



The SonicWALL Network Security Appliance Series

FIREWALL

Unified Threat Management Firewall

- **Unified Threat Management**
- **Scalable multi-core hardware and Reassembly-Free Deep Packet Inspection**
- **Application intelligence, control and visualization**
- **Stateful high availability and load balancing**
- **High performance and lowered TCO**
- **Advanced routing services and networking features**
- **Standards-based Voice over IP (VoIP)**
- **Secure distributed wireless LAN services**
- **Onboard Quality of Service (QoS)**

Organizations of all sizes depend on their networks to access internal and external mission-critical applications. As advances in networking continue to provide tremendous benefit to organizations, they are increasingly challenged by sophisticated and financially-motivated attacks designed to disrupt communication, degrade performance and compromise data. Malicious attacks penetrate outdated stateful packet inspection firewalls with advanced application layer exploits. Point products add layers of security, but are costly, difficult to manage, limited in controlling network misuse and ineffective against the latest multipronged attacks.

The SonicWALL® Network Security Appliance (NSA) Series of Unified Threat Management (UTM) Firewalls, utilizing a unique multi-core design and patented Reassembly-Free Deep Packet Inspection™ (RFDPI) technology*, offers complete protection without compromising network performance. The NSA Series overcomes the limitations of existing security solutions by scanning the entirety of each packet for current internal and external threats in real-time.

The NSA Series applies UTM protection against a comprehensive array of attacks, combining intrusion prevention, anti-virus and, anti-spyware, anti-spam and content filtering with application intelligence, control and visualization. With advanced routing, stateful high-availability and high-speed IPSec and SSL VPN technology, the NSA Series adds security, reliability, functionality and productivity to branch offices, central sites and distributed mid-enterprise networks, while minimizing cost and complexity.

Comprised of the SonicWALL NSA 240, NSA 2400, NSA 3500 and NSA 4500, the NSA Series offers a scalable range of solutions designed to meet the network security needs of any organization.

Features and Benefits

Unified Threat Management integrates intrusion prevention, gateway anti-virus, anti-spyware, application intelligence and control, content filtering and anti-spam to block malware and spam, and offer granular application control and prevent data leakage.

Scalable multi-core hardware and Reassembly-Free Deep Packet Inspection scans and eliminates threats of unlimited file sizes, with near-zero latency across thousands of connections at wire speed.

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.

Stateful high availability and load balancing features maximize total network bandwidth and maintain seamless network uptime, delivering uninterrupted access to mission-critical resources, and ensuring that VPN tunnels and other network traffic will not be interrupted in the event of a failover.

High performance and lowered TCO are achieved by using the processing power of multiple cores in unison to dramatically increase throughput and provide simultaneous inspection capabilities, while lowering power consumption.

Advanced routing services and networking features incorporate 802.1q VLANs, Multi-WAN failover, zone and object-based management, load balancing, advanced NAT modes, and more, providing granular configuration flexibility and comprehensive protection at the administrator's discretion.

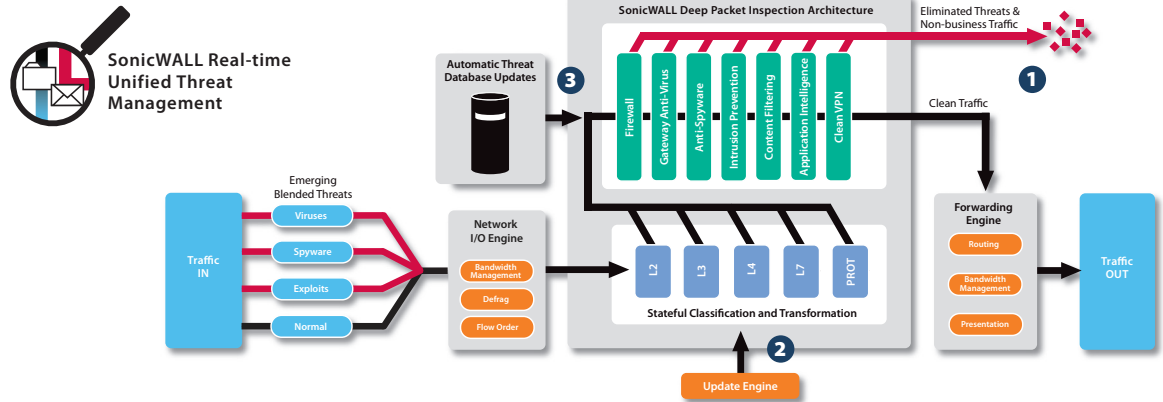
Standards-based Voice over IP (VoIP) capabilities provide the highest levels of security for every element of the VoIP infrastructure, from communications equipment to VoIP-ready devices such as SIP Proxies, H.323 Gatekeepers and Call Servers.

