Network Security Appliance Series

Next-Generation Firewalls

Your organization faces unprecedented security challenges. The sophistication and volume of attacks increase exponentially, resulting in lost company, personal and customer data, stolen intellectual property, damaged reputations and lost productivity. Security is more complex. You need to clarify what is important when assessing alternatives. With the (bring your own) BYO revolution, the explosion of personal devices connecting to the network, led by smartphones and tablets, slows performance and decreases productivity. Also, mobile applications, such as social media and video streaming, consume an enormous amount of bandwidth. This creates two distinct problems: ensuring security and maintaining productivity. IT managers often compromise security by turning off features to maintain network performance.

Now your organization can be both secure and productive without compromising network performance. The Dell™ SonicWALL™ Network Security Appliance (NSA) Series is the one of the most secure, highest performing Next-Generation Firewall lines. It delivers enterprise-class security and performance without compromise, using the same architecture as the flagship SuperMassive Next-Generation Firewall line—initially developed for the world's most demanding carriers and enterprises. At the same time, it offers Dell's acclaimed

ease of use and high value. Based on years of research and development, the NSA Series is designed from the ground up for distributed enterprises, small- to medium-sized businesses, branch offices, school campuses and government agencies. The NSA Series combines a revolutionary multi-core architecture with a patented* Reassembly-Free Deep Packet Inspection® (RFDPI) single-pass threat-prevention engine in a massively scalable design. This offers industry-leading protection, performance, and scalability, with the highest number of concurrent connections, lowest latency, and most connections-per-second in its class with no file size limitations. Highly respected independent third-party testing firms have evaluated and/or certified the technology for your confidence and assurance.

Unlike competing legacy firewall and intrusion prevention technologies, the NSA Series looks at all traffic, regardless of port or protocol. The NSA Series blocks advanced encrypted malware attacks, with the industry's highest on-the-fly SSL decryption rates. Also, authentication server integration efficiently enforces acceptable use policy through granular application controls for bandwidth management and enhanced productivity. Unlike antiquated two-box solutions that do not share threat information, the NSA Series integrates firewall and IPS. This connected

intelligence enforces policy decisions to intensify security effectiveness, while slashing management burdens and organizational risk. The Dell SonicWALL Global Management System (GMS) enables distributed enterprises to manage thousands of SonicWALL security appliances over a consolidated single-pane-of-glass view, easing administration and reducing total cost of ownership. Comprehensive real-time visualization shows you what is happening on your network with thorough on-box and off-box reporting.

- **Best in-class protection**
- **Multi-core architecture**
- **Ultra high performance**
- **Intrusion prevention**
- **Gateway anti-malware**
- **Secure remote access**
- **Secure wireless**
- **URL filtering**
- **Gateway anti-spam**
- **Application control**
- **Centralized management**

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

The Dell SonicWALL NSA Series Next-Generation Firewalls utilize the latest multi-core hardware design and Reassembly-Free Deep Packet Inspection to protect the network from internal and external attacks without compromising performance. The NSA Series combines intrusion prevention, file and content inspection, application intelligence and control, high availability and advanced networking features.

