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 Intelligence 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 Reassembly-Free 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 E-Class NSA Series delivers powerful threat prevention 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 Intelligence Service, 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, email 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. Utilizing 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, anti-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, E-Class NSA appliances are ideal solutions 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 Intelligence and Custom Control. Application Intelligence Service 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 email 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 intelligence 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®

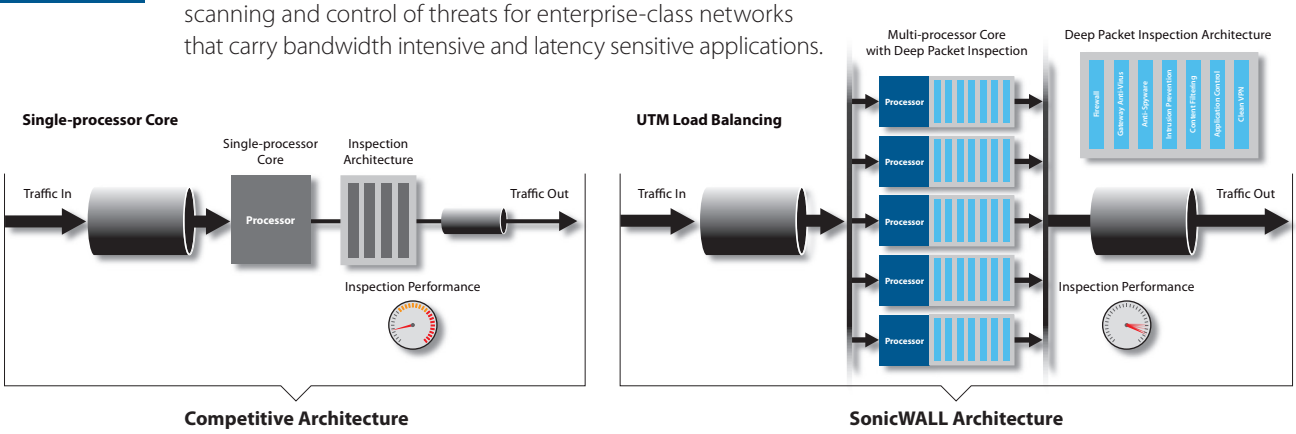
PROTECTION AT THE SPEED OF BUSINESS™

E-Class Network Security Appliance Architecture

Comprehensive, Integrated, Best-of-Breed Threat Protection

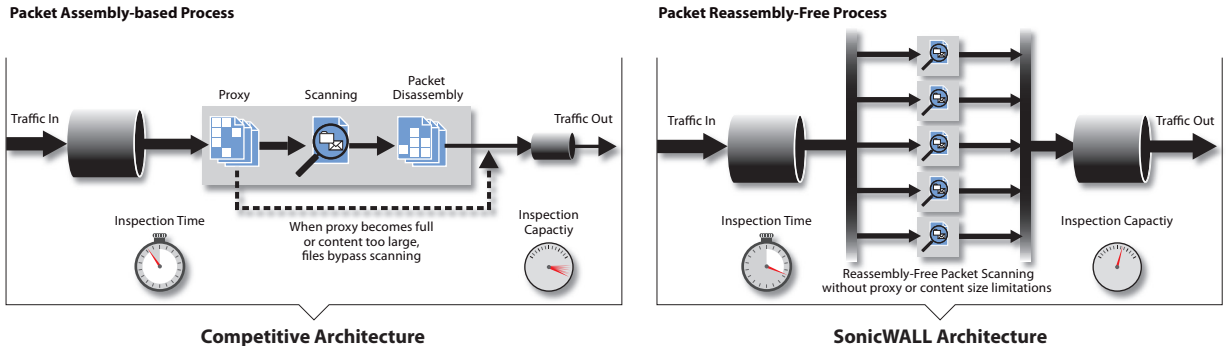
Unified Threat Management Load Balancing

Single processor designs that include multiple protection technologies are severely limited by a single centralized processor. SonicWALL UTM load balancing integrates a high-speed Reassembly-Free 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.

