Achieve Deeper Network Security and Application Control

Dell Next-Generation Firewalls

Abstract

Next-generation firewalls (NGFWs) have emerged to revolutionize network security as we once knew it. Yet to safeguard an organization from today's ever-evolving threats, NGFWs must be able to deliver an even deeper level of network security. Not only must they ensure that every byte of every packet is inspected but also they must maintain the high performance and low latency that busy networks require. In addition, they must combine high-performance SSL decryption and inspection, an intrusion prevention system (IPS) that features sophisticated anti-evasion technology, granular control over and visibility into application and user activity across the network, and a network-based malware protection system that leverages the power of the cloud. Only when these technologies are working together can organizations truly block the sophisticated new threats that emerge on a daily basis.

Yet not all next-generation firewalls are the same. Dell™ SonicWALL™ NGFWs are the only firewalls capable of providing organizations of any size with a deeper level of network security. These industry-leading firewalls are designed using a scalable, multi-core hardware architecture and a patented, single-pass, low-latency, Reassembly-Free Deep Packet Inspection® (RFDPI) engine that scans all traffic, regardless of port or protocol. In addition to advanced SSL decryption and IPS capabilities, Dell SonicWALL NGFWs also have access to a cloud database that is updated continually with more than 15 million signatures. Not only that, they're easy to manage *and* they deliver a low total cost of ownership.

Introduction: Deeper network security

Rising security threats

The growing use of cloud computing, mobile solutions, bring your own device (BYOD) policies — and the rise of shadow IT — have added new levels of risk, complexity and cost to

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

Today's organizations need an NGFW that can deliver a deeper level of network security and app control without compromising performance.

securing an organization's data and intellectual property. Businesses of every size must now combat a wide range of increasingly sophisticated threats, including advanced persistent threats (APTs), cybercriminal activity, spam and malware. At the same time, many organizations are grappling with tighter budgets and don't have the resources to easily address these threats.

The move to next-generation firewalls

To combat growing security challenges, more and more organizations are migrating from traditional firewalls that focus only on stateful packet inspection (SPI) and access control rules to NGFWs, which have revolutionized network security by providing more robust protection against emerging threats. In addition to traditional firewall features, NGFWs feature a tightly integrated IPS, real-time decryption and inspection of SSL sessions and full control and visualization of application traffic as it crosses the network.

Not all next-generation firewalls are created equal

Modern attacks employ numerous complex techniques to avoid detection as they sneak quietly into corporate networks to steal intellectual property. These attacks are often encoded using complicated algorithms to evade detection by intrusion prevention systems. Once the target has been exploited, the attacker will attempt to download and install malware onto the compromised system. In many instances, the malware used is a newly evolved variant that traditional anti-virus solutions cannot detect. Also, the advanced attack often relies on SSL encryption to hide the malware download or even to disguise command and control traffic that is sent by the attacker from halfway around the world.

Some organizations rely on NGFWs that compromise network performance for protection, which leads to lowered productivity. Other organizations actually turn off or limit existing security measures to keep up with high network performance demands. With today's new threats and threat vectors, this is an extremely risky practice.

Clearly, more advanced detection and protection capabilities are needed. Ultimately, today's organizations need an NGFW that can deliver a deeper level of network security without compromising performance—at a total cost of ownership that is maximized for both large enterprises and small businesses.

Dell SonicWALL NGFWs deliver exactly this type of protection. Dell SonicWALL NGFWs feature SSL decryption and inspection that extends protection to SSL-encrypted traffic, an IPS with advanced anti-evasion technology, context-aware application control and cloud-based malware protection that keeps abreast of the latest threats.

How Dell SonicWALL NGFWs deliver deeper network security

Byte-by-byte packet inspection

Dell SonicWALL NGFWs are equipped with a patented, single-pass, low-latency, Reassembly-Free Deep Packet Inspection® (RFDPI) engine that inspects every byte of every packet while maintaining high performance and low latency. The RFDPI engine uses a combination of complex countermeasure techniques, real-time decision methodologies and data normalization to block threats within files, attachments and compressed archives — regardless of their size — and transform them as needed to perform normalized traffic analysis.

SSL decryption and inspection

SSL decryption and inspection is arguably the single most important feature required to provide a deeper level of network security. According to recent research (NSS Labs, 2013), as much as 35 percent of corporate network traffic is encrypted using SSL. So organizations that are not inspecting SSL traffic are effectively blind to a third of the traffic on the network. Further, attacks that utilize SSL will have

a 100 percent success rate in this type of scenario. To combat these sophisticated attacks effectively, organizations need the ability to inspect all traffic on any port, regardless of whether that traffic is SSL-encrypted or not. One of the challenges, however, is that most NGFWs available today offer dismal performance when decrypting and inspecting SSL traffic. Dell SonicWALL NGFWs offer best-in-class scalability and performance for SSL decryption and inspection, as evaluated by both Network World magazine and NSS Labs.

An IPS with anti-evasion capabilities

Cybercriminals often try to circumvent the intrusion prevention system by using complex algorithms designed to evade detection. Some network security vendors' products may not perform adequate data normalization to decode threats before the IPS has a chance to examine them. This enables encoded threats to compromise corporate networks without being noticed. Dell SonicWALL NGFWs are equipped with a tightly integrated IPS with advanced anti-evasion capabilities so that advanced threats are detected and stopped before they can harm the network. Dell offers cutting-edge IPS threat protection that is capable of reverse-engineering these advanced evasion techniques.

In the 2013 NSS Labs Security Value Map™ (SVM) for IPS, the Dell SonicWALL SuperMassive E10800 with integrated IPS earned the coveted "Recommended" rating. In fact, the Dell SonicWALL integrated network security solution, which includes IPS, was tested alongside many dedicated IPS offerings.

