SonicWall Gen 7 NS*sp* Series

The SonicWall Network Security services platform™ (NS*sp*) series has next-generation firewalls with high port density and multi-gig speed interfaces, that can process several million connections for zero-day and advanced threats. Designed for large enterprise, higher education, government agencies and MSSPs, it eliminates attacks in real time without slowing performance. It is designed to be highly reliable and deliver uninterrupted services to organizations.

HIGHLIGHTS

SonicWall NS*sp* Series

- High port density
- 100 GbE ports
- Integrates with on-prem and cloud-based sandboxing
- Intuitive user interface with central management
- 80+ Gbps Threat prevention throughput
- Redundant power
- Up to 100 Gbps firewall inspection throughput
- TLS 1.3 support
- Supports millions of simultaneous TLS connections
- Low TCO
- Powered by SonicWall Capture Labs threat research team

NS*sp* Spec Preview. View full specs »

100 GbE	Up to 100 Gbps	40M
Ports	Firewall inspection throughput	Max Connections (NS*sp* 15700)

Learn more about SonicWall Gen 7 NS*sp* Series:

sonicwall.com/NS*sp*

DATASHEET

Enterprise-Class Firewalls

As businesses evolve along with an increase in managed and unmanaged devices, networks, cloud workloads, SaaS applications, users, Internet speeds, and encrypted connections, a firewall that can't support any one of these becomes a bottleneck. A firewall should be a source of strength and not a point of weakness.

The SonicWall NS*sp* firewall's multiple 100G/40G/25G/10G interfaces allow you to process several million simultaneous encrypted and unencrypted connections with unparallel threat prevention technology. With more than 70% of all sessions being encrypted, having a firewall that can process and examine this traffic without impacting the end user experience is critical to productivity and information security.

The NS*sp* 15700's unified policy enables organizations to simply and intuitively create access and security policies in a single interface.

Simplified management and reporting

Ongoing management, monitoring and reporting of network activities are handled through the SonicWall Network Security Manager. This provides an intuitive dashboard for managing firewall operations as well as provide historical reports – from a single source. 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.

Deployment

Next-Generation Firewall (NGFW)

- Managed through a single pane of glass
- NS*sp* integrates with the rest of the SonicWall ecosystem of solutions
- Gain full visibility into your network to see what applications, devices, and users are doing to enforce policies as well as eliminate threats and bandwidth bottlenecks
- Integrate with Capture ATP with RTDMI for cloud-based sandboxing or Capture Security appliance for on-premise malware detection

Deep Packet Inspection of SSL/ TLS (DPI-SSL) for hidden threats

- The NS*sp* provides inspection for over millions of simultaneous TLS/SSL and SSH encrypted connections regardless of port or protocol
- Inclusion and exclusion rules allow customization based on specific organizational compliance and/or legal requirements
- Support for TLS cipher suites up to TLS 1.3

Segmentation and Networking

- Operate across several segmented networks, clouds, or service definitions, with unique templates, device groups, and policies across multiple devices and tenants
- MSSPs can also support multiple customers with a clean pipe along with unique policies

Multi-instance Firewall (only for NS*sp* 15700)

- Multi-instance is the next generation of multi-tenancy
- Each tenant is isolated with dedicated compute resources to avoid resource starvation
- It features physical and logical ports/tenants
- It supports independent tenant policy and configuration management
- Leverage version independence and High Availability (HA) support for tenants

Wire Mode Functionality

- Bypass Mode for the quick and relatively non-interruptive introduction of firewall hardware into a network
- Inspect Mode to extend Bypass Mode without functionally altering the low-risk, zero latency packet path
- Secure Mode to actively interposing the firewall's multi-core processors into the packet processing path
- Tap Mode to ingest a mirrored packet stream via a single switch port on the firewall, eliminating the need for physically intermediated insertion

Advanced Threat Protection

- SonicWall Capture Advanced Threat Protection™ (ATP) is used by over 150,000 customers across the world through a variety of solutions and it helps to discover and stop over 1,200 new forms of malware each business day
- NS*sp* integrates with Capture Security appliance to detect and block unknown threats with on-premises sandboxing thats uses Real-Time Deep Memory Inspection™ (RTDMI).

