce application policies based on AD user/group (without having to trace IP address to user ID), adding insight into usage and traffic.

**Adaptability**

Another important capability of NGFWs is dynamic adaptation to changing threats. Vendors should constantly update their devices with new signatures to stop threats and stay on top of the evolving malware landscape.

**Payload scanning and performance**

All of the above requirements demand full payload scanning at optimal throughput rates in order to avoid having to sacrifice security for performance.

---

1: Defining the Next-Generation Firewall,” Gartner RAS Core Research Note G00171540, John Pescatore, Greg Young, 12 October 2009, R3210 04102010
How to Achieve Maximum Protection and Minimum Latency with NGFW Hardware

In today's enterprise organizations, protection and performance go hand-in-hand. Organizations can no longer tolerate the reduced security provided by legacy SPI firewalls, nor can they tolerate the network bottlenecks associated with some NGFWs. Any delays in firewall or network performance can degrade quality in latency-sensitive and collaborative applications, which in turn can negatively affect service levels and productivity. To make matters worse, some IT organizations even disable functionality in their network security solutions to avoid slowdowns in network performance.

A NGFW must perform several protection- and performance-based functions in order to meet the demands of today's enterprise networks.

Scanning and controlling all content
Organizations large and small, in both the public and private sectors, face new threats from vulnerabilities in commonly-used applications. Malware lurks in social networks. Meanwhile, workers use business and home office computers for online blogging, socializing, messaging, videos, music, games, shopping and e-mail.

Application intelligence and control
Streaming video, peer-to-peer (P2P), and hosted or cloud-based applications expose organizations to potential infiltration, data leakage and downtime. In addition to introducing security threats, these applications drain bandwidth and productivity, and compete with mission-critical applications for precious bandwidth. Importantly, enterprises need tools to guarantee bandwidth for critical business relevant applications and need application intelligence and control to protect both inbound and outbound flows of traffic, while ensuring the velocity and security to provide a productive work environment.

DPI requires high-performance NGFWs
Outdated proxy designs that reassemble content using sockets bolted to anti-malware engines are plagued with inefficiencies. The overhead of memory thrashing leads to high latency, low performance, and file size limitations. Outdated DPI methods gather and store traffic in memory to scan it. When using this proxy or assembly approach, memory is consumed until it runs out, resulting in a firewall either passing traffic through un-scanned (unacceptable) or blocking all traffic until memory is freed up. Moreover, real-time applications are negatively impacted when unacceptable latency is introduced.
Dell SonicWALL NGFWs: Hardware Overview

By combining high-performance multi-core architecture and patented reassembly-free DPI technology (RFDPI), Dell SonicWALL Next-Generation Firewalls deliver industry leading application intelligence and control, intrusion prevention, malware protection, and SSL inspection at multi-gigabit speeds.

RFDPI vs. Buffering
Traditionally, deep packet inspection of large files requires buffering the payload due to the limited processing power, memory, or available storage of the security appliance. This introduces latency to the network, sometimes to the point where inspection was bypassed in the interest of network performance.

To overcome these challenges to provide real-time, full packet DPI capabilities without sacrificing performance, The Dell SonicWALL RFDPI engine uses a combination of complex pattern matching, heuristics, correlation, advanced real time decision methodologies, normalization (X, Y, Z and more) yet still maintains extremely high performance, low latency, and high efficiency, regardless of file size.

How the Dell SonicWALL RFDPI Engine Works
Dell SonicWALL’s RFDPI engine is capable of doing much more than simple pattern matching. When creating signatures, packet types are taken into account as well. If it is determined that a particular packet type (for example encrypted ICMP) is being utilized exclusively by malicious software, that file would be deemed malicious as well. The technology looks for the elements in the flow that contain harmful code, and can parse through the unimportant bits.

Further, RFDPI is capable of parsing magic numbers (integer values used to determine file formats) and then compare them against predefined lists to compare actual versus expected file content values. This allows the engine to identify new variants of malware which may be disguised as innocent files.

