SonicWall Gen 7 NS*a* Series

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.

Gen 7 NS*a* 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.

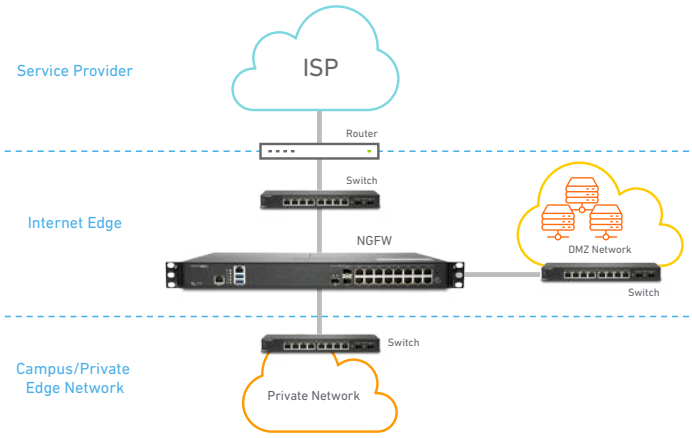
Deployments

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:

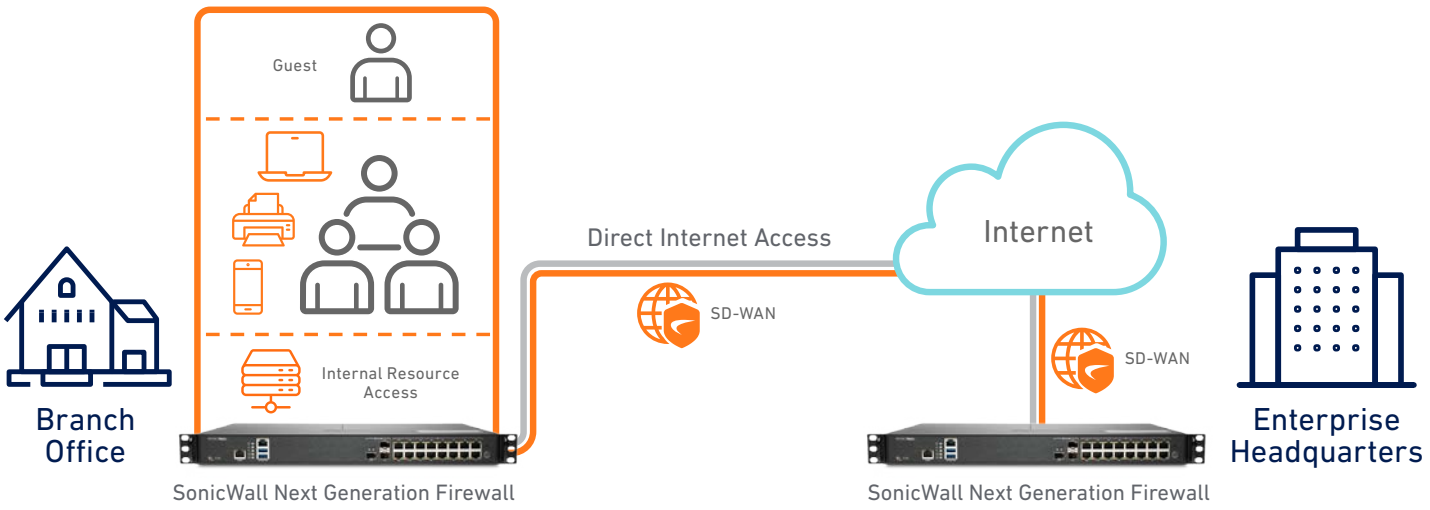
- Deploy a proven NGFW solution with highest performance and port density (including 40 GbE and 10 GbE connectivity) in its class
- Gain visibility and inspect encrypted traffic, including TLS 1.3, to block evasive threats coming from the Internet — all without compromising performance
- Protect your 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



