SONICWALL

SonicWall Network Security appliance (NSa) series

Industry-validated security effectiveness and performance for mid-sized networks, distributed enterprises and data centers

The SonicWall Network Security appliance (NSa) series provides organizations that range in scale from mid-sized networks to distributed enterprises and data centers with advanced threat prevention in a high-performance security platform. Utilizing innovative deep learning technologies in the SonicWall Capture Cloud Platform, the NSa series delivers the automated real-time breach detection and prevention organizations need.

Cutting-edge threat prevention with superior performance

Today's network threats are highly evasive and increasingly difficult to identify using traditional methods of detection. Staying ahead of sophisticated attacks requires a more modern approach that heavily leverages security intelligence in the cloud. Without that cloud intelligence, gateway security solutions can't keep pace with today's complex threats. NSa series next-generation firewalls (NGFWs) integrate two advanced security technologies to deliver cutting-edge threat prevention that keeps your network one step ahead. Enhancing SonicWall's multi-engine Capture Advanced Threat Protection (ATP) service is our patent-pending Real-Time Deep Memory Inspection (RTDMI™) technology. The RTDMI engine proactively detects and blocks mass market, zero-day threats and unknown malware by inspecting directly in memory. Because of the real-time architecture, SonicWall RTDMI technology is precise, minimizes false positives, and identifies and mitigates sophisticated attacks where the malware's weaponry is exposed for less than 100 nanoseconds. In combination, SonicWall's patented* single-pass Reassembly-Free Deep Packet Inspection (RFDPI) engine examines every byte of every packet, inspecting both inbound and outbound traffic on the firewall. By leveraging the SonicWall Capture Cloud Platform in addition to on-box capabilities including intrusion prevention, anti-malware and web/URL filtering, the NSa series blocks even the most insidious threats at the gateway.

Further, SonicWall firewalls provide complete protection by performing full decryption and inspection of TLS/SSL and SSH encrypted connections regardless of port or protocol. The firewall looks deep inside every packet (the header and data) searching for protocol non-compliance, threats, zero-days, intrusions, and even defined criteria. The deep packet inspection engine detects and prevents hidden attacks that leverage cryptography, blocks encrypted malware downloads, ceases the spread of infections, and thwarts command and control (C&C) communications and data exfiltration. Inclusion and exclusion rules allow total control to customize which traffic is subjected to decryption and inspection based on specific organizational compliance and/or legal requirements.

When organizations activate deep packet inspection functions such as IPS, anti-virus, anti-spyware, TLS/SSL decryption/inspection and others on their firewalls,

Benefits:

- Superior threat prevention and performance
- Patent-pending real-time deep memory inspection technology
- Patented reassembly-free deep packet inspection technology
- On-box and cloud-based threat prevention
- TLS/SSL decryption and inspection
- Industry-validated security effectiveness
- Multi-core hardware architecture
- Dedicated Capture Labs threat research team

Network control and flexibility

- Secure SD-WAN
- Powerful SonicOS operating system
- Application intelligence and control
- Network segmentation with VLANs
- High-speed wireless security

Easy deployment, setup and ongoing management

- Zero-Touch Deployment
- Cloud-based and on-premises centralized management
- Scalable line of firewalls
- Low total cost of ownership

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

network performance often slows down, sometimes dramatically. NSa series firewalls, however, feature a multi-core hardware architecture that utilizes specialized security microprocessors. Combined with our RTDMI and RFDPI engines, this unique design eliminates the performance degradation networks experience with other 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 distributed organizations requiring advanced flexibility in their network design, the SD-WAN technology in SonicOS is a perfect complement to NSa firewalls deployed at the headquarters or at remote and branch sites. Instead of relying on more expensive legacy technologies such as MPLS and T1, organizations using SD-WAN can choose lower-cost public Internet services while continuing to achieve a high level of application availability and predictable performance.

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 SonicWave 802.11ac Wave 2 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.

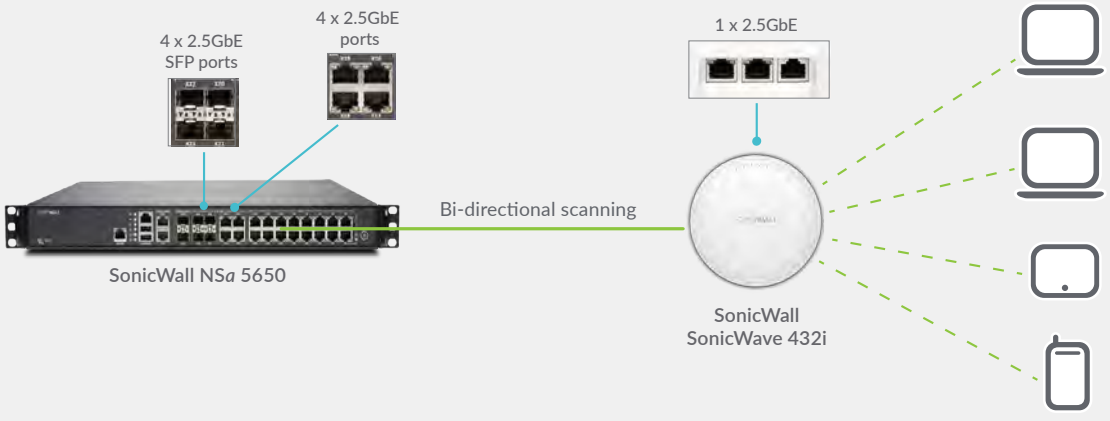
Easy deployment, setup and ongoing management

Like all SonicWall firewalls, the NSa series tightly integrates key security, connectivity and flexibility technologies into a single, comprehensive solution. This includes SonicWave wireless access points and the SonicWall WAN Acceleration (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.

Cloud-based centralized management, reporting, licensing and analytics are handled through the SonicWall Capture Security Center. A key component of the Capture Security Center is Zero-Touch Deployment. This cloud-based feature simplifies and speeds the deployment and provisioning of SonicWall firewalls at remote and branch office locations. 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.

Secure, High-speed Wireless

Combine an NSa series next-generation firewall with a SonicWall SonicWave 802.11ac Wave 2 wireless access point to create a high-speed wireless network security solution. NSa series firewalls and SonicWave access points both feature 2.5 GbE ports that enable multi-gigabit wireless throughput offered in Wave 2 wireless technology. The firewall scans all wireless traffic coming into and going out of the network using deep packet inspection technology and then removes harmful threats such as malware and intrusions, even over encrypted connections. Additional security and control capabilities such as content filtering, application control and intelligence and Capture Advanced Threat Protection can be run on the wireless network to provide added layers of protection.

