SonicWall Network Security Appliance (NSA) Series

Industry-validated security effectiveness and performance for mid-sized networks

The SonicWall Network Security Appliance (NSA) series provides mid-sized networks, branch offices and distributed enterprises with advanced threat prevention in a high-performance security platform. Combining next-generation firewall technology with our patented* Reassembly-Free Deep Packet Inspection (RFDPI) engine on a multi-core architecture, the NSA series offers the security, performance and control organizations require.

Superior threat prevention and performance

NSA series next-generation firewalls (NGFWs) integrate a series of advanced security technologies to deliver a superior level of threat prevention. Our patented single-pass RFDPI threat prevention engine examines every byte of every packet, inspecting both inbound and outbound traffic simultaneously. The NSA series leverages on-box capabilities including intrusion prevention, anti-malware and web/URL filtering in addition to cloud-based services such as CloudAV and SonicWall Capture multi-engine sandboxing to block zero-day threats at the gateway. Unlike other security products that cannot inspect large files for hidden threats, NSA firewalls scan files of any size across all ports and protocols. The security architecture in SonicWall NGFWs has been validated as one of the industry's best for security effectiveness by NSS Labs which awarded SonicWall its "Recommended" rating for the fourth consecutive year.

Going beyond intrusion prevention, anti-malware and web filtering, SonicWall NGFWs provide a further level of protection by decrypting and inspecting SSL/TLS encrypted web traffic for hidden threats in real time. With the continued growth of encrypted web traffic, organizations are effectively blind to an estimated one-third of their network traffic. This makes SSL/TLS decryption and inspection a critical component of any security solution.

When organizations activate deep packet inspection functions such as intrusion prevention, anti-virus, anti-spyware, SSL decryption/inspection and others on their firewalls network performance often slows down, sometimes dramatically. NSA series firewalls feature a multi-core hardware architecture that utilizes specialized security microprocessors. Combined with our RFDPI engine, this unique design eliminates the performance degradation networks experience with other firewalls.

In today's security environment it's not enough to rely on solely on outside parties for threat information. That's why SonicWall formed its own in-house threat research team more than 15 years ago. This dedicated team gathers, analyzes and vets data from over one million sensors in its Global Response Intelligent Defense (GRID) network. SonicWall also participates in industry collaboration efforts and engages with threat research communities to gather and share samples of attacks and vulnerabilities.

Benefits:

Superior threat prevention and performance

- Patented reassembly-free deep packet inspection technology
- On-box and cloud-based threat prevention
- SSL/TLS decryption and inspection
- Industry-validated security effectiveness
- Multi-core hardware architecture
- Dedicated in-house threat research team

Network control and flexibility

- Powerful SonicOS operating system
- Application intelligence and control
- Network segmentation with VLANs
- Wireless network security

Easy deployment, setup and ongoing management

- Tightly integrated solution
- Centralized management
- Scalability through multiple hardware platforms
- Low total cost of ownership

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

This shared threat intelligence is used to develop real-time countermeasures that are automatically deployed to our customers' firewalls.

Network control and flexibility

At the core of the NSA series is SonicOS, SonicWall's feature-rich operating system. SonicOS provides organizations with the network control and flexibility they require through application intelligence and control, real-time visualization, an intrusion prevention system (IPS) featuring sophisticated anti-evasion technology, high-speed virtual private networking (VPN) and other robust security features.

Using application intelligence and control, network administrators can identify and categorize productive applications from those that are unproductive or potentially dangerous, and control that traffic through powerful application-level policies on both a per-user and a per-group basis (along with schedules and exception lists). Business-critical applications can be prioritized and allocated more bandwidth while non-essential applications are bandwidth-limited. Real-time monitoring and visualization provides a graphical representation of applications, users and bandwidth usage for granular insight into traffic across the network.

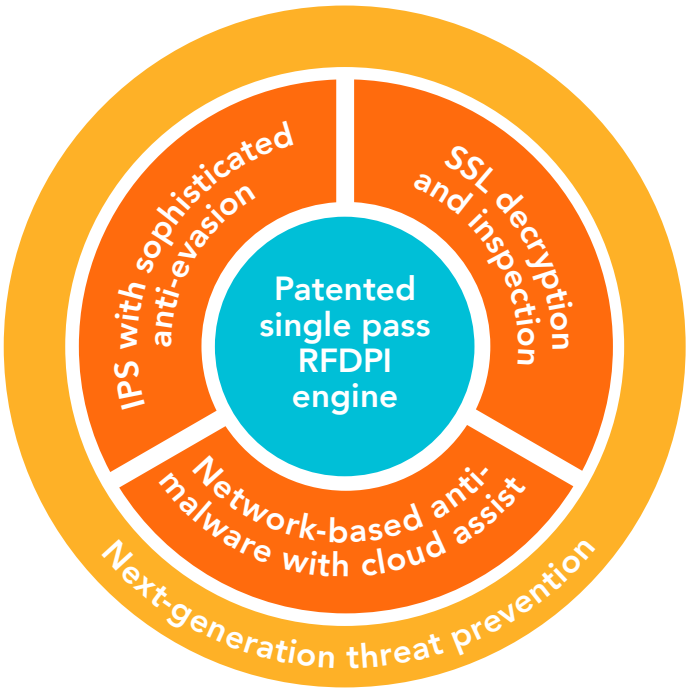
For organizations that require advanced flexibility in their network design, SonicOS offers the tools to securely segment the network through the use of virtual LANs (VLANs) which enable network administrators to create a virtual LAN interface that allows for network separation into one or more logical groups. Administrators create rules that determine the level of communication with devices on other VLANs.

