AWS GovCloud (US)

Azure Government

Gartner Peer Insights

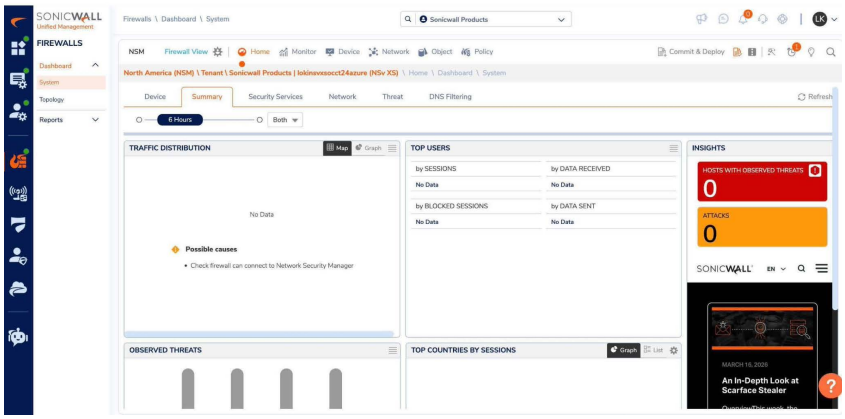
DATASHEET

NSv XS

Remote Access, Better Security

The SonicWall Network Security NSv XS Virtual Firewalls deliver enterprise-class security, streamlined management, complete visibility, and flexible deployment, while delivering superior performance for virtual workloads.

Vulnerabilities within virtual environments yield serious security implications and challenges. But protecting all these security vectors requires consistently applying 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, Proxmox) and public cloud (AWS, Azure) platforms
- Cloud Secure Edge Connector Support

Virtual machine protection

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

NS*v* firewall series helps 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 helps simplify management tasks, reduces configuration errors and speeds 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* XS firewalls. It is powered by the feature-rich SonicOSX 8 operating system with an intuitive user interface (UI), advanced security, networking and management capabilities. 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 ThreatProtection (ATP) multiengine sandbox for analysis.

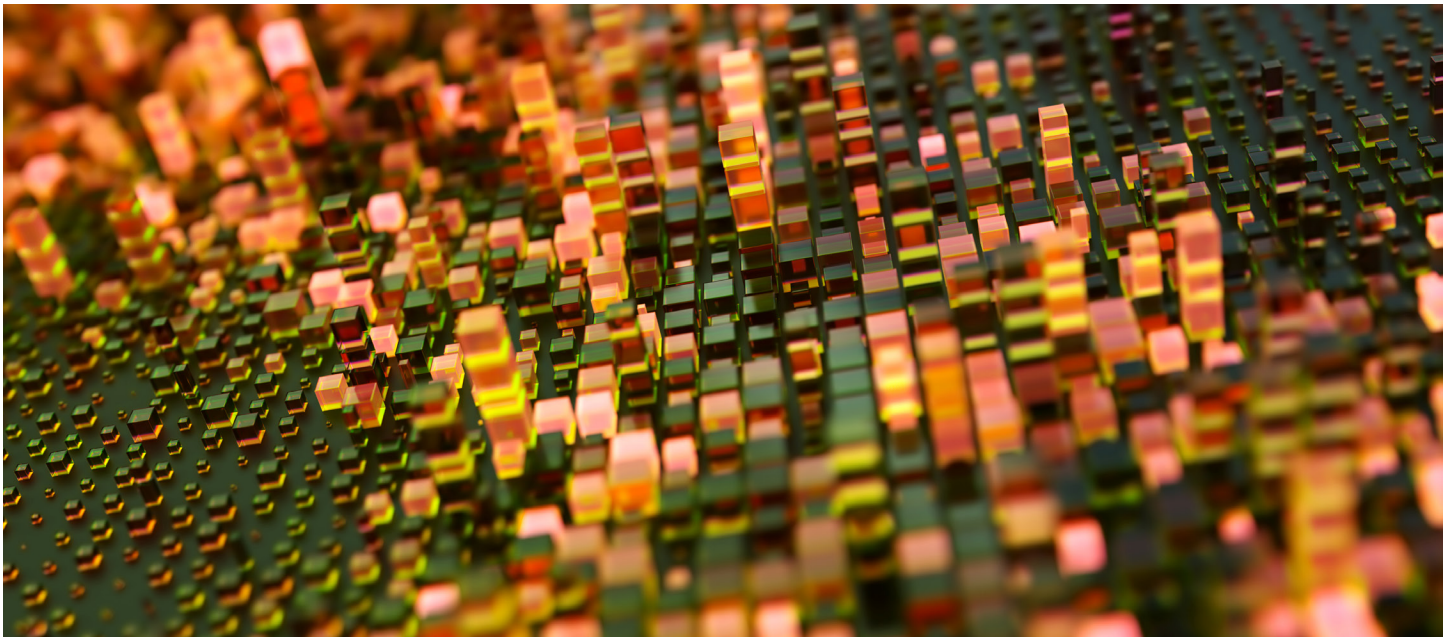
Capture ATP harnesses Real-Time Deep Memory Inspection (RTDMI), a SonicWall patented technology, to discover and block malware and zero-day threats that reside in memory.

