Why protection and performance matter

By Daniel Ayoub, CISSP, CISM, CISA

Next-Generation Firewalls combine multi-core architecture with real-time Deep Packet Inspection to fulfill the protection and performance demands of today's enterprise network

Abstract

Protection and performance go hand-in-hand for Next-Generation Firewalls (NGFWs). Organizations should not have to sacrifice throughput and productivity for security. Outdated firewalls pose a serious security risk to organizations since they fail to inspect data payload of network packets. Many vendors tout Stateful Packet Inspection (SPI) speeds only, but the real measure of security and performance is deep packet inspection throughput and effectiveness. To address this deficiency, many firewall vendors adopted the malware inspection approach used by traditional desktop anti-virus: buffer downloaded files, then inspect for malware. This method not only introduces significant latency and but also poses significant security risks since temporary memory storage can limit the maximum file size. Independent NSS Lab tests demonstrate that the Dell™ SonicWALL™ SuperMassive™ E10800 Next-Generation Firewall incorporating multi-core architecture and Reassembly-Free Deep Packet Inspection® (RFDPI) overcome these limitations to provide enterprises with both extremely high-levels of protection and performance that they require.

Defining Next-Generation Firewall

In basic terms, a Next-Generation Firewall (NGFW) leverages deep packet inspection (DPI) firewall technology by integrating intrusion prevention systems (IPS), and application intelligence and control.

Industry definitions

Gartner defines an NGFW as "a wire-speed integrated network platform that performs deep inspection of traffic and blocking of attacks."[1] 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

The evolution of Next-Generation Firewalls

Earlier-generation firewalls

First generation firewalls of the 1980s provided packet filtering based upon criteria such as port, protocol and MAC/IP address, and operated at layer 2 and 3 of the OSI model. Second generation firewalls of the 1990s incorporated stateful packet inspection (SPI), which verified that 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 of the past decade have more processing power and broader capabilities, including deep packet inspection (DPI) of the entire packet payload, intrusion prevention, malware detection, gateway anti-virus, 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

Web 2.0 applications (e.g., Salesforce.com, SharePoint, and Farmville) now run all over TCP port 80 as well as encrypted SSL (TCP port 443). Today's NGFWs inspect the payload of packets and match signatures for nefarious activities such as known vulnerabilities, exploit attacks, viruses and malware all on the fly. DPI also means that administrators can create very granular permit and deny rules for controlling specific applications and web sites (example: Yahoo instant messenger-chat is allowed but not file transfers). Since the contents of packets are inspected, exporting all sorts of statistical information is also possible, meaning administrators can now easily mine the traffic analytics

[1] "Defining the Next-Generation Firewall," Gartner RAS Core Research Note G00171540, John Pescatore, Greg Young, 12 October 2009, R3210 04102010

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 feature requirements

The following are feature requirements for Next-Generation Firewalls:

Legacy features

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 IPS

Effective intrusion prevention systems require advanced capabilities to combat evasion techniques and enable scanning and inspection of inbound and outbound communications to identify malicious or suspicious communications and protocols.
For effective threat protection as well as intrusion prevention, organizations need best-in-class firewall and intrusion prevention, without the complexity of managing separate appliances, GUI's, 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 the dynamic adaptation to changing threats. Dell SonicWALL constantly updates 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.

Performance

In order to achieve the highest return on investment (ROI) for bandwidth services and optimize an organization's productivity level, while still ensuring maximum security, 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. Dell SonicWALL NGFW solutions can improve performance significantly by applying patented Dell SonicWALL RFDPI[2] technology to enable DPI without buffering and packet reassembly. From a hardware perspective, Dell SonicWALL NGFWs can also maximize throughput by incorporating parallel processing over advanced multi-core architecture.

Why you need a Next-Generation Firewall

The SPI generation of firewalls addressed security in a world where malware was not a major issue and web pages were just documents to be read. Ports, IP addresses, and protocols were the key factors to be managed. But as the Internet evolved, the ability to deliver dynamic content from the server and client browsers introduced a wealth of applications we now call Web 2.0.

