Unified Threat Management and Next-Generation Network Security Platforms

Executive Summary

Sponsored by:

Executive Summary

Overview

The majority of IT organizations have historically relied on a patchwork of point products to construct the technology pillar of their information security architectures. For practically every new class of threat, the routine has been to purchase, deploy, and maintain yet another agent, appliance, or, perhaps managed service. But the pressure has been steadily mounting, and now the pot is boiling over.

For a variety of reasons, today's organizations must account for: (a) more points of entry into their networks, (b) a greater number and variety of resources that require protection, and (c) a substantially faster, more elusive, and more diverse population of threats poised to exploit any exposed weaknesses. And, of course, they must do so without breaking the bank.

In this regard, Unified Threat Management (UTM) and Next-Generation Network Security Platforms (NNSPs) can provide a measure of relief. The reductions in cost and complexity, and improvements in security effectiveness achieved by having multiple countermeasures available in a single device are clearly advantageous. Furthermore, steady improvements in the areas of manageability and performance are expanding the number of use cases for which these solutions are suitable.

Security Incite believes that organizations of all types and sizes – not just SMBs – should be evaluating the UTM devices and NNSPs for use in their computing environments. When doing so, however, it is important to keep two points in mind. First, all products in this category are not created equal. There will inevitably be a lot of variation among available solutions, especially when it comes to price/performance, security stopping power, and the degree of true "unification" that has been achieved. And the second point is that even though a lot of progress has been made, this does not mean UTM will be the right approach for all scenarios or, for that matter, all organizations.

End User Requirements

Prevailing conditions relative to the threat, business, and technology landscapes have changed the nature and scope of information security requirements. For instance, establishing comprehensive protection for computing systems and associated information assets is not just a good business practice; in many cases it is now mandated by any number of regulations and corporate policies. In addition, what constitutes "comprehensive" has expanded substantially in recent years. The net result it

that security practitioners need to consider three distinct dimensions – functional, logical, and physical – when architecting their organization's defenses.

Functional requirements

Today's hackers are less interested in gaining notoriety than they are in making money. Consequently, for the past several years there has been a noticeable spike in threat development and greater focus on successfully evading commonly deployed countermeasures in order to "obtain" valuable information (like intellectual property and credit card data). New threats are being generated more rapidly than ever before, diminishing the effectiveness of conventional reactive countermeasures such as patching and antivirus software. And the concerns of the past (e.g., file-level viruses, worms, and denial-of-service attacks) are now being over-shadowed by an array of newer attacks, such as spyware, spear phishing, keylogging Trojans, rootkits, and even targeted attacks.

In response, organizations need to establish defenses that provide greater functional coverage. Positive-model countermeasures that operate on the basis of specifying allowed traffic and then blocking everything else (e.g., firewalls) should be "blended" with negative-model controls that subsequently filter the allowed traffic for any malicious, known attack elements (e.g., intrusion prevention). Purely preventive mechanisms used to block unwanted traffic should be complemented by capabilities geared more toward monitoring for suspicious activity or recovering from attacks that have already occurred. And type-specific countermeasures should also be included to address threats that warrant focused attention, such as spyware and rootkits, due to the need for specialized inspection techniques.

In terms of network-based security solutions, this translates into having to implement the following types of countermeasures and capabilities:

- *Core functionality* includes network firewall, IPSec VPN, intrusion detection/prevention, and network antivirus;
- *Common functionality* includes URL filtering, anti-spyware/malware, application control (e.g., for instant messaging, Skype, BitTorrent clients, etc.), SSL VPN, and host integrity checking; and,
- *Extended functionality* includes web application firewall, application-specific security (e.g., for VoIP), and data leak prevention.

Logical requirements

Another consequence of the shift in hacker motivation to fraud is threats are steadily migrating up the computing stack. By focusing on system and application-layer weaknesses hackers can enable their creations to slip

through traditional network-centric countermeasures deployed by most organizations. Of course, it doesn't help matters that web applications, in particular, have proven to be notoriously vulnerable and are widely recognized as promising "front doors" to all sorts of lucrative data.

In any event, the implication is that establishing comprehensive defenses depends on implementing countermeasures that provide complete logical coverage. Threats and vulnerabilities need to be addressed at all layers of the computing stack. In other words, protection is necessary not only for network and system-level components but also for:

- *Application services* (e.g., layer-7 protocols such as HTTP, FTP, and SMTP);
- *Utility applications* (e.g., web, directory, and database servers);
- *Business applications* (e.g., Word, Outlook, and SAP); and
- *Individual data elements* (e.g., social security numbers (SSNs), personal healthcare information).

PERVASIVE PERIMETERIZATION

"De-perimeterization" has garnered a lot of attention. But is it really a practical approach to pursue?

Pervasive perimeterization, just like de-perimeterization, acknowledges that conventional perimeter defenses have been eroded. But it does not call for their dissolution. Nor does it rely on futures such as "inherently secure communications" and "data-level authentication".

