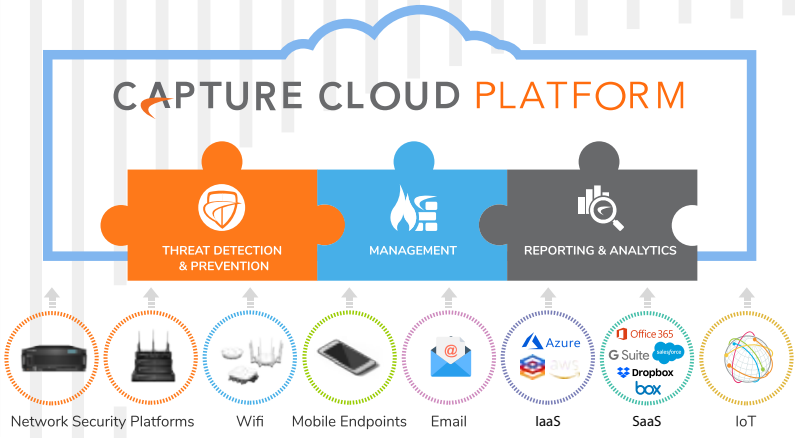
SonicWall Network Security virtual (NSv) firewall series

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, demonstrates significant operational and economic advantages. However, vulnerabilities within virtual environments are well-documented. New vulnerabilities are discovered regularly that yield serious security implications and challenges. To ensure applications and services are delivered safely, efficiently and in a scalable manner, while still combating threats harmful to all parts of the virtual framework including virtual machines (VMs), application workloads and data must be among the top priorities.



BENEFITS

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 control
- Application intelligence and control
- Segmentation security and security zoning
- Support across private cloud (ESXi, Hyper-V) and public cloud (AWS, Azure) platforms
- BYOL and PAYG licensing

Virtual machine protection

- Zero-day threat protection with Capture ATP
- Data confidentiality
- Secure communication with data leakage prevention
- Traffic validation, inspection and monitoring
- System safety and integrity
- Virtual network resilience and availability

Find the right SonicWall virtual solution for your business:
sonicwall.com/NSv

DATASHEET

The SonicWall Network Security virtual (NS*v*) firewall series helps security teams reduce these types of security risks and vulnerabilities, which can cause serious disruption to your business-critical services and operations. NS*v* next-generation virtual firewalls integrate two advanced security technologies to deliver cutting-edge threat prevention that keeps your network one step ahead.

SonicWall's RTDMI™ and RFDPI® Technology

SonicWall's patent-pending Real-Time Deep Memory Inspection (RTDMI™) technology enhances our award-winning multi-engine Capture Advanced Threat Protection (ATP) sandboxing service. The RTDMI engine proactively detects and blocks mass market, zero-day threats and unknown malware by inspecting directly in memory. Because of the real-time architecture, SonicWall RTDMI technology is precise, minimizes false positives, and identifies and mitigates sophisticated attacks where the malware's weaponry is exposed for less than 100 nanoseconds. In combination, SonicWall's patented* single-pass Reassembly-Free Deep Packet Inspection (RFDPI®) engine examines every byte of every packet, inspecting both inbound and outbound traffic on the firewall.

The NS*v* series delivers the automated real-time breach detection and prevention organizations need by utilizing innovative deep learning technologies in the SonicWall Capture Cloud Platform. This platform delivers cloud-based threat prevention and network management plus reporting and analytics for organizations of any size. This platform consolidates threat intelligence gathered from multiple sources including our Capture ATP, as well as more than 1 million SonicWall sensors located around the globe. By leveraging the SonicWall Capture Cloud Platform in addition to capabilities including intrusion prevention, anti-malware and web/URL filtering, the NS*v* series blocks even the stealthiest threats at the gateway.

NS*v* is easily deployed and provisioned in a virtual environment, typically between virtual networks (VNs) or virtual private clouds (VPCs). 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 VM safety and integrity. Security threats (such as cross-virtual-machine or side-channel attacks, common network-based intrusions, and application and protocol vulnerabilities) are neutralized successfully through SonicWall's comprehensive suite of security inspection services1. 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 ATP multi-engine sandboxing with RTDMI technology.

