The SonicWALL Network Security Appliance Series

FIREWALL

Next-Generation Firewall

- **Next-Generation Firewall**
- **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**
- **Network productivity**
- **Advanced routing services and networking**
- **Standards-based Voice over IP (VoIP)**
- **SonicWALL Clean Wireless**
- **Onboard Quality of Service (QoS)**
- **Integrated modules support**

Organizations of all sizes depend on their networks to access internal and external mission-critical applications. As advances in networking continue to provide tremendous benefits, organizations 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 Malicious attacks penetrate outdated stateful packet inspection firewalls with advanced application layer exploits.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.

By utilizing a unique multi-core design and patented Reassembly-Free Deep Packet Inspection™ (RFDPI) technology*, the SonicWALL® Network Security Appliance (NSA) Series of Next-Generation Firewalls offers complete protection without compromising network performance. The low latency 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 offers intrusion prevention, malware protection, and application intelligence, control and visualization, while delivering breakthrough performance. 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 220, NSA 220 Wireless-N, NSA 250M, NSA 250M Wireless-N, 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

Next-Generation Firewall features integrate intrusion prevention, gateway anti-virus, anti-spyware and URL filtering with application intelligence and control, and SSL decryption to block threats from entering the network and provide granular application control without compromising performance.

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.

Network productivity increases because IT can identify and throttle or block unauthorized, unproductive and non-work related applications and web sites, such as Facebook® or YouTube®, and can optimize WAN traffic when integrated with SonicWALL WAN Acceleration Appliance (WXA) solutions.

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.

SonicWALL Clean Wireless optionally integrated into dual-band wireless models or via SonicWALL SonicPoint wireless access points provides powerful and secure 802.11a/b/g/n 3x3 MIMO wireless, and enables scanning for rogue wireless access points in compliance with PCI DSS.

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.

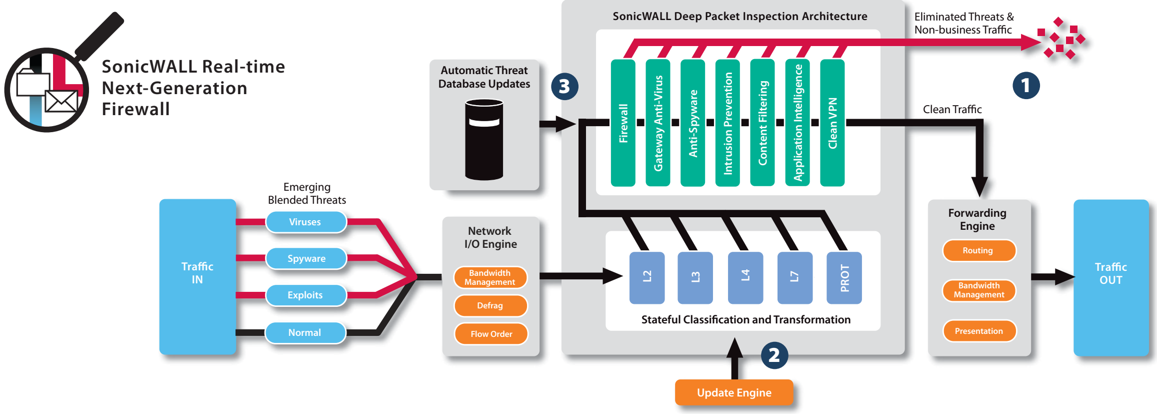
Integrated modules support on NSA 250M and NSA 250M Wireless-N appliances reduce acquisition and maintenance costs through equipment consolidation, and add deployment flexibility.

*U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Dynamic Security Architecture and Management



Best-in-Class Threat Protection

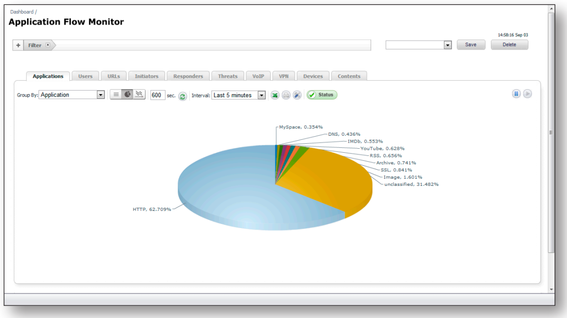
1. SonicWALL deep packet inspection protects against network risks such as viruses, worms, Trojans, spyware, phishing attacks, emerging threats and Internet misuse. Application intelligence and control adds highly-configurable controls to prevent data leakage and manage bandwidth at the application level.