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

Content Filtering Services

- Compare requested web sites against a massive database in the cloud containing millions of rated URLs, IP addresses and web sites
- Create and apply policies that allow or deny access to sites based on individual or group identity, or by time of day, for over 50 pre-defined categories

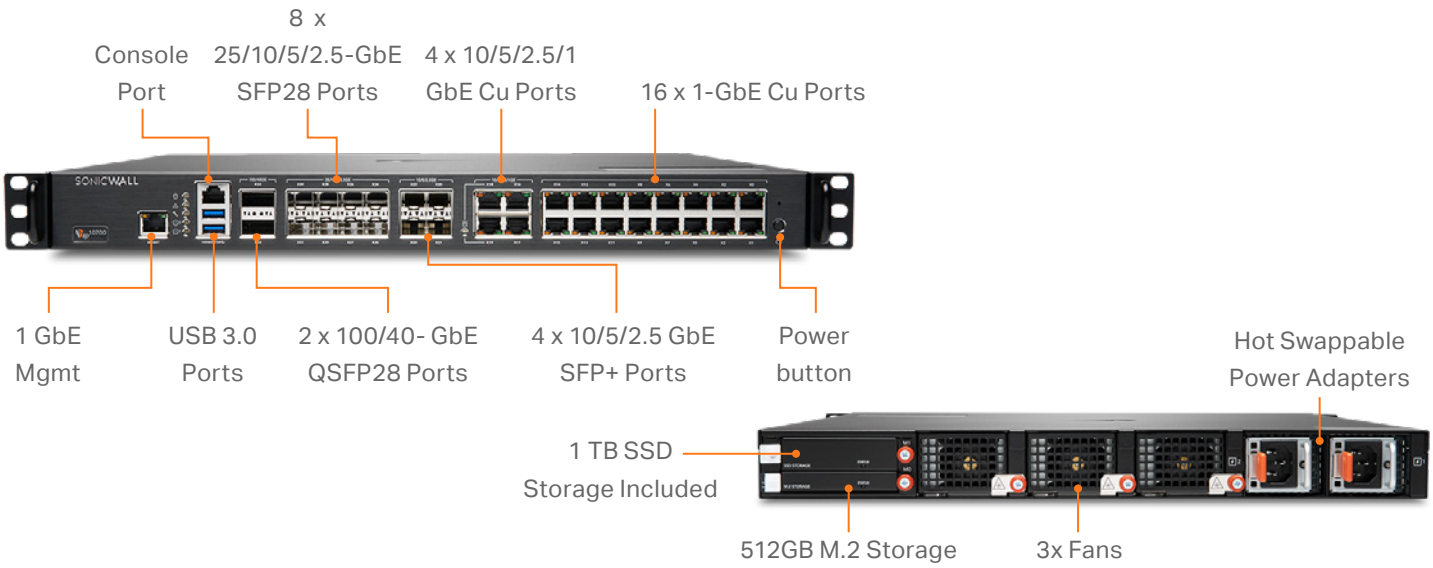
Intrusion Prevention System (IPS)

- Delivers a configurable, high performance Deep Packet Inspection engine for extended protection of key network services such as Web, e-mail, file transfer, Windows services and DNS
- Designed to protect against application vulnerabilities as well as worms, trojans, spyware and backdoor exploits
- The extensible signature language provides proactive defense against newly discovered application and protocol vulnerabilities
- SonicWall IPS offloads the costly and time-consuming burden of maintaining and updating signatures for new attacks through SonicWall's industry-leading Distributed Enforcement Architecture (DEA)