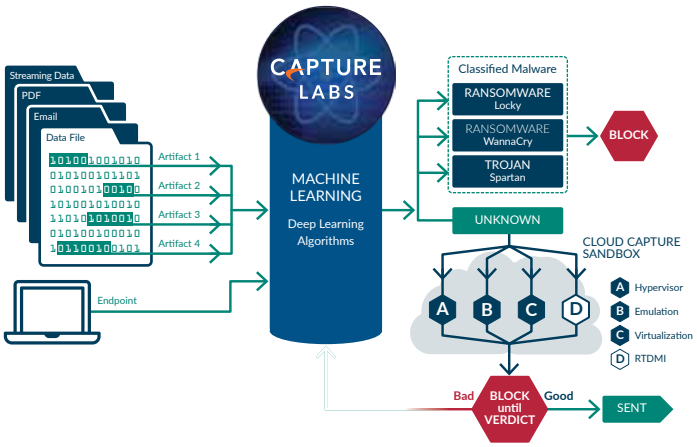
Segmentation Security

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, NS*v* 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.

NS*v* automatically enforces segmentation restrictions based upon dynamic criteria, such as user identity credentials, geo-IP location and the security stature of mobile endpoints. For extended security, NS*v* 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 manages segment security enforcement from a single pane of glass.

Since segments are only as effective as the security that can be enforced between them, NS*v* applies intrusion prevention system (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.

* U.S. Patents 7,310,815; 7,600,257; 7,738,380; 7,835,361; 7,991,723



Flexible Deployment Use Cases

With infrastructure support for high availability implementation, NS*v* fulfills scalability and availability requirements of Software Defined Data Centers. It ensures system resiliency, service reliability, and regulatory conformance. Optimized for broad range of public, private and hybrid deployment use cases, NS*v* 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 with 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 NS*v* series is available in multiple virtual flavors carefully packaged for a broad range of virtualized and cloud deployment use cases. Delivering multi-gigabit threat prevention and encrypted traffic inspection performance, the NS*v* series adapts to capacity-level increases and ensures VN and VPC safety. The series also ensures application workloads and data assets are available as well as secure.

Govern Centrally

NS*v* deployments can be centrally managed either on premises with SonicWall Global Management System (GMS²), or with Capture Security Center², SonicWall's open, scalable cloud security management, monitoring, reporting and analytics platform 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.

Unified Policy with SonicOSX 7.0

SonicWall SonicOSX 7.0 and upwards features Unified Policy that offers integrated management of various security policies across SonicWall on-prem and virtual firewalls, starting with the NS*v* series.

It comes with a new web interface that supports a radically different approach – the emphasis is on user-first design.

It leads to an intuitive set up of contextual security policies through actionable alerts, and with point-and-click simplicity.

Visually, it is also more attractive than the classic interface. In a single-pane view of a firewall, the interface presents the user with information on the effectiveness of various security rules.

It enables the user to modify the predefined rules for gateway antivirus, antispyware, content filtering, intrusion prevention, geo-IP filtering, and deep-packet inspection of encrypted traffic in a seamless fashion.

With the Unified Policy, SonicWall delivers a more streamlined experience that reduces configuration errors and deployment time for a better overall security posture.

Flexible Licensing

NS*v* supports Bring Your Own License (BYOL) and Pay As You Go (PAYG) licensing. The BYOL license for NS*v* can be purchased directly from SonicWall, a partner or reseller. Whereas, PAYG license is purchased directly from the AWS Marketplace. This type of license is a usage-based license wherein payment is made as per usage on an hourly or annual basis.

Govern 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

- 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

Features

SonicOS Platform

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

Automated breach prevention[1]

NS*v* delivers complete advanced threat protection, including high-performance intrusion and malware prevention, and cloud-based sandboxing with SonicWall's RTDMI technology.

Around-the-clock security[1]

NS*v* ensures lateral movement protection, plus inbound and outbound traffic protection. New threat updates are automatically pushed to firewalls with active security services, and take effect immediately without reboots or interruptions.

Zero-day protection[1]

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

Threat API

NS*v* 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

NS*v* strengthens internal security by enabling segmentation of 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]

NS*v* provides granular control over network traffic at the user, email address, schedule, and IP-subnet levels, with application-specific policies. It controls custom applications by creating signatures based on specific parameters or patterns unique to an application. Internal or external network access is allowed or denied based on various criteria.

Data leakage prevention

NS*v* provides the ability to scan streams of data for keywords. This restricts 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

NS*v* can select among various bandwidth management settings to reduce network bandwidth usage by an application using packet monitor. This provides further control over the network.

