NSv 270/470/870

The SonicWall Network Security virtual NSv 270/470/870 firewalls, deliver enterprise-class security, streamlined management, complete visibility, flexible deployment, while delivering superior performance for virtual workloads.

Vulnerabilities within virtual environments are discovered regularly that yield serious security implications and challenges. But protecting all these security vectors requires the ability to also consistently apply the right security policy to the right network control point, as some security failures can be attributed to ineffective policies or misconfigurations.

HIGHLIGHTS

Public, private and government cloud security

- Next-gen firewall with automated real-time breach detection and prevention capabilities
- Patented Real-Time Deep Memory Inspection (RTDMI™) technology
- Patented Reassembly-Free Deep Packet Inspection (RFDPI) technology
- Complete end-to-end visibility and streamlined management with Unified Policy
- Application intelligence and control
- DNS security
- Reputation-based Content Filtering Service (CFS 5.0)
- Wi-Fi 6 firewall management
- Network access control integration with Aruba ClearPass
- Supports AWS and Azure US Government clouds
- Integrates with Microsoft Azure Sentinel for faster incident response
- Supports private cloud (ESXi, Hyper-V, KVM, Nutanix) and public cloud (AWS, Azure) platforms

Virtual machine protection

- Data confidentiality
- Secure communication with data leakage prevention
- Traffic validation, inspection and monitoring
- Virtual network resilience and availability

DATASHEET

NS*v* firewall series help security teams reduce these types of security risks and vulnerabilities, which can cause serious disruption to business-critical services and operations. It enables enterprises to control dynamic traffic passing through a firewall and provides visibility and insight into disparate policies. It help simplify management tasks, reduce configuration errors and speed up deployment time, all of which contribute to a better overall security posture.

SonicOSX and Security Services

The SonicOSX architecture is at the core of NS*v* 270/470/870 firewalls. It is powered by the feature-rich SonicOSX 7 operating system with intuitive user interface (UI), advanced security, networking and management capabilities.

Built from the ground up, SonicOSX 7.0 features Unified Policy that offers integrated management of various security policies. Easily provision layer 3 to layer 7 controls in a single rule base on every firewall, providing a centralized location for configuring policies. The new web interface provides graphical visualizations of critical threat information, and displays actionable alerts prompting you to configure contextual security policies with point-and-click simplicity.

NS*v* further integrates SD-WAN, TLS 1.3 support, real-time visualization, high-speed virtual private networking (VPN) and other robust security features. Unknown threats are sent to SonicWall's cloud-based Capture Advanced Threat Protection (ATP) multiengine sandbox for analysis. Capture ATP harnesses Real-Time Deep Memory Inspection (RTDMI), a SonicWall patented technology, to discover and block malware and zero-day threats that reside in memory.

With the combination of Capture ATP, RTDMI technology and security advanced services, NS*v* series firewalls stop malware at the gateway before it gets to your critical systems.

Deployments

1. Cloud Edge: Secure Public, Private and Government Clouds

- Secure workloads on Amazon Web Services (AWS) and Microsoft Azure
- Protect cloud applications and cloud infrastructures from cyber threats with advanced next-generation firewall features that incorporates VPN, IPS, CFS, AV and much more
- Decrypt encrypted traffic easily and utilize TLS 1.3 support for improved security
- Ensure compliance with regulatory standards by implementing threat prevention and segmentation capabilities
- Gain complete visibility and control of traffic across multiple regions and availability zones with Unified Policy
- Attain cost benefit and efficiency by shifting from CAPEX to OPEX
- Secure AWS and Azure clouds designated for US Government agencies and their customers by deploying NS*v* firewalls
- Secure virtualized compute resources and hypervisors to protect private cloud workloads on VMware ESXi, Microsoft Hyper-V, Nutanix and KVM
- Prevent threats with complete visibility into intra-host communication between virtual machines
- Ensure appropriate application of security policies throughout the virtual environment
- Deliver safe application enablement rules by application, user and device, regardless of VM location
- Implement proper security zoning and isolations
- Integrate with Microsoft Azure Sentinel, a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution to expedite incident response

