



Network Security Appliance Series

Next-generation firewalls

Today's organizations face unprecedented security challenges. The sophistication and volume of attacks is increasing exponentially, often resulting in lost company, personal and customer data; stolen intellectual property; damaged reputations; and lost productivity. At the same time, security has become more complex. Organizations are grappling with the BYOD revolution and the explosion of personal devices connecting to the network. Personal smartphones and tablets slow network performance and productivity, and mobile applications such as social media and video streaming consume an enormous amount of bandwidth. In order to address these network security and productivity challenges, some organizations have chosen to compromise their 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 next-generation firewalls (NGFWs) deliver network security that does not compromise performance. It delivers world-class security and performance without compromise, using the same architecture as the flagship SuperMassive next-generation firewall line. At the same time, the NSA Series offers Dell's acclaimed ease of use and high value.

At the same time, the NSA series 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. It 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 gives organizations industry-leading protection, performance and scalability with a high number of concurrent connections, low latency and high connections-per-second with no file size limitations. Highly respected independent third-party testing firms have evaluated and/or certified the technology of the NSA Series firewalls.

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 malware attacks with the industry's highest on-the-fly SSL decryption rates. Its 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.



Benefits:

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

In addition, NSA Series firewalls feature network-based malware protection with cloud assist to provide organizations with an essential, primary layer of defense against millions of variants of malware.

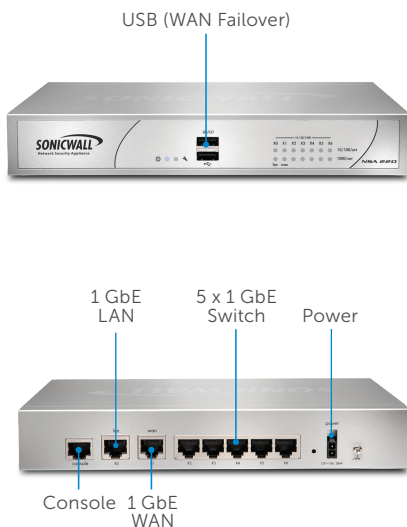
NSA Series firewalls are also easy to administer and cost-effective because they support Dell's award-winning Global Management System platform that is capable of managing hundreds or even thousands of Dell SonicWALL firewalls from a single pane-of-glass console. Comprehensive real-time visualization shows what is happening on the network with thorough, on-box and off-box reporting.

*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 (NGFWs) 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, content and URL inspection, application intelligence and control, high availability and other advanced networking features.

Network Security Appliance 220 and 220 Wireless-N

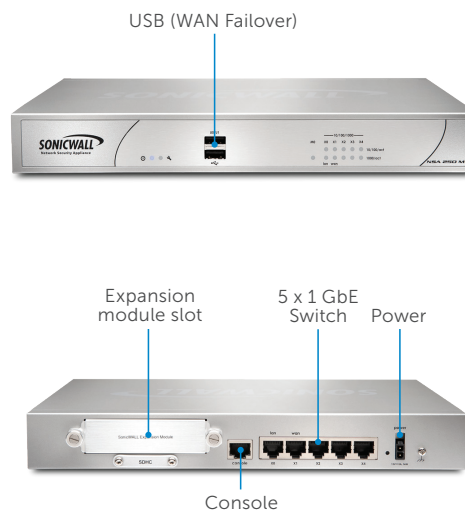


The Dell SonicWALL NSA 220 offers SMBs and branch offices in-depth frontline security, application and user control, network productivity and optional 802.11n dual-band wireless.