Network Security Appliance 3600
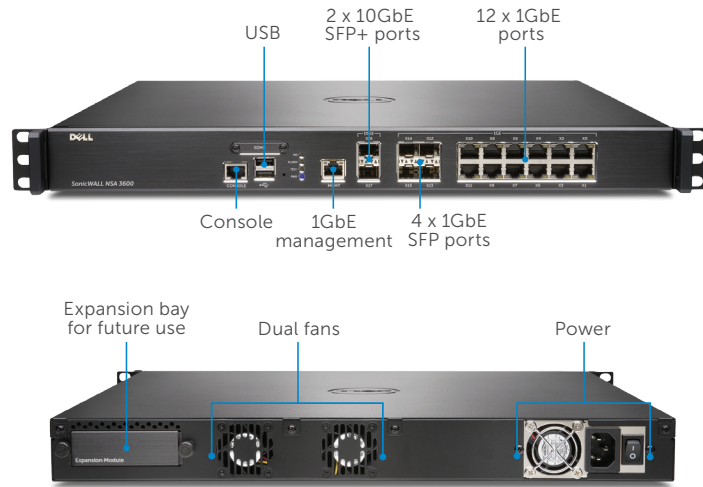
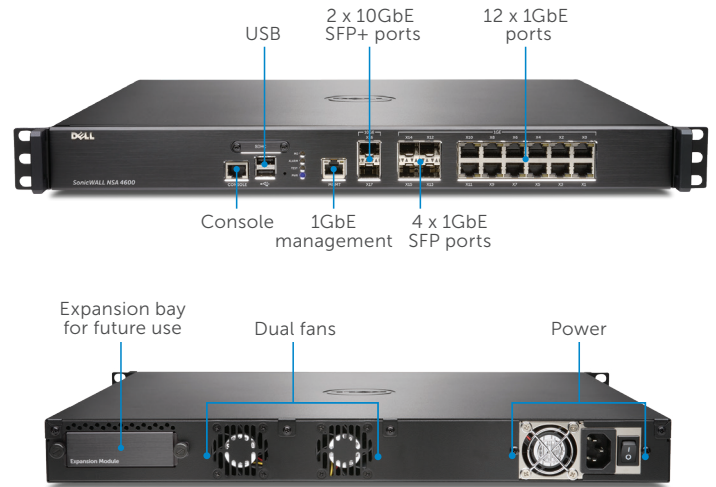The Dell SonicWALL NSA 3600 is ideal for branch office sites in distributed enterprise, small- to medium-sized businesses and retail environments.

Firewall	NSA 3600
Firewall throughput[1]	3.4 Gbps
IPS throughput[2]	1.1 Gbps
Anti-malware throughput[2]	600 Mbps
Full DPI throughput[2]	500 Mbps
IMIX throughput[3]	900 Mbps
Maximum DPI connections	175,000
New connections/sec	20,000/sec

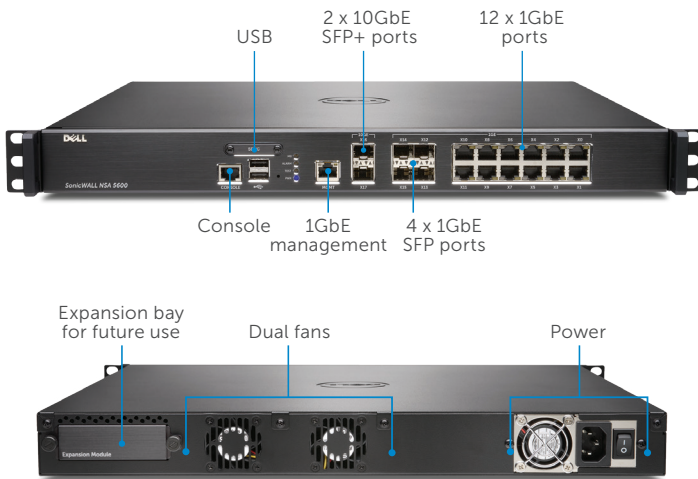| Description	SKU
NSA 3600 firewall only	01-SSC-3850
NSA 3600 TotalSecure (1-year)	01-SSC-3853
Comprehensive Gateway Security Suite (1-year)	01-SSC-4429
Gateway Anti-Malware/IPS (1-year)	01-SSC-4435
Silver Support 24x7 (1-year)	01-SSC-4302

Network Security Appliance 4600

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

Firewall	NSA 4600
Firewall throughput[1]	6.0 Gbps
IPS throughput[2]	2.0 Gbps
Anti-malware throughput[2]	1.1 Gbps
Full DPI throughput[2]	800 Mbps
IMIX throughput[3]	1.6 Gbps
Maximum DPI connections	250,000
New connections/sec	40,000/sec

Description	SKU
NSA 4600 firewall only	01-SSC-3840
NSA 4600 TotalSecure (1-year)	01-SSC-3843
Comprehensive Gateway Security Suite (1-year)	01-SSC-4405
Secure Upgrade Plus (3-year)	01-SSC-4267
Silver Support 24x7 (1-year)	01-SSC-4290

