

Request for Proposal

**Talbot County Public Schools
12 Magnolia St.
Easton, Maryland 21601
Phone 410-822-0330
Fax 410-820-4260**

District Firewall/Router Appliance Talbot County Public Schools Data Center

CONTACT: Steve Wilson
PHONE: 410-822-0330, EXT 128
Email: swilson@talbotschools.org

Minority Business Enterprises (MBE's) are encouraged to participate.

The Talbot County Public Schools reserves the right to waive any informality in, or to reject, any or all proposals.

The Talbot County Public Schools does not discriminate in admissions, access, treatment, or employment in its programs and activities on the basis of race, sex, age, color, national origin, religion, disability, sexual orientation or other basis prohibited by law. Appropriate accommodations for individuals with disabilities will be provided upon request.

By order of Talbot County Public Schools

Dr. Sharon Pepukayi
Superintendent of Schools

Talbot County Public Schools
12 Magnolia St.
Easton, Maryland 21601
Phone 410-822-0330
Fax 410-820-4260

Request for Proposal

Firewall/Router Appliance	
RFP Number	24-0110
RFP Contact Information	Stephen Wilson, IT Director swilson@talbotschools.org
RFP Release Date	January 12, 2024
RFP Documents	Maryland e-Market place eMMA https://emma.maryland.gov/page.aspx/en/rfp/request_browse_public TCPS Website http://www.tcps.k12.md.us/index.php/departments/technology/technology-request-proposals Emailed by request- Contact Steve Wilson - swilson@talbotschools.org
Last date to email questions	February 7, 2024 Email questions to Steve Wilson swilson@talbotschools.org Subject Line Q&A RFP 24-0110
Final question response	February 9, 2024
RFP closing Date – Time and Opening	February 14, 2024 - 2:30 PM E.S.T - Public opening Talbot County Education Center 12 Magnolia St. Easton, MD 21601
Submission Requirements	1) Sealed Bid 2 copies marked "Proposal for RFP 24-0110 – "Firewall/Router Appliance" 2) Emailed to swilson@talbotschools.org - Subject Line must read "Proposal for RFP 24-0110" emails will be opened and printed just prior to RFP closing time.
RFP Selection	Prior to USAC form 471 filing date
Award of contract	Contingent upon Talbot County Board of Education approval and funding and on E-Rate funding approval
Contract Start date	July 1, 2024
Contract End Date	June 30, 2025

RFP Description:

This RFP is for new Network Firewall/Router Appliance and warranty service to be delivered between July 1, 2024 and June 30, 2025. Talbot County Public Schools has standardized on Sonic Wall Products. TCPS will entertain proposed solutions from other manufacturers, it is the vendor's responsibility and obligation to provide documentation and other evidence that a non- SonicWall product is functionally equivalent or better. Equipment that is shown to be equivalent in function and warranty is acceptable. In the instance that the solution is non- SonicWall, proof of equal functionality must be shown. Failure to show equal functionality may result in the disqualification of the bid.

This project is subject to the approval of funds by the Talbot County Public Schools Board of Education, its funding agency, the Talbot County Council, and approval by the Universal Service Administrative Company (USAC) , Schools and Libraries Division (SLD). Any vendor to be considered for the award must be a SonicWall partner or equivalent statue is offering a substitute product and meet all the criteria as required by USAC/SLD. In the event of partial funding of this project, TCPS reserves the right to prioritize and purchase a partial amount of bid prices.

Included in this RFP is a complete description of the proposed equipment, part numbers, extended warranties , and installation location. List all equipment and software proposed to include model numbers, version numbers, etc. All equipment should be priced FOB Talbot County Education Center, 12 Magnolia Street Easton MD 21601, and is subject to approval by TCPS.

In addition to the USAC/SLD websites, RFP notices will be posted in the Talbot County Public Schools' Website and available at the Talbot County Public Schools' Central Office and posted on the Maryland eMarketPlace (eMMA).