| Firewall | NSA 220 and 220 W |
|-------------------------|-------------------|
| Firewall throughput | 600 Mbps |
| IPS throughput | 195 Mbps |
| Anti-malware throughput | 115 Mbps |
| Full DPI throughput | 110 Mbps |
| IMIX throughput | 180 Mbps |
| Maximum DPI connections | 85,000 |
| New connections/sec | 32,000/sec |

| Description | NSA 220 and 220 W |
|---|-------------------|
| NSA 220 firewall only | 01-SSC-9750 |
| NSA 220 Wireless-N firewall only | 01-SSC-9752 |
| NSA 220 TotalSecure (1-year) | 01-SSC-9744 |
| NSA 220 Wireless-N TotalSecure (1-year) | 01-SSC-9745 |
| Comprehensive Gateway Security Suite (1-year) | 01-SSC-4648 |
| Gateway Anti-Malware/IPS (1-year) | 01-SSC-4612 |
| Dynamic Support Support 24x7 (1-year) | 01-SSC-4630 |

Network Security Appliance 250M and 250M Wireless-N

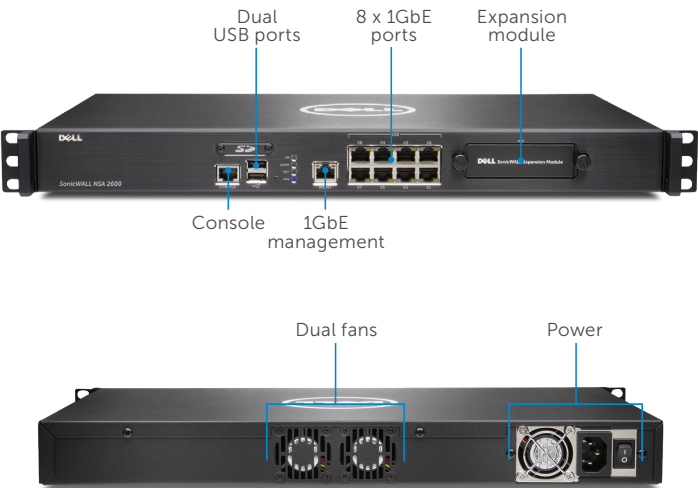


The Dell SonicWALL NSA 250M offers branch offices and distributed enterprises in-depth frontline security, application and user control, network productivity, an expansion slot for specialized modules and optional 802.11n dual-band wireless.

| Firewall | NSA 250M and 250M W |
|-------------------------|---------------------|
| Firewall throughput | 750 Mbps |
| IPS throughput | 250 Mbps |
| Anti-malware throughput | 140 Mbps |
| Full DPI throughput | 130 Mbps |
| IMIX throughput | 210 Mbps |
| Maximum DPI connections | 110,000 |
| New connections/sec | 64,000/sec |

| Description | NSA 250M and 250M W |
|---|---------------------|
| NSA 250M firewall only | 01-SSC-9755 |
| NSA 250M Wireless-N firewall only | 01-SSC-9757 |
| NSA 250M TotalSecure (1-year) | 01-SSC-9747 |
| NSA 250M Wireless-N TotalSecure (1-year) | 01-SSC-9748 |
| Comprehensive Gateway Security Suite (1-year) | 01-SSC-4606 |
| Gateway Anti-Malware/IPS (1-year) | 01-SSC-4570 |
| Dynamic Support Support 24x7 (1-year) | 01-SSC-4588 |

Network Security Appliance 2600

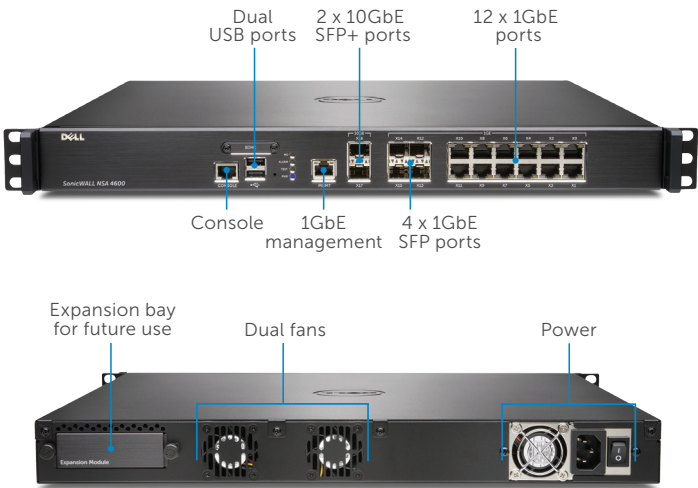


The Dell SonicWALL NSA 2600 is designed to address the needs of growing small organizations, branch offices and school campuses.