2: U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361
Identifying new mutations of malware
Much of the signatures employed by Dell SonicWALL firewalls are custom written to look for specific code fragments common to malware families. This means that RFDPI does not need to look for an entire file or executable to determine if a flow is malicious, and allows it to identify new mutations in malware. This provides an additional layer of protection against “commercial” malware utilized by the underground economy.

Automating DPI with heuristics
The RFDI engine offers further protection from nefarious activity by utilizing heuristic (anomalous experience-based) techniques reducing the number of incidents resulting in labor-intensive investigations to search through thousands of entries in system logs. Intelligent policy creation allows for heuristic features such as blocking compressed files that have been password protected or blocking MS-Office files which contain Visual BASIC macros.

Application intelligence and control
Dell SonicWALL Application Intelligence and Control leverages RFDPI to scan every packet to identify applications in use and who is using them. It maintains a signature database to protect networks automatically and seamlessly.

Thoroughly scanning all network traffic, it provides complete application intelligence and control, regardless of port or protocol, by identifying application traffic and users.

Add on: Deep Packet Inspection for SSL
Available as an optional add-on license on specific models, Deep Packet Inspection for SSL (DPI SSL) extends protection to the SSL encrypted traffic, enabling enhanced compliance, content filtering, and data leak prevention, as well as eliminating another vector for malware. Encrypted traffic is decrypted, inspected and re-encrypted transparently to the user and can be configured for both inbound and outbound connections.

Simplified Real-Time Monitoring for IT
The Dell SonicWALL Application Flow Monitor provides real-time graphs of application activity allowing administrators to modify policies to increase network productivity. In addition, the solution provides NetFlow/IPFIX with extensions exports for additional off-the-box traffic analysis and visualization.
Advantages of multi-core architecture in NGFW performance

Dell SonicWALL's multi-core hardware architecture has two key advantages to accelerate the processing of network traffic. The first advantage is that Cavium CPUs are custom built to 'understand' network communications at the hardware level.

The second advantage is the ability to parallel process data streams across multiple cores. Dell SonicWALL's multi-core architecture enables each CPU to process a portion of network packets simultaneously in parallel with other CPUs, making optimal use of available processor cycles.
This optimal combination offers high-performance and efficient solutions for packet, content and security processing.

A multi-core architecture maximizes performance and scalability, while minimizing power consumption, by combining hardware acceleration with high performance multi-core processor architecture techniques.

For large datacenters where space and temperature are important factors, the Dell SonicWALL SuperMassive™ E10000 Series firewalls are designed with power, space, and cooling (PSC) in mind, thus providing the leading Gbps/Watt ratio in the industry for application control and threat prevention.

**Why multi-core processors are ideal for DPI performance**

Other vendors have chosen general-purpose processors and separate security co-processors—a solution that does not scale. Still others have chosen to design and build ASIC (Application-Specific Integrated Circuits) platforms. Traditional single-processor and ASIC solutions cannot keep up with evolving complex attacks in real time from both inside and outside the network perimeter due to the increased inspection demands required.

General-purpose processors rely on a single processing CPU for handling all functions. They do not provide any type of security acceleration, and usually require additional third-party security co-processors for the necessary security acceleration. General-purpose processors rely on a single processing CPU for handling all functions. They do not provide any type of security acceleration, and usually require additional third-party security co-processors for the necessary security acceleration. Since a general purpose processor runs at a higher clock speed and requires additional co-processors, it is less energy efficient during general operation. Additionally, general-purpose processor solutions are limited by bus speeds between the general-purpose processor and security co-processor.

General-purpose processors can also be comparatively limited in memory bandwidth, resulting in slower packet processing. Overall, general-purpose single processor designs offer a less-than-ideal hardware platform for high-performance DPI on NGFWs.

