SonicWALL® E-CLASS Network Security Appliance

FIREWALL

Next-Generation Firewall

- **Next-Generation Firewall**
- **10 GbE connectivity**
- **Powerful intrusion prevention**
- **Application intelligence, control and visualization**
- **Reassembly-Free Deep Packet Inspection technology**
- **Flexible deployment**
- **Deep Packet Inspection of SSL-encrypted traffic (DPI SSL)**
- **SonicWALL Global Response Intelligent Defense (GRID) Network**

Efficiently delivering critical corporate solutions, while also contending with employee use of wasteful and often dangerous applications can be a serious challenge for IT administrators. Critical applications need bandwidth prioritization while social media and gaming applications need to be bandwidth throttled or even completely blocked. Stateful packet inspection firewalls used in many organizations rely on port and protocol, they cannot solve the problem because they are not able to identify the applications. Boiling it down, stateful packet inspection firewalls cannot sort out the good from the bad.

SonicWALL® E-Class Network Security Appliance (NSA) Series solutions provide enterprise-performance featuring tightly integrated intrusion prevention, anti-malware protection and application intelligence, control and visualization. Combining SonicWALL's patented Reassembly-Free Deep Packet Inspection™ (RFDPI)* technology with a powerful multi-core hardware platform, E-Class NSA Series solutions can analyze and control thousands of unique applications, even if encrypted with SSL. The E-Class NSA Series can be deployed as either a Next-Generation Firewall or Unifed Threat Management Firewall.

Comprised of SonicWALL E-Class NSA E8510, E8500, E7500, E6500 and E5500 appliances, the E-Class NSA Series offers a broad range of scalable solutions for the most demanding of enterprise deployments in data centers, campus networks and distributed environments. As inline solutions, the E-Class NSA Series leverages existing infrastructure while adding an extra layer of network security and visibility. In security gateway deployments, it adds secure remote access, high availability and other enterprise features.

The E-Class NSA Series is a key part of SonicWALL's portfolio of enterprise-class products and services for network security, email security and secure remote access.

Features and Benefits

SonicWALL's **Next-Generation Firewall** including Reassembly-Free Deep Packet Inspection tightly integrates intrusion prevention, malware protection, and newly enhanced application intelligence and control with real-time visualization.

10 GbE connectivity on the NSA E8510 allows deployment to environments with a 10 GbE infrastructure.

Powerful intrusion prevention protects against a comprehensive array of network-based application layer threats by scanning packet payloads for worms, Trojans, software vulnerabilities, application exploits, and other malicious code.

Application intelligence, control and visualization provides granular control and real-time visualization of applications to guarantee bandwidth prioritization and ensure maximum network security and productivity.

Reassembly-Free Deep Packet Inspection technology provides control for thousands of applications and detects millions of pieces of malware to protect the network automatically and seamlessly, while inspecting hundreds of thousands of connections simultaneously across all ports, with near zero latency and unlimited stream size.

Flexible deployment as either a traditional gateway or as an inline solution allows administrators to keep their existing network infrastructure, while adding application intelligence and control as an extra layer of security and visibility.

Deep Packet Inspection of SSL-encrypted traffic (DPI SSL) transparently decrypts and scans both inbound and outbound HTTPS traffic using SonicWALL RFDPI. The traffic is then re-encrypted and sent to its original destination if no threats or vulnerabilities are discovered.

The **SonicWALL Global Response Intelligent Defense (GRID) Network** continually updates threat protection, intrusion detection and prevention and application control services on a 24x7 basis to maximize security. The full suite of threat prevention services can defend against over a million unique malware attacks.

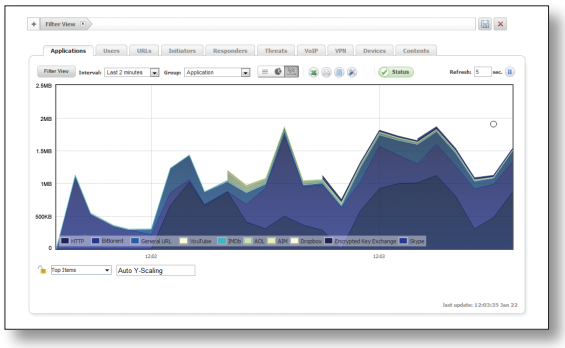
* U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

