

The SonicWALL Network Security Appliance Series

NETWORK SECURITY

High-performance Network Security Appliances

The SonicWALL® Network Security Appliance (NSA) Series is designed to deliver scalable, high-performance multi-function threat management to small- to medium-sized and distributed enterprise organizations. By offering ultimate security at unprecedented speed, the SonicWALL NSA Series allows medium enterprise organizations to lower total costs of operation while enhancing productivity, regulatory compliance and network throughput, for a greater return on technology investment.

Every SonicWALL Network Security Appliance solution is a next generation Unified Threat Management firewall, utilizing a breakthrough multi-core hardware design and **patented Reassembly-Free Deep Packet Inspection™ (RFDPI) technology*** to deliver real-time protection against the full spectrum of internal and external network attacks, at performance levels outpacing conventional solutions three-fold. Each NSA Series product combines high-speed intrusion prevention, file and content inspection, and powerful Application Firewall controls with an extensive array of advanced networking and configuration flexibility features in 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

Value Proposition for Your Business

- Next-generation network security appliances utilizing multi-core processor technology and real-time deep packet inspection
- Increased deal size targeted to medium enterprises
- Clearly-delineated upsell path for new revenue opportunities, built upon SonicWALL's solid success in the small- to mid-sized network security market and expansion into enterprise markets

Value Proposition for Your Customer

- Provides economical entry-point to SonicWALL's next-generation security platform that dramatically increases throughput and simultaneous inspection capabilities by combining a reassembly-free inspection engine and a multi-core security processor architecture to increase UTM performance
- State-of-the-art Application Firewall and Gateway Threat Protection sets a new standard of protection and control of applications, users and confidential data
- Integrates Stateful High Availability allowing customers to maximum uptime and continuous operation
- Extends SonicWALL's legendary ease of use to enterprise networks, for rapid deployment with a highly extensible feature set covering a wide range of applications
- Support for advanced networking features including 802.1q VLANs, Multi-WAN failover, zone and object-based management, load balancing and advanced NAT modes, providing the ultimate in configuration flexibility
- Delivers enterprise-class security to central sites, branch offices and remote offices through a scalable line of security appliances, managed individually, or as a holistic group, easily managed utilizing SonicWALL's Global Management System
- Scalable SonicWALL NSA 240 solutions can be configured using primary or secondary 3G or modem wireless interfaces for future-proofed extensibility

Competitive Advantages

- SonicWALL's Reassembly-Free Deep Packet Inspection (RFDPI) technology removes the restrictive, time consuming process of buffering traffic, delivering both greater efficiency and breakthrough inspection performance
- SonicWALL RFDPI utilizes a innovative per-packet scanning engine designed to handle unlimited file sizes and virtually hundreds of thousands of concurrent downloads, offering ultimate scalability and performance for today's networked environment
- SonicWALL RFDPI exceeds competitive solutions by inspecting and classifying traffic irrespective of protocols, ensuring the widest protection coverage
- Revolutionary multi-core performance utilizes up to 8 cores for ultra-high-speed multi-layer threat protection over external and internal networks

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



Competitive Advantages (continued)

- Application layer scanning and policy control is done using SonicWALL's power Application Firewall.
- Application Firewall is a set of granular, application specific policies that allow custom access control on per user, per e-mail user, per schedule and per IP subnet levels. Among its wide range of policies, its capabilities include restricting transfer of specific files and documents, blocking e-mail attachments using a user-configurable criteria, customized application control, bandwidth limiting for matched policies, as well as denying internal and external Web access based on various user configurable options.

Qualifying Questions for your Customer

- Have your business network performance requirements scaled beyond the capabilities of your current security appliances?
- Has your organization been affected by increases in sophisticated threats from both inside and outside the perimeter?
- Is your organization using real-time collaboration tools, Web 2.0 applications, IM, peer-to-peer applications, VoIP, streaming media or telepresence applications?
- Are you concerned about greater risk of data theft and deletion, regulatory non-compliance, systems downtime, loss of productivity and bandwidth consumption?
- Are you currently using stateful packet inspection technology that scans only the header, missing threats hidden within correctly-addressed packets?
- Does your current solution disassemble and reassemble packets, resulting in network throughput bottlenecks, or inaccurately blocked or allowed network traffic?
- Does your current security solution allow traffic to bypass security scanning based on large file sizes and imposed limits on concurrent files that it can scan?

PRO Migration Matrix

PRO Series		Move to NSA Series		Feature Upgrades to NSA
PRO 2040		NSA 2400		<ul style="list-style-type: none"> ■ Increased performance up to 3x processing speed ■ Support on SonicOS 5.0 or higher. (PRO Series only supports SonicOS 4.0 or lower) ■ Application Firewall: application-level access control and prevention of data leakage ■ IPv6 ready
PRO 3060		NSA 3500		
PRO 4060		NSA 4500		
PRO 4100		NSA 4500		

NSA Series Features

Features	NSA 240	NSA 2400 PRO 2040 Replacement	NSA 3500 PRO 3060 Replacement	NSA 4500 PRO 4060/PRO 4100 Replacement
SonicOS Supported	SonicOS 5.1 or higher	SonicOS 5.0 or higher	SonicOS 5.0 or higher	SonicOS 5.0 or higher
Users and Nodes	Unrestricted	Unrestricted	Unrestricted	Unrestricted
Interfaces	3) GE Gigabit Ports+ (6) 10/100, 2 USB Future Use, PC Card Slot (Optional 3G/Analog Modem), 1 Console Interface	(6) 10/100/1000 Copper Gigabit Ports, 1 Console Interface, 2 USB (Future Use)	(6) 10/100/1000 Copper Gigabit Ports, 1 Console Interface, 2 USB (Future Use)	(6) 10/100/1000 Copper Gigabit Ports, 1 Console Interface, 2 USB (Future Use)
Power Supply	Single 36W External Power Supply	Single 180W ATX Power Supply	Single 180W ATX Power Supply	Single 180W ATX Power Supply
VLAN Interfaces	10/25 ²	128	128	256
High Availability	Optional Active/Passive with State Synch ²	Optional Active/Passive with State Synch	Optional Active/Passive with State Synch	Active/Passive with State Synch
Stateful Throughput ¹	600 Mbps	775 Mbps	1.5 Gbps	2.75 Gbps
3DES/AES Throughput ¹	150 Mbps	300 Mbps	625 Mbps	1.0 Gbps
Gateway Anti-Virus Throughput ¹	115 Mbps	160 Mbps	350 Mbps	690 Mbps
Intrusion Prevention Throughput ¹	195 Mbps	275 Mbps	750 Mbps	1.4 Gbps
UTM Throughput ¹	110 Mbps	150 Mbps	240 Mbps	600 Mbps
New Connections Per Second	2,000	4,000	7,000	10,000
Site-to-Site VPNs	25/50 ²	75	800	1,500
IPv6 Ready	Yes	Yes	Yes	Yes
Application Firewall	Optional	Optional	Optional	Optional

¹ Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services. VPN throughput UDP traffic at 1418 byte packet size adhering to RFC 2544. UTM performance is based on HTTP tests run on the Spirent Avalanche/Reflector. Testing done with multiple flows through multiple port pairs. ² Only with the NSA 240 Series Expansion Upgrade.

For more information, visit www.sonicwall.com and login to PartnerLink.

SonicWALL, Inc.

2001 Logic Drive
San Jose, CA 95124

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