Built into every NSA series firewall is a wireless access controller that enables organizations to extend the network perimeter securely through the use of wireless technology. Together, SonicWall firewalls and SonicPoint 802.11ac wireless access points create a wireless network security solution that combines industry-leading next-generation firewall technology with high-speed wireless for enterprise-class network security and performance across the wireless network.

Easy deployment, setup and ongoing management

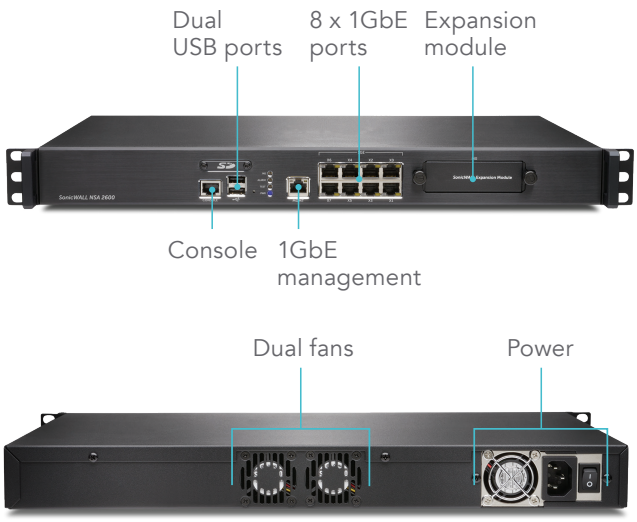
Like all SonicWall firewalls, the NSA series tightly integrates key security, connectivity and flexibility technologies into a single, comprehensive solution. This includes SonicPoint wireless access points and the SonicWall WAN Acceleration Appliance (WXA) series, both of which are automatically detected and provisioned by the managing NSA firewall. Consolidating multiple capabilities eliminates the need to purchase and install point products that don't always work well together. This reduces the effort it takes to deploy the solution into the network and configure it, saving both time and money.

Ongoing management and monitoring of network security are handled centrally through the firewall or through the SonicWall Global Management System (GMS), providing network administrators with a single pane of glass from which to manage all aspects of the network. Together, the simplified deployment and setup along with the ease of management enable organizations to lower their total cost of ownership and realize a high return on investment.



Network Security Appliance 2600

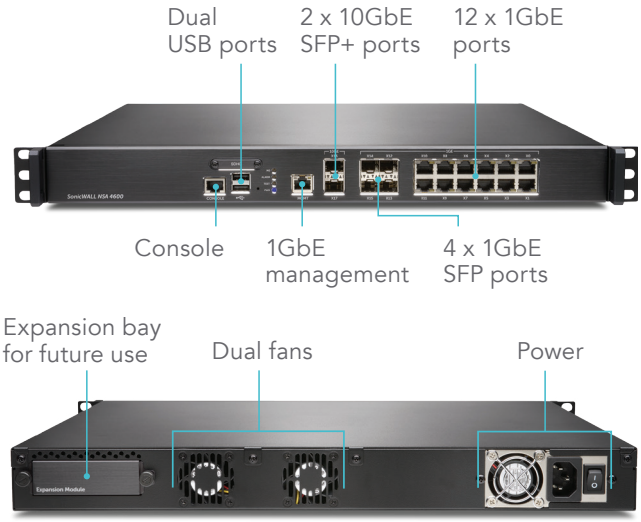
The SonicWall NSA 2600 is designed to address the needs of growing small organizations, branch offices and school campuses.



Firewall	NSA 2600
Firewall throughput	1.9 Gbps
IPS throughput	700 Mbps
Anti-malware throughput	400 Mbps
Full DPI throughput	300 Mbps
IMIX throughput	600 Mbps
Maximum DPI connections	125,000
New connections/sec	15,000/sec
Description	**SKU**
NSA 2600 firewall only	01-SSC-3860
NSA 2600 TotalSecure (1-year)	01-SSC-3863

Network Security Appliance 3600/4600

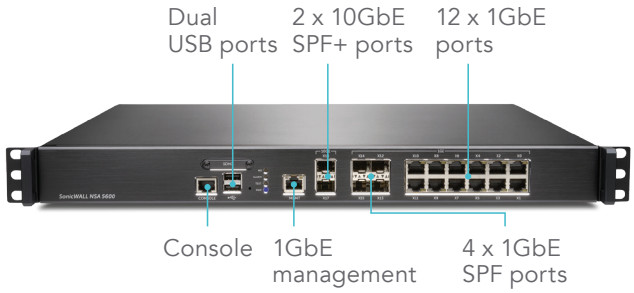
The SonicWall NSA 3600/4600 is ideal for branch office and small- to medium-sized corporate environments concerned about throughput capacity and performance.

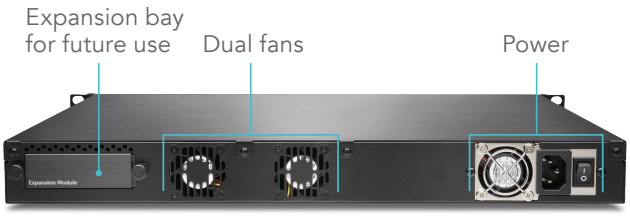


Firewall	NSA 3600	NSA 4600
Firewall throughput	3.4 Gbps	6.0 Gbps
IPS throughput	1.1 Gbps	2.0 Gbps
Anti-malware throughput	600 Mbps	1.1 Gbps
Full DPI throughput	500 Mbps	800 Mbps
IMIX throughput	900 Mbps	1.6 Gbps
Maximum DPI connections	175,000	200,000
New connections/sec	20,000/sec	40,000/sec
Description	**SKU**	
Firewall only	01-SSC-3850	01-SSC-3840
TotalSecure (1-year)	01-SSC-3853	01-SSC-3843

Network Security Appliance 5600

The SonicWall NSA 5600 is ideal for distributed, branch office and corporate environments needing significant throughput.

