

SonicWALL® E-CLASS Network Security Appliance



FIREWALL

Next-Generation Firewall

- **Next-Generation Firewall**
- **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**

It can be a real challenge for IT administrators to efficiently deliver critical corporate solutions while also contending with employee use of wasteful and often dangerous applications. 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, 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.

The SonicWALL® E-Class Network Security Appliance (NSA) E8500 provides a Next-Generation Firewall with tightly integrated intrusion prevention, malware protection and powerful application intelligence, control and visualization. With the patented SonicWALL Reassembly-Free Deep Packet Inspection™ (RFDPI) technology*, the NSA E8500 can analyze and control over 2,800 applications, even if they are encrypted with SSL. This exceptional combination of software sophistication and incredibly powerful hardware leaves little room for application traffic to hide on the network, since SonicWALL's RFDPI engine is capable of inspecting hundreds of thousands of connections simultaneously across all ports, with near zero latency and without file size limitations.

The NSA E8500 can be deployed both inline and as a gateway in a network. When deployed as an inline solution, the NSA E8500 allows administrators to leave their existing infrastructure intact and add application intelligence and control as an extra layer of security and visibility to their network. The NSA E8500 can also serve as a full-featured security gateway with all the required remote access, high availability and enterprise features expected in demanding deployments.

Features and Benefits

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

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 over 2,800 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. Patent 7,310,815-A method and apparatus for data stream analysis and blocking.



Specifications



SonicWALL NSA E8500
01-SSC-8866
Includes a DPI SSL license and 1-year of Security Services including IPS/GAV/Application Control



SonicWALL NSA E8500 High Availability
01-SSC-8867

NSA E8500	
Firewall	
Stateful Throughput ¹	8.0 Gbps
IPS Performance ²	3.7 Gbps
GAV Performance ²	2.25 Gbps
Full Deep Packet Inspection (DPI) Performance ²	2.2 Gbps
IMIX Performance ²	2.0 Gbps
Maximum Connections ³	1,500,000
Maximum DPI Connections	1,250,000
New Connections/Sec	80,000
Nodes Supported	Unrestricted
Denial of Service Attack Prevention	22 classes of DoS, DDoS and scanning attacks
SonicPoints Support (Maximum)	128
VPN	
3DES/AES Throughput ⁴	4.0 Gbps
Site-to-Site VPN Tunnels	10,000
Bundled Global VPN Client Licenses (Maximum)	2,000 (10,000)
Bundled SSL VPN Licenses (Maximum)	2 (50)
Bundled Virtual Assist Technicians (Maximum)	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 SonicWALL-to-SonicWALL VPN, SCEP
Redundant 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 Service	Intrusion Prevention (included), Gateway Anti-Virus, Anti-Spyware, Application Intelligence and Control (included)
Content Filtering Service (CFS) Premium Edition	HTTP URL, HTTP/S IP, keyword and content scanning ActiveX, Java Applet, and Cookie blocking, bandwidth management on filtering categories, 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 (included)	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 transparently decrypt HTTPS traffic in both directions, 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.
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)	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
Internal Database/Single Sign-on 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 Sync, Active/Active DPI 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, IEEE 802.3
Wireless Standards (With SonicPoint APs)	802.11 a/b/g/n, WEP, WPA, WPA2, TKIP, 802.1x, EAP-PEAP, EAP-TTLS
Hardware	
Interfaces	4 Gigabit Ethernet, 4 SFP (SX, LX or TX), 1 GbE HA Interface, 2 USB, 1 Console Interface
Memory (RAM)	4 GB
Flash Memory	512 MB Compact Flash
3G Wireless/Modem ⁶	With 3G USB Adapter/Modem
Power Supply	Dual 250W ATX, Hot Swappable
Fans	Dual Fans, Hot Swappable
Display	Front LCD Display
Power Input	100-240Vac, 60-50Hz
Max Power Consumption	150 W
Total Heat Dissipation	511.5 BTU
MTBF	12.4 Years
Certifications	Pending: EAL4+, FIPS 140-2, ICSA Firewall 4.1; Current: VPNC
Form Factor	1U rack-mountable
Dimensions	17 x 16.75 x 1.75 in/43.18 x 42.54 x 4.44 cm
Weight	17.30 lbs/7.9 kg
WEEE Weight	17.30 lbs/7.9 kg
Major Regulatory	FCC Class A, CES Class A, CE, C-Tick, VCCI, Compliance MIC, UL, cUL, TUVGS, 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. ⁵ USB 3G card and modem are not included. See <http://www.sonicwall.com/us/products/cardsupport.html> for supported USB devices. ⁶ The Comprehensive Anti-Spam Service supports an unrestricted number of users but is recommended for 250 users or less.

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