SPI does not inspect the data portion of the packet and hackers effectively exploit this fact. To address the new threats, SPI firewall vendors incorporated traditional malware protection and methods that were used on file servers and PCs. The technique was a band-aid fix to add malware protection on an SPI firewall, as it had two significant flaws: latency and complexity.

The first flaw was the introduction of latency while the file is buffered with file size limitations. Firewall vendors have worked around this issue by sending keep-alive packets to prevent this, yet the overall effect is the introduction of latency. The use of memory to buffer files for inspection causes not only additional latency but also a space issue which is addressed by limiting the overall file size to a preset amount (generally 100MB). The use of the Internet is growing and sharing of larger files is increasing; hybrid SPI/malware detection technology does not scale.

The second flaw was that traditional point solutions were difficult to deploy, manage and update, increasing operating complexity and overhead costs. Sophisticated malicious attacks penetrate traditional stateful packet inspection products. These solutions simply do not provide sufficient, timely and unified protection against increasingly complex threats.

To overcome these flaws, Dell SonicWALL offers the most effective, highest-performance NGFW solutions available today. Recently, NSS Labs conducted independent testing of the Dell SonicWALL's Next-Generation Firewall at their labs facility in Austin, Texas. Dell SonicWALL's SuperMassive E10800 running SonicOS 6.0 earned the highest rating of 'Recommend'

[2] U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361

from NSS Labs for two consecutive years. This proven SonicOS architecture is at the core of every Dell SonicWALL firewall. The results of those tests are explored further at the end of this paper.

What the enterprise requires

Organizations are suffering from application chaos. Network communications no longer rely simply on store-and-forward applications like email, but 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 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.

Protection and performance

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 the 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.

Scanning and controlling all content

Organizations large and small, in both the public and private sector, 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 email.

Application intelligence and control

Applications such as 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 NGFW

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 introduced.

The Dell SonicWALL approach

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

Dell SonicWALL Next-Generation Firewalls, featuring Dell SonicWALL's patented[3] RFDPI technology, provide security and control for organizations of all sizes with tightly integrated intrusion prevention, malware protection, and application intelligence, control and real-time visualization. Dell SonicWALL NGFW solutions scan 100 percent of traffic and massively scale to meet the needs of the highest-performance networks. Dell SonicWALL Application Intelligence, Control and Visualization lets administrators control and manage both business and non-business related applications to enable network and user productivity.

Dell SonicWALL Next-Generation Firewalls can scan files of unlimited size across any port and without security or performance degradation. The number of simultaneous files or network streams does not limit Dell SonicWALL Next-Generation Firewalls, so infected files do not have a chance to slip through undetected when the firewall is under heavy load. In addition, Dell SonicWALL Next-Generation Firewalls can apply all security and application control technologies to SSL encrypted traffic, ensuring that this does not become a new malware vector into the network. Dell SonicWALL Next-Generation Firewalls are FIPS 140-2 and Common Criteria (EAL 4 Augmented) certified. Dell SonicWALL products are available on GSA Schedule, NASA SEWP IV and other Federal contract vehicles.

[3] * U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

RFDPI vs. buffering

IT administrators selecting a deep packet inspection firewall need to be aware that some devices have limited processing power, memory and storage making inspection of large size files for threats impossible for most vendors without buffering the payload which introduces latency, or having to bypass inspection entirely rendering the security moot.

Why the Dell SonicWALL approach is better

Dell SonicWALL RFDPI overcomes these challenges to provide real-time, full packet DPI capabilities without sacrificing performance or security. The 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.

Dell SonicWALL multi-core architecture

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

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, which inefficiently increases development complexity. Since a general-purpose processor runs at a higher clock speed and requires additional co-processors, it is less energy efficient, and consumes more power 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.