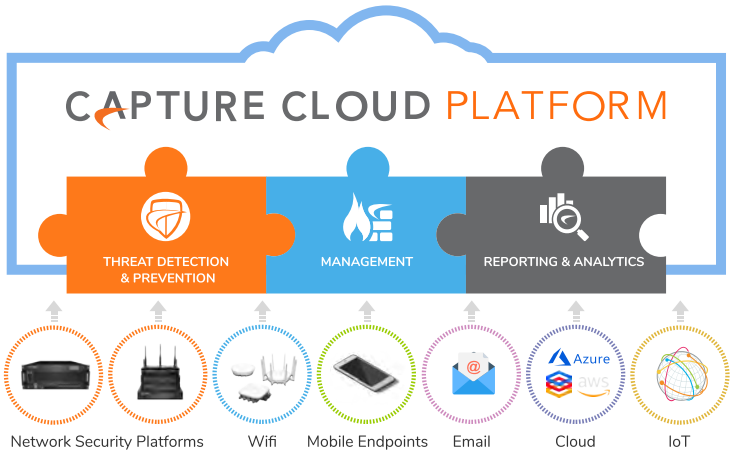


Capture Cloud Platform

SonicWall's Capture Cloud Platform delivers cloud-based threat prevention and network management plus reporting and analytics for organizations of any size. The platform consolidates threat intelligence gathered from multiple sources including our award-winning multi-engine network sandboxing service, Capture Advanced Threat Protection, as well as more than 1 million SonicWall sensors located around the globe.

If data coming into the network is found to contain previously-unseen malicious code, SonicWall's dedicated, in-house Capture Labs threat research team develops signatures that are stored in the Capture Cloud Platform database and deployed to customer firewalls for up-to-date protection. New updates take effect immediately without reboots or interruptions. The signatures resident on the appliance protect against wide classes of attacks, covering tens of thousands of individual threats. In addition to the countermeasures on the appliance, NSa firewalls also have continuous access to the Capture Cloud Platform database which extends the onboard signature intelligence with tens of millions of signatures.

In addition to providing threat prevention, the Capture Cloud Platform offers single pane of glass management and administrators can easily create both real-time and historical reports on network activity.



Advanced threat protection

At the center of SonicWall's automated, real-time breach prevention are two advanced malware detection technologies; Capture Advanced Threat Protection™ (Capture ATP) and Capture Security appliance™ (CSa).

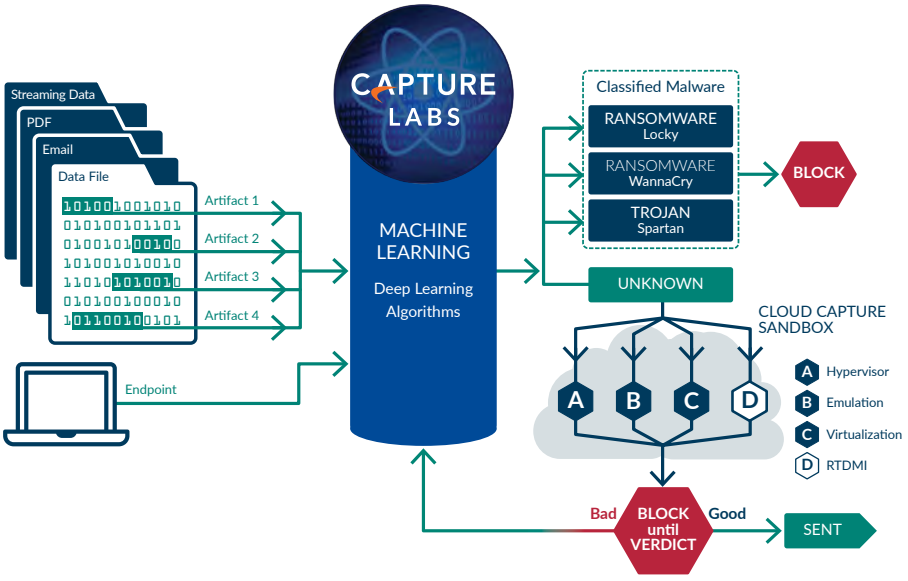
Capture ATP is a cloud-based multi-engine sandbox platform, which includes Real-Time Deep Memory Inspection™ (RTDMI), virtualized sandboxing, full system emulation and hypervisor level analysis technology. CSa is an on-premises device that features RTDMI, which utilizes memory-based static and dynamic techniques for fast and accurate verdicts. Both solutions extend advanced threat protection to detect and prevent zero-day threats in a variety of SonicWall solutions such as next-generation firewalls.

Suspicious files are sent to either solution where they are analyzed using deep learning algorithms with the option to hold them at the gateway until a verdict is determined.

In the case of Capture ATP, when files are identified as malicious, they are blocked, and a hash is immediately created within the Capture ATP database for all customers to leverage to block follow-on attacks. These signatures are eventually sent to firewalls to create static defenses. Results generated by CSa are not shared outside your organization for privacy and compliance reasons.

These services analyze a broad range of operating systems and file types, including executable programs, DLL, PDFs, MS Office documents, archives, JAR and APK.

For complete endpoint protection, the SonicWall Capture Client combines next-generation antivirus technology with SonicWall's cloud-based multi-engine sandbox with optional integration with SonicWall firewalls.



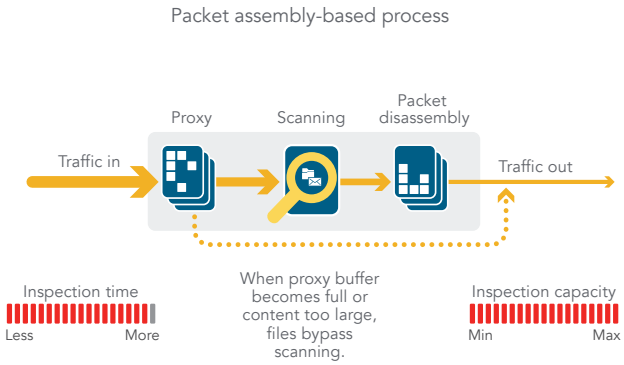
SONICWALL®

Reassembly-Free Deep Packet Inspection engine

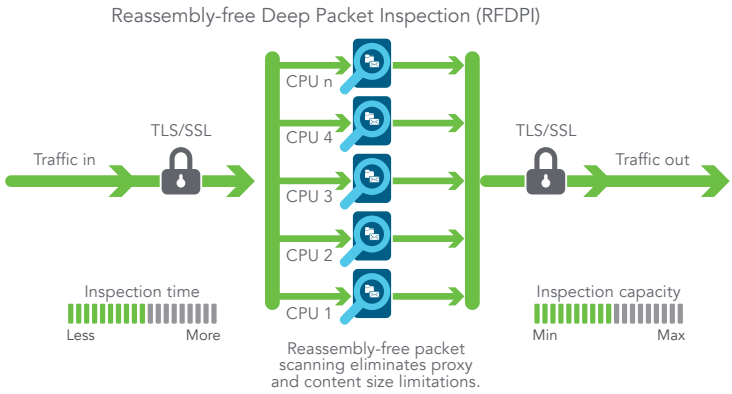
The SonicWall Reassembly-Free Deep Packet Inspection (RFDPI) is a single-pass, low latency inspection system that performs stream-based, bi-directional traffic analysis at high speed without proxying or buffering to effectively uncover intrusion attempts and malware downloads while identifying application traffic regardless of port and protocol. This proprietary engine 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 TLS/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 proxy-based architecture