| 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 |
| Comprehensive Gateway Security Suite (1-year) | 01-SSC-4453 |
| Gateway Anti-Malware/IPS (1-year) | 01-SSC-4459 |
| Silver Support 24x7 (1-year) | 01-SSC-4314 |

Network Security Appliance 3600/4600



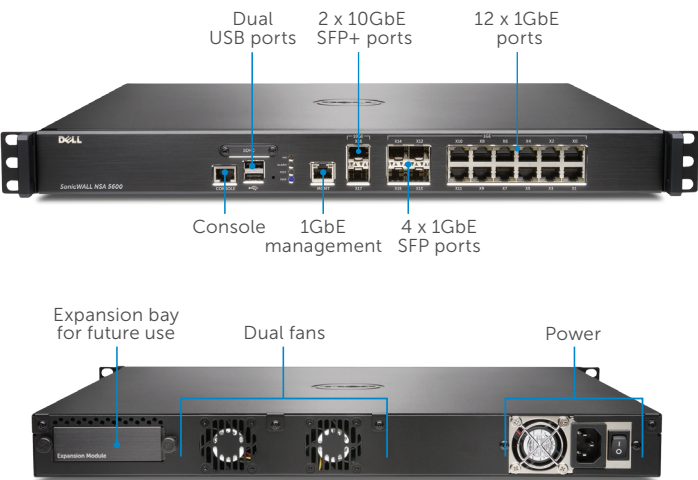
The Dell SonicWALL NSA 3600/4600 is ideal for branch office and small- to medium-sized corporate environments concerned about throughput capacity and performance.

| 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 | NSA 3600 | NSA 4600 |
|---|-------------|-------------|
| Firewall only | 01-SSC-3850 | 01-SSC-3840 |
| TotalSecure (1-year) | 01-SSC-3853 | 01-SSC-3843 |
| Comprehensive Gateway Security Suite (1-year) | 01-SSC-4429 | 01-SSC-4405 |
| Gateway Anti-Malware/IPS (1-year) | 01-SSC-4435 | 01-SSC-4411 |
| Silver Support 24x7 (1-year) | 01-SSC-4302 | 01-SSC-4290 |



Network Security Appliance 5600

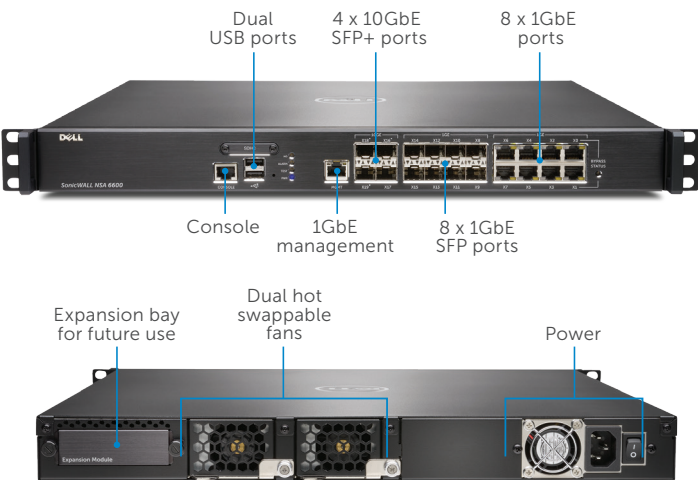


The Dell SonicWALL NSA 5600 is ideal for distributed, branch office and corporate environments needing significant throughput.

| 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 | 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



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 | 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 |
| 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 |