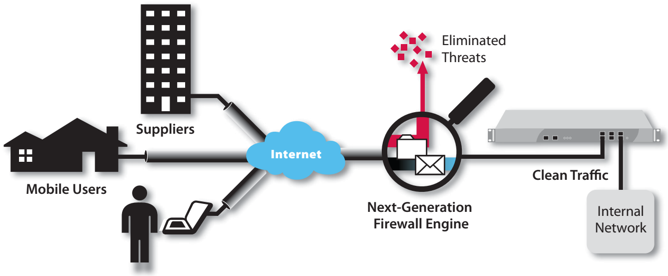
2. The SonicWALL Reassembly-Free Deep Packet Inspection (RFDPI) technology utilizes SonicWALL's multi-core architecture to scan packets in real-time without stalling traffic in memory. This functionality allows threats to be identified and eliminated over unlimited file sizes and unrestricted concurrent connections, without interruption.

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.

Application Intelligence and Control

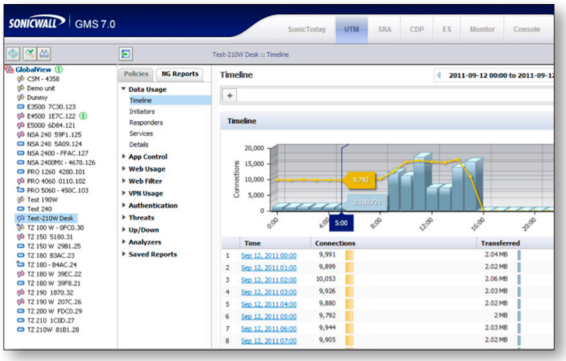
SonicWALL Application Intelligence and Control provides granular control and real-time visualization of applications to guarantee bandwidth prioritization and ensure maximum network security and productivity. An integrated feature of SonicWALL Next-Generation Firewalls, it uses SonicWALL RFDPI technology 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. SonicWALL Application Traffic Analytics provides real-time and indepth historical analysis of data transmitted through the firewall including application activities by user.


Dashboard /
Application Flow Monitor
14:58:16 Sep 03
Group By: Application
600 sec.
Interval: Last 5 minutes



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.



Test-210W Desk :: Timeline

GlobalView
CSM - 4358
Demo unit
Dummy
E3500 7C30.123
E4500 1E7C.122
E5000 6D84.121
NSA 240 59F1.125
NSA 240 5A09.124
NSA 2400 - FFAC.127
NSA 2400MX - 4678.126
PRO 1260 4280.101
PRO 4060 0110.102
PRO 5060 - 450C.103
Test 190W
Test 240
Test-210W Desk
TZ 100 W - 0FC0.30
TZ 150 5180.31
TZ 150 W 2981.25
TZ 180 83AC.23
TZ 180 - 84AC.24
TZ 180 W 39EC.22
TZ 180 W 39F8.21
TZ 190 1870.32
TZ 190 W 207C.26
TZ 200 W FDC0.29
TZ 210 1C0D.27
TZ 210W 81B1.28

Data Usage
Timeline
Initiators
Responders
Services
Details
App Control
Web Usage
Web Filter
VPN Usage
Authentication
Threats
Up/Down
Analyzers
Saved Reports

Timeline
2011-09-12 00:00 to 2011-09-1

	Time	Connections	Transferred
1	Sep 12, 2011 00:00	9,991	2.04 MB
2	Sep 12, 2011 01:00	9,899	2.02 MB
3	Sep 12, 2011 02:00	10,053	2.06 MB
4	Sep 12, 2011 03:00	9,926	2.03 MB
5	Sep 12, 2011 04:00	9,880	2.02 MB
6	Sep 12, 2011 05:00	9,792	2 MB
7	Sep 12, 2011 06:00	9,944	2.03 MB
8	Sep 12, 2011 07:00	9,905	2.02 MB

