SonicWall Network Security Appliance (NS *to)*

Security for midsize networks, distributed enterprises and data centers with high levels of performance and effectiveness validated by the industry

The SonicWall Network Security appliance (NS *to)* provides to
Organizations ranging from midsize networks to distributed enterprises and data centers advanced threat prevention capabilities on a high-performance security platform.

Using innovative deep learning technologies on the SonicWall Capture Cloud platform, the NS series *to*
provides the automated and real-time breach detection and prevention capabilities organizations need.

Innovative Threat Prevention with Superior Performance

Today's network threats are highly evasive and increasingly difficult to identify using traditional detection methods. Staying one step ahead of sophisticated attacks requires a more modern approach that makes extensive use of cloud security intelligence. Without that intelligence in the cloud, security solutions at the gateway cannot keep up with today's complex threats. NS Series Next Generation Firewalls (NGFWs) *to* They integrate two advanced security technologies to provide innovative threat prevention features that keep your network one step ahead. SonicWall's Capture Advanced Threat Protection (ATP) multi-engine service is enhanced by our patent pending Real Time Deep Memory Inspection (RTDMI ™) technology. The RTDMI engine proactively detects and blocks zero-day threats and unknown mass market malware by directly inspecting memory. Thanks to its real-time architecture, SonicWall RTDMI technology is accurate, minimizes false positives, and identifies and mitigates sophisticated attacks.

where the harmful mechanisms of malware are exposed for less than 100 nanoseconds. Combined with it, SonicWall's patented * Reassembly Free Deep Packet Inspection (RFDPI) engine examines every byte in every packet, inspecting the incoming and outgoing traffic at the firewall. By using the SonicWall Capture Cloud platform along with built-in capabilities such as intrusion prevention, antimalware, and Web / URL filtering, the NS series *to* blocks even the most dangerous threats on the gateway.

Additionally, SonicWall firewalls provide comprehensive protection
decrypting and inspecting encrypted connections using TLS / SSL and SSH, regardless of port and protocol. The firewall examines each packet in depth (header and data) for protocol breaches, threats, zero-day attacks, intrusions, and even defined criteria. Deep packet inspection engine detects and prevents stealth attacks using cryptography, blocks encrypted malware downloads, stops the spread of infections, and thwarts command-and-control communications

and the exfiltration of data. The include and exclude rules provide total control that allows you to customize which traffic should be subjected to decryption and inspection based on specific legal and / or corporate requirements.

When organizations enable deep packet inspection features such as IPS, antivirus, antispyware, decryption / TLS inspection /

SSL, etc., on your firewalls, network performance often slows down, sometimes drastically. NS series firewalls *to,* however, they offer a multi-core hardware architecture with specialized security microprocessors. In combination with

Advantage:

Superior performance and threat prevention

- Patent pending real-time deep memory inspection technology
- Patented deep packet inspection technology without
  reassembled
- Integrated and cloud-based threat prevention
- Decryption and TLS / SSL inspection
- Industry validated security effectiveness
- Hardware architecture
  multicore
- Dedicated Capture Labs Threat Research Team

Network control and flexibility

- Powerful SonicOS operating system
- Application intelligence and control
- Segmentation of the network with VLANs
- High speed wireless security

Simple functions of implementation, configuration and continuous management

- Tightly integrated solution
- Centralized management
- Scalability with multiple hardware platforms
- Reduced total cost of ownership

** US Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723*

Our RTDMI and RFDPI engines, this unique design eliminates the performance loss experienced by networks with other firewalls.

Network control and flexibility

NS series *to* uses SonicOS, the SonicWall operating system, which offers a host of features. SonicOS provides organizations with the network control and flexibility they require through application intelligence and control functions, real-time visualization, an Intrusion Prevention System (IPS) with sophisticated anti-evasion technology, virtual private networks (High-speed VPN) and other robust security features.

Thanks to the intelligence and application control functions, the
Network administrators can identify productive applications and distinguish between those that are unproductive or potentially dangerous, as well as control traffic through powerful application-level policies by both users and groups (along with scheduling capabilities and exception lists). Business-critical applications can be prioritized, allocated higher volume of bandwidth, and bandwidth limited for non-essential applications. Supervisory functions

and real-time visualization offer a graphical representation of applications, users and bandwidth usage that offers a granular view of the traffic of the entire network.

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

Each NS firewall *to* It has a built-in wireless access controller that enables organizations to securely extend the network perimeter using wireless technology. SonicWall firewalls, along with wireless access points

SonicWave 802.11ac Wave 2, create a wireless network security solution that combines industry-leading next-generation firewall technology with high-speed wireless connectivity to deliver enterprise-class, high-speed wireless network security and performance throughout the wireless network.

Simple deployment, configuration and ongoing management features

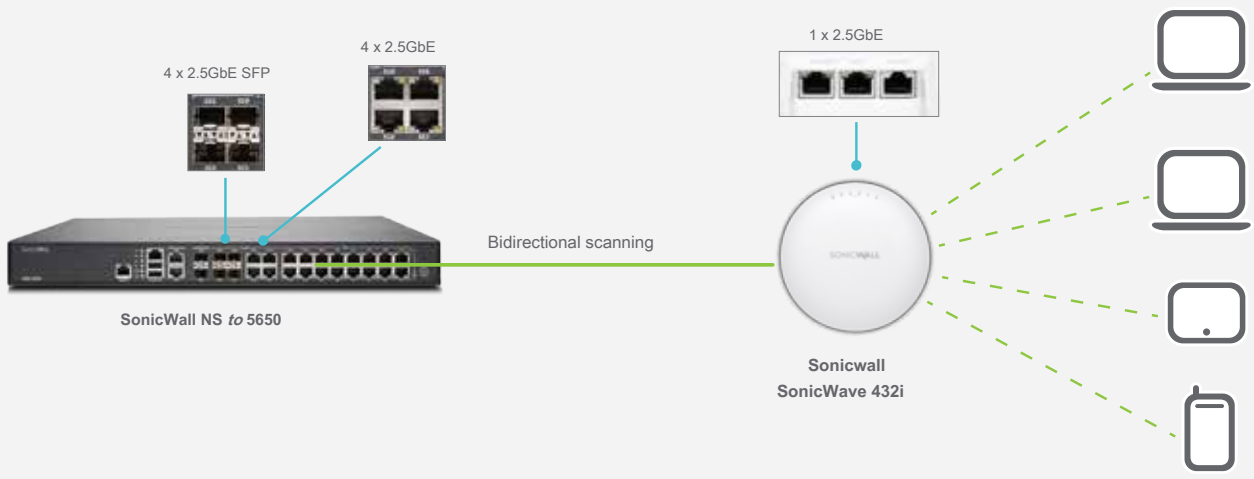
Like all SonicWall firewalls, the NS series *to* tightly integrates key security technologies,

connectivity and flexibility in a single complete solution. This includes SonicWave Wireless Access Points and the SonicWall WAN Acceleration (WXA) WAN Acceleration Series, all of which are automatically detected and made available by the NS firewall. *to* management. Consolidating multiple features eliminates the need to purchase and install one-off products that don't always work well together. In this way, the effort involved in implementing the solution on the network and its configuration is reduced, thus saving time and money.

Management, reporting, licensing and analysis functions in the cloud are centralized in the SonicWall Capture Security Center. Administrators have an intuitive dashboard at their disposal to manage all aspects of the network in real time, including critical security alerts. Simplified deployment and configuration, coupled with ease of management, enable organizations to lower the total cost of ownership and achieve a high return on investment.