Achieve deeper network security

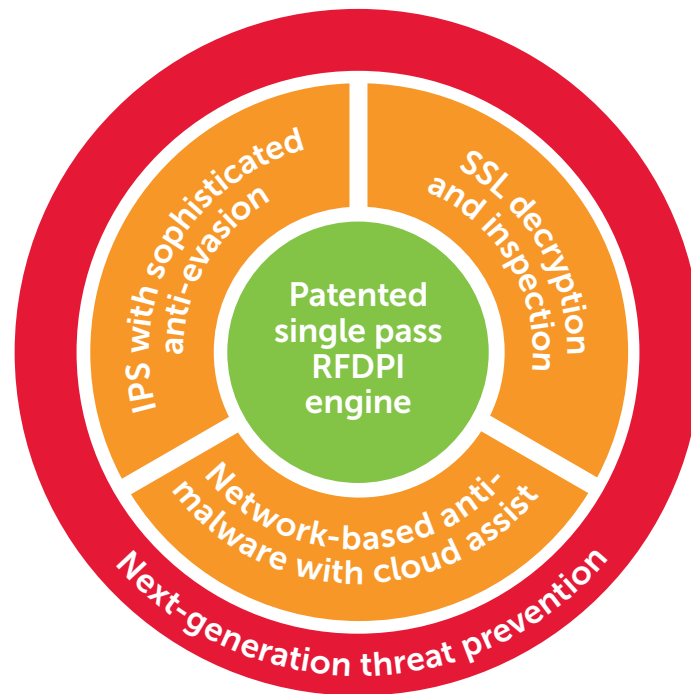
Dell SonicWALL NSA Series firewalls are capable of providing organizations of any size with a deeper level of network security because they are designed using a scalable, multi-core hardware architecture and a patented, single-pass, low-latency, Reassembly-Free Deep Packet Inspection® (RFDPI) engine that can scan every byte of every packet while maintaining high performance. The Dell SonicWALL NSA Series goes deeper than other firewalls with an RFDPI engine that combines real-time SSL decryption and inspection, an intrusion prevention system (IPS) that features sophisticated anti-evasion technology and a network-based malware protection system that leverages the power of the cloud. Now organizations can block daily new threats as they appear.

It is estimated that organizations are blind to approximately one third of their network traffic due to SSL encryption. SSL Decryption and Inspection technology available on the Dell SonicWALL NSA Series enables the RFDPI engine to decrypt and inspect all of network traffic on every port.

Every hour new variants of malware are developed. The Dell SonicWALL NSA Series keeps you abreast of these threats with network-based malware protection that leverages a cloud database which is updated continually and currently contains more than 13 million variants of malware.

The Dell SonicWALL Intrusion Prevention Service (IPS) protects against an array of network-based application vulnerabilities and exploits. New application vulnerabilities are discovered every day making ongoing IPS updates critical in keeping

protection up to date from emerging threats. Dell SonicWALL goes a step beyond traditional solutions with an intrusion prevention system that features sophisticated anti-evasion technology. It scans all network traffic for worms, Trojans, software vulnerabilities, backdoor exploits, and other types of malicious attacks. Cybercriminals often try to circumvent the IPS by using complex algorithms to evade detection. Dell NGFWs feature advanced threat protection to decode hidden attacks before they can harm your organization. By focusing on known malicious traffic, Dell SonicWALL IPS filters out false positives while increasing network reliability and performance. Designed to protect against both internal and external threats, Dell SonicWALL IPS monitors network traffic for malicious or anomalous behavior, then blocks or logs traffic based on predefined policy.