Secure communication
NS*v* ensures the data exchange between groups of virtual machines is done securely, including isolation, confidentiality, integrity, and information flow control within these networks via the use of segmentation.

Access control
NS*v* validates that only VMs that satisfy a given set of conditions are able to access data belonging to another through the use of VLANs.

User authentication
NS*v* creates policies to control or restrict VM and workload access by unauthorized users.

Data confidentiality
NS*v* blocks information theft and illegitimate access to protected data and services.

Virtual network resilience and availability
NS*v* prevents disruption or degradation of application services and communications.

System safety and integrity
NS*v* stops unauthorized takeover of VM systems and services.

Traffic validation, inspection and monitoring mechanisms
NS*v* detects irregularities and malicious behaviors to stop attacks targeting VM workloads.

Deployment options
NS*v* can be deployed on a wide variety of virtualized and cloud platforms for various private/public cloud security use cases.

Flexible Licensing Models
SonicWall offers perpetual and non-perpetual licensing models. Perpetual licensing is a traditional operating model where the firewall and security service licenses must be purchased separately. Hence, these licenses expire separately. Non-perpetual licensing is a unique offering wherein the firewall and security service licenses are bundled together and expire at the same time. For public cloud deployments, both perpetual and non-perpetual licensing are available as Bring Your Own License (BYOL) model.

SonicWall non-perpetual or subscription licensing model provides flexibility and simplicity, as a single SKU bundles firewall software and security services. This is available across both private cloud (ESXi and Hyper-V) and public cloud (AWS, Azure) offerings. Service expiration notifications are sent before service expires.

Non-perpetual licensing model is available in three flavors– IPS/App Control Subscription, TotalSecure Subscription and TotalSecure Advanced Subscription, over a one year period. Based on the offering tiers, NS*v* software is bundled in a combination of Intrusion Prevention System (IPS), application control, support, Capture Security Center (CSC), Comprehensive Gateway Security Suite (CGSS) or Advanced Gateway Security Suite (AGSS).

[1]Requires SonicWall Advanced Gateway Security Services (AGSS) subscription.
[2]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[1]			
Supported Hypervisors	VMware ESXi v5.5 / v6.0 / v6.5 / v6.7, Microsoft Hyper-V Win 2012 / 2016, KVM Ubuntu 16.04 / CentOS 7, Nutanix AHV (AOS 5.15 LTS/Prism Central 5.16.1.2)[9]			
Supported Public Cloud Platforms (Instance Type)	AWS (c5.large), Azure (Std D2 v2)			
Licensing	BYOL, PAYG[2]			
Max Supported vCPUs	2	2	2	2
Interface Count (ESXi/Hyper-V/KVM)	8/8/8	8/8/8	8/8/8	8/8/8
Max Mgmt/DataPlane Cores	1/1	1/1	1/1	1/1
Min Memory[3]	4 GB	4 GB	4 GB	4 GB
Max Memory[4]	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	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)	10(10)	10(25)	10(25)
SSL VPN Clients Included[7]	2	2	2	2
SSL VPN Clients Maximum[7]	50	50	50	50
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			

NSv Series system specifications continued

Networking	NSv 10	NSv 25	NSv 50	NSv 100
IP address assignment	Static, DHCP, internal DHCP server[10], DHCP relay[10]			
NAT modes	1:1, many:1, 1:many, flexible NAT (overlapping IPs), PAT			
Max VLAN	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	SIP			
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, L2TP, PPTP, RADIUS			
Max SD-WAN groups	12	12	18	32
Max SD-WAN members per product	24	24	36	64

Firewall General	NSv 200	NSv 300	NSv 400	NSv 800	NSv 1600
Operating system	SonicOS[1]				
Supported Hypervisors	VMware ESXi v5.5 / v6.0 / v6.5 / v6.7, Microsoft Hyper-V, KVM Ubuntu 16.04 / CentOS 7, Nutanix AHV (AOS 5.15 LTS/Prism Central 5.16.1.2)[9]				
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)
Licensing	BYOL, PAYG[2]				
Max Supported vCPUs	2	3	4	8	16
Interface Count (ESXi/Hyper-V/KVM/AWS/Azure)	8/8/8/2/2	8/8/8/-/-	8/8/8/4/4	8/8/8/8/8	8/8/8/8/8
Max Mgmt/DataPlane Cores	1/1	1/2	1/3	1/7	1/15
Min Memory[3]	6 GB	6 GB	8 GB	10 GB	12 GB
Max Memory[4]	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[5]				