High-speed secure wireless technology

Combine a Next Generation NS Series Firewall *to* with a SonicWall SonicWave 802.11ac Wave 2 wireless access point to create a high-speed wireless network security solution. NS series firewalls *to* and SonicWave access points include 2.5GbE ports that enable the multi-gigabit wireless performance offered by Wave 2 wireless technology. The firewall scans all wireless traffic entering and leaving the network using deep packet inspection technology, since It then removes harmful threats like malware and intrusions, even through encrypted connections. Additional security and control capabilities can be used in the wireless network, such as content filtering, application control and intelligence, and Capture Advanced Threat Protection, to provide additional layers of protection.



Capture Cloud Platform

SonicWall's Capture Cloud platform provides cloud-based network management and threat prevention capabilities, as well as reporting and analytics, for organizations of any size. The platform consolidates threat intelligence gathered from various 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 world.

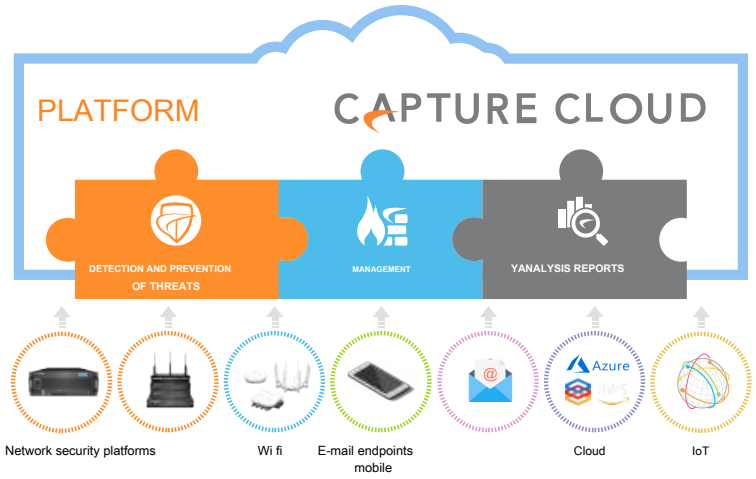
If data accessing the network is found to contain previously unseen malicious code, SonicWall Capture Labs' dedicated internal threat research team develops definitions that are stored in the Capture Cloud platform database and are implemented in

client firewalls to provide up-to-date protection. New updates take effect immediately with no need to restart or interrupt

the system. Device-resident definitions offer protection against a wide variety of attack types, each of which can cover tens of thousands of individual threats. In addition to the countermeasures built into the device, NS firewalls *to* they also have continuous access to the Capture Cloud platform database,

which includes tens of millions of definitions.

Along with threat prevention, the Capture Cloud platform also offers a single management console and enables administrators to easily create real-time and historical reports on network activity.



Advanced Threat Protection

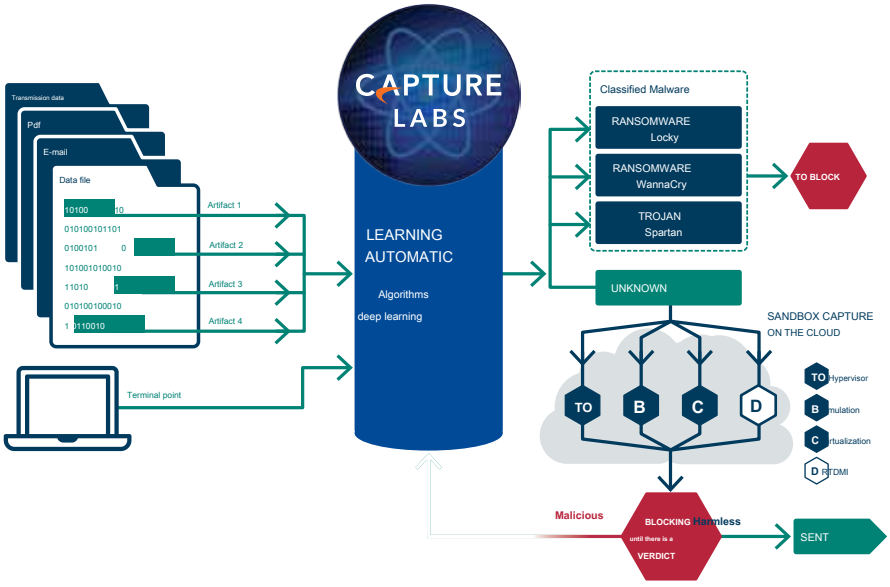
The core of SonicWall's automated real-time breach prevention is the Capture Advanced Threat Protection service, a cloud-based multi-engine sandbox that extends the

firewall protection against threats to detect and prevent zero-day threats. Suspicious files are sent to the cloud, where they are analyzed using deep learning algorithms, with the option to hold them at the gateway until a verdict is rendered. The multi-engine sandbox platform, including real-time deep memory inspection, virtualized sandboxing, full system emulation, and hypervisor-level analytics technology, executes suspicious code and analyzes its behavior. When a malicious file is detected, it is immediately locked and a hash is created within Capture ATP. Soon after, a definition is sent to

firewalls to prevent possible derived attacks.

The service scans a wide variety of operating systems and file types, including executable programs, DLLs, PDFs, MS Office documents, archives, JARs, and APKs.

In order to provide comprehensive endpoint protection, SonicWall Capture Client combines next-generation antivirus technology with SonicWall's cloud-based multi-engine sandbox.



SONICWALL

Deep packet inspection engine without reassembly

SonicWall's No Reassembly Deep Packet Inspection (RFDPI) is a low latency, single pass inspection system that performs bi-directional analysis of traffic based on high flows.

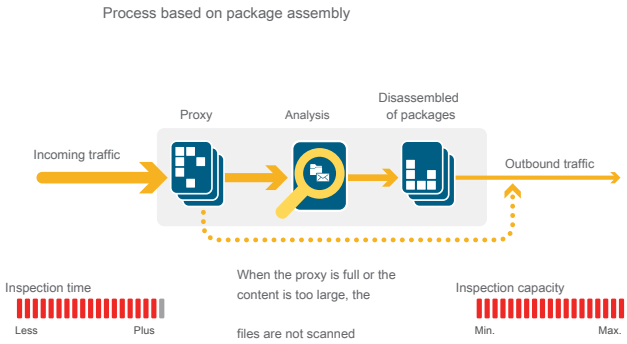
speed without buffering or proxies to discover potential intrusion attempts or malware downloads and to identify application traffic regardless of port and protocol. This proprietary engine relies on inspecting useful data from data traffic to detect threats

at Layers 3-7 and subjects network flows to extensive and repeated normalization and decryption processes in order to neutralize advanced evasion techniques that seek to bypass detection engines and introduce malicious code into the network.

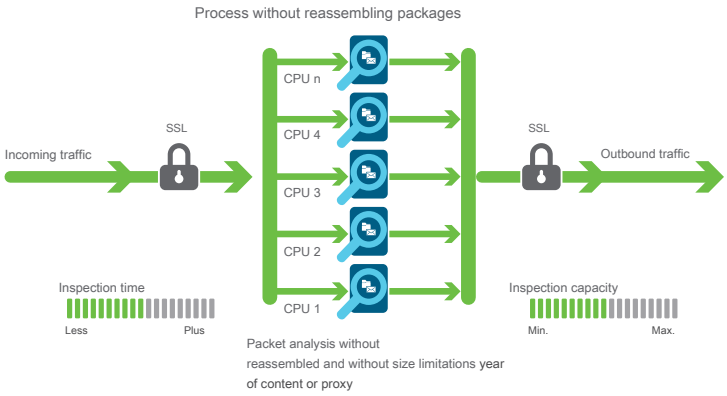
Once a packet has undergone the necessary pre-processing, including TLS / SSL decryption, it is parsed with the help of a single proprietary in-memory representation of three definition databases (intrusion attacks, malware, and applications). The connection status is updated

constantly on the firewall and is checked against these databases until an attack or other security event is identified, in which case a preset action is taken.