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

Flexible licensing includes Secure Connect, Advanced (APSS) and Managed Protection Security Suite (MPSS) to meet your unique needs.

MPSS augments IT resources with managed firewall services from the SonicSentry Network Operation Center (NOC). When operating in Global Mode, users can leverage a new Cloud Secure Edge (CSE) Connector integration to gain a centralized, easy-to-manage option for securing 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.

SONICWALL®



Cyber Warranty

An embedded cyber warranty is included with your security suite to mitigate the costs of a security breach, meet compliance requirements, and promote peace of mind.

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 incorporate 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, Proxmox 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

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 XS
Operating system	SonicOSX
Supported Hypervisors	VMware ESXi, Microsoft Hyper-V, KVM Ubuntu/CentOS, Proxmox
Supported Government Clouds[7]	AWS and Azure (in US East and West regions)
Supported AWS Instance Types	t3a.small m7a.medium c7a.medium r7a.medium
Supported Azure Instance Types[9]	Standard_DS1_v2 Standard_B1ms Standard_DC1ds_v3 Standard_DC1s_v3 Standard_F
Licensing	BYOL, PAYG[1]
Max Supported vCPUs	1
Interface Count (ESXi/Hyper-V**/KVM//AWS/ Azure)	8/8/8/8/2/2
Max Mgmt/DataPlane Cores	1
Min Memory[2]	2 GB
Max Memory[3]	4 GB
Supported IP/Nodes	Unlimited
Minimum Storage	60 GB
SSO users	100
Logging	Analyzer, Local Log, Syslog
High Availability (HA)	Active/Passive[4]

SONICWALL®

Firewall/VPN Performance[5]	NSv XS
Firewall Inspection Throughput	2 Gbps
Threat Prevention Throughput	800Mbps
IPS Throughput	1 Gbps
TLS/SSL DPI Throughput	400 Mbps
VPN Throughput	700 Mbps
Connections per second	6,500
Maximum connections (SPI)	40,000
Maximum connections (DPI)	25,000
TLS/SSL DPI Connections	4,000
VPN	**NSv XS**
Site-to-Site VPN Policies	25
Site-to-Site VPN Tunnels	700
IPSec VPN clients (Maximum)	25 (100)
SSL VPN Clients Included	2
SSL VPN Clients (Maximum)	25
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 XS**
IP address assignment	Static, DHCP, internal DHCP server[6], DHCP relay[6]
NAT modes	1:1, many:1, 1:many, flexible NAT (overlapping IPs), PAT
Logical VLAN and tunnel interfaces (maximum)[7]	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	100

[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]VLAN interfaces are not supported on Azure and AWS. Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). 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 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.
[6]Supported on Private Cloud and not on Public Cloud Platforms.
[7]Government cloud is only available through BYOL
[8]GVC clients available for MSSP program are 25 on NSv and 50 on NSv
[9]Azure Backup services are not supported in NSv

SONICWALL®

SonicOSX 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
- REST APIs
- SonicWall Wi-Fi 6 AP integration
- Reputation-based Content Filtering
- Service (CFS 5.0)
- DNS filtering
- SD-WAN
  - SD-WAN Intelligent Routing
  - SD-WAN Scalability
  - SD-WAN Usability Wizard
- Switch between Classic/ Classic/Global and Policy mode[3]