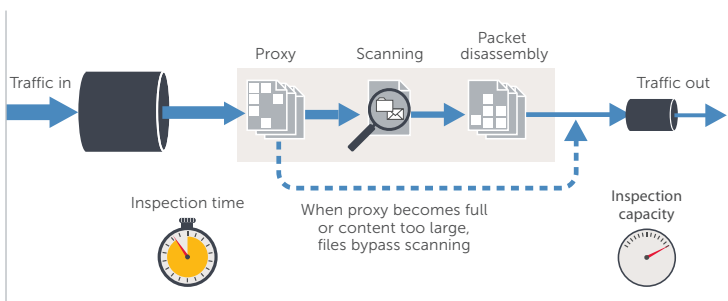
Reassembly-Free Deep Packet Inspection engine

The Dell SonicWALL Reassembly-Free Deep Packet Inspection (RFDPI) engine provides superior threat protection and application control without compromising performance. 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.

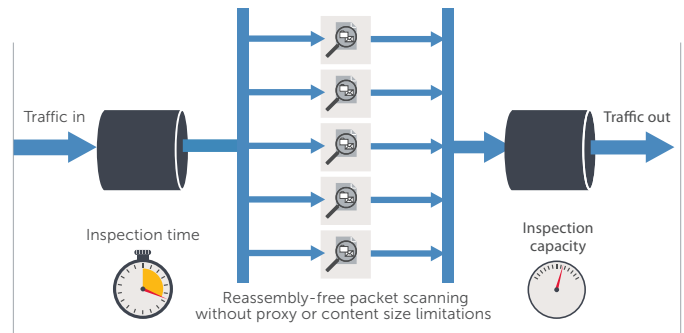
In most cases, the connection is terminated and proper logging and notification events are created. However, the engine can also be configured for inspection only or, in case of application detection, to provide Layer 7 bandwidth management services for the remainder of the application stream as soon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

Packet assembly-based process



Competitive architecture

Packet reassembly-free process

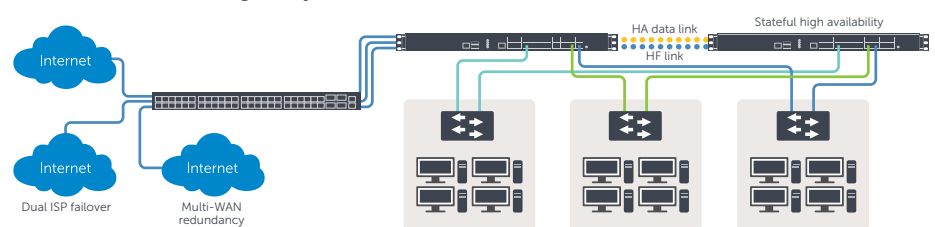


Dell SonicWALL architecture

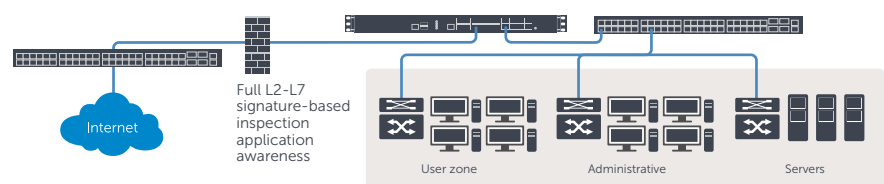
Flexible, customizable deployment options—NSA Series at-a-glance

Every Dell SonicWALL NSA appliance utilizes a breakthrough, multi-core hardware design and Reassembly-Free Deep Packet Inspection 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.

NSA Series as central-site gateway



NSA Series as in-line NGFW solution



Security and protection

The dedicated, in-house Dell SonicWALL Threat Research Team works on researching and developing countermeasures 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 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 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 NGFWs are able to block traffic from dangerous domains or entire geographies in order to reduce the risk profile of the network.