All questions or requests for RFP interpretation shall be submitted in writing via email to Steve Wilson swilson@talbotschools.org

All bidders shall be registered as a service provider with the Universal Service Administrative Company–School and Libraries Division (USAC-SLD) for the E-Rate Program. Bidders agree to comply with all requirements of the E-Rate Program for service providers. All bidders shall furnish their Service Provider Identification Number (SPIN) on their bid form. Minority Business Enterprises are encouraged to participate.

Talbot County Public Schools reserves the right to waive any informality in, or to reject any and all bids.

Talbot County Public Schools reserves the right to award the contract (subject to funding) to the vendor who offers the best solution in the sole opinion of the school system.

Talbot County Public Schools reserves the right to terminate a contract for failure to comply with the terms of the contract.

The Form 472 Billed Entity Applicant Reimbursement or BEAR method of reimbursement will be utilized for reimbursement of eligible E-Rate funds. Service provider shall invoice the full amount and the Board of Education will apply for the E-Rate discount. The service provider is responsible for stating the eligibility percentage of all products or services to be offered on the Bid Form. These eligibility percentages will be used by the applicant on the Form 471.

Depending on the products and/or services offered the applicant may elect to use the Form 474 Service Provider Invoice (SPI) method. Using this method the service provider will invoice the applicant for only the non-discount portion of the cost as shown on the Funding Commitment Decision Letter (FCDL). The service

provider may then file a Form 474 for reimbursement from USAC for the discount portion of the cost as also shown on the FCDL. Whichever method is used, the service provider is responsible for stating the eligibility percentage of all products or services to be offered on the Bid Form. These eligibility percentages will be used by the applicant on the Form 471. The service provider will be notified of the reimbursement method to be used when the purchase order is issued.

If the service provider intends for there to be a contract for the services being bid, then a copy of the contract signed by the bidder shall be submitted with the bid. The contract shall also include a signature line for approval by the bidding entity.

If your bid includes any item for which either the manufacturer or USAC have determined E-Rate funding eligibility, then you must list the part number/SKU of the item, its E-Rate eligibility percentage, and the source of the eligibility determination. Include this documentation with your bid submission.

Attach to the Bid a complete description of the proposed equipment including performance specifications, proposed technological solutions, equipment, warranties, etc. List all equipment and software proposed to include description, SKU, cost, model numbers, version numbers, etc. All equipment and services are subject to approval by TCPS. Service provider shall identify any specific services, components or costs that are not eligible for E-Rate funding. **Any components or services not eligible for E-Rate funding must be cost allocated separately on the Bid Form.**

Service provider shall identify on the Bid Form which products and/or services are eligible for E-Rate funding in either Category 2 Internal Connections or in Category 2 Basic Maintenance of Internal Connections, including their percentage of E-Rate eligibility. See the Bid Form.

On the bid form itemize all equipment/services including all accessories included in the bid if these are prices as separate items. For example: cables, optical receivers, fan units, configuration, licenses, installation, power supplies, etc.

A manufacturer's multi-year warranty for a period of five years that is provided as an integral part of an eligible component, as a separately identifiable cost, or included in the cost of the component. If your bid includes any such warranty, provide a detailed description.

List separately support and service costs that are identified as E-Rate eligible Category 2 Basic Maintenance of Internal Connections. Contract term for eligible support services shall be for a term of five years to begin July 1, 2024.

Any bid containing pricing for Basic Maintenance of Internal Connections (BCIM) shall cross reference the specific equipment, building location, and term of service (beginning and end dates).

The Talbot County Public Schools does not discriminate in admissions, access, treatment, or employment in its programs and activities on the basis of race, sex, age, color, national origin, religion, disability, sexual orientation or other basis prohibited by law. Appropriate accommodations for individuals with disabilities will be provided upon request.

Limited Lifetime Warranty: All proposed products and software will be covered by a lifetime warranty until the product support end date. Specify if this service is not available for this location. Software support: defect repairs and software maintenance upgrades will be available at no charge through the product end of support date.