2. Internet Edge

- Protect corporate resources from attacks at the Internet gateway.
- Secure Internet edge from the most advanced attacks with advanced security features and automatically block threats
- Ensure compliance with regulatory standards by implementing threat prevention and segmentation capabilities
- Improve business efficiency, performance and reduce costs by leveraging SonicOSX enhancements
- Segment critical PoS (Point of Sale) systems, to ensure business continuity
- Gain complete visibility and control of traffic across multiple regions and availability zones with Unified Policy

NSv Series System Specifications

Firewall General	NSv 270	NSv 470	NSv 870
Operating system	SonicOSX[11]		
Supported Hypervisors	VMware ESXi v5.5/v6.0/v6.5/v6.7/v7.0/v8.0, Microsoft Hyper-V, KVM Ubuntu 16.04 / CentOS 7, Nutanix AHV (AOS 5.15 LTS/Prism Central 5.16.1.2)[10]		
Supported Government Clouds[12]	AWS and Azure (in US East and West regions)		
Supported AWS Instance Types	c5.large c5n.large c5d.large m5.large m5n.large	c5.xlarge c5n.xlarge c5d.xlarge m5.xlarge m5n.xlarge	c5.2xlarge c5n.2xlarge c5d.2xlarge m5.2xlarge m5n.2xlarge
Supported Azure Instance Types	Standard D2 v2 Standard_B2ms Standard_D2V4 Standard_D2ds_V4 Standard_D2s_v4	Standard D3 v2 Standard_B4ms Standard_DS3_v2 Standard_D2ds_V4	Standard D4 v2 Standard_A8_v2 Standard_F8 Standard_F8s Standard_D8_v4 Standard_D8_v3 Standard_D8s_v3
Licensing	BYOL, PAYG[1]		
Max Supported vCPUs	2	4	8
Interface Count (ESXi/Hyper-V/KVM/Nutanix/AWS/Azure)	8/8/8/8/8/8	8/8/8/8/8/8	8/8/8/8/8/8
Max Mgmt/DataPlane Cores	1/1	1/3	1/7
Min Memory[2]	4 GB	8 GB	10 GB
Max Memory[3]	6 GB	10 GB	14 GB
Supported IP/Nodes	Unlimited		
Minimum Storage	60 GB		
SSO users	500	10,000	15,000
Logging	Analyzer, Local Log, Syslog		
High availability	Active/Passive[4]		

SONICWALL

Firewall/VPN Performance[5,7]	NSv 270	NSv 470	NSv 870
Firewall Inspection Throughput	6 Gbps	9 Gbps	14 Gbps
Threat Prevention Throughput	1.6 Gbps	2.9 Gbps	8 Gbps
IPS Throughput	4 Gbps	6 Gbps	8 Gbps
TLS/SSL DPI Throughput	800 Mbps	2 Gbps	4 Gbps
VPN Throughput[8]	1.4 Gbps	3.5 Gbps	8 Gbps
Connections per second	13,760	37,270	75,640
Maximum connections (SPI)	225,000	1.5M	3M
Maximum connections (DPI)	125,000	1.5M	2M
TLS/SSL DPI Connections	8,000	20,000	30,000
VPN	**NSv 270**	**NSv 470**	**NSv 870**
Site-to-Site VPN Tunnels	75	6000	10,000
IPSec VPN clients[13] (Maximum)	50(1000)	2000(4000)	2000(6000)
SSL VPN Clients Included[6]	2	2	2
SSL VPN Clients Maximum[6]	100	200	300
Encryption/authentication	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B, Common Access Card (CAC)		
Key exchange	Diffie Hellman Groups 1, 2, 5, 14v		
Route-based VPN	RIP, OSPF, BGP		
Networking	**NSv 270**	**NSv 470**	**NSv 870**
IP address assignment	Static, DHCP, internal DHCP server[9], DHCP relay[9]		
NAT modes	1:1, many:1, 1:many, flexible NAT (overlapping IPs), PAT		
Logical VLAN and tunnel interfaces (maximum)[7]	128	128	128
Routing protocols	BGP, OSPF, RIPv1/v2, static routes, policy-based routing		
QoS	Bandwidth priority, max bandwidth, guaranteed bandwidth, DSCP marking, 802.1p		
Authentication	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, internal user database, Terminal Services, Citrix		
Local user database	250	2500	3200