ASIC platforms have inherent design challenges and limitations when used in network security appliances. One is that it often prohibits the vendor’s ability to field-upgrade the ASIC micro code to deal with an evolving security landscape; the lack of available microcode space may prevent the vendor to deal with changing protocols, upgraded standards or bugs without significant performance degradation.
This means there is no guarantee the customer can upgrade the appliance to deal with future networking needs.

**NSS Labs Testing of Dell SonicWALL SuperMassive Line**

NSS Labs is a global leader in independent security product testing and certification. Recently evaluated in the NSS Labs 2013 Next-Generation Firewall Security Value Map™, the Dell SonicWALL SuperMassive™ E10800 (running SonicOS 6.0) earned the highest rating of ‘Recommend’ from NSS Labs for the second year in a row.

**NSS Labs NGFW analysis criteria states:**
“A Next-Gen Firewall must provide granular control based upon applications, not just ports. This capability is needed to re-establish a secure perimeter where unwanted applications are unable to tunnel over HTTP/S. As such, granular application control is a requirement of Next-Gen Firewalls since it enables the administrator to define security policies based upon applications rather than ports alone.”

**Breakdown of NSS Labs testing results**
The SuperMassive line of NFGW appliances demonstrated one of the highest security effectiveness ratings, and scored 100 percent in the stability and reliability, firewall, application control, and identity awareness tests. Resistance to known evasion, obfuscation, and fragmentation techniques were also perfect, with the Dell SonicWALL NGFW achieving a 100 percent score across the board in all related tests.

The SuperMassive E10800 was tested and rated by NSS Labs at 16.6 Gbps of Next-Gen Firewall throughput, and was able to scale into multi-gigabit throughput in the computationally expensive SSL decryption tests while maintaining extremely competitive TCO.
The SuperMassive E10800 earned scores of 100 percent for “Block Unwanted Applications” and for “Block Specific Action.” NSS Labs testing found that Dell SonicWALL SuperMassive E10800 correctly enforced complex outbound and inbound policies consisting of multiple rules, objects and applications. SuperMassive is capable of enforcing application control on every port, including non-standard ports for a particular application.

Moreover, as separately demonstrated in the 2012 NSS Labs Security Value Map (SVM) for IPS the SuperMassive E10800 Next-Generation Firewall with integrated IPS not only garnered the NSS Labs “Recommend” rating but also outperformed many dedicated IPS vendors. As stated by NSS Labs, the “Resistance to known evasion techniques was perfect, with the Dell SonicWALL SuperMassive SonicOS 6.0 achieving a 100% score across the board in all related tests. IP fragmentation, TCP stream segmentation, RPC fragmentation, URL obfuscation, HTML Evasion and FTP evasion all failed to trick the product into ignoring valid attacks. Not only were the fragmented and obfuscated attacks blocked successfully, but all of them were also decoded accurately.”

Conclusion

Designed to meet the needs of large enterprise, government, university, and multi-tenant/service providers, the Dell SonicWALL SuperMassive E10000 Series delivers scalability, reliability, and deep security at multi-gigabit speeds. Utilizing the Dell SonicWALL RFDPI engine to scan every byte of every packet, this single integrated solution delivers full content inspection of the entire stream and superior intrusion prevention, malware protection, application intelligence, control and real-time visualization, and inspection for SSL encrypted sessions while ensuring high performance and low latency.

The SuperMassive 9000 Series Next-Generation Firewall platform brings that same high level of protection and performance to the enterprise in a highly efficient yet powerful solution. Designed for scalability, reliability, and deep security at multi-gigabit speeds, it offers ultimate security with uncompromising performance.

Dell SonicWALL Next-Generation Firewalls, including the Dell SonicWALL TZ 215, Network Security Appliance (NSA) Series, E-Class NSA Series, and SuperMassive 9000 and E10000 Series, overcome the limitations of traditional firewall solutions and enable enterprise businesses to scale their network security to meet the demands of emerging threats, while ensuring the network performance meets key business objectives.