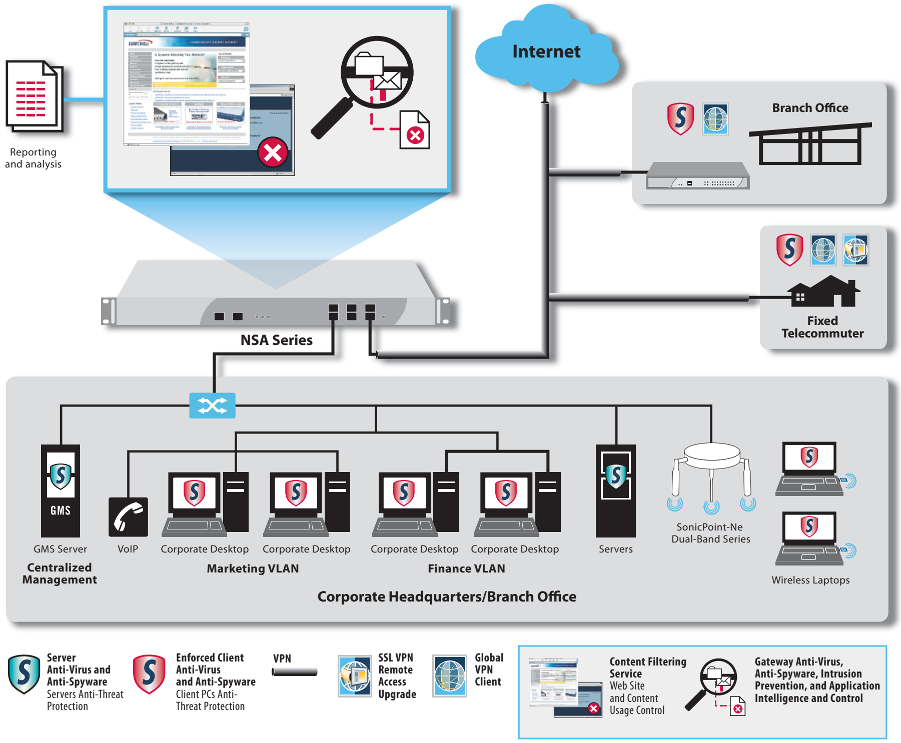
Centralized Policy Management

The Network Security Appliance Series can be managed using the SonicWALL Global Management System, which provides flexible, powerful and intuitive tools to manage configurations, view real-time monitoring metrics and integrate policy and compliance reporting and application traffic analytics, all from a central location.

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

Every SonicWALL Network Security Appliance solution delivers Next-Generation Firewall 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 large distributed and corporate central-site environments requiring high throughput capacity and performance
- The SonicWALL **NSA 3500** is ideal for distributed, branch office and corporate environments needing significant throughput capacity and performance
- The SonicWALL **NSA 2400** is ideal for branch office and small- to medium-sized corporate environments concerned about throughput capacity and performance
- The SonicWALL **NSA 220, NSA 220 Wireless-N, NSA 250M and NSA 250M Wireless-N** are ideal for branch office sites in distributed enterprise, small- to medium-sized businesses and retail environments


Reporting and analysis
Internet
Branch Office
Fixed Telecommuter
NSA Series
GMS
GMS Server
Centralized Management
VoIP
Corporate Desktop
Corporate Desktop
Marketing VLAN
Corporate Desktop
Corporate Desktop
Finance VLAN
Servers
SonicPoint-Ne Dual-Band Series
Wireless Laptops
Corporate Headquarters/Branch Office
Server Anti-Virus and Anti-Spyware Servers Anti-Threat Protection
Enforced Client Anti-Virus and Anti-Spyware Client PCs Anti-Threat Protection
VPN
SSL VPN Remote Access Upgrade
Global VPN Client
Content Filtering Service Web Site and Content Usage Control
Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, and Application Intelligence and Control

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.