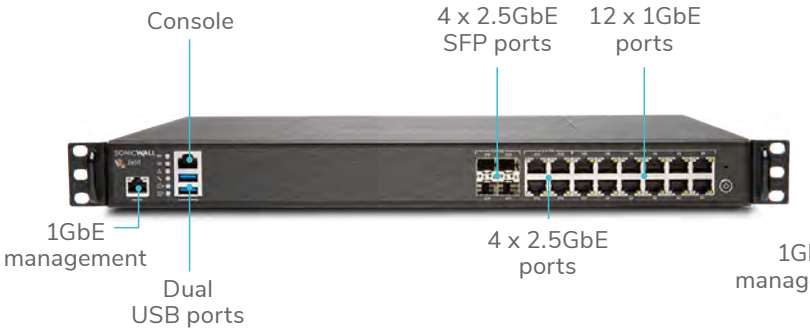
SonicWall stream-based architecture

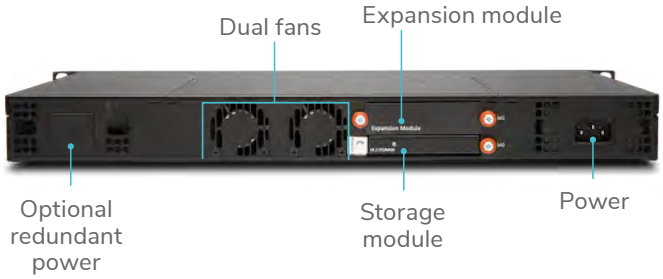
Centralized management and reporting

For highly regulated organizations wanting to achieve a fully coordinated security governance, compliance and risk management strategy, SonicWall provides administrators a unified, secure and extensible platform to manage SonicWall firewalls, wireless access points and Dell N-Series and X-Series switches through a correlated and auditable workstream process. Enterprises can easily consolidate the management of security appliances, reduce administrative and troubleshooting complexities, and govern all operational aspects of the security infrastructure, including centralized policy management and enforcement; real-time event monitoring; user activities; application identifications; flow analytics and forensics; compliance and audit reporting; and more. In addition, enterprises meet the firewall's change management requirements through workflow automation which provides the agility and confidence to deploy the right firewall policies at the right time and in conformance with compliance regulations. Available on premises as SonicWall Global Management System and in the cloud as Capture Security Center, SonicWall management and reporting solutions provide a coherent way to manage network security by business processes and service levels, dramatically simplifying lifecycle management of your overall security environments compared to managing on a device-by-device basis.

NSa 2650

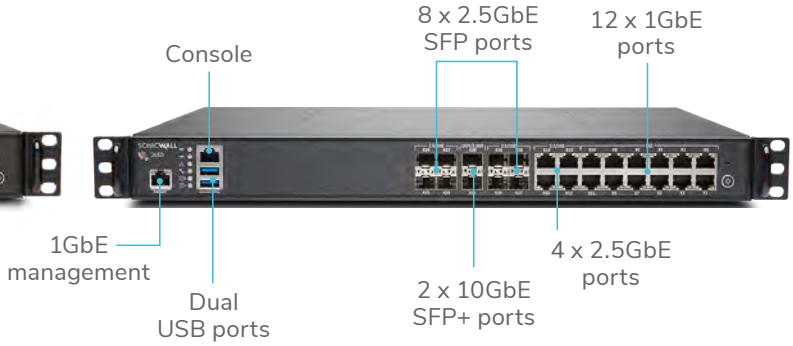
The NSa 2650 delivers high-speed threat prevention over thousands of encrypted and even more unencrypted connections to mid-sized organizations and distributed enterprises.

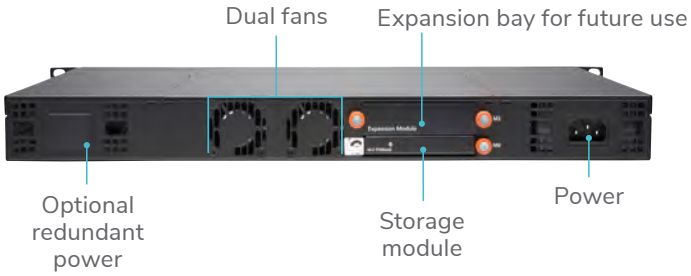




NSa 3650

The SonicWall NSa 3650 is ideal for branch office and small- to medium-sized corporate environments concerned about throughput capacity and performance.



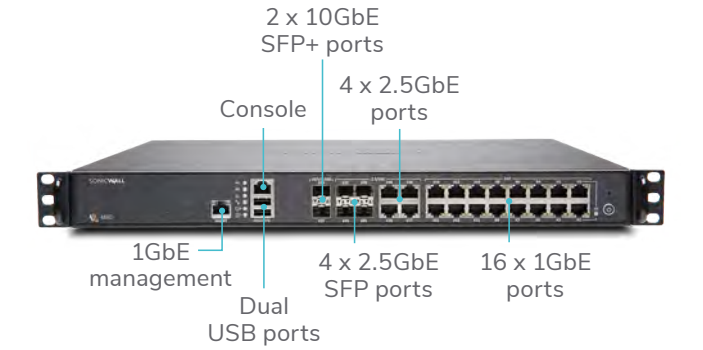


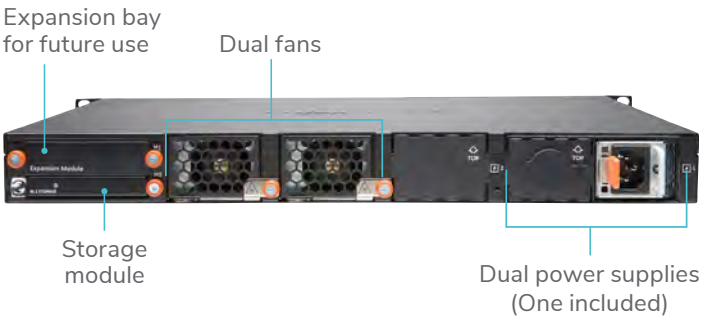
Firewall	NSa 2650
Firewall throughput	3.0 Gbps
IPS throughput	1.4 Gbps
Anti-malware throughput	1.3 Gbps
Threat Prevention throughput	1.5 Gbps
Maximum connections	1,000,000
New connections/sec	14,000/sec
Storage module	16 GB
Description	**SKU**
NSa 2650 firewall only	01-SSC-1936
NSa 2650 TotalSecure Advanced (1-year)	01-SSC-1988

Firewall	NSa 3650
Firewall throughput	3.75 Gbps
IPS throughput	1.8 Gbps
Anti-malware throughput	1.5 Gbps
Threat Prevention throughput	1.75 Gbps
Maximum connections	2,000,000
New connections/sec	14,000/sec
Storage module	32 GB
Description	**SKU**
NSa 3650 firewall only	01-SSC-1937
NSa 3650 TotalSecure Advanced (1-year)	01-SSC-4081

NSa 4650

The SonicWall NSa 4650 secures growing medium-sized organizations and branch office locations with enterprise-class features and uncompromising performance.



