SonicWall Network Security virtual (NSv) series

Deep security for public, private or hybrid cloud environments

The design, implementation and deployment of modern network architectures, such 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/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[1]. 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.

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 it 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

Benefits:

Public and private cloud security

- Gain complete visibility into intra-host communication between virtual machines for 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
- Implement proper security zoning and isolations

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

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[3], and with SonicWall Capture Cloud Security Center[3] (CCSC), an open, scalable cloud security management, monitoring, reporting and analytics software that is delivered as a cost-effective as-a-service offering. CCSC 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 NS*a* Series, SuperMassive™ Series and TZ Series.

Refer to the SonicWall SonicOS Platform datasheet for complete list of features and capabilities.

Automated breach prevention[1]

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

Around-the-clock security[1]

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

Zero-day protection[1]

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[1]

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.

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.

Deployment options[2]

NSv can be deployed on a wide variety of virtualized and cloud platforms for various private/public cloud security use cases.

---

[1] *Requires SonicWall Advanced Gateway Security Services (AGSS) subscription.*
[2] *Virtual machine image (VMI) support for MS Hyper-V, Amazon and MS Azure will be on a forthcoming release*
[3] *SonicWall Global Management System and Capture Cloud Security Center require separate licensing or subscription.*

SONICWALL®

SonicWall Global Management System (GMS)

Establish a managed security governance, compliance and risk management security program

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

NSv Series system specifications

Firewall General	NSv 10	NSv 25	NSv 50	NSv 100
Operating system	SonicOS			
Supported platform	VMware ESXi v5.5 / v6.0 / v6.5			
Max Cores	2	2	2	2
Max Mgmt/DataPlane Cores	1/1	1/1	1/1	1/1
Min Memory Required	4G	4G	4G	4G
Supported IP/Nodes	10	25	50	100
Storage	60 GB			
SSO users	25	50	100	100
Logging	Analyzer, Local Log, Syslog			
High availability	Active/Passive with State Sync			
Firewall/VPN Performance				
Connections per second	1,800	5,000	8,000	12,000
Maximum connections (SPI)	10,000	50,000	125,000	150,000
Maximum connections (DPI)	10,000	50,000	100,000	125,000
SSL DPI Connections	500	1,000	2,000	4,000
VPN				
Site-to-Site VPN Tunnels	10	10	25	50
IPSec VPN clients (max)	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				
IP address assignment	IP address assignment Static, DHCP, internal DHCP server, DHCP relay			
NAT modes	NAT modes 1:1, many:1, 1:many, flexible NAT (overlapping IPs), PAT, transparent mode			
VLAN interfaces	25	25	50	50
Routing protocols	BGP, OSPF, RIPv1/v2, static routes, policy-based routing, multicast			
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			

NSv Series system specifications con't

Firewall General	NSv 200	NSv 300	NSv 400	NSv 800	NSv 1600
Operating system	SonicOS				
Supported platform	VMware ESXi v5.5 / v6.0 / v6.5				
Max Cores	2	3	4	8	16
Max Mgmt/DataPlane Cores	1/1	1/2	1/3	1/8	1/15
Min Memory Required	4G	4G	6G	8G	10G
Supported IP/Nodes	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Storage	60 GB				
SSO users	500	5,000	10,000	15,000	20,000
Logging	Analyzer, Local Log, Syslog				
High availability	Active/Passive with State Sync				
Firewall/VPN Performance					
Connections per second	15,000	15,000	60,000	130,000	229,000
Maximum connections (SPI)	225,000	1M	1.5M	3M	4M
Maximum connections (DPI)	125,000	500,000	1.25M	2M	2.5M
TLS/SSL Connections	8,000	12,000	20,000	30,000	50,000
VPN					
Site-to-Site VPN Tunnels	75	100	6000	10,000	25,000
IPSec VPN clients (max)	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					
IP address assignment	IP address assignment Static, DHCP, internal DHCP server, DHCP relay				
NAT modes	NAT modes 1:1, many:1, 1:many, flexible NAT (overlapping IPs), PAT, transparent mode				
VLAN interfaces	50	256	500	512	512
Routing protocols	BGP, OSPF, RIPv1/v2, static routes, policy-based routing, multicast				
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				