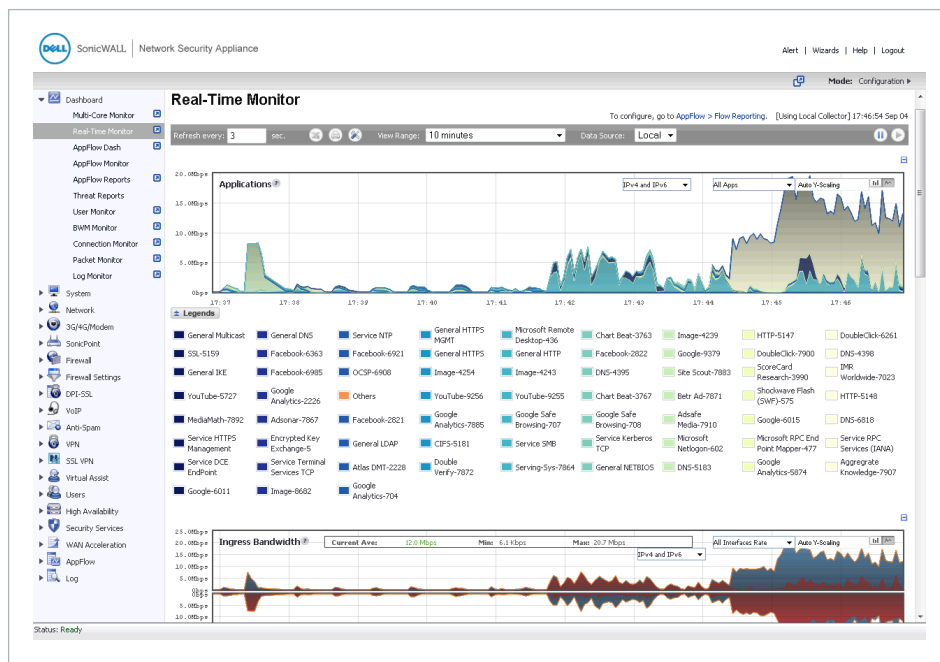


Application intelligence and control

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.

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 the 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.



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 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. |

Features

Threat prevention

| Feature | Description |
|-----------------------------------|---|
| Network-based malware protection | 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. |
| CloudAssist malware protection | 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 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. |

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, user groups, exclusion lists and a range of actions with full SSO user identification through LDAP/AD/Terminal Services/Citrix integration. |

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 | The 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. |



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 iOS and 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
- Centralized policy management
- Single Sign-On (SSO)
- Terminal service/Citrix support
- Solera Networks Forensics integration