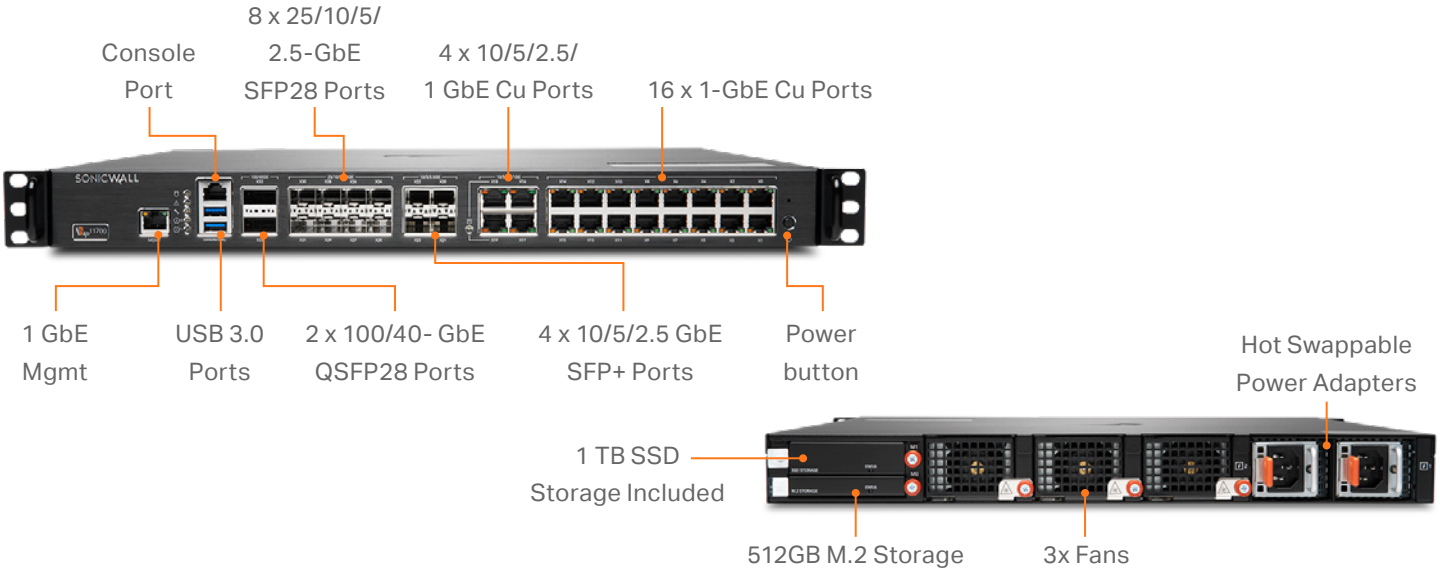
IoT and Application Control

- The NS*sp* catalogs thousands of applications through App Control and monitors their traffic for anomalous behavior