While ASIC platforms have a place in high-speed packet forwarding, they have inherent design challenges and limitations when used in network security appliances. One particularly significant challenge is the inherent limitation in a vendor's ability to field-upgrade the ASIC micro code to deal with the evolving security landscape. With ASIC solutions, the lack of available microcode space may prevent the vendor from adding new functionality required to deal with changing protocols, upgraded standards or bugs without significant performance degradation. This limits ASIC-based security appliances, as there is no guarantee the customer can upgrade the appliance to deal with future networking needs. Moreover, ASICs are mainly used for SPI, as they perform very slowly for DPI.

Dell SonicWALL Reassembly-Free Deep Packet Inspection Engine

Dell SonicWALL RFDPI can match within files, attachments and certain compressed archives, regardless of size, and it transforms as needed to perform normalized pattern matching. The underlying algorithm of Dell SonicWALL RFDPI applies deterministic finite automata (DFAs) to provide deterministic, low latency matching.

RFDPI enables Dell SonicWALL Next-Generation Firewalls to extend their protection to block malware. Most competitive solutions available are capable of scanning only six protocols (HTTP, SMTP, IMAP, POP3, FTP and SMB), providing a false sense of security since any malicious traffic transmitted via any other protocol is not subject to inspection. Only Dell SonicWALL RFDPI scans every packet on all ports and protocol every time with comprehensive anti-x technology to allow for detection and blocking of known viruses and malware regardless of the transmitting protocol.

However, Dell SonicWALL's RFDPI engine is capable of doing much more than simple pattern matching. When creating signatures, data such as 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 based on this alone. Dell SonicWALL's intelligent malware detection technology looks for the elements in the flow that contain harmful code and can parse through the benign envelope of unimportant bits. Further, when it comes to determining vulnerabilities as part of file scanning, 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. These techniques allow the Dell SonicWALL RFDPI engine to identify new variants of malware, which may be disguised as innocent files, yet have never been seen before.

Much of the signatures employed by Dell SonicWALL firewalls are custom written to look for specific code fragments common to malware families rather than individual variants. This means that RFDPI does not need to look for an entire file or executable to determine if a flow is malicious. Instead, RFDPI can identify the malicious parts of malware that are contained in new mutations thus, providing an additional layer of protection against a large part of the "commercial" malware utilized as part of an underground economy.

Dell SonicWALL's 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.

In addition, Dell SonicWALL Application Intelligence and Control leverages RFDPI to scan every packet to identify applications in use and who is using them. Dell SonicWALL 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.

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.

Administrators must also be able to visualize application traffic to control network use and to adjust network policy based on critical observations. 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.

Third-party validation testing

Why you should test your infrastructure

According to the 2013 NSS Labs Security Value Map™, many Next-Generation Firewall products have demonstrated mixed results. Recent NSS Labs group tests provide detailed performance and security effectiveness data across a broad spectrum of devices in this increasingly crowded market to enable potential purchasers to make informed decisions.

The validation of NSS Labs

NSS Labs is a global leader in independent security product testing and certification. Their analysis is known as one of the industry's most comprehensive, real-world tests to date. The NSS Labs Next-Generation Firewall Security Value Map™ depicts some of their most important findings, charting Block rates (including overall protection, evasions, leakage and security stability) and Price per Protected Mbps. Gartner has recognized the value of NSS Labs certifications by adding them to the short list of criteria for products to achieve ranking in the Gartner Magic Quadrant for Network IPS.

Since 1991, NSS Labs has led the information security research and testing communities, providing unique and valuable information to IT decision-makers.

NSS Labs test results

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.

The SuperMassive 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 was also perfect, with the Dell SonicWALL Next-Gen Firewall 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.

NSS Labs analysis 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." 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

As verified by independent testing, a multi-core architecture supporting Reassembly-Free Deep Packet Inspection can provide protection-in-depth and enterprise performance levels. The SonicOS architecture is at the core of every Dell SonicWALL firewall from the TZ Series to the SuperMassive E10800, so organizations can choose from an entire proven line which massively scales to meet the needs of the highest performance networks.

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 to meet key business objectives.