Request for Proposal

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

Request for Proposals
Firewall Network Security Appliances

Proposal Posting Date: 1/24/2025
Proposal Due Date: 2/24/2025 3:30 p.m.

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

Sharon M. Pepukayi Ed.D.
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 Network Security Appliances	
RFP Number	25-0124
RFP Contact Information	Stephen Wilson, Director, Information Technology swilson@talbotschools.org
RFP Release Date	January 24, 2025
RFP Documents	Maryland e-Market place https://emaryland.buyspeed.com/bso/ Talbot County Public Schools http://www.tcps.k12.md.us/departments/Technology
Last date to email questions	February 18, 2025 Email questions to Steve Wilson swilson@talbotschools.org Subject Line Q&A RFP 25- 0124
Final question response	February 19, 2025
RFP closing Date – Time and Opening	February 24, 2025 3:30 PM E.S.T No RFPs will be accepted after this time
RFP Delivery	All submissions be will be e-filed to TCPSfinance@talbotschools.org or the eMaryland Marketplace (Emma) dropbox
RFP Selection	Prior to USAC form 471 filing date
Award of contract	Contingent upon 1) TCPS BOE RFP approval March 19, 2025 2) Talbot County Budget funding approval May 30, 2025 3) USAC/SLD Funding approval June 2025 (approximately
Contract Start date	July 1, 2025
Contract End Date	June 30, 2026

RFP Description:

This RFP is for new Network Firewall Appliances and warranty service to be delivered between July 1, 2025 and June 30, 2026. 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, it's 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 Sonic Wall partner or equivalent status for the proposed products and services 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.

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 applicant intends that the Form 472 Billed Entity Applicant Reimbursement (BEAR) method for reimbursement will be utilized of eligible Category 2 E-Rate funds. If the Form 472 BEAR method is selected the service provider will be notified when the purchase order is issued. If not specifically stated on the purchase order, the applicant shall utilize the Form 474 SPI method.

Under some circumstances the applicant may elect to use the Form 474 Service Provider Invoice (SPI) method for reimbursement of eligible Category 2 E-Rate funds. Service provider shall invoice the applicant for only the

non-discount portion of the cost as indicated 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 indicated on the FCDL.

Whichever reimbursement 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. This provision is a condition of your bid submission and cannot be modified, changed, or nullified by any statement or language in your bid, service agreement, or contract.

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 up to three years that is provided as an integral part of an eligible component, without a separately identifiable cost, may be 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 minimum of one year to begin July 1, 2025. However, the Board will consider awarding the contract for multiple years up to a 5-year term.

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).

Evaluation

70% Price of the eligible products and services
15% Price of ineligible products, services, and fees
15% Prior experience with the vendor

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

Tilghman Elementary

Percent E-Rate Eligible____%

		Total Price	IC	BMIC
1	SONICWALL NSa 2700, Hardware only Part Number 02-SSC-4324 or equivalent			
1	24x7 SUPPORT FOR NSa 2700 SERIES 5YR Part Number 02-SSC-8132 or equivalent			

Building Total $_____

White Marsh Elementary

Percent E-Rate Eligible____%

		Total Price	IC	BMIC
1	SONICWALL NSa 2700, Hardware only Part Number 02-SSC-4324 or equivalent			
1	24x7 SUPPORT FOR NSa 2700 SERIES 5YR Part Number 02-SSC-8132 or equivalent			

Building Total $_____

Chapel District Elementary

Percent E-Rate Eligible____%

		Total Price	IC	BMIC
1	SONICWALL NSa 2700, Hardware only Part Number 02-SSC-4324 or equivalent			
1	24x7 SUPPORT FOR NSa 2700 SERIES 5YR Part Number 02-SSC-8132 or equivalent			

Building Total $_____

Easton Middle School

Percent E-Rate Eligible____%

		Total Price	IC	BMIC
1	SONICWALL NSA 4700, Hardware Only, Part Number 02-SSC-4328 or equivalent			
1	24X7 SUPPORT FOR NSA 4700 5YR, Part Number 02-SSC-9184 or equivalent			

Building Total $_____

Easton High School

Percent E-Rate Eligible____%

		Total Price	IC	BMIC
1	SONICWALL NSA 5700, Hardware Only Part Number 02-SSC-4330 or equivalent			
1	24X7 SUPPORT FOR NSA 5700 5YR Part Number 02-SSC-9898 or equivalent			

Building Total $_____

Easton Elementary School

Percent E-Rate Eligible____%

		Total Price	IC	BMIC
1	SONICWALL NSA 5700, Hardware Only Part Number 02-SSC-4330 or equivalent			
1	24X7 SUPPORT FOR NSA 5700 5YR Part Number 02-SSC-9898 or equivalent			

Building Total $_____

St. Michaels Middle High & Elementary School (Campus School)

Percent E-Rate Eligible____%

		Total Price	IC	BMIC
1	SONICWALL NSA 4700, Hardware Only, Part Number 02-SSC-4328 or equivalent			
1	24X7 SUPPORT FOR NSA 4700 5YR Part Number 02-SSC-9184 or equivalent			

Building Total $_____

Talbot County Public School's Education Center serving all schools

Percent E-Rate Eligible____%

		Total Price	IC	BMIC
1	SONICWALL NSA 6700, Hardware Only Part Number 02-SSC-4332 or equivalent			
1	24X7 SUPPORT FOR NSA 6700 5YR Part Number 02-SSC-9269 or equivalent			

Building 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

Contract Affidavit

A. AUTHORITY

I HEREBY AFFIRM THAT: I, _____ (name of affiant) am the _____ (title) and duly authorized representative of _____ (Contractor name) and that I possess the legal authority to make this affidavit on behalf of the business for which I am acting.

B. CERTIFICATION OF REGISTRATION OR QUALIFICATION WITH THE STATE DEPARTMENT OF ASSESSMENTS AND TAXATION

I FURTHER AFFIRM THAT:
The business named above is a (check applicable items):
(1) Corporation: ___ domestic or ___ foreign;
(2) Limited Liability Company: ___ domestic or ___ foreign;
(3) Partnership: ___ domestic or ___ foreign;
(4) Statutory Trust: ___ domestic or ___ foreign;
(5) ___ Sole Proprietorship
and is registered or qualified as required under Maryland Law.