Instead, by deploying countermeasures to establish additional "perimeters" throughout the internal network and on individual endpoints as well, organizations effectively *evolve* their defenses to more fully embrace the practice of defense-in-depth.

Physical requirements

The third dimension deals with the glaringly obvious fact that a security strategy based primarily on defending an organization's Internet boundaries is no longer sufficient. Threats now have more points of entry into enterprise networks due to increasing user mobility, the proliferation of remote offices, and greater degrees of interaction and collaborative business processes between businesses and their customers and partners. There has also been recognition, particularly in the form of industry regulations that the risk of internal threats is far from negligible. The result is the need for organizations to establish comprehensive physical coverage by pursuing a strategy of "pervasive perimeterization." In other words, appropriate countermeasures should be deployed not only at primary connections to the Internet, but ideally at multiple points within the "internal" network as well.

Specific locations that require consideration include:

- Branch office Internet and WAN connections;
- The interface to high-profile segments and sensitive enclaves;
- The core of the enterprise network;
- Within the data center (e.g., front-ending virtualized desktop server farms);
- Consumer-to-business connections;
- Business-to-business connections;
- Employee-to-business connections (e.g., for remote access); and
- Employee-to-internet connections (e.g., web and email security gateways).

Solution Architectures

When evaluating solutions to address the tall order of establishing comprehensive functional, logical, and physical coverage for network-based security, there are a number of alternatives that security practitioners can consider. A brief treatment of the available options is as follows:

1. *Do nothing* – Achieving perfect security is impossible. At the same time, however, failing to implement countermeasures to prevent and/or react faster to widely recognized threats borders on negligence. It's safe to say that no business wants to be the next TJX or Hannaford Brothers; so even though doing nothing is an option, it's clearly not a good one.

2. *Use point products* – Maintaining the status quo and relying solely on a vast collection of point products causes the solution to directly mirror the diversity and complexity of the problem. This is simply not a sustainable approach. **It is inefficient, expensive, and ultimately ineffective.** The cost to operate an ever-expanding set of tools steadily rises even as threats continue to penetrate through the inevitable gaps that characterize this type of patchwork defense. That said point products typically afford the greatest levels of performance, functional specialization, and configurability. Quite often they are also the only option for dealing with new classes of threats when they first emerge.

3. *Implement conventional UTM* – Early generation UTM devices are familiar to most organizations. These products typically started "life" as firewalls and subsequently accumulated a wide range of additional capabilities (VPN, IPS, etc.). Although they provide a decent measure of consolidation – thereby reducing infrastructure complexity and costs – they often have limitations in terms of the robustness of the included countermeasures, the degree of integration and configurability, and/or overall performance and scalability. As such, the products in this category have had limited traction outside of SMBs and the branch office locations for larger enterprises.

4. *Deploy enterprise-class UTM* – The latest UTM products differ from their predecessors in that they have new architectures. In particular, the underlying hardware and software is being designed specifically to meet the needs for UTM. Simple things are now accounted for, such as having disk space to support quarantining of spam and viruses. More importantly the hardware has been beefed up considerably, and first stabs are being made to optimize associated software, including the interactions between different countermeasures. As former limitations are incrementally addressed, this opens the door for UTM devices to be used in a much wider variety of large company scenarios.

5. *Use Next-Generation Network Security Platforms (NNSPs)* – Not satisfied with just addressing technical limitations, the purveyors of this relatively recent entry on the scene have also instituted a name change to help escape the connotation between "UTM" and low volume, low criticality use cases. The chief difference relative to enterprise-class UTM solutions lies in the approach that is being taken, of which there are two main varieties:

    - Emphasis on "less being more" refers to those solutions that combine a smaller set of operationally related countermeasures (e.g., firewall, VPN, and IPS for an access control gateway) in order to provide greater performance and/or controls that are more robust. In general, the tighter focus also affords the opportunity for greater degrees of integration, software optimization, and configurability.

    - Emphasis on "the platform" refers to those solutions that are focused predominately on the underlying plumbing needed to make things go. Hardware and a collection of system-level capabilities – such as native load balancing and failover, internal switching, and a virtualization subsystem – are provided to support a wide variety of countermeasures (typically sourced from third parties) that can be arranged practically any way the customer wants. The goal is to deliver levels of performance, scalability, adaptability, resilience, and

choice that exceed those possible with conventional fixed-format UTM products.

Clearly there are some valid differences between these product categories, but it is important to realize that many of the distinctions are vendor-driven and the lines continue to blur. For instance, true, single-function point products are actually quite rare commodities in today's network security market. Just about every firewall available today includes VPN capabilities, and most incorporate at least rudimentary intrusion prevention. It is also increasingly common for the underlying hardware/platform to be "purpose-built", "architected specifically for UTM", or otherwise "specialized" in some manner.

