

SonicWALL® E-CLASS Network Security Appliance



NETWORK SECURITY

SonicWALL NSA E8500 for Application Intelligence and Control

- **Application intelligence and control**
- **SonicWALL Reassembly-Free Deep Packet Inspection**
- **Powerful intrusion prevention**
- **Flexible deployment**
- **Dynamic security**
- **Deep Packet Inspection of SSL-encrypted traffic (DPI SSL)**

A fundamental problem continues to emerge for CIOs and IT administrators: as they strive to increase workforce productivity and improve the quality of internal services, they lack insight into the total traffic intelligence on their networks. This information is required for accurate performance analysis, threat discovery and for the ability to take immediate action to ensure smooth operations of critical systems.

Capturing traffic intelligence has become increasingly elusive for conventional tools that identify protocols by their respective ports, as newer applications become more Web-enabled and increasingly utilize common protocols such as HTTP/HTTPS. As a result, traditional firewalls have grown blind to the application traffic on the network, to the threats that can travel through these applications and to the inefficient use of the network through these applications. For example, although HTTP/HTTPS traffic looks benign to traditional firewalls, it can carry some of the most bandwidth intensive and potentially security compromising applications, including streaming video and audio, chat traffic and various document formats. The same can be said for social networking sites which, although not formally classified as true applications, utilize the same technologies, exposing companies to malware and competing for bandwidth with mission critical applications. To regain control of this traffic, traditional firewalls must evolve far beyond basic stateful inspection and must analyze traffic at the application layer. The ability to perform this task relies completely on deep packet inspection, which is the only technology capable of exposing all of these types of network activity.

The SonicWALL E-Class Network Security Appliance (NSA) E8500 offers Dynamic Security for the Global Network by providing powerful application intelligence and control along with network intrusion detection and prevention. With the patented SonicWALL® Reassembly-Free Deep Packet Inspection™ (RFDPI) engine and sophisticated application intelligence capabilities, the NSA E8500 can analyze and control over 2,700 unique applications, whether they are encrypted with SSL or are unencrypted. This exceptional combination of software sophistication and incredibly powerful hardware leaves little room for application traffic to hide on the network, since SonicWALL's patented RFDPI™ engine is capable of inspecting hundreds of thousands of connections simultaneously across all ports equally, with nearly 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

Application intelligence and control is provided by a configurable set of granular application-specific policies that can be applied per user, application, schedule or IP subnet. These policies can be used to restrict transfer of specific files and documents, scan email attachments via user-configurable criteria, automate application bandwidth allocation, control and inspect both internal and external Web access and enable users to add custom signatures.

SonicWALL Reassembly-Free Deep Packet Inspection is capable of controlling over 2,700 unique application uses on the network while inspecting hundreds of thousands of connections simultaneously across all ports, with nearly zero latency and unlimited stream size.

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

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

Dynamic security 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 1,000,000+ unique malware attacks.

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.

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

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	Intrusion Prevention (included), Gateway Anti-Virus, Anti-Spyware, Application Intelligence and Control (included)
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	HTTPS, SMTP, POP3, IMAP and FTP, Enforced McAfee™ Clients Email attachment blocking
Comprehensive Anti-Spam Service	Yes
Application Intelligence (included)	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 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
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 Sync, Active/Active UTM 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*	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, CE-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 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.

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



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™