

# 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**
- **WAN Acceleration**

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.

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

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.

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

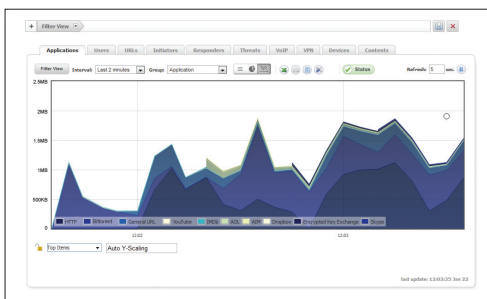
\* U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Application Intelligence and Control Technology

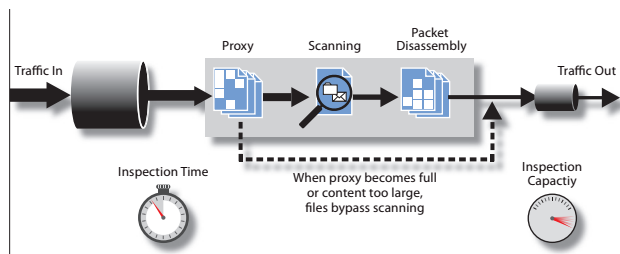
SonicWALL Application Intelligence and Control provides granular control and real-time visualization of applications to guarantee bandwidth prioritization and ensure maximum network security and productivity. An integrated feature of SonicWALL Next-Generation Firewalls, it uses Reassembly-Free Deep Packet 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 web site connections and user activity, and can continuously send data to NetFlow/IPFIX analyzers.



Reassembly-Free Deep Packet Inspection Engine

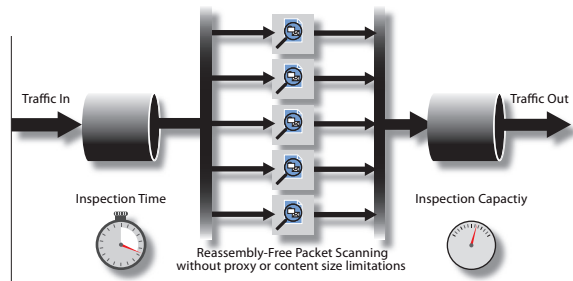
The SonicWALL Reassembly-Free Deep Packet Inspection delivers a scalable application inspection engine that can analyze files and content of any size in real-time without reassembling packets or application content. This means of inspection is designed specifically for real-time applications and latency 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.

Packet Assembly-based Process



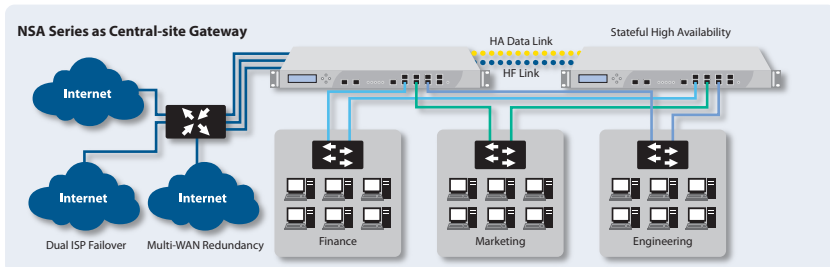
Competitive Architecture

Packet Reassembly-Free Process



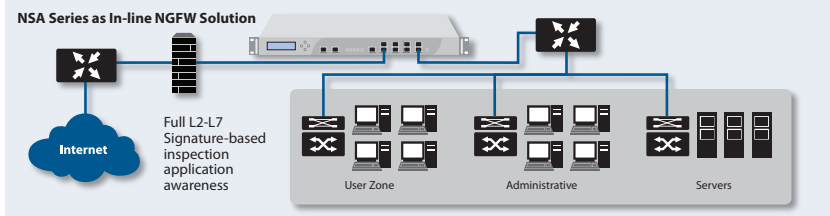
SonicWALL Architecture

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**

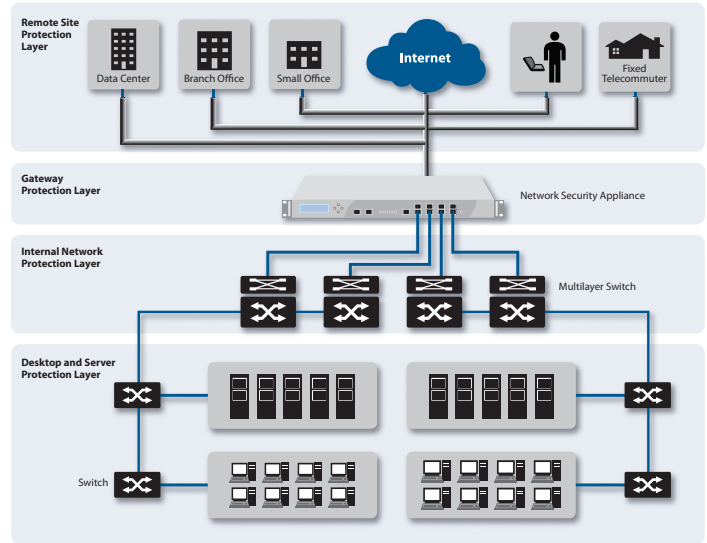
Easily integrated into existing environments, E-Class NSAs centralize gateway-level protection across all incoming and outgoing applications, files and content-based traffic, while controlling bandwidth and applications, without significantly impacting performance or scalability.