I further affirm that the above business is in good standing both in Maryland and (IF APPLICABLE) in the jurisdiction where it is presently organized, and has filed all its annual reports, together with filing fees, with the Maryland State Department of Assessments and Taxation. The name and address of its resident agent (IF APPLICABLE) filed with the State Department of Assessments and Taxation is:
Name and Department ID
Number:_____ Address:_____
and that if it does business under a trade name, it has filed a certificate with the State Department of Assessments and Taxation that correctly identifies that true name and address of the principal or owner.

C. EMPLOYMENT OF SEX OFFENDERS AND OTHER CRIMINAL OFFENDERS

I further affirm that I am aware of, and the above business will comply with, the following requirements of Section 11-722 of the Criminal Procedure Article, and Section 6-113 of the Education Article, Annotated Code of Maryland:

Maryland Law requires sex offenders to register with the State and with the local law enforcement agency in the county in which they will reside, work, or attend school. A TCPS contractor may not knowingly employ an individual to work at a school if the individual is a registrant. A contractor violating this Law is guilty of a misdemeanor and may be subject to imprisonment not exceeding five years or a fine not exceeding $5,000, or both.

See *Section 11-722 of the Criminal Procedure Article, Annotated Code of Maryland.*

A TCPS contractor or subcontractor may not knowingly assign an employee to work on school premises with direct, unsupervised, and uncontrolled access to children, if the employee has been convicted of:

1) Section 3-307 of the Criminal Law Article, Maryland Annotated Code, *Sexual Offense in the Third Degree*;
2) Section 3-308 of the Criminal Law Article, Maryland Annotated Code, *Sexual Offense in the Fourth Degree*;
3) An offense under the laws of another state that would constitute a violation of Sections 3-307 or 3-308 of the Criminal Law Article if committed in Maryland;
4) Child sexual abuse under Section 3-602 of the Criminal Law Article, Annotated Code of Maryland;
5) An offense under the laws of another state that would constitute child sexual abuse under Section 3-602 of the Criminal Law Article if committed in Maryland;

6) A crime of violence as defined in Section 14-101 of the Criminal Law Article, Annotated Code of Maryland; or

7) An offense under the laws of another state that would constitute a crime of violence under Section 14-101 of the Criminal Law Article if committed in Maryland.

See Section 6-113 of the Education Article, Annotated Code of Maryland

D. CONTRACTOR SCREENING OF EMPLOYMENT APPLICANTS HAVING DIRECT CONTACT WITH MINORS (if applicable)

In addition to the requirements of Section C above, Contractor shall comply with the requirements of Section 6-113.2 of the Education Article, Maryland Annotated Code, regarding screening of applicants for employment.

E. AFFIRMATION REGARDING BRIBERY CONVICTIONS

I further affirm, neither I or to the best of my knowledge, the above firm, nor any of its officers, directors, or partners, or any of its employees directly involved in obtaining contracts with the State or any County, bi-County, or multi-County agency, or subdivision of the State have been convicted of, or have pleaded nolo contendere to a charge of, or have during the course of any official investigation or other proceeding admitted in writing or under oath, acts or omissions committed after July 1, 1977 which constitute bribery, attempted bribery, or conspiracy to bribe under the provisions of Article 27 of the Annotated Code of Maryland or under the laws of any other State or the Federal government.

F. AFFIRMATION REGARDING COLLUSION

I further affirm that neither I nor, to the best of my knowledge, information and belief, the above business has:

1) Agreed, conspired, connived or colluded to produce a deceptive show of competition in the compilation of the accompanying bid or offer that is being submitted; or,
2) In any manner, directly or indirectly, entered into any agreement of any kind to fix the bid/ proposal price of the bidder/offeror of any competitor, or otherwise taken any action in restraint of free competitive bidding in connection with the contract for which the accompanying bid or offer is submitted.

G. AFFIRMATION REGARDING DEBARMENT

I further affirm that neither I nor, to the best of my knowledge, information and belief, the above business, or any of its officers, directors, partners, or any of its employees directly involved in obtaining contracts with public bodies, has ever been suspended or debarred (including being issued a limited denial of participation) by any public entity, except as follows (use a separate sheet to list each debarment or suspension, providing the dates of the suspension or debarment, the name of the public entity, the status of the proceedings, the name(s) and position of the parties involved, and all pertinent details).

I further affirm that (1) the business was not established and it does not operate in a manner designed to evade the application of or defeat the purpose of debarment pursuant to Section 16-101, et seq, of the State Finance and Procurement Article of the Annotated Code of Maryland; and, (2) the business is not a successor, assignee, subsidiary, or affiliate of a suspended or debarred business, except as follows (indicate the reasons why the affirmations cannot be given without qualification): _____

_____

_____

Violations of any of these provisions may result in immediate termination for cause.

I DO SOLEMNLY DECLARE AND AFFIRM UNDER THE PENALTIES OF PERJURY THAT THE CONTENTS OF THIS AFFIDAVIT ARE TRUE AND CORRECT TO THE BEST OF MY KNOWLEDGE, INFORMATION, AND BELIEF.

Date: _____

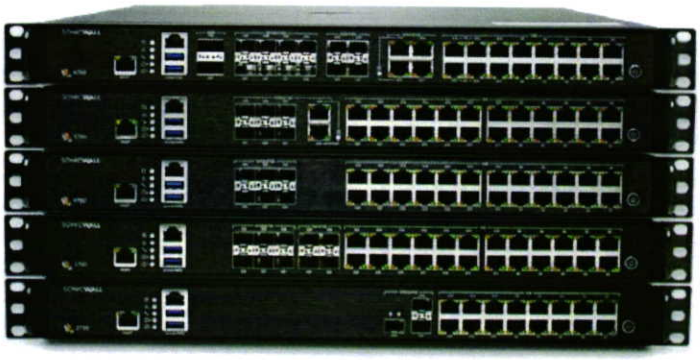
By: _____
(printed name of Authorized Representative and affiant)

_____
(signature of Authorized Representative and affiant)

SonicWall Gen 7 NSa Series

SonicWall Generation 7 (Gen 7) Network Security Appliance (NSa) next-generation firewalls (NGFWs) offers medium- to large-sized enterprises industry-leading performance at the lowest total cost of ownership in their class.