At the end of the day, this means enterprises may find that more than one type of solution is capable of meeting their needs. Still, if a best-fit approach is pursued, then the outcome will most likely be a combination of most, if not all, of the options listed above. This is particularly true for larger shops where there are more total scenarios to account for and the differences between them are typically more substantial. Again, the key is for each organization to focus on their specific situation and come up with the mix that best fits their cultural mindset, at the same time that it achieves a balance between security effectiveness, operational efficiency, and total cost of ownership.

Value Propositions

For architects, engineers, and administrators in the trenches the appeal of UTM devices and NNSPs is fairly obvious. Bigger pieces of the functional and logical security puzzle can be achieved with fewer physical devices. However, convincing senior executives controlling the budget that this represents a worthwhile investment is a completely different matter. So here are a few aspects of the UTM/NNSP concept that support the core objectives of every member of the senior management team, i.e., making more money or spending less.

- *Reduce infrastructure complexity* – Taking a pure, point product approach to information security inevitably entails many devices. And not just the ones that run the requisite security functions. Additional infrastructure is needed to link them all together, such as switches, routers, and load balancers. In fact, herein lies one of the fallacies with regard to the scalability of point products. Although, each individual unit may support greater throughput, if multiple units are still needed for each type of countermeasure, then the resulting series of "sandwiches" (of load balancers, switches, and security devices) can get insanely complex – not to mention costly. Typically, UTM also affords the tangential benefit of needing to work with fewer vendors, as well as being able to gain some associated economies of scale when

it comes to purchasing products.

- *Simplify operations* – In addition to having fewer boxes to maintain, initial installation, integration, and ongoing configuration and operation of the security devices themselves is simpler and more efficient. This holds true and varies in direct proportion to the extent that the solution eliminates the need to install and harden operating system and associated security software, and to the extent that the vendor has integrated the different functions and their management.

- *Enhance security effectiveness* – In general, employing these solutions enables organizations to bring more security capabilities into play in more locations than would otherwise be the case. Additional gains are also possible depending on the nature and extent to which the individual countermeasures are integrated. In any event, the result should be a stronger defensive posture and, therefore, fewer incidents. This means less downtime for crucial business systems, less exposure of sensitive data, and fewer resources needed to put things back in order, including the company's reputation.

- *Foster greater flexibility* – Deploying UTM devices and NNSPs provides a measure of adaptability and allows customers to use capabilities at their own pace. Some features may go unused upon deployment, but then can be turned on in the event the need arises (e.g., if a main AV gateway fails, or a certain business unit decides it needs its very own WLAN) – all without having to purchase, deploy, and maintain an entirely new product.

- *Solidify compliance posture* – A good deal of achieving compliance with applicable security and privacy regulations comes down to being able to demonstrate the presence of a "reasonable and appropriate" set of defenses. In this regard, multi-function appliances can help cover a lot of ground or, in other words, check boxes on auditor's inspection sheets.

Selection Criteria

The potential benefits for UTM solutions can be considerable. Yet, users are cautioned to pay careful attention during the procurement process because there is still a lot of feature and function variability. The market has not commoditized to the point that all the solutions are the same. Thus, organizations have a clear opportunity to find a best-fit alternative. But this also means there are still some lemons out there as well.

Accordingly, Security Incite recommends organizations use the following criteria to guide their evaluation of candidate solutions.

- ***Security functionality***. Does the product include a reasonable set of security services, i.e., ones you need today and ones that may be needed in the future, but not a lot that are superfluous? If not best in class, are the countermeasures at least "good enough", particularly in terms of detection/prevention strength, coverage (e.g., for protocols, applications, and technologies), and feature set? Do the individual components work together to provide a greater level of aggregate protection?

- ***Performance***. Does the product use a general-purpose operating system and ordinary server hardware, or is the system/hardware "specialized" for performance purposes (e.g., with dedicated processors for cryptographic and/or content processing operations, or custom ASICs)? To what extent has the software been optimized for performance (e.g., are packets "cracked" multiple times, are inspection techniques applied selectively or to every packet/session regardless of its type)? Are published performance ratings for real-world conditions (i.e., with mixed traffic types and high availability, NAT, dynamic routing, and logging all turned on)? Do independent test results support vendor throughput and latency claims?

- ***Reliability***. Does the product portfolio include one or more models that support features such as: a dedicated management port; native failover and clustering; an out-of-band management interface and separate control and data planes so that the system is manageable even when under duress; redundant components, such as fans, power supplies, and disks; and a configurable option for failing open or closed?

- ***Management***. Does the associated management application include the ability to remotely manage multiple devices at once, as well as other scalability features such as hierarchical policies, delegated administration, object re-use, and flexible grouping? Is more than one management application needed to account for different countermeasures or device models? Is there a high degree of intuitiveness and ease of use pervasive across the full set of lifecycle management functions (e.g., configuration, monitoring, troubleshooting, and reporting)? Is there support for granular, role-based administration to maintain separation of duties? Are the configuration controls sufficiently granular and are there virtual systems capabilities to support complex deployment scenarios?

