DATASHEET

SonicWall mid-range Gen 8 NSa Series.

Best-in-class threat protection
for distributed enterprises & campuses.

SonicWall's latest mid-range next-gen firewalls, Network Security Appliance (NS*a*) Series, offers medium and large enterprises industry-leading threat prevention performance at the lowest total cost of ownership in their class. The firewalls are the cornerstones of the threat protection solution that includes simplified centralized firewall management, Zero Trust enablement, flexible licensing with an option of managed firewall services, and an embedded cyber warranty for risk mitigation.

The Gen 8 firewalls deliver comprehensive security features such as intrusion prevention, VPN, application control, malware analysis, URL filtering, DNS Security, GeoIP and Botnet services, protecting the perimeter from advanced threats without becoming a bottleneck.

NS*a* 2800

NS*a* 3800

NS*a* 4800

NS*a* 5800

NS*a* 6800

Gen 8 NS*a* Series Spec Preview.

Up to 40 Gbps	Up to 55 Gbps	Up to 20 Million
Threat Prevention Throughput	Firewall Throughput	Connections

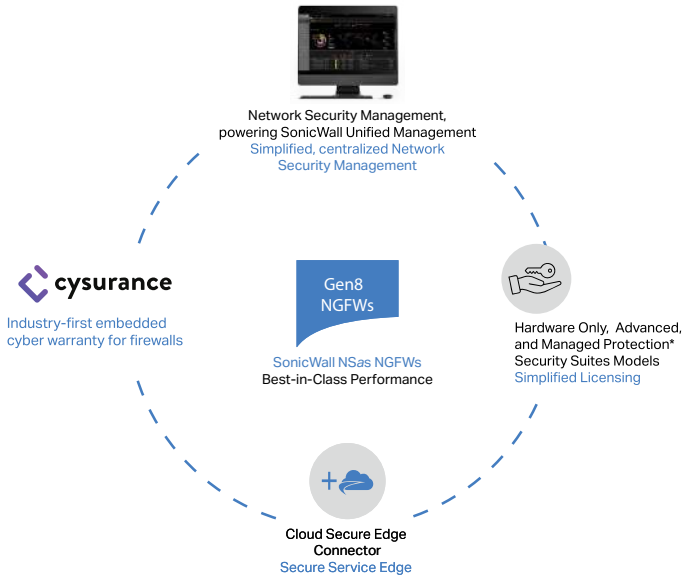
sonicwall.com

HIGHLIGHTS

- Form Factor: 1U Rack-mountable
- Support for 10/5/2.5/1G ports
- Multi-gigabit Threat and Malware Analysis Throughput
- Superior TLS performance (sessions and throughput)
- Best-in-class price-performance
- Expandable storage
- Advanced DNS Filtering
- Reputation-based Content Filtering Service (CFS 5.0)
- Simplified Centralized SaaS and On-Premises management via Network Security Manager
- Wi-Fi 6 firewall management
- SonicWall Unified Management Support
- Enterprise Internet Edge Ready
- Secure SD-WAN capability
- TLS 1.3 support
- Simplified licensing including Hardware Only, Advanced and Managed Protection Security Suites
- Powered by SonicWall Capture Labs threat research team
- SonicWall Switch, SonicWave Access Point and Capture Client integration
- Cloud Secure Edge Connector Support
- Embedded Warranty up to USD$200K by Cysurance included in Security Suites

SONICWALL®

Gen 8 NSa firewalls drive strong security with a comprehensive solution encompassing of threat protection, centralized management, reporting and analytics, security and managed service options, Secure Service Edge (SSE) integration, and cyber warranty.



Hardware

Gen 8 NS*a* Series, built with the latest hardware components, delivers multi-gigabit threat prevention throughput — even for encrypted traffic. Featuring a high port density, the firewall solutions support network and hardware redundancy with high availability and dual power adapters including one for redundancy.

