E-Class Network Security Appliance Series

Next-Generation Firewall

Today's enterprise applications reside on both the network and in the cloud. These applications can be either productive business solutions or counterproductive—and often dangerous—diversions. Critical applications need bandwidth prioritization, while social media and gaming applications need to be bandwidth throttled or even completely blocked. Traditional stateful packet inspection firewalls only scan for ports and protocols—not applications—so they cannot tell the good applications from the bad.

Dell™ 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 Dell 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. Integrated application traffic analytics reporting provides the E-Class NSA Series with powerful insight into network usage.

Comprised of Dell SonicWALL E-Class NSA E8510, E8500, 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 Dell SonicWALL's portfolio of enterprise-class products and services for network security, email security and secure remote access.

- **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)**
- **Dell SonicWALL Global Response Intelligent Defense (GRID) Network**
- **WAN Acceleration**
- **Remote access for the mobile enterprise**
- **Active/Active Clustering**
- **Border Gateway Protocol (BGP) support**
- **More concurrent SSL VPN sessions**

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

Features and benefits

Dell 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, data leakage prevention, 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 Dell SonicWALL RFDPI. The traffic is then re-encrypted and sent to its original destination if no threats or vulnerabilities are discovered.

The **Dell 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.

WAN acceleration decreases latency and increases transfer speeds between remote sites for even higher network efficiency gains.

Remote access for the mobile enterprise provides secure connectivity to corporate resources from Windows®, Linux®, Apple® Macintosh and iOS and Google® Android™ devices.

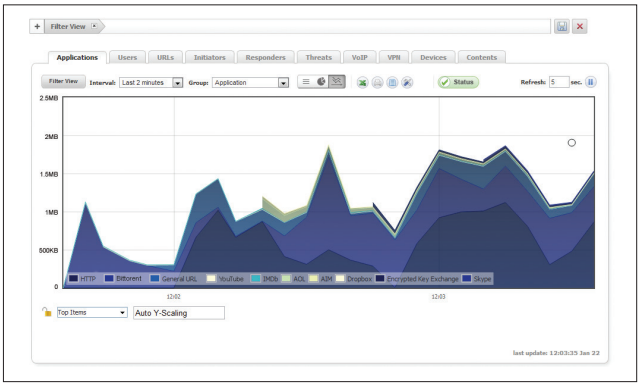
Active/Active Clustering of up to four pairs of Dell SonicWALL firewalls lets you assign traffic flows to each node, providing load sharing, redundancy and greater throughput without a single point of failure.

Border Gateway Protocol (BGP) support enables alternate network access paths (ISPs) if one path fails. Combined with Active/Active Clustering, BGP improves business continuity and productivity.

More concurrent SSL VPN sessions add scalability, while extending End Point Control to Microsoft® Windows® devices ensures anti-malware and firewalls are up-to-date.

Application intelligence and control technology

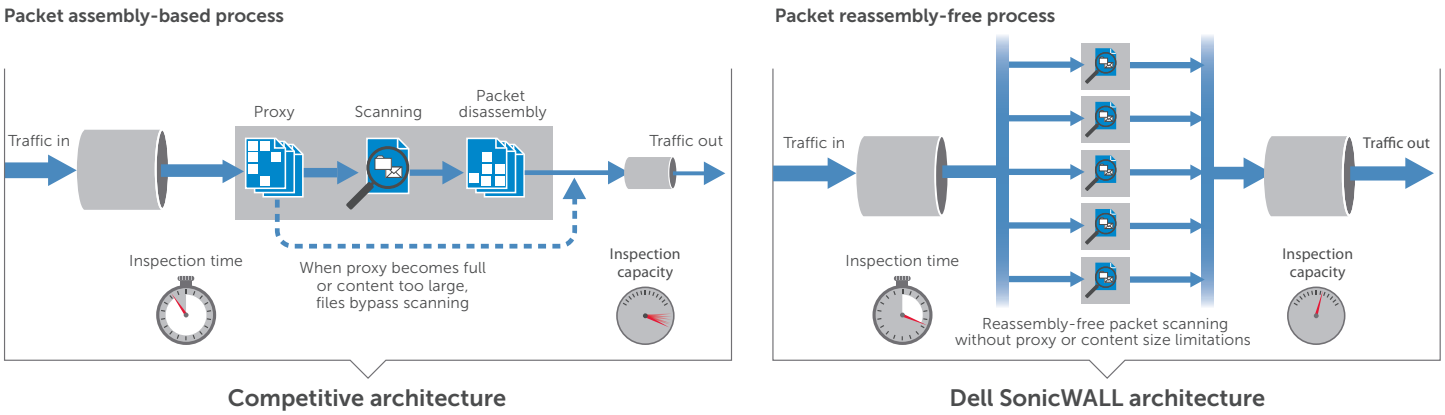
Dell SonicWALL Application Intelligence and Control provides granular control, DLP and real-time visualization of applications to guarantee bandwidth prioritization and ensure maximum network security and productivity. An integrated feature of Dell SonicWALL Next-Generation Firewalls, it uses Reassembly-Free 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 3,700 applications and millions of malware threats, it can maintain granular control over applications, prioritize or throttle bandwidth and deny web site access. The Dell SonicWALL App Flow Monitor provides real-time graphs of applications, ingress and egress bandwidth, active web site connections and user activity, and can continuously send data to NetFlow/IPFIX analyzers.



