eBOOK | SECURITY

SMART SECURITY FOR ESCALATING CHALLENGES

Next-generation firewalls ease management issues spanning a multi-dimensional landscape of rapidly evolving threats, application-related issues, and bandwidth hurdles

SONICWALL®

NETWORKWORLD
Custom Solutions Group

INSIDE

EXECUTIVE SUMMARY

Traditional firewalls, which account for an estimated 95 percent of current deployments,[1] cannot keep up with the demands of today's networks. According to CSO, "Traditional stateful inspection firewalls, with their port- and protocol-based controls, have limited visibility into the contemporary Web-based network landscape."[2]

This document examines the challenges IT administrators face in keeping their organization secure and ensuring that critical applications get the bandwidth they need, while limiting the bandwidth that unessential applications consume. In an increasingly complex world, CIOs and IT managers are turning to Next-Generation Firewalls that features new levels of management and ease-of-use to help them more effortlessly meet today's threats and organizational demands.

INTRODUCTION

IT administrators are bandwidth challenged. Their networks are struggling to keep up with employee and customer demands for increased social networking, virtualization, mobile devices, rich media, cloud computing and other applications, all of which have the potential to introduce new security threats and productivity drains into the organization.

Bandwidth consumed by a deluge of Web 2.0, social media and streaming multimedia traffic can dramatically reduce bandwidth available to business-critical applications. Some of this traffic may be crucial to business activity, while much can be non-productive and time wasting. Nielson, the ratings organization, estimates there that Facebook® now averages more

SonicWALL SUPERMASSIVE E10000 SERIES

SonicWALL ramped up security capabilities to protect the world's highest performance networks from malware of all kinds.

The SuperMassive™ E10000 Series security platform and technology is capable for detecting and controlling applications, preventing intrusions, and blocking malware at up to 120 Gbps without introducing latency to the network.

Designed to eliminate choosing between performance and security, the SuperMassive E10000 Series incorporates SonicWALL's massively scalable architecture to provide application control, intrusion prevention, malware protection and SSL inspection at multi-gigabit speeds.

Three years ago we set out to design the fastest, most effective, next-generation security platform on the planet and we called this Project SuperMassive," said John Gmuender, Vice President of Engineering and Chief Technical Officer of SonicWALL.[4] "Given the increasing bandwidth speeds and the escalating volume, frequency, and sophistication of Internet threats, we knew this technology platform needed to be massively scalable. I'm very happy to say that with SuperMassive E10000 Series we have achieved this goal."

The SuperMassive E10000 Series is engineered to deliver ultra-low latency deep packet inspection and is suited for securing enterprise networks, data centers and server farms. SonicWALL's patented Reassembly-Free Deep Packet Inspection®* engine provides a highly-efficient single-pass design that consolidates all security features into a unified scanning and policy engine, enabling the platform to deliver industry-leading deep packet inspection performance.

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

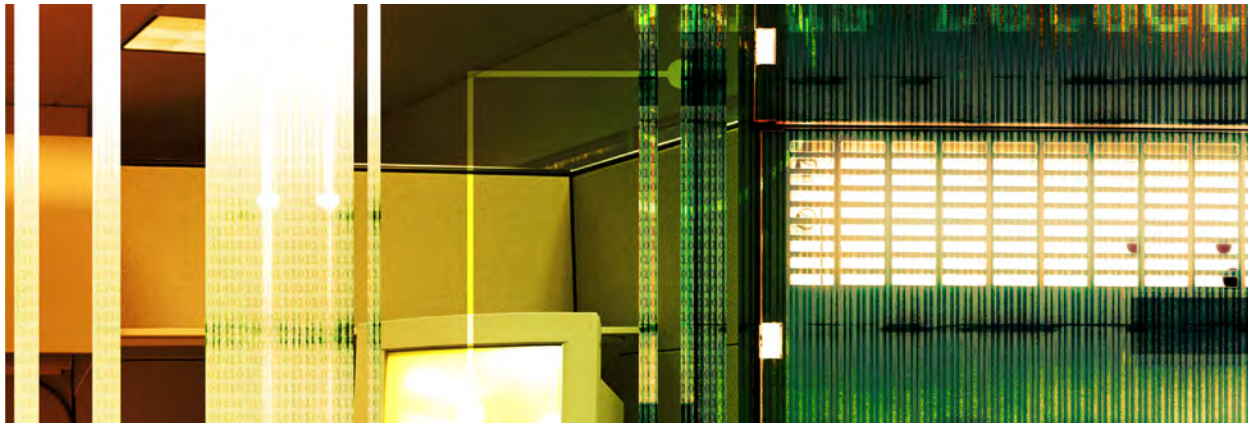
than 137 million unique visitors monthly, and Twitter® more than 23 million each month. As companies increasingly use these platforms for marketing and customer contact, it becomes increasingly difficult to delineate the distinction between professional and personal use: for example, a recent study[3] indicted that "Gen-Y" Facebook participants use their profile "as an extension of their professional personality, even though they are socializing with family and friends. Furthermore, "they add an average of 16 co-workers each to their 'friend' group."