With comprehensive security features such as intrusion prevention, VPN, application control, malware analysis, URL filtering, DNS Security, Geo-IP and Bot-net services, it protects the perimeter from advanced threats without becoming a bottleneck.



Gen 7 NSa Series Spec Preview. View full specs »

Up to 19 Gbps	Up to 8 Million	40G/25G/10G/ 5G/2.5G/1G
Threat Prevention Throughput	Connections	Ports

HIGHLIGHTS

- 1 RU – Form Factor
- Support for 40G/25G/10G/5G/2.5G/1G ports
- Multi-gigabit Threat and Malware Analysis Throughput
- Superior TLS performance (sessions and throughput)
- Expandable storage
- DNS security
- Reputation-based Content Filtering Service (CFS 5.0)
- Wi-Fi 6 firewall management
- Network access control integration with Aruba ClearPass
- Enterprise Internet Edge Ready
- Latest Generation 7 SonicOS support
- Secure SD-WAN capability
- Intuitive user interface with central management
- TLS 1.3 support
- Best-in-class price-performance
- Powered by SonicWall Capture Labs threat research team
- High port density for easy networking
- SonicWall Switch, SonicWave Access Point and Capture Client integration
- Redundant power
- Cloud Secure Edge Connector Support

DATASHEET

Featuring a high port density including multiple 40 GbE and 10 GbE ports, the solution supports network and hardware redundancy with high availability, and dual power supplies.

SonicWall Generation 7 (Gen 7) Network Security Appliance (NS*a*) next-generation firewalls (NGFWs) offers medium- to large-sized enterprises industry-leading performance at the lowest total cost of ownership in their class.

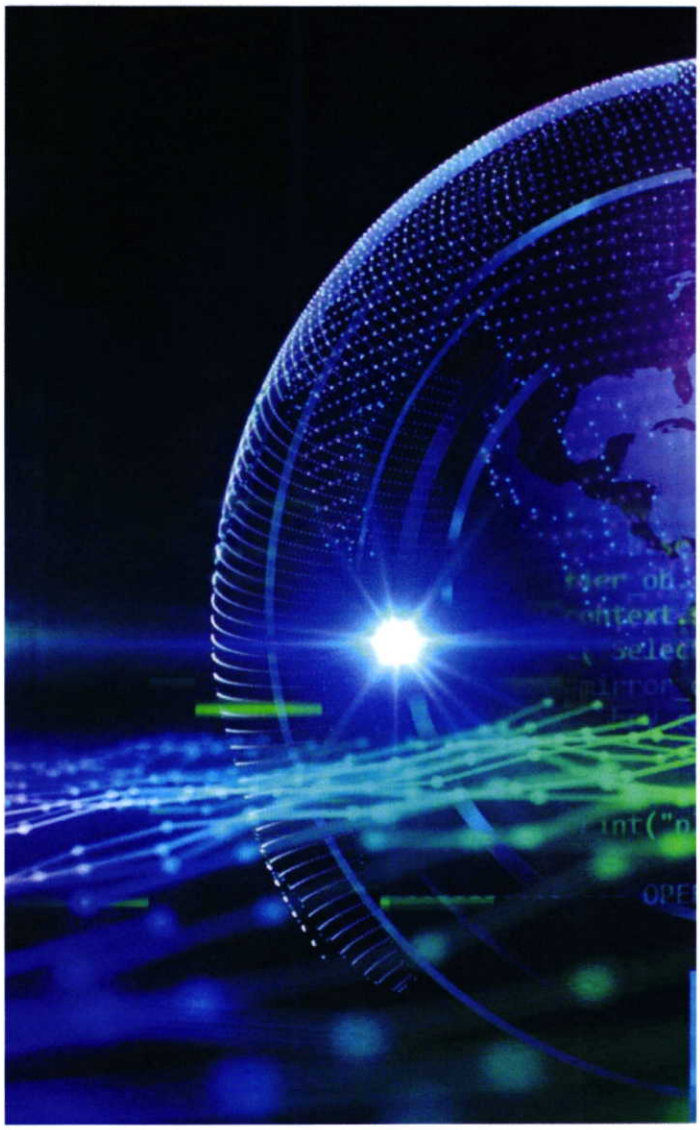
With comprehensive security features such as intrusion prevention, VPN, application control, malware analysis, URL filtering, DNS Security, Geo-IP and Bot-net services, it protects the perimeter from advanced threats without becoming a bottleneck.

The Gen 7 NS*a* Series has been built from the ground up with the latest hardware components, all designed to deliver multi-gigabit threat prevention throughput — even for encrypted traffic. Featuring a high port density including multiple 40 GbE and 10 GbE ports, the solution supports network and hardware redundancy with high availability, and dual power supplies.

Generation 7 – SonicOS 7 and Security Services

The Gen 7 NS*a* Series runs on SonicOS 7.0, a new operating system built from the ground up to deliver a modern user interface, intuitive workflows and user-first design principles. SonicOS 7 provides multiple features designed to facilitate enterprise-level workflows. It offers easy policy configuration, zero-touch deployment and flexible management — all of which allow enterprises to improve both their security and operational efficiency.

The Gen 7 NS*a* Series supports advanced networking features, such as SD-WAN, dynamic routing, layer 4-7 high-availability and high-speed VPN functionality. In addition to integrating firewall and switch capabilities, the appliance provides a single-pane-of-glass interface to manage both switches and access points.



Built to mitigate the advanced cyberattacks of today and tomorrow, the Gen 7 NS*a* Series offers access to SonicWall's advanced firewall security services, allowing you to protect your entire IT infrastructure. Solutions and services such as Cloud Application Security, Capture Advanced Threat Protection (ATP) cloud-based sandboxing, patented Real-Time Deep Memory Inspection (RTDMI™) and Reassembly-Free Deep Packet Inspection (RFDPI) — for all traffic including TLS 1.3 — offer comprehensive gateway protection from most stealthy and dangerous malware, including zero-day and encrypted threats.