Software

Reassembly-Free Deep Packet Inspection engine

Dell 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

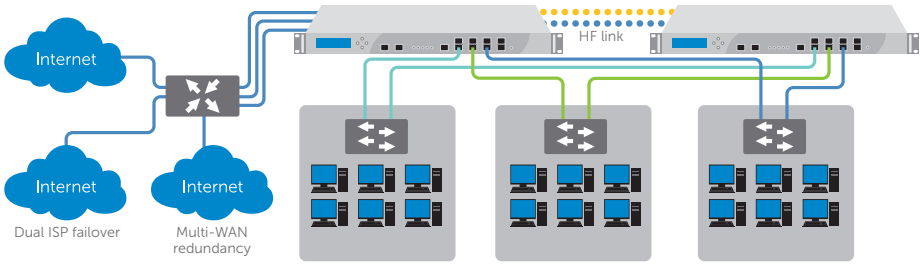
Deployed as a central-site gateway, the E-Class NSA Series provides a high-speed scalable platform, providing network segmentation and security using VLANs and security zones. Redundancy features include WAN Load balancing, ISP failover and Active/Active DPI.

Layer 2 bridge mode

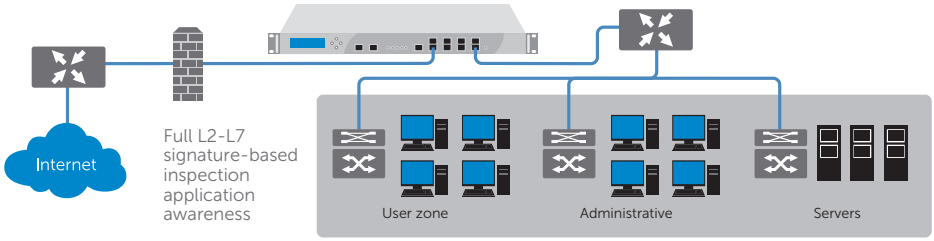
Layer 2 bridge mode provides inline intrusion detection and prevention, adds an additional level of zone-based security to network segments or business units and simplifies layered security. Additionally, this enables administrators to limit access to sensitive data by specific business unit or database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

Wire mode

In addition to, Layer 2 Bridge Mode and other traditional interface modes, E-Class NSA also features Wire Mode, which provides four methods non-disruptive, incremental insertion into networks: Bypass Mode, Inspect Mode, Secure Mode and Tap Mode.



E-Class NSA Series as in-line NGFW solution



Multi-layer protection

Remote site protection

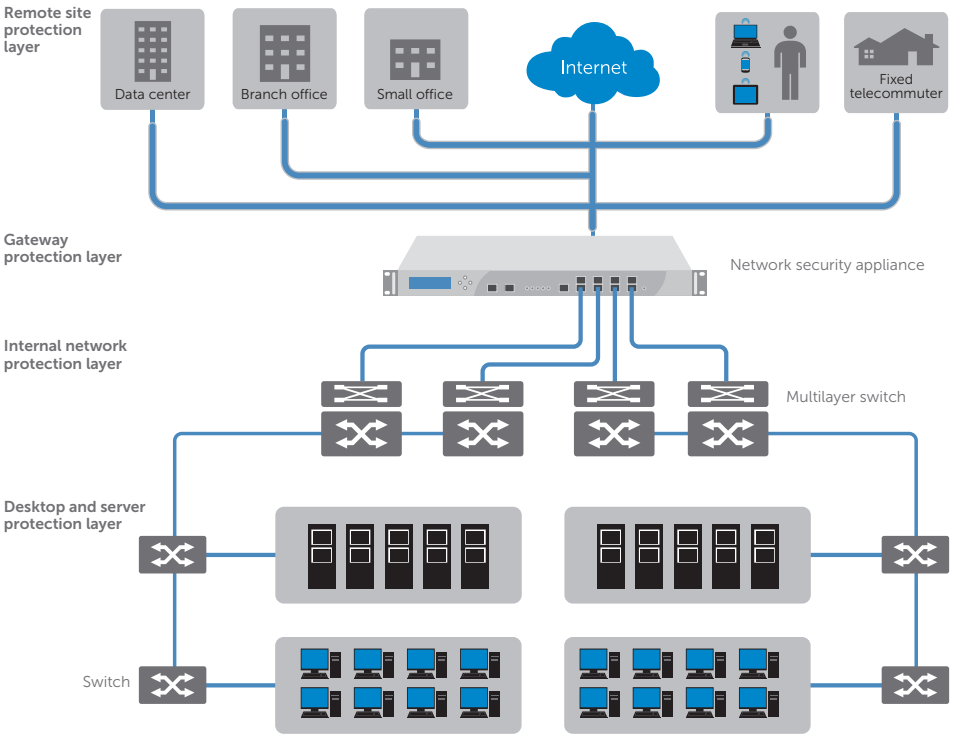
The E-Class NSA Series incorporates ultra-high performance Virtual Private Networks (VPNs) that easily scale to thousands of endpoints and branch offices. Innovative Dell SonicWALL Clean VPN™ technology prevents vulnerabilities and malicious code by decontaminating traffic before it enters the corporate 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.