Secure distributed wireless LAN services enable the appliance to function as a wireless switch and controller that automatically detects and configures SonicPoint wireless access points

Onboard Quality of Service (QoS) features use industry standard 802.1p and Differentiated Services Code Points (DSCP) Class of Service (CoS) designators to provide powerful and flexible bandwidth management that is vital for VoIP, multimedia content and business-critical applications.

* U.S. Patent 7,310,815-A method and apparatus for data stream analysis and blocking.





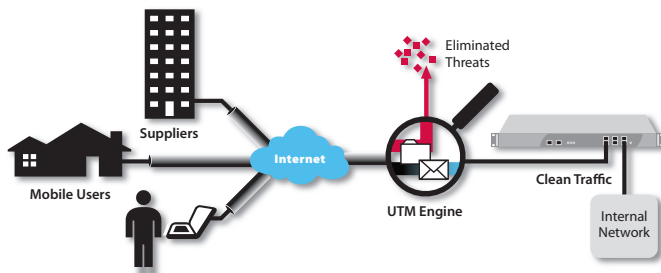
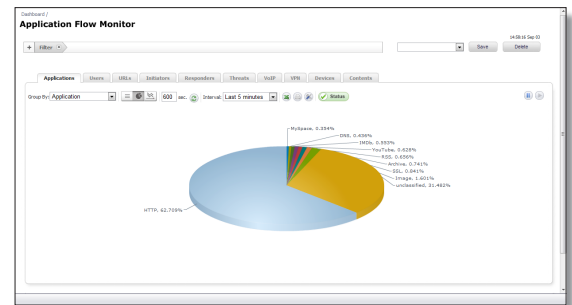
Best-in-Class Threat Protection

- 1 SonicWALL deep packet inspection protects against network risks such as viruses, worms, Trojans, spyware, phishing attacks, emerging threats and Internet misuse. Application intelligence and control adds highly-configurable controls to prevent data leakage and manage bandwidth at the application level.
- 2 The SonicWALL Reassembly-Free Deep Packet Inspection (RFDPI) technology utilizes SonicWALL's multi-core architecture to scan packets in real-time without stalling traffic in memory.
- 3 The SonicWALL NSA Series provides dynamic network protection through continuous, automated security updates, protecting against emerging and evolving threats, without requiring any administrator intervention.

This functionality allows threats to be identified and eliminated over unlimited file sizes and unrestricted concurrent connections, without interruption.

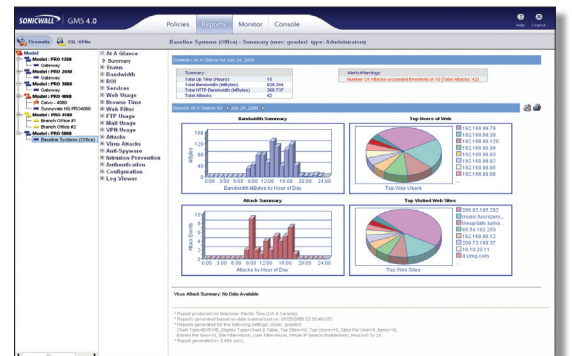
Application Intelligence and Control

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 SonicWALL Reassembly-Free Deep Packet Inspection™ technology to identify and control applications in use with easy-to-use pre-defined application categories (such as social media or gaming)—regardless of port or protocol. The SonicWALL Application Flow Monitor provides real-time graphs of applications, ingress and egress bandwidth, active Web site connections and user activity.