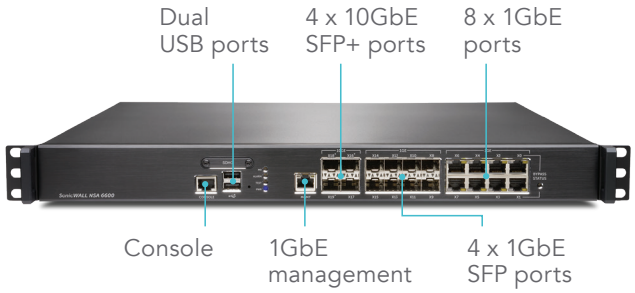


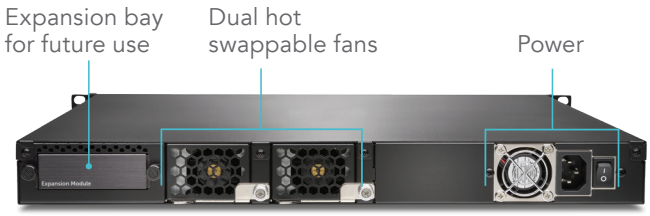


Firewall	NSA 5600
Firewall throughput	9.0 Gbps
IPS throughput	3.0 Gbps
Anti-malware throughput	1.7 Gbps
Full DPI throughput	1.6 Gbps
IMIX throughput	2.4 Gbps
Maximum DPI connections	375,000
New connections/sec	60,000/sec
Description	**SKU**
NSA 5600 firewall only	01-SSC-3830
NSA 5600 TotalSecure (1-year)	01-SSC-3833

Network Security Appliance 6600

The SonicWall NSA 6600 is ideal for large distributed and corporate central site environments requiring high throughput capacity and performance.





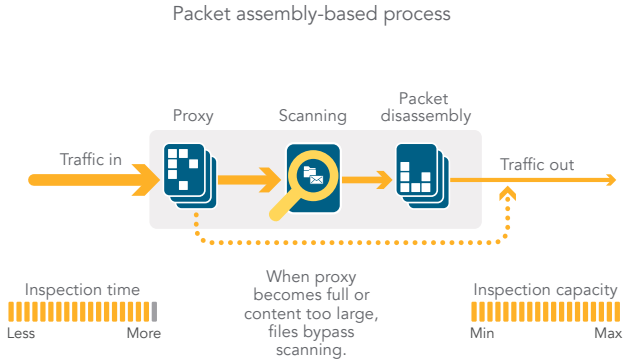
Firewall	NSA 6600
Firewall throughput	12.0 Gbps
IPS throughput	4.5 Gbps
Anti-malware throughput	3.0 Gbps
Full DPI throughput	3.0 Gbps
IMIX throughput	3.5 Gbps
Maximum DPI connections	500,000
New connections/sec	90,000/sec
Description	**SKU**
NSA 6600 firewall only	01-SSC-3820
NSA 6600 TotalSecure (1-year)	01-SSC-3823

Reassembly-Free Deep Packet Inspection engine

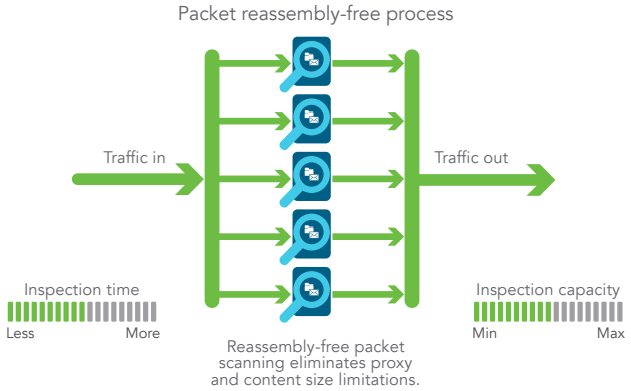
The SonicWall Reassembly-Free Deep Packet Inspection (RFDPI) engine provides superior threat protection and application control without compromising performance. It relies on streaming traffic payload inspection to detect threats at Layers 3-7, and takes network streams through extensive and repeated normalization and decryption in order to neutralize advanced evasion techniques that seek to confuse detection engines and sneak malicious code into the network.

Once a packet undergoes the necessary pre-processing, including SSL decryption, it is analyzed against a single, proprietary memory representation of three signature databases: intrusion attacks, malware and applications. The connection state is then advanced to represent the position of the stream relative to these databases until it encounters a state of attack, or other "match" event, at which point a pre-set action is taken.

In most cases, the connection is terminated and proper logging and notification events are created. However, the engine can also be configured for inspection only or, in case of application detection, to provide Layer 7 bandwidth management services for the remainder of the application stream as soon as the application is identified.