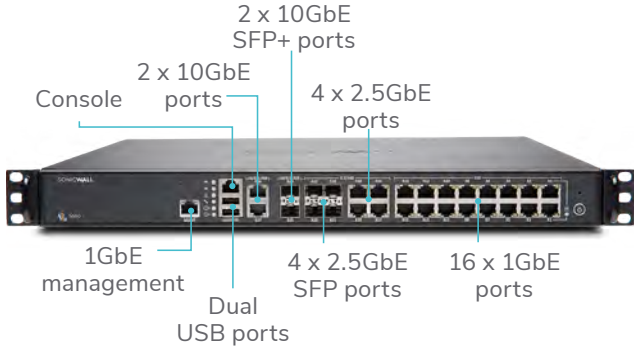


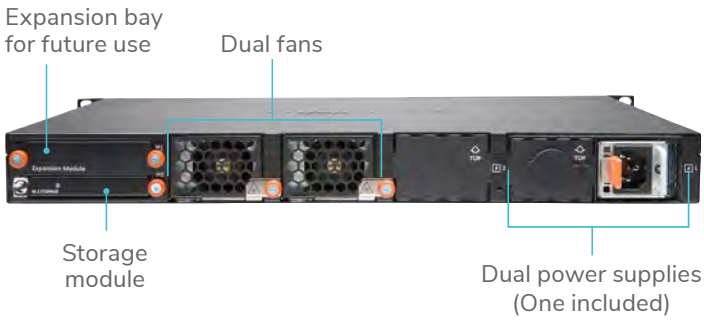
Firewall	NSa 4650
Firewall throughput	6.0 Gbps
IPS throughput	2.3 Gbps
Anti-malware throughput	2.45 Gbps
Threat Prevention throughput	2.5 Gbps
Maximum connections	3,000,000
New connections/sec	40,000/sec
Storage module	32 GB

Description	SKU
NSa 4650 firewall only	01-SSC-1938
NSa 4650 TotalSecure Advanced (1-year)	01-SSC-4094

NSa 5650

The SonicWall NSa 5650 is ideal for distributed, branch office and corporate environments needing significant throughput and high port density.



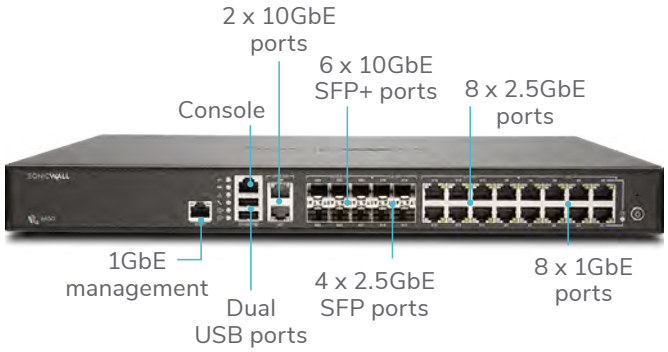


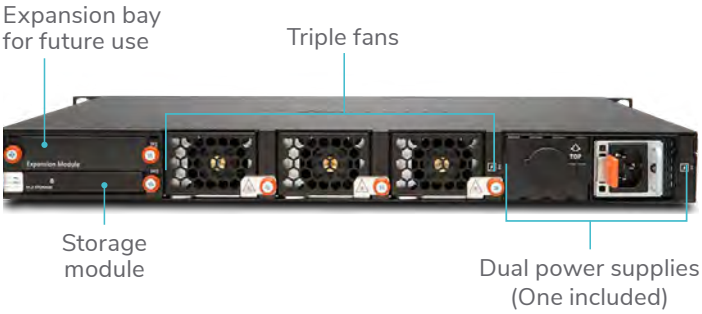
Firewall	NSa 5650
Firewall throughput	6.25 Gbps
IPS throughput	3.4 Gbps
Anti-malware throughput	2.8 Gbps
Threat Prevention throughput	3.4 Gbps
Maximum connections	4,000,000
New connections/sec	40,000/sec
Storage module	64 GB

Description	SKU
NSa 5650 firewall only	01-SSC-1939
NSa 5650 TotalSecure Advanced (1-year)	01-SSC-4342

NSa 6650

The SonicWall NSa 6650 is ideal for large distributed and corporate central site sites requiring high throughput capacity and performance.

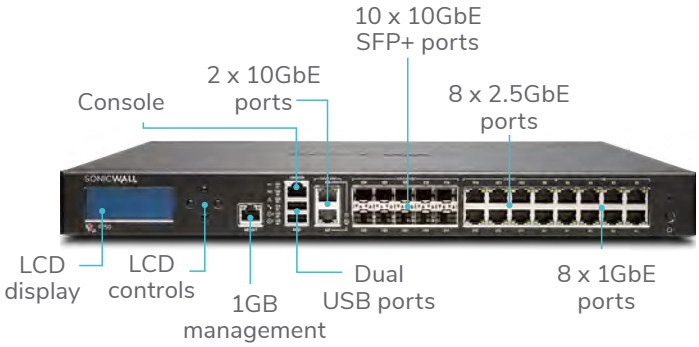




Firewall	NSa 6650
Firewall throughput	12.0 Gbps
IPS throughput	6.0 Gbps
Anti-malware throughput	5.4 Gbps
Threat Prevention throughput	5.5 Gbps
Maximum connections	5,000,000
New connections/sec	90,000/sec
Storage module	64 GB
Description	**SKU**
NSa 6650 firewall only	01-SSC-1940
NSa 6650 TotalSecure Advanced (1-year)	01-SSC-2209

NSa 9250/9450/9650

The SonicWall NSa 9250/9450/9650 provide distributed enterprises and data centers with scalable, deep security at multi-gigabit speeds.