SonicWALL Clean VPN

The Network Security Appliance Series includes innovative SonicWALL Clean VPN™ technology which decontaminates vulnerabilities and malicious code from remote mobile users and branch offices traffic before it enters the corporate network, and without user intervention.



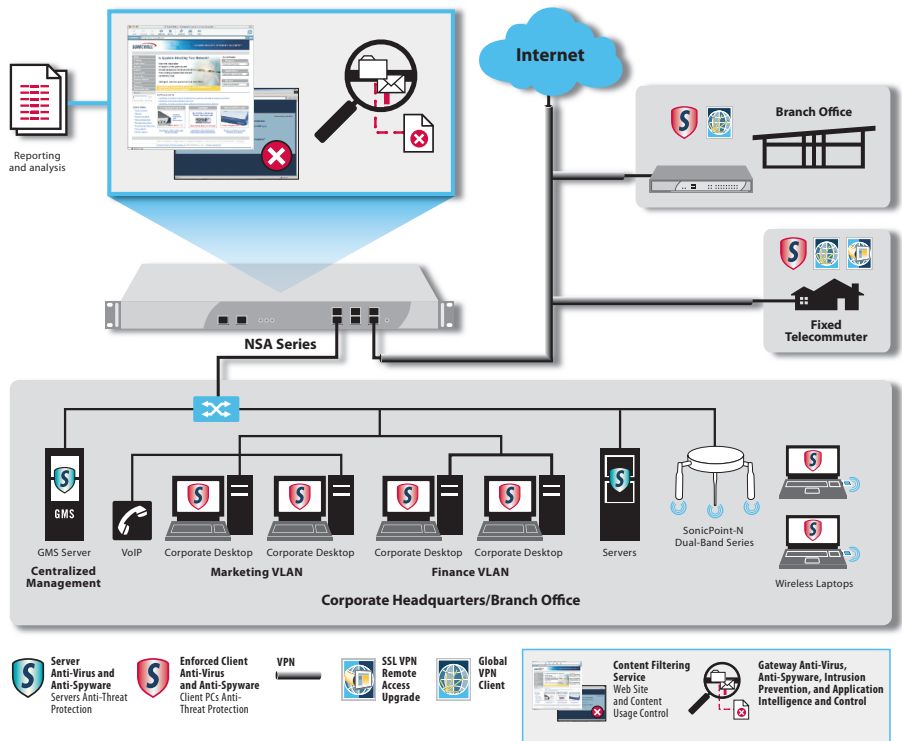
Centralized Policy Management

The Network Security Appliance Series can be managed using the SonicWALL Global Management System (GMS®), which provides flexible, powerful and intuitive tools to centrally manage configurations, view real-time monitoring metrics and integrate policy and compliance reporting.

Flexible, Customizable Deployment Options – NSA Series At-A-Glance

Every SonicWALL Network Security Appliance solution delivers Unified Threat Management protection, utilizing a breakthrough multi-core hardware design and Reassembly-Free Deep Packet Inspection for internal and external network protection without compromising network performance. Each NSA Series product combines high-speed intrusion prevention, file and content inspection, and powerful application intelligence and control with an extensive array of advanced networking and flexible configuration features. The NSA Series offers an accessible, affordable platform that is easy to deploy and manage in a wide variety of corporate, branch office and distributed network environments.

- The SonicWALL **NSA 4500** is ideal for corporate central-site and large distributed environments requiring high throughput capacity and performance
- The SonicWALL **NSA 3500** is ideal for corporate, branch office and distributed environments needing significant throughput capacity and performance
- The SonicWALL **NSA 2400** is ideal for small- to medium-sized corporate and branch office environments concerned about throughput capacity and performance
- The SonicWALL **NSA 240** is ideal for small- to medium-sized businesses and branch office sites



Security Services and Upgrades



Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention and Application Intelligence and Control 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 delivers a suite of configurable tools designed to prevent data leakage while providing granular application-level controls along with tools enabling visualization of network traffic.



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.



Content Filtering Service enforces protection and productivity policies by employing an innovative rating architecture, utilizing a dynamic database to block up to 56 categories of objectionable Web content.



ViewPoint Reporting delivers easy-to-use, Web-based capabilities that provide administrators with instant comprehensive 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.



