The SonicWALL Network Security Appliance Series

NETWORK SECURITY

Next Generation Unified Threat Management Protection

- **SonicWALL's next generation security**
- **Scalable multi-core hardware and reassembly-free deep packet inspection**
- **Stateful high availability and load balancing features**
- **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Malicious attacks penetrate outdated stateful packet inspection firewalls by exploiting higher network levels. 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 revolutionizes network security, utilizing a breakthrough multi-core design and patented Reassembly-Free Deep Packet Inspection™ (RFDPI) technology* offering complete protection without compromising network performance. This platform was first made available on the SonicWALL E-Class NSA Series, and it is now available for mid-sized organizations.

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. Built on a high-speed multi-core processing platform, the NSA Series enables deep packet inspection without adversely impacting the performance of mission-critical networks and applications.

The NSA Series applies next-generation Unified Threat Management (UTM) against a comprehensive array of attacks, combining intrusion prevention, anti-virus and anti-spyware with the application-level control of SonicWALL Application Firewall. With advanced routing, stateful high-availability and high-speed 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 2400, NSA 3500, NSA 4500 and NSA 5000**, the NSA Series offers a scalable range of solutions designed to meet the network security needs of any organization.

Features and Benefits

SonicWALL's next generation security incorporates a new level of UTM that integrates intrusion prevention, gateway anti-virus and anti-spyware and features the Application Firewall suite of configurable tools to prevent data leakage and offer granular application control.

Scalable multi-core hardware and reassembly-free deep packet inspection scans and eliminates threats of unlimited file sizes, and provides virtually unrestricted concurrent connections with uncompromising speed.

Stateful high availability and load balancing features in SonicOS 5.0 Enhanced 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 advanced networking and security technology including 802.1q VLANs, WAN/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.

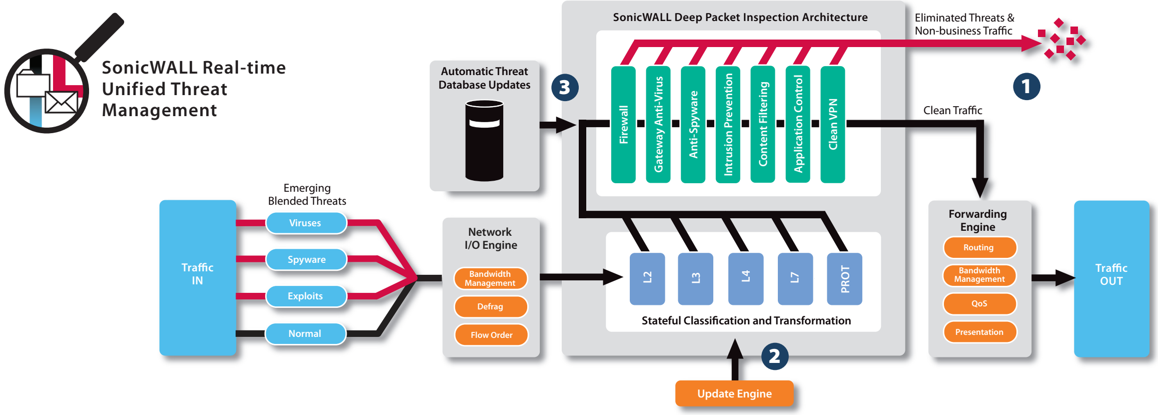
Standards-based Voice over IP (VoIP) capabilities provide the highest levels of security for every element of the VoIP infrastructure, from communications equipment to VoIP-ready devices such as SIP Proxies, H.323 Gatekeepers and Call Servers.

Secure distributed wireless LAN services enable the appliance to function as a secure wireless switch and controller that automatically detects and configures SonicPoints,™ SonicWALL wireless access points, for secure remote access in distributed network environments.

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.