Architecture

The Gen 8 NS*a* Series runs on SonicOS 8, a new operating system that delivers a modern user interface, intuitive workflows and user-first design principles. SonicOS 8 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 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 appliances provide a single-pane-of-glass interface to manage both switches and access points.

Threat Protection and Security Services

Built to mitigate the advanced cyberattacks of today and tomorrow, the Gen 8 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 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.

Simplified licensing includes Hardware Only, Advanced (APSS) and Managed Protection Security Suite (MPSS) to meet your unique needs. MPSS augments resources with managed services for firewalls.

A Cloud Secure Edge Connector integration provides secure access to their private applications behind the firewalls. Users and devices can adhere to a Zero-Trust framework for application access.

Cyber Warranty

An embedded cyber warranty is offered as part of your security suite to mitigate costs of security breach, meet compliance requirements and promote peace of mind.

SONICWALL®

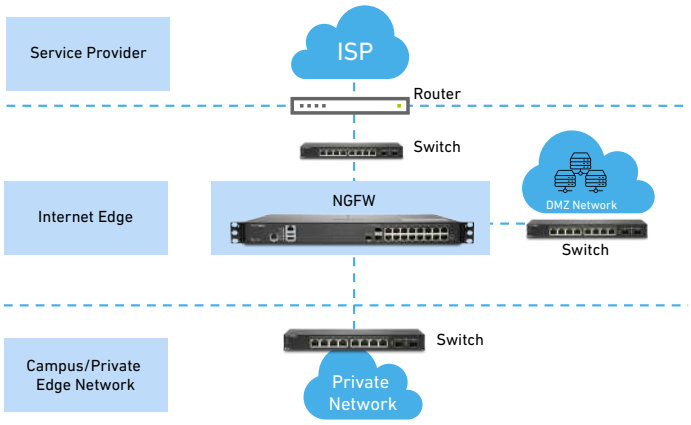
Deployments

The Gen 8 NS*a* Series has two main deployment options for medium and distributed enterprises:

Internet Edge Deployment

In this standard deployment option, the Gen 8 NS*a* Series NGFW protects private networks from malicious traffic coming from the internet, allowing you to:

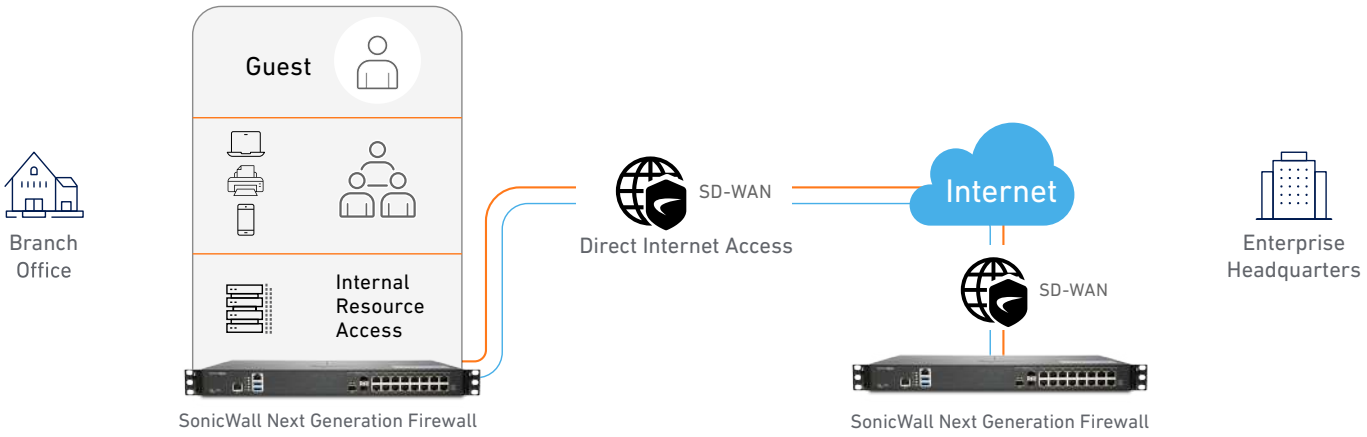
- Deploy a proven NGFW solution with highest performance in its class
- Gain visibility and inspect encrypted traffic, including TLS 1.3, to block evasive threats coming from the Internet — all without compromising performance
- Protect your enterprise with integrated security, including malware analysis, 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