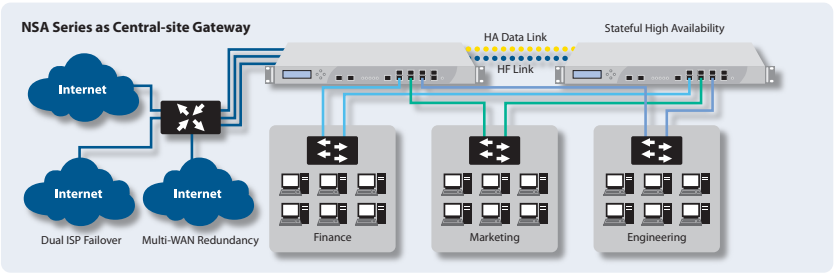


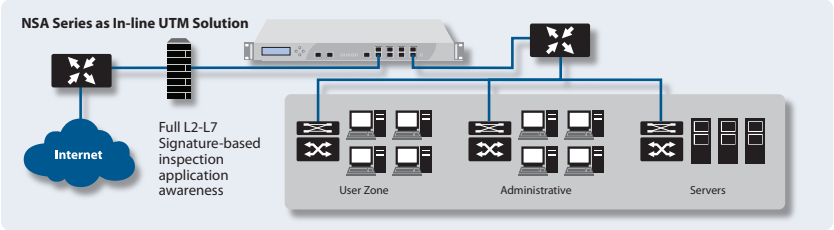
Unified Threat Management Engine

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 E-Class NSA Series provides a high-speed scalable platform, providing network segmentation and security using VLANs and security zones. Redundancy features include WAN Load balancing, ISP failover and Active/Active UTM.

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.

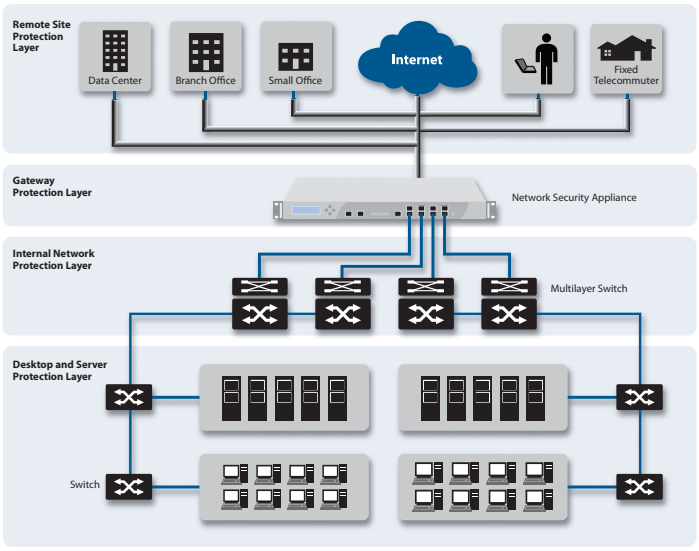
Multi-layer Protection

Remote Site Protection
The E-Class NSA Series incorporates ultra-high performance Virtual Private Networks (VPNs) that easily scale 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 endpoint 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 endpoints that do not have the latest signature or engine updates. When enforcement is enabled on the appliance, each endpoint 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, Intrusion Prevention and Application Intelligence 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 56 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.

SonicWALL Comprehensive Anti-Spam Service blocks spam phishing and virus-laden emails at the gateway. There is no need to redirect an MX Record or send email to another vendor, with one click the service is activated and immediately starts blocking junk email and saving valuable network bandwidth.

Specifications

E-Class NSA Series SKUs

SonicWALL NSA E7500
01-SSC-7000

SonicWALL NSA E7500 TotalSecure* (1-year)
01-SSC-7027

SonicWALL NSA E6500
01-SSC-7004

SonicWALL NSA E6500 TotalSecure* (1-year)
01-SSC-7028

SonicWALL NSA E5500
01-SSC-7008

SonicWALL NSA E5500 TotalSecure* (1-year)
01-SSC-7029

SonicWALL NSA E7500 Security Services

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

SonicWALL GAV / IPS / Application Intelligence 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 Intelligence 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 Intelligence 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.

*Includes one-year of Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Application Intelligence Service, Content Filtering Service, E-Class Support 24x7 and ViewPoint Reporting.