- ***Flexibility and Compatibility***. Will the devices be able to fit seamlessly into the organization's computing environment based on support for various networking and security capabilities, such as: ports/interfaces, routing protocols, VLANs, QoS, directories, and authentication mechanisms? Will the solution be able to adapt to changing conditions, both in the near term (e.g., via frequent, dynamic content updates) as well as over the long haul (e.g., based on having a modular/extensible design)?

- ***Integration and Unification***. To what extent have the included countermeasures been combined to maximize processing efficiency? Are there sensible internal handoffs between countermeasures to enhance the ability to detect and respond to threats? Have management functions such as logging and reporting been consolidated, and has rule configuration been sensibly integrated to simplify policy instantiation and to minimize the potential for errors and omissions?

Summary

The scope of the security problem continues to grow, and fighting the battle with point products alone is clearly a losing proposition. Ultimately, IT organizations must find more effective and efficient ways to establish defenses that provide comprehensive functional, logical, and physical coverage.

Security Incite believes UTM solutions are poised to be a big part of the answer and, therefore, deserve close consideration. Significant strides have been made to deliver greater performance, more robust security capabilities, and better manageability – in part by offering a spectrum of different solutions, including newer, enterprise-class products and Next-Generation Network Security Platforms. This does not mean these products are appropriate for every enterprise use case. But it does mean that the number of roles they can adequately fill has grown considerably; and this is a trend that enterprises can expect to continue.

About the Lead Analyst:

Mark Bouchard, CISSP, is the founder of Missing Link Security Services LLC, a consulting firm specializing in information security and risk management strategies. A former META Group analyst, Mark has assessed and projected the business and technology trends pertaining to a wide range of networking and information security topics for over 10 years. He is passionate about helping enterprises address their information security challenges. During his career he has assisted hundreds of organizations worldwide with strategic and tactical initiatives alike, from the development of multi-year strategies and overall architectures to the justification, selection, acquisition, implementation and operation of security and networking solutions.

About Security Incite:

Security Incite is an industry analyst firm specializing in the information security market. Our mission is straightforward: Help subscribers protect their information assets more effectively by making better decisions. We provide timely analysis on information security topics and publish detailed, actionable reports to ensure that high profile projects are executed successfully.

Security Incite was founded to address a real need to provide objective, relevant and inciteful security research by focusing on what's right, as opposed to what pays well. Focusing on bold, thought-provoking and irreverent analysis, Security Incite helps organizations make better decisions. Our tagline is "No Bias. No Bull. Real Incite," which does a good job of explaining our philosophy and our focus.

SonicWALL E-Class Network Security Appliance

NETWORK SECURITY

SonicWALL E-Class NSA for Enterprise-class Deployments

- **Multi-core Performance Architecture**
- **Unified Threat Management Security Platform**
- **Deployment Flexibility**
- **Application Firewall and Custom Control**
- **Dynamic Protection**

Protection and Performance

The SonicWALL® E-Class Network Security Appliance (NSA) Series is the industry's first multi-core Unified Threat Management (UTM) solution, delivering enterprise-class deep packet inspection without significantly impacting network throughput. Combining a powerful deep packet inspection firewall with multiple layers of protection technology and a suite of high availability features, the E-Class NSA E7500, E6500 and E5500 appliances offer a broad range of scalable solutions for enterprise deployments in distributed environments, campus networks and data centers.

SonicWALL E-Class NSAs are engineered to be the most scalable, reliable and highest performing multifunction threat appliances in their class. The NSA Series prevents against a vast spectrum of network attacks with unprecedented speed. This speed of protection is enabled through the NSA multi-core architecture, a parallel performance design for ultra-high-speed threat protection and deployment scalability. Taking protection to new levels of control is Application Firewall, a set of customizable protection tools that empowers administrators with precise control over network traffic. Operational reliability is delivered through a high availability suite of features at the hardware and system level to optimize uptime and improve security coverage.

The NSA Series is a key part of SonicWALL's portfolio of enterprise-class products and services for network security, e-mail protection and secure remote access. All E-Class solutions offer outstanding protection and performance while delivering elegant simplicity and unparalleled value. SonicWALL's E-Class delivers the high performance protection required by enterprise-class networks in a solution that is engineered to drive the cost and complexity out of running a secure network.

Features and Benefits

Multi-core Performance Architecture. At the heart of the E-Class NSA is the SonicWALL multi-core performance architecture designed to provide breakthrough deep packet inspection and granular network intelligence over real-time network traffic without impacting network performance. The SonicWALL E-Class NSA can effectively deliver ultra-high-speed performance through the concurrent use of specialized security processing cores. Using the processing power of multiple cores in unison dramatically increases throughput and simultaneous inspection capabilities while lowering overhead impact.