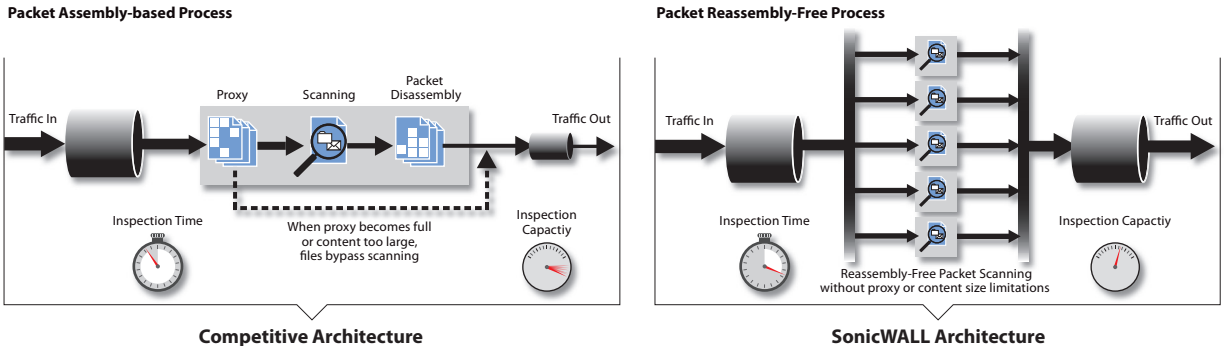
Application Intelligence and Control Technology

SonicWALL Application Intelligence and Control provides granular control and real-time visualization of applications to guarantee bandwidth prioritization and ensure maximum network security and productivity. An integrated feature of SonicWALL Next-Generation Firewalls, it uses Reassembly-Free Deep Packet Inspection technology to identify and control applications in use, regardless of port or protocol. With a continuously expanding threat signature database that currently recognizes over 3,500 applications and millions of malware threats, it can maintain granular control over applications, prioritize or throttle bandwidth and deny Web site access. The SonicWALL App Flow Monitor provides real-time graphs of applications, ingress and egress bandwidth, active Website connections and user activity, and can continuously send data to NetFlow/IPFIX analyzers.

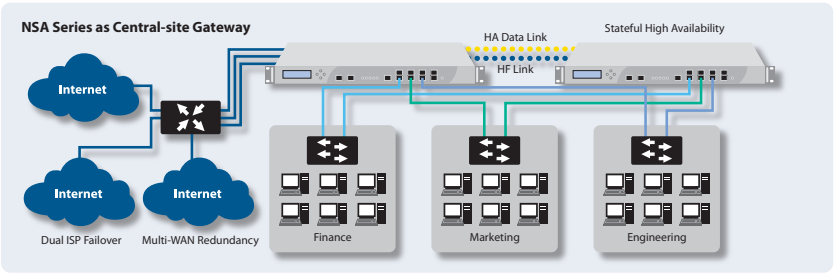


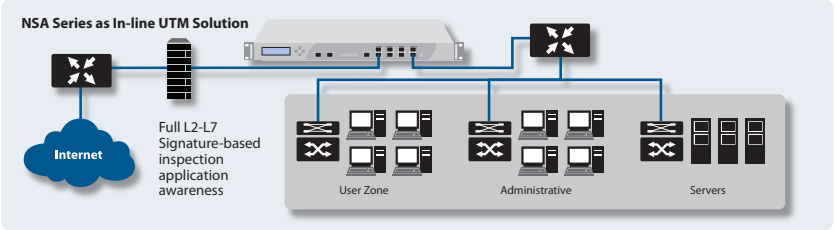
Reassembly-Free Deep Packet Inspection Engine

The SonicWALL Reassembly-Free Deep Packet Inspection delivers a scalable application 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 control 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 DPI.

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.

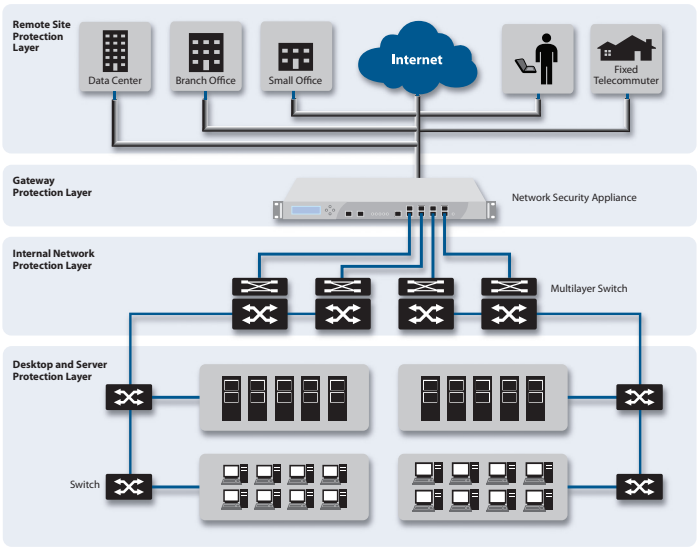
Multi-layer Protection

Remote Site Protection
The E-Class NSA Series incorporates ultra-high performance Virtual Private Networks (VPNs) that easily scale to thousands of endpoints 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 endpoint 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.

