

# SonicWall NSa 2700

The SonicWall Network Security Appliance (NSa) 2700 next-generation firewall (NGFW) offers medium- to large-sized enterprises industry-leading performance at the lowest total cost of ownership in its class.

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

The NSa 2700 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 16 x 1GbE ports and three x 10 GbE ports), the solution supports network and hardware redundancy with high availability, clustering and dual power supplies.

## Generation 7 – SonicOS 7.0 and Security Services

The SonicWall NSa 2700 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 7.0 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 NSa 2700 supports advanced networking features, such as SD-WAN, dynamic routing, layer 4-7 clustering 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 NSa 2700 offers access to SonicWall's premier advanced firewall security services, allowing you to protect your entire security infrastructure. Solutions and services such as Cloud Application Security, Capture Advanced Threat Protection (ATP) cloud-based sandboxing, Real-Time Deep Memory Inspection (RTDMI™) and Reassembly-Free Deep Packet Inspection (RFDPI) — along with Deep Packet Inspection (DPI) for all traffic including TLS 1.3 — offer comprehensive gateway protection from most stealthy and dangerous malware, including zero-day and encrypted threats.



## Highlights:

- 1 RU – Form Factor
- 16 x 1 GbE interfaces
- 3 x 10 GbE interfaces
- 2 Gbps Threat and Malware Analysis Throughput
- Enterprise Internet Edge Ready
- Latest Generation 7 SonicOS support
- Secure SD-WAN capability
- Intuitive single pane of glass management
- TLS 1.3 support
- Best-in-class price-performance
- Fast DPI performance
- Low TCO in its class
- High port density for easy networking
- SonicWall Switch, SonicWave Access Point and Capture Client integration
- Redundant power

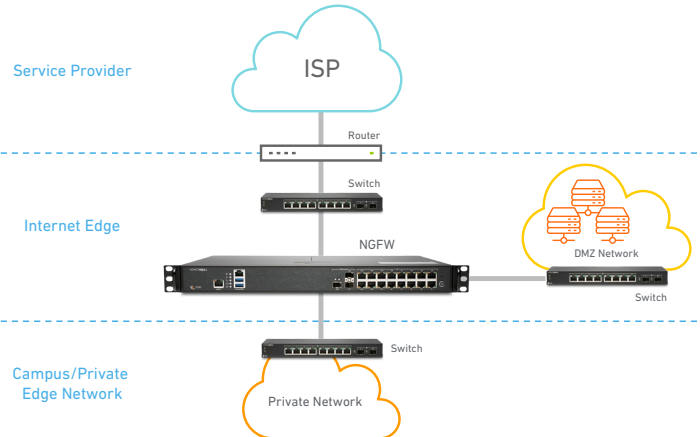
## Deployments

SonicWall NSa 2700 has two main deployment options for medium and distributed enterprises:

### Internet Edge Deployment

In this standard deployment option, SonicWall NSa 2700 protects private networks from malicious traffic coming from the internet, allowing you to:

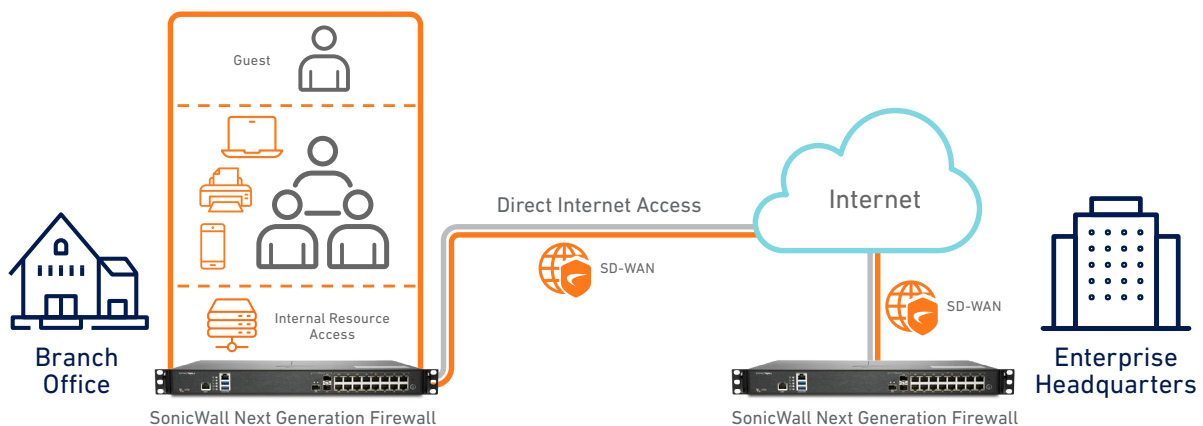
- Deploy a proven NGFW solution with highest performance and port density (including 10 GbE connectivity) in its class
- Gain visibility and inspect encrypted traffic, including TLS 1.3, to block evasive threats coming from the Internet — all without compromising performance
- Protect your enterprise 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 NSa 2700 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 10 GbE connectivity to support a distributed enterprise and wide area networks





