

# SonicWall Network Security virtual (NSv) series

Next-gen security for public, private or hybrid cloud environments

The design, implementation and deployment of modern network architectures, such as virtualization and cloud, continue to be a game-changing strategy for many organizations. Virtualizing the data center, migrating to the cloud, or a combination of both, have demonstrated significant operational and economic advantages. However, vulnerabilities within virtual environments are well-documented. New ones are discovered regularly that yield serious security implications and challenges. To ensure application services are delivered safely, efficiently and in a scalable manner, while combating threats harmful to all parts of the virtual framework including virtual machines (VM), application workloads and data must be among the top priorities.

SonicWall Network Security virtual (NSv) firewalls help security teams reduce these types of security risks and vulnerabilities, which can cause serious disruption to your business-critical services and operations. With full-featured security tools and services including reassembly-free deep packet inspection (RFDPI), security controls and networking services

equivalent to what a SonicWall physical firewall provides, NSv effectively shield all critical components of your private or public cloud environments.

NSv is easily deployed and provisioned in a multi-tenant virtual environment, typically between virtual networks (VNs). This allows it to capture communications and data exchanges between virtual machines for automated breach prevention, while establishing stringent access control measures for data confidentiality and VMs safety and integrity. Security threats (such as cross-virtual-machine or side-channel attacks and common network-based intrusions and application and protocol vulnerabilities) are neutralized successfully through SonicWall's comprehensive suite of security inspection services<sup>1</sup>. All VM traffic is subjected to multiple threat analysis engines, including intrusion prevention, gateway anti-virus and anti-spyware, cloud anti-virus, botnet filtering, application control and Capture Advanced Threat Protection multi-engine sandboxing.

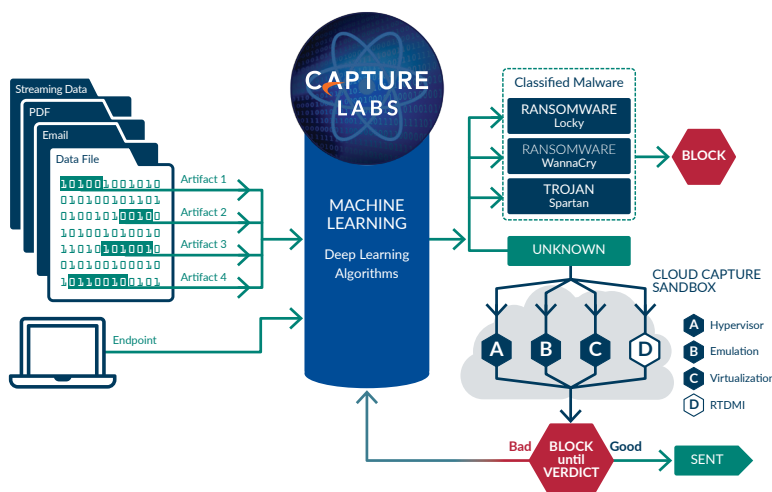
## Benefits:

### Public and private cloud security

- Attain Next-Gen firewall capabilities coupled with agility, scalability and security of the cloud without performance impact
- Gain complete visibility and control of your virtual infrastructure for automated real-time threat prevention
- Ensure appropriate placement of security policies for application throughout the virtual environment
- Deliver safe application enablement rules by application, user and device regardless of VM location
- Leverage multi-tenancy and micro-segmentation, with proper security zoning and isolations
- Platform support across private cloud platform (ESXi) and public cloud platforms (AWS<sup>2</sup>, Azure)

### Virtual machine protection

- Defend against zero-day vulnerabilities with Capture Advanced Threat Protection (ATP)
- Prevent unauthorized takeover of virtual systems
- Stop unauthorized access to protected data assets
- Block malicious and intrusive actions, such as spreading malware, executing operating system commands, file system browsing and C&C communication
- Prevent service disruption of any part or entire virtual ecosystem



## Segmentation Security

For optimal effectiveness against Advanced Persistent Threats (APTs), network security segmentation must apply an integrated set of dynamic, enforceable barriers to advanced threats. With segment-based security capabilities, NSv can group similar interfaces and apply the same policies to them, instead of having to write the same policy for each interface. By applying security policies to the inside of the VN, segmentation can be configured to organize network resources into different segments, and allow or restrict traffic between those segments. This way, access to critical internal resources can be strictly controlled.