Overwhelmed IT resources can be ineffective in sufficiently monitoring, maintaining and updating security defenses. Significant changes to the application landscape and ever-present compliance requirements are raising the bar in terms of what constitutes adequate protection for the enterprise.

Traditional firewalls cannot provide the multi-dimensional management capabilities needed to battle today's threats and satisfy end-user needs. While these systems inspect network traffic based on information pertaining to a combination of the packet's source and destination address, malicious web applications can utilize SSL encryption and nonstandard ports to slip through undetected.

Next-generation firewalls, however, have evolved to provide granular application intelligence and control with superior intrusion prevention and malware protection. «

NEW AND EVOLVING APPLICATION CHALLENGES



Technology such as interactive Web 2.0 transactions, high-speed mobile telecommunications and cloud-based Software-as-a-Service (SaaS) applications has opened new channels to the enterprise. As a result, the threat matrix continues to expand exponentially. "Thanks to the explosive popularity of Web 2.0, thousands of Web-based business and consumer apps and attacks are launched primarily through the application layer," according to CSO.[5] Furthermore, it reported, "Attackers have become adept at using low-and-slow techniques in targeted attacks that evade intrusion-prevention systems (IPS)."

Organizations are moving beyond store-and-forward and session-based applications like email, Web pages and traditional client/server applications as they incorporate rich media, WiFi and cellular wireless access, peer-to-peer applications, chat and to accommodate employees' personally owned devices. "Gartner predicts that 90 percent of businesses will support corporate applications on mobile devices by 2014. Today, mobile devices are critical building blocks of business infrastructure," said Patrick Sweeney,[6] vice president of product management and corporate marketing at SonicWall.

Enterprises are increasingly reliant on the applications that leave them most vulnerable to security and network performance issues. Email, instant messaging and VoIP applications such as Skype are considered essential everyday resources.

It is not realistic to simply shut down such services, as an organization would be shutting itself off from better collaboration, higher productivity and lower costs that these technologies enable. But it is also not practical to allow all applications unfettered access to bandwidth, as non-essential network use such as video and music streaming may sap the performance of essential applications.

THANKS TO THE EXPLOSIVE POPULARITY OF WEB 2.0, THOUSANDS OF WEB-BASED BUSINESS AND CONSUMER APPS AND ATTACKS ARE LAUNCHED PRIMARILY THROUGH THE APPLICATION LAYER.

Organizations need to take a closer look at the current state of their network security and ways in which they can allow productivity enhancing Web 2.0 tools without slowing business processes or opening their networks up to harmful threats.

Traditional firewalls and intrusion prevention systems inspect packets on the wire. They lack the application-specific knowledge to discern an acceptable request from a threatening one or the ability to differentiate between essential and non-essential use of the same application by different workers. «

BUSINESS-CRITICAL PRIORITIES

Aaron's® Inc. is the nation's leader in the sales and lease ownership and specialty retailing of residential and office furniture, consumer electronics, home appliances and accessories.

The company chose to implement a VPN over broadband rather than more expensive T1 connections to aggregate large amounts of data from its more than 1,800 company-operated and franchised stores back to its corporate office, but needed to control which applications utilize its VPN bandwidth. "We need to ensure bandwidth is available for business-critical applications, which would in turn affect the performance in the operation of the stores," said Jason Tate, director of network services at Aaron's.

The company implemented a secure distributed VPN connecting SonicWALL network Security Appliances (NSA) and E-Class NSA E6500 and E5500 firewalls in in corporate offices and regional fulfillment centers, with approximately 1,500 TZ Series firewalls distributed across the retail stores.

SonicWALL's application intelligence, control and visualization have enabled Tate to see traffic from the stores and identify the applications traversing the remote networks. Now it can manage and prioritize social networking traffic like Facebook with SonicWALL's application intelligence, control and visualization feature to boost employee productivity and protect the organization. Click here for more on Aaron's.