## SonicWall NSa 2700 specifications

FIREWALL GENERAL	NSa 2700
Operating system	SonicOS 7.0
Interfaces	16x1GbE, 3x10G SFP+, 2 USB 3.0, 1 Console, 1 Management port
Storage	64GB M.2
Expansion	Storage Expansion Slot (Up to 256GB)
VLAN interfaces	256
Access points supported (maximum)	256
Management	Network Security Manager, CLI, SSH, Web UI, GMS, REST APIs
Sign-On (SSO) Users	30,000
FIREWALL/VPN PERFORMANCE	NSa 2700
Firewall inspection throughput <sup>1</sup>	5.5 Gbps
Threat prevention throughput <sup>2</sup>	3.0 Gbps
Application inspection throughput <sup>2</sup>	3.6 Gbps
IPS throughput <sup>2</sup>	3.4 Gbps
Anti-malware inspection throughput <sup>2</sup>	2.9 Gbps
TLS/SSL inspection and decryption throughput (DPI SSL) <sup>2</sup>	800 Mbps
IPSec VPN throughput <sup>3</sup>	2.10 Gbps
Connections per second	21,500
Maximum connections (DPI)	500,000
Maximum connections (SPI)	1,500,000
Maximum connections (DPI-SSL)	125,000
VPN	NSa 2700
Site-to-site VPN tunnels	2,000
IPSec VPN clients (maximum)	50 (1000)
SSL VPN licenses (maximum)	2 (500)
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	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	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)

## SonicWall NSa 2700 specifications, continued

SECURITY SERVICES		NSa 2700
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	
Comprehensive Anti-Spam Service	Supported	
Application Visualization	Yes	
Application Control	Yes	
Capture Advanced Threat Protection	Yes	
NETWORKING		NSa 2700
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, SSO, Novell, internal user database, Terminal Services, Citrix, Common Access Card (CAC)	
Local user database	250	
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	
Certifications pending	FIPS 140-2 (with Suite B) Level 2, UC APL, VPNC, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-virus, Common Criteria NDPP (Firewall and IPS)	
Common Access Card (CAC)	Supported	
High availability	Active/Active with stateful synchronization	
HARDWARE		NSa 2700
Form factor	1U Rack Mountable	
Power supply	60W	
Maximum power consumption (W)	21.5	
Input power	100-240 VAC, 50-60 Hz	
Total heat dissipation	73.32 BTU	
Dimensions	43 x 32.5 x 4.5 (cm) 16.9 x 12.8 x 1.8 in	
Weight	4.0 kg / 8.8 lbs	
WEEE weight	4.2 kg / 9.3 lbs	
Shipping weight	6.4 kg / 14.1 lbs	
Environment (Operating/Storage)	32°-105° F (0°-40° C)/-40° to 158° F (-40° to 70° C)	
Humidity	5-95% non-condensing	
REGULATORY		NSa 2700
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	

<sup>1</sup> Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services.

<sup>2</sup> Threat Prevention/GatewayAV/Anti-Spyware/IPS throughput measured using industry standard Spirent WebAvalanche HTTP performance test and Ixia 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.

<sup>3</sup> VPN throughput measured using UDP traffic at 1280 byte packet size 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
- SD-WAN scalability
- SD-WAN Usability Wizard<sup>1</sup>
- SonicCoreX and SonicOS containerization<sup>1</sup>
- Connections scalability (SPI, DPI, DPI SSL)

## Enhanced dashboard<sup>1</sup>

- Enhanced device view
- Top traffic and user summary
- Insights to threats
- Notification center

## TLS/SSL/SSH decryption and inspection

- TLS 1.3 with enhanced security<sup>1</sup>
- 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<sup>2</sup>

- 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

## Intrusion prevention<sup>2</sup>

- 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<sup>2</sup>

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

## Application identification<sup>2</sup>

- 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<sup>2</sup>

- URL filtering
- Proxy avoidance
- Keyword blocking
- 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 (NSa 2650 and above)
- 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<sup>1</sup>
  - Dashboard
  - Device information, application, threats
  - Topology view
  - Simplified policy creation and management
- Policy/Objects usage statistics<sup>1</sup>
  - Used vs Un-used
  - Active vs Inactive
- Global search for static data
- Storage support<sup>1</sup>
- Internal and external storage management<sup>1</sup>
- 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<sup>1</sup>
- SonicExpress mobile app support
- SNMPv2/v3
- Centralized management and reporting with SonicWall Global Management System (GMS)<sup>2</sup>
- 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 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

<sup>1</sup> New feature, available on SonicOS 7.0

<sup>2</sup> Requires added subscription

Product	SKU
NSa 2700 with TotalSecure Essential Edition (1-year)	02-SSC-7369
NSa 2700 with Secure Upgrade Plus Essential Edition (3-year)	02-SSC-7370
NSa 2700 High Availability	02-SSC-7367

Services	SKU
Essential Protection Service Suite - Capture ATP, Threat Prevention, Content Filtering, Anti-Spam and 24x7 Support for NSa 2700 (1-year)	02-SSC-7346
Advanced Protection Service Suite (1-year)	02-SSC-6905
Capture Advanced Threat Protection for NSa 2700 (1-year)	02-SSC-6911
Gateway Anti-Virus, Intrusion Prevention and Application Control (1-year)	02-SSC-6929
Content Filtering Service for NSa 2700 (1-year)	02-SSC-7358
Comprehensive Anti-Spam Service for NSa 2700 (1-year)	02-SSC-7371
24x7 Support for NSa 2700 (1-year)	02-SSC-6899

### 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](http://www.sonicwall.com/PES).

## 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](http://www.sonicwall.com).