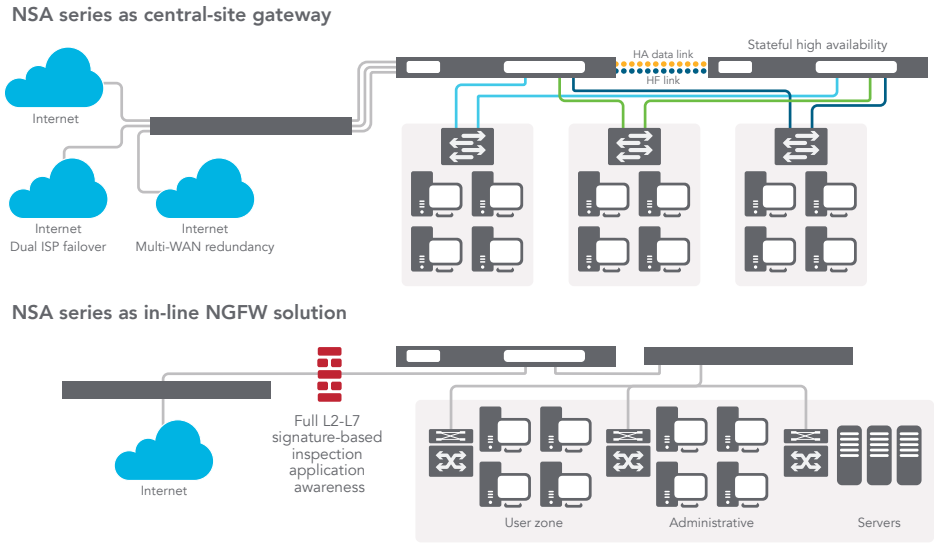
Competitive architecture



SonicWall architecture

Flexible, customizable deployment options – NSA series at-a-glance

Every SonicWall NSA appliance utilizes a breakthrough, multi-core hardware design and RFDPI for internal and external network protection without compromising network performance. The NSA series NGFWs combine 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 affordable platform that is easy to deploy and manage in a wide variety of large, branch office and distributed network environments.



SONICWALL™

Security and protection

The dedicated, in-house SonicWall Threat Research Team works on researching and developing counter-measures to deploy to the firewalls in the field for up-to-date protection. The team leverages more than one million sensors across the globe for malware samples, and for telemetry feedback on the latest threat information, which in turn is fed into the intrusion prevention, anti-malware and application detection capabilities.

SonicWall NGFW customers benefit from continuously updated threat protection around the clock, with new updates taking effect immediately without reboots or interruptions. The signatures resident on the appliances are designed to protect against wide classes of attacks, covering tens of thousands of individual threats with a single signature.

In addition to the countermeasures on the appliance, NSA appliances also have access to the SonicWall CloudAV Service, which extends the onboard signature intelligence with over 30 million signatures. This CloudAV database is accessed via a proprietary, light-weight protocol by the firewall to augment the inspection done on the appliance.

With Geo-IP and botnet filtering capabilities, SonicWall NGFWs are able to block traffic from dangerous domains or entire geographies in order to reduce the risk profile of the network.

Application intelligence and control

Application intelligence informs administrators of application traffic traversing their network, so they can schedule application controls based on business priority, throttle unproductive applications and block potentially dangerous applications. Real-time visualization identifies traffic anomalies as they happen, enabling immediate countermeasures against potential inbound or outbound attacks or performance bottlenecks.

SonicWall Application Traffic Analytics provide granular insight into application traffic, bandwidth utilization and security threats, as well as powerful troubleshooting and forensics capabilities. Additionally, secure Single Sign-On (SSO) capabilities ease the user experience, increase productivity and reduce support calls.

The SonicWall Global Management System (GMS®) simplifies management of application intelligence and control using an intuitive, web-based interface.

Features

RFDPI engine	
Feature	Description
Reassembly-Free Deep Packet Inspection (RFDPI)	This high-performance, proprietary and patented inspection engine performs stream-based, bi-directional traffic analysis, without proxying or buffering, to uncover intrusion attempts and malware and to identify application traffic regardless of port.
Bi-directional inspection	Scans for threats in both inbound and outbound traffic simultaneously to ensure that the network is not used to distribute malware and does not become a launch platform for attacks in case an infected machine is brought inside.
Stream-based inspection	Proxy-less and non-buffering inspection technology provides ultra-low latency performance for DPI of millions of simultaneous network streams without introducing file and stream size limitations, and can be applied on common protocols as well as raw TCP streams.
Highly parallel and scalable	The unique design of the RFDPI engine works with the multi-core architecture to provide high DPI throughput and extremely high new session establishment rates to deal with traffic spikes in demanding networks.
Single-pass inspection	A single-pass DPI architecture simultaneously scans for malware, intrusions and application identification, drastically reducing DPI latency and ensuring that all threat information is correlated in a single architecture.

Capture advanced threat protection	
Feature	Description
Multi-engine sandboxing	The multi-engine sandbox platform, which includes virtualized sandboxing, full system emulation and hypervisor level analysis technology, executes suspicious code and analyzes behavior, providing comprehensive visibility into malicious activity.
Broad file type and size analysis	Analyzes a broad range of file types including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems (Windows, Android, Mac OS X) and multi-browser environments.
Rapid deployment of signatures	When a file is identified as malicious, a signature is immediately deployed to firewalls with an active SonicWall Capture subscription as well as GRID Gateway Anti-virus and IPS signature databases plus URL, IP and domain reputation databases within 48 hours.
Block until verdict	To prevent potentially malicious files from entering the network, files sent to the cloud for analysis can be held at the gateway until a verdict is determined.