Check one of the following:

() The warranty described above is normally provided to the products proposed at no additional charge and is available to this location; 12 Magnolia St., Easton Md 21601

() An equivalent warranty described above is normally offered at an additional charge. The charge is provided above at a rate to cover a five-year period and is available to this location; 12 Magnolia St., Easton Md 21601. A copy of that Service Level Agreement (SLA) and part number is enclosed.

Talbot County Public School's Data Centers serving all schools

IC = Internal Connections
BMIC = Basic Maintenance of IC

Part Number (or Equivalent)	Description	Qty	Unit	Ext	Percent E-Rate Eligible	
					as IC	BMIC
02-SSC-1719	SONICWALL NSSP 11700 HIGH AVAILABILITY	1				
02-SSC-8399	SONICWALL NSSP 11700	1				
02-SSC-1605	ESSENTIAL PROTECTION SERVICE SUITE FOR NSSP 11700 5YR	1				

Total \$ _____

My company, _____ is an Authorized Reseller of Sonicwall products (or the alternative products proposed) and have a Service Provider Application Number (SPIN).

Authorized Signature _____ Date _____

_____ Email _____

Name Printed

_____ Phone _____ Ext _____

Name of Company

_____ Company Address

USAC Service Provider Identification Number (SPIN) _____

Cost of E-Rate ineligible items or services, if any (attach detailed list): \$ _____

Total project cost for all parts, materials, services, FOB 12 Magnolia St., Easton Md 21601 \$ _____

Product Data Sheet Attached



SonicWall Gen 7 NSsp Series

The SonicWall Network Security services platform™ (NSsp) 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 NSsp Series

- High port density
- 100 GbE ports
- Integrates with on-prem and cloud-based sandboxing
- Intuitive user interface with central management
- DNS security
- Reputation-based Content Filtering Service (CFS 5.0)
- Wi-Fi 6 firewall management
- Network access control integration with Aruba ClearPass
- 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



NSsp Spec Preview. [View full specs »](#)

100 GbE

Ports

Up to 100 Gbps

Firewall inspection throughput

40M

Max Connections (NSsp 15700)

Learn more about SonicWall Gen 7 NSsp Series:

sonicwall.com/NSsp

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 NSsp firewall's multiple 100G/40G/25G/10G interfaces allow you to process several million simultaneous encrypted and unencrypted connections with unparalleled 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 NSsp 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
- NSsp 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 patented 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 NSsp 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 NSsp 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
- NSsp integrates with Capture Security appliance to detect and block unknown threats with on-premises sandboxing that 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.
- Reputation-based Content Filtering Service (CFS 5.0) lets you enforce Internet use policies and control internal access to inappropriate, unproductive and potentially illegal web

content with comprehensive content filtering covering 93 web categories. Reputation-based content filtering provides a reputation score that forecasts the security risk of a URL.

Intrusion Prevention System (IPS)