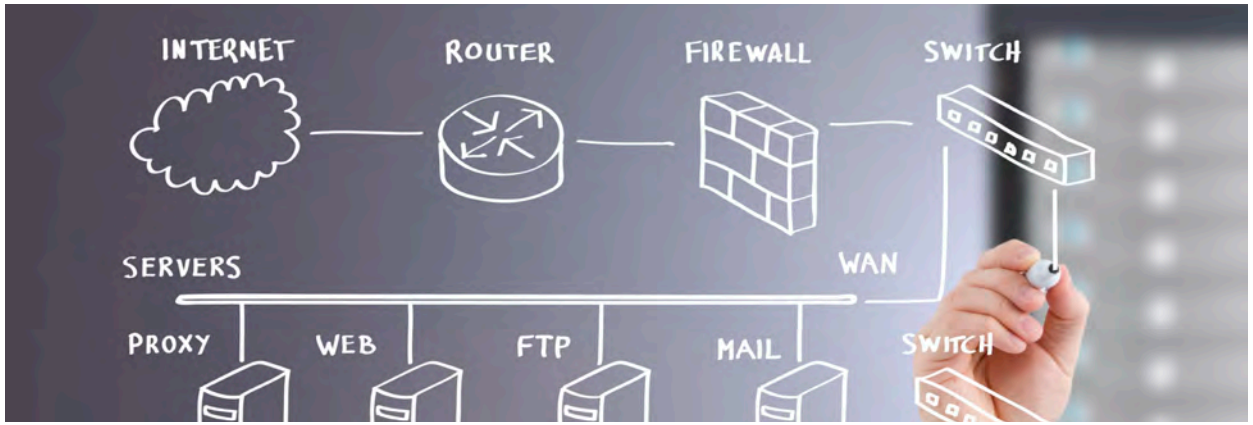
CROSS-VECTOR THREAT PROTECTION

The SonicWALL Global Response Intelligent Defense (GRID) Network gathers, analyzes and vets cross-vector threat information from millions of sources around the world, which can then be utilized to improve the effectiveness of existing security solutions in real time and applied to research on future threats and defenses.

Historically, security products often grouped threats by vectors corresponding to particular protocols/applications by which suspect traffic might breach the network—for example, email or web traffic. But an email may contain a URL that has been defined as suspect, so using the cross-vector approach the GRID Network can block browser access to the URL on the Web vector as well as blocking access to the message on the email vector. At the same time browser access of certain web content could be considered malicious, thus causing an analysis of the web content access and potential deployment of anti-malware signature(s) in case the web content was indeed confirmed to be malicious.

"GRID Network represents internal collaboration between different technologies and research that SONICwall has and does," says Alex Dubrovsky, Director of Software Engineering & Threat Research at SonicWALL. The GRID Network encompasses all the information that flows through the SonicWALL data center, including the company's security solutions, content filtering access data, threat prevention detection information, electronic "honey pots" designed to collect spam, phishing and virus emails, real time blacklist providers, contributing industry professionals and SonicWALL Anti-Spam Desktop users.

SMART NETWORK MANAGEMENT



Critical applications need bandwidth prioritization while social media and gaming applications need to be bandwidth throttled or completely blocked. Stateful packet inspection firewalls used in many organizations rely on port and protocol, and are not able to identify applications and in order to sort out the good from the bad.

Many organizations are unaware that their current network protection is insufficient. Hackers can insert malformed data into packets, enabling web applications to share too much information with the attacker. Cyber thieves can insert access controls into an application, allowing them to access specific content or functions meant only for authorized users.

But there are ways to uncover the potential risks to an organization's network and prevent them, while bolstering employee productivity at the same time. Next-Generation Firewalls with application intelligence and control features enable application access control with pre-defined user applications, regulate Web traffic, email, email attachments, and file transfers, and support bandwidth management.

Next-Generation Firewalls use application intelligence, control and visualization to provide granular control and real-time visualization of applications to guarantee bandwidth prioritization and ensure maximum network security and productivity. IT can protect, manage and control everything that passes through

THWARTING CYBER BULLIES

Crete-Monee School District 201-U, located south of Chicago, is an award-winning district with one of the most envied mathematics programs in the State of Illinois, a national championship choral music program and a full menu of varsity athletics. By restricting traffic to suspect and counterproductive sites, the district has freed up bandwidth for legitimate web applications and made it a safer learning environment.