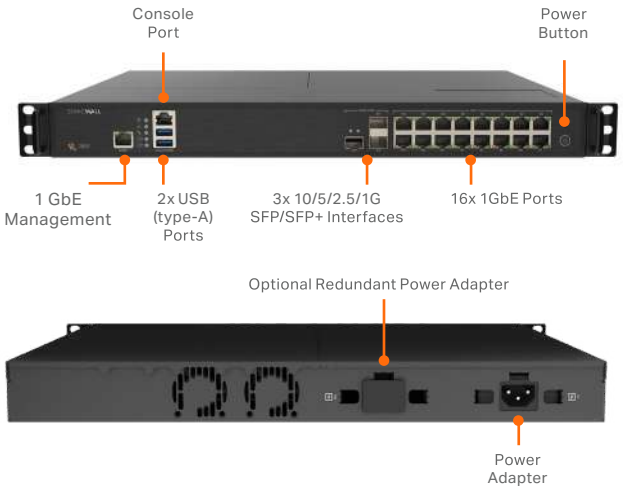
The SonicWall Gen 8 NS*a* Series supports SD-WAN and can be centrally managed, making it an ideal fit for medium and distributed enterprises. This deployment allows organizations to:

- 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

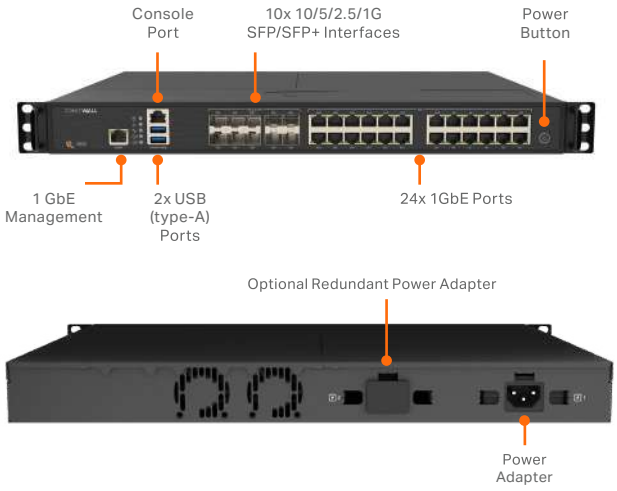


SonicWall Gen 8 NS*a* Series

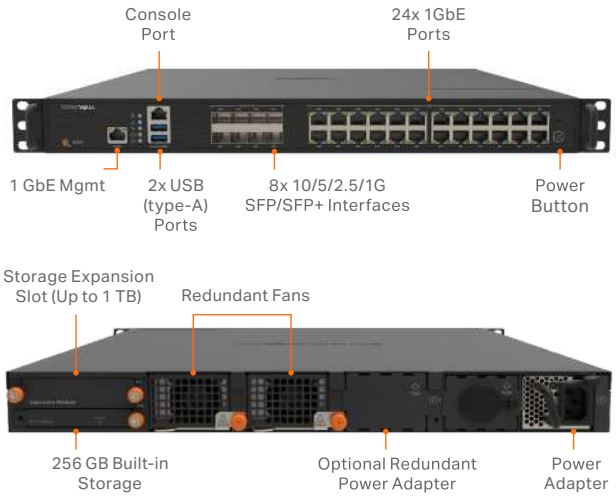
NSa 2800



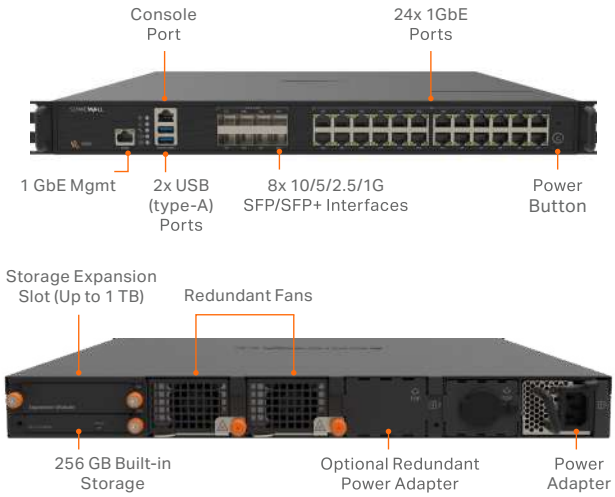
NSa 3800



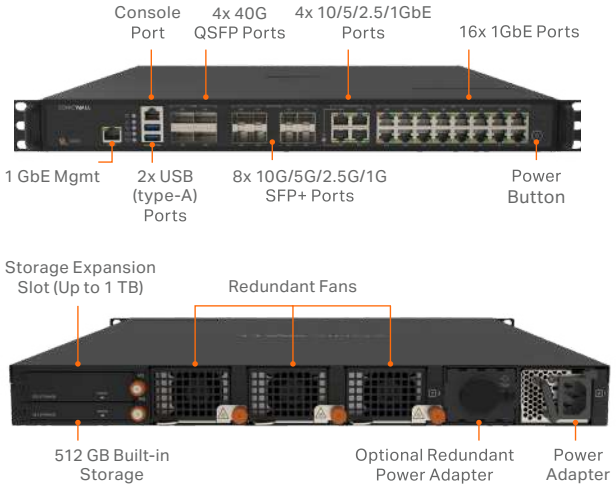
NSa 4800



NSa 5800



NSa 6800



Gen 8 NS*a* Series System Specifications

Firewall	NS*a* 2800	NS*a* 3800	NS*a* 4800	NS*a* 5800	NS*a* 6800
Operating system	SonicOS 8				
Interfaces	16x 1GbE, 3x 10/5/2.5/1G SFP/SFP+, 2x USB (type-A), 1 Console, 1 Mgmt. port	24x 1GbE, 10x 10/5/2.5/1G SFP/SFP+, 2x USB (type-A), 1 Console, 1 Mgmt. port	24x 1GbE, 8x 10/5/2.5/1G SFP/SFP+, 2x USB (type-A), 1 Console, 1 Mgmt. port	24x 1GbE, 8x 10/5/2.5/1G SFP/SFP+, 2x USB (type-A), 1 Console, 1 Mgmt. port	16x 1GbE, 4x 10/5/2.5/1G, 8x 10/5/2.5/1G SFP/SFP+, 4x 40G QSFP, 2x USB (type-A), 1 Console, 1 Mgmt. port
Storage/(Expansion)	128 GB (Up to 512 GB)	256 GB (Up to 512 GB)	256 GB (Up to 1 TB)	256 GB (Up to 1 TB)	512 GB (Up to 1 TB)
Centralized Management	Network Security Manager (NSM) 3.0 and above, CLI, SSH, Web UI, REST APIs				
Logical VLAN and tunnel interfaces (maximum)	256	256	512	512	512
SAML Single Sign-On Users[1]	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[2]	8 Gbps	12 Gbps	20 Gbps	30 Gbps	55 Gbps
Threat Prevention throughput[3]	6 Gbps	8 Gbps	13 Gbps	24 Gbps	40 Gbps
