Achieve deeper network security

SonicWall next-generation firewalls

Abstract

Next-generation firewalls (NGFWs) have become the new norm in network security for organizations of all sizes. Unlike their predecessors which offered limited protection from today's continually evolving threats, NGFWs deliver a much deeper level of security across wired and wireless networks. Not only do they inspect every byte of every packet while maintaining the high performance and low latency that busy networks require, they also combine high-performance SSL decryption and inspection, an intrusion prevention system (IPS) that features sophisticated anti-evasion technology and a network-based malware protection system that leverages the power of the cloud. This powerful combination enables organizations to block sophisticated new threats that emerge on a daily basis.

SonicWall™ NGFWs provide organizations of any size a deeper level of network security without compromising network performance. Designed with a scalable, multi-core hardware architecture and a patented[1], single-pass, low latency, Reassembly-Free Deep Packet Inspection® (RFDPI) engine, these high-performance security appliances efficiently scan all traffic regardless of port or protocol. In addition to advanced SSL decryption and IPS capabilities, SonicWall NGFWs also have access to a continually updated cloud database that contains tens of millions of malware variants. In addition they are easy to manage and deliver a low total cost of ownership.

Introduction: The need for a deeper level of network security

Rising security threats

The growing use of cloud and mobile computing, Bring Your Own Device (BYOD) policies — and the rise of shadow IT — have added new levels of risk, complexity and cost to securing an organization's data and intellectual property. Organizations of every size must now combat a wide range of increasingly sophisticated threats, including advanced persistent threats

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

(APTs), cybercriminal activity, spam and malware. At the same time, many are also grappling with tighter budgets and don't have the resources to easily address this.

The move to NGFWs

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

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

Not all NGFWs are created equal

Modern attacks have become more difficult to identify and employ several complex techniques to avoid detection as they sneak quietly into corporate networks to steal intellectual property. These attacks are often encoded using complicated algorithms designed to evade detection by intrusion prevention systems. Once the target has been exploited, the attacker attempts 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 across the world.

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

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

Delivering a deeper level of network security

SonicWall NGFWs deliver a deeper level of network security without compromising performance. SonicWall NGFWs feature SSL decryption and inspection that extends protection to SSL-encrypted traffic, an IPS with advanced anti-evasion technology and cloud-based malware prevention that secures networks from the latest threats.

How SonicWall NGFWs deliver deeper network security

Byte-by-byte packet inspection

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 with almost no 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.

SonicWall NGFWs scan all traffic, regardless of port or protocol, to protect the network from internal and external attacks against application vulnerabilities. Application intelligence and control capabilities are used to examine every packet and identify which applications are in use, who is using them and how much bandwidth they are consuming.

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 the 2016 SonicWall Security Annual Threat Report, Secure Sockets Layer/ Transport Layer Security (SSL/TLS) encryption continued to surge, leading to under-the-radar hacks affecting at least 900 million users in 2015. This leaves organizations that are not inspecting SSL traffic effectively blind to much of the traffic on the network. Further, attacks that utilize SSL will have a 100% success rate in this type of scenario. In order 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. SonicWall NGFWs offer best-in-class scalability and performance for SSL decryption and deep packet 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 (IPS) by using complex algorithms designed to evade detection. Some network security vendor 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. SonicWall NGFWs are equipped with a tightly integrated IPS featuring advanced anti-evasion capabilities that detect and stop advanced threats before they can harm the network. SonicWall's cutting-edge IPS threat protection is capable of reverse-engineering even the most advanced evasion techniques.

The SonicWall SuperMassive E10800 with integrated IPS earned the top "Recommended" rating in the 2016 NSS Labs Next-Generation Firewall Security Value Map (SVM). Part of NSS Labs' NGFW testing includes IPS-specific components and SonicWall had one of the highest ratings for both security effectiveness and performance.

Network-based malware protection that is updated continuously

Each hour of every day, hundreds of new malware variants are developed. Although some NGFWs offer network-based, anti-malware technology, many of these systems are limited to just a few thousand malware signatures, with updates occurring infrequently as once per day. SonicWall NGFWs access a cloud database containing tens of millions of malware variants that is updated every few minutes around the clock, so that organizations can achieve real-time protection against the latest threats.

Yet SonicWall's RFDPI engine does much more than pattern matching. When creating its custom firewall countermeasures, 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, SonicWall NGFWs have been independently tested on an ongoing monthly basis and certified for network-based malware protection by ICSA Labs (ICSA Labs 2016).

The security of an industry leader

SonicWall has over 20 years of experience in the industry, and Gartner has recognized SonicWall as an industry leader in network security. In the NSS Labs 2016 Next-Generation Firewall Product Analysis Report, SonicWall's SuperMassive firewall scored 100 percent in anti-evasion, stability and reliability, firewall policy enforcement and application control tests. In its article *Scaling Up with SonicWall's SuperMassive*, Network World magazine reported "The SuperMassive is aptly

> *"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

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 NGFW customers benefit from SonicWall's commitment to delivering a deeper level of security for around-the-clock protection across the entire organization.

A range of NGFWs for every organization

SonicWall offers a range of NGFWs to fit the needs of organizations of every size:

- **SonicWall™ SuperMassive Series** — This series is highly scalable to meet the needs of data centers, carriers, service providers, large institutions and enterprise organizations. For the fourth consecutive year, the SuperMassive E10800 has earned the top rating of "Recommended" in the 2016 NSS Labs SVM and has achieved one of the highest security effectiveness ratings in the industry. It has also achieved scores of 100 percent for anti-evasion, stability and reliability, firewall policy enforcement and application control testing in the NSS Labs 2016 Next-Generation Firewall Product Analysis Report. The SuperMassive 9000 series firewalls ensures security effectiveness by enforcing intelligent policy decisions, which helps to ease administrative burdens. Housed in an efficient, one- or two-rack unit appliance, SuperMassive 9000 series firewalls also save valuable space and lower power and cooling costs.
- **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. Using the same security engine and services as the SuperMassive series, the NSA series firewalls boost performance while reducing cost and complexity. And, because the NSA series firewalls are affordable and easy to deploy, configure and maintain, they are an ideal choice for distributed enterprises with remote and branch offices, SMBs, school campuses and other public institutions.

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

Conclusion

SonicWall NGFWs provide organizations of any size with a deeper level of network security without compromising performance. They scan all traffic regardless of port or protocol — including SSL-encrypted traffic; they can detect anti-evasion techniques; and they have network-based anti-malware with access to a cloud database that is continually updated, in addition to being both easy to manage and affordable. Further, SonicWall has been recognized as an industry leader by Gartner, and the SonicWall SuperMassive E10800 consistently earns the highest rating of "Recommended" in NSS Labs' Next-Generation Firewall Security Value Map. Organizations that adopt SonicWall NGFWs will benefit from advanced protection against ever-evolving, persistent IT security threats.

SonicWall NGFWs are part of SonicWall'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 SonicWall solutions, visit www.sonicwall.com.

SONICWALL™

About Us

Over a 25 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.

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

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Refer to our website for additional information.
www.sonicwall.com