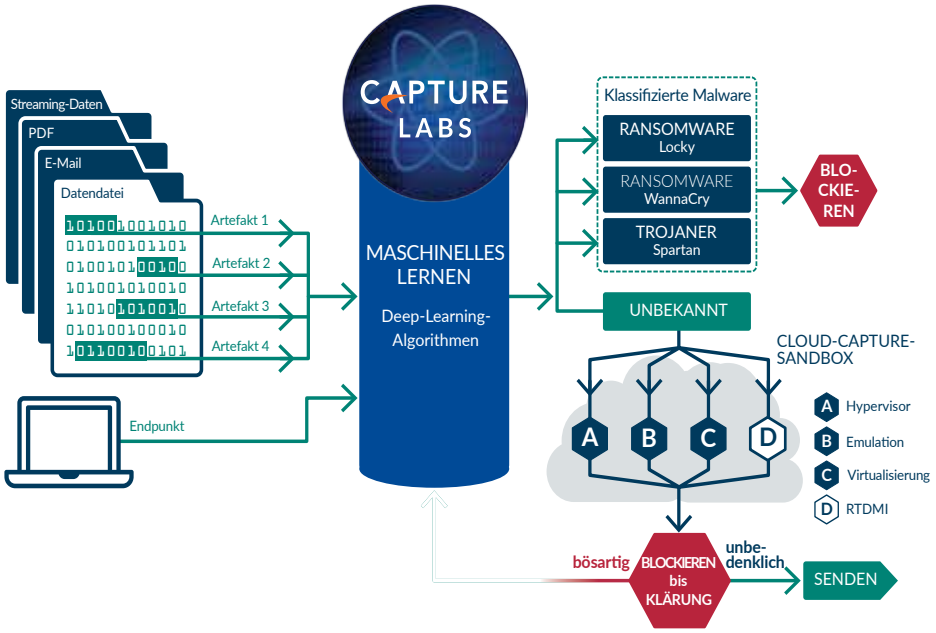
SonicWall Network Security virtual (NSv) Series

Umfassende Sicherheit für Public-, Private- und Hybrid-Cloud-Umgebungen

Nach wie vor sind Design, Implementierung und Nutzung moderner Netzwerkarchitekturen wie Virtualisierung und Cloud ein wesentlicher Erfolgsfaktor für viele Organisationen. Die Virtualisierung des Rechenzentrums, die Migration in die Cloud oder eine Kombination davon bieten bedeutende operative und wirtschaftliche Vorteile. Allerdings gibt es auch gut dokumentierte Schwachstellen innerhalb virtueller Umgebungen. Regelmäßig werden neue Schwachstellen aufgedeckt, die ernsthafte Herausforderungen und Probleme für die Sicherheit bedeuten. Um eine sichere, effiziente und skalierbare Bereitstellung von Anwendungsservices zu gewährleisten und gleichzeitig Bedrohungen zu bekämpfen, die alle Teile des virtuellen Frameworks einschließlich virtueller Maschinen (VMs) betreffen, sollten Anwendungs-Workloads und Daten ganz oben auf der Prioritätenliste stehen.

Die Firewalls der SonicWall Network Security virtual (NSv) Series unterstützen Ihre Security Mitarbeiter im Kampf gegen diese Sicherheitsrisiken und Schwachstellen, die Ihre geschäftskritischen Services und Prozesse ernsthaft beeinträchtigen können. Mit umfassenden Sicherheitstools und -services wie etwa Reassembly-Free Deep Packet Inspection (RFDPI), Sicherheitskontrollen und Netzwerkdiensten, die dieselbe Leistung wie eine physische SonicWall-Firewall bieten, schützt die NSv Series alle kritischen Komponenten Ihrer Private-/Public-Cloud-Umgebungen effektiv vor Bedrohungen.

Die NSv-Firewalls lassen sich spielend leicht in einer mandantenfähigen virtuellen Umgebung – typischerweise zwischen virtuellen Netzwerken (VNs) – implementieren und bereitstellen. Auf diese Weise können sie einerseits strenge Zugriffskontrollen anwenden, um die Vertraulichkeit von Informationen und die Sicherheit und Integrität der VMs zu gewährleisten, und andererseits die Kommunikation und den Datenaustausch zwischen virtuellen Maschinen überwachen und so für eine automatisierte Breach-Prevention sorgen. Sicherheitsbedrohungen (wie z. B. Attacken, die zwischen virtuellen Maschinen laufen, Side-Channel-Angriffe, gängige netzwerkbasierte Eindringversuche sowie Anwendungs- und Protokollschwachstellen) werden durch die umfassende SonicWall-Suite leistungsstarker Security-Inspection-Services erfolgreich gestoppt. Der gesamte VM-Datenverkehr wird von mehreren Bedrohungsanalyse-Engines verschiedenen Prüfungen unterzogen, darunter Intrusion-Prevention, Gateway-Anti-Virus und -Anti-Spyware, Cloud-Anti-Virus, Botnet-Filtering, Anwendungskontrolle und Capture Advanced Threat Protection-Multi-Engine-Sandboxing.