NSv can automatically enforce segmentation restrictions based upon dynamic criteria, such as user identity credentials, geo-IP location and the security stature of mobile endpoints. For extended security, NSv is also capable of integrating multi-gigabit network switching into its security segment policy and enforcement. It directs segment policy to traffic at switching points throughout the network, and globally manage segment security enforcement from a single pane of glass.

Since segments are only as effective as the security that can be enforced between them, NSv applies intrusion prevention service (IPS) to scan incoming and outgoing traffic on the VLAN segment to enhance security for internal network traffic. For each segment, it enforces a full range of security services on multiple interfaces based on enforceable policy.

## Flexible Deployment Use Cases

With infrastructure support for high availability (HA) implementation, NSv fulfills scalability and availability requirements of Software Defined Data Centers (SDDC). It ensures system resiliency, service reliability, and regulatory conformance. Optimized for broad range of public, private and hybrid deployment use cases, NSv can adapt to service-level changes and ensure VMs and their application workloads and data assets are available, as well as secure. It can do it all at multi-Gbps speed and low latency.

Organizations gain all the security advantages of a physical firewall, with the operational and economic benefits of virtualization. This includes system scalability, operation agility, provisioning speed, simple management and cost reduction.

The NSv Series is available in multiple virtual flavors carefully packaged for broad range of virtualized and cloud deployment use cases. Delivering multi-gigabit threat prevention and encrypted traffic inspection performance, the NSv Series can adapt to capacity-level increases and ensure VNs safety and application workloads and data assets are available as well as secure.

## Governs Centrally

NSv deployments are centrally managed using both on premise with SonicWall GMS<sup>3</sup>, and with SonicWall Capture Security Center<sup>3</sup>, an open, scalable cloud security management, monitoring, reporting and analytics software that is delivered as a cost-effective as-a-service offering.

Capture Security Center gives the ultimate in visibility, agility and capacity to govern the entire SonicWall virtual and physical firewall ecosystem with greater clarity, precision, and speed – all from a single-pane-of-glass.

## Features

### SonicOS Platform

The SonicOS architecture is at the core of every SonicWall physical and virtual firewall including the NSv and NSa Series, SuperMassive™ Series and TZ Series. Refer to the SonicWall SonicOS Platform datasheet for complete list of features and capabilities.

### Automated breach prevention<sup>1</sup>

This includes complete advanced threat protection, including high-performance intrusion and malware prevention, and cloud-based sandboxing.

### Around-the-clock security<sup>1</sup>

New threat updates are automatically pushed to firewalls in the field with active security services, and take effect immediately without reboots or interruptions.

## 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).

### Zero-day protection<sup>1</sup>

NSv protects against zero-day attacks with constant updates against the latest exploit methods and techniques that cover thousands of individual exploits.

### Threat API

NSv receives and leverages any and all proprietary, original equipment manufacturer and third-party intelligence feeds to combat advanced threats, such as zero-day, malicious insider, compromised credentials, ransomware and advanced persistent threats.

### Zone protection

NSv strengthens internal security by segmenting the network into multiple security zones, with intrusion prevention service keeping threats from propagating across the zone boundaries. Creating and applying access rules and NAT policies to traffic passing through the various interfaces, it can allow or deny internal or external network access based on various criteria.

### Application intelligence and control<sup>1</sup>

With application-specific policies, NSv provides granular control over network traffic on the level of users, email addresses, schedules, and IP-subnets. It controls custom applications by creating signatures based on specific parameters or patterns unique to an application in its network communications. Internal or external network access are allowed or denied based on various criteria.

## GOVERNS CENTRALLY

- Establish an easy path to comprehensive security management, analytic reporting and compliance to unify your network security defense program
- Automate and correlate workflows to form a fully coordinated security governance, compliance and risk management strategy

## COMPLIANCE

- Helps make regulatory bodies and auditors happy with automatic PCI, HIPAA and SOX security reports
- Customize any combination of security auditable data to help you move towards specific compliance regulations

## RISK MANAGEMENT

- Move fast and drive collaboration, communication and knowledge across the shared security framework
- Make informed security policy decisions based on time-critical and consolidated threat information for higher level of security efficiency

*GMS provides a holistic approach to security governance, compliance and risk management*

### Data leakage prevention

NSv provides the ability to scan streams of data for keywords. This restrict the transfer of certain file names, file types, email attachments, attachment types, email with certain subjects, and email or attachments with certain keywords or byte patterns.