Dynamic Security Architecture and Management



Best-in-Class Threat Protection

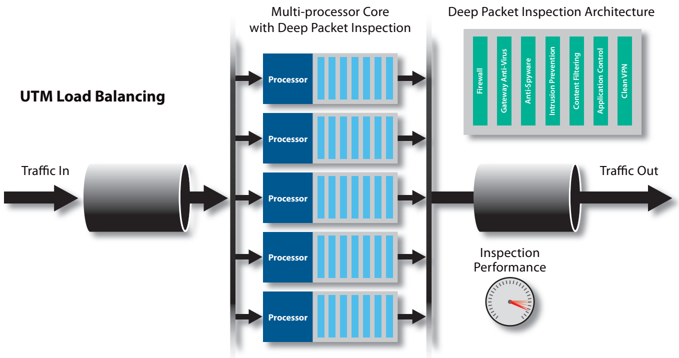
1. SonicWALL deep packet inspection protects against network risks such as viruses, worms, Trojans, spyware, phishing attacks, emerging threats and Internet misuse. Application Firewall adds highly-configurable controls to prevent data leakage and manage bandwidth at the application level.

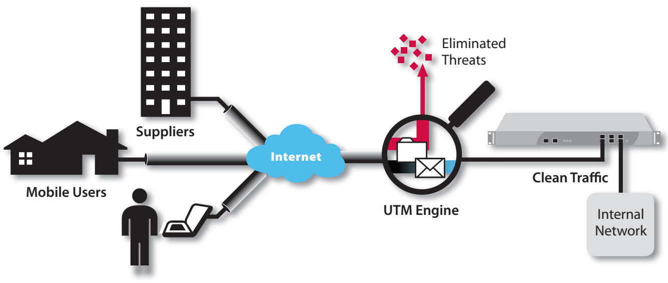
2. The SonicWALL Reaseembly-Free Deep Packet Inspection (RFDPI) technology utilizes SonicWALL's multi-core architecture to scan packets in real-time without stalling traffic in memory. This functionality allows threats to be identified and eliminated over unlimited file sizes and unrestricted concurrent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

3. The Network Security Appliance Series provides dynamic network protection through continuous, automated security updates, protecting against emerging and evolving threats, without requiring any administrator intervention.

Unified Threat Management Load Balancing

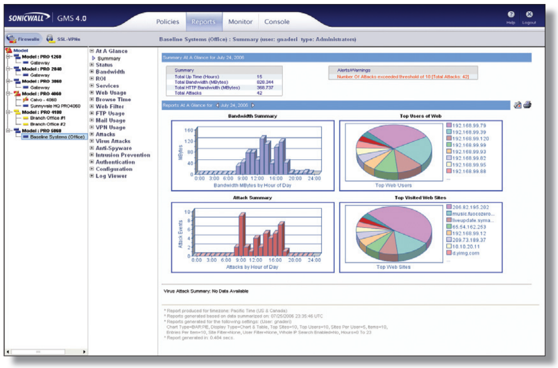
Single processor designs that include multiple protection technologies are severely limited by a single centralized processor. SonicWALL UTM load balancing integrates a high-speed deep packet inspection and traffic classification engine onto multiple security cores inspecting applications, files and content-based traffic in real time without significantly impacting performance or scalability. This enables the scanning and control of threats for networks that carry bandwidth intensive and latency sensitive applications.





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.



Baseline Systems (Office) : Summary (user: gnaderl type: Administrators)

Summary At A Glance for July 24, 2006

Summary	
Total Up Time (Hours)	15
Total Bandwidth (MBytes)	828.344
Total HTTP Bandwidth (MBytes)	368.737
Total Attacks	42

Alerts/Warnings
Number Of Attacks exceeded threshold of 10 [Total Attacks: 42]

Reports At A Glance for July 24, 2006

Virus Attack Summary: No Data Available

* Report produced for timezone: Pacific Time (US & Canada)
* Reports generated based on data summarized on: 07/25/2006 23:35:46 UTC
* Reports generated for the following settings: (User: gnaderl)
Chart Type=BAR:PIE, Display Type=Chart & Table, Top Sites=10, Top Users=10, Sites Per User=5, Items=10, Entries Per Item=10, Site Filter=None, User Filter=None, Whole IP Search Enabled=No, Hours=0 To 23
* Report generated in: 0.464 secs.