Firewall/VPN Performance[6]	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

NSv Series system specifications continued

Firewall/VPN Performance[6]	NSv 200	NSv 300	NSv 400	NSv 800	NSv 1600
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 Clients Included[7]	2	2	2	2	2
SSL VPN Clients Maximum[7]	100	150	200	300	400
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[10], DHCP relay[10]				
NAT modes	1:1, many:1, 1:many, flexible NAT (overlapping IPs), PAT				
Max VLAN[8]	128	128	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				
VoIP	SIP				
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, L2TP, PPTP, RADIUS				
Max SD-WAN groups	38	38	70	102	102
Max SD-WAN members per product	76	76	140	204	204

[1]Currently supporting SonicOS 6.5.x.
[2]PAYG is currently available only on AWS.
[3]Memory with Jumbo frame disabled.
[4]Memory with Jumbo frame enabled. Additional memory is required for Jumbo frames. Jumbo frames are not supported on Azure and AWS.
[5]High availability available on VMware ESXi platform, Azure and Microsoft Hyper-V, while HA is not supported on AWS. Available on Azure from SonicOS 6.5.4.4-44v-21-987 firmware and onwards.
[6]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.
[7]Increased SSL VPN number will be available only from SonicOS 6.5.4.4-44v-21-723 firmware and onwards.
[8]VLAN interfaces are not supported on Azure and AWS.
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.
[9]Certified on SonicOS 6.5.4.4-44v-21-757 firmware
[10]Supported on Private Cloud and not on Public Cloud Platforms

Features

RFDPI Engine

Feature	Description
Reassembly-Free Deep Packet Inspection (RFDPI)	This high-performance, proprietary and patented inspection engine performs stream-based, bi-directional traffic analysis, without proxying or buffering, to uncover intrusion attempts and malware and to identify application traffic regardless of port.
Bi-directional inspection	Scans for threats in both inbound and outbound traffic simultaneously to ensure that the network is not used to distribute malware and does not become a launch platform for attacks in case an infected machine is brought inside.
Stream-based inspection	Proxy-less and non-buffering inspection technology provides ultra-low latency performance for DPI of millions of simultaneous network streams without introducing file and stream size limitations, and can be applied on common protocols as well as raw TCP streams.
Highly parallel and scalable	The unique design of the RFDPI engine works with the multi-core architecture to provide high DPI throughput and extremely high new session establishment rates to deal with traffic spikes in demanding networks.
Single-pass inspection	A single-pass DPI architecture simultaneously scans for malware, intrusions and application identification, drastically reducing DPI latency and ensuring that all threat information is correlated in a single architecture.

Firewall and Networking

Feature	Description
REST APIs	Allows the firewall to receive and leverage 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.
Stateful packet inspection	All network traffic is inspected, analyzed and brought into compliance with firewall access policies.
High availability[1]	The NS*v* series supports Active/Passive (A/P) with state synchronization.
DDoS/DoS attack protection	SYN flood protection provides a defense against DoS attacks using both Layer 3 SYN proxy and Layer 2 SYN blacklisting technologies. Additionally, it protects against DoS/DDoS through UDP/ICMP flood protection and connection rate limiting.
IPv6 support	Internet Protocol version 6 (IPv6) is in its early stages to replace IPv4. With SonicOS, the hardware will support filtering and wire mode implementations.
Flexible deployment options	The NS*v* series can be deployed in traditional NAT, Layer 2 bridge, wire and network tap modes.
WAN load balancing	Load-balances multiple WAN interfaces using Round Robin, Spillover or Percentage methods.
Advanced quality of service (QoS)	Guarantees critical communications with 802.1p, DSCP tagging, and remapping of VoIP traffic on the network.
SIP proxy support	Blocks spam calls by requiring that all incoming calls are authorized and authenticated by SIP proxy.
Biometric authentication	Supports mobile device authentication such as fingerprint recognition that cannot be easily duplicated or shared to securely authenticate the user identity for network access.
Open authentication and social login	Enable guest users to use their credentials from social networking services such as Facebook, Twitter, or Google+ to sign in and access the Internet and other guest services through a host's wireless, LAN or DMZ zones using pass-through authentication.