Application inspection throughput[3]	7 Gbps	9 Gbps	13 Gbps	24 Gbps	40 Gbps
IPS throughput[2]	7 Gbps	8 Gbps	13 Gbps	24 Gbps	40 Gbps
Anti-malware inspection throughput[3]	6 Gbps	8 Gbps	13 Gbps	24 Gbps	40 Gbps
TLS/SSL inspection and decryption throughput[3]	1.8 Gbps	3 Gbps	4.2 Gbps	8 Gbps	10.5 Gbps
IPSec VPN throughput[4]	5.5 Gbps	8 Gbps	11 Gbps	21 Gbps	27 Gbps
Connections per second	50,000	90,000	140,000	240,000	280,000
Maximum Connections (SPI)	2,000,000	3,000,000	6,000,000	8,000,000	20,000,000
Maximum connections (DPI)	1,000,000	1,200,000	3,000,000	5,000,000	15,000,000
Maximum connections (TLS)	150,000	300,000	600,000	750,000	1,500,000
VPN and ZTNA					
Site-to-site VPN tunnels	2,000	3,000	4,000	6,000	6,000
IPSec VPN clients (max)	50 (1,000)	50 (1,000)	500 (3,000)	2,000 (4,000)	2,000 (6,000)
SSL-VPN licenses (max)	2 (500)	2 (500)	2 (1,000)	2 (1,500)	2 (1,500)
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[5]	Microsoft® Windows 7, Windows 8, Windows 8.1 and Windows 10				
NetExtender[6]	Microsoft® Windows 10, Windows 10/11 and Linux				
Mobile Connect[7]	Apple® iOS, Mac OS X, Google® Android™, Chrome OS, Windows				
SonicWall Private Access powered by Cloud Secure Edge[8]	Included in 3&Free Loyalty Program				
Security services					
Deep Packet Inspection services	Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, TLS Decryption				
Content Filtering Service (CFS)	Reputation-based URL filtering, 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 8 NS*a* Series System Specifications