DELL SonicWALL

Network Security Appliance 5600

USB · 2 x 10GbE SFP+ ports · 12 x 1GbE ports

Console · 1GbE management · 4 x 1GbE SFP ports

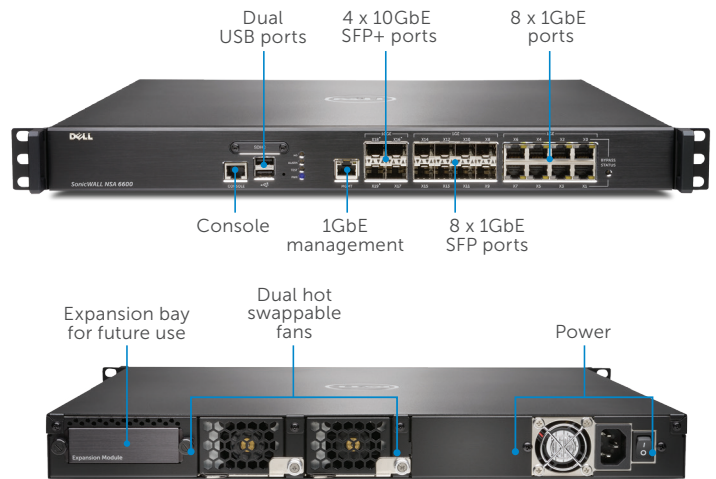Expansion bay for future use · Dual fans · Power

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

Firewall	NSA 5600
Firewall throughput[1]	9.0 Gbps
IPS throughput[2]	3.0 Gbps
Anti-malware throughput[2]	1.7 Gbps
Full DPI throughput[2]	1.6 Gbps
IMIX throughput[3]	2.4 Gbps
Maximum DPI connections	500,000
New connections/sec	60,000/sec

Description	SKU
NSA 5600 firewall only	01-SSC-3830
NSA 5600 TotalSecure (1-year)	01-SSC-3833
Comprehensive Gateway Security Suite (1-year)	01-SSC-4234
Gateway Anti-Malware/IPS (1-year)	01-SSC-4240
Gold Support 24x7 (1-year)	01-SSC-4284

Network Security Appliance 6600

Dual USB ports · 4 x 10GbE SFP+ ports · 8 x 1GbE ports

Console · 1GbE management · 8 x 1GbE SFP ports

Expansion bay for future use · Dual hot swappable fans · Power

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

Firewall	NSA 6600
Firewall throughput[1]	12.0 Gbps
IPS throughput[2]	4.5 Gbps
Anti-malware throughput[2]	3.0 Gbps
Full DPI throughput[2]	3.0 Gbps
IMIX throughput[3]	3.5 Gbps
Maximum DPI connections	600,000
New connections/sec	90,000/sec

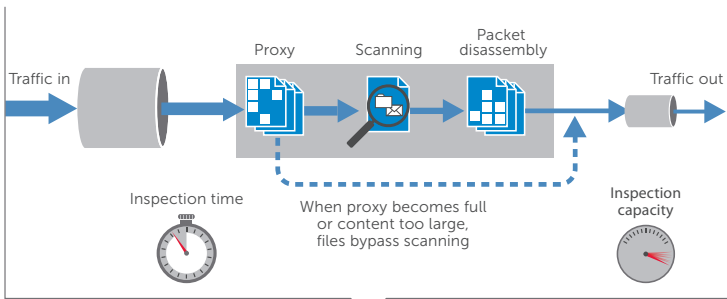| Description	SKU
NSA 6600 firewall only	01-SSC-3820
NSA 6600 TotalSecure (1-year)	01-SSC-3823
Comprehensive Gateway Security Suite (1-year)	01-SSC-4210
Gateway Anti-Malware/IPS (1-year)	01-SSC-4216
Gold Support 24x7 (1-year)	01-SSC-4278