Users can leverage a new Cloud Secure Edge Connector integration to provide a centralized and easy-to-manage option to provide secure access to their private applications. This approach ensures that user and device trust are repeatedly verified before granting access to specific applications, regardless of location and endpoint type.

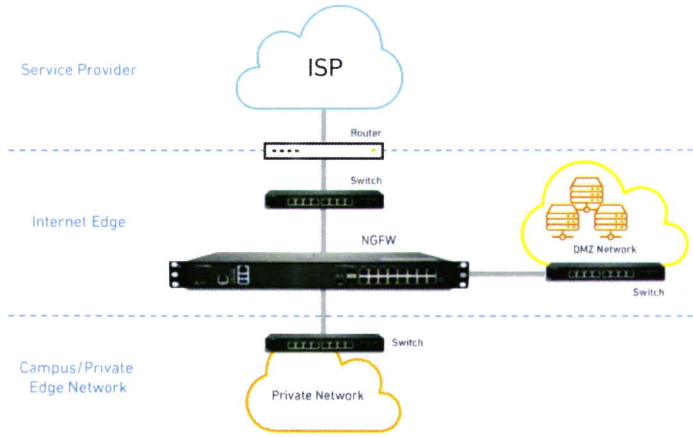
Deployments

The Gen 7 NS*a* Series has two main deployment options for medium and distributed enterprises:

Internet Edge Deployment

In this standard deployment option, the Gen 7 NS*a* Series NGFW protects private networks from malicious traffic coming from the internet, allowing you to:

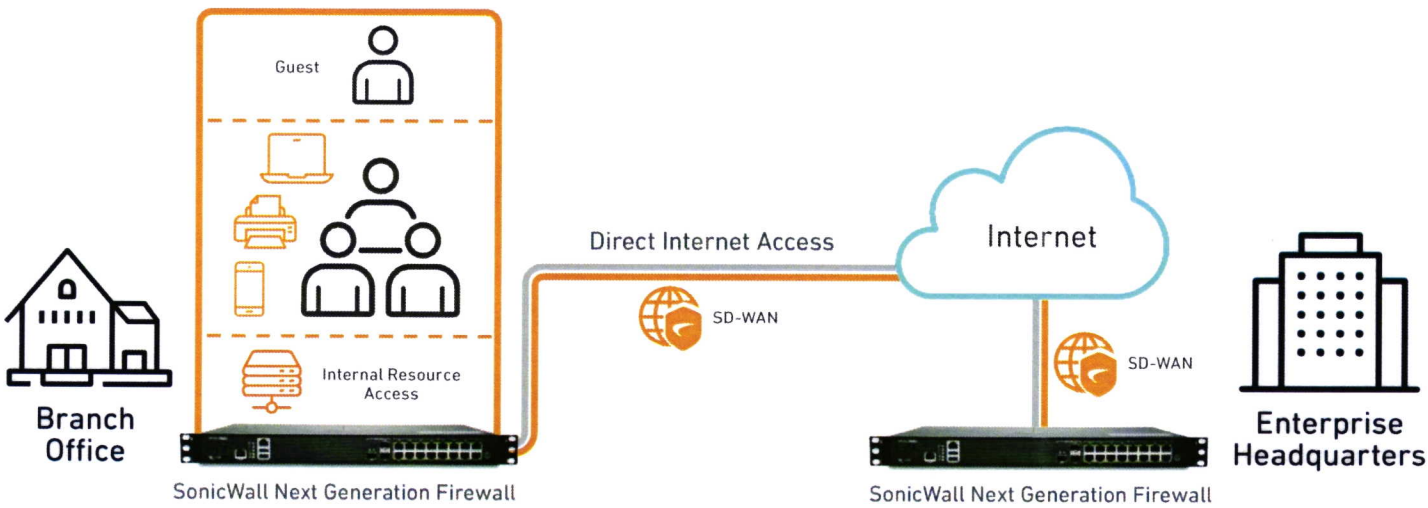
- Deploy a proven NGFW solution with highest performance and port density (including 40 GbE and 10 GbE connectivity) in its class
- Gain visibility and inspect encrypted traffic, including TLS 1.3, to block evasive threats coming from the Internet — all without compromising performance
- Protect your enterprise with integrated security, including malware analysis, cloud app security, URL filtering and reputation services
- Save space and money with an integrated NGFW solution that includes advanced security and networking capabilities
- Reduce complexity and maximize efficiency using a central management system delivered through an intuitive single-pane-of-glass user interface