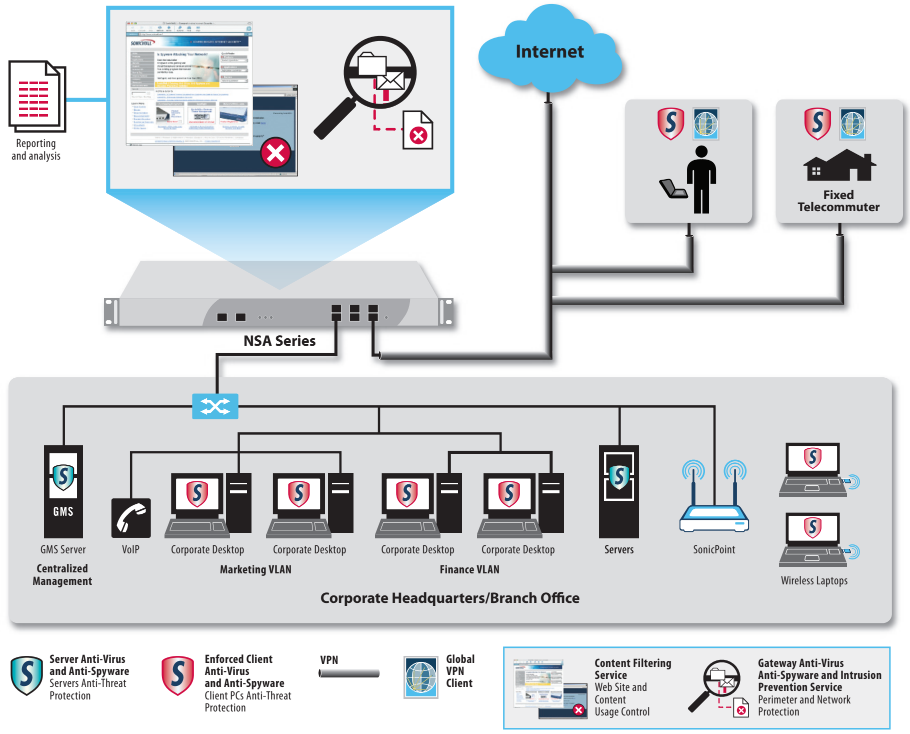
Centralized Policy Management

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 next generation 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 Firewall controls 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.

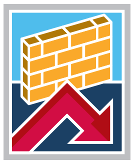
- The SonicWALL **NSA 5000** sits at the top of the line, and is ideal for the most demanding campus and distributed network environments
- The SonicWALL **NSA 4500** is ideal for corporate central-site and large distributed environments
- The SonicWALL **NSA 3500** is ideal for corporate, branch office and distributed environments
- The SonicWALL **NSA 2400** is ideal for small-to-midsize corporate and branch office environments


Reporting and analysis
Internet
Fixed Telecommuter
NSA Series
GMS
GMS Server
Centralized Management
VoIP
Corporate Desktop
Corporate Desktop
Marketing VLAN
Corporate Desktop
Corporate Desktop
Finance VLAN
Servers
SonicPoint
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
Global VPN Client
Content Filtering Service
Web Site and Content Usage Control
Gateway Anti-Virus Anti-Spyware and Intrusion Prevention Service
Perimeter and Network Protection

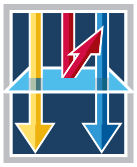
Key Features

Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention Service and Application Firewall 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 Firewall delivers a suite of configurable tools designed to prevent data leakage while providing granular application-level controls.

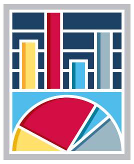
Enforced Client and Server Anti-Virus and Anti-Spyware delivers comprehensive virus and spyware protection for laptops, desktops and servers using a single integrated client and offers automated network-wide enforcement of anti-virus and anti-spyware policies, definitions and software updates.



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.



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.