DELL SonicWALL

Reassembly-Free Deep Packet Inspection engine

The Dell SonicWALL Reassembly-Free Deep Packet Inspection (RFDPI) engine provides superior threat protection and application control without compromising performance. This patented engine relies on streaming traffic payload inspection in order to detect threats at Layers 3-7. The RFDPI engine 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 re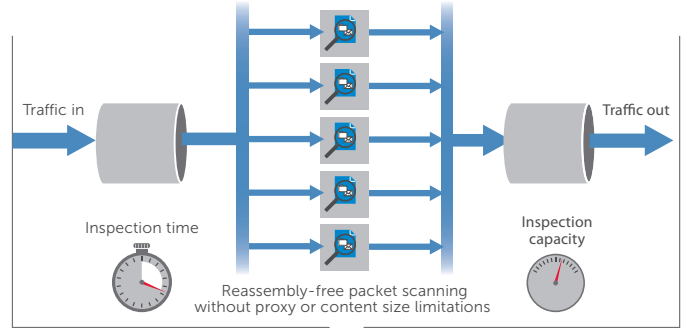lative to these databases until it encounters a state of attack, or other "match" event, at which point a pre-set action is taken. In most cases, the connection is terminated and proper logging and notification events are created. However, the engine can also be configured for inspection only or, in 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.

Packet assembly-based process

Traffic in — Proxy — Scanning — Packet disassembly — Traffic out

Inspection time

When proxy becomes full or content too large, files bypass scanning

Inspection capacity

Competitive architecture

Packet reassembly-free process

Traffic in — Traffic out

Inspection time

Reassembly-free packet scanning without proxy or content size limitations
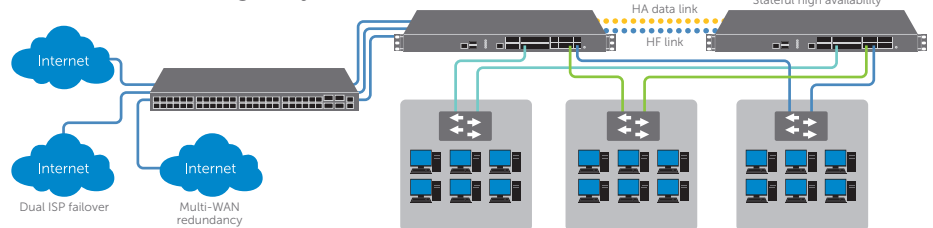
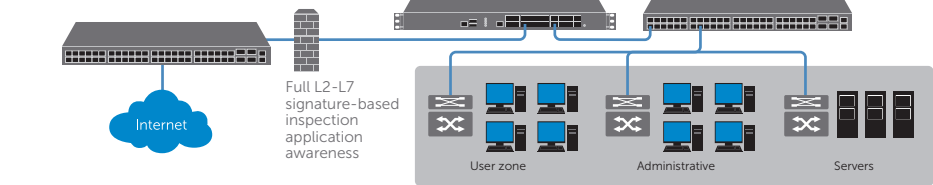Inspection capacity

Dell SonicWALL architecture

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 affordable platform that is easy to deploy and manage in a wide variety of corporate, branch office and distributed network environments.

NSA Series as central-site gateway

Internet

Internet — Dual ISP failover

Internet — Multi-WAN redundancy

HA data link

HF link

Stateful high availability

NSA Series as in-line NGFW solution

Internet

Full L2-L7 signature-based inspection application awareness

User zone — Administrative — Servers

DELL SonicWALL

Security and protection

The dedicated, in-house Dell 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. Dell SonicWALL Next-Generation Firewall customers with the latest security capabilities are provided 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 up to tens of thousands of individual threats with a single signature.

In addition to the countermeasures on the appliance, NSA appliance also have access to the Dell SonicWALL CloudAV Service, which extends the onboard signature intelligence with more than twelve 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, Dell SonicWALL Next-Gen Firewalls are able to block traffic from dangerous domains or entire geographies in order to reduce the risk profile of the network.
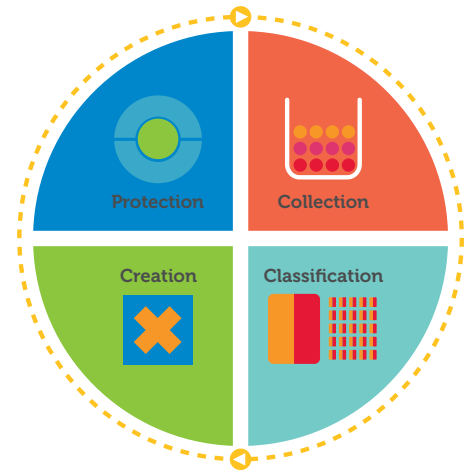
Application intelligence and control

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.