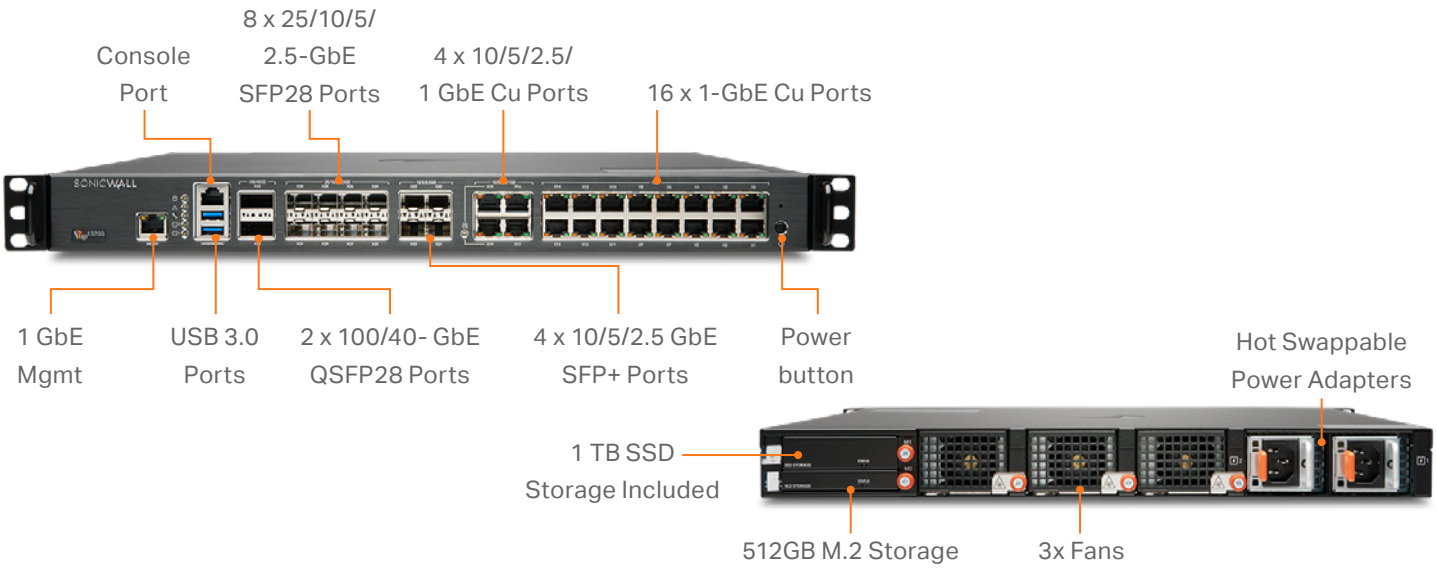
NS*sp* 10700



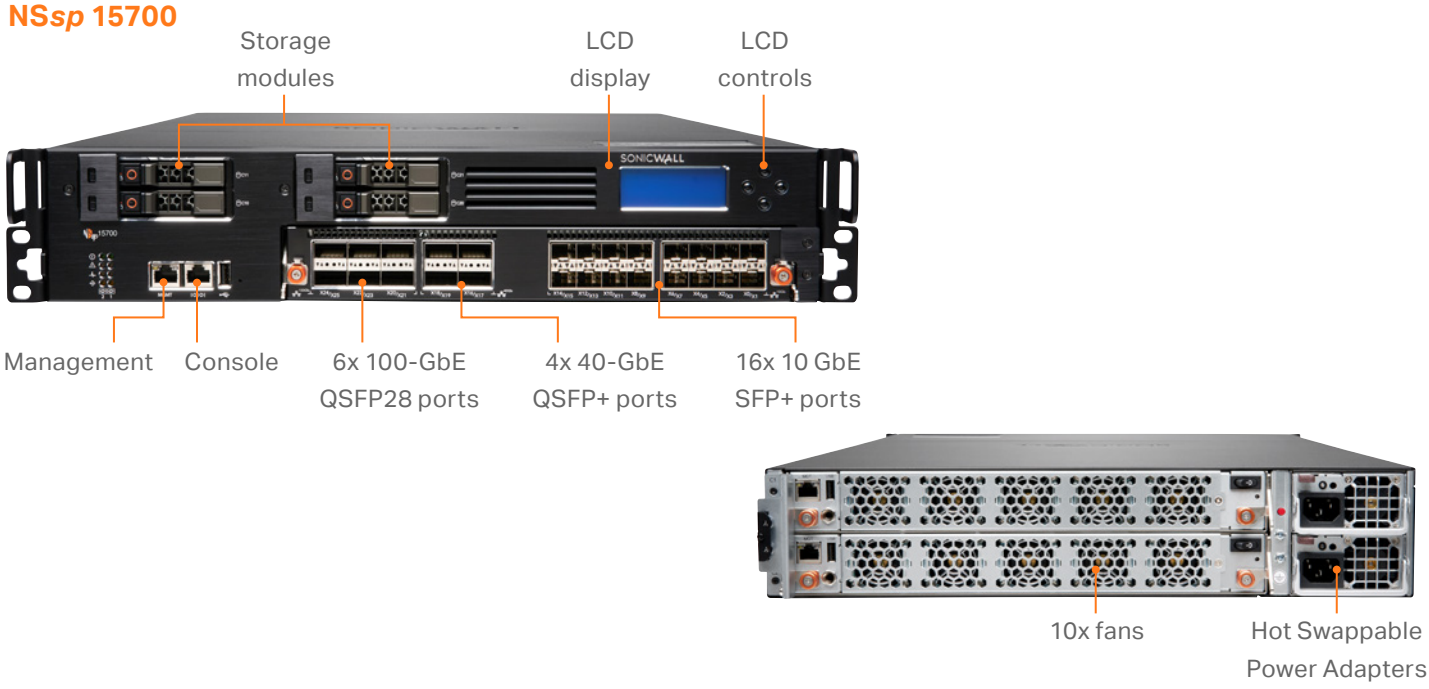
NS*sp* 11700



NS*sp* 13700



NS*sp* 15700



SonicWall NS*sp* Series specifications

Firewall General	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Operating System	SonicOS 7.0.1	SonicOS 7.0.1	SonicOS 7.0.1	SonicOSX 7.0.1
Interfaces	2x100/40-GbE QSFP28, 8x25/10/5/2.5-GbE SFP28 4x10G/5G/2.5G/1G (SFP+), 4 x 10G/5G/2.5G/1G (Cu); 16 x 1GbE (Cu) 2 USB 3.0, 1 Console, 1 Mgmt. port	2x100/40-GbE QSFP28, 8x25/10/5/2.5-GbE SFP28 4x10G/5G/2.5G/1G (SFP+), 4 x 10G/5G/2.5G/1G (Cu); 16 x 1GbE (Cu) 2 USB 3.0, 1 Console, 1 Mgmt. port	2x100/40-GbE QSFP28, 8x25/10/5/2.5-GbE SFP28, 4x10/5/2.5-GbE SFP+, 4x10/5/2.5/1-GbE Cu, 16x1-GbE 2 USB 3.0, 1 Console, 1 Mgmt. port	6 x 100-GbE QSFP28, 4 x 40-GbE QSFP+, 16 x 10 GbE SFP+ 3 USB 3.0, 1 Console, 1 Mgmt. port
Total storage	1.5TB	1.5TB	1.5TB	2 x 480 GB SSD
Management	CLI, SSH, Web UI, REST APIs			
SSO Users	100,000			
Access points supported (maximum)	512	512	512	512
Logging	Analytics, Local Log, Syslog, IPFIX, NetFlow			