**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.

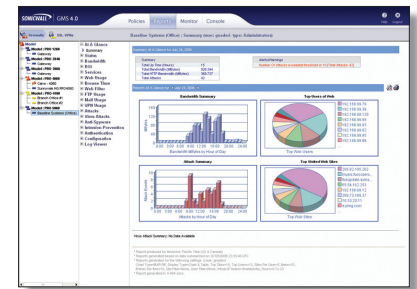
**Desktop and Server Protection**

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 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.



**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 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.

## Specifications

### 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](http://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.

### Certifications



	NSA E5500	NSA E6500	NSA E7500	NSA 8500	NSA 8510
<b>Firewall</b>					
<b>SonicOS Version</b>	SonicOS Enhanced 5.6 (or higher)				SonicOS Enhanced 5.8.0.6 (or higher)
<b>Stateful Throughput<sup>1</sup></b>	3.9 Gbps	5 Gbps	5.6 Gbps	8.0 Gbps	
<b>GAV Performance<sup>2</sup></b>	1.0 Gbps	1.69 Gbps	1.84 Gbps	2.25 Gbps	
<b>IPS Performance<sup>2</sup></b>	2.0 Gbps	2.3 Gbps	2.58 Gbps	3.7 Gbps	
<b>Full Deep Packet Inspection (DPI) Performance<sup>2</sup></b>	850 Mbps	1.59 Gbps	1.7 Gbps	2.2 Gbps	
<b>IMIX Performance<sup>2</sup></b>	1.1 Gbps	1.4 Gbps	1.6 Gbps	2.0 Gbps	
<b>Maximum Connections<sup>2</sup></b>	750,000	1,000,000	1,500,000	1,500,000	
<b>Maximum Full DPI Connections</b>	500,000	600,000	1,000,000	1,250,000	
<b>New Connections/Sec</b>	30,000	60,000	64,000	85,000	
<b>Nodes Supported</b>	Unrestricted				
<b>Denial of Service Attack Prevention</b>	22 classes of DoS, DDoS and scanning attacks				
<b>SonicPoints Supported (Maximum)</b>	96				128
<b>VPN</b>					
<b>3DES/AES Throughput<sup>4</sup></b>	1.7 Gbps	2.7 Gbps	3.0 Gbps	4.0 Gbps	
<b>Site-to-Site VPN Tunnels</b>	4,000	6,000	10,000		
<b>Bundled Global VPN Client Licenses (Maximum)</b>	2,000 (4,000)	2,000 (6,000)	2,000 (10,000)		
<b>Bundled SSL VPN Licenses (Maximum)</b>	2 (50)	2 (50)	2 (50)		
<b>Virtual Assist Bundled (Maximum)</b>	1 (25)	1 (25)	1 (25)		
<b>Encryption/Authentication/DH Groups</b>	DES, 3DES, AES (128, 192, 256-bit)/MDS, SHA-1/DH Groups 1, 2, 5, 14				
<b>Key Exchange</b>	IKE, IKEv2, Manual Key, PKI (X.509), L2TP over IPSec				
<b>Route-based VPN</b>	Yes (OSPF, RIP)				
<b>Certificate Support</b>	Verisign, Thawte, Cybertrust, RSA Keon, Entrust, and Microsoft CA for SonicWALLto-SonicWALL VPN, SCEP				
<b>Redundant VPN Gateway</b>	Yes				
<b>Global VPN Client Platforms Supported</b>	Microsoft® Windows 2000, Windows XP, Microsoft® Vista 32-bit/64 bit, Windows 7				
<b>SSL VPN Platforms Supported</b>	Microsoft® Windows 2000 / XP / Vista 32/64-bit / Windows 7 32/64-bit, Mac 10.4+, Linux FC 3+ / Ubuntu 7+ / OpenSUSE				
<b>Security Services</b>					
<b>Deep Packet Inspection Service</b>	Intrusion Prevention, Gateway Anti-Virus, Anti-Spyware and Application Intelligence				
<b>Content Filtering Service (CFS) Premium Edition</b>	HTTP, URL, HTTPS IP, keyword and content scanning ActiveX, Java Applet, and Cookie blocking, bandwidth management on rating categories, custom allow/forbid lists				
<b>Enforced Client Anti-Virus and Anti-Spyware</b>	HTTP/S, SMTP, POP3, IMAP and FTP, Enforced McAfee™ Clients Email attachment blocking				
<b>Comprehensive Anti-Spam Service<sup>5</sup></b>	Supported				
<b>Application Intelligence and Control</b>	Application bandwidth management and control, prioritize or block application by signatures, control file transfers, scan for key words or phrases				
<b>DPISSL</b>	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.				
<b>Networking</b>					
<b>IP Address Assignment</b>	Static, (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP relay				
<b>NAT Modes</b>	1:1, 1:many, many:1, many:many, flexible NAT (overlapping IPs), PAT, transparent mode				