[1]PAYG is currently available only on AWS
[2]Memory with Jumbo frame disabled.
[3]Memory with Jumbo frame enabled. Additional memory is required for Jumbo frames. Jumbo frames are not supported on Azure and AWS.
[4]High availability is available on VMware ESXi platform, KVM, Azure, Microsoft Hyper-V and Nutanix. NSv 270 supports HA by using D3v2 VM size. HA is not supported on AWS. HA on Azure requires server size that supports three or more interfaces.
[5]Published performance numbers are up to the specification and the actual performance may vary depending on underlying hardware, network conditions; firewall configuration and activated services. Performance and capacities may also vary based on underlying virtualization infrastructure, and we recommend additional testing within your environment to ensure your performance and capacity requirements are met. Performance metrics were observed using Intel Xeon Processor (Platinum 8268 @2.9GHz, 3.9GHz Turbo, 37.5M Cache) running SonicOS 7.0.1 with VMware vSphere 7.0
[6]SSL VPN clients available for MSSP program are 50 on NSv 270 and 75 on NSv 470. Increased SSL VPN number will be available only from SonicOS 6.5.4.4-44v-21-723 firmware and onwards.
[7]VLAN interfaces are not supported on Azure and AWS.
Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). 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 with default firewall settings. 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.
[8]All perfoarmance parameters are tested using Dell R740 with SR-IOV and Turbo boost.
[9]Supported on Private Cloud and not on Public Cloud Platforms.
[10]Nutanix AHV is supported on SonicWall NSv 270/470/870 running SonicOSX 7.0.0 firmware and onwards.
[11]SonicOSX 7.0.1 onwards user will be able to select and switch between Classic/Global and Policy mode.
[12]Government cloud is only available through BYOL
[13]GVC clients available for MSSP program are 25 on NSv 270 and 50 on NSv 470

SONICWALL

SonicOSX 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
- REST APIs
- SonicWall Switch integration[1]
- SonicWall Wi-Fi [6] AP integration
- Reputation-based Content Filtering Service (CFS 5.0)
- DNS filtering
- SD-WAN
  - SD-WAN Scalability
  - SD-WAN Usability Wizard
- API
  - Full API Support
- Multi-Tenancy[3]
  - Multi-Tenant Support
  - Tenant View with Firmware Support per Tenant
- Switch between Classic/Global and Policy mode[4]

Unified Policy

- Unified Policy combines layer 3 to layer 7 rules:
  - Source/Destination IP/Port/Service
  - Application Control
  - CFS/Web Botnet/Geo-IP
  - Rule Diagram
  - Single Pass Security Services enforcement - IPS/GAV/AS/Capture ATP
  - Profile Based Objects for Endpoint Security/BWM/QoS/CFS/ Intrusion Prevention
- Action Profiles for Security/DoS Rules
- Rule management:
  - Cloning
  - Shadow rule analysis
  - In-cell editing
  - Rule Export
  - Group editing
- Managing views
  - Used/un-used rules
  - Active/in-active rules
  - Sections/Custom Grouping
  - Customizable Grid/Layout

TLS/SSL/SSH decryption and inspection

- TLS1.3
- Supporting TLS 1.3 with enhanced security
- Deep packet inspection for TLS/SSL/SSH
- Inclusion/exclusion of objects, groups or hostnames
- SSL control
- Granular DPI SSL controls per zone or rule

Capture advanced threat protection[2]

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

Intrusion prevention[2]

- Signature-based scanning
- Network access control integration with Aruba ClearPass
- Automatic signature updates
- Bi-directional inspection engine
- 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 database

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 (RIP/OSPF/BGP)

Enhanced Dashboard

- Enhanced Device View
- Top Traffic and User summary
- Insights to threats
- Notification Center
- Enhanced Packet Monitoring
- SSH Terminal on UI
- New Design/Template
- Industry and Global Average Comparison