In most cases, the system ends the connection and creates logging and notification events. However, the engine can also be configured to perform inspection only or, in the case of application discovery, to provide Layer 7 bandwidth management services for the rest of the application flow as soon as an application is identified.



Competitor architecture



SonicWall architecture

Global reporting and management

For highly regulated organizations that want to coordinate security, control, compliance, and their risk management strategy, SonicWall provides administrators with a unified, secure, and extensible platform to manage firewalls, wireless access points, and series switches. N and Dell X-series using a correlated and auditable workflow process. Enterprises can easily consolidate the management of security devices, reduce administrative and solution complexities

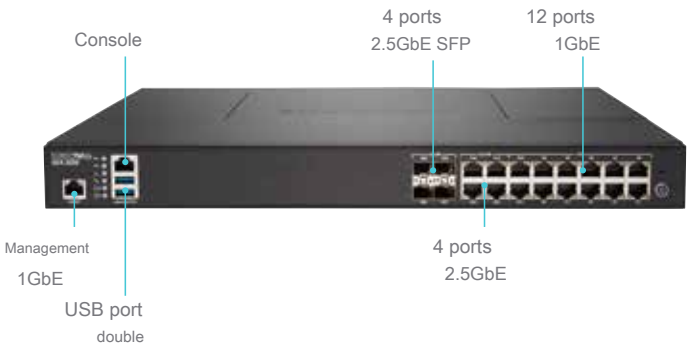
problems, and control all operational aspects of the security infrastructure, such as centralized policy management and enforcement, real-time event monitoring, user activities, application identification, flow analysis and forensics, compliance and audit reports, among other functions. Additionally, businesses meet firewall change management requirements by automating workflow, providing the agility and confidence to implement the appropriate firewall policies at the right time.

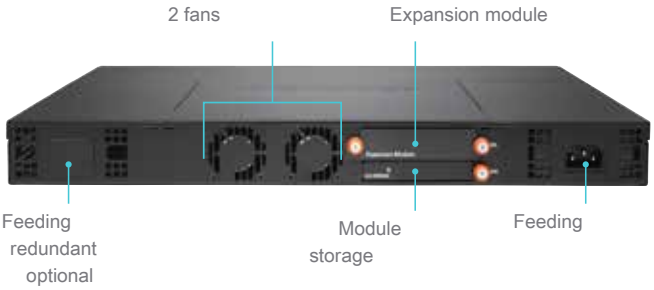
and in accordance with current regulations. Available locally as a SonicWall Global Management System and in the cloud as a Capture Security Center, SonicWall management and reporting solutions provide a consistent way to manage network security through business processes and service levels. In this way they dramatically simplify the life cycle management of their security environments, compared to device-by-device management.

SONICWALL®

NS *to* 2650

The NS *to* provides medium-sized organizations and distributed enterprises with high-speed threat prevention capabilities over thousands of encrypted and even more unencrypted connections.

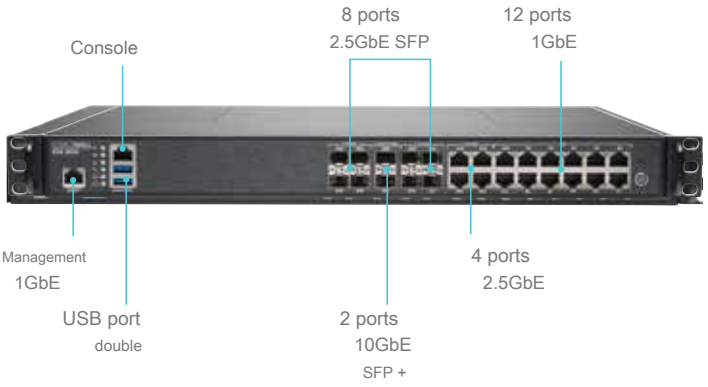


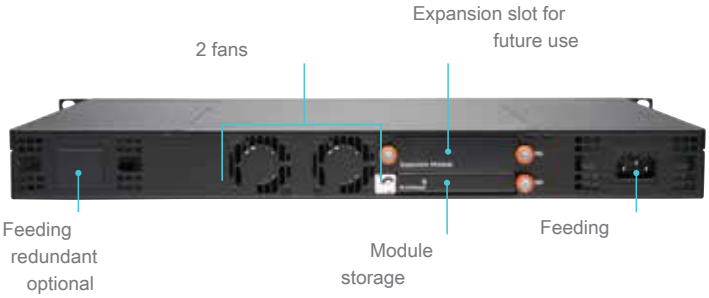


Firewall	NS *to* 2650
Firewall performance	3.0 Gbps
IPS performance	1.4 Gbps
Antimalware performance	600 Mbps
Full DPI performance IMIX	600 Mbps
performance	700 Mbps
Maximum DPI connections	500,000
New connections / s	14,000 / sec.
Storage module	16 GB
Description	**SKU**
NS firewall only *to* 2650 NS *to* 2650 TotalSecure	01-SSC-1936
Advanced (1 year)	01-SSC-1988

NS *to* 3650

The SonicWall NS *to* 3650 is ideal for small and medium business and branch office network environments that are concerned about their data transfer capacity and performance level.

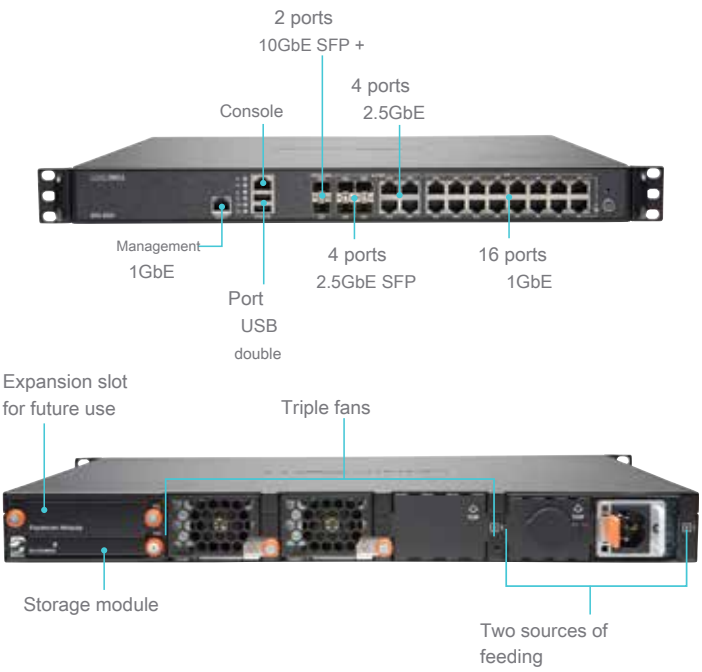




Firewall	NS *to* 3650
Firewall performance	3.75 Gbps
IPS performance	1.8 Gbps
Antimalware performance	800 Mbps
Full DPI performance IMIX	730 Mbps
performance	900 Mbps
Maximum DPI connections	750,000
New connections / s	14,000 / sec.
Storage module	32 GB
Description	**SKU**
NS firewall only *to* 3650 NS *to* 3650 TotalSecure	01-SSC-1937
Advanced (1 year)	01-SSC-4081