Virtual Assist is a remote support tool that enables a technician to assume control of a PC or laptop for the purpose of providing remote technical assistance. With permission, the technician can gain instant access to a computer using a Web browser, making it easy to diagnose and fix a problem remotely without the need for a pre-installed "fat" client.



Dynamic Support Services are available 8x5 or 24x7 depending on customer needs. Features include world-class technical support, crucial firmware updates and upgrades, access to extensive electronic tools and timely hardware replacement to help organizations get the greatest return on their

SonicWALL investment.



Global VPN Client Upgrades utilize a software client that is installed on Windows-based computers and increase workforce productivity by providing secure access to email, files, intranets, and applications for remote users. Upgrade licenses are available in a variety of user counts allowing this solution to scale as the organization grows.



SSL VPN Remote Access Upgrades provide clientless remote network level access for PC, Mac and Linux-based systems. With integrated SSL VPN technology, SonicWALL UTM appliances enable seamless and secure remote access to email, files, intranets, and applications from a variety of client platforms via NetExtender, a lightweight client that is pushed onto the user's machine. NetExtender is installed and configured automatically, requiring no user interaction.



Comprehensive Anti-Spam Service (CASS) offers small- to medium-sized businesses comprehensive protection from spam and viruses, with instant deployment over existing SonicWALL firewalls. CASS speeds deployment, eases administration and reduces overhead by consolidating solutions, providing one-click anti-spam services, with advanced configuration in just ten minutes.

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.