Firewall	NS*a* 2800	NS*a* 3800	NS*a* 4800	NS*a* 5800	NS*a* 6800
Comprehensive Anti-Spam Service	●	●	●	●	●
Application Visualization	●	●	●	●	●
Application Control	●	●	●	●	●
Capture Advanced Threat Protection	●	●	●	●	●
DNS Filtering	●	●	●	●	●
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	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+, SAML SSO[1], Radius accounting NTLM, internal user database, 2FA, Terminal Services, Citrix, Common Access Card (CAC)				
Local user database	1,000	1,000	2,500	2,500	3,200
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	IPv6/USGv6				
High availability	Active/Passive with stateful synchronization				
Hardware					
Form factor	1U Rack-mountable				
Power supply (W)	90	150	450	450	450
Maximum power consumption (W)	52.8	102.3	110.4	119.4	201.7
Input power (AC)	100-240 VAC, 50-60 Hz	100-240 VAC, 50-60 Hz	100-240 VAC, 50-60Hz	100-240 VAC, 50-60Hz	100-240 VAC, 50-60Hz
Redundant power supply	N/A	1 (Optional)	1 (Optional)	1 (Optional)	1 (Optional)
Total heat dissipation (BTU)	180.01	341	377.4	407.5	461.32
Dimensions (Unit: cm)	43 x 32.5 x 4.5 Shipping: 57.5 x 47.5 x 18.5	43 x 32.5 x 4.5 Shipping: 57.5 x 47.5 x 18.5	43 x 46 x 4.5 Shipping: 69.5 x 59.5 x 21	43 x 46 x 4.5 Shipping: 69.5 x 59.5 x 21	43 x 46 x 4.5 Shipping: 69.5 x 59.5 x 21
Weight (kg)	4.6	4.6	7.4	7.4	7.4
WEEE weight (kg)	4.8	4.8	9.3	9.3	9.3
Shipping weight (kg)	7.2	7.2	13.2	13.2	13.2
Environment (Operating/Storage)	0°C to +40°C / -40°C to +70°C				
Humidity	5-95% non-condensing				
Regulatory					
Major regulatory compliance	FCC Class A, ICES Class A, CE (EMC, LVD, RoHS), UL, cUL, Mexico DGN Notice by UL, ANATEL, WEEE, REACH, SCIP, RCM, MIC Terminal, VCCI Class A, KCC/MSIP, BSMI, MTCTE/TEC, CB				

● = Service available.