Unified Threat Management Security Platform. The E-Class NSA Series delivers a highly redundant security and connectivity platform that is purpose-built for high-speed internal and external network protection, consolidating and extending security functionality throughout the network. E-Class NSAs integrate real-time gateway anti-virus, spyware and intrusion prevention to secure networks and VPNs against an extensive array of dynamic threats including worms, Trojans, viruses, malware and software vulnerabilities.

Deployment Flexibility. Designed for highly redundant operations, the E-Class NSA appliances are an ideal solution for wired or wireless applications requiring high-speed access and heavy workgroup segmentation. With integrated support for standards-based VoIP, virtual local area networks (VLANs), enterprise-class routing and quality of service (QoS) E-Class NSAs increase deployment flexibility and enhance productivity.

Application Firewall and Custom Control. Application Firewall is a configurable set of granular, application-specific policies that allow custom access control per network user, application, schedule or IP subnet level. These policies can restrict transfer of specific files and documents, scan e-mail attachments using user-configurable criteria, automate bandwidth, control inspect internal and external Web access, and support custom signatures.

Dynamic Protection. Dynamic threat protection, content filtering and application control services are continually updated on a 24x7 basis to maximize security and decrease cost. IT productivity is increased by eliminating ad-hoc patch management for servers and workstations, automating the application of new protection signatures and removing the necessity to manually update security policies.

SONICWALL®

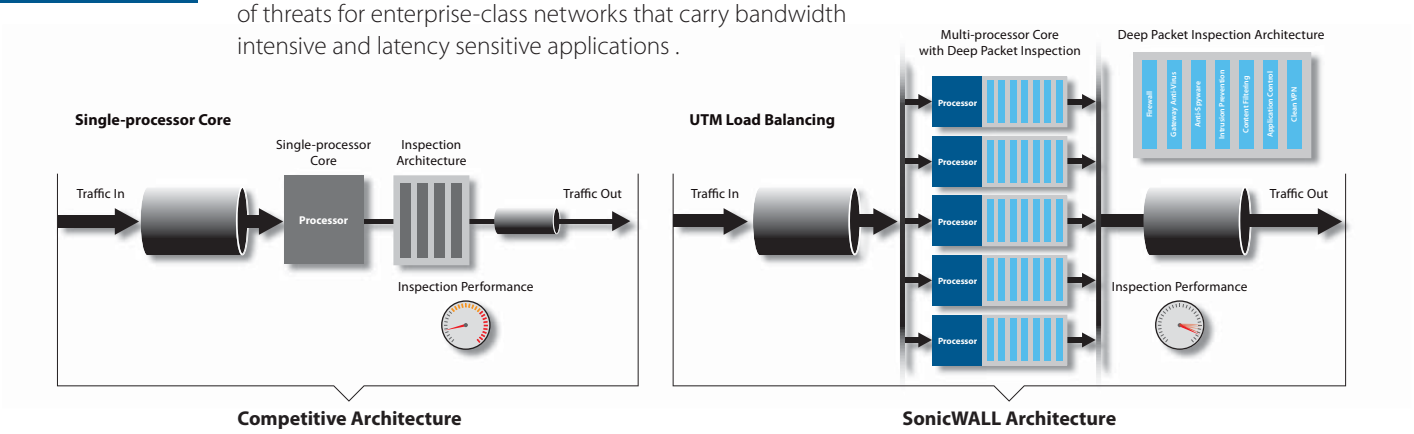
PROTECTION AT THE SPEED OF BUSINESS™

E-Class Network Security Appliance Architecture

Comprehensive, Integrated Best-of-Breed Threat Protection

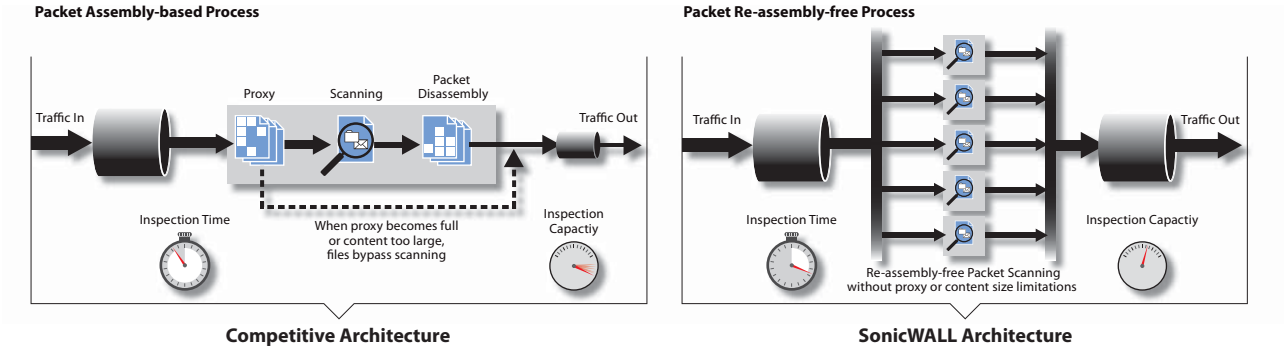
Unified Threat Management Load Balancing

Single processor designs that include multiple protection technologies are severely limited by a single centralized processor. SonicWALL UTM load balancing integrates a high-speed deep packet inspection and traffic classification engine onto multiple security cores inspecting applications, files and content-based traffic in real time without significantly impacting performance or scalability. This enables the scanning and control of threats for enterprise-class networks that carry bandwidth intensive and latency sensitive applications .