### Application layer bandwidth management

Using packet monitor, NSv can select among various bandwidth management settings to reduce network bandwidth usage by an application. This helps gain further control over the network.

### Secure communication

NSv ensures that data exchange between groups of virtual machines is done securely, including isolation, confidentiality, integrity, and information flow control within these networks via use of segmentation.

### Access control

NSv validates that only VMs that satisfy a given set of conditions are able to access data that belongs to another through the use of VLANs.

### User authentication

NSv creates policies to control or restrict VM and workload access by unauthorized users.

### Data confidentiality

NSv blocks information theft and illegitimate access to protected data and services.

### Virtual network resilience and availability

NSv prevents disruption or degradation of application services and communications.

### System safety and integrity

NSv stops unauthorized takeover of VM systems and services.

### Traffic validation, inspection and monitoring mechanisms

NSv detects irregularities and malicious behaviors and stop attacks targeting VM workloads.

<sup>1</sup> Requires SonicWall Advanced Gateway Security Services (AGSS) subscription.

<sup>2</sup> Pending AWS Marketplace availability

<sup>3</sup> SonicWall Global Management System and Capture Security Center require separate licensing or subscription.

## NSv Series system specifications

Firewall General	NSv 10	NSv 25	NSv 50	NSv 100
Operating system	SonicOS			
Supported Hypervisors	VMware ESXi v5.5 / v6.0 / v6.5			
Max Supported vCPUs	2	2	2	2
Interface Count (ESXi)	8	8	8	8
Max Mgmt/DataPlane Cores	1/1	1/1	1/1	1/1
Min Memory <sup>1</sup>	4 GB	4 GB	4 GB	4 GB
Max Memory <sup>2</sup>	6 GB	6 GB	6 GB	6 GB
Supported IP/Nodes	10	25	50	100
Minimum Storage	60 GB			
SSO users	25	50	100	100
Logging	Analyzer, Local Log, Syslog			
High availability	Active/Passive			
Firewall/VPN Performance <sup>1</sup>	NSv 10	NSv 25	NSv 50	NSv 100
Firewall Inspection Throughput	2 Gbps	2.5 Gbps	3 Gbps	3.5 Gbps
Full DPI Throughput (GAV/GAS/IPS)	450 Mbps	550 Mbps	650 Mbps	750 Mbps
Application Inspection Throughput	1 Gbps	1.25 Gbps	1.5 Gbps	1.75 Gbps
IPS Throughput	1 Gbps	1.25 Gbps	1.5 Gbps	1.75 Gbps
Anti-Malware Inspection Throughput	450 Mbps	550 Mbps	650 Mbps	750 Mbps
IMIX Throughput	750 Mbps	850 Mbps	950 Mbps	1100 Mbps
TLS/SSL DPI Throughput	650 Mbps	750 Mbps	850 Mbps	950 Mbps
VPN Throughput	500 Mbps	550 Mbps	600 Mbps	650 Mbps
Connections per second	1,800	5,000	8,000	10,000
Maximum connections (SPI)	2,500	6,250	12,500	25,000
Maximum connections (DPI)	2,500	6,250	12,500	25,000
TLS/SSL DPI Connections	500	1,000	2,000	4,000
VPN	NSv 10	NSv 25	NSv 50	NSv 100
Site-to-Site VPN Tunnels	10	10	25	50
IPSec VPN clients	10	10	25	25
SSL VPN NetExtender Clients (Maximum)	2(10)	2(25)	2(25)	2(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 10	NSv 25	NSv 50	NSv 100
IP address assignment	Static, DHCP, internal DHCP server, DHCP relay			
NAT modes	1:1, many:1, 1:many, flexible NAT (overlapping IPs), PAT			
VLAN Interfaces	25	25	50	50
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			
VoIP	Full H323-v1-5, SIP			
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, L2TP, PPTP, RADIUS			

<sup>1</sup>Memory with Jumbo frame disabled.

<sup>2</sup>Memory with Jumbo frame enabled. Additional memory is required for Jumbo frame enabled.