NS *to* 4650

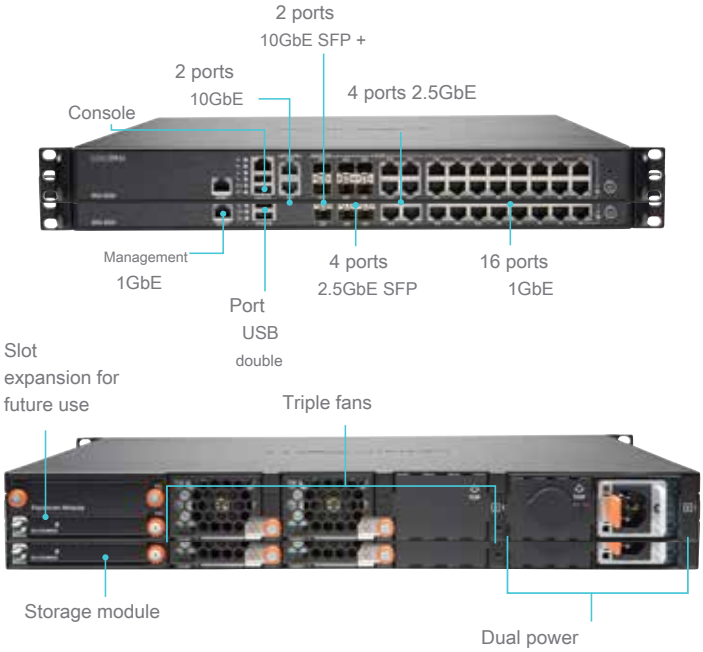
SonicWall NS *to* 4650 protects growing midsize organizations and branch offices with enterprise-class capabilities and without compromising performance.



Firewall	NS *to* 4650
Firewall performance	6.0 Gbps
IPS performance	2.3 Gbps
Antimalware performance	1.25 Gbps
Full DPI performance IMIX	1.2 Gbps
performance	1.3 Gbps
Maximum DPI connections	1,000,000
New connections / s	40,000 / sec.
Storage module	32 GB
Description	**SKU**
NS firewall only *to* 4650 NS *to* 4650 TotalSecure	01-SSC-1938
Advanced (1 year)	01-SSC-4094

NS *to* 5650

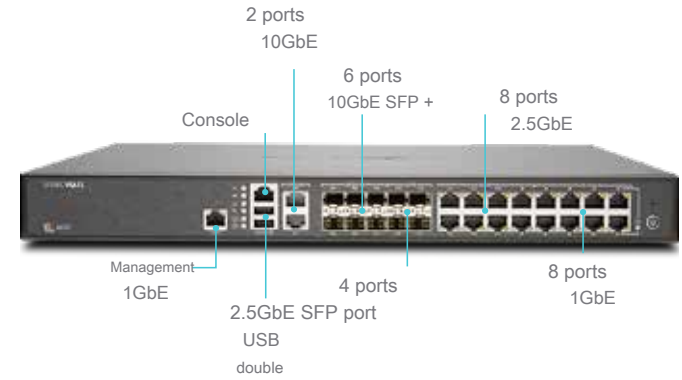
SonicWall NS *to* The 5650 is ideal for corporate environments, distributed networks, and branch offices that require considerable data transfer capacity and high port density.

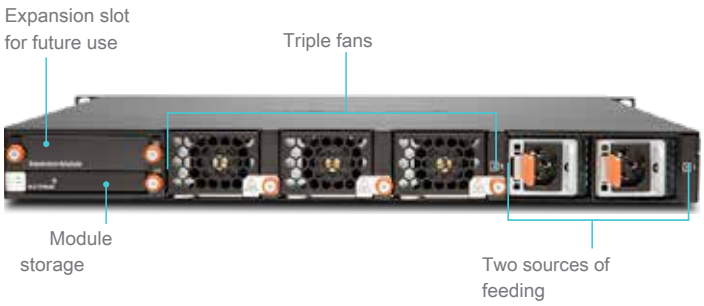


Firewall	NS *to* 5650
Firewall performance	6.25 Gbps
IPS performance	3.4 Gbps
Antimalware performance	1.7 Gbps
Full DPI performance IMIX	1.7 Gbps
performance	1.45 Gbps
Maximum DPI connections	1,500,000
New connections / s	40,000 / sec.
Storage module	64 GB
Description	**SKU**
NS firewall only *to* 5650 NS *to* 5650 TotalSecure	01-SSC-1939
Advanced (1 year)	01-SSC-4342

NS *to* 6650

SonicWall NS *to* The 6650 is ideal for distributed sites and large corporate headquarters that require high data transfer capacity and a high level of performance.

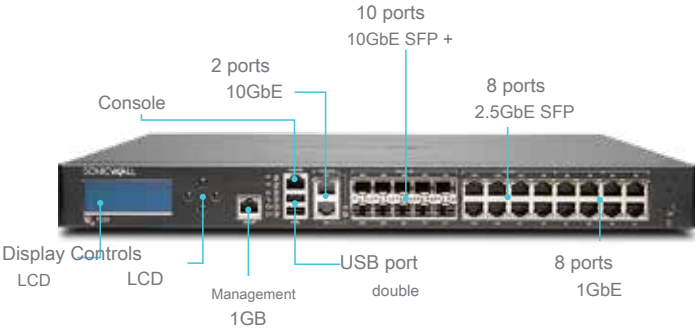


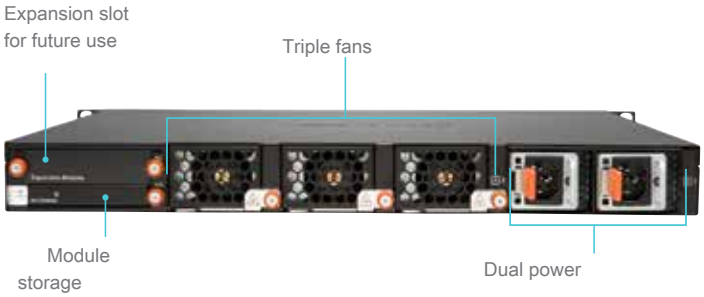


Firewall	NS *to* 6650
Firewall performance	12.0 Gbps
IPS performance	6.0 Gbps
Antimalware performance	3.5 Gbps
Full DPI performance IMIX	3.1 Gbps
performance	2.65 Gbps
Maximum DPI connections	2,000,000
New connections / s	90,000 / sec.
Storage module	64 GB
Description	**SKU**
NS firewall only *to* 6650 NS *to* 6650 TotalSecure	01-SSC-1940
Advanced (1 year)	01-SSC-2209

NS *to* 9250/9450/9650

SonicWall NS *to* 9250/9450/9650 provide scalable deep security for distributed enterprises and data centers at multi-gigabit speeds.





Firewall	NS *to* 9250	NS *to* 9450	NS *to* 9650
Performance of firewall	12.0 Gbps	17.1 Gbps	17.1 Gbps
IPS performance	7.2 Gbps	10.2 Gbps	10.3 Gbps
Performance antimalware	3.7 Gbps	5.0 Gbps	5.5 Gbps
DPI performance full	3.3 Gbps	5.0 Gbps	5.5 Gbps
IMIX performance	2.65 Gbps	4.1 Gbps	4.1 Gbps
DPI connections maxims	3,000,000	4,000,000	5,000,000
New connections / s	90,000 / sec.	130,000 / sec.	130,000 / sec.
Module storage	128 GB	128 GB	256 GB
Description	**SKU**	**SKU**	**SKU**
NS firewall only *to*	01-SSC-1941	01-SSC-1942	01-SSC-1943
NS *to* TotalSecure Advanced (1 year)	01-SSC-2854	01-SSC-4358	01-SSC-3475