NSA Series system specifications

| | NSA 220/W | NSA 250M/W |
|---|---|------------------------------------|
| Operating system | SonicOS 5.9 | |
| Security cores | 2 | |
| 1 GbE interfaces | 7 x 1GbE | 5 x 1GbE |
| Management interfaces | CLI, SSH, GUI, GMS | |
| Memory (RAM) | 512 MB | 512 MB |
| Expansion | 2 USB, SD Card | 1 Module Interface, 2 USB, SD Card |
| Firewall inspection throughput ¹ | 600 Mbps | 750 Mbps |
| Full DPI throughput ² | 110 Mbps | 130 Mbps |
| Application inspection throughput ² | 195 Mbps | 250 Mbps |
| IPS throughput ² | 195 Mbps | 250 Mbps |
| Anti-malware inspection throughput ² | 115 Mbps | 140 Mbps |
| IMIX throughput ³ | 180 Mbps | 210 Mbps |
| VPN throughput ³ | 150 Mbps | 200 Mbps |
| Connections per second | 2,200/sec | 3,000/sec |
| Maximum connections (SPI) | 85,000 | 110,000 |
| Maximum connections (DPI) | 32,000 | 64,000 |
| SonicPoints supported (Maximum) | 16 | 16 |
| Single Sign On (SSO) Users | 250 | 250 ⁴ |
| VPN | NSA 220/W | NSA 250M/W |
| Site-to-site tunnels | 25 | 50 |
| IPSec VPN clients (Maximum) | 2 (25) | 2 (25) |
| SSL VPN licenses (Maximum) | 2 (15) | 2 (15) |
| 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 | NSA 220/W | NSA 250M/W |
| IP 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 | 25 | 35 |
| 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) | Supported | |
| Wireless | NSA 220/W | NSA 250M/W |
| Standards | 802.11a/b/g/n (WEP, WPA, WPA2, 802.11i, TKIP, PSK, 02.1x, EAP-PEAP, EAP-TTLS | |
| Virtual access points (VAPs)5– antennas (5 dBi Diversity) | External triple, detachable | |
| Radio power–802.11a/802.11b/802.11g | 15.5 dBm max/18 dBm max/17 dBm @ 6 Mbps, 13 dBm @ 54 Mbps | |
| Radio power–802.11n (2.4GHz)/802.11n (5.0GHz) | 19 dBm MCS 0, 11 dBm MCS 15/17 dBm MCS 0, 12 dBm MCS 15 | |
| Radio receive sensitivity–802.11a/802.11b/802.11g | -95 dBm MCS 0, -81 dBm MCS 15/-90 dBm @ 11Mbps/-91 dBm @ 6Mbps, -74 dBm @ 54 Mbps | |
| Radio receive sensitivity– 802.11n (2.4GHz)/802.11n (5.0GHz) | -89 dBm MCS 0, -70 dBm MCS 15/-95 dBm MCS 0, -76 dBm MCS 15 | |
| Hardware | NSA 220/W | NSA 250M/W |
| Power supply | 36W external | |
| Fans | No fan/1 internal fan | 2 internal fans |
| Input power | 100-240 VAC, 60-50 Hz | |
| Maximum power consumption (W) | 11W/15W | 12W/16W |
| Form factor | Desktop / 1U Rack Mountable Kit Available | |
| Dimensions | 7.125 x 1.5 x 10.5 in 18.10 x 3.81 x 26.67 cm | |
| Weight | 1.95 lbs/0.88 kg/2.15 lbs/0.97 kg | 3.05 lbs/1.38 kg/3.15 lbs/1.43 kg |
| WEEE weight | 3.05 lbs/1.38 kg/3.45 lbs/1.56 kg | 4.4 lbs/2.0kg/4.65 lbs/2.11 kg |
| Shipping weight | 4.35lb/4.7lb | 5.6 lb/5.9 lb |
| 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, GOST-R (NSA 220), CU (NSA 250M) | |
| Environment | 40-105° F, 0-40° C | |
| Humidity | 5-95% 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. ⁴ Please refer to the latest SonicOS 5.9 release for the latest number of SSO users. *Future use.



NSA Series system specifications

| | NSA 2600 | NSA 3600 | NSA 4600 | NSA 5600 | NSA 6600 |
|--|---|---|-------------|---------------|--|
| Operating system | SonicOS 6.1 | | | | |
| Security cores | 4 | 6 | 8 | 10 | 24 |
| 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 | 750,000 | 750,000 |
| Maximum connections (DPI) | 125,000 | 175,000 | 200,000 | 500,000 | 500,000 |
| SonicPoints supported (Maximum) | 32 | 48 | 64 | 96 | 96 |
| Single Sign On (SSO) Users | 250 | 500 | 1,000 | 2,500 | 4,000 |
| VPN | NSA 2600 | NSA 3600 | NSA 4600 | NSA 5600 | NSA 6600 |
| Site-to-site tunnels | 75 | 800 | 1,500 | 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 (25) | 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 | 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 | 50 | 50 | 200 | 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 | | | | |
| 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 | 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.