Networking

- PortShield[1]
- Jumbo frames
- Path MTU discovery
- Enhanced logging
- VLAN trunking
- Port mirroring (NS*a* 2650 and above)

SONICWALL

- Layer-2 QoS
- Port security
- Dynamic routing (RIP/OSPF/BGP)
- SonicWall wireless controller[1]
- Policy-based routing (ToS/ metric and ECMP)
- NAT
- DHCP server
- Bandwidth management
- Link aggregation[1] (static and dynamic)
- Port redundancy[1]
- A/P high availability with state sync
- A/A clustering[1]
- Inbound/outbound load balancing
- L2 bridge,[1] wire/virtual wire mode, tap mode, NAT mode
- 3G/4G WAN failover[1]
- Asymmetric routing
- Common Access Card (CAC) support
- SonicCoreX and SonicOS Containerization

Decryption Policy

- Unified Policy for SSL/TLS traffic

DoS Policy

- Unified Policy for DoS/DDoS attack prevention

VoIP

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

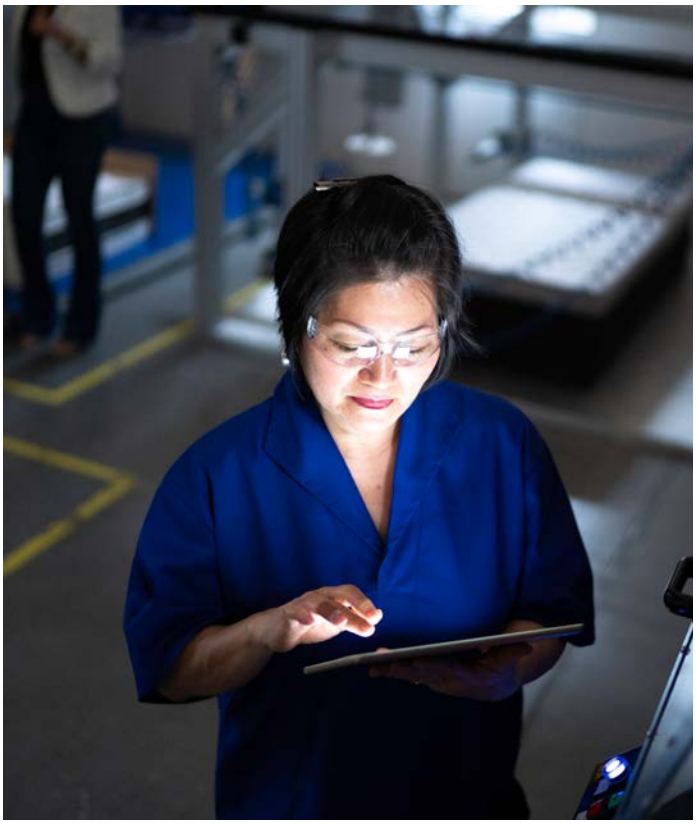
Management and monitoring

- Web GUI
- Command-line interface (CLI)
- Zero-Touch registration & provisioning
- SonicExpress mobile app support
- SNMPv2/v3
- Centralized management and reporting with Network Security Manager (NSM)[2]
- Logging
- Netflow/IPFix exporting
- Cloud-based configuration backup
- Application and bandwidth visualizer
- IPv4 and IPv6 Management
- Off-box reporting (Scrutinizer)
- LCD management screen[1]
- Dell N-Series and X-Series switch management including cascaded switches[1]
- Network Security Manager Reporting

Wireless[1]

- 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
- Guest cyclic quota
- LHM guest portal

[1] Not supported on NS*v* Series firewalls
[2] Requires added subscription
[3] Available only on NSsp firewalls
[4] Available on SonicOSX 7.0.1 onwards



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

Learn more about SonicWall NSv 270/470/870 Series

www.sonicwall.com/NSv

About SonicWall

SonicWall delivers stable, scalable, seamless cybersecurity for the hyper-distributed era and a work reality where everyone is remote, mobile and unsecure. By knowing the unknown, providing real-time visibility and enabling breakthrough economics, SonicWall closes the cybersecurity business gap for enterprises, governments and SMBs worldwide. For more information, visit www.sonicwall.com.

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