Management and Reporting

Feature	Description
Cloud-based and on-premises management	Configuration and management of SonicWall appliances is available via the cloud through the SonicWall Capture Security Center and on-premises using SonicWall Global Management System (GMS).
Powerful single device management	An intuitive web-based interface allows quick and convenient configuration, in addition to a comprehensive command-line interface and support for SNMPv2/3.
IPFIX/NetFlow application flow reporting	Exports application traffic analytics and usage data through IPFIX or NetFlow protocols for real-time and historical monitoring and reporting with tools such as SonicWall Scrutinizer or other tools that support IPFIX and NetFlow with extensions.

Virtual Private Networking (VPN)

Feature	Description
Auto-provision VPN	Simplifies and reduces complex distributed firewall deployment down to a trivial effort by automating the initial site-to-site VPN gateway provisioning between SonicWall firewalls while security and connectivity occurs instantly and automatically.
IPSec VPN for site-to-site connectivity	High-performance IPSec VPN allows the NS*v* series to act as a VPN concentrator for thousands of other large sites, branch offices or home offices.
SSL VPN or IPSec client remote access	Utilizes clientless SSL VPN technology or an easy-to-manage IPSec client for easy access to email, files, computers, intranet sites and applications from a variety of platforms.

[1]High availability is currently not supported on AWS

Features

Virtual Private Networking (VPN) Continued	
Feature	Description
Redundant VPN gateway	When using multiple WANs, a primary and secondary VPN can be configured to allow seamless, automatic failover and failback of all VPN sessions.
Route-based VPN	The ability to perform dynamic routing over VPN links ensures continuous uptime in the event of a temporary VPN tunnel failure, by seamlessly re-routing traffic between endpoints through alternate routes.

Content/Context Awareness	
Feature	Description
User activity tracking	User identification and activity are made available through seamless AD/LDAP/Citrix1/Terminal Services1 SSO integration combined with extensive information obtained through DPI.
GeoIP country traffic identification	Identifies and controls network traffic going to or coming from specific countries to either protect against attacks from known or suspected origins of threat activity, or to investigate suspicious traffic originating from the network. Ability to create custom country and Botnet lists to override an incorrect country or Botnet tag associated with an IP address. Eliminates unwanted filtering of IP addresses due to misclassification.
Regular expression DPI filtering	Prevents data leakage by identifying and controlling content crossing the network through regular expression matching. Provides the ability to create custom country and Botnet lists to override an incorrect country or Botnet tag associated with an IP address.

Breach Prevention Subscription Services

Capture Advanced Threat Protection	
Feature	Description
Multi-engine sandboxing	The multi-engine sandbox platform, which includes virtualized sandboxing, full system emulation, and hypervisor level analysis technology, executes suspicious code and analyzes behavior, providing comprehensive visibility to malicious activity.
Real-Time Deep Memory Inspection (RTDMI)	This patent-pending cloud-based technology detects and blocks malware that does not exhibit any malicious behavior and hides its weaponry via encryption. By forcing malware to reveal its weaponry into memory, the RTDMI engine proactively detects and blocks mass-market, zero-day threats and unknown malware.
Block until verdict	To prevent potentially malicious files from entering the network, files sent to the cloud for analysis can be held at the gateway until a verdict is determined.
Broad file type and size analysis	Supports analysis of a broad range of file types, either individually or as a group, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, Mac OS X and multi-browser environments.
Rapid deployment of signatures	When a file is identified as malicious, a signature is immediately deployed to firewalls with SonicWall Capture ATP subscriptions and Gateway Anti-Virus and IPS signature databases and the URL, IP and domain reputation databases within 48 hours.
Capture Client	Capture Client is a unified client platform that delivers multiple endpoint protection capabilities, including advanced malware protection and support for visibility into encrypted traffic. It leverages layered protection technologies, comprehensive reporting and endpoint protection enforcement.

Encrypted Threat Prevention	
Feature	Description
TLS/SSL decryption and inspection	Decrypts and inspects TLS/SSL encrypted traffic on the fly, without proxying, for malware, intrusions and data leakage, and applies application, URL and content control policies in order to protect against threats hidden in encrypted traffic. Included with security subscriptions for all NS*v* series models.
SSH inspection	Deep packet inspection of SSH (DPI-SSH) decrypts and inspect data traversing over SSH tunnel to prevent attacks that leverage SSH.