Dell 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 user experience, increase productivity and reduce support calls.
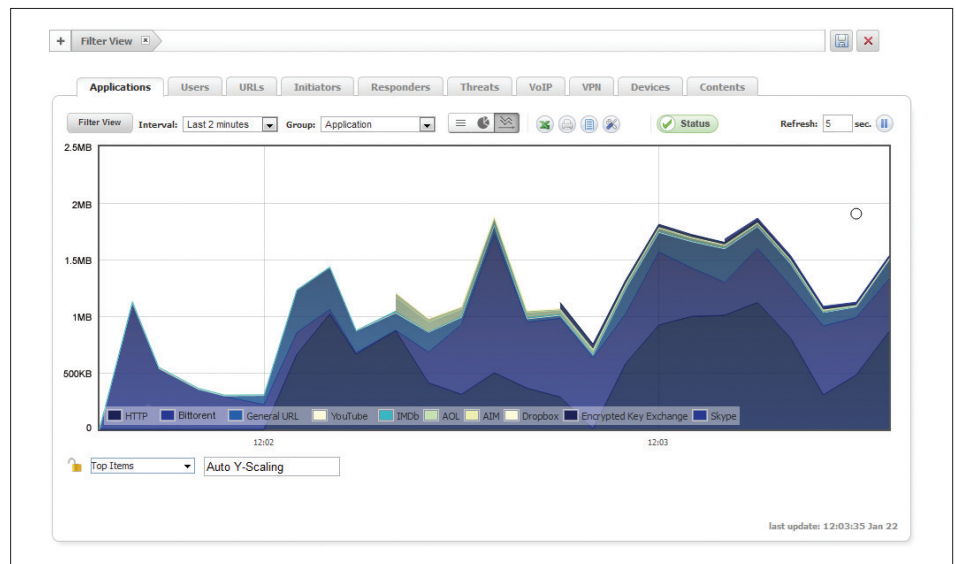
The Dell SonicWALL Global Management System (GMS®) simplifies management of application intelligence and control using an intuitive web-based interface.

DELL SonicWALL

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, malware and 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 for application identification, drastically reducing DPI latency and ensuring that all threat information is correlated in a single architecture.

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 Dell 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 immediate effect 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.

DELL SonicWALL

Features

Threat prevention	
Feature	Description
Gateway anti-malware	The Dell 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	A continuously updated database of over 12 million threat signatures resides in the Dell SonicWALL cloud servers and is referenced to augment the capabilities of the onboard signature database, providing RFDPI with extensive coverage of threats.
Around-the-clock security updates	The Dell 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 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.

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 4,300 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	Restricts or prioritizes applications or application categories in order to maximize available bandwidth for critical applications while eliminating or reducing undesired 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, users groups, exclusion lists and a range of actions with full SSO user identification through LDAP/AD/Terminal Services/Citrix integration.

DELL SonicWALL

Features

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 provides the ability to protect 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 Mode, and Network Tap modes.
High availability/clustering	The NSA Series supports Active/Passive with state synchronization, Active/Active 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 based 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 QoS	Guarantees critical communications with 802.1p and 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	With Dell SonicWALL GMS, monitors, configures and reports on multiple Dell SonicWALL appliances through a single management console with an intuitive interface, to reduce management costs and complexity.
Powerful single device management	An intuitive web-based interface allows quick and convenient configuration, in addition to a comprehensive CLI and support for SNMPv2/3.
IPFIX/NetFlow application flow reporting	Exports application traffic analytics and usage data through IPFIX or NetFlow protocols for real-time and historical monitoring and reporting with tools, such as Dell SonicWALL Scrutinizer or other tools that support IPFIX and NetFlow with extensions.

Virtual Private Networking

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.