Vorteile:

Sicherheit in Public und Private Clouds

- Umfassender Einblick in die Intra-Host-Kommunikation zwischen virtuellen Maschinen, um einen effektiven Bedrohungsschutz zu garantieren
- Geeignete Platzierung von Sicherheitsregeln für Anwendungen in der gesamten virtuellen Umgebung
- Regeln für ein sicheres Application-Enablement nach Anwendung, Benutzer und Inhalt unabhängig vom VM-Standort
- Implementierung geeigneter Sicherheitszonen sowie Isolierung

Schutz virtueller Maschinen

- Schutz vor Zero-Day-Schwachstellen dank Capture Advanced Threat Protection (ATP)
- Verhindern einer unerlaubten Übernahme virtueller Systeme
- Stoppen eines unerlaubten Zugriffs auf geschützte Datenressourcen
- Blockieren von bösartigen Aktivitäten und Eindringversuchen, wie z. B. Verbreitung von Malware, Ausführung von Betriebssystembefehlen, Durchsuchung des Dateisystems und Ausführung von C&C-Kommunikation
- Vermeidung von Serviceunterbrechungen des gesamten virtuellen Ökosystems bzw. von Teilen davon

Sicherheit durch Segmentierung

Für einen optimalen Schutz vor Advanced Persistent Threats (APTs) muss bei der Netzwerksegmentierung ein integrierter Satz an dynamischen, durchsetzbaren Abwehrmechanismen gegen hoch entwickelte Bedrohungen angewendet werden. Zudem lassen sich bei der NSv Series mit segmentbasierten Sicherheitsfunktionen ähnliche Schnittstellen gruppieren und dieselben Regeln darauf anwenden, anstatt die gleichen Regeln für jede einzelne Schnittstelle separat einrichten zu müssen. Durch die Anwendung von Sicherheitsregeln innerhalb des virtuellen Netzwerks lassen sich die Netzwerkressourcen in verschiedenen Segmenten organisieren. Den Datenverkehr zwischen diesen Segmenten kann man entsprechend zulassen oder einschränken. Auf diese Weise lässt sich der Zugriff auf kritische interne Ressourcen streng kontrollieren.

Die NSv Series kann automatisch Segmentierungseinschränkungen auf Basis dynamischer Kriterien durchsetzen, wie etwa Anmeldedaten des Benutzers, Geo-IP-Standort und Sicherheitsstatus mobiler Endpunkte. Für eine erhöhte Sicherheit kann die NSv Series auch Multi-Gigabit-Netzwerk-Switching in ihre Richtlinien für Sicherheitssegmente integrieren und durchsetzen. Segmentrichtlinien werden auf den Datenverkehr an Schaltpunkten im gesamten Netzwerk angewendet. Außerdem lässt sich die Segmentsicherheit global von einer zentralen Konsole aus verwalten.

Da Segmente nur so effektiv sind wie die Sicherheit, die sich zwischen ihnen erzielen lässt, nutzen die NSv-Firewalls einen Intrusion-Prevention-Service (IPS), um ein- und ausgehenden Verkehr im VLAN-Segment zu durchleuchten und so die Sicherheit des internen Netzwerkverkehrs zu optimieren. Für jedes Segment lassen sich entsprechend der festgelegten Richtlinien eine Vielzahl an Sicherheitsservices auf mehrere Schnittstellen anwenden.

Flexible Implementierungsmöglichkeiten

Dank Infrastrukturunterstützung für eine Hochverfügbarkeitsimplementierung erfüllt die NSv Series die Skalierbarkeits- und Verfügbarkeitsanforderungen von Software-defined-Data-Center (SDDC) und sorgt darüber hinaus für Systemstabilität, Servicezuverlässigkeit und die Einhaltung gesetzlicher Bestimmungen. Für eine große Bandbreite an Public-, Private- und Hybrid-Implementierungsmöglichkeiten optimiert, lässt sich die NSv Series an Änderungen auf Service-Ebene anpassen und stellt dabei sicher, dass VMs sowie deren Anwendungs-Workloads und Datenressourcen sicher und verfügbar bleiben. Dabei gewährleistest die Serie Multi-GBit/s-Geschwindigkeiten und geringe Latenzzeiten.