[1] SAML Single Sign-On is available on SonicOS 8.1 and above.

[2] Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services.

[3] Threat Prevention/Gateway AV/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.

[4] 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.

[5] For the most recent information, please refer to SonicWall Global VPN Client Release Notes at: SonicWall Techdocs.

[6] For the most recent information, please refer to NetExtender Release Notes at: SonicWall Techdocs.

[7] For the most recent information, please refer to Mobile Connect Release Notes at: SonicWall Techdocs.

[8] Included with 3-year bundle.

SONICWALL

SonicOS 8 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
- Connections scalability (SPI, DPI, TLS)

Enhanced dashboard

- 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
- Deep packet inspection for TLS/SSL/SSH
- Inclusion/exclusion of objects, groups or hostnames
- SSL control
- Enhancements for TLS with CFS
- Granular DPI SSL controls per zone or rule

Capture advanced threat protection[1]

- Real-Time Deep Memory Inspection
- Cloud-based multi-engine analysis[1]
- Virtualized sandboxing
- Hypervisor level analysis
- Full system emulation
- Broad file type examination
- Automated and manual submission
- Real-time threat intelligence updates[1]
- Block until verdict
- Capture Client[2]

Intrusion prevention[1]

- 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[1]

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

Application identification[1]

- Application control
- Application bandwidth management
- Custom application signature creation
- Data leakage prevention
- Application reporting over NetFlow/IPFIX
- Comprehensive application signature database

Traffic visualization and analytics

- User activity
- Application/bandwidth/threat usage
- Cloud-based analytics

Web content filtering[1]

- 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

VPN & ZTNA

- 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, and Android
- Route-based VPN (OSPF, RIP, BGP)
- Secure Private Access by Cloud Secure Edge

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
- 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
  - Dashboard
  - Device information, application, threats
  - Topology view
  - Simplified policy creation and management
  - Policy/Objects usage statistics
  - Used vs Unused
  - Active vs Inactive
- Global search for static data
- Storage support

SONICWALL®

SonicOS 8.0 Feature Summary

Management, monitoring and support cont'd

- Internal and external storage management
- WWAN USB card support (5G/LTE/4G/3G)
- Network Security Manager (NSM) support
- SonicWall Unified Management and SonicWall AI for Monitoring and Insight (SAMI)
- Web GUI
- Command line interface (CLI)
- Zero-Touch registration & provisioning
- CSC Simple Reporting
- SonicExpress mobile app support
- SNMPv2/v3
- 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

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]Requires Security Suite subscription

Learn more about SonicWall Gen 8 NS*a* Series

https://www.sonicwall.com/products/firewalls/mid-range

© 2025 SonicWall Inc. ALL RIGHTS RESERVED.

Authorized Distributor :

SecureOne
Optimize with SECURITY

HQ Office (KL)
SecureOne Distribution Sdn Bhd
200801027033 (828358 - X)
No.7, Jalan 1/109E, Desa Business Park,
Taman Desa, Jalan Kelang Lama,
58100 Kuala Lumpur, Malaysia.

Tel: +6(03) 7984 6086 Fax: +6(03) 7984 6032
Email: sales@secureone.com.my

Northern Office
SecureOne Distribution (Northern) Sdn Bhd
201201003647 (977172 - H)
1A-2-02 @ One Precint (1160),
Lengkok Mayang Pasir,
11950 Bayan Baru, Penang, Malaysia.

Tel: +6(04) 619 2692 Fax: +6(04) 619 2699
Email: northern@secureone.com.my

www.secureone.com.my