Intrusion prevention	
Feature	Description
Countermeasure-based protection	Tightly integrated intrusion prevention system (IPS) leverages signatures and other countermeasures to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities.
Automatic signature updates	The SonicWall Threat Research Team continuously researches and deploys updates to an extensive list of IPS countermeasures that covers more than 50 attack categories. The new updates take effect immediately, without any reboot or service interruption required.
Intra-zone IPS protection	Bolsters internal security by segmenting the network into multiple security zones with intrusion prevention, preventing threats from propagating across the zone boundaries.
Botnet command and control (CnC) detection and blocking	Identifies and blocks command and control traffic originating from bots on the local network to IPs and domains that are identified as propagating malware or are known CnC points.
Protocol abuse/anomaly detection and prevention	Identifies and blocks attacks that abuse protocols in an attempt to sneak past the IPS.
Zero-day protection	Protects the network against zero-day attacks with constant updates against the latest exploit methods and techniques that cover thousands of individual exploits.
Anti-evasion technology	Extensive stream normalization, decoding and other techniques ensure that threats do not enter the network undetected by utilizing evasion techniques in Layers 2-7.

Features

Threat prevention	
Feature	Description
Network-based malware protection	The SonicWall RFDPI engine scans all inbound, outbound and intra-zone traffic for viruses, Trojans, key loggers and other malware in files of unlimited length and size across all ports and TCP streams.
CloudAV malware protection	A continuously updated database of over 30 million threat signatures resides in the SonicWall cloud servers and is referenced to augment the capabilities of the onboard signature database, providing RFDPI with extensive coverage of threats.
Cloud-based sandboxing	SonicWall Capture Advance Threat Protection Service uses cloud-based, multi-engine sandboxing, including full system emulation, virtualization and hypervisor level techniques, to analyze suspicious files, detect malicious behavior and block unknown and zero-day attacks at the gateway.
Around-the-clock security updates	The SonicWall Threat Research Team analyzes new threats and releases countermeasures 24 hours a day, 7 days a week. New threat updates are automatically pushed to firewalls in the field with active security services, and take effect immediately without reboots or interruptions.
SSL decryption and inspection	Decrypts and inspects SSL traffic on the fly, without proxying, for malware, intrusions and data leakage, and applies application, URL and content control policies in order to protect against threats hidden in SSL encrypted traffic.
Bi-directional raw TCP inspection	The RFDPI engine is capable of scanning raw TCP streams on any port bi-directionally, preventing attacks that try to sneak by outdated security systems that focus on securing a few well-known ports.
Extensive protocol support	Identifies common protocols such as HTTP/S, FTP, SMTP, SMBv1/v2 and others, which do not send data in raw TCP, and decodes payloads for malware inspection, even if they do not run on standard, well-known ports.
Enforced Anti-Virus and Anti-Spyware Client software	Automatically detect non-compliant endpoint machines and install the Anti-Virus and Anti-Spyware software* machine-by-machine across the network regardless of whether devices are inside the corporate network or outside connected via VPN. Windows only.
**Requires the SonicWall Anti-Virus and Anti-Spyware Client software*	

Application intelligence and control	
Feature	Description
Application control	Controls applications, or individual application features, which are identified by the RFDPI engine against a continuously expanding database of over 3600 application signatures, to increase network security and enhance network productivity.
Custom application identification	Controls custom applications by creating signatures based on specific parameters or patterns unique to an application in its network communications, in order to gain further control over the network.
Application bandwidth management	Granularly allocates and regulates available bandwidth for critical applications or application categories while inhibiting non-essential application traffic.
On-box/off-box traffic visualization	Identifies bandwidth utilization and analyzes network behavior with real-time, on-box application traffic visualization and off-box application traffic reporting via NetFlow/IPFix.
Granular control	Controls applications, or specific components of an application, based on schedules, user groups, exclusion lists and a range of actions with full SSO user identification through LDAP/AD/Terminal Services/Citrix integration.

Content filtering	
Feature	Description
Inside/outside content filtering	Content Filtering Service enforces acceptable use policies and blocks access to websites containing information or images that are objectionable or unproductive. Content Filtering Client extends policy enforcement to block internet content for devices located outside the firewall perimeter.
Granular controls	Blocks content using the predefined categories or any combination of categories. Filtering can be scheduled by time of day, such as during school or business hours, and applied to individual users or groups.
Dynamic rating architecture	All requested web sites are cross-referenced against a dynamically updated database in the cloud categorizing millions of URLs, IP addresses and domains in real time.
Web caching	URL ratings are cached locally on the SonicWall firewall so that the response time for subsequent access to frequently visited sites is only a fraction of a second.

Features

Enforced anti-virus and anti-spyware	
Feature	Description
Multi-layered protection	A firewall's gateway anti-virus solution provides the first layer of defense at the perimeter; however, viruses can still enter the network through laptops, thumb drives and other unprotected systems. Utilizes a layered approach to anti-virus and anti-spyware protection to extend to both client and server.
Automated enforcement	Ensures every computer accessing the network has the most recent version of anti-virus and anti-spyware signatures installed and active, eliminating the costs commonly associated with desktop anti-virus and anti-spyware management.
Automated deployment and installation	Machine-by-machine deployment and installation of anti-virus and anti-spyware clients is automatic across the network, minimizing administrative overhead.
Always on, automatic virus protection	Frequent anti-virus and anti-spyware updates are delivered transparently to all desktops and file servers to improve end-user productivity and reduce security management.
Spyware protection	Powerful spyware protection scans and blocks the installation of a comprehensive array of spyware programs on desktops and laptops before they can transmit confidential data, providing greater desktop security and performance.