Certifications

Common Criteria EAL4+ CERTIFIED

FIPS 140-2 VALIDATED

ICSA labs CERTIFIED FIREWALL - CORPORATE

	NSA E5500	NSA E6500	NSA E7500
Firewall			
SonicOS Version	SonicOS Enhanced 5.6 (or higher)		
Stateful Throughput[1]	3.9 Gbps	5 Gbps	5.6 Gbps
GAV Performance[2]	1.0 Gbps	1.69 Gbps	1.84 Gbps
IPS Performance[2]	2.0 Gbps	2.3 Gbps	2.58 Gbps
UTM Performance[2]	850 Mbps	1.59 Gbps	1.7 Gbps
IMIX Performance[2]	1.1 Gbps	1.4 Gbps	1.6 Gbps
Maximum Connections[3]	750,000	1,000,000	1,500,000
Maximum UTM Connections	500,000	600,000	1,000,000
New Connections/Sec	15,000	20,000	25,000
Nodes Supported	Unrestricted		
Denial of Service Attack Prevention	22 classes of DoS, DDoS and scanning attacks		
SonicPoints Supported (Maximum)	96	128	128
VPN			
3DES/AES Throughput[4]	1.7 Gbps	2.7 Gbps	3 Gbps
Site-to-Site VPN Tunnels	4,000	6,000	10,000
Bundled Global VPN Client Licenses (Maximum)	2,000 (4,000)	2,000 (6,000)	2,000 (10,000)
Bundled SSL VPN Licenses (Maximum)	2 (50)	2 (50)	2 (50)
Virtual Assist Bundled (Maximum)	1 (25)	1 (25)	1 (25)
Encryption/Authentication/DH Groups	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1/DH Groups 1, 2, 5, 14		
Key Exchange	IKE, IKEv2, Manual Key, PKI (X.509), L2TP over IPSec		
Route-based VPN	Yes (OSPF, RIP)		
Certificate Support	Verisign, Thawte, Cybertrust, RSA Keon, Entrust, and Microsoft CA for SonicWALLto-SonicWALL VPN, SCEP		
Redundant VPN Gateway	Yes		
Global VPN Client Platforms Supported	Microsoft® Windows 2000, Windows XP, Microsoft® Vista 32-bit/64 bit, Windows 7		
SSL VPN Platforms Supported	Microsoft® Windows 2000 / XP / Vista 32/64-bit / Windows 7, Mac 10.4+, Linux FC 3+ / Ubuntu 7+ / OpenSUSE		
Security Services			
Deep Packet Inspection Service	Intrusion Prevention, Gateway Anti-Virus, Anti-Spyware and Application Intelligence		
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 Email attachment blocking		
Comprehensive Anti-Spam Service	Yes		
Application Intelligence	Provides application level enforcement and bandwidth control, regulate Web traffic, email, email attaches and file transfers, scan and restrict documents and files for key words and phrase		
DPI-SSL	Provides the ability to decrypt HTTPS traffic transparently, scan this traffic for threats using SonicWALL's Deep Packet Inspection technology (GAV/AS/IPS/Application Intelligence/CFS), then re-encrypt the traffic and send it to its destination if no threats or vulnerabilities are found. This feature works for both clients and servers.		
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)	400	500	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, Novell, internal user database, Terminal Services, Citrix		
IPv6	Ready	Ready	Ready
Internal Database/Single Sign-on Users	1,500/2,500 Users	2,500/4,000 Users	2,500/7,000 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, Solera Networks		
High Availability	Active/Passive with State Synch, Active/Active UTM		
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, IEEE 802.3		
Wireless Standards	802.11 a/b/g/n, WEP, WPA, WPA2, TKIP, 802.1x, EAP-PEAP, EAP-TTLS		
Hardware			
Interfaces	(8) 10/100/1000 Copper Gigabit Ports, 1Gbe HA Interface, 1 Console Interface, 2 USB	(8) 10/100/1000 Copper Gigabit Ports, 1Gbe HA Interface, 1 Console Interface, 2 USB	1 Console Interface, 4 Gigabit Ethernet, 4 SFP (SX, LX or TX), 1 Gbe HA Interface, 2 USB
Memory (RAM)	1 GB	1 GB	2 GB
Flash Memory	512 MB Compact Flash	512 MB Compact Flash	512 MB Compact Flash
3G Wireless/Modem*	With 3G USB Adapter Modem		
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
MTBF	11.9	11.9	12.4
Certifications	EAL4+, FIPS 140-2 Level 2, VPNC, ICSA Firewall 4.1		
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] Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services.

[2] UTM/Gateway AV/Anti-Spyware/IPS throughput measured using industry standard Spirent WebAvalanche HTTP performance test and Ixia test tools. Testing done with multiple flows through multiple port pairs.

[3] Actual maximum connection counts are lower when UTM services are enabled.

[4] VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544.

*USB 3G card and modem are not included. See http://www.sonicwall.com/us/products/cardsupport.html for supported USB devices."

SonicWALL's line-up of comprehensive protection

NETWORK SECURITY | SECURE REMOTE ACCESS | WEB AND E-MAIL SECURITY | BACKUP AND RECOVERY | POLICY AND MANAGEMENT

SonicWALL, Inc.
2001 Logic Drive, San Jose, CA 95124
T +1 408.745.9600 F +1 408.745.9300
www.sonicwall.com

SONICWALL®
PROTECTION AT THE SPEED OF BUSINESS™