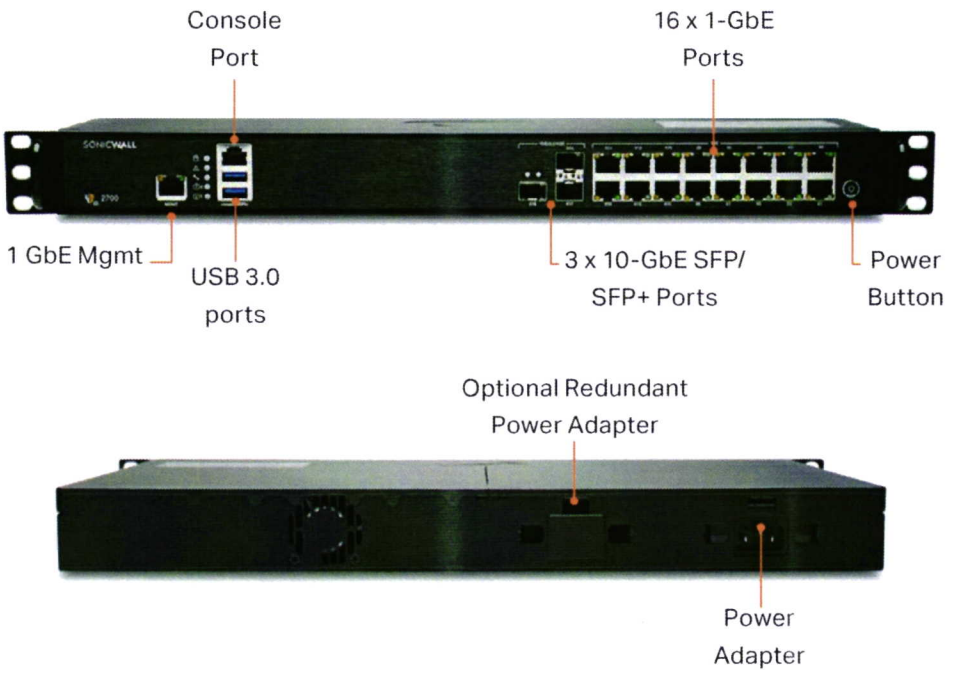
Medium and Distributed Enterprises

The SonicWall Gen 7 NS*a* Series supports SD-WAN and can be centrally managed, making it an ideal fit for medium and distributed enterprises. This deployment allows organizations to:

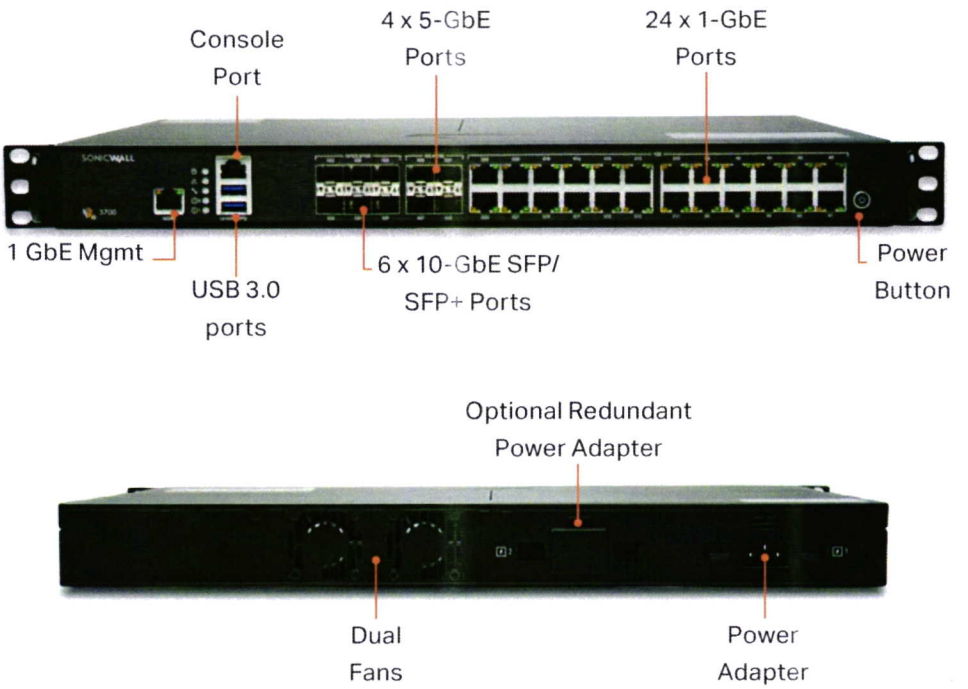
- Future-proof against an ever-changing threat landscape by investing in a NGFW with multi-gigabit threat analysis performance
- Provide direct and secure internet access to distributed branch offices instead of back-hauling through corporate headquarters
- Allow distributed branch offices to securely access internal resources in corporate headquarters or in a public cloud, significantly improving application latency
- Automatically block threats that use encrypted protocols such as TLS 1.3, securing networks from the most advanced attacks.
- Reduce complexity and maximize efficiency using a central management system delivered through an intuitive single pane of glass user interface
- Leverage high port density that includes 40 GbE and 10 GbE connectivity to support a distributed enterprise and wide area networks