Firewall and networking	
Feature	Description
Stateful packet inspection	All network traffic is inspected, analyzed and brought into compliance with firewall access policies.
DDoS/DoS attack protection	SYN flood protection provides a defense against DOS attacks using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. Additionally, it protects against DOS/DDoS through UDP/ICMP flood protection and connection rate limiting.
Flexible deployment options	The NSA series can be deployed in traditional NAT, Layer 2 bridge, wire and network tap modes.
IPv6 support	Internet Protocol version 6 (IPv6) is in its early stages to replace IPv4. With the latest SonicOS 6.2, the hardware will support filtering and wire mode implementations.
High availability/clustering	The NSA series supports Active/Passive (A/P) with state synchronization, Active/Active (A/A) DPI and Active/Active clustering high availability modes. Active/Active DPI offloads the deep packet inspection load to cores on the passive appliance to boost throughput.
WAN load balancing	Load-balances multiple WAN interfaces using Round Robin, Spillover or Percentage methods.
Policy-based routing	Creates routes based on protocol to direct traffic to a preferred WAN connection with the ability to fail back to a secondary WAN in the event of an outage.
Advanced quality of service (QoS)	Guarantees critical communications with 802.1p, DSCP tagging, and remapping of VoIP traffic on the network.
H.323 gatekeeper and SIP proxy support	Blocks spam calls by requiring that all incoming calls are authorized and authenticated by H.323 gatekeeper or SIP proxy.

Management and reporting	
Feature	Description
Global Management System	SonicWall GMS monitors, configures and reports on multiple SonicWall appliances through a single management console with an intuitive interface, reducing management costs and complexity.
Powerful single device management	An intuitive web-based interface allows quick and convenient configuration, in addition to a comprehensive command-line interface and support for SNMPv2/3.
Application flow reporting	Exports application traffic analytics and usage data for real-time and historical monitoring and reporting with tools such as SonicWall GMS or Analyzer.

Virtual private networking (VPN)	
Feature	Description
IPSec VPN for site-to-site connectivity	High-performance IPSec VPN allows the NSA series to act as a VPN concentrator for thousands of other large sites, branch offices or home offices.
SSL VPN or IPSec client remote access	Utilizes clientless SSL VPN technology or an easy-to-manage IPSec client for easy access to email, files, computers, intranet sites and applications from a variety of platforms.
Redundant VPN gateway	When using multiple WANs, a primary and secondary VPN can be configured to allow seamless, automatic failover and failback of all VPN sessions.
Route-based VPN	The ability to perform dynamic routing over VPN links ensures continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly re-routing traffic between endpoints through alternate routes.

Content/context awareness	
Feature	Description
User activity tracking	User identification and activity are made available through seamless AD/LDAP/Citrix1/Terminal Services1 SSO integration combined with extensive information obtained through DPI.
GeoIP country traffic identification	Identifies and controls network traffic going to or coming from specific countries to either protect against attacks from known or suspected origins of threat activity, or to investigate suspicious traffic originating from the network.
Regular expression DPI filtering	Prevents data leakage by identifying and controlling content crossing the network through regular expression matching.

SonicOS feature summary

Firewall

- Reassembly-Free Deep Packet Inspection
- Deep packet inspection for SSL
- Stateful packet inspection
- Stealth mode
- Common Access Card (CAC) support
- DOS attack protection
- UDP/ICMP/SYN flood protection
- SSL decryption and inspection
- IPv6 security

Intrusion prevention

- Signature-based scanning
- Automatic signature updates
- Bidirectional inspection engine
- Granular IPS rule capability
- GeoIP and reputation-based filtering
- Regular expression matching

Anti-malware

- Stream-based malware scanning
- Gateway anti-virus
- Gateway anti-spyware
- Bi-directional inspection
- No file size limitation
- Cloud malware database

Application control

- Application control
- Application component blocking
- Application bandwidth management
- Custom application signature creation
- Data leakage prevention
- Application reporting over NetFlow/IPFIX
- User activity tracking (SSO)
- Comprehensive application signature database

Web content filtering

- URL filtering
- Anti-proxy technology
- Keyword blocking
- Bandwidth manage CFS rating categories
- Unified policy model with app control
- 56 content filtering categories
- Content Filtering Client

VPN

- IPSec VPN for site-to-site connectivity
- SSL VPN and IPSec client remote access
- Redundant VPN gateway
- Mobile Connect for iOS, Mac OS X, Windows, Chrome, Android and Kindle Fire
- Route-based VPN (OSPF, RIP)

Networking

- Jumbo frames
- Layer-2 network discovery
- IPv6
- Path MTU discovery
- Enhanced logging
- VLAN trunking
- RSTP (Rapid Spanning Tree Protocol)
- Port mirroring
- Layer-2 QoS
- Port security
- Dynamic routing
- SonicPoint wireless controller
- Policy-based routing
- Advanced NAT
- DHCP server
- Bandwidth management
- Link aggregation
- Port redundancy
- A/P high availability with state sync
- A/A clustering
- Inbound/outbound load balancing
- L2 bridge, wire mode, tap mode, NAT mode

VoIP

- Granular QoS control
- Bandwidth management
- DPI for VoIP traffic
- H.323 gatekeeper and SIP proxy support