Application Intelligence and Control provides real-time visualization of network traffic, customizable policies and highly granular control over applications and users.

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.

E-Class Support 24x7 is 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, moderated discussion groups, and more.

Deep Packet Inspection for of SSL-Encrypted Traffic (DPI SSL) transparently decrypts and scans both inbound and outbound HTTPS traffic using SonicWALL RFDPI. The traffic is then re-encrypted and sent to its original destination if no threats or vulnerabilities are discovered.

Enforced Client 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.

E-Class NSA Series SKUs

SonicWALL NSA E8510
01-SSC-9770

SonicWALL NSA E8500
01-SSC-8866

SonicWALL NSA E8500 High Availability
01-SSC-8867

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 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 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 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.

Specifications

	NSA E5500	NSA E6500	NSA E7500	NSA 8500	NSA 8510
Firewall					
SonicOS Version	SonicOS Enhanced 5.6 (or higher)				SonicOS Enhanced 5.8.1 (or higher)
Stateful Throughput[1]	3.9 Gbps	5 Gbps	5.6 Gbps	8.0 Gbps	
GAV Performance[2]	1.0 Gbps	1.69 Gbps	1.84 Gbps	2.25 Gbps	
IPS Performance[2]	2.0 Gbps	2.3 Gbps	2.58 Gbps	3.7 Gbps	
Full Deep Packet Inspection (DPI) Performance[2]	850 Mbps	1.59 Gbps	1.7 Gbps	2.2 Gbps	
IMIX Performance[2]	1.1 Gbps	1.4 Gbps	1.6 Gbps	2.0 Gbps	
Maximum Connections[3]	750,000	1,000,000	1,500,000	1,500,000	
Maximum Full DPI Connections	500,000	600,000	1,000,000	1,250,000	
New Connections/Sec	30,000	60,000	64,000	85,000	
Nodes Supported	Unrestricted				
Denial of Service Attack Prevention	22 classes of DoS, DDoS and scanning attacks				
SonicPoints Supported (Maximum)	96	128			
VPN					
3DES/AES Throughput[4]	1.7 Gbps	2.7 Gbps	3.0 Gbps	4.0 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 32/64-bit, 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, bandwidth management on rating categories, custom allow/forbid lists				
Enforced Client Anti-Virus and Anti-Spyware	HTTP/S, SMTP, POP3, IMAP and FTP, Enforced McAfee™ Clients Email attachment blocking				
Comprehensive Anti-Spam Service[5]	Supported				
Application Intelligence and Control	Application bandwidth management and control, prioritize or block application by signatures, control file transfers, scan for key words or phrases				
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	Yes				
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				
Link Aggregation	Yes				
Port Redundancy	Yes				
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, NetFlow v5/v9, IPFIX with Extensions, Real-time Visualization				
High Availability	Active/Passive with State Synch, Active/Active DPI				
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		(4) SFP (SX, LX or TX), (4) 10/100/1000 GbE, 1GbE HA Interface, 2 USB, 1 Console Interface		(2) SFP+ 10GbE, (4) 10/100/1000 GbE, 1 GbE HA Interface, 2 USB, 1 Console Interface
Memory (RAM)	1 GB	1 GB	2 GB	4 GB	
Flash Memory	512 MB Compact Flash				
3G Wireless/Modem[6]	With a supported 3G Adapter or Analog Modem				
Power Supply	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			ICSA Firewall 4.1	—
Certifications Pending	—			EAL4+, FIPS 140-2 Level 2, VPNC	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] Full DPI/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 Full DPI 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.* [5] The Comprehensive Anti-Spam Service supports an unrestricted number of users but is recommended for 250 users or less.

Certifications

Common Criteria EAL4+ CERTIFIED

FIPS VALIDATED 140-2

ICSA labs CERTIFIED FIREWALL - ENTERPRISE

SonicWALL's line-up of dynamic security solutions

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®
DYNAMIC SECURITY FOR THE GLOBAL NETWORK™