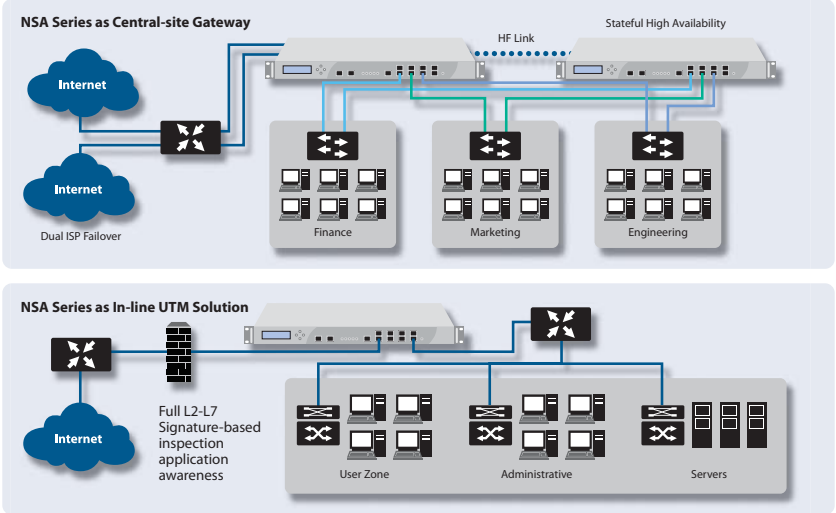


Unified Threat Management Engine

The SonicWALL E-Class NSA UTM engine delivers the first scalable application layer inspection engine that can analyze files and content of any size in real time without reassembling packets or application content. This means of inspection is designed specifically for real-time applications and latency sensitive traffic, delivering complete control and inspection without having to proxy connections. Using this engine design, high-speed network traffic is inspected more efficiently and reliably for an improved end user experience.



Flexible, Customizable Deployment Options



Central-site Gateway

Deployed as a Central-site Gateway the NSA Series provides a high-speed scalable platform, providing network segmentation and security using VLAN's and security zones. Redundancy features include WAN Load balancing, ISP fail-over and stateful high availability.

Layer 2 Bridge Mode

Layer 2 bridge mode provides inline intrusion detection and prevention, adds an additional level of zone-based security to network segments or business units and simplifies layered security. Additionally, this enables administrators to limit access to sensitive data by specific business unit or database server.

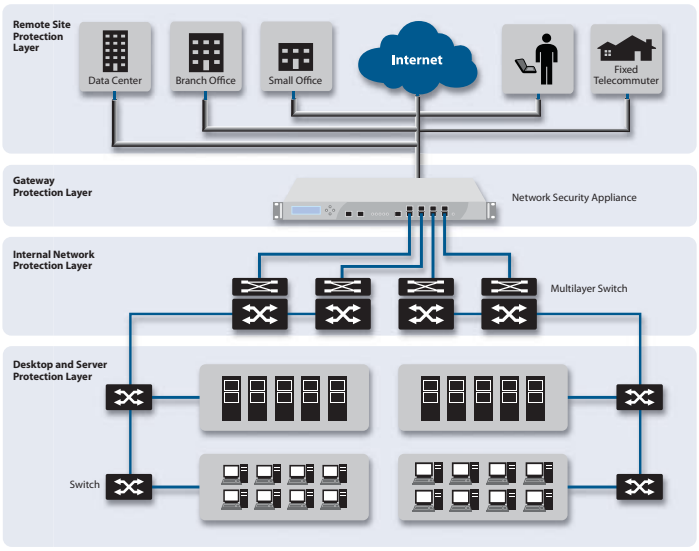
Multi-layer Protection

Remote Site Protection
The E-Class NSA Series incorporates ultra-high performance Virtual Private Networks (VPNs) that easily scales to thousands of end points and branch offices. Innovative SonicWALL Clean VPN™ technology prevents vulnerabilities and malicious code by decontaminating traffic before it enters the corporate network, in real time and without user intervention.

Gateway Protection
Easily integrated into existing environments, E-Class NSAs centralize gateway-level protection across all incoming and outgoing applications, files and content-based traffic, while controlling bandwidth and applications, without significantly impacting performance or scalability.

Internal Protection
The highly-configurable E-Class NSA Series extends protection over the internal network by inspecting traffic over LAN interfaces and VLANs. Specifically designed for LAN network threats, the E-Class NSA Series monitors and responds to internally spreading malware, denial of service attacks, exploited software vulnerabilities, confidential documents, policy violations and network misuse.