Application intelligence and control

The explosion of applications that rely on network access has made it difficult for administrators to monitor user activity and application traffic usage. This has led to productivity concerns and additional security risks. Dell SonicWALL NGFWs help solve these problems with an add-on application intelligence and control service. A context-aware monitoring engine gives administrators full visibility into application and user activity on the network. Armed with this information, administrators can easily create acceptable-use policies for allowing or blocking specific applications and apply them to individuals or groups within the organization. Dell SonicWALL NGFWs also enable powerful bandwidth management to ensure that critical network resources remain available for maximum productivity. In addition, a tightly integrated Application Flow Monitor provides real-time graphs of applications, inbound and outbound bandwidth, active website connections, and user activity for visual insight into network usage. The data from the graphs can be used to generate reports based on user ID.

Network-based malware prevention is updated continuously

Each hour of every day, hundreds of new variants of malware are developed. Although several NGFWs offer network-based, anti-malware technology, many of these systems are limited to just a few thousand malware signatures, and many are updated as infrequently as once per day. Dell SonicWALL NGFWs access a cloud database with more than 15 million signatures that is updated every few minutes around the clock, enabling organizations to achieve real-time protection against the latest threats.

The Dell SonicWALL RFDPI engine is capable of doing even more than pattern matching. When creating its custom firewall signatures, Dell SonicWALL NGFWs look for specific code fragments common to malware families rather than individual variants. This means that the RFDPI engine can identify the malicious code contained in new mutations to provide an additional layer of protection. In addition, Dell SonicWALL NGFWs have been independently tested and certified for network-based malware protection by ICSA Labs (ICSA Labs 2013).

> "The SuperMassive is aptly named . . . [it] can decrypt SSL traffic very fast — in fact these one-off tests show it to be the fastest device by far."
>
> *Network World magazine, 2012*

The Network Security Appliance (NSA) Series delivers the high level of security, application control and performance that administrators have come to expect.

The security of an industry leader

Dell SonicWALL has more than 20 years of experience in the industry, and Gartner has recognized Dell SonicWALL as an industry leader in network security. In the NSS Labs 2013 NGFW Product Analysis Report, the Dell SonicWALL SuperMassive E10800 firewall scored 100 percent in anti-evasion, stability and reliability, firewall, application control, and identity awareness tests. In 2012, Network World magazine reported in its article *Scaling Up With SonicWALL's SuperMassive*, "The SuperMassive is aptly named . . . [it] can decrypt SSL traffic very fast — in fact these one-off tests show it to be the fastest device by far." All SonicWALL Dell NGFW customers benefit from Dell's commitment to delivering a deeper level of security for around-the-clock protection across the entire organization.

A range of next-generation firewalls for every organization

Dell offers a range of next-generation firewalls to fit the needs of organizations of every size:

- **Dell™ SonicWALL™ SuperMassive Series** — This series is highly scalable, making it ideal for large enterprise organizations that are continually adding new users. For the second consecutive year, the SuperMassive E10800 has earned the top rating of "Recommended" in NSS Labs' 2013 Next-Generation Firewall Security Value Map. In addition, it has achieved one of the highest security effectiveness ratings in the industry and earned scores of 100 percent for anti-evasion, stability and reliability, firewall, application control, and identity awareness testing in NSS Labs' 2013 NGFW Product Analysis Report. The SuperMassive 9000 Series of firewalls ensures security effectiveness by enforcing intelligent policy decisions, which helps ease administrative burdens. Housed in an elegant, one-rack unit appliance, SuperMassive 9000 firewalls also save space and lower power and cooling costs.
- **Dell SonicWALL NSA Series** — The Network Security Appliance (NSA) Series delivers the high level of security, application control and performance that administrators have come to expect. And because the NSA Series firewalls are affordable and easy to deploy, configure and maintain, they are an ideal choice for the mid market and SMBs.

Conclusion

Dell SonicWALL NGFWs provide organizations of any size with a deeper level of network security without compromising performance because they are designed to scan all traffic regardless of port or protocol — including SSL-decrypted traffic. They can detect anti-evasion techniques and have network-based anti-malware capabilities with access to a cloud database that is continually updated. In addition, these firewalls are easy to manage and affordable. Further, Dell SonicWALL is recognized as an industry leader by Gartner, and the Dell SonicWALL SuperMassive E10800 next-generation firewall earned the highest rating of "Recommended" in NSS Labs' 2013 NGFW Security Value Map. Organizations that adopt Dell SonicWALL NGFWs will benefit from their advanced protection against ever-evolving, persistent IT security threats.

Dell NGFWs are part of Dell's overall portfolio of end-to-end Connected Security solutions, which ensure that organizations of all sizes can protect their intellectual property in an increasingly connected world. To learn more about Dell SonicWALL NGFWs, please visit software.dell.com/solutions/network-security.

For more information

Dell SonicWALL
2001 Logic Drive
San Jose, CA 95124

www.sonicwall.com
T +1 408.745.9600
F +1 408.745.9300

For More Information

About Dell Software

Dell Software helps customers unlock greater potential through the power of technology—delivering scalable, affordable and simple-to-use solutions that simplify IT and mitigate risk. The Dell Software portfolio addresses five key areas of customer needs: data center and cloud management, information management, mobile workforce management, security, and data protection. This software, when combined with Dell hardware and services, drives unmatched efficiency and productivity to accelerate business results.

If you have any questions regarding your potential use of this material, contact:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.dellsoftware.com
Refer to our Web site for regional and international office information.