Firewall	NSa 9250	NSa 9450	NSa 9650
Firewall throughput	12.0 Gbps	17.1 Gbps	17.1 Gbps
IPS throughput	7.2 Gbps	10.2 Gbps	10.3 Gbps
Anti-malware throughput	6.5 Gbps	8.0 Gbps	8.5 Gbps
Threat Prevention throughput	6.5 Gbps	9.0 Gbps	9.4 Gbps
Maximum connections	7,500,000	10,000,000	12,500,000
New connections/sec	90,000/sec	130,000/sec	130,000/sec
Storage modules	1 TB, 128 GB	1 TB, 128 GB	1 TB, 256 GB
Description	**SKU**	**SKU**	**SKU**
NSa firewall only	01-SSC-1941	01-SSC-1942	01-SSC-1943
NSa TotalSecure Advanced (1-year)	01-SSC-2854	01-SSC-4358	01-SSC-3475

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.

Feature	Description
Secure SD-WAN	An alternative to more expensive technologies such as MPLS, Secure SD-WAN enables distributed enterprise organizations to build, operate and manage secure, high-performance networks across remote sites for the purpose of sharing data, applications and services using using readily-available, low-cost public internet services.
REST APIs	Allows the firewall to receive and leverage any and all proprietary, original equipment manufacturer and third-party intelligence feeds to combat advanced threats such as zero-day, malicious insider, compromised credentials, ransomware and advanced persistent threats.
Stateful packet inspection	All network traffic is inspected, analyzed and brought into compliance with firewall access policies.
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.
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.
IPv6 support	Internet Protocol version 6 (IPv6) is in its early stages to replace IPv4. With SonicOS, the hardware will support filtering and wire mode implementations.
Flexible deployment options	The NSa series can be deployed in traditional NAT, Layer 2 bridge, wire and network tap modes.
WAN load balancing	Load-balances multiple WAN interfaces using Round Robin, Spillover or Percentage methods.
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.
Single and cascaded Dell N-Series and X-Series switch management	Manage security settings of additional ports, including Portshield, HA, PoE and PoE+, under a single pane of glass using the firewall management dashboard for Dell's N-Series and X-Series network switch.
Biometric authentication	Supports mobile device authentication such as fingerprint recognition that cannot be easily duplicated or shared to securely authenticate the user identity for network access.
Open authentication and social login	Enable guest users to use their credentials from social networking services such as Facebook, Twitter, or Google+ to sign in and access the Internet and other guest services through a host's wireless, LAN or DMZ zones using pass-through authentication.

MANAGEMENT AND REPORTING

Feature	Description
Cloud-based and on-premises management	Configuration and management of SonicWall appliances is available via the cloud through the SonicWall Capture Security Center and on-premises using SonicWall Global Management System (GMS).
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.
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 SonicWall Scrutinizer or other tools that support IPFIX and NetFlow with extensions.

VIRTUAL PRIVATE NETWORKING (VPN)

Feature	Description
Auto-provision VPN	Simplifies and reduces complex distributed firewall deployment down to a trivial effort by automating the initial site-to-site VPN gateway provisioning between SonicWall firewalls while security and connectivity occurs instantly and automatically.
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/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. Ability to create custom country and Botnet lists to override an incorrect country or Botnet tag associated with an IP address. Eliminates unwanted filtering of IP addresses due to misclassification.
Regular expression DPI filtering	Prevents data leakage by identifying and controlling content crossing the network through regular expression matching. Provides the ability to create custom country and Botnet lists to override an incorrect country or Botnet tag associated with an IP address.

Breach prevention subscription services

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 to malicious activity.
Real-Time Deep Memory Inspection (RTDMI)	This patent-pending cloud-based technology detects and blocks malware that does not exhibit any malicious behavior and hides its weaponry via encryption. By forcing malware to reveal its weaponry into memory, the RTDMI engine proactively detects and blocks mass-market, zero-day threats and unknown malware.
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.
Broad file type and size analysis	Supports analysis of a broad range of file types, either individually or as a group, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including 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 SonicWall Capture ATP subscriptions and Gateway Anti-Virus and IPS signature databases and the URL, IP and domain reputation databases within 48 hours.
Capture Client	Capture Client is a unified client platform that delivers multiple endpoint protection capabilities, including advanced malware protection and support for visibility into encrypted traffic. It leverages layered protection technologies, comprehensive reporting and endpoint protection enforcement.

CAPTURE SECURITY APPLIANCE (CSa)

Feature	Description
Compliance-centered malware detection	Analyze suspicious files in your own environment without sending files or results to a third-party cloud.
Built-in integrations	CSa supports out of the box integrations with other security solutions (firewalls and email security) from SonicWall.
Near real-time protection	SonicWall's patented RTDMI technology helps detect malware quickly, even for previously unknown malware, that CSa can enable the block until verdict capability on SonicWall next-generation firewalls.
Deployment	CSa can be configured on a private network directly connected to a singular edge firewall or be reachable over the Internet directly or using VPN by branch firewalls.

ENCRYPTED THREAT PREVENTION

Feature	Description
TLS/SSL decryption and inspection	Decrypts and inspects TLS/SSL encrypted 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 encrypted traffic. Included with security subscriptions for all NSa series models.
SSH inspection	Deep packet inspection of SSH (DPI-SSH) decrypts and inspect data traversing over SSH tunnel to prevent attacks that leverage SSH.

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 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	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.

THREAT PREVENTION

Feature	Description
Gateway anti-malware	The 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.
Capture Cloud malware protection	A continuously updated database of tens of millions of 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.
Around-the-clock security updates	New threat updates are automatically pushed to firewalls in the field with active security services, and take effect immediately without reboots or interruptions.
Bi-directional raw TCP inspection	The RFDPI engine is capable of scanning raw TCP streams on any port bi-directionally preventing attacks that they 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	Control applications, or individual application features, that are identified by the RFDPI engine against a continuously expanding database of over thousands of application signatures, to increase network security and enhance network productivity.
Custom application identification	Control 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 allocate and regulate available bandwidth for critical applications or application categories while inhibiting nonessential application traffic.
Granular control	Control 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	Enforce acceptable use policies and block access to HTTP/HTTPS websites containing information or images that are objectionable or unproductive with Content Filtering Service and Content Filtering Client.
Enforced Content Filtering Client	Extend policy enforcement to block internet content for Windows, Mac OS, Android and Chrome devices located outside the firewall perimeter.
Granular controls	Block 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.
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.

ENFORCED ANTIVIRUS AND ANTI-SPYWARE

Feature	Description
Multi-layered protection	Utilize the firewall capabilities as the first layer of defense at the perimeter, coupled with endpoint protection to block, viruses entering network through laptops, thumb drives and other unprotected systems.
Automated enforcement option	Ensure every computer accessing the network has the appropriate antivirus software and/or DPI-SSL certificate installed and active, eliminating the costs commonly associated with desktop antivirus management.
Automated deployment and installation option	Machine-by-machine deployment and installation of antivirus and anti-spyware clients is automatic across the network, minimizing administrative overhead.
Next-generation antivirus	Capture Client uses a static artificial intelligence (AI) engine to determine threats before they can execute and roll back to a previous uninfected state.
Spyware protection	Powerful spyware protection scans and blocks the installation of a comprehensive array of spyware programs on desktops and laptops before they transmit confidential data, providing greater desktop security and performance.