SONICWALL

Benefits

RFDPI engine	
Benefit	Description
Reassembly-Free Deep Packet Inspection (RFDPI)	This proprietary, proprietary, high-performance inspection engine performs bi-directional, stream-based traffic analysis without buffering or proxies to discover potential intrusion attempts or malware attacks and to identify application traffic regardless of port.
Bidirectional inspection	It scans incoming and outgoing traffic simultaneously for threats to prevent the network from being used for malware distribution or becoming a launching pad for attacks should an infected computer enter.
Flow-based inspection	Proxy and bufferless inspection technology provides ultra-low latency DPI performance for millions of simultaneous network streams with no stream or file size limitations, and can be applied to common protocols and raw TCP streams.
Highly parallel and scalable	The unique design of the RFDPI engine, combined with the multi-core architecture, provides high DPI performance and extremely high new session establishment rates to cope with the peak traffic of the most demanding networks.
Single pass inspection	The single-pass DPI architecture simultaneously scans traffic for malware and intrusion detection and for application identification, dramatically reducing DPI latency and ensuring that all threat information is correlated in a single architecture.
Firewall and interconnection	
Benefit	Description
REST APIs	They allow the firewall to receive and use any proprietary, OEM, or third-party intelligence information to combat advanced threats such as zero-day attacks, malicious internal users, compromised credentials, ransomware, and advanced persistent threats.
Dynamic packet inspection	All network traffic is inspected, analyzed, and subject to firewall access policies.
High availability / clustering (clusters)	NS series *to* Supports Active / Passive (A / P) high availability modes with State Synchronization, Active / Active (A / A) DPI and Active / Active clustered (clustering). Active / Active DPI diverts the load from deep packet inspection to the cores of the passive device in order to improve performance.
Protection against DDoS / DOS attacks	SYN flood protection provides a defense against DoS attacks by using level 3 (SYN proxy) and level 2 (SYN) blacklist technologies. It also offers protection against DoS / DDoS attacks through UDP / ICMP flood protection and connection rate limiting functions.
Support for IPv6	Internet Protocol Version 6 (IPv6) is in the early stages of replacing IPv4. With SonicOS, the hardware will be compatible with filtering and Wire mode implementations.
Flexible deployment options	NS series *to* It can be implemented in traditional NAT mode, Layer 2 bridge mode, Wire mode, and Network TAP mode.
WAN load balancing	Load balancing multiple WAN interfaces using Round Robin or Spillover or using percentage-based methods. Ensures critical communications with 802.1p
Advanced Quality of Service (QoS) H.323	and DSCP tagging and remapping of VoIP traffic on the network.
Gatekeeper and SIP proxy support	Block spam calls: all incoming calls must be authorized and authenticated using the H.323 Gatekeeper or SIP proxy.
Management of individual and cascaded Dell N and X series switches.	Manage additional port security settings, including Portshield, HA, PoE, and PoE +, from a single console using the firewall management dashboard for the Dell N and Dell X series network switch.
Biometric authentication	It supports mobile device authentication, such as fingerprint recognition, which cannot be easily duplicated or shared, in order to securely authenticate the identity of the user so that they can access the network.
Open authentication and social login	Allows guest users to use their credentials from social networking services, such as Facebook, Twitter, or Google+, to log in and access the Internet and other guest user services over a wireless connection from a host, LAN, or DMZ zones, using a pass-through authentication.
Management and reports	
Benefit	Description
Cloud-based and local management	Configuration and management functions for SonicWall appliances available in the cloud through the SonicWall Capture Security Center and locally using the SonicWall Global Management System (GMS).
Powerful individual device management	It offers an intuitive web-based interface that can be quickly and easily configured, a comprehensive command-line interface, and support for SNMPv2 / 3.
IPFIX / Netflow reports of application flows	Export application traffic analysis and usage data using IPFIX or NetFlow protocols to monitor and report on real-time and old data with tools such as SonicWall Scrutinizer or others compatible with IPFIX and NetFlow with extensions.
Virtual private networks (VPN)	
Benefit	Description
VPN with automatic provisioning	Simplify and minimize the complexity of distributed firewall deployments by automating the initial provisioning of the end-to-end VPN gateway between SonicWall firewalls, while the security and connectivity systems work instantly and automatically.
IPSec VPN for inter-site connectivity	High-performance IPSec VPN enables the NS series *to* act as a VPN concentrator for thousands of large sites, branch offices or home offices.
Remote access via SSL VPN or IPSec client	It enables the use of clientless SSL VPN technology or an easy-to-manage IPSec client for easy access to e-mails, 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 automatic reconnection and recovery of all VPN sessions.
Routing-based VPN	Dynamic routing over VPN links ensures uninterrupted service in the event of temporary VPN tunnel failure, as traffic between endpoints can easily be re-routed through alternate routes.

Contextual / content recognition	
Benefit	Description
Tracking user activity	Thanks to the seamless integration of SSO functions with AD / LDAP / Citrix1 / Terminal Services1, in combination with the extensive information provided by the DPI, it is possible to identify users and their activities.
GeoIP - Identification of traffic based on country	Identify and monitor network traffic to or from specified countries to provide protection against attacks from threats of known or suspected origin, or to investigate suspicious traffic originating from the network. Create custom lists of countries and Botnets to override wrong country or Botnet labels associated with an IP address. Eliminates unwanted IP address filtering due to misclassification.
DPI filtering of regular expressions	It prevents data leakage by identifying and controlling the content that traverses the network through regular expression matching. Create custom lists of countries and Botnets to override wrong country or Botnet labels associated with an IP address.

Breach Prevention Subscription Services

Capture Advanced Threat Protection	
Benefit	Description
Multi-engine sandboxing	The multi-engine sandbox platform, including virtualized sandboxing, full system emulation, and hypervisor-level analytics technology, executes suspicious code and analyzes its behavior, providing complete visibility into 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 weapons using encryption. By forcing malware to reveal its damaging mechanisms in memory, the RTDMI engine proactively detects and blocks zero-day threats and unknown mass market malware.
Lock until there is a verdict	To prevent potentially dangerous files from accessing the network, files sent to the cloud for analysis can be held at the gateway until a verdict is rendered.
Scan a wide variety of file types and sizes	Supports analysis of a wide variety of file types, either individually or in groups, such as executable programs (PE), DLLs, PDFs, MS Office documents, archives, JARs and APKs, as well as multiple operating systems, such as Windows , Android, Mac OS X and multi-browser environments.
Quick definition implementation	When a malicious file is detected, a definition is immediately made available to SonicWall Capture ATP subscription firewalls and sent to the Gateway Anti-Virus and IPS definition databases and URL reputation databases, IP and domains within 48 hours.
Capture Client	Capture Client is a unified client platform that provides multiple endpoint protection capabilities, such as advanced malware protection and support for encrypted traffic visibility. It uses multi-layer protection technologies, comprehensive reporting capabilities, and endpoint protection hardening capabilities.
Encrypted Threat Prevention	
Benefit	Description
Decryption and TLS / SSL inspection	Decrypt and inspect TLS / SSL encrypted traffic on the fly, without the need for proxies, for malware, intrusions and data breaches, and enforces application, URL, and content control policies to protect against hidden threats in SSL-encrypted traffic. Included with security subscriptions for all NS series models *to.*
SSH inspection	SSH Deep Packet Inspection (DPI-SSH) decrypts and inspects the data passing through SSH tunnels to prevent attacks using SSH.
Intrusion prevention	
Benefit	Description
Protection based on countermeasures	The tightly integrated Intrusion Prevention System (IPS) uses definitions and other countermeasures to scan useful packet data for vulnerabilities and exploits, thus covering a wide range of attacks and vulnerabilities.
Automatic updates of definitions	SonicWall's Threat Research Team investigates and implements IPS countermeasures, continually updating a long list that covers more than 50 attack categories. New updates take effect on the spot, without requiring a reboot or interrupting your service.
IPS protection between zones	It strengthens internal security by segmenting the network into multiple security zones with intrusion prevention to prevent the spread of threats from one zone to another.
Detection and blocking of command and control (CnC) activities from botnet attacks	Identifies and blocks command and control traffic originating from bots on the local network and directed to IPs and domains identified as malware propagators or known as CnC points.
Protocol abuse / anomaly	Identify and block attacks that abuse protocols to try to bypass the IPS.
Zero day protection	Protect your network from zero-day attacks with constant updates against the latest exploit methods and techniques, covering thousands of individual exploits.
Anti-evasion technology	Extensive flow normalization, decoding, and other techniques prevent threats from penetrating the network undetected using evasion techniques at Layers 2-7.
Threat prevention	
Benefit	Description
Gateway antimalware	RFDPI engine scans all inbound, outbound, and intra-zone traffic for viruses, Trojans, keyloggers, and other malware in files of unlimited length and size on all TCP ports and streams .
Capture Cloud Antimalware Protection	SonicWall cloud servers have a database of tens of millions of threat definitions that is continually updated and used to augment the capabilities of the integrated definition database, providing RFDPI technology with extensive threat coverage.
24 hour security updates	New threat updates are automatically transferred to firewalls with active security services, where they are immediately effective without the need to restart the system or interrupt the service.
Bidirectional TCP Inspection (Raw)	The RFDPI engine can analyze raw TCP streams on any port and in both directions, preventing attacks that try to infiltrate outdated security systems that focus on protecting only a few more popular ports.
Broad protocol support	Identifies common protocols, such as HTTP / S, FTP, SMTP, SMBv1 / v2 and other types, that do not send data in raw TCP, and decodes payloads for malware inspection, even if they are not running on standard and well-known ports .