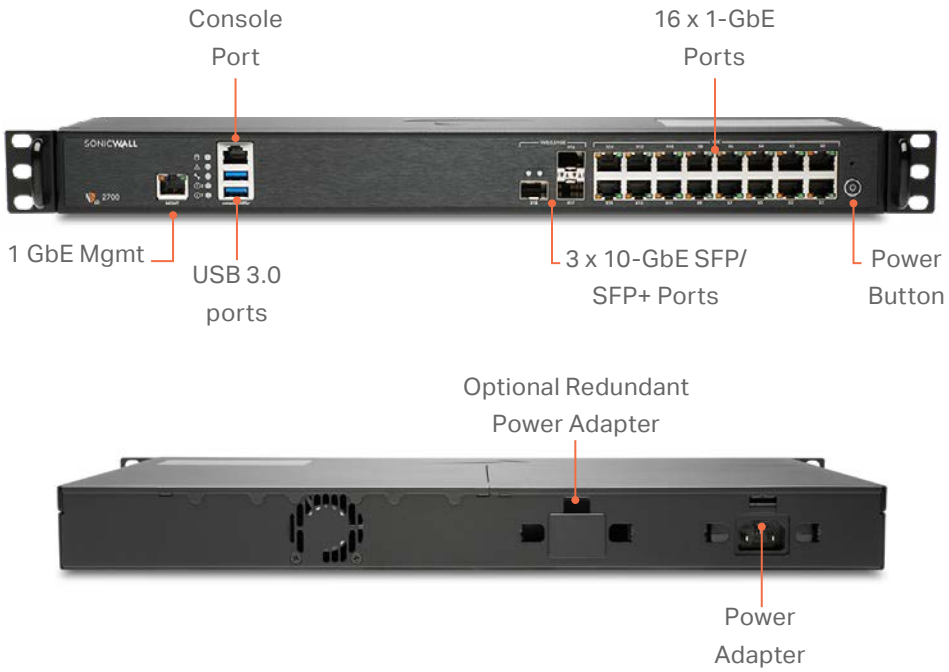
Medium and Distributed Enterprises

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:

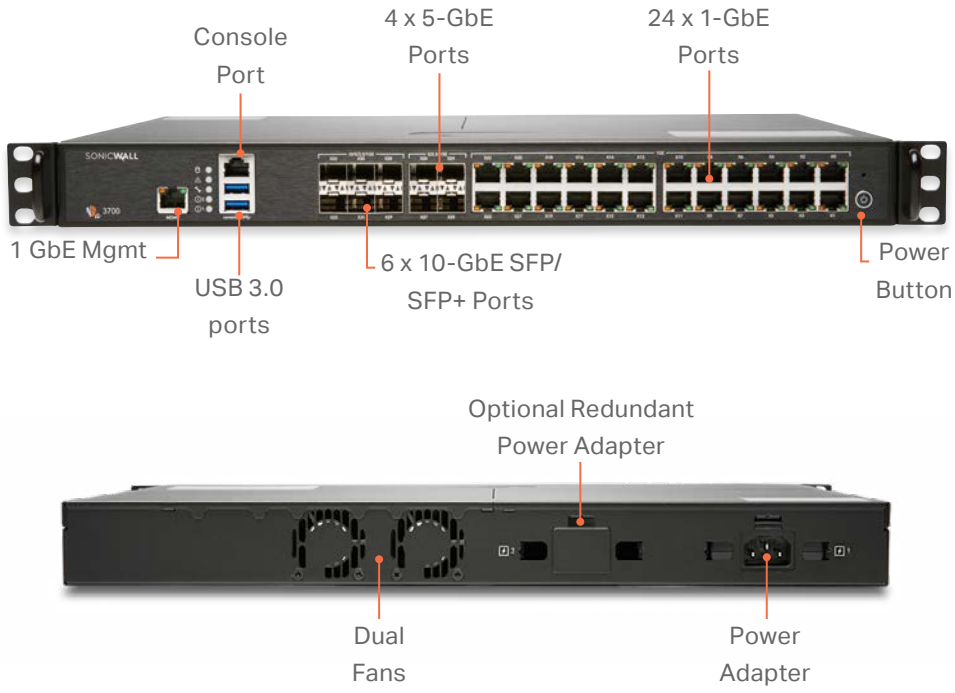
- Future-proof against an ever-changing threat landscape by investing in a NGFW with multi-gigabit threat analysis performance
- Provide direct and secure internet access to distributed branch offices instead of back-hauling through corporate headquarters
- Allow distributed branch offices to securely 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