SonicOS feature summary

Firewall

- Stateful packet inspection
- Reassembly-Free Deep Packet Inspection
- DDoS attack protection (UDP/ICMP/ SYN flood)
- IPv4/IPv6
- Biometric authentication for remote access
- DNS proxy
- REST APIs

TLS/SSL/SSH decryption and inspection[1]

- Deep packet inspection for TLS/SSL/SSH
- Inclusion/exclusion of objects, groups or hostnames
- TLS/SSL control
- Granular DPI SSL controls per zone or rule

Capture advanced threat protection[1]

- Real-Time Deep Memory Inspection
- 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
- Block until verdict
- Capture Client

Intrusion prevention[1]

- Signature-based scanning
- Automatic signature updates
- Bi-directional inspection
- Granular IPS rule capability
- GeoIP enforcement
- Botnet filtering with dynamic list
- Regular expression matching

Anti-malware[1]

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

Application identification[1]

- Application control
- Application bandwidth management
- Custom application signature creation
- Data leakage prevention
- Application reporting over NetFlow/IPFIX
- Comprehensive application signature database

Traffic visualization and analytics

- User activity
- Application/bandwidth/threat usage
- Cloud-based analytics

HTTP/HTTPS Web content filtering[1]

- URL filtering
- Proxy avoidance
- Keyword blocking
- Policy-based filtering (exclusion/inclusion)
- HTTP header insertion
- Bandwidth manage CFS rating categories
- Unified policy model with app control
- Content Filtering Client

VPN

- Auto-provision 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, BGP)

Networking

- Secure SD-WAN
- PortShield
- Jumbo frames
- Enhanced logging
- VLAN trunking
- RSTP (Rapid Spanning Tree Protocol)
- Port mirroring
- Layer-2 QoS
- Port security
- Dynamic routing (RIP/OSPF/BGP)
- SonicWall wireless controller
- Policy-based routing (ToS/metric and ECMP)
- NAT
- DNS security
- DHCP server
- Bandwidth management
- Link aggregation (static and dynamic)
- Port redundancy
- A/P high availability with state sync
- A/A clustering
- Inbound/outbound load balancing
- L2 bridge, wire/virtual wire mode, tap mode
- 3G/4G WAN failover
- Asymmetric routing
- Common Access Card (CAC) support

Wireless

- WIDS/WIPS
- RF spectrum analysis
- Rogue AP prevention
- Fast roaming (802.11k/r/v)
- Auto-channel selection
- Floor plan view/Topology view
- Band steering
- Beamforming
- AirTime fairness
- MiFi extender
- Guest cyclic quota
- LHM guest portal

VoIP

- Granular QoS control
- Bandwidth management
- SIP and H.323 transformations per access rule
- H.323 gatekeeper and SIP proxy support

Management and monitoring

- Capture Security Center, GMS, Web UI, CLI, REST APIs, SNMPv2/v3
- Logging
- Netflow/IPFix exporting
- Cloud-based configuration backup
- BlueCoat Security Analytics Platform
- SonicWall access point management
- Dell N-Series and X-Series switch management including cascaded switches

Local storage

- Logs
- Reports
- Firmware backups

[1]*Requires added subscription*

SONICWALL®

NSa series system specifications

Firewall general	NSa 2650	NSa 3650	NSa 4650	NSa 5650
Operating system	SonicOS 6.5.4			
Interfaces	4 x 2.5-GbE SFP, 4 x 2.5-GbE, 12 x 1-GbE, 1 GbE Management, 1 Console	2 x 10-GbE SFP+, 8 x 2.5-GbE SFP, 4 x 2.5-GbE, 12 x 1-GbE, 1 GbE Management, 1 Console	2 x 10-GbE SFP+, 4 x 2.5-GbE SFP, 4 x 2.5-GbE, 16 x 1-GbE, 1 GbE Management, 1 Console	2 x 10-GbE SFP+, 2 x 10-GbE, 4 x 2.5-GbE SFP, 4 x 2.5-GbE, 16 x 1-GbE, 1 GbE Management, 1 Console
Expansion	1 Expansion Slot (Rear)*			
Built-in storage (SSD)	16 GB	32 GB	32 GB	64 GB
Management	CLI, SSH, Web UI, Capture Security Center, GMS, REST APIs			
SSO users	40,000	50,000	60,000	70,000
Maximum access points supported	48	96	128	192
Logging	Analyzer, Local Log, Syslog			
Firewall/VPN Performance	**NSa 2650**	**NSa 3650**	**NSa 4650**	**NSa 5650**
Firewall inspection throughput[1]	3.0 Gbps	3.75 Gbps	6.0 Gbps	6.25 Gbps
Threat Prevention throughput[2]	1.5 Gbps	1.75 Gbps	2.5 Gbps	3.4 Gbps
Application inspection throughput[2]	1.85 Gbps	2.1 Gbps	3.0 Gbps	4.25 Gbps
IPS throughput[2]	1.4 Gbps	1.8 Gbps	2.3 Gbps	3.4 Gbps
Anti-malware inspection throughput[2]	1.3 Gbps	1.5 Gbps	2.45 Gbps	2.8 Gbps
TLS/SSL decryption and inspection throughput (DPI SSL)[2]	300 Mbps	320 Mbps	675 Mbps	800 Mbps
VPN throughput[3]	1.45 Gbps	1.5 Gbps	3.0 Gbps	3.5 Gbps
Connections per second	14,000/sec	14,000/sec	40,000/sec	40,000/sec
Maximum connections (SPI)	1,000,000	2,000,000	3,000,000	4,000,000
Maximum connections (DPI)	500,000	750,000	1,000,000	1,500,000
Default/Maximum Connections (DPI SSL)	100,000/60,000	100,000/40,000	175,000/145,000	175,000/125,000
VPN	**NSa 2650**	**NSa 3650**	**NSa 4650**	**NSa 5650**
Site-to-site tunnels	1,000	3,000	4,000	6,000
IPSec VPN clients (max)	50 (1,000)	500 (3,000)	2,000 (4,000)	2,000 (6,000)
SSL VPN NetExtender clients (max)	2 (350)	2 (500)	2 (1,000)	2 (1,500)
Encryption/Authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B Cryptography			
Key exchange	Diffie Hellman Groups 1, 2, 5, 14v			
Route-based VPN	RIP, OSPF, BGP			
Networking	**NSa 2650**	**NSa 3650**	**NSa 4650**	**NSa 5650**
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	400	500
Routing protocols	BGP, OSPF, RIPv1/v2, static routes, policy-based routing			
QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p			
Authentication	LDAP (multiple domains), XAUTH/RADIUS, SSO, 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 (in progress)	ICSA Firewall, ICSA Anti-Virus, FIPS 140-2, Common Criteria NDPP (Firewall and IPS), UC APL, USGv6, CsFC			
High availability[5]	Active/Passive with State Sync	Active/Passive with State Sync Active/Active Clustering		Active/Passive with State Sync, Active/Active DPI with State Sync, Active/Active Clustering
Hardware	**NSa 2650**	**NSa 3650**	**NSa 4650**	**NSa 5650**
Power supply	Dual, redundant 120W (one included)		Dual, redundant 350W (one included)	
Fans	Dual, Fixed		Dual, Removable	
Input power	100-240 VAC, 50-60 Hz			
Maximum power consumption (W)	37.2	46	93.6	103.6
MTBF @25°C in hours	162,231	156,681	154,529	153,243
MTBF @25°C in years	18.5	17.9	17.6	17.5
Form factor	1U Rack Mountable			
Dimensions	16.9 x 12.8 x 1.8 in (43 x 32.5 x 4.5 cm)		16.9 x 16.3 x 1.8 in (43 x 41.5 x 4.5 cm)	
Weight	11.5 lb (5.2 kg)	11.7 lb (5.3 kg)	15.2 lb (6.9 kg)	15.2 lb (6.9 kg)
WEEE weight	12.1 lb (5.5 kg)	12.3 lb (5.6 kg)	19.6 lb (8.9 kg)	19.6 lb (8.9 kg)
Shipping weight	17.0 lb (7.7 kg)	17.2 lb (7.8 kg)	24.9 lb (11.3 kg)	24.9 lb (11.3 kg)
Major regulatory	FCC Class A, ICES Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, UL/cUL, TUV/GS, CB, Mexico CoC by UL, WEEE, REACH, BSMI, KCC/MSIP, ANATEL			
Environment (Operating/Storage)	32°-105° F (0°-40° C)/-40° to 158° F (-40° to 70° C)			
Humidity	10-90% non-condensing			