Specifications

Firewall	NSA 240	NSA 2400	NSA 3500	NSA 4500
SonicOS Version				
SonicOS Enhanced 5.6 (or higher)				
Stateful Throughput ¹	600 Mbps	775 Mbps	1.5 Gbps	2.75 Gbps
GAV Performance ²	115 Mbps	160 Mbps	350 Mbps	690 Mbps
IPS Performance ²	195 Mbps	275 Mbps	750 Mbps	1.4 Gbps
UTM Performance ²	110 Mbps	150 Mbps	240 Mbps	600 Mbps
IMIX Performance ²	195 Mbps	235 Mbps	580 Mbps	700 Mbps
Maximum Connections ³	85,000/110,000 ⁴	225,000	325,000	500,000
Maximum DPI Connections	32,000/50,000 ⁴	125,000	175,000	250,000
New Connections/Sec	2,000	4,000	7,000	10,000
Nodes Supported	Unrestricted			
Denial of Service Attack Prevention	22 classes of DoS, DDoS and scanning attacks			
SonicPoints Supported (Maximum)	16	32	48	64
VPN				
3DES/AES Throughput ⁵	150 Mbps	300 Mbps	625 Mbps	1.0 Gbps
Site-to-Site VPN Tunnels	25/50 ⁶	75	800	1,500
Bundled Global VPN Client Licenses (Maximum)	2 (25)	10 (250)	50 (1,000)	500 (3,000)
Bundled SSL VPN Licenses (Maximum)	2 (15)	2 (25)	2 (30)	2 (30)
Virtual Assist Bundled (Maximum)	1 30-day trial (5)	1 (5)	2 (10)	2 (10)
Encryption/Authentication/DH Group	DES, 3DES, AES (128, 192, 256-bit), MD5, SHA-1/DH Groups 1, 2, 5, 14			
Key Exchange	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			
Dead Peer Detection	Yes			
DHCP Over VPN	Yes			
IPSec NAT Traversal	Yes			
Redundant VPN Gateway	Yes			
Global VPN Client Platforms Supported	Microsoft* Windows 2000, Windows XP, Microsoft* Vista 32/64-bit, Windows 7 32/64-bit			
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	Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention and Application Intelligence and Control			
Content Filtering Service Premium Edition	(CFS) HTTP URL, HTTPS 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 ⁷			
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 ⁸	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)	10/25 ⁹	25	50	200
Routing	OSPF, RIPV1/v2, static routes, policy-based routing, Multicast			
QoS	Bandwidth priority, maximum bandwidth, guaranteed bandwidth, DSCP marking, 802.1p			
IPv6	Yes			
Authentication	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, internal user database, Terminal Services, Citrix			
Internal Database/Single Sign-on Users	100/100 Users	250/250 Users	300/500 Users	1,000/1,000 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				
Zone Security	Yes			
Schedules	One Time, Recurring			
Object-based/Group-based Management	Yes			
DDNS	Yes			
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	Optional Active/Passive with State Sync ¹⁰	Optional Active/Passive with State Sync	Active/Passive with State Sync	Active/Passive 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	802.11 a/b/g/n, WPA2, WPA, TKIP, 802.1x, EAP-PEAP, EAP-TTLS			
Hardware				
Interfaces	(3) GE Gigabit Ports+ (6) 10/100, 2 USB, PC Card Slot (Optional 3G/Analog Modem), 1 Console Interface	(6) 10/100/1000 Copper Gigabit Ports, 1 Console Interface, 2 USB		
Memory (RAM)	256 MB	512 MB	512 MB	512 MB
Flash Memory	32 MB Compact Flash	512 MB Compact Flash		
3G Wireless/Modem ¹¹	With 3G USB Adapter Modem			
Power Supply	36W External	Single 180W ATX Power Supply		
Fans	No Fan	2 Fans		
Power Input	10-240V, 50-60Hz	100-240Vac, 60-50Hz		
Max Power Consumption	15W	42W	64W	66W
Total Heat Dissipation	51.18TU	144BTU	219BTU	225BTU
Certifications	EAL4+, VPNC, ICSA Firewall 4.1		EAL4+, FIPS 140-2 Level 2, VPNC, ICSA Firewall 4.1	
Certifications Pending	FIPS 140-2		-	
Form Factor and Dimensions	7.125 x 1.5 x 10.5 in/ 18.10 x 3.81 x 26.67 cm	1U rack-mountable/ 17 x 10.25 x 1.75 in/ 43.18 x 26 x 4.44 cm	1U rack-mountable/ 17 x 13.25 x 1.75 in/ 43.18 x 33.65 x 4.44 cm	
Weight	2.55lb/1.16kg	8.05 lbs/ 3.65 kg	11.30 lbs/ 5.14 kg	
WEEE Weight	3.15lb/1.43kg	8.05 lbs/ 3.65 kg	11.30 lbs/ 5.14 kg	
Major Regulatory	FCC Class A, CES Class A, CE, C-Tick, VCCI, Compliance MIC, UL, cUL, TUV/GS, CB, NOM, RoHS, WEEE			
Environment	32-105° F, 0-40° C	40-105° F, 5-40° C		
MTBF	9.5 years	16.0 years	14.3 years	14.1 years
Humidity	0-95% non-condensing		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 UTM services are enabled. ⁴ Only with the NSA 240 Stateful HA and Expansion Upgrade. ⁵ VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544. ⁶ Supported on the NSA 3500 and higher. ⁷ Not available on NSA 2400. ⁸ USB 3G card and modem are not included. See <http://www.sonicwall.com/us/products/cardsupport.html> for supported USB devices. ⁹ The Comprehensive Anti-Spam Service supports an unrestricted number of users but is recommended for 250 users or less.



Network Security Appliance 4500
01-SSC-7012
NSA 4500 TotalSecure* (1-year)
01-SC-7032



Network Security Appliance 3500
01-SSC-7016
NSA 3500 TotalSecure* (1-year)
01-SC-7033



Network Security Appliance 2400
01-SSC-7020
NSA 2400 TotalSecure* (1-year)
01-SC-7035



Network Security Appliance 240
TotalSecure* (1-year)
01-SSC-8760



SonicWALL PC Card to
ExpressCard Adapter
(for NSA 240)
01-SSC-2887

For more information on SonicWALL network security solutions, please visit www.sonicwall.com.

*Includes one-year of Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, and Application Intelligence and Control Service, Content Filtering Service, Dynamic Support 24x7 and ViewPoint Reporting.

Certifications



SonicWALL, Inc.

2001 Logic Drive, San Jose, CA 95124
T +1 408.745.9600 F +1 408.745.9300
www.sonicwall.com

SonicWALL's line-up of dynamic security solutions

NETWORK SECURITY

SECURE REMOTE ACCESS

WEB AND E-MAIL SECURITY

BACKUP AND RECOVERY

POLICY AND MANAGEMENT