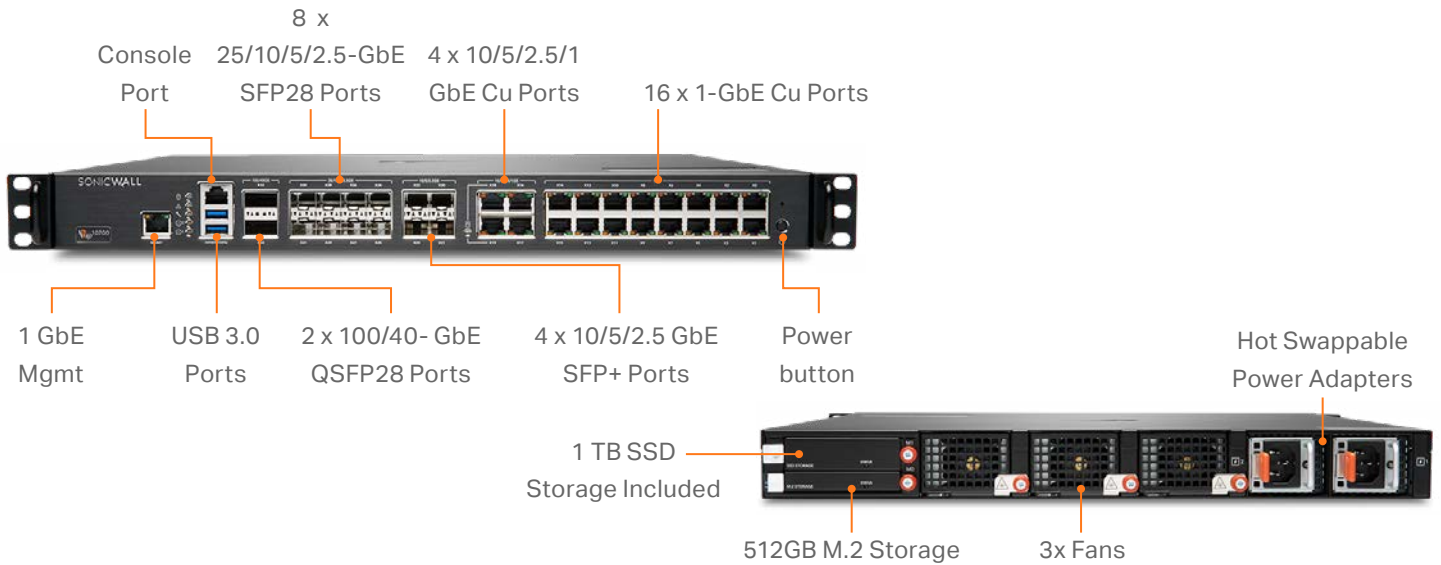
- Delivers a configurable, high performance Deep Packet Inspection engine for extended protection of key network services such as Web, e-mail, file transfer, Windows services and DNS

- 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)