Unified Policy

- Unified Policy combines layer 3 to layer 7 rules:
  - Source/Destination IP/Port/Service
  - Application Control
  - CFS/Web Botnet/GeoIP
  - 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
- Managing views
  - Used/un-used rules
  - Active/in-active rules
  - Sections/Custom Grouping
  - Customizable Grid/Layout

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
- TLS control
- Granular DPI TLS controls per zone or rule

Capture advanced threat protection[1]

- 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[1]

- 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[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, Chrome, Android and Kindle Fire
- Route-based VPN (RIP/OSPF/BGP)
- Secure Private Access to Cloud Secure Edge

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

SONICWALL

- 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 aggregation (static and dynamic)
- A/P high availability with state sync
- Inbound/outbound load balancing
- L2 bridge, wire/virtual wire mode, tap mode, NAT mode
- Asymmetric routing
- Common Access Card (CAC) support

Decryption Policy

- Unified Policy for SSL/TLS traffic

DoS Policy

- Unified Policy for DoS/DDoS attack preventione

VoIP

- Granular QoS control

[1] Requires Security Suite Subscription

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

Management and monitoring

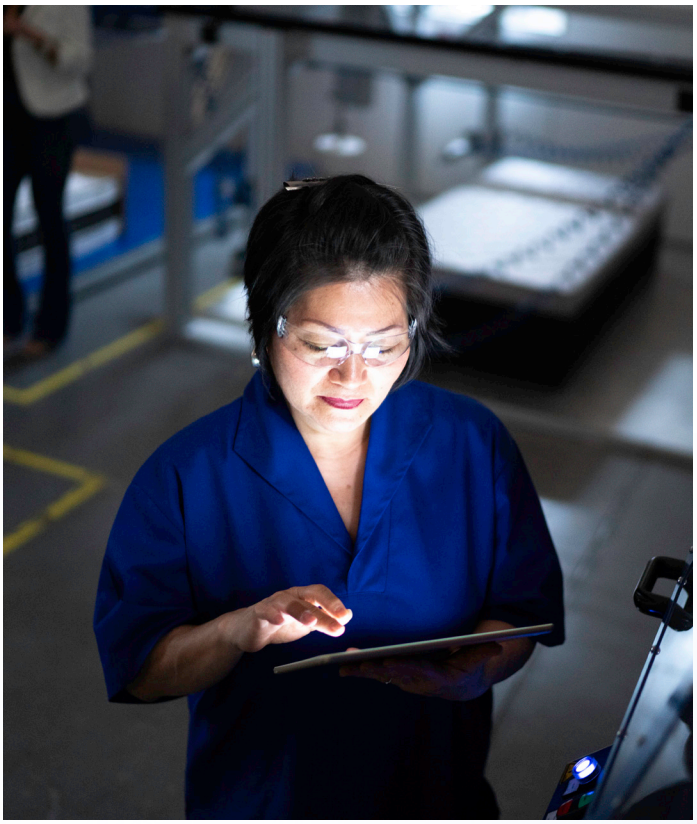
- SonicWall Unified Management and SonicWall AI for Monitoring and Insight (SAMI)
- Centralized management and reporting with Network Security Manager (NSM)
- Capture Threat Assessment (CTA) v2.0
- New design or template
- Industry and global average comparison
- New UI/UX, Intuitive feature layout
  - 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

- Web GUI
- Command-line interface (CLI)
- Zero-Touch registration & provisioning
- SonicExpress mobile app support
- SNMPv2/v3
- Logging
- Netflow/IPFix exporting
- Cloud-based configuration backup
- BlueCoat security analytics platform
- Application and bandwidth visualizer
- IPv4 and IPv6 Management
- Off-box reporting (Scrutinizer)

Debugging and diagnostics

- Enhanced packet monitoring
- SSH terminal on UI

SONICWALL



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 NS*v* XS Series

www.sonicwall.com/NSv

SonicWall, Inc.

1033 McCarthy Boulevard | Milpitas, CA 95035 | Refer to our website for additional information.

SONICWALL®