NSv Series ordering information

Product	SKU
SonicWall NSv 10 Virtual Appliance Total Secure Advanced Edition (1-year)	01-SSC-5875
SonicWall NSv 25 Virtual Appliance Total Secure Advanced Edition (1-year)	01-SSC-5923
SonicWall NSv 50 Virtual Appliance Total Secure Advanced Edition (1-year)	01-SSC-5926
SonicWall NSv 100 Virtual Appliance Total Secure Advanced Edition (1-year)	01-SSC-5929
SonicWall Nsv 200 Virtual Appliance Total Secure Advanced Edition (1-year)	01-SSC-5950
SonicWall Nsv 300 Virtual Appliance Total Secure Advanced Edition (1-year)	01-SSC-6084
SonicWall NSv 400 Virtual Appliance Total Secure Advanced Edition (1-year)	01-SSC-5964
SonicWall NSv 800 Virtual Appliance Total Secure Advanced Edition (1-year)	01-SSC-6101
SonicWall NSv 1600 Virtual Appliance Total Secure Advanced Edition (1-year)	01-SSC-6108
NSv 10 support and security subscriptions	**SKU**
Advanced Gateway Security Suite Bundle for NSv 10 Virtual Appliance (1-year)	01-SSC-5008
Advanced Gateway Security Suite Bundle for NSv 10 Virtual Appliance (1-year)	01-SSC-4830
NSv 25 support and security subscriptions	**SKU**
Advanced Gateway Security Suite Bundle for NSv 25 Virtual Appliance (1-year)	01-SSC-5165
24x7 Support for NSv 25 Virtual Appliance (1-year)	01-SSC-5161
NSv 50 support and security subscriptions	**SKU**
Advanced Gateway Security Suite Bundle for NSv 50 Virtual Appliance (1-year)	01-SSC-5194
24x7 Support for NSv 50 Virtual Appliance (1-year)	01-SSC-5189
NSv 100 support and security subscriptions	**SKU**
Advanced Gateway Security Suite Bundle for NSv 100 Virtual Appliance (1-year)	01-SSC-5219
24x7 Support for NSv 100 Virtual Appliance (1-year)	01-SSC-5216
NSv 200 support and security subscriptions	**SKU**
Advanced Gateway Security Suite Bundle for NSv 200 Virtual Appliance (1-year)	01-SSC-5306
Capture Advanced Threat Protection for NSv 200 Virtual Appliance (1-year)	01-SSC-5309
Content Filtering Service Premium Business Edition for NSv 200 Virtual Appliance (1-year)	01-SSC-5335
Gateway Anti-Malware, Intrusion Prevention And Application Control for NSv 200 Virtual Appliance (1-year)	01-SSC-5364
24x7 Support for NSv 200 Virtual Appliance (1-year)	01-SSC-5303
NSv 300 support and security subscriptions	**SKU**
Advanced Gateway Security Suite Bundle for NSv 300 Virtual Appliance (1-year)	01-SSC-5584
Capture Advanced Threat Protection for NSv 300 Virtual Appliance (1-year)	01-SSC-5587
Content Filtering Service Premium Business Edition for NSv 300 Virtual Appliance (1-year)	01-SSC-5649
Gateway Anti-Malware, Intrusion Prevention And Application Control for NSv 300 Virtual Appliance (1-year)	01-SSC-5671
24x7 Support for NSv 300 Virtual Appliance (1-year)	01-SSC-5581
NSv 400 support and security subscriptions	**SKU**
Advanced Gateway Security Suite Bundle for NSv 400 Virtual Appliance (1-year)	01-SSC-5681
Capture Advanced Threat Protection for NSv 400 Virtual Appliance (1-year)	01-SSC-5684
Content Filtering Service Premium Business Edition for NSv 400 Virtual Appliance (1-year)	01-SSC-5690
Gateway Anti-Malware, Intrusion Prevention And Application Control for NSv 400 Virtual Appliance (1-year)	01-SSC-5693
24x7 Support for NSv 400 Virtual Appliance (1-year)	01-SSC-5678
NSv 800 support and security subscriptions	**SKU**
Advanced Gateway Security Suite Bundle for NSv 800 Virtual Appliance (1-year)	01-SSC-5737
Capture Advanced Threat Protection for NSv 800 Virtual Appliance (1-year)	01-SSC-5748
Content Filtering Service Premium Business Edition for NSv 800 Virtual Appliance (1-year)	01-SSC-5774
Gateway Anti-Malware, Intrusion Prevention And Application Control for NSv 800 Virtual Appliance (1-year)	01-SSC-5777
24x7 Support for NSv 800 Virtual Appliance (1-year)	01-SSC-5709
NSv 1600 support and security subscriptions	**SKU**
Advanced Gateway Security Suite Bundle for NSv 1600 Virtual Appliance (1-year)	01-SSC-5787
Capture Advanced Threat Protection for NSv 1600 Virtual Appliance (1-year)	01-SSC-5789
Content Filtering Service Premium Business Edition for NSv 1600 Virtual Appliance (1-year)	01-SSC-5801
Gateway Anti-Malware, Intrusion Prevention And Application Control for NSv 1600 Virtual Appliance (1-year)	01-SSC-5803
24x7 Support for NSv 1600 Virtual Appliance (1-year)	01-SSC-5785
Management, Reporting and Analytics	**SKU**
SonicWall GMS 10-node software license	01-SSC-3363
SonicWall GMS E-Class 24x7 Software Support for 10 nodes (1-year)	01-SSC-6514
SonicWall Scrutinizer virtual appliance with Flow Analytics Module software license for up to 5 nodes (includes one year of 24x7 Software Support)	01-SSC-3443
SonicWall Scrutinizer with Flow Analytics Module software license for up to 5 nodes (includes one year of 24x7 Software Support)	01-SSC-4002
SonicWall Scrutinizer Advanced Reporting Module software license for up to 5 nodes (includes one year of 24x7 Software Support)	01-SSC-3773

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear.

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

Datasheet-NSvVirtualFirewalls-US-VG-MKTG2509

SONICWALL®