NSa series system specifications con't

Firewall general	NSa 6650	NSa 9250	NSa 9450	NSa 9650
Operating system	SonicOS 6.5.4			
Interfaces	6 x 10-GbE SFP+, 2 x 10-GbE, 4 x 2.5-GbE SFP, 8 x 2.5-GbE, 8 x 1-GbE, 1 GbE Management, 1 Console	10 x 10-GbE SFP+, 2 x 10-GbE, 8 x 2.5-GbE, 8 x 1-GbE, 1 GbE Management, 1 Console	10 x 10-GbE SFP+, 2 x 10-GbE, 8 x 2.5-GbE, 8 x 1-GbE, 1 GbE Management, 1 Console	10 x 10-GbE SFP+, 2 x 10-GbE, 8 x 2.5-GbE, 8 x 1-GbE, 1 GbE Management, 1 Console
Expansion	1 Expansion Slot (Rear)*			
Built-in storage (SSD)	64 GB	1TB, 128 GB	1TB, 128 GB	1TB, 256 GB
Management	CLI, SSH, Web UI, Capture Security Center, GMS, REST APIs	CLI, SSH, Web UI, GMS, REST APIs		
SSO users	70,000	80,000	90,000	100,000
Maximum access points supported	192	192	192	192
Logging	Analyzer, Local Log, Syslog, IPFIX, NetFlow			
Firewall/VPN Performance	**NSa 6650**	**NSa 9250**	**NSa 9450**	**NSa 9650**
Firewall inspection throughput[1]	12.0 Gbps	12.0 Gbps	17.1 Gbps	17.1 Gbps
Threat Prevention throughput[2]	5.5 Gbps	6.5 Gbps	9.0 Gbps	9.4 Gbps
Application inspection throughput[2]	6.0 Gbps	7.8 Gbps	10.8 Gbps	11.5 Gbps
IPS throughput[2]	6.0 Gbps	7.2 Gbps	10.2 Gbps	10.3 Gbps
Anti-malware inspection throughput[2]	5.4 Gbps	6.5 Gbps	8.0 Gbps	8.5 Gbps
TLS/SSL decryption and inspection throughput (DPI SSL)[2]	1.45 Gbps	1.5 Gbps	2.1 Gbps	2.25 Gbps
VPN throughput[3]	6.0 Gbps	6.75 Gbps	10.0 Gbps	10.0 Gbps
Connections per second	90,000/sec	90,000/sec	130,000/sec	130,000/sec
Maximum connections (SPI)	5,000,000	7,500,000	10,000,000	12,500,000
Maximum connections (DPI)	2,000,000	3,000,000	4,000,000	5,000,000
Default/Maximum Connections (DPI SSL)	250,000/170,000	250,000/170,000	450,000/290,000	550,000/320,000
VPN	**NSa 6650**	**NSa 9250**	**NSa 9450**	**NSa 9650**
Site-to-site tunnels	8,000	12,000	12,000	12,000
IPSec VPN clients (max)	2,000 (6,000)	2,000 (6,000)	2,000 (6,000)	2,000 (6,000)
SSL VPN NetExtender clients (max)	2 (2,000)	2 (3,000)	2 (3,000)	50 (3,000)
Encryption/Authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B Cryptography			
Key exchange	Diffie Hellman Groups 1, 2, 5, 14v			
Route-based VPN	RIP, OSPF, BGP			
Networking	**NSa 6650**	**NSa 9250**	**NSa 9450**	**NSa 9650**
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			
QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p			
Authentication	LDAP (multiple domains), XAUTH/RADIUS, SSO, 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 (in progress)	ICSA Firewall, ICSA Anti-Virus, FIPS 140-2, Common Criteria NDPP (Firewall and IPS), UC APL, USGv6, CsFC			
High availability[5]	Active/Passive with State Sync, Active/Active DPI with State Sync, Active/Active Clustering			
Hardware	**NSa 6650**	**NSa 9250**	**NSa 9450**	**NSa 9650**
Power supply	Dual, redundant 350W (one included)	Dual, redundant, 350W		
Fans	Triple, Removable			
Input power	100-240 VAC, 50-60 Hz			
Maximum power consumption (W)	144.3	86.7	90.9	113.1
MTBF @25°C in hours	157,193	139,783	134,900	116,477
MTBF @25°C in years	17.9	15.96	15.4	13.3
Form factor	1U Rack Mountable			
Dimensions	16.9 x 16.3 x 1.8 in (43 x 41.5 x 4.5 cm)			
Weight	17.9 lb (8.1 kg)	17.9 lb (8.1 kg)		
WEEE weight	22.5 lb (10.2 kg)	22.5 lb (10.2 kg)		
Shipping weight	27.8 lb (12.6 kg)	27.8 lb (12.6 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			
Environment (Operating/Storage)	32°-105° F (0°-40° C)/-40° to 158° F (-40° to 70° 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] Threat Prevention/Gateway AV/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. Threat Prevention throughput measured with Gateway AV, Anti-Spyware, IPS and Application Control enabled. DPI SSL performance measured on HTTPS traffic with IPS enabled.
[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] For every 125,000 DPI connections reduced, the number of available DPI SSL connections increases by 3,000 except for NSa 9250 and above.
[5] Active/Active Clustering and Active/Active DPI with State Sync require purchase of Expanded License except for NSa 9250 and above.
**Future use. All specifications, features and availability are subject to change.*