DELL SonicWALL

Features

Content/context awareness

Feature	Description
User activity tracking	User identification and activity are made available through seamless AD/LDAP/Citrix/Terminal Services 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
- TCP reassembly
- Stealth mode
- Common Access Card (CAC) support
- DOS attack protection
- UDP/ICMP/SYN flood protection

Intrusion prevention
- Signature-based scanning
- Automatic signature updates
- Outbound threat prevention
- IPS exclusion list
- GeoIP and reputation-based filtering
- Regular expression matching

Anti-Malware
- Stream-based malware scanning
- Gateway anti-virus
- Gateway anti-spyware
- SSL decryption
- Bi-directional inspection
- No file size limitation
- CloudAV threat database

Application control
- Application control
- Application component blocking
- Application bandwidth management
- Custom application signature creation
- Application traffic visualization
- 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

VPN
- IPSec VPN for site-to-site connectivity
- SSL VPN or IPSec client remote access
- Redundant VPN gateway
- Mobile Connect for Apple® iOS and Google® Android™
- Route-based VPN (OSPF, RIP)

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

Management and monitoring
- Web GUI
- Command line interface (CLI)
- SNMPv2/v3
- Off-box reporting (Scrutinizer)
- Centralized management and reporting
- Logging
- Netflow/IPFix exporting
- App traffic visualization
- LCD management screen
- Centralized policy management
- Single Sign-On (SSO)
- Terminal service/Citrix support
- Solera Networks Forensics integration

DELL SonicWALL

NSA Series system specifications

	NSA 3600	NSA 4600	NSA 5600	NSA 6600
Operating system	SonicOS 6.1			
Security cores	6	8	10	24
10 GbE interfaces	2 x 10-GbE SFP+			4 x 10-GbE SFP+
1 GbE interfaces	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	2.0 GB	4.0 GB	4.0 GB
Expansion	1 Expansion Slot (Rear)*, SD Card*			
Firewall inspection throughput[1]	3.4 Gbps	6.0 Gbps	9.0 Gbps	12.0 Gbps
Full DPI throughput[2]	500 Mbps	800 Mbps	1.6 Gbps	3.0 Gbps
Application inspection throughput[2]	1.1 Gbps	2.0 Gbps	3.0 Gbps	4.5 Gbps
IPS throughput[2]	1.1 Gbps	2.0 Gbps	3.0 Gbps	4.5 Gbps
Anti-malware inspection throughput[2]	600 Mbps	1.1 Gbps	1.7 Gbps	3.0 Gbps
IMIX throughput[3]	900 Mbps	1.6 Gbps	2.4 Gbps	3.5 Gbps
SSL Inspection and Decryption (DPI SSL)[2]	300 Mbps	500 Mbps	800 Mbps	1.3 Gbps
VPN throughput[3]	1.5 Gbps	3.0 Gbps	4.5 Gbps	5.0 Gbps
Connections per second	20,000/sec	40,000/sec	60,000/sec	90,000/sec
Maximum connections (SPI)	325,000	500,000	750,000	1,000,000
Maximum connections (DPI)	175,000	250,000	500,000	600,000
SonicPoints supported (Maximum)	48	64	96	96
VPN				
Site-to-site tunnels	800	1,500	4000	6000
IPSec VPN clients (Maximum)	50 (1,000)	500 (3,000)	2,000 (4,000)	2,000 (6,000)
SSL VPN licenses (Maximum)	2 (30)	2 (30)	2 (50)	2 (50)
Encryption/Authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1			
Key exchange	Diffie Hellman Groups 1, 2, 5, 14			
Route-based VPN	RIP, OSPF			
Networking				
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	512			
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			
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	VPNC, ICSA Firewall, ICSA Anti-Virus			
Certifications pending	FIPS 140-2, Common Criteria EAL1+			
Common Access Card (CAC)	Pending			
Hardware				
Power supply	Single, Fixed 250W			
Fans	Dual, Fixed			Dual, redundant, hot swappable
Input power	100-240 VAC, 60-50 Hz			
Maximum power consumption (W)	74.3	86.7	90.9	113.1
Form factor	1U Rack Mountable			
Dimensions	17x19.1x1.75 in (43.3x48.5x4.5 cm)			
Weight	13.56 lb (6.15 Kg)			14.93 lb (6.77 Kg)
WEEE weight	14.24 lb (6.46 Kg)			19.78 lb (8.97 Kg)
Shipping weight	20.79lb (9.43 Kg)			26.12 lb (11.85 Kg)
Major regulatory	FCC Class A, CE, C-Tick, VCCI, Compliance KCC, UL, cUL, TUV/GS, CB, NOM, RoHS, WEEE , ANATEL, BSMI			
Environment	32-105 F, 0-40 deg C			
Humidity	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/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.