Intrusion Prevention	
Feature	Description
Countermeasure-based protection	Tightly integrated intrusion prevention system (IPS) leverages signatures and other countermeasures to scan packet payloads for vulnerabilities and exploits, covering a broad spectrum of attacks and vulnerabilities.
Automatic signature updates	The SonicWall Threat Research Team continuously researches and deploys updates to an extensive list of IPS countermeasures that covers more than 50 attack categories. The new updates take immediate effect without any reboot or service interruption required.
Intra-zone IPS protection	Bolsters internal security by segmenting the network into multiple security zones with intrusion prevention, preventing threats from propagating across the zone boundaries.
Botnet command and control (CnC) detection and blocking	Identifies and blocks command and control traffic originating from bots on the local network to IPs and domains that are identified as propagating malware or are known CnC points.

Features

Intrusion Prevention Continued	
Feature	Description
Protocol abuse/anomaly	Identifies and blocks attacks that abuse protocols in an attempt to sneak past the IPS.
Zero-day protection	Protects the network against zero-day attacks with constant updates against the latest exploit methods and techniques that cover thousands of individual exploits.
Anti-evasion technology	Extensive stream normalization, decoding and other techniques ensure that threats do not enter the network undetected by utilizing evasion techniques in Layers 2-7.

Threat Prevention	
Feature	Description
Gateway anti-malware	The RFDPI engine scans all inbound, outbound and intra-zone traffic for viruses, Trojans, key loggers and other malware in files of unlimited length and size across all ports and TCP streams.
Capture Cloud malware protection	A continuously updated database of tens of millions of threat signatures resides in the SonicWall cloud servers and is referenced to augment the capabilities of the onboard signature database, providing RFDPI with extensive coverage of threats.
Around-the-clock security updates	New threat updates are automatically pushed to firewalls in the field with active security services, and take effect immediately without reboots or interruptions.
Bi-directional raw TCP inspection	The RFDPI engine is capable of scanning raw TCP streams on any port bi-directionally preventing attacks that they to sneak by outdated security systems that focus on securing a few well-known ports.
Extensive protocol support	Identifies common protocols such as HTTP/S, FTP, SMTP, SMBv1/v2 and others, which do not send data in raw TCP, and decodes payloads for malware inspection, even if they do not run on standard, well-known ports.

Application Intelligence and Control	
Feature	Description
Application control	Control applications, or individual application features, that are identified by the RFDPI engine against a continuously expanding database of over thousands of application signatures, to increase network security and enhance network productivity.
Custom application identification	Control custom applications by creating signatures based on specific parameters or patterns unique to an application in its network communications, in order to gain further control over the network.
Application bandwidth management	Granularly allocate and regulate available bandwidth for critical applications or application categories while inhibiting nonessential application traffic.
Granular control	Control applications, or specific components of an application, based on schedules, user groups, exclusion lists and a range of actions with full SSO user identification through LDAP/AD/Terminal Services/Citrix integration.

Content Filtering	
Feature	Description
Inside/outside content filtering	Enforce acceptable use policies and block access to HTTP/HTTPS websites containing information or images that are objectionable or unproductive with Content Filtering Service and Content Filtering Client.
Enforced Content Filtering Client	Extend policy enforcement to block internet content for Windows, Mac OS, Android and Chrome devices located outside the firewall perimeter.
Granular controls	Block content using the predefined categories or any combination of categories. Filtering can be scheduled by time of day, such as during school or business hours, and applied to individual users or groups.
Web caching	URL ratings are cached locally on the SonicWall firewall so that the response time for subsequent access to frequently visited sites is only a fraction of a second.

Enforced Antivirus and Anti-Spyware	
Feature	Description
Multi-layered protection	Utilize the firewall capabilities as the first layer of defense at the perimeter, coupled with endpoint protection to block, viruses entering network through laptops, thumb drives and other unprotected systems.
Automated enforcement option	Ensure every computer accessing the network has the appropriate antivirus software and/or DPI-SSL certificate installed and active, eliminating the costs commonly associated with desktop antivirus management.
Automated deployment and installation option	Machine-by-machine deployment and installation of antivirus and anti-spyware clients is automatic across the network, minimizing administrative overhead.
Next-generation antivirus	Capture Client uses a static artificial intelligence (AI) engine to determine threats before they can execute and roll back to a previous uninfected state.
Spyware protection	Powerful spyware protection scans and blocks the installation of a comprehensive array of spyware programs on desktops and laptops before they transmit confidential data, providing greater desktop security and performance.