## NSv Series system specifications con't

Firewall General	NSv 200	NSv 300	NSv 400	NSv 800	NSv 1600
Operating system	SonicOS				
Supported Hypervisors	VMware ESXi v5.5 / v6.0 / v6.5				
Supported Public Cloud Platforms (Instance Type)	AWS (c5.large), Azure (Std D2 v2)	N/A	AWS (c5.xlarge), Azure (Std D3 v2)	AWS (c5.2xlarge), Azure (Std D4 v2)	AWS (c5.4xlarge), Azure (Std D5 v2)
Max Supported vCPUs	2	3	4	8	16
Interface Count (ESXi/AWS/Azure)	8/3/2	8/-/-	8/4/4	8/4/8	8/8/8
Max Mgmt/DataPlane Cores	1/1	1/2	1/3	1/7	1/15
Min Memory <sup>1</sup>	4 GB	6 GB	8 GB	10 GB	12 GB
Max Memory <sup>2</sup>	6 GB	8 GB	10 GB	14 GB	18 GB
Supported IP/Nodes	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Minimum Storage	60 GB				
SSO users	500	5,000	10,000	15,000	20,000
Logging	Analyzer, Local Log, Syslog				
High availability	Active/Passive <sup>3</sup>				
Firewall/VPN Performance <sup>4</sup>	NSv 200	NSv 300	NSv 400	NSv 800	NSv 1600
Firewall Inspection Throughput	4.1 Gbps	5.9 Gbps	7.8 Gbps	13.9 Gbps	17.2 Gbps
Full DPI Throughput (GAV/GAS/IPS)	900 Mbps	1.6 Gbps	2.2 Gbps	4.0 Gbps	6.4 Gbps
Application Inspection Throughput	2.3 Gbps	3.4 Gbps	4.1 Gbps	5.5 Gbps	6.4 Gbps
IPS Throughput	2.3 Gbps	3.4 Gbps	4.1 Gbps	5.5 Gbps	6.7 Gbps
Anti-Malware Inspection Throughput	900 Mbps	1.6 Gbps	2.2 Gbps	4.0 Gbps	6.6 Gbps
IMIX Throughput	1.5 Gbps	2.3 Gbps	2.8 Gbps	4.2 Gbps	5.3 Gbps
TLS/SSL DPI Throughput	1.1 Gbps	1.2 Gbps	1.8 Gbps	3.4 Gbps	5.1 Gbps
VPN Throughput	750 Mbps	1.4 Gbps	1.9 Gbps	4.2 Gbps	8.4 Gbps
Connections per second	13,760	24,360	37,270	75,640	125,000
Maximum connections (SPI)	225,000	1M	1.5M	3M	4M
Maximum connections (DPI)	125,000	500,000	1.5M	2M	2.5M
TLS/SSL DPI Connections	8,000	12,000	20,000	30,000	50,000
VPN	NSv 200	NSv 300	NSv 400	NSv 800	NSv 1600
Site-to-Site VPN Tunnels	75	100	6000	10,000	25,000
IPSec VPN clients (Maximum)	50(1000)	50(1000)	2000(4000)	2000(6000)	2000(10,000)
SSL VPN NetExtender Clients (Maximum)	2(100)	2(100)	2(100)	2(100)	2(100)
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 200	NSv 300	NSv 400	NSv 800	NSv 1600
IP address assignment	Static, DHCP, internal DHCP server, DHCP relay				
NAT modes	1:1, many:1, 1:many, flexible NAT (overlapping IPs), PAT				
VLAN Interfaces	50	256	500	512	512
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				
VoIP	Full H323-v1-5, SIP				
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, L2TP, PPTP, RADIUS				

<sup>1</sup>Memory with Jumbo frame disabled.

<sup>2</sup>Memory with Jumbo frame enabled. Additional memory is required for Jumbo frame enabled.

<sup>3</sup>High availability available on VMware ESXi platform.

<sup>4</sup>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 W Processor (W-2195 2.3GHz, 4.3GHz Turbo, 24.75M Cache) running SonicOSv 6.5.0.2 with VMware vSphere 6.5.

Testing Methodologies:

Maximum performance based on RFC 2544 (for firewall).

Full DPI/Gateway AV/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.

VPN throughput measured using UDP traffic at 1418 byte packet size adhering to RFC 2544. All specifications and features are subject to change.