Analyzer is a flexible, easy to use web-based application traffic analytics and reporting tool that provides powerful real-time and historical insight into the health, performance and security of the 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 firewall 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 for threats 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 220/W**	**NSA 250M/W**	**NSA 2400**	**NSA 3500**	**NSA 4500**
SonicOS Version	SonicOS 5.8.11		SonicOS Enhanced 5.6 (or higher)		
Stateful Throughput[1]	600 Mbps	750 Mbps	775 Mbps	1.5 Gbps	2.75 Gbps
GAV Performance[2]	115 Mbps	140 Mbps	160 Mbps	350 Mbps	690 MBps
IPS Performance[2]	195 Mbps	250 Mbps	275 Mbps	750 Mbps	1.4 Gbps
Full DPI Performance[2]	110 Mbps	130 Mbps	150 Mbps	240 Mbps	600 Mbps
IMIX Performance[2]	180 Mbps	210 Mbps	235 Mbps	580 Mbps	700 Mbps
Maximum Connections[3]	85,000	110,000	225,000	325,000	500,000
Maximum DPI Connections	32,000	64,000	175,000	250,000	
New Connections/Sec	2,200	3,000	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	24	32	48	64
VPN					
3DES/AES Throughput[5]	150 Mbps	200 Mbps	300 Mbps	625 Mbps	1.0 Gbps
Site-to-Site VPN Tunnels	25	50	75	800	1,500
Bundled Global VPN Client Licenses (Maximum)	2 (25)	2 (25)	10 (250)	50 (1,000)	500 (3,000)
Bundled SSL VPN Licenses (Maximum)	2 (15)	2 (15)	2 (25)	2 (30)	2 (30)
Virtual Assist Bundled (Maximum)	1 30-day trial (5)	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				
Gateway-enforced Client Anti-Virus and Anti-Spyware	SonicWALL Enforced Client Anti-Virus and Anti-Spyware – McAfee or Kaspersky Lab				
Comprehensive Anti-Spam Service†	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[6]	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)	25	35	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	150/150 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	Analyzer, Local Log, Syslog, Solera Networks, NetFlow v5/v9, IPFIX with Extensions, Real-time Visualization				
High Availability	Optional 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				
WAN Acceleration Support[8]	Yes				
Built-in Wireless LAN					
Standards	802.11a/b/g/n (WEP, WPA, WPA2, 802.11i, TKIP, PSK,02.1x, EAP-PEAP, EAP-TTLS		—	—	—
Virtual Access Points (VAPs)5–Antennas (5 dBi Diversity)	External Triple, detachable		—	—	—
Radio Power–802.11a/802.11b/802.11g	15.5 dBm max/18 dBm max/17 dBM @ 6 Mbps, 13 dBM @ 54 Mbps		—	—	—
Radio Power–802.11n (2.4GHz)/802.11n (5.0GHz)	19 dBm MCS 0, 11 dBm MCS 15/17 dBm MCS 0, 12 dBm MCS 15		—	—	—
Radio Receive Sensitivity–802.11a/802.11b/802.11g	-95 dBm MCS 0, -81 dBm MCS 15/-90 dBm @ 11Mbps/ -91 dBm @ 6Mbps, -74 dBm @ 54 Mbps		—	—	—
Radio Receive Sensitivity–802.11n (2.4GHz)/802.11n (5.0GHz)	-89 dBm MCS 0, -70 dBm MCS 15/ -95 dBm MCS 0, -76 dBm MCS 15		—	—	—
Hardware					
Interfaces	(7) 10/100/1000 Copper Gigabit Ports, 2 USB, 1 Console Interface	(5) 10/100/1000 Copper Gigabit Ports, 2 USB, 1 Console Interface Module Slot	(6) 10/100/1000 Copper Gigabit Ports, 1 Console Interface, 2 USB		
Module	No	Yes	No	No	No
Memory (RAM)	512 MB				
Flash Memory	32 MB Compact Flash		512 MB Compact Flash		
3G Wireless/Modem[7]*	With 3G/4G USB Adapter or Modem		—	With 3G/4G USB Adapter or Modem	
Power Supply	36W External		Single 180W ATX Power Supply		
Fans	No Fan/1 Internal Fan	2 Internal Fans	2 Fans		
Power Input	10-240V, 50-60Hz				
Max Power Consumption	11W/15W	12W/16W	42W	64W	66W
Total Heat Dissipation	37BTU/50BTU	41BTU/55BTU	144BTU	219BTU	225BTU
Certifications	VPNC, ICSA Firewall 4.1		EAL4+, FIPS 140-2 Level 2, VPNC, ICSA Firewall 4.1, IPv6 Phase 1, IPv6 Phase 2		
Certifications Pending	EAL4+, FIPS 140-2 Level 2, IPv6 Phase 1, IPv6 Phase 2		—		
Form Factor and Dimensions	1U rack-mountable/ 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	1.95 lbs/0.88 kg/ 2.15 lbs/0.97 kg	3.05 lbs/1.38 kg/ 3.15 lbs/1.43 kg	8.05 lbs/ 3.65 kg		11.30 lbs/ 5.14 kg
WEEE Weight	V 3.05 lbs/1.38 kg/ 3.45 lbs/1.56 kg	4.4 lbs/2.0kg/ 4.65 lbs/2.11 kg	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	40-105° F, 0-40° C		40-105° F, 5-40° C		
MTBF	28 years/15 years	23 years/14 years	14.3 years	14.1 years	14.1 years
Humidity	5-95% 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] Full DPI Performance/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 Next-Generation Firewall services are enabled. [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. *USB 3G card and modem are not included. See http://www.sonicwall.com/us/products/cardsupport.html for supported USB devices. † The Comprehensive Anti-Spam Service supports an unrestricted number of users but is recommended for 250 users or less. [8] With SonicWALL WXA Series Appliance.

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 250M 01-SSC-9755

Network Security Appliance 250M Wireless-N 01-SSC-9757 (US/Canada)

Network Security Appliance 250M TotalSecure* 01-SSC-9747

Network Security Appliance 250M Wireless-N TotalSecure* 01-SSC-9748 (US/Canada)

Network Security Appliance 220 01-SSC-9750

Network Security Appliance 220 Wireless-N 01-SSC-9752 (US/Canada)

Network Security Appliance 220 TotalSecure* 01-SSC-9744

Network Security Appliance 220 Wireless-N TotalSecure* 01-SSC-9745 (US/Canada)

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 and Dynamic Support 24x7.

Certifications

Common Criteria
EAL4+ CERTIFIED

FIPS VALIDATED 140-2

ICSAlabs CERTIFIED FIREWALL - CORPORATE

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

SONICWALL®
DYNAMIC SECURITY FOR THE GLOBAL NETWORK™