Management and monitoring

- Web GUI
- Command line interface (CLI)
- SNMPv2/v3
- Centralized management and reporting
- Logging
- Netflow/IPFix exporting
- App traffic visualization
- Centralized policy management
- Single Sign-On (SSO)
- Terminal service/Citrix support
- BlueCoat Security Analytics Platform
- Application and bandwidth visualization
- IPv4 and IPv6 Management

IPv6

- IPv6 filtering
- 6rd (rapid deployment)
- DHCP prefix delegation
- Wire mode
- BGP

Capture ATP

- Cloud-based multi-engine analysis
- Virtualized sandboxing
- Hypervisor level analysis
- Full system emulation
- Broad file type examination
- Automated and manual submission
- Real-time threat intelligence updates
- Auto-block capability

NSA series system specifications

	NSA 2600	NSA 3600	NSA 4600	NSA 5600	NSA 6600
Operating system	SonicOS 6.2.2				
Security processing cores	4 x 800 MHz	6 x 800 MHz	8 x 1.1 GHz	10 x 1.3 GHz	24 x 1.0 GHz
10 GbE interfaces	—	2 x 10-GbE SFP+			4 x 10-GbE SFP+
1 GbE interfaces	8 x 1 GbE	4 x 1-GbE SFP, 12 x 1 GbE			8 x 1-GbE SFP, 8 x 1 GbE (1 LAN Bypass pair)
Management interfaces	1 GbE, 1 Console				
Memory (RAM)	2.0 GB			4.0 GB	
Expansion	1 Expansion Slot (Rear)*, SD Card*				
Firewall inspection throughput[1]	1.9 Gbps	3.4 Gbps	6.0 Gbps	9.0 Gbps	12.0 Gbps
Full DPI throughput[2]	300 Mbps	500 Mbps	800 Mbps	1.6 Gbps	3.0 Gbps
Application inspection throughput[2]	700 Mbps	1.1 Gbps	2.0 Gbps	3.0 Gbps	4.5 Gbps
IPS throughput[2]	700 Mbps	1.1 Gbps	2.0 Gbps	3.0 Gbps	4.5 Gbps
Anti-malware inspection throughput[2]	400 Mbps	600 Mbps	1.1 Gbps	1.7 Gbps	3.0 Gbps
IMIX throughput[3]	600 Mbps	900 Mbps	1.6 Gbps	2.4 Gbps	3.5 Gbps
SSL Inspection and Decryption (DPI SSL)[2]	200 Mbps	300 Mbps	500 Mbps	800 Mbps	1.3 Gbps
VPN throughput[3]	1.1 Gbps	1.5 Gbps	3.0 Gbps	4.5 Gbps	5.0 Gbps
Connections per second	15,000/sec	20,000/sec	40,000/sec	60,000/sec	90,000/sec
Maximum connections (SPI)	225,000	325,000	400,000	562,500	750,000
Maximum connections (DPI)	125,000	175,000	200,000	375,000	500,000
SonicPoints supported (Maximum)	32	48	64	96	128
Single Sign-on (SSO) Users	30,000	40,000	50,000	60,000	70,000
VPN	**NSA 2600**	**NSA 3600**	**NSA 4600**	**NSA 5600**	**NSA 6600**
Site-to-site tunnels	250	1,000	3,000	4,000	6,000
IPSec VPN clients (Maximum)	10 (250)	50 (1,000)	500 (3,000)	2,000 (4,000)	2,000 (6,000)
SSL VPN licenses (Maximum)	2 (250)	2 (350)	2 (500)	2 (1000)	2 (1500)
Encryption/Authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B Cryptography				
Key exchange	Diffie Hellman Groups 1, 2, 5, 14				
Route-based VPN	RIP, OSPF				
Networking	**NSA 2600**	**NSA 3600**	**NSA 4600**	**NSA 5600**	**NSA 6600**
IP address assignment	Static (DHCP PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP Relay				
NAT modes	1:1, many:1, 1:many, flexible NAT (overlapping IPS), PAT, transparent mode				
VLAN interfaces	256	256	256	400	500
Routing protocols	BGP, OSPF, RIPv1/v2, static routes, policy-based routing, multicast				
QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p				
Authentication	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, internal user database, Terminal Services, Citrix, Common Access Card (CAC)				
VoIP	Full H323-v1-5, SIP				
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3				
Certifications	ICSA Firewall, ICSA Anti-Virus, FIPS 140-2, Common Criteria NDPP (Firewall and IPS), UC APL				
Hardware	**NSA 2600**	**NSA 3600**	**NSA 4600**	**NSA 5600**	**NSA 6600**
Power supply	200W	Single, Fixed 250W			
Fans	Dual, Fixed				Dual, redundant, hot swappable
Input power	100-240 VAC, 60-50 Hz				
Maximum power consumption (W)	49.4	74.3	86.7	90.9	113.1
Form factor	1U Rack Mountable				
Dimensions	1.75 x 10.25 x 17 in (4.5 x 26 x 43 cm)	1.75 x 19.1 x 17 in (4.5 x 48.5 x 43 cm)			
Weight	10.1 lb (4.6 kg)	13.56 lb (6.15 Kg)			14.93 lb (6.77 Kg)
WEEE weight	11.0 lb (5.0 kg)	14.24 lb (6.46 Kg)			19.78 lb (8.97 Kg)
Shipping weight	14.3 lb (6.5 kg)	20.79lb (9.43 Kg)			26.12 lb (11.85 Kg)
Major regulatory	FCC Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, MSIP/KCC Class A, UL, cUL, TUV/GS, CB, Mexico CoC by UL, WEEE , REACH, ANATEL, BSMI, CU				
Environment	32-105 F, 0-40 deg C				
Humidity	10-90% non-condensing				
MTBF (Years)	20.2	16.8	16.0	15.4	13.3