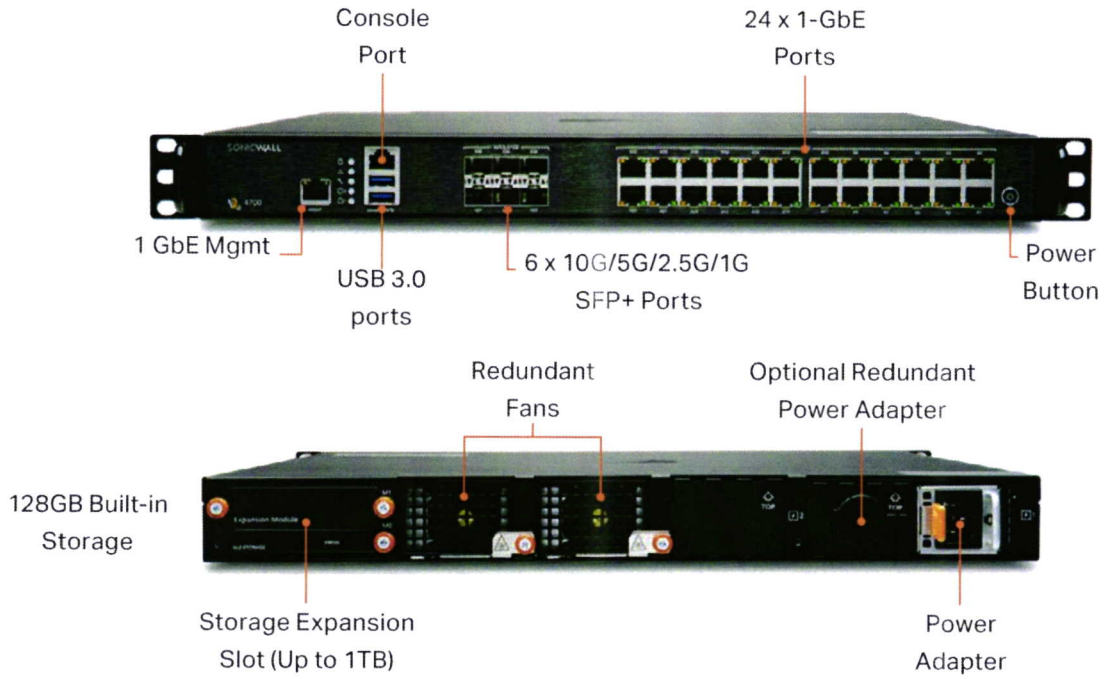
NS*a* 2700



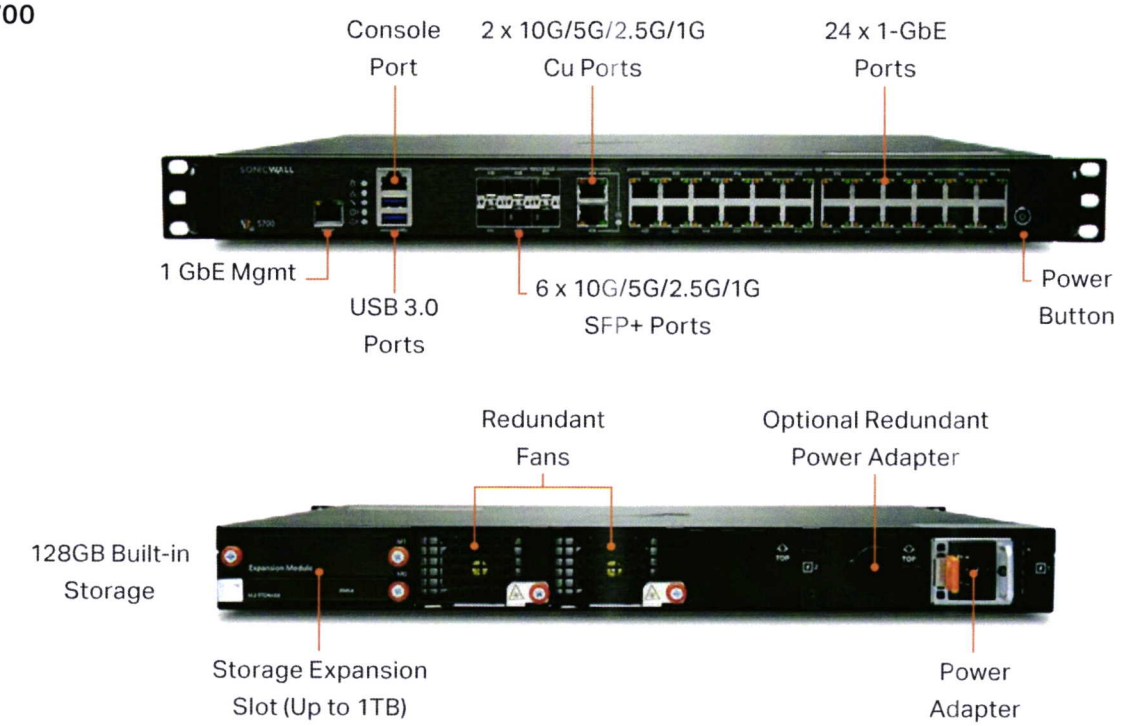
NS*a* 3700



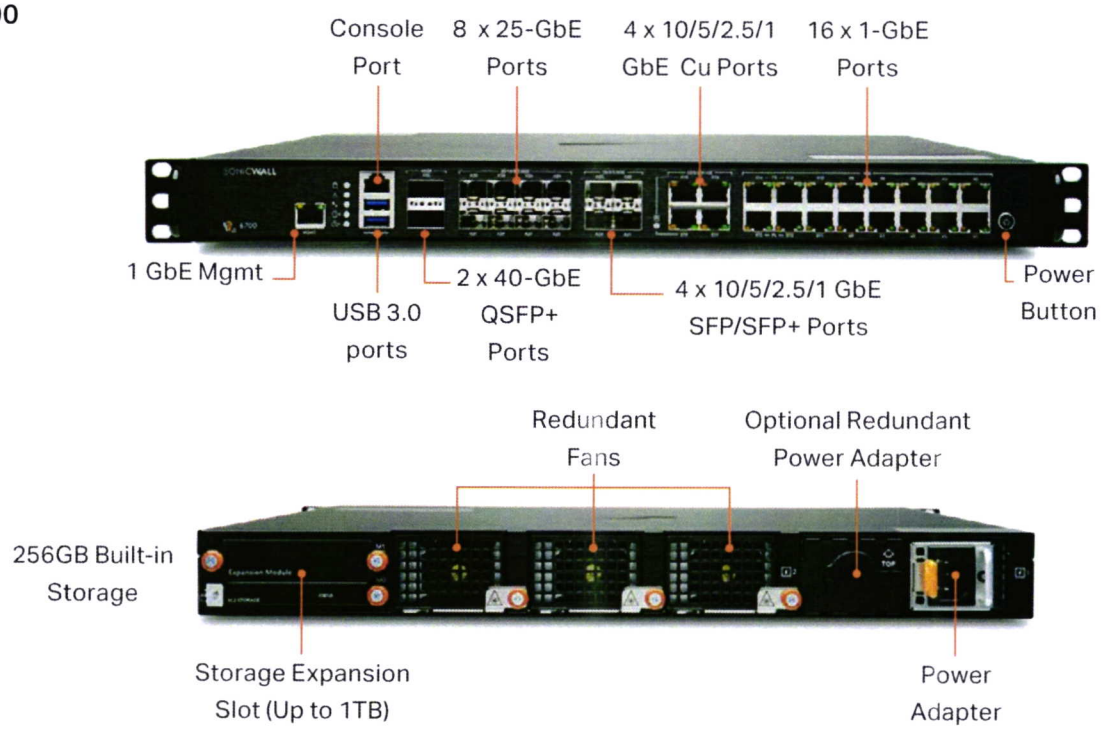
NSa 4700

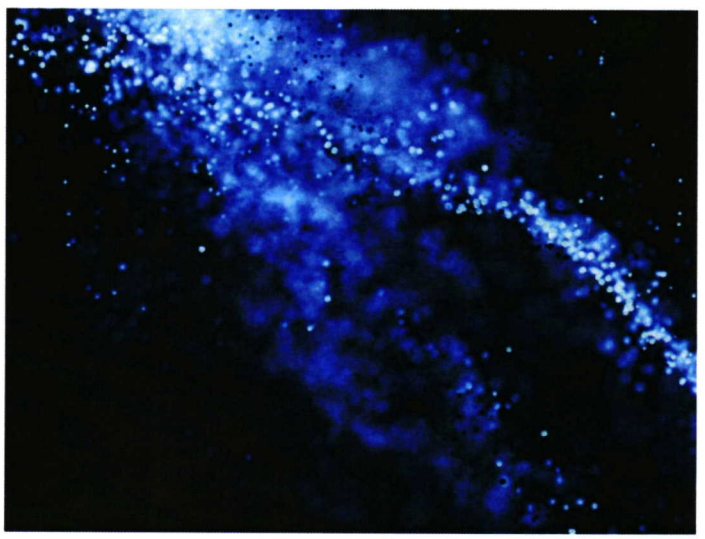


NSa 5700



NS*a* 6700





PARTNER ENABLED SERVICES

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

www.sonicwall.com/PES

Gen 7 NS*a* Series System Specifications

Firewall	NS*a* 2700	NS*a* 3700	NS*a* 4700	NS*a* 5700	NS*a* 6700
Operating system	SonicOS 7				
Interfaces	16x1GbE, 3x10G SFP+, 2 USB 3.0, 1 Console, 1 Mgmt. port	24x1GbE, 6x10G SFP+, 4x5G SFP+, 2 USB 3.0, 1 Console, 1 Mgmt. port	6 x 10G/5G/2.5G/1G (SFP+); 24 x 1GbE Cu 2 USB 3.0, 1 Console, 1 Mgmt. port	6 x 10G/5G/2.5G/1G (SFP+); 2x 10G/5G/2.5G/1G (Cu); 24 x 1GbE Cu 2 USB 3.0, 1 Console, 1 Mgmt. port	2x40G; 8x25G, 4 x10G/5G/2.5/1G SFP+, 4 x 10G/5G/2.5G/1G (Cu); 16 x 1GbE (Cu) 2 USB 3.0, 1 Console, 1 Mgmt. port
Storage	64GB M.2	128GB M.2	128GB	128GB	256GB M.2
Expansion	Storage Expansion Slot (Up to 256GB)	Storage Expansion Slot (Up to 256GB)	Storage Expansion Slot (Up to 1TB)	Storage Expansion Slot (Up to 1TB)	Storage Expansion Slot (Up to 1TB)
Logical VLAN and tunnel interfaces (maximum)	256	256	512	512	512
SSO Users	40,000	40,000	50,000	50,000	70,000
Access points supported (maximum)	512	512	512	512	512
Firewall/VPN Performance					
Firewall inspection throughput[1]	5.2 Gbps	5.5 Gbps	18 Gbps	28 Gbps	36 Gbps
Threat Prevention throughput[2]	3.0 Gbps	3.5 Gbps	9.5 Gbps	15 Gbps	19 Gbps
Application inspection throughput[2]	3.6 Gbps	4.2 Gbps	11 Gbps	18 Gbps	20 Gbps
IPS throughput[2]	3.4 Gbps	3.8 Gbps	10 Gbps	17 Gbps	20 Gbps