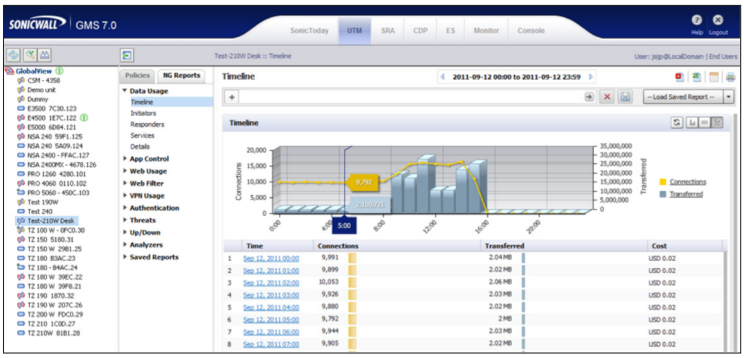


Desktop and server protection

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 Dell SonicWALL Global Management System (GMS®) provides organizations, distributed enterprises and service providers with a flexible, powerful and intuitive solution to centrally manage and report on E-Class NSA Next-Generation Firewalls.



Global Management System

DELL Software

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.

Analyzer is an easy-to-use web-based application traffic analytics and reporting tool that provides real-time and historical insight into the health, performance and security of the 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 Dell 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 (McAfee) working in conjunction with Dell SonicWALL firewalls, guarantees that all endpoints have the latest versions of anti-virus and anti-spyware software installed and active.

SonicWALL Mobile Connect™, a single unified client app for Apple® iOS and Google® Android™, provides smartphone and tablet users superior network-level access to corporate and academic resources over encrypted SSL VPN connections.

Specifications

Firewall	NSA E5500	NSA E6500	NSA 8500	NSA 8510
SonicOS version	SonicOS Enhanced 5.6 (or higher)		SonicOS Enhanced 5.8.0.6 (or higher)	
Stateful throughput[1]	3.9 Gbps	5 Gbps	8.0 Gbps	
GAV performance[2]	1.0 Gbps	1.69 Gbps	2.25 Gbps	
IPS performance[2]	2.0 Gbps	2.3 Gbps	3.7 Gbps	
Full Deep Packet Inspection (DPI) performance[2]	850 Mbps	1.59 Gbps	2.2 Gbps	
IMIX performance[2]	1.1 Gbps	1.4 Gbps	2.0 Gbps	
Maximum connections[3]	750,000	1,000,000	1,500,000	
Maximum full DPI connections	500,000	600,000	1,250,000	
New connections/sec	30,000	60,000	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	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, SHA2/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 Dell SonicWALL to-Dell 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			
Mobile Connect platforms supported	iOS 4.2 and higher, Android™ 4.0 and higher			
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	McAfee®			
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 Dell 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 v3: Global management with Dell SonicWALL GMS			
Logging and reporting	Analyzer, Scrutinizer, GMS, 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			
WAN acceleration support[6]	Yes			
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	4 GB	
Flash memory	512 MB compact flash			
3G wireless/modem*	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, IPv6 phase 1, IPv6 phase 2		ICSA firewall 4.1	
Certifications pending	—		EAL4+, FIPS 140-2 level 2, VPNC, ICSA Firewall 4.1, IPv6 phase 1 and 2	EAL4+, FIPS 140-2 level 2, VPNC, ICSA Firewall 4.1, IPv6 phase 1 and 2
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.
[6] With Dell SonicWALL WXA Series Appliances

Network Security Appliance E8510
01-SSC-9770

Network Security Appliance E8500
01-SSC-8866

Network Security Appliance E6500
01-SSC-7004

Network Security Appliance E6500 TotalSecure* (1-year) 01-SSC-7028

Network Security Appliance E5500
01-SSC-7008

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

Network Security Appliance E8500 Security Services

GAV/IPS/Application Intelligence for NSA E8500 (1-year) 01-SSC-8940

Comprehensive Gateway Security Suite for NSA E8500 (1-year) 01-SSC-8950

E-Class Support 24x7 for NSA E8500 (1-year) 01-SSC-8946

Network Security Appliance E6500 Security Services

GAV/IPS/Application Intelligence for NSA E6500 (1-year) 01-SSC-6131

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

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

Network Security Appliance E5500 Security Services

GAV/IPS/Application Intelligence for NSA E5500 (1-year) 01-SSC-6132

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

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 and E-Class Support 24x7.

Security Monitoring Services from Dell SecureWorks are available for this appliance Series. For more information, visit **www.dell.com/secureworks**

Certifications

Common Criteria EAL4+ CERTIFIED

FIPS VALIDATED 140-2

ICSA labs CERTIFIED FIREWALL - CORPORATE

DELL Software