[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/GatewayAV/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] *VPN throughput measured using UDP traffic at 1280 byte packet size adhering to RFC 2544. All specifications, features and availability are subject to change.*
**Future use.*

SONICWALL™

NSA series ordering information

Product	SKU
NSA 2600 TotalSecure (1-year)	01-SSC-3863
NSA 3600 TotalSecure (1-year)	01-SSC-3853
NSA 4600 TotalSecure (1-year)	01-SSC-3843
NSA 5600 TotalSecure (1-year)	01-SSC-3833
NSA 6600 TotalSecure (1-year)	01-SSC-3823
NSA 2600 security and support subscriptions	**SKU**
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for NSA 2600 (1-year)	01-SSC-1470
Capture Advanced Threat Protection for NSA 2600 (1-year)	01-SSC-1475
Threat Prevention–Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSA 2600 (1-year)	01-SSC-4459
Silver 24x7 Support for NSA 2600 (1-year)	01-SSC-4314
Content Filtering Premium Business Edition for NSA 2600 (1-year)	01-SSC-4465
Enforced Client Anti-Virus & Anti-Spyware — Kaspersky	Based on user count
Comprehensive Anti-Spam Service for NSA 2600 (1-year)	01-SSC-4471
NSA 3600 security and support subscriptions	**SKU**
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for NSA 3600 (1-year)	01-SSC-1480
Capture Advanced Threat Protection for NSA 3600 (1-year)	01-SSC-1485
Threat Prevention–Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSA 3600 (1-year)	01-SSC-4435
Silver 24x7 Support for NSA 3600 (1-year)	01-SSC-4302
Content Filtering Premium Business Edition for NSA 3600 (1-year)	01-SSC-4441
Enforced Client Anti-Virus & Anti-Spyware — Kaspersky	Based on user count
Comprehensive Anti-Spam Service for NSA 3600 (1-year)	01-SSC-4447
NSA 4600 security and support subscriptions	**SKU**
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for NSA 4600 (1-year)	01-SSC-1490
Capture Advanced Threat Protection for NSA 4600 (1-year)	01-SSC-1495
Threat Prevention–Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSA 4600 (1-year)	01-SSC-4411
Silver 24x7 Support for NSA 4600 (1-year)	01-SSC-4290
Content Filtering Premium Business Edition for NSA 4600 (1-year)	01-SSC-4417
Enforced Client Anti-Virus & Anti-Spyware — Kaspersky	Based on user count
Comprehensive Anti-Spam Service for NSA 4600 (1-year)	01-SSC-4423
NSA 5600 security and support subscriptions	**SKU**
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for NSA 5600 (1-year)	01-SSC-1550
Capture Advanced Threat Protection for NSA 5600 (1-year)	01-SSC-1555
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSA 5600 (1-year)	01-SSC-4240
Gold 24x7 Support for NSA 5600 (1-year)	01-SSC-4284
Content Filtering Premium Business Edition for NSA 5600 (1-year)	01-SSC-4246
Enforced Client Anti-Virus & Anti-Spyware — Kaspersky	Based on user count
Comprehensive Anti-Spam Service for NSA 5600 (1-year)	01-SSC-4252
NSA 6600 security and support subscriptions	**SKU**
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for NSA 6600 (1-year)	01-SSC-1560
Capture Advanced Threat Protection for NSA 6600 (1-year)	01-SSC-1565
Threat Prevention–Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSA 6600 (1-year)	01-SSC-4216
Gold 24x7 Support for NSA 6600 (1-year)	01-SSC-4278
Content Filtering Premium Business Edition for NSA 6600 (1-year)	01-SSC-4222
Enforced Client Anti-Virus & Anti-Spyware — Kaspersky	Based on user count
Comprehensive Anti-Spam Service for NSA 6600 (1-year)	01-SSC-4228
Modules and accessories*	**SKU**
10GBASE-SR SFP+ Short Reach Module	01-SSC-9785
10GBASE-LR SFP+ Long Reach Module	01-SSC-9786
10GBASE SFP+ 1M Twinax Cable	01-SSC-9787
10GBASE SFP+ 3M Twinax Cable	01-SSC-9788
1000BASE-SX SFP Short Haul Module	01-SSC-9789
1000BASE-LX SFP Long Haul Module	01-SSC-9790
1000BASE-T SFP Copper Module	01-SSC-9791
Management and reporting	**SKU**
SonicWall GMS 10 Node Software License	01-SSC-3363
SonicWall GMS E-Class 24x7 Software Support for 10 node (1-year)	01-SSC-6514

**Please consult with your local SonicWall reseller for a complete list of supported SFP and SFP+ modules*

SONICWALL™

Regulatory model numbers:

NSA 2600–1RK29-0A9

NSA 3600–1RK26-0A2

NSA 4600–1RK26-0A3

NSA 5600–1RK26-0A4

NSA 6600–1RK27-0A5

About Us

Over a 25 year history, SonicWall has been the industry's trusted security partner. From network security to access security to email security, SonicWall has continuously evolved its product portfolio, enabling organizations to innovate, accelerate and grow. With over a million security devices in almost 200 countries and territories worldwide, SonicWall enables its customers to confidently say yes to the future.

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, CA 95054
Refer to our website for additional information.
www.sonicwall.com

Datasheet-NetworkSecurityAppliance-US-VG-26120

SONICWALL™