DELL SonicWALL

NSA Series ordering information

Product	SKU
NSA 3600, 2 SFP+ 10GbE ports, 4 SFP 1GbE ports, 12 Copper 1GbE ports	01-SSC-3850
NSA 4600, 2 SFP+ 10GbE ports, 4 SFP 1GbE ports, 12 Copper 1GbE ports	01-SSC-3840
NSA 5600, 2 SFP+ 10GbE ports, 4 SFP 1GbE ports, 12 Copper 1GbE ports	01-SSC-3830
NSA 6600, 4 SFP+ 10GbE ports, 8 SFP 1GbE ports, 8 Copper 1GbE ports	01-SSC-3820
NSA 3600 Support and Security Subscriptions	**Sku**
Comprehensive Gateway Security Suite−Application Intelligence, Threat Prevention, Content Filtering with Support for 3600 (1-year)	01-SSC-4429
Threat Prevention−Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for 3600 (1-year)	01-SSC-4435
Silver 24x7 Support for the NSA 3600 (1-year)	01-SSC-4302
Content Filtering Premium Business Edition for 3600 (1-year)	01-SSC-4441
Comprehensive Anti-Spam Service For NSA 3600 (1-year)	01-SSC-4447
NSA 4600 Support and Security Subscriptions	**Sku**
Comprehensive Gateway Security Suite−Application Intelligence, Threat Prevention, Content Filtering with Support for 4600 (1-year)	01-SSC-4405
Threat Prevention−Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for 4600 (1-year)	01-SSC-4411
Silver 24x7 Support for the NSA 4600 (1-year)	01-SSC-4290
Content Filtering Premium Business Edition for 4600 (1-year)	01-SSC-4417
Comprehensive Anti-Spam Service For NSA 4600 (1-year)	01-SSC-4423
NSA 5600 Support and Security Subscriptions	**SKU**
Comprehensive Gateway Security Suite−Application Intelligence, Threat Prevention, Content Filtering with Support for 5600 (1-year)	01-SSC-4234
Threat Prevention−Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for 5600 (1-year)	01-SSC-4240
Gold 24x7 Support for the NSA 5600 (1-year)	01-SSC-4284
Content Filtering Premium Business Edition for 5600 (1-year)	01-SSC-4246
Comprehensive Anti-Spam Service For NSA 5600 (1-year)	01-SSC-4252
NSA 6600 Support and Security Subscriptions	**SKU**
Comprehensive Gateway Security Suite−Application Intelligence, Threat Prevention, Content Filtering with Support for 6600 (1-year)	01-SSC-4210
Threat Prevention−Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for 6600 (1-year)	01-SSC-4216
Gold 24x7 Support for the NSA 6600 (1-year)	01-SSC-4278
Content Filtering Premium Business Edition for 6600 (1-year)	01-SSC-4222
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**
Dell SonicWALL GMS 10 Node Software License	01-SSC-3363
Dell SonicWALL GMS E-Class 24x7 Software Support for 10 node (1-year)	01-SSC-6514
Dell SonicWALL Scrutinizer Virtual Appliance with Flow Analytics Module Software License for up to 5 nodes (includes one year of 24x7 Software Support)	01-SSC-3443
Dell SonicWALL Scrutinizer with Flow Analytics Module Software License for up to 5 nodes (includes one year of 24x7 Software Support)	01-SSC-4002
Dell SonicWALL Scrutinizer Advanced Reporting Module Software License for up to 5 nodes (includes one year of 24x7 Software Support)	01-SSC-3773

*Please consult with a Dell SE for a complete list of supported SFP and SFP+ modules

DELL SonicWALL

DELL SonicWALL