Organisationen profitieren von allen Sicherheitsfunktionen einer physischen Firewall sowie den operativen und wirtschaftlichen Vorteilen der Virtualisierung. Dazu zählen Systemskalierbarkeit und operative Agilität sowie eine schnelle Bereitstellung, einfache Verwaltung und Reduzierung der Kosten.

Die NSv-Firewalls sind in verschiedenen virtuellen Varianten in Form von Paketen für eine große Bandbreite an Implementierungsoptionen in virtualisierten Umgebungen und der Cloud verfügbar. Ausgestattet mit Multi-Gigabit-Performance zum Schutz vor Bedrohungen und zur Prüfung von verschlüsseltem Verkehr, passt sich die NSv Series an Auslastungsspitzen an und sorgt dafür, dass VNs, Anwendungsworkloads und Datenressourcen verfügbar und sicher bleiben.

Zentrale Verwaltung

NSv-Implementierungen lassen sich zentral verwalten, sowohl lokal mit SonicWall GMS[3] als auch mit SonicWall Capture Security Center[3], einer offenen, skalierbaren Cloud-basierten Sicherheitsmanagement-, Überwachungs-, Reporting- und Analysesoftware, die sich kosteneffizient als Software-as-a-Service(SaaS)-Lösung bereitstellen lässt. Capture Security Center bietet eine extrem hohe Transparenz, Agilität und Leistung, um das gesamte virtuelle und physische SonicWall-Firewall-Ökosystem von einer zentralen Konsole aus schneller, gezielter und genauer verwalten zu können.

Funktionen

SonicOS-Plattform

Die SonicOS-Architektur bildet das Herzstück jeder physischen und virtuellen SonicWall-Firewall, einschließlich der NSv und NS*a* Series, SuperMassive™ Series und TZ Series. Eine vollständige Liste der Features und Funktionen entnehmen Sie bitte dem Datenblatt zur SonicWall SonicOS Platform.

Automatisierte Breach-Prevention[1]

Dazu gehört ein umfassender Schutz vor raffinierten Bedrohungen, einschließlich leistungsstarker Abwehrmechanismen gegen Eindringlinge und Malware sowie Cloud-basiertem Sandboxing.

Sicherheit rund um die Uhr[1]

Neue Updates zu Bedrohungen werden automatisch an Firewalls mit aktivierten Sicherheitsservices weitergeleitet und sind ohne Neustart oder andere Unterbrechungen sofort wirksam.

Zero-Day-Schutz[1]

Die NSv Series bietet Schutz vor Zero-Day-Angriffen – dank laufender Updates zu den neuesten Exploit-Techniken und -Methoden, die Tausende verschiedener Exploits abdecken.

API gegen Bedrohungen

Die NSv-Firewalls erhalten sämtliche Intelligence-Feeds von proprietären Anbietern, OEMs und Drittanbietern. Auf diese Weise können sie raffinierte Bedrohungen wie Zero-Day-Angriffe, Insiderbedrohungen, Ransomware, Advanced Persistent Threats und Gefahren durch kompromittierte Zugangsdaten effektiv bekämpfen.

ZENTRALE VERWALTUNG

- Schaffen Sie eine einfache Lösung für umfassendes Sicherheitsmanagement, Analyseberichte und Compliance und vereinheitlichen Sie Ihr Netzwerksicherheitsprogramm.
- Sie können Workflows automatisieren und abgleichen, um eine komplett aufeinander abgestimmte Security-Governance-, Compliance- und Risikomanagementstrategie zu erstellen.

COMPLIANCE

- Regulierungsbehörden und Auditoren profitieren von automatischen PCI-, HIPAA- und SOX-Sicherheitsberichten.
- Sie können jegliche Kombination auditierbarer Netzwerksicherheitsdaten anpassen und sich so in Richtung spezifischer Compliance-Vorgaben entwickeln.

RISIKOMANAGEMENT

- Handeln Sie schnell und treiben Sie Zusammenarbeit, Kommunikation und Wissen im gemeinsamen Sicherheitsframework voran.
- Treffen Sie fundierte Entscheidungen zu Sicherheitsregeln auf Basis zeitkritischer und konsolidierter Bedrohungsinformationen für eine effizientere Sicherheit.