<b>VLAN Interfaces (802.1q)</b>	400	500	512		
<b>Routing</b>	OSPF, RIPv1/v2, static routes, policy-based routing, Multicast				
<b>QoS</b>	Bandwidth priority, maximum bandwidth, guaranteed bandwidth, DSCP marking, 802.1p				
<b>Authentication</b>	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, Internal user database, Terminal Services, Citrix				
<b>IPv6</b>	Yes				
<b>Internal Database/Single Sign-on Users</b>	1,500/2,500 Users	2,500/4,000 Users	2,500/7,000 Users		
<b>VoIP</b>	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				
<b>Link Aggregation</b>	Yes				
<b>Port Redundancy</b>	Yes				
<b>System</b>					
<b>Management and Monitoring</b>	Web GUI (HTTP, HTTPS), Command Line (SSH, Console), SNMP v2: Global management with SonicWALL GMS				
<b>Logging and Reporting</b>	Analyzer, Scrutinizer, GMS, Local Log, Syslog, Solera Networks, NetFlow v5/v9, IPFIX with Extensions, Real-time Visualization				
<b>High Availability</b>	Active/Passive with State Synchron, Active/Active DPI				
<b>Load Balancing</b>	Yes, (Outgoing with percent-based, round robin and spill-over) (Incoming with round robin, random distribution, sticky IP, block remap and symmetrical remap)				
<b>Standards</b>	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3				
<b>Wireless Standards</b>	802.11 a/b/g/n, WEP, WPA, WPA2, TKIP, 802.1x, EAP-PEAP, EAP-TTLS				
<b>WAN Acceleration Support<sup>6</sup></b>	Yes				
<b>Hardware</b>					
<b>Interfaces</b>	(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	
<b>Memory (RAM)</b>	1 GB	1 GB	2 GB	4 GB	
<b>Flash Memory</b>	512 MB Compact Flash				
<b>3G Wireless/Modem<sup>7</sup></b>	With a supported 3G Adapter or Analog Modem				
<b>Power Supply</b>	Single 250W ATX Power Supplies		Dual 250W ATX, Hot Swappable		
<b>Fans</b>	Dual Fans, Hot Swappable				
<b>Display</b>	Front LCD Display				
<b>Power Input</b>	100-240vac, 60-50Hz				
<b>Max Power Consumption</b>	81 W	90 W			150 W
<b>Total Heat Dissipation</b>	276 BTU	307 BTU	511.5 BTU		
<b>MTBF</b>	11.9	11.9	12.4		
<b>Certifications</b>	EAL4+, FIPS 140-2 Level 2, VPNC, ICSA Firewall 4.1, IPv6 Phase 1, IPv6 Phase 2		ICSA Firewall 4.1		—
<b>Certifications Pending</b>	—		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
<b>Form Factor</b>	1U rack-mountable				
<b>Dimensions</b>	17 x 16.75 x 1.75 in/43.18 x 42.54 x 4.44 cm				
<b>Weight</b>	15.00 lbs/6.80 kg	15.10 lbs/6.85 kg	17.30 lbs/7.9 kg		
<b>WEEE Weight</b>	15.00 lbs/6.80 kg	15.10 lbs/6.85 kg	17.30 lbs/7.9 kg		
<b>Major Regulatory</b>	FCC Class A, CES Class A, CE, C-Tick, VCCI, Compliance MIC, UL, cUL, TUV/GS, CB, NOM, RoHS, WEEE				
<b>Environment</b>	40-105° F, 5-40° C				
<b>Humidity</b>	10-90% non-condensing				

<sup>1</sup> Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services. <sup>2</sup> 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. <sup>3</sup> Actual maximum connection counts are lower when Full DPI services are enabled. <sup>4</sup> VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544. <sup>5</sup> USB 3G card and modem are not included. See <http://www.sonicwall.com/us/products/cardsupport.html> for supported USB devices. <sup>6</sup> The Comprehensive Anti-Spam Service supports an unrestricted number of users but is recommended for 250 users or less. <sup>7</sup> With SonicWALL WX Series Appliances

### SonicWALL's line-up of dynamic security solutions



### SonicWALL, Inc.

2001 Logic Drive, San Jose, CA 95124  
T +1 408.745.9600 F +1 408.745.9300  
[www.sonicwall.com](http://www.sonicwall.com)



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™