Application intelligence and control	
Benefit	Description
App control	Control applications, or individual application functions, identified by the RFDPI engine by matching against an ever-growing database of thousands of application definitions, with the goal of increasing network security and productivity.
Custom application identification	Control custom applications by creating definitions based on specific parameters or patterns unique to an application in your network communications for greater control of your network.
Application bandwidth management	Fine-tune and regulate available bandwidth for critical applications or categories of applications, while limiting non-essential 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 complete user identification via SSO through LDAP / AD / Terminal Services / Citrix integration.
Content filtering	
Benefit	Description
Filtering content in and out	Enforce acceptable use policies and block access to HTTP / HTTPS websites containing unacceptable or unproductive information or images with Content Filtering Service and Content Filtering Client.
Hardened content filtering client	Extend policy enforcement to block Internet content for Windows, Mac OS, Android, and Chrome devices 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, for example during work or school hours, and applied to individual users or groups.
Web caching	URL classifications are cached in the SonicWall firewall, reducing the response time for subsequent access to frequently visited sites to just a fraction of a second.
Hardened antivirus and antispyware	
Benefit	Description
Protection at various levels	Use firewall features, such as the first layer of defense at the perimeter, along with endpoint protection, to block viruses that penetrate your network through laptops, flash drives, and other unprotected systems.
Automated application option	Make sure that all computers accessing the network have the appropriate antivirus software and / or DPI-SSL certificate installed and active. This eliminates the costs commonly associated with managing desktop antivirus solutions.
Automated installation and deployment option	Machine-to-machine deployment and installation of antivirus and antispyware clients occurs automatically across the network, minimizing administrative overhead.
Next-generation antivirus	Capture Client uses a static artificial intelligence engine to identify threats before they can be executed and return the system to a pre-infection state.
Antispyware protection	The powerful spyware protection feature scans and blocks the installation of a full suite of spyware programs on desktops and laptops before they transmit sensitive data, helping to increase the security and performance of desktops.

SonicOS Capabilities Overview

Firewall

- Dynamic packet inspection
- Deep packet inspection without reassembly
- Protection against DDoS attacks (UDP / ICMP / SYN floods)
- IPv4 / IPv6
- Biometric authentication for remote access
- ProxyDNS
- REST APIs

Decryption and inspection TLS / SSL / SSH 1

- Deep packet inspection for TLS / SSL / SSH
- Include / exclude objects, groups, or host names
- TLS / SSL control
- Granular SSL DPI controls by zone or standard

CaptureAdvancedThreat Protection 1

- Real-time deep memory inspection
- Cloud-based multi-engine analytics
- Virtualized sandboxing
- Hypervisor level analysis
- Full system emulation
- Analysis of a wide variety of file types
- Automatic and manual delivery
- Real-time threat intelligence updates
- Block until there is a verdict
- CaptureClient

Intrusion prevention 1

- Analysis based on definitions
- Automatic updates of definitions
- Bidirectional inspection
- Capability for detailed IPS rules
- Reinforcement of GeoIP policies
- Filtering botnets with dynamic list
- Regular expression matching

Antimalware 1

- Malware analysis based on flows
- GatewayAnti-Virus
- GatewayAnti-Spyware
- Bidirectional inspection
- Unlimited file size
- Malware database in the cloud

Application Identification 1

- Application control
- Application bandwidth management
- Create custom application definitions
- Data leak prevention
- Application reports through NetFlow / IPFIX
- Complete database of application definitions

Traffic visualization and analysis

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

Web content filtering 1

- URL filtering
- Proxy bridging
- Blocking based on keywords
- HTTP header insert
- Bandwidth management according to CFS classification categories
- Unified policy model with application control
- Content FilteringClient

VPN

- VPN with automatic provisioning
- IPSec VPN for inter-site connectivity
- Remote access via VPN and client IPSec
- Redundant VPN gateway
- MobileConnect for iOS, MacOSX, Windows, Chrome, Android, and Kindle Fire
- Route-based VPN (OSPF, RIP, BGP)

Interconnection

- PortShield
- Jumbo frames
- Improved protocolization
- VLAN trunking
- RSTP (Rapid Spanning Tree Protocol)
- Port mirroring
- QoS level 2
- Port security
- Dynamic routing (RIP / OSPF / BGP)
- SonicWall Wireless Controller
- Policy-based routing (ToS / metric and ECMP)
- NAT
- DNS / ProxyDNS
- DHCP server
- Bandwidth management
- Link aggregation (static and dynamic)
- Port redundancy
- High availability A / Pcon State Sync
- A / A clustering
- Inbound / outbound load balancing
- Layer 2 bridge mode, wireless / virtual wire mode, tap mode
- ReconnectionWAN3G / 4G
- Asymmetric routing
- Support for CommonAccess Cards (CAC)

Wireless connection

- WIDS / WIPS
- Radio frequency spectrum analysis
- Prevention of unauthorized access points
- Fast roaming (802.11k / r / v)
- Mesh networks (802.11s)
- Floor plan view / topology view
- Band steering
- Beamforming
- AirTime fairness
- MiFi extend
- Temporary access for guest users
- LHM Guest Portal

Voip

- Granular QoS control
- Bandwidth management
- SIPyH.323 transformations by access rule
- Support forGatekeeperH.323 andproxySIP

Management and supervision

- Capture Security Center, GMS, Web UI, CLI, REST APIs, SNMPv2 / v3
- Protocolization
- NetFlow / IPFIX exports
- Cloud-based configuration backup
- BlueCoat Security Analysis Platform
- SonicWall access point management
- Dell NyDell series switch management X, including cascade switches