NSA Series ordering information

| Product | SKU |
|--|-------------|
| NSA 220 TotalSecure (1-year) | 01-SSC-9744 |
| NSA 220 Wireless-N TotalSecure (1-year) | 01-SSC-9745 |
| NSA 250M TotalSecure (1-year) | 01-SSC-9747 |
| NSA 250M Wireless-N TotalSecure (1-year) | 01-SSC-9748 |
| 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 220W and 220 Wireless-N support and security subscriptions | SKU |
| Comprehensive Gateway Security Suite—Application Intelligence, Threat Prevention, Content Filtering with Support for NSA 220 (1-year) | 01-SSC-4648 |
| Threat Prevention—Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSA 220 (1-year) | 01-SSC-4612 |
| Dynamic Support for NSA 220 (1-year) | 01-SSC-4630 |
| Content Filtering Premium Business Edition for NSA 220 (1-year) | 01-SSC-4618 |
| Comprehensive Anti-Spam Service for NSA 220 (1-year) | 01-SSC-4642 |
| NSA 250M and 250M Wireless-N support and security subscriptions | SKU |
| Comprehensive Gateway Security Suite—Application Intelligence, Threat Prevention, Content Filtering with Support for NSA 250M (1-year) | 01-SSC-4606 |
| Threat Prevention—Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSA 250M (1-year) | 01-SSC-4570 |
| Dynamic Support for NSA 250M (1-year) | 01-SSC-4588 |
| Content Filtering Premium Business Edition for NSA 250M (1-year) | 01-SSC-4576 |
| Comprehensive Anti-Spam Service for NSA 250M (1-year) | 01-SSC-4600 |
| NSA 2600 support and security subscriptions | SKU |
| Comprehensive Gateway Security Suite—Application Intelligence, Threat Prevention, Content Filtering with Support for NSA 2600 (1-year) | 01-SSC-4453 |
| 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 |
| Comprehensive Anti-Spam Service for NSA 2600 (1-year) | 01-SSC-4471 |
| NSA 3600 support and security subscriptions | SKU |
| Comprehensive Gateway Security Suite—Application Intelligence, Threat Prevention, Content Filtering with Support for NSA 3600 (1-year) | 01-SSC-4429 |
| 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 |
| 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 NSA 4600 (1-year) | 01-SSC-4405 |
| 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 |
| Comprehensive Anti-Spam Service for NSA 4600 (1-year) | 01-SSC-4423 |



NSA Series ordering information

| NSA 5600 support and security subscriptions | SKU |
|---|-------------|
| Comprehensive Gateway Security Suite—Application Intelligence, Threat Prevention, Content Filtering with Support for NSA 5600 (1-year) | 01-SSC-4234 |
| 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 |
| 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 NSA 6600 (1-year) | 01-SSC-4210 |
| 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 |
| 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 |
| NSA 220/250M Rack-mount kit | SKU |
| NSA 220 Rack Mount Kit | 01-SSC-9212 |
| NSA 250M Rack Mount Kit | 01-SSC-9211 |
| NSA 250M expansion modules | SKU |
| 4-Port GbE Expansion Module for NSA 250M series | 01-SSC-8619 |
| 2 Port SFP Module | 01-SSC-8826 |
| 1-Port T1/E1 Module M1 | 01-SSC-8829 |
| 1-port ADSL Annex A Module M1 | 01-SSC-8827 |
| 1-port ADSL Annex B Module M1 | 01-SSC-8828 |
| 2-port GbE with LAN Bypass Module M1 | 01-SSC-8830 |
| 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 Security Products SE for a complete list of supported SFP and SFP+ modules

Regulatory model numbers:

| | |
|----------------------|--------------------|
| NSA 220—APL24-08E | NSA 2600—1RK29-0A9 |
| NSA 220 W—APL24-08F | NSA 3600—1RK26-0A2 |
| NSA 250M—APL25-090 | NSA 4600—1RK26-0A3 |
| NSA 250M W—APL25-091 | NSA 5600—1RK26-0A4 |
| | NSA 6600—1RK27-0A5 |

For more information

Dell SonicWALL
2001 Logic Drive
San Jose, CA 95124
www.sonicwall.com
T +1 408.745.9600
F +1 408.745.9300

Dell Software

5 Polaris Way, Aliso Viejo, CA 92656 | www.dell.com
If you are located outside North America, you can find local office information on our Web site.

© 2013 Dell, Inc. ALL RIGHTS RESERVED. Dell, Dell Software, the Dell Software logo and products—as identified in this document—are registered trademarks of Dell, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