Desktop and Server Protection
In addition to network and gateway based protection, the E-Class NSA Series provides additional end point protection for workstations and servers through an enforced anti-virus and anti-spyware client with advanced heuristics. This enforced client solution delivers network access control by restricting Internet access on end points that do not have the latest signature or engine updates. When enforcement is enabled on the appliance, each end point is directed to download the



enforced anti-virus and anti-spyware client without any administrator intervention, automating the deployment of end point security.

Centralized Policy Management
The SonicWALL Global Management System (GMS) provides flexible, powerful and intuitive tools to centrally manage E-Class NSA configurations across distributed enterprises, view real-time monitoring metrics and integrate policy and compliance reporting.

Subscription Services

Each E-Class Network Security Appliance supports an expanding array of dynamic subscription-based services and software designed to integrate seamlessly into any network.

Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service delivers intelligent, real-time network security protection against sophisticated application layer and content-based attacks including viruses, spyware, worms, Trojans and software vulnerabilities such as buffer overflows.

Enforced Client and Server Anti-Virus and Anti-Spyware delivers comprehensive virus and spyware protection for laptops, desktops and servers using a single integrated client and offers automated network-wide enforcement of anti-virus and anti-spyware policies, definitions and software updates.

Content Filtering Service enforces protection and productivity policies by employing an innovative rating architecture, utilizing a dynamic database to block over 55 categories of objectionable Web content.

ViewPoint is an easy-to-use Web-based reporting tool that provides instant insight into network performance and security. Delivered through a series of historical reports using dashboards and detailed summaries, ViewPoint helps organizations of all sizes track Internet usage, fulfill regulatory compliance requirements and monitor the security status of their network.

SonicWALL E-Class Support 24x7
Designed specifically for E-Class customers, E-Class Support 24x7 delivers enterprise-class support features and quality of service. E-Class Support 24x7 includes direct access to a team of highly-trained senior support engineers for telephone and Web-based technical support on a 24x7x365 basis, software and firmware updates and upgrades, Advance Exchange hardware replacement, access to electronic support tools and moderated discussion groups, and more.

Specifications

E-Class NSA Series SKUs

SonicWALL NSA E7500
01-SSC-7000

SonicWALL NSA E6500
01-SSC-7004

SonicWALL NSA E5500
01-SSC-7008

SonicWALL NSA E7500 Security Services

SonicWALL Content Filtering Service Premium Business Edition for NSA E7500 (1-Year)
01-SSC-7329

SonicWALL GAV / IPS / Application Firewall for NSA E7500 (1-Year)
01-SSC-6130

SonicWALL Comprehensive Gateway Security Suite for NSA E7500 (1-Year)
01-SSC-9220

SonicWALL E-Class Support 24x7 for NSA E7500 (1-Year)
01-SSC-7254

SonicWALL NSA E6500 Security Services

SonicWALL Content Filtering Service Premium Business Edition for NSA E6500 (1-Year)
01-SSC-7330

SonicWALL GAV / IPS / Application Firewall for NSA E6500 (1-Year)
01-SSC-6131

SonicWALL Comprehensive Gateway Security Suite for NSA E6500 (1-Year)
01-SSC-9221

SonicWALL E-Class Support 24x7 for NSA E6500 (1-Year)
01-SSC-7257

SonicWALL NSA E5500 Security Services

SonicWALL Content Filtering Service Premium Business Edition for NSA E5500 (1-Year)
01-SSC-7331

SonicWALL GAV / IPS / Application Firewall for NSA E5500 (1-Year)
01-SSC-6132

SonicWALL Comprehensive Gateway Security Suite for NSA E5500 (1-Year)
01-SSC-9222

SonicWALL E-Class Support 24x7 for NSA E5500 (1-Year)
01-SSC-7260

Multi-year SKUs are available, please visit www.sonicwall.com.