Firewall/VPN Performance	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Firewall inspection throughput[1]	42 Gbps	47 Gbps	60 Gbps	105 Gbps
Threat Prevention throughput[2]	28 Gbps	37 Gbps	45.5 Gbps	82 Gbps
Application inspection throughput[2]	30 Gbps	44 Gbps	57 Gbps	86 Gbps
IPS throughput[2]	28 Gbps	37 Gbps	48 Gbps	76.5 Gbps
TLS/SSL inspection and decryption throughput (DPI SSL)[2]	10 Gbps	11.5 Gbps	16.5 Gbps	21 Gbps
VPN throughput[3]	22.5 Gbps	26.7 Gbps	29 Gbps	32 Gbps
Connections per second	280,000	280,000	280,000	800,000
Maximum connections (SPI)	15,000,000	20,000,000	25,000,000	40,000,000
Maximum connections (DPI)	12,000,000	17,000,000	22,000,000	40,000,000
Maximum connections (DPI SSL)	1,500,000	1,750,000	2,000,000	4,000,000

VPN	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Site-to-site VPN tunnels	6,000	12,000	12,000	25,000
IPSec VPN clients (max)	2000 (6000)	2000 (6000)	2,000 (6,000)	2,000 (10,000)
SSL VPN licenses (max)	100 (3000)	100 (3000)	100 (3000)	256 (3000)
Encryption/authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA (1,256,384,512) Suite B Cryptography		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			
Certificate support	Verisign, Thawte, Cybertrust, RSA Keon, Entrust and Microsoft CA for SonicWall-to- SonicWall VPN, SCEP			
VPN features	Dead Peer Detection, DHCP Over VPN, IPSec NAT Traversal, Redundant VPN Gateway, Route-based VPN			
Global VPN client platforms supported	Microsoft® Windows 11, Windows 10 (64-bit and 32-bit)			
NetExtender	Microsoft Windows Vista 32/64-bit, Windows 7, Windows 8.0 32/64-bit, Windows 8.1 32/64-bit, Mac OS X 10.4+, Linux FC3+/Ubuntu 7+/OpenSUSE			
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (Embedded)			

Networking	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Multi-Instance Firewall	N/A	N/A	N/A	Max Tenants per Hardware: 12
IP address assignment	Static (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP Relay			

SonicWall NS*sp* Series specifications

Networking	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
NAT modes	1:1, many:1, 1:many, flexible NAT (overlapping IP), PAT, transparent mode			
Logical VLAN and tunnel interfaces (maximum)	1024			
Wire Mode	–	–	–	Yes
Routing protocols	BGP4, OSPF, RIPv1/ v2, static routes, policy-based routing	BGP4, OSPF, RIPv1/ v2, static routes, policy-based routing	BGP4, OSPF, RIPv1/ v2, static routes, policy-based routing	BGP, OSPF, RIPv1/ v2, static routes, policy-based routing
QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1e (WMM)			
Authentication	LDAP (multiple domains), XAUTH/RADIUS, TACACS+, SSO, Radius accounting NTLM, internal user database, 2FA, Terminal Services, Citrix, Common Access Card (CAC)		LDAP (multiple domains), XAUTH/RADIUS, SSO, Novell, internal user database, Terminal Services, Citrix, Common Access Card (CAC)	
Local user database	4,000	4,000	4,000	5,000
VoIP	Full H323-v1-5, SIP			
Standards	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
FIPS 140-2 Compliant	Pending	Pending	Pending	Yes
Certifications	ICSA Enterprise Firewall, ICSA Antivirus, IPv6/USGv6			
Certifications (in progress)	Common Criteria NDPP Firewall with VPN and IPS			
High availability	Active/Passive with stateful synchronization			