1 *Requires additional subscription*

SONICWALL®

NS Series System Specifications *to*

General firewall	NS *to* 2650	NS *to* 3650	NS *to* 4650	NS *to* 5650
OS	SonicOS 6.5.2			
Security Processing Cores	4	6	8	10
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) * 32GB			
Integrated storage	16 GB		32 GB	64 GB
Management	CLI, SSH, IUWeb, Capture Security Center, GMS, REST APIs			
Users with SSO	40,000	50,000	60,000	70,000
Maximum number of access points supported	48	96	128	192
Protocolization	Analyzer, Local Log, Syslog			
Firewall / VPN performance	**NS *to* 2650**	**NS *to* 3650**	**NS *to* 4650**	**NS *to* 5650**
Firewall inspection performance [1]	3.0 Gbps	3.75 Gbps	6.0 Gbps	6.25 Gbps
Full DPI performance [2]	600 Mbps	730 Mbps	1.2 Gbps	1.7 Gbps
Application inspection performance [2]	1.4 Gbps	2.1 Gbps	3.0 Gbps	4.25 Gbps
IPS performance [2]	1.4 Gbps	1.8 Gbps	2.3 Gbps	3.4 Gbps
Anti-malware inspection performance [2]	600 Mbps	800 Mbps	1.25 Gbps	1.7 Gbps
IMIX performance	700 Mbps	900 Mbps	1.3 Gbps	1.45 Gbps
TLS / SSL decryption and inspection performance (DPI SSL) [2]	250 Mbps	300 Mbps	500 Mbps	800 Mbps
VPN performance [3]	1.3 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 number of connections (DPI) Maximum	500,000	750,000	1,000,000	1,500,000
number of connections (DPI SSL) Standard connections	18,000	24,000	30,000	37,000
(DPI / DPI SSL) [4]	500,000 / 12,000	625,000 / 15,000	750,000 / 18,000	1,000,000 / 19,000
VPN	**NS *to* 2650**	**NS *to* 3650**	**NS *to* 4650**	**NS *to* 5650**
Tunnels between sites	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) Encryption /	2 (350)	2 (500)	2 (1,000)	2 (1,500)
Authentication	DES, 3DES, AES (128, 192, 256 bit), MD5, SHA-1, Crypto Suite B			
Key exchange	Diffie Hellman Groups 1, 2, 5, 14v			
Routing-based VPN	RIP, OSPF, BGP			
Interconnection	**NS *to* 2650**	**NS *to* 3650**	**NS *to* 4650**	**NS *to* 5650**
IP address assignment NAT	Static, (DHCP, PPPoE, L2TP and PPTP client), internal DHCP server, DHCP relay			
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, maximum 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	H323-v1-5 full, SIP			
Standards	TCP / IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP / IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3 ICSA Firewall, ICSA			
Certifications (in progress)	Anti-Virus, FIPS 140-2, Common Criteria NDPP (Firewall e PS), 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, Clustering active / active
Hardware	**NS *to* 2650**	**NS *to* 3650**	**NS *to* 4650**	**NS *to* 5650**
Power supply	Dual, redundant 120W (one included)		Dual, redundant 350W (one included)	
Fans	Two, fixed		Triple, removable	
Input power	100-240 V AC, 50-60 Hz			
Maximum power consumption (W) MTBF at	37.2	46	93.6	103.6
25 ° C in hours	162,231	156,681	154,529	153,243
MTBF at 25 ° C in years	18.5	17.9	17.6	17.5
Form factor	1U rack mount ready			
Dimensions	43 x 32.5 x 4.5 cm (16.9 x 12.8 x 1.8 inches)		43 x 41.5 x 4.5 cm (16.9 x 16.3 x 1.8 inches)	
Weight	5.2 kg (11.5 lb)	5.3 kg (11.7 lb)	6.9 kg (15.2 lb)	6.9 kg (15.2 lb)
WEEE weight	5.5 kg (12.1 lb)	5.6 kg (12.3 lb)	8.9 kg (19.6 lb)	8.9 kg (19.6 lb)
Shipping weight	7.7 kg (17.0 lb)	7.8 kg (17.2 lb)	11.3 kg (24.9 lb)	11.3 kg (24.9 lb)
Compliance with standards	FCC Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, MSIP / KCC Class A, UL, cUL, TÜV / GS, CB, Mexico CoC by UL, EEE, REACH, ANATEL, BSMI			
Environment (Operational / Storage)	0 ° -40 ° C (32 ° -105 ° F) / - 40 ° to 70 ° C (-40 ° to 158 ° F)			
Humidity	10-90%, non-condensing			

SONICWALL®

NS Series System Specifications *to* (cont.)

General firewall	NS *to* 6650	NS *to* 9250	NS *to* 9450	NS *to* 9650
OS	SonicOS 6.5.2			
Security Processing Cores	24	24	32	32
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 Knosola	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) * 128GB			
Integrated storage	64 GB		128 GB	256 GB
Management	CLI, SSH, IUWeb, Capture Security Center, GMS, REST APIs	CLI, SSH, IUWeb, GMS, REST APIs		
Users with SSO	70,000	80,000	90,000	100,000
Maximum number of access points supported	192	192	192	192
Protocolization	Analyzer, Local Log, Syslog, IPFIX, NetFlow			
Firewall / VPN performance	**NS *to* 6650**	**NS *to* 9250**	**NS *to* 9450**	**NS *to* 9650**
Firewall inspection performance [1]	12.0 Gbps	12.0 Gbps	17.1 Gbps	17.1 Gbps
Full DPI performance [2]	3.1 Gbps	3.3 Gbps	5.0 Gbps	5.5 Gbps
Application inspection performance [2]	6.0 Gbps	7.75 Gbps	10.8 Gbps	11.5 Gbps
IPS performance [2]	6.0 Gbps	7.2 Gbps	10.2 Gbps	10.3 Gbps
Anti-malware inspection performance [2]	3.5 Gbps	3.7 Gbps	5.0 Gbps	5.5 Gbps
IMIX performance	2.65 Gbps	2.65 Gbps	4.1 Gbps	4.1 Gbps
TLS / SSL decryption and inspection performance (DPI SSL) [2]	1.45 Gbps	1.5 Gbps	2.1 Gbps	2.25 Gbps
VPN performance [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 number of connections (DPI) Maximum	2,000,000	3,000,000	4,000,000	5,000,000
number of connections (DPI SSL) Standard connections	100,000	100,000	200,000	300,000
(DPI / DPI SSL) [4]	1,500,000 / 45,000	2,000,000 / 48,000	3,000,000 / 134,000	4,000,000 / 210,000
VPN	**NS *to* 6650**	**NS *to* 9250**	**NS *to* 9450**	**NS *to* 9650**
Tunnels between sites	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) Encryption /	2 (2,000)	2 (3,000)	2 (3,000)	50 (3,000)
Authentication	DES, 3DES, AES (128, 192, 256 bit), MD5, SHA-1, Crypto Suite B			
Key exchange	Diffie Hellman Groups 1, 2, 5, 14v			
Routing-based VPN	RIP, OSPF, BGP			
Interconnection	**NS *to* 6650**	**NS *to* 9250**	**NS *to* 9450**	**NS *to* 9650**
IP address assignment NAT	Static, (DHCP, PPPoE, L2TP and PPTP client), internal DHCP server, DHCP relay			
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, maximum 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	H323-v1-5 full, SIP			
Standards	TCP / IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP / IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3 ICSA Firewall, ICSA			
Certifications (in progress)	Anti-Virus, FIPS 140-2, Common Criteria NDPP (Firewall e PS), UC APL, USGv6, CsFC			
High availability [5]	Active / Passive with State Sync, Active / Active DPI with State Sync, Active / Active Clustering			
Hardware	**NS *to* 6650**	**NS *to* 9250**	**NS *to* 9450**	**NS *to* 9650**
Power supply	Dual, redundant 350W (one included)	Dual, redundant, 350W		
Fans	Triple, removable			
Input power	100-240 V AC, 50-60 Hz			
Maximum power consumption (W) MTBF at	144.3	86.7	90.9	113.1
25 ° C in hours	157,193	139,783	134,900	116,477
MTBF at 25 ° C in years	17.9	15.96	15.4	13.3
Form factor	1U rack mount ready			
Dimensions	43 x 41.5 x 4.5 cm (16.9 x 16.3 x 1.8 inches)			
Weight	8.1 kg (17.9 lb)	8.1 kg (17.9 lb)		
WEEE weight	10.2 kg (22.5 lb)	10.2 kg (22.5 lb)		
Shipping weight	12.6 kg (27.8 lb)	12.6 kg (27.8 lb)		
Compliance with standards	FCC Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, MSIP / KCC Class A, UL, cUL, TÜV / GS, CB, Mexico CoC by UL, WEEE, REACH, ANATEL, BSMI			
Environment (Operational / Storage)	0 ° -40 ° C (32 ° -105 ° F) / - 40 ° to 70 ° C (-40 ° to 158 ° F)			
Humidity	10-90%, non-condensing			

[1] Test methods: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services.