[1]. High availability is currently not supported on AWS

SonicOS feature summary

Global control over

- Centralized control of IPv6 visibility
- Globally disabling IPv6 traffic processing
- Disabling default VPN policies, configuration screens, and auto-generated rules

Login and user security

- User lockout based on login attempts by IP address range
- User lockout from CLI
- Force password change on the first login
- Two-factor authentication (TOTP) support
- Guest user policy zero-touch portal support
- Guest service IPv6 support
- TACACS+ accounting support
- Quota control for all users
- Dynamic botnet HTTP authentication

Networking and system

- SD-WAN support
- DNS security / DNS sinkhole support
- FQDN over TCP DNS
- FQDN address objects for NAT
- DHCPv6 relay
- IPv6 addressing mode for H.323 VoIP application layer gateway
- Multiple control plane (CP) core support
- HTTP/HTTPS redirection with data plane offload
- IP helper offload to data plane
- Firmware backup on local storage
- High availability encryption
- High availability firmware upload support
- Policy based routing optimization of static and dynamic routes
- Performance/ throughput improvements
- Watchdog feature to monitor firewall health
- Enhanced scalability for advanced routing over VPN numbered tunnel interfaces
- Update H.323 libraries based on OSS Noklava v10.5.0 ASN.1 compiler
- Task thread priority updates
- SSLVPN and bookmark on Data Plane

Security services

- Capture ATP block until verdict granular control
- Capture ATP friendly filename display for non-HTTP protocols
- CFS blocking of individual YouTube videos
- Support HTTPS content filtering and DPI-SSL together
- Next gen anti-virus (SentinelOne) and DPI-SSL enforcement
- Wan DDOS protection performance enhancement

Policies / objects

- Access rule enhancements
- App based routing
- Dynamic address objects
- CFS policy exclusion
- Policy based HTTPS content filter objects
- URI list groups support in content filter objects
- CFS custom header insertion for HTTP requests
- UUID for rules and objects
- UUID for CFS policies
- Source MAC override for NAT policies

DPI-SSL / DPI-SSH

- DPI-SSL dynamic cloud based white list
- DPI-SSH blocking of SSH port forwarding
- DPI-SSH blocking of X11 forwarding
- SSL decryption port preservation in packet mirror / packet capture
- DPI-SSL granular control per zone
- Access rules based DPI-SSL control
- DPI-SSL client block or allow expired CA certificates
- TLS certificate status request extension
- Support for local CRL
- Enhanced DPI-SSL certificate verification
- Support for ECDSA-related ciphers
- OpenSSL LTS release support for federal certification

Logging, monitoring and reporting

- Ability to verify that DPI was performed on a specific packet
- Filename and URI logging for app control
- Logon records displayed for administrator
- Configuration auditing
- Logging of NAT mapping for TCP connections
- FTP support for log automation
- Capture Security Center (CSC) reporting & analytics support for NS*v*
- Capture ATP logging of email sender/recipient
- Capture threat assessment client enhancements (SWARM v3)
- Function to reset the SFR (SWARM) statistical data
- Option to select output language for SonicFlow report

API

- SonicOS API phase 1
- SonicOS API authentication support
- SonicOS API phase 2
- LHM RESTful API

SonicOS web management UI

- SonicOS global search
- Usability improvements for content pages
- Per user client side UI preferences storage
- Pin friendly name to SonicOS web management screens
- Refactored SonicOS web interface layout

Learn more about SonicWall NS*v* Series

www.sonicwall.com/NS*v*

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.

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

© 2021 SonicWall Inc. ALL RIGHTS RESERVED.

Datasheet-NS*v*VirtualFirewalls-COG-4307

Authorized Distributor :

SecureOne
Optimize with SECURITY

HQ Office (KL)
SecureOne Distribution Sdn Bhd (828358 - X)
No.7, Jalan 109E, Desa Business Park,
Taman Desa, Jalan Kelang Lama,
58100 Kuala Lumpur, Malaysia.

Tel: +6(03) 7984 6086 Fax: +6(03) 7984 6032
Email: sales@secureone.com.my

Northern Office
SecureOne Distribution (Northern) Sdn Bhd (977172 - H)
1A-2-02 @ One Precint (1160),
Lengkok Mayang Pasir,
11950 Bayan Baru, Penang, Malaysia.

Tel: +6(04) 619 2692 Fax: +6(04) 619 2699
Email: northern@secureone.com.my

www.secureone.com.my