## NSv Series ordering information

Product	AWS SKU <sup>1</sup>	Azure SKU	ESXi SKU
SonicWall NSv 10 Virtual Appliance TotalSecure Advanced Edition (1-year)	—	—	01-SSC-5875
SonicWall NSv 25 Virtual Appliance TotalSecure Advanced Edition (1-year)	—	—	01-SSC-5923
SonicWall NSv 50 Virtual Appliance TotalSecure Advanced Edition (1-year)	—	—	01-SSC-5926
SonicWall NSv 100 Virtual Appliance TotalSecure Advanced Edition (1-year)	—	—	01-SSC-5929
SonicWall NSv 200 Virtual Appliance TotalSecure Advanced Edition (1-year)	02-SSC-0906	02-SSC-0868	01-SSC-5950
SonicWall NSv 300 Virtual Appliance TotalSecure Advanced Edition (1-year)	—	—	01-SSC-5964
SonicWall NSv 400 Virtual Appliance TotalSecure Advanced Edition (1-year)	02-SSC-0912	02-SSC-0888	01-SSC-6084
SonicWall NSv 800 Virtual Appliance TotalSecure Advanced Edition (1-year)	02-SSC-0914	02-SSC-0889	01-SSC-6101
SonicWall NSv 1600 Virtual Appliance TotalSecure Advanced Edition (1-year)	02-SSC-0921	02-SSC-0895	01-SSC-6109
Product	AWS SKU <sup>1</sup>	Azure SKU	ESXi SKU
SonicWall NSv 10 Virtual Appliance TotalSecure Advanced Edition (3-year)	—	—	01-SSC-5008
SonicWall NSv 25 Virtual Appliance TotalSecure Advanced Edition (3-year)	—	—	01-SSC-4830
SonicWall NSv 50 Virtual Appliance TotalSecure Advanced Edition (3-year)	—	—	01-SSC-5165
SonicWall NSv 100 Virtual Appliance TotalSecure Advanced Edition (3-year)	—	—	01-SSC-5161
SonicWall NSv 200 Virtual Appliance TotalSecure Advanced Edition (3-year)	02-SSC-0903	02-SSC-0866	01-SSC-5194
SonicWall NSv 300 Virtual Appliance TotalSecure Advanced Edition (3-year)	—	—	01-SSC-5189
SonicWall NSv 400 Virtual Appliance TotalSecure Advanced Edition (3-year)	02-SSC-0911	02-SSC-0887	01-SSC-5219
SonicWall NSv 800 Virtual Appliance TotalSecure Advanced Edition (3-year)	02-SSC-0913	02-SSC-0891	01-SSC-5216
SonicWall NSv 1600 Virtual Appliance TotalSecure Advanced Edition (3-year)	02-SSC-0920	02-SSC-0897	01-SSC-5306
Product	AWS SKU <sup>1</sup>	Azure SKU	ESXi SKU
SonicWall NSv 10 Virtual Appliance TotalSecure Advanced Edition (5-year)	—	—	01-SSC-5584
SonicWall NSv 25 Virtual Appliance TotalSecure Advanced Edition (5-year)	—	—	01-SSC-5587
SonicWall NSv 50 Virtual Appliance TotalSecure Advanced Edition (5-year)	—	—	01-SSC-5649
SonicWall NSv 100 Virtual Appliance TotalSecure Advanced Edition (5-year)	—	—	01-SSC-5671
SonicWall NSv 200 Virtual Appliance TotalSecure Advanced Edition (5-year)	02-SSC-0901	02-SSC-0864	01-SSC-5581
SonicWall NSv 300 Virtual Appliance TotalSecure Advanced Edition (5-year)	—	—	01-SSC-5681
SonicWall NSv 400 Virtual Appliance TotalSecure Advanced Edition (5-year)	02-SSC-0910	02-SSC-0886	01-SSC-5684
SonicWall NSv 800 Virtual Appliance TotalSecure Advanced Edition (5-year)	02-SSC-0918	02-SSC-0890	01-SSC-5690
SonicWall NSv 1600 Virtual Appliance TotalSecure Advanced Edition (5-year)	02-SSC-0919	02-SSC-0896	01-SSC-5693

<sup>1</sup>Pending AWS Marketplace availability

## About Us

SonicWall has been fighting the cybercriminal industry for over 27 years, defending small, medium-sized businesses and enterprises worldwide. Our combination of products and partners has enabled an automated real-time breach detection and prevention solution tuned to the specific needs of the more than 500,000 organizations in over 215 countries and territories, so you can do more business with less fear. For more information, visit [www.sonicwall.com](http://www.sonicwall.com) or follow us on Twitter, LinkedIn, Facebook and Instagram.