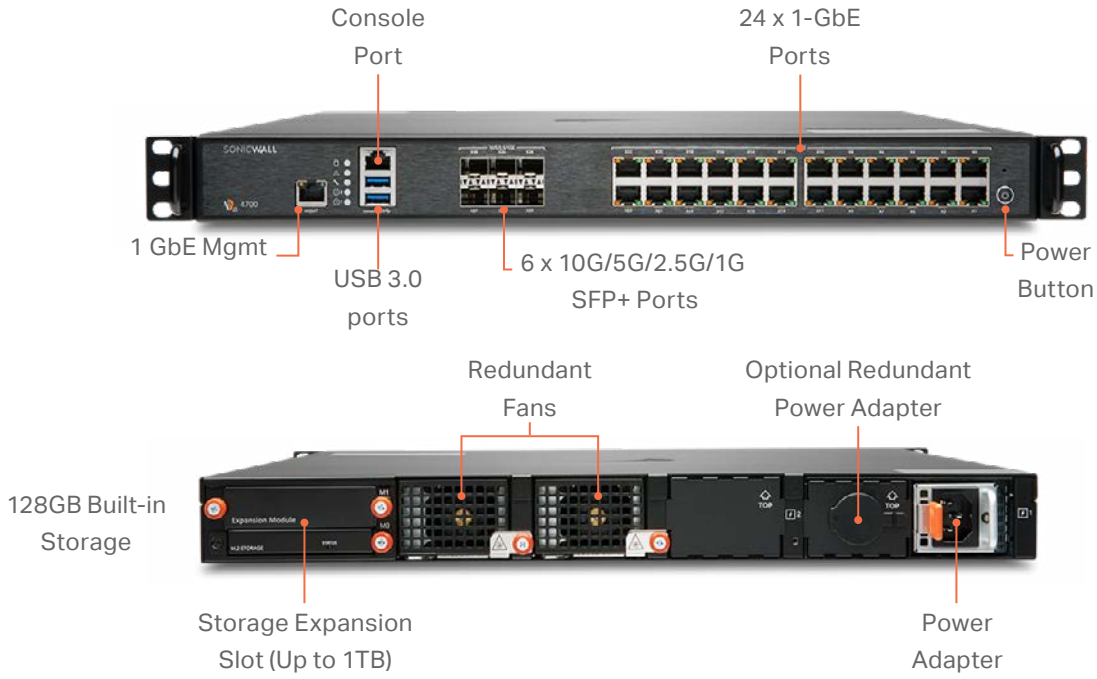


NS*a* 3700

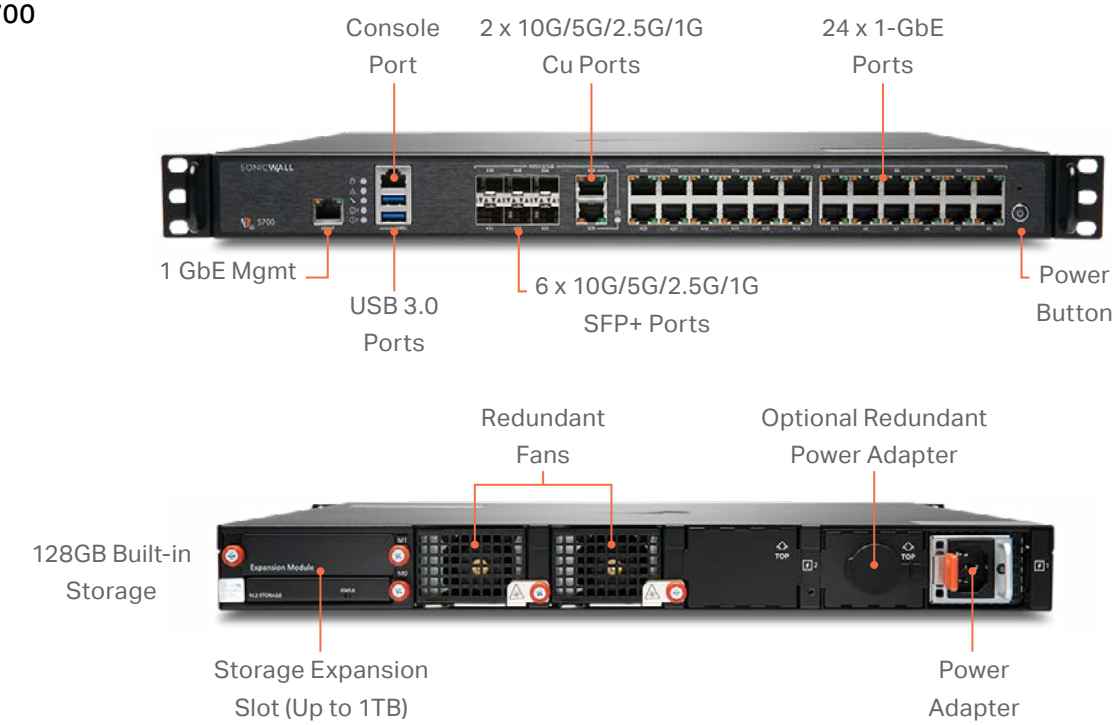


SonicWall Gen 7 NS*a* Series Cont'd

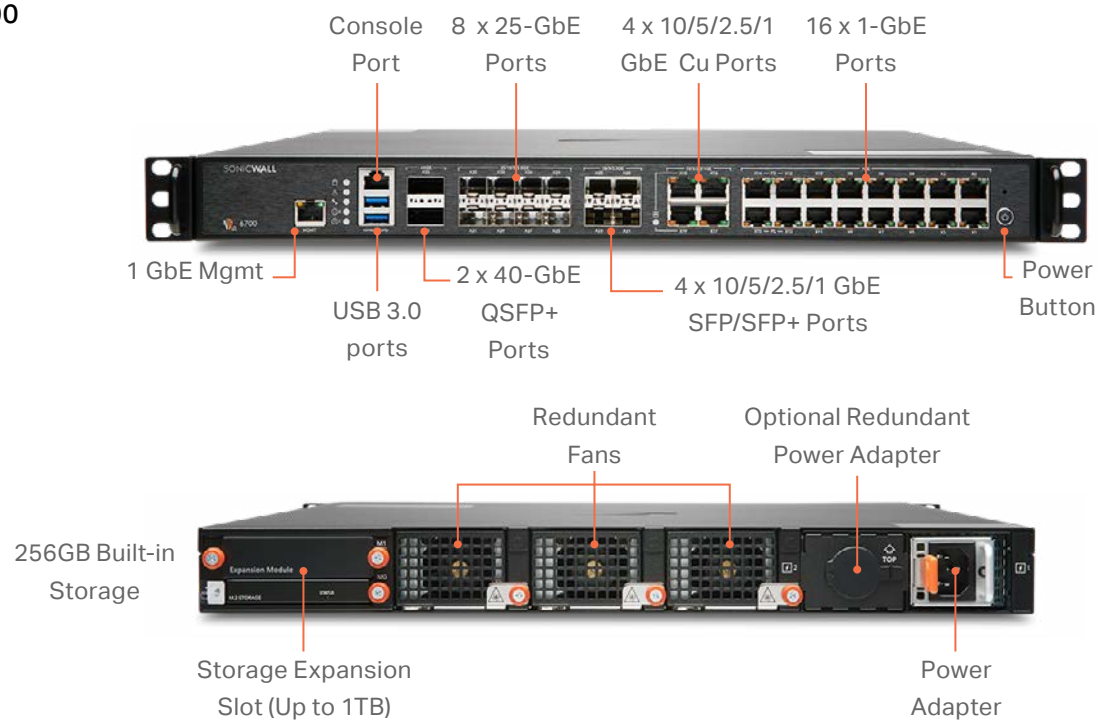
NS*a* 4700



NS*a* 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				

Gen 7 NS*a* Series System Specifications

Firewall	NS*a* 2700	NS*a* 3700	NS*a* 4700	NS*a* 5700	NS*a* 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, , 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.

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 (CS*a*) 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

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 NS*a* 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