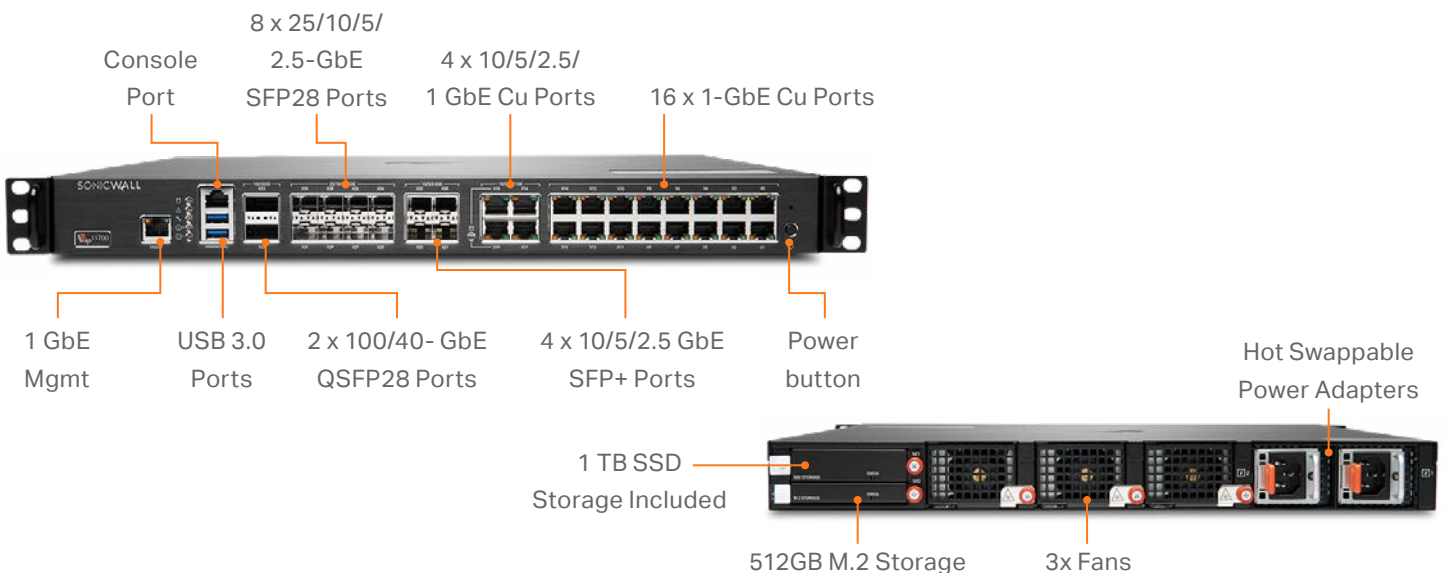
IoT and Application Control

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

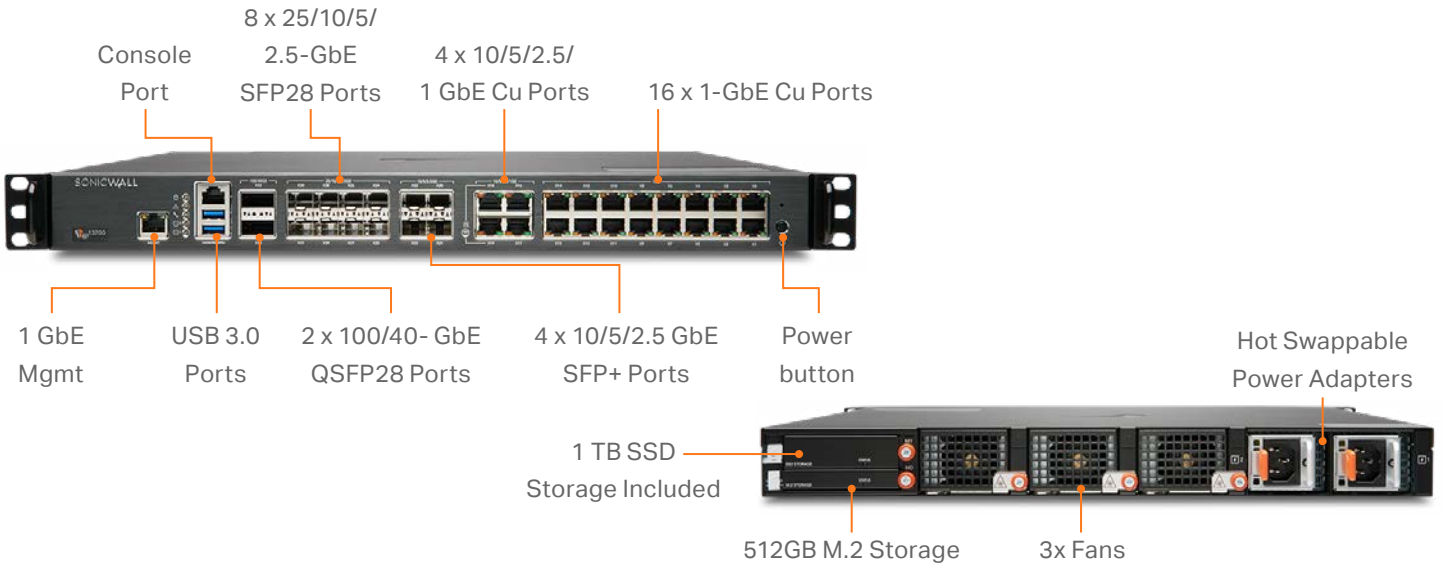
NSsp 10700



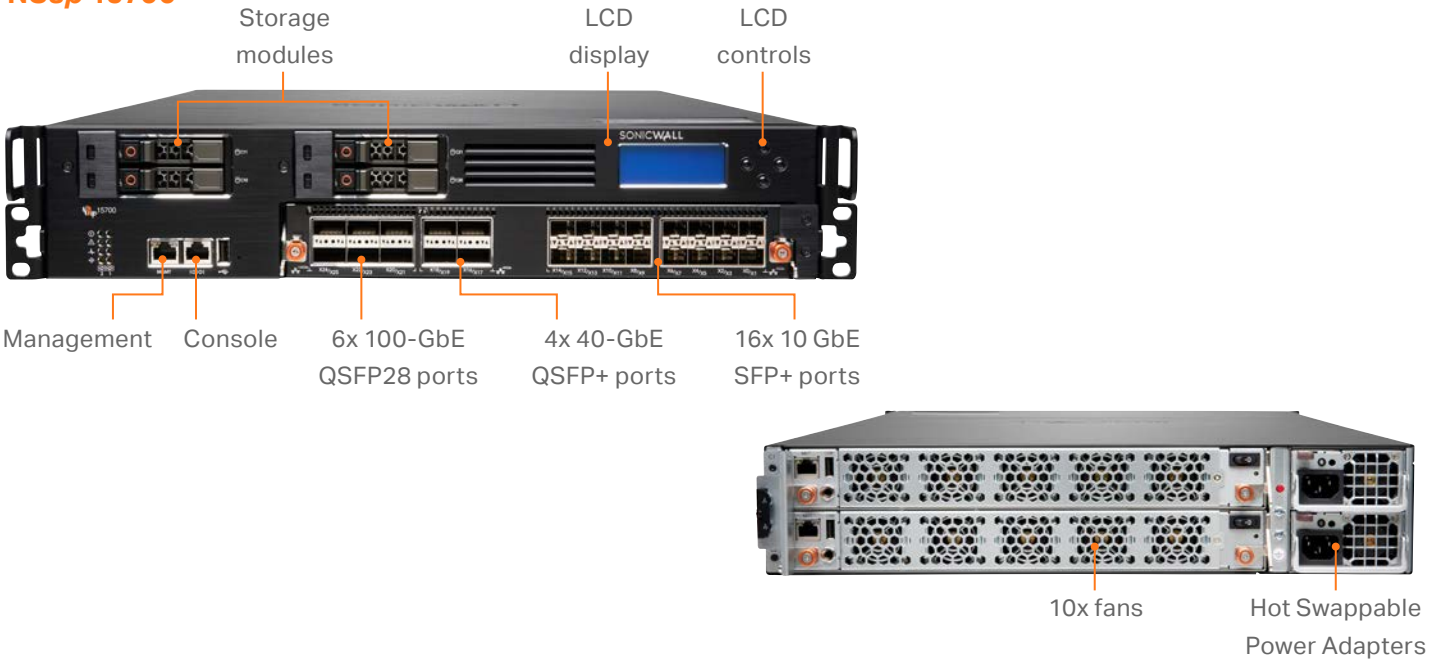
NSsp 11700



NSsp 13700



NSsp 15700



SonicWall NSsp Series specifications

Firewall General	NSsp 10700	NSsp 11700	NSsp 13700	NSsp 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	NSsp 10700	NSsp 11700	NSsp 13700	NSsp 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	NSsp 10700	NSsp 11700	NSsp 13700	NSsp 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	NSsp 10700	NSsp 11700	NSsp 13700	NSsp 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 NSsp Series specifications

Networking	NSsp 10700	NSsp 11700	NSsp 13700	NSsp 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	NSsp 10700	NSsp 11700	NSsp 13700	NSsp 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	NSsp 10700	NSsp 11700	NSsp 13700	NSsp 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
- SonicWall Wi-Fi 6 AP 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 protection¹

- 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 prevention¹

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

Anti-malware¹

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

Application identification¹

- 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 filtering¹

- URL filtering
- Proxy avoidance
- Keyword blocking
- Reputation-based Content Filtering Service (CFS 5.0)
- DNS filtering

- 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 NSsp 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 cont'd

Management and monitoring

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

© 2023 SonicWall Inc. ALL RIGHTS RESERVED.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners. The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products. Except as set forth in the terms and conditions as specified in the license agreement for this product, SonicWall and/or its affiliates assume no liability whatsoever and disclaims any express, implied or statutory warranty relating to its products including, but not limited to, the implied warranty of merchantability, fitness for a particular purpose, or non-infringement. In no event shall SonicWall and/or its affiliates be liable for any direct, indirect, consequential, punitive, special or incidental damages (including, without limitation, damages for loss of profits, business interruption or loss of information) arising out of the use or inability to use this document, even if SonicWall and/or its affiliates have been advised of the possibility of such damages. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.