[2] Full DPI / Gateway AV / Anti-Spyware / IPS performance measured using the standard Spirent WebAvalanche HTTP performance test and Ixia testing tools. Multiple streams through multiple pairs of ports have been used for testing.

[3] VPN performance measurement based on UDP traffic with 1280-byte packets in accordance with RFC 2544 Specifications, capabilities, 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, excluding NSa 9250 and above.

[5] Active / Active Clustering and Active / Active DPI with State Sync require the purchase of extended licenses.

** Future use. Specifications, features and availability are subject to change.*

NS Series Ordering Information *to*

NS *to* 2650	SKU
NS *to* 2650 TotalSecure Advanced Edition (1 year)	01-SSC-1988
Advanced Gateway Security Suite - Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for NS *to* 2650 (1 year) Capture Advanced Threat	01-SSC-1783
Protection for NS *to* 2650 (1 year)	01-SSC-1935
Threat Prevention - Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NS *to* 2650 (1 year) 24x7 support for NS *to* 2650 (1 year)	01-SSC-1976
Content Filtering Service for NS *to* 2650 (1 year) Capture Client	01-SSC-1541
	01-SSC-1970
	Based on the number of users
Comprehensive Anti-Spam Service for NS *to* 2650 (1 year)	01-SSC-2001
NS *to* 3650	**SKU**
NS *to* 3650 TotalSecure Advanced Edition (1 year)	01-SSC-4081
Advanced Gateway Security Suite - Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for NS *to* 3650 (1 year) Capture Advanced Threat	01-SSC-3451
Protection for NS *to* 3650 (1 year)	01-SSC-3457
Threat Prevention - Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NS *to* 3650 (1 year) 24x7 NS support *to* 3650 (1 year)	01-SSC-3632
Content Filtering Service for NS *to* 3650 (1 year) Capture Client	01-SSC-3439
	01-SSC-3469
	Based on the number of users
Comprehensive Anti-Spam Service for NS *to* 3650 (1 year)	01-SSC-4030
NS *to* 4650	**SKU**
NS *to* 4650 TotalSecure Advanced Edition (1 year)	01-SSC-4094
Advanced Gateway Security Suite - Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for NS *to* 4650 (1 year) Capture Advanced Threat	01-SSC-3493
Protection for NS *to* 4650 (1 year)	01-SSC-3499
Threat Prevention - Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NS *to* 4650 (1 year) 24x7 NS support *to* 4650 (1 year)	01-SSC-3589
Content Filtering Service for NS *to* 4650 (1 year) Capture Client	01-SSC-3487
	01-SSC-3583
	Based on the number of users
Comprehensive Anti-Spam Service for NS *to* 4650 (1 year)	01-SSC-4062
NS *to* 5650	**SKU**
NS *to* 5650 TotalSecure Advanced Edition (1 year)	01-SSC-4342
Advanced Gateway Security Suite - Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for NS *to* 5650 (1 year) Capture Advanced Threat	01-SSC-3674
Protection for NS *to* 5650 (1 year)	01-SSC-3680
Threat Prevention - Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NS *to* 5650 (1 year) 24x7 NS support *to* 5650 (1 year)	01-SSC-3698
Content Filtering Service for NS *to* 5650 (1 year) Capture Client	01-SSC-3660
	01-SSC-3692
	Based on the number of users
Comprehensive Anti-Spam Service for NS *to* 5650 (1 year)	01-SSC-4068
NS *to* 6650	**SKU**
NS *to* 6650 TotalSecure Advanced Edition (1 year)	01-SSC-2209
Advanced Gateway Security Suite - Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for NS *to* 6650 (1 year) Capture Advanced Threat	01-SSC-8761
Protection for NSa 6650 (1 year)	01-SSC-8930
Threat Prevention - Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NS *to* 6650 (1 year) 24x7 Gold Support for NS *to* 6650 (1	01-SSC-8979
year) Content Filtering Service for NS *to* 6650 (1 year) Capture Client	01-SSC-8663
	01-SSC-8972
	Based on the number of users
Comprehensive Anti-Spam Service for NS *to* 6650 (1 year)	01-SSC-9131
NS *to* 9250	**SKU**
NS *to* 9250 TotalSecure Advanced Edition (1 year)	01-SSC-2854
Advanced Gateway Security Suite - Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for NS *to* 9250 (1 year) Capture Advanced Threat	01-SSC-0038
Protection for NS *to* 9250 (1 year)	01-SSC-0121
Threat Prevention - Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NS *to* 9250 (1 year) 24x7 NS support *to* 9250 (1 year)	01-SSC-0343
Content Filtering Service for NS *to* 9250 (1 year) Capture Client	01-SSC-0032
	01-SSC-0331
	Based on the number of users
NS *to* 9450	**SKU**
NS *to* 9450 TotalSecure Advanced Edition (1 year)	01-SSC-4358
Advanced Gateway Security Suite - Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for NS *to* 9450 (1 year) Capture Advanced Threat	01-SSC-0414
Protection for NS *to* 9450 (1 year)	01-SSC-0855
Threat Prevention - Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NS *to* 9450 (1 year) 24x7 support for NS *to* 9450 (1 year)	01-SSC-1196
Content Filtering Service for NS *to* 9450 (1 year) Capture Client	01-SSC-0407
	01-SSC-1158
	Based on the number of users

NS Series Ordering Information *to* (cont.)

NS *to* 9650	SKU
NS *to* 9650 TotalSecure Advanced Edition (1 year)	01-SSC-3475
Advanced Gateway Security Suite - Capture ATP, Threat Prevention, Content Filtering and 24x7 Support for NS *to* 9650 (1 year) Capture Advanced Threat	01-SSC-2036
Protection for NS *to* 9650 (1 year)	01-SSC-2042
Threat Prevention - Intrusion Prevention, Gateway Anti-Virus, Gateway Anti-Spyware, Cloud Anti-Virus for NS *to* 9650 (1 year) 24x7 NS support *to* 9650 (1 year)	01-SSC-2142
Content Filtering Service for NS *to* 9650 (1 year) Capture Client	01-SSC-1989
	01-SSC-2136
	Based on the number of users
Modules and accessories *	**SKU**
10GBASE-SR SFP + short-range module	01-SSC-9785
10GBASE-LR SFP + long-range module Twinax cable	01-SSC-9786
(1M) 10GBASE SFP +	01-SSC-9787
Twinax Cable (3M) 10GBASE SFP +	01-SSC-9788
1000BASE-SX SFP Short Distance Module	01-SSC-9789
1000BASE-LX SFP Long Distance Module	01-SSC-9790
1000BASE-T SFP Copper Module	01-SSC-9791

** For a complete list of supported SFP and SFP + modules, consult your local SonicWall reseller*

Official model numbers:

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

About us

SonicWall has been fighting the cybercrime industry for over 26 years, defending small, medium and large businesses around the world. Our combination of products and partners has enabled us to create a real-time cyber defense solution tailored to the specific needs of more than 500,000 businesses in more than 150 countries, so you can fully focus on your business without having to worry about threats.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
For more information, see our website.
www.sonicwall.com

Datasheet-NetworkSecurityAppliance-US-VG-MKTG2832