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 and private cloud security**
- Next-gen firewall with automated real-time breach detection and prevention capabilities
- Patent-pending 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
- Segmentation security and security zoning
- Support across 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
- SonicOSX 7.0

Find the right SonicWall solution for your enterprise:
[sonicwall.com/NSv](sonicwall.com/NSv)
NSv 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 NSv 240/470/870 firewalls. It is powered by the feature rich **SonicOSX 7.0** operating system with new modern looking UX/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 presents meaningful visualizations of threat information, and displays actionable alerts prompting you to configure contextual security policies with point-and-click simplicity.

NSv 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. Enhancing Capture ATP is our patent-pending Real-Time Deep Memory Inspection (RTDMI™) technology. As one of Capture ATP’s engine, RTDMI detects and blocks malware and zero-day threats by inspecting directly in memory.

By leveraging Capture ATP with RTDMI technology, in addition to security advanced services, NSv series firewalls stop malware, ransomware and other advanced threats at the gateway.

**Deployments**

1. **Cloud Edge and Data Center Secure Public 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
   - Appropriately scale and right-size your infrastructure
   - 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 Private Clouds
   - 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
   - Gain complete visibility and streamlined provisioning of traffic across multiple locations and availability zones with Unified Policy
   - Decrypt encrypted traffic easily and utilize TLS 1.3 support for improved security

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
### Firewall Series System Specifications

#### Operating System
- **NSv 270**: SonicOSX
- **NSv 470**: SonicOSX
- **NSv 870**: SonicOSX

#### Supported Hypervisors
- VMware ESXi 5.5 / 6.0 / 6.5 / 6.7
- Microsoft Hyper-V
- KVM
- Ubuntu 16.04 / CentOS 7
- Nutanix AHV (AOS 5.15 LTS/Prism Central 5.16.1.2)

#### Supported Public Cloud Platforms (Instance Type)
- AWS (c5.large), Azure (Std D2 v2)
- AWS (c5.xlarge), Azure (Std D3 v2)
- AWS (c5.2xlarge), Azure (Std D4 v2)

#### Licensing
- BYOL, PAYG²

#### Max Supported vCPUs
- **NSv 270**: 2
- **NSv 470**: 4
- **NSv 870**: 8

#### Interface Count (ESXi/Hyper-V/KVM/Nutanix/AWS/Azure)
- 8/8/8/8/2/2
- 8/8/8/4/4
- 8/8/8/8/8

#### Min Memory³
- **NSv 270**: 6 GB
- **NSv 470**: 8 GB
- **NSv 870**: 10 GB

#### Max Memory⁴
- **NSv 270**: 6 GB
- **NSv 470**: 10 GB
- **NSv 870**: 14 GB

#### Minimum Storage
- **NSv 270**: 60 GB

#### SSO users
- **NSv 270**: 500
- **NSv 470**: 10,000
- **NSv 870**: 15,000

#### Logging
- Analyzer, Local Log, Syslog

#### High availability
- Active/Passive⁵

#### Site-to-Site VPN Tunnels
- **NSv 270**: 75
- **NSv 470**: 6000
- **NSv 870**: 10,000

#### IPSec VPN clients (Maximum)
- **NSv 270**: 50(1000)
- **NSv 470**: 2000(4000)
- **NSv 870**: 2000(6000)

#### 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
- RIPv2, OSPF, BGP

#### Networking
- IP address assignment
  - Static, DHCP, internal DHCP server, DHCP relay
- NAT modes
  - 1:1, many:1, 1:many, flexible NAT (overlapping IP addresses), PAT
- Max VLAN⁶
  - **NSv 270**: 128
  - **NSv 470**: 128
  - **NSv 870**: 128
- Routing protocols
  - BGP, OSPF, RIPv2
- 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

---

¹Pending availability.
²PAYG is currently available only on AWS.
³Memory with Jumbo frame disabled. Additional memory is required for jumbo frames. Jumbo frames are not supported on Azure and AWS.
⁴Memory with Jumbo frame enabled. Additional memory is required for jumbo frames. Jumbo frames are not supported on AWS.
⁵High availability is available on VMware ESXi platform, KVM, Azure, Microsoft Hyper-V and Nutanix. HA is not supported on AWS.
⁶Published 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 (W-2195 2.3GHz, 4.6GHz Turbo, 24.75M Cache) running SonicOSv 6.5.0.2 with VMware vSphere 6.5.
⁷Increased SSL VPN number will be available only from SonicOS 6.5.4-44v-21-722 firmware and onwards. vLAN interfaces are not supported on Azure and AWS.
⁸High availability is available on VMware ESXi platform, KVM, Azure, Microsoft Hyper-V and Nutanix. HA is not supported on AWS.
⁹Supported on Private Cloud and not on Public Cloud Platforms.
¹⁰Nutanix AHV is supported on SonicWall NSv 270/470/870 running SonicOSX 7.0.0 firmware and onwards.
¹¹SonicOSX 7.0.1 onwards user will be able to select and switch between Classic/Global and Policy mode.
SonicOSX 7.0 feature summary

Firewall
• Stateful packet inspection
• Reassembly-Free Deep Packet Inspection
• DoS attack protection (UDP/ICMP/SYN flood)
• IPv4/IPv6 support
• Biometric authentication for remote access
• DNS proxy
• REST APIs
• SonicWall Switch integration

SD-WAN
• SD-WAN Scalability
• SD-WAN Usability Wizard

API
• Full API Support
• Multi-Tenancy
  • Multi-Tenant Support
  • Tenant View with Firmware Support per Tenant
• Switch between Classic/Global and Policy mode

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/GAVIAS/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
• Inclusion/exclusion of objects, groups or hostnames
• SSL control
• Granular DPI SSL controls per zone or rule

Capture advanced threat protection
• 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
• Signature-based scanning
• Automatic signature updates
• Bi-directional inspection engine
• Granular IPS rule capability
• GeoIP enforcement
• Botnet filtering with dynamic list
• Regular expression matching

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

Application identification
• 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
• 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 (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
• 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
- Link aggregation¹ (static and dynamic)
- Port redundancy¹
- A/P high availability with state sync
- A/A clustering¹
- Inbound/outbound load balancing
- L2 bridge,² wire/virtual wire mode, tap mode, NAT mode
- 3G/4G WAN failover¹
- 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
- BlueCoat security analytics platform
- Application and bandwidth visualizer
- IPv4 and IPv6 Management
- Off-box reporting (Scrutinizer)
- LCD management screen¹

Wireless¹
- 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
- Guest cyclic quota
- LHM guest portal

¹ Not supported on NSv Series firewalls
² Requires added subscription
³ Available only on NSsp firewalls
⁴ Available on SonicOSX 7.0.1 onwards

---

¹ Not supported on NSv Series firewalls
² Requires added subscription
³ Available only on NSsp firewalls
⁴ Available on SonicOSX 7.0.1 onwards
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 or follow us on Twitter, LinkedIn, Facebook and Instagram.

Learn more about SonicWall NSv 240/470/870 Series

www.sonicwall.com/NSv

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