"Cyber-bullying is huge right now," says Tom Gawczynski, network administrator for the district, which serves a growing population of more than 5,000 students and deployed a SonicWALL E-Class Network Security Appliance (NSA) E6500 with Content Filtering Service (CFS). "We need flexible content filtering that can permit Deans to access Facebook and monitor suspicious activity, while blocking students from accessing it in the classroom."

SMART NETWORK MANAGEMENT *continued*

the network, while identifying and understanding potential risks.

To better manage network resources, IT needs the ability to track individual user activities locally or on remote network sites to gain insight into traffic usage across the entire network and get a closer look at application usage, web sites visited, backup activity, and VPN connections per user. Traffic analysis utilizing granular next-generation syslog data provides advanced troubleshooting capabilities to assist in identifying the location of network outages and slowdowns by surfacing which applications are used by what users and systems. IT gains in-depth insight into how employees utilize resources and how applications impact the network on a daily, weekly, monthly or even yearly basis.

Integrating Next-Generation Firewalls, traffic analytics and a WAN acceleration appliance ensures an organization is able to analyze and manage bandwidth use of the network, block undesirable applications, identify network inefficiencies and reduce traffic between sites. «

CLOSING HACKER'S HONEY POT

Hackers constantly probed the network at State University of New York (SUNY) College at Old Westbury in attempts to steal information and leverage the networked devices as a hidden launching ground for outbound attacks.

"We look like a honey pot to the bad guys," said Marc Seybold, CIO at Old Westbury and current chair, SUNY Council of Chief Information Officers. In addition, students and staff expose their devices to threats off-campus and on the Internet, and then return to campus with the potential to compromise the College's network.

A SonicWALL E-Class Network Security Appliance (NSA) E7500 Next-Generation Firewall in paired High Availability (HA) mode helps Seybold shape and optimize bandwidth over his gateway firewall while adding an extra layer of network security and visibility for secure remote access.

BOTTOM LINE

Enterprises today are faced with a multi-dimensional landscape of rapidly evolving threats, application-related issues, and bandwidth challenges. They can meet this challenge by transitioning to a more advanced security platform that consolidates core Next-Generation Firewall application intelligence, control and visualization, and gateway protection capabilities along with other critical network optimization services. With the ability to managed bandwidth usage by application, users or even time of day, the organization can comfortably embrace the innovative business tools that increase collaboration, lower costs and boost productively. «

APPLICATION INTELLIGENCE THROUGH SonicWALL

SonicWALL®, Inc. provides intelligent network security and data protection solutions that enable customers and partners — around the world — to dynamically secure, control, and scale their global networks. Built upon a shared network of millions of global touch points, SonicWALL Dynamic Security begins by leveraging the SonicWALL Global Response Intelligent Defense (GRID) Network and the SonicWALL Threat Center that provide continuous communication, feedback, and analysis regarding the nature and changing behavior of threats worldwide. SonicWALL Research Labs continuously processes this information, proactively delivering defenses and dynamic updates that defeat the latest threats. Leveraging its patented Reassembly-Free Deep Packet Inspection® technology in combination with a high speed, multi-core parallel hardware architecture, SonicWALL enables simultaneous, multi-threat scanning and analysis at wire speed and provides the technical framework that allows the entire solution to scale for deployment in high bandwidth networks. Solutions are available for the SMB through the Enterprise, and are deployed in large campus environments, distributed enterprise settings, government, retail point-of-sale and healthcare segments, as well as through service providers.

For more information, visit www.sonicwall.com.

SONICWALL®

NETWORKWORLD
Custom Solutions Group

FOOTNOTES:

[1] Source: "The Rising Next-Gen Firewall Opportunity" Channelnomics, Dec 16, 2011, http://channelnomics.com/2011/12/16/rising-next-gen-firewall-opportunity

[2] Source: "Next-generation firewalls: In Depth", CSO Oct 17, 2011, http://www.csoonline.com/article/691651/next-generation-firewalls-in-depth

[3] Source: Facebook Study, January 2012, http://personalbranding.com/2012/01/millennial-branding-gen-y-facebook-study

[4] Source: SonicWALL SuperMassive announcement, April 27, 2011

[5] Source: "Next-generation firewalls: In Depth", CSO Oct 17, 2011, http://www.csoonline.com/article/691651/next-generation-firewalls-in-depth

[6] Source: SonicWALL press release: http://www.sonicwall.com/us/company/Press_Releases.html/us/company/Press_Releases.html