Hardware	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Power supply	2x350W	2x350W	2x350W	Dual, Redundant, 1,200W
Fans	3 (removable)	3 (removable)	3 (removable)	10
Redundant Power Supply	100-240 VAC, 50-60 Hz			
Maximum power consumption (W)	155.3	155.3	181.2	834.4
Total heat dissipation	529.57 BTU	529.57 BTU	617.89 BTU	2845.3 BTU
Form factor	1U Rack Mountable	1U Rack Mountable	1U Rack Mountable	2U Rack Mountable
Dimensions	43 x 46 x 4.5 (cm) 16.9 x 18.1 x 1.8 in	43 x 46 x 4.5 (cm) 16.9 x 18.1 x 1.8 in	43 x 46 x 4.5 (cm) 16.9 x 18.1 x 1.8 in	68.6 x 43.8 x 8.8 (cm)
Weight	9.1 Kg	9.1 Kg	9.1 Kg	26 Kg
WEEE weight	11 Kg	11 Kg	11 Kg	30.1 Kg
Shipping weight	14.9 Kg	14.9 Kg	14.9 Kg	37.3 Kg
Environment (Operating/Storage)	32°-105° F (0°-40° C)/-40° to 158° F (-40° to 70° C)			
Humidity	0-90% R.H non-condensing	0-90% R.H non-condensing	0-90% R.H non-condensing	10-95% non-condensing

Regulatory	NS*sp* 10700	NS*sp* 11700	NS*sp* 13700	NS*sp* 15700
Regulatory model numbers	1RK54-118	1RK54-119	1RK54-118	2RK05-0FE
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	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	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	FCC Class A, ICES Class A, CE (EMC Class A, LVD, RoHS), C-Tick, VCCI Class A, MSIP/ KCC Class A, UL, cUL, TUV/GS, CB, Mexico UL DGN notification, WEEE, REACH, ANATEL, BSMI

[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/GatewayAV/Anti-Spyware/IPS throughput measured using industry standard Keysight HTTP performance 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.

[3] VPN throughput measured with UDP traffic using 1418 byte packet size AESGMAC16-256 Encryption adhering to RFC 2544. All specifications, features and availability are subject to change.

SonicOSX and SonicOS feature summary

Firewall

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

Unified Security Policy

- Unified Policy combines Layer 4 to Layer 7 rules:
  - Source/Destination IP/Port/Service
  - Application Control
  - CFS/Web Filtering
  - Single Pass Security Services enforcement
  - IPS/GAV/AS/Capture ATP
- Rule management:
  - Cloning
  - Shadow rule analysis
  - In-cell editing
  - Group editing
- Managing views
  - Used/un-used rules
  - Active/in-active rules
  - Sections

TLS/SSL/SSH decryption and inspection

- TLS 1.3
- Deep packet inspection for TLS/SSL/SSH
- Inclusion/exclusion of objects, groups or hostnames
- SSL control
- Granular DPI-SSL controls per zone or rule
- Decryption Policies for SSL/TLS and SSH

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 integration

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 antivirus
- 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
- 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

- Multi-instance firewall (only on NS*sp* 15700)
- PortShield
- Jumbo frames
- Path MTU discovery
- Enhanced logging
- VLAN trunking
- Port mirroring
- Layer-2 QoS
- Port security
- Dynamic routing (RIP/OSPF/BGP)
- Policy-based routing (ToS/metric and ECMP)
- NAT
- DHCP server
- Bandwidth management
- Link aggregation (static and dynamic)
- Port redundancy
- A/P high availability with state sync
- Inbound/outbound load balancing
- High availability - Active/Standby with state sync
- Wire/virtual wire mode, tap mode, NAT mode
- Asymmetric routing

VoIP

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

Management and monitoring

- Web GUI
- Command line interface (CLI)
- Zero-Touch registration & provisioning
- Rest API
- SonicExpress mobile app support

Management and monitoring cont'd

- SNMPv2/v3
- Centralized management and reporting with SonicWall Network Security Manager (NSM)[1]
- Logging
- Netflow/IPFix exporting
- Cloud-based configuration backup
- Application and bandwidth visualization
- IPv4 and IPv6 management

[1] Requires added subscription

Find the right SonicWall firewall for your enterprise

www.sonicwall.com/firewalls

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

SONICWALL

Datasheet-NSsp-US-JK-9465