Anti-malware inspection throughput[2]	2.9 Gbps	3.5 Gbps	9.5 Gbps	16 Gbps	18.5 Gbps
TLS/SSL inspection and decryption throughput (DPI SSL)[2]	800 Mbps	850 Mbps	5 Gbps	7 Gbps	9 Gbps
IPSec VPN throughput[3]	2.10 Gbps	2.2 Gbps	11 Gbps	15 Gbps	19 Gbps
Connections per second	21,000	22,000	115,000	228,000	228,000
Maximum Connections (SPI)	1,500,000	2,000,000	4,000,000	5,000,000	8,000,000
MAX DPI-SSL Connections	125,000	150,000	350,000	350,000	750,000
Maximum connections (DPI)	500,000	750,000	2,000,000	3,500,000	6,000,000
VPN					
Site-to-site VPN tunnels	2,000	3,000	4,000	6,000	6,000
IPSec VPN clients (max)	50 (1000)	50 (1000)	500 (3000)	2000 (4000)	2000 (6000)
SSL VPN licenses (max)	2 (500)	2 (500)	2 (1000)	2 (1500)	2 (1500)
Encryption/Authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B Cryptography				
Key exchange	Diffie Hellman Groups 1, 2, 5, 14v				
Route-based VPN	RIP, OSPF, BGP				
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	Windows 10		Microsoft® Windows Vista 32/64-bit, Windows 7 32/64-bit, Windows 8.0 32/64-bit, Windows 8.1 32/64-bit, Windows 10		
NetExtender	Windows 10 and Linux		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, Android, Kindle Fire, Chrome OS, Windows 10		Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (Embedded)		
Security services					
Deep Packet Inspection services	Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, DPI SSL				
Content Filtering Service (CFS)	HTTP URL, HTTPS IP, keyword and content scanning, Comprehensive filtering based on file types such as ActiveX, Java, Cookies for privacy, allow/forbid lists				