	NSA E5500	NSA E6500	NSA E7500
Firewall			
SonicOS Version	SonicOS Enhanced 5.0 (or higher)		
Stateful Throughput[1]	2 Gbps	3 Gbps	5.5 Gbps
GAV Performance[2]	750 Mbps	900 Mbps	1.8 Gbps
IPS Performance[2]	550 Mbps	850 Mbps	1.2 Gbps
UTM Performance Throughput	400 Mbps	750 Mbps	1 Gbps
Maximum Connections	700,000	750,000	1,000,000
New Connections/Sec	10,000	19,000	25,000
Nodes Supported	Unrestricted		
Denial of Service Attack Prevention	22 classes of DoS, DDoS and scanning attacks		
VPN			
3DES/AES Throughput[1]	1.5 Gbps	2.5 Gbps	4 Gbps
Site-to-Site VPN Tunnels	4,000	6,000	10,000
Bundled Global VPN Client Licenses for Remote Access	2,000	2,000	2,000
Encryption / Authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1		
Key Exchange	IKE, IKEv2, Manual Key, PKI (X.509)		
L2TP/IPSec	Yes		
Certificate Support	Verisign, Thawte, Baltimore, RSA Keon, Entrust, and Microsoft CA for SonicWALLto-SonicWALL VPN		
Redundant VPN Gateway	Yes		
Global VPN Client Platforms Supported	Microsoft® Windows 2000, Windows XP, Microsoft® Vista 32-bit		
Deep Packet Inspection Security Services			
Deep Packet Inspection Signature Service	Comprehensive signature database. Peer- to-peer and instant messaging control and signature updates through Distributed Enforcement Architecture		
Content Filtering Service (CFS) Premium Edition	HTTP URL,HTTPS IP, keyword and content scanning ActiveX, Java Applet, and Cookie blocking		
Gateway-enforced Client Anti-Virus and Anti-Spyware	HTTP/S, SMTP, POP3, IMAP and FTP, Enforced McAfee™ Clients E-mail attachment blocking		
Application Firewall	Provides application level enforcement and bandwidth control, regulate Web traffic, e-mail, e-mail attaches and file transfers, scan and restrict documents and files for key words and phrase		
Networking			
IP Address Assignment	Static, (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP relay		
NAT Modes	1:1, 1:many, many:1, many:many, flexible NAT (overlapping IPs), PAT, transparent mode		
VLAN Interfaces (802.1q)	256	256	512
Routing	OSPF, RIPv1/v2, static routes, policy-based routing, Multicast		
QoS	Bandwidth priority. maximum bandwidth, guaranteed bandwidth, DSCP marking, 802.1p		
Authentication	XAUTH/RADIUS, Active Directory, SSO, LDAP, internal user database		
User Database	1,500 users	2,500 users	2,500 users
VoIP	Full H.323v1-5, SIP, gatekeeper support, outbound bandwidth management, VoIP over WLAN, deep inspection security, full interoperability with most VoIP gateway and communications devices		
System			
Management and Monitoring	Web GUI (HTTP, HTTPS), Command Line (SSH, Console), SNMP v2: Global management with SonicWALL GMS		
Logging and Reporting	ViewPoint®, Local Log, Syslog		
High Availability	Active/Passive with State Sync		
Load Balancing	Yes, (Outgoing with percent-based, round robin and spill-over) (Incoming with round robin, random distribution, sticky IP, block remap and symmetrical remap)		
Standards	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS		
Wireless Standards	802.11 a/b/g, WEP, WPA, TKIP, 802.1x, EAP-PEAP, EAP-TTLS		
Hardware			
Interfaces	(8) 10/100/1000 Copper Gigabit Ports, 1Gbe HA Interface, 1 Console Interface, 2 USB (Future Use)	(8) 10/100/1000 Copper Gigabit Ports, 1Gbe HA Interface, 1 Console Interface, 2 USB (Future Use)	1 Console Interface, 4 Gigabit Ethernet, 4 SFP (SX, LX or TX), 1 Gbe HA Interface, 2 USB (Future Use)
Memory (RAM)	1 GB	1 GB	2 GB
Flash Memory	512 MB Compact Flash	512 MB Compact Flash	16 MB, 512 MB Compact Flash
Power Supply	Single 250W ATX Power Supplies	Single 250W ATX Power Supplies	Dual 250W ATX, Hot Swappable
Fans	Dual Fans, Hot Swappable		
Display	Front LCD Display		
Power Input	100-240Vac, 60-50Hz		
Max Power Consumption	81 W	90 W	150 W
Total Heat Dissipation	276 BTU	307 BTU	511.5 BTU
Certifications Pending	ICSA IPSec VPN 1.0d, ICSA Firewall 4.1, FIPS 140-2 Level 2, EAL-4+		
Form Factor	1U rack-mountable		
Dimensions	17 x 16.75 x 1.75 in/43.18 x 42.54 x 4.44 cm		
Weight	15.00 lbs/ 6.80 kg	15.10 lbs/ 6.85 kg	17.30 lbs/7.9 kg
WEEE Weight	15.00 lbs/ 6.80 kg	15.10 lbs/ 6.85 kg	17.30 lbs/7.9 kg
Major Regulatory	FCC Class A, CES Class A, CE, C-Tick, VCCI, Compliance MIC, UL, cUL, TUV/GS, CB, NOM, RoHS, WEEE		
Environment	40-105° F, 5-40° C		
Humidity	10-90% non-condensing		

[1]Firewall and VPN throughput measured using UPD traffic adhering to RFC 2544. [2]Gateway AV/Anti-Spyware/IPS throughput measured using industry standard Spirent WebAvalanche HTTP Performance test.

SonicWALL, Inc.

1143 Borregas Avenue
Sunnyvale CA 94089-1306

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

SONICWALL®
PROTECTION AT THE SPEED OF BUSINESS™