Specifications

Network Security Appliance 2400
01-SSC-7020

Network Security Appliance 3500
01-SSC-7016

Network Security Appliance 4500
01-SSC-7012

Network Security Appliance 5000
01-SSC-7042

Certifications

Common Criteria
EAL4+ CERTIFIED

FIPS VALIDATED 140-2

	NSA 2400	NSA 3500	NSA 4500	NSA 5000
Firewall				
SonicOS Version	SonicOS Enhanced 5.0 (or higher)			
Stateful Throughput*	450 Mbps	1 Gbps	1.5 Gbps	1.8 Gbps
GAV Performance*	100 Mbps	310 Mbps	500 MBps	680 Mbps
IPS Performance*	120 Mbps	220 Mbps	410 Mbps	500 Mbps
UTM Performance Throughput*	50 Mbps	170 Mbps	300 Mbps	350 Mbps
IMIX Performance*	225 Mbps	440 Mbps	680 Mbps	820 Mbps
Maximum Connections	48,000	128,000	450,000	600,000
New Connections/Sec	3,000	5,000	7,500	8,500
Nodes Supported	Unrestricted			
Denial of Service Attack Prevention	22 classes of DoS, DDoS and scanning attacks			
SonicPoints Supported (Maximum)	32	32	64	64
VPN				
3DES/AES Throughput*	300 Mbps	625 Mbps	845 Mbps	1.1 Gbps
Site-to-Site VPN Tunnels	75	800	1,500	2,500
Bundled Global VPN Client Licenses for Remote Access (Maximum)	10 (250)	50 (1,000)	500 (3,000)	1,000 (3,500)
Encryption / Authentication	DES, 3DES, AES (128, 192, 256-bit), MD5, SHA-1			
Key Exchange	IKE, IKEv2, Manual Key, PKI (X.509)			
L2TP/IPSec	Yes			
Certificate Support	Verisign, Thawte, Cybertrust, RSA Keon, Entrust, and Microsoft CA for SonicWALL-to-SonicWALL VPN			
Dead Peer Detection	Yes			
DHCP Over VPN	Yes			
IPSec NAT Traversal	Yes, NAT_Tv00 and v03			
Redundant VPN Gateway	Yes			
Global VPN Client Platform Supported	Microsoft® Windows 2000, Windows XP, Microsoft® Vista 32-bit			
Deep Packet Inspection Security Services				
Deep Packet Inspection Signature Service	Comprehensive signature database. Peer- to-peer and instant messaging control and signature updates through Distributed Enforcement Architecture			
Content Filtering Service (CFS) Premium Edition	HTTP URL,HTTPS IP, keyword and content scanning ActiveX, Java Applet, and cookie blocking			
Gateway-enforced Client Anti-Virus and Anti-Spyware	HTTP/S, SMTP, POP3, IMAP and FTP, Enforced McAfee™ Clients E-mail attachment blocking			
Application Firewall	Provides application level enforcement and bandwidth control, regulate Web traffic, e-mail, e-mail attaches and file transfers, scan and restrict documents and files for key words and phrases			
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)	128	128	256	256
Routing	OSPF, RIPv1/v2, static routes, policy-based routing, Multicast			
QoS	Bandwidth priority, maximum bandwidth, guaranteed bandwidth, DSCP marking, 802.1p			
IPv6	IPv6 Ready			
Authentication	XAUTH/RADIUS, Active Directory, SSO, LDAP, internal user database			
User Database	250 users	500 users	1,000 users	1,500 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	Yes			
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			
High Availability	Optional 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			
Wireless Standards	802.11 a/b/g, WEP, WPA, TKIP, 802.1x, EAP-PEAP, EAP-TTLS			
Hardware				
Interfaces	(6) 10/100/1000 Copper Gigabit Ports, 1 Console Interface, 2 USB (Future Use)			
Memory (RAM)	512 MB	512 MB	512 MB	1 GB
Flash Memory	512 MB Compact Flash			
Power Supply	Single 180W ATX Power Supply			
Fans	2 Fans			
Power Input	100-240Vac, 60-50Hz			
Max Power Consumption	42W	64W	66W	66W
Total Heat Dissipation	144BTU	219BTU	225BTU	225BTU
Certifications	–	EAL4+, FIPS 140-2 Level 2		
Certifications Pending	EAL4+, FIPS 140-2 Level 2, ICSA Firewall 4.1	ICSA Firewall 4.1		
Form Factor and Dimensions	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	8.05 lbs/ 3.65 kg	11.30 lbs/ 5.14 kg		
WEEE Weight	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, 5-40° C			
Humidity	10-90% non-condensing			

*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.

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

SonicWALL, Inc.

1143 Borregas Avenue
Sunnyvale CA 94089-1306

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

SONICWALL®