SONICWALL

Gen 7 NSa Series System Specifications

Firewall	NSa 2700	NSa 3700	NSa 4700	NSa 5700	NSa 6700
Comprehensive Anti-Spam Service	Supported				
Application Visualization	Yes				
Application Control	Yes				
Capture Advanced Threat Protection	Yes				
Networking					
IP address assignment	Static (DHCP, PPPoE, L2TP and PPTP client), Internal DHCP server, DHCP relay				
NAT modes	1:1, 1:many, many:1, many:many, flexible NAT (overlapping IPs), PAT, transparent mode				
Routing protocols	BGP4, 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)				
Local user database	1000	1000	2500	2500	3200
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	Yes	Yes	Pending	Pending	Pending
Certifications	ICSA Enterprise Firewall, ICSA Antivirus, IPv6/USGv6				
Certifications (in process)	Common Criteria NDPP Firewall with VPN and IPS				
Common Access Card (CAC)	Supported				
High availability	Active/Passive with stateful synchronization				
Hardware					
Form factor	1U Rack Mountable				
Fans	1	2	2 (removable)	2 (removable)	3 (removable)
Power supply	60W	90W	350W	350W	350W
Maximum power consumption (W)	21.5	36.3	108.1	128.1	139.2
Redundant Power Supply	100-240 VAC, 50-60 Hz				
Total heat dissipation	73.32 BTU	123.78 BTU	368.62 BTU	436.82 BTU	474.67 BTU
Dimensions	43 x 32.5 x 4.5 (cm) 16.9 x 12.8 x 1.8 in	43 x 32.5 x 4.5 (cm) 16.9 x 12.8 x 1.8 in	43 x 46.5 x 4.5 (cm) 16.9 x 18.1 x 1.8 in	43 x 46.5 x 4.5 (cm) 16.9 x 18.1 x 1.8 in	43 x 46.5 x 4.5 (cm) 16.9 x 18.1 x 1.8 in
Weight	4.0 kg / 8.8 lbs	4.6 kg / 10.2 lbs	7.8 Kg	7.8 Kg	8.1 Kg
WEEE weight	4.2 kg / 9.3 lbs	4.8 kg / 10.6 lbs	9.6 Kg	9.6 Kg	9.9 Kg
Shipping weight	6.4 kg / 14.1 lbs	7 kg / 15.4lbs	13.5 Kg	13.5 Kg	13.8 Kg
Environment (Operating/Storage)	32°-105° F (0°-40° C)/-40° to 158° F (-40° to 70° C)				
Humidity	5-95% non-condensing	5-95% non-condensing	0-90% R.H non-condensing	0-90% R.H non-condensing	0-90% R.H non-condensing
Regulatory					
Regulatory model numbers	1RK51-109	1RK52-110	1RK53-115	1RK53-116	1RK54-118
Major regulatory compliance	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				

[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.

SONICWALL

SonicOS 7.0 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
- Full API support
- SonicWall Switch integration
- SonicWall Wi-Fi 6 AP integration
- SD-WAN scalability
- SD-WAN Usability Wizard[1]
- Connections scalability (SPI, DPI, DPI SSL)
- Enhanced dashboard[1]
- Enhanced device view
- Top traffic and user summary
- Insights to threats
- Notification center
- Cloud Secure Edge Connector

TLS/SSL/SSH decryption and inspection

- TLS 1.3 with enhanced security[1]
- Deep packet inspection for TLS/SSL/SSH
- Inclusion/exclusion of objects, groups or hostnames
- SSL control
- Enhancements for DPI-SSL with CFS
- Granular DPI SSL controls per zone or rule
- Capture advanced threat protection[2]
- Real-Time Deep Memory Inspection
- Cloud-based multi-engine analysis[2]
- Virtualized sandboxing
- Hypervisor level analysis
- Full system emulation
- Broad file type examination
- Automated and manual submission
- Real-time threat intelligence updates[2]
- Block until verdict
- Capture Client[2]

Intrusion prevention[2]

- 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-malware[2]

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

Application identification[2]

- 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[2]

- 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
- Unified policy model with app control
- Content Filtering Client

VPN

- Secure SD-WAN
- 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

- PortShield
- Jumbo frames
- Path MTU discovery
- Enhanced logging
- VLAN trunking
- Port mirroring (SonicWall Switch)
- Layer-2 QoS
- Port security
- Dynamic routing (RIP/OSPF/BGP)
- SonicWall wireless controller
- Policy-based routing (ToS/metric and ECMP)
- NAT
- DHCP server
- Bandwidth management
- A/P high availability with state sync
- Inbound/outbound load balancing
- High availability - Active/Standby with state sync
- L2 bridge, wire/virtual wire mode, tap mode, NAT mode
- Asymmetric routing
- Common Access Card (CAC) support

VoIP

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

Management, monitoring and support

- Capture Security Appliance (CSa) support
- Capture Threat Assessment (CTA) v2.0
- New design or template
- Industry and global average comparison
- New UI/UX, Intuitive feature layout[1]
- Dashboard
- Device information, application, threats
- Topology view

SONICWALL

SonicOS 7.0 Feature Summary cont'd

- Simplified policy creation and management
- Policy/Objects usage statistics[1]
- Used vs Un-used
- Active vs Inactive
- Global search for static data
- Storage support[1]

Management, monitoring and support cont'd

- Internal and external storage management[1]
- WWAN USB card support (5G/LTE/4G/3G)
- Network Security Manager (NSM) support
- Web GUI
- Command line interface (CLI)
- Zero-Touch registration & provisioning
- CSC Simple Reporting[1]
- SonicExpress mobile app support
- SNMPv2/v3
- Centralized management and reporting with SonicWall Global Management System (GMS)[2]
- API for reporting and analytics
- Logging
- Netflow/IPFix exporting
- Cloud-based configuration backup
- BlueCoat security analytics platform
- Application and bandwidth visualization
- IPv4 and IPv6 management
- CD management screen
- Dell N-Series and X-Series switch management including cascaded switches

Debugging and diagnostics

- Enhanced packet monitoring
- SSH terminal on UI

Wireless

- SonicWave AP cloud and firewall management
- WIDS/WIPS
- Rogue AP prevention
- Fast roaming (802.11k/r/v)
- 802.11s mesh networking
- Auto-channel selection
- RF spectrum analysis
- Floor plan view
- Topology view
- Band steering
- Beamforming
- AirTime fairness
- Bluetooth Low Energy
- MiFi extender
- RF enhancements and improvements
- Guest cyclic quota

[1] New feature, available on SonicOS 7.0
[2] Requires added subscription

Learn more about SonicWall Gen 7 NSa Series

www.sonicwall.com/products/firewalls

About SonicWall

SonicWall is a cybersecurity forerunner with more than 30 years of expertise and a relentless focus on its partners. With the ability to build, scale and manage security across the cloud, hybrid and traditional environments in real time, SonicWall can quickly and economically provide purpose-built security solutions to any organization around the world. Based on data from its own threat research center, SonicWall delivers seamless protection against the most evasive cyberattacks and supplies actionable threat intelligence to partners, customers and the cybersecurity community.

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