NSa series ordering information

NSa 2650	SKU
NSa 2650 TotalSecure Advanced Edition (1-year)	01-SSC-1988
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, and 24x7 Support for NSa 2650 (1-year)	01-SSC-1783
Capture Advanced Threat Protection for NSa 2650 (1-year)	01-SSC-1935
Threat Prevention–Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSa 2650 (1-year)	01-SSC-1976
24x7 Support for NSa 2650 (1-year)	01-SSC-1541
Content Filtering Service for NSa 2650 (1-year)	01-SSC-1970
Capture Client	Based on user count
Comprehensive Anti-Spam Service for NSa 2650 (1-year)	01-SSC-2001

NSa 3650	SKU
NSa 3650 TotalSecure Advanced Edition (1-year)	01-SSC-4081
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, and 24x7 Support for NSa 3650 (1-year)	01-SSC-3451
Capture Advanced Threat Protection for NSa 3650 (1-year)	01-SSC-3457
Threat Prevention–Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSa 3650 (1-year)	01-SSC-3632
24x7 Support for NSa 3650 (1-year)	01-SSC-3439
Content Filtering Service for NSa 3650 (1-year)	01-SSC-3469
Capture Client	Based on user count
Comprehensive Anti-Spam Service for NSa 3650 (1-year)	01-SSC-4030

NSa 4650	SKU
NSa 4650 TotalSecure Advanced Edition (1-year)	01-SSC-4094
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, and 24x7 Support for NSa 4650 (1-year)	01-SSC-3493
Capture Advanced Threat Protection for NSa 4650 (1-year)	01-SSC-3499
Threat Prevention–Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSa 4650 (1-year)	01-SSC-3589
24x7 Support for NSa 4650 (1-year)	01-SSC-3487
Content Filtering Service for NSa 4650 (1-year)	01-SSC-3583
Capture Client	Based on user count
Comprehensive Anti-Spam Service for NSa 4650 (1-year)	01-SSC-4062

NSa 5650	SKU
NSa 5650 TotalSecure Advanced Edition (1-year)	01-SSC-4342
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, and 24x7 Support for NSa 5650 (1-year)	01-SSC-3674
Capture Advanced Threat Protection for NSa 5650 (1-year)	01-SSC-3680
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSa 5650 (1-year)	01-SSC-3698
24x7 Support for NSa 5650 (1-year)	01-SSC-3660
Content Filtering Service for NSa 5650 (1-year)	01-SSC-3692
Capture Client	Based on user count
Comprehensive Anti-Spam Service for NSa 5650 (1-year)	01-SSC-4068

NSa 6650	SKU
NSa 6650 TotalSecure Advanced Edition (1-year)	01-SSC-2209
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, and 24x7 Support for NSa 6650 (1-year)	01-SSC-8761
Capture Advanced Threat Protection for NSa 6650 (1-year)	01-SSC-8930
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSa 6650 (1-year)	01-SSC-8979
24x7 Support for NSa 6650 (1-year)	01-SSC-8663
Content Filtering Service for NSa 6650 (1-year)	01-SSC-8972
Capture Client	Based on user count
Comprehensive Anti-Spam Service for NSa 6650 (1-year)	01-SSC-9131

NSa 9250	SKU
NSa 9250 TotalSecure Advanced Edition (1-year)	01-SSC-2854
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, and 24x7 Support for NSa 9250 (1-year)	01-SSC-0038
Capture Advanced Threat Protection for NSa 9250 (1-year)	01-SSC-0121
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSa 9250 (1-year)	01-SSC-0343
24x7 Support for NSa 9250 (1-year)	01-SSC-0032
Content Filtering Service for NSa 9250 (1-year)	01-SSC-0331
Capture Client	Based on user count

NSa series ordering information con't

NSa 9450	SKU
NSa 9450 TotalSecure Advanced Edition (1-year)	01-SSC-4358
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, and 24x7 Support for NSa 9450 (1-year)	01-SSC-0414
Capture Advanced Threat Protection for NSa 9450 (1-year)	01-SSC-0855
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSa 9450 (1-year)	01-SSC-1196
24x7 Support for NSa 9450 0 (1-year)	01-SSC-0407
Content Filtering Service for NSa 9450 (1-year)	01-SSC-1158
Capture Client	Based on user count

NSa 9650	SKU
NSa 9650 TotalSecure Advanced Edition (1-year)	01-SSC-3475
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, 24x7 Support for NSa 9650 (1-year)	01-SSC-2036
Capture Advanced Threat Protection for NSa 9650 (1-year)	01-SSC-2042
Threat Prevention – Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NSa 9650 (1-year)	01-SSC-2142
24x7 Support for NSa 9650 0 (1-year)	01-SSC-1989
Content Filtering Service for NSa 9650 (1-year)	01-SSC-2136
Capture Client	Based on user count

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

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

SonicWall NSa/NSv Firewall Bundle

The following NSa series firewalls are eligible to receive a one-year license to the corresponding NSv Virtual Appliance TotalSecure Subscription* at no additional cost.

Eligible NSa Firewall	Corresponding NSv Firewall
NSa 5650	NSv 200
NSa 6650	NSv 200
NSa 9250	NSv 400
NSa 9450	NSv 400
NSa 9650	NSv 400

* *NSv Virtual Appliance TotalSecure Subscription includes NSv virtual firewall, Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention and Application Firewall Service, Content Filtering Service and 24x7 Support.*

Regulatory model numbers:

NSa 2650 - 1RK38-0C8
NSa 3650 - 1RK38-0C7
NSa 4650 - 1RK39-0C9
NSa 5650 - 1RK39-0CA
NSa 6650 - 1RK39-0CB
NSa 9250 - 1RK39-0CC
NSa 9450 - 1RK39-0CD
NSa 9650 - 1RK39-0CE

Partner Enabled Services

Need help to plan, deploy or optimize your SonicWall solution? SonicWall Advanced Services Partners are trained to provide you with world class professional services. Learn more at www.sonicwall.com/PES.

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

Datasheet-NetworkSecurityAppliance-COG-2464