GMS bietet einen ganzheitlichen Ansatz für Security-Governance, Compliance und Risikomanagement.

Zonenschutz

Durch die Segmentierung des Netzwerks in mehrere Sicherheitszonen bieten die NSv-Firewalls einen verbesserten Schutz vor internen Bedrohungen. Dabei verhindert ein Intrusion-Prevention-Service, dass sich Bedrohungen über Zonengrenzen hinaus ausbreiten. Administratoren können für Datenverkehr über verschiedene Schnittstellen Zugriffsregeln und NAT-Richtlinien erstellen und anwenden und auf Grundlage diverser Kriterien den internen oder externen Netzwerkzugriff erlauben oder verweigern.

Application-Intelligence und Anwendungskontrolle[1]

Durch anwendungsspezifische Richtlinien ermöglicht die NSv Series eine gezielte Kontrolle des Netzwerkverkehrs auf Ebene von Benutzern, E-Mail-Adressen, Zeitplänen und IP-Subnetzen. Die NSv Series ermöglicht die Erstellung von Signaturen auf der Grundlage bestimmter Parameter oder Muster, die nur bei der Netzwerkkommunikation bestimmter Anwendungen vorkommen. Auf diese Weise lassen sich benutzerdefinierte Anwendungen kontrollieren. Der interne oder externe Netzwerkzugriff wird auf Basis verschiedener Kriterien erlaubt oder verweigert.

Schutz vor Datenlecks

Mithilfe der NSv Series lassen sich Datenströme nach Schlüsselwörtern durchsuchen. Auf diese Weise kann die Übertragung bestimmter Dateinamen, Dateitypen, E-Mail-Anhänge, Typen von Anhängen, E-Mails mit bestimmten Betreffzeilen sowie E-Mails oder Anhänge mit bestimmten Schlüsselwörtern oder Byte-Mustern eingeschränkt werden.

Bandbreitenverwaltung auf der Anwendungsebene

Mithilfe des Packet Monitor-Features kann die NSv Series aus verschiedenen Einstellungen für die Bandbreitenverwaltung wählen, um die Bandbreitennutzung im Netzwerk durch bestimmte Anwendungen zu reduzieren. Auf diese Weise lässt sich eine erweiterte Kontrolle über das Netzwerk erreichen.

Sichere Kommunikation

Die NSv Series stellt einen sicheren Datenaustausch zwischen mehreren Gruppen virtueller Maschinen sicher. Mithilfe der Segmentierung lassen sich innerhalb dieser Netzwerke Isolierung, Vertraulichkeit, Integrität und Informationsflusskontrolle gewährleisten.

Zugriffskontrolle

Die NSv-Firewalls sorgen dafür, dass VMs nur bei Einhaltung bestimmter Bedingungen über VLANs auf Daten einer anderen VM zugreifen können.

Benutzerauthentifizierung

Die NSv-Firewalls erstellen Regeln zur Kontrolle oder Einschränkung des VM- und Workload-Zugriffs durch unbefugte Benutzer.

Vertraulichkeit von Informationen

Die NSv Series verhindert Datendiebstahl und unberechtigten Zugriff auf geschützte Daten und Services.

Stabilität und Verfügbarkeit virtueller Netzwerke

Die NSv Series verhindert eine Störung oder Beeinträchtigung von Anwendungsdiensten und -kommunikation.

Systemsicherheit und Integrität

Die NSv-Firewalls verhindern eine unerlaubte Übernahme von VM-Systemen und -Services.

Mechanismen zur Validierung, Prüfung und Überwachung von Datenverkehr

Die NSv Series erkennt Unregelmäßigkeiten bzw. böswilliges Verhalten und stoppt Angriffe, die auf VM-Workloads abzielen.

Implementierungsoptionen[2]

Die NSv Series lässt sich auf zahlreichen virtualisierten und Cloud-Plattformen für unterschiedliche Sicherheitsszenarien in Private-/Public-Cloud-Umgebungen implementieren.

[1] Erfordert ein SonicWall Advanced Gateway Security Services (AGSS)-Abo.
[2] Virtual-Machine-Image(VMI)-Unterstützung für MS Hyper-V, Amazon und MS Azure wird in einem kommenden Release verfügbar sein.
[3] Für SonicWall Global Management System und Capture Security Center ist eine separate Lizenzierung bzw. ein separates Abo erforderlich.

NSv Series – Systemdaten

Firewall allgemein	NSv 10	NSv 25	NSv 50	NSv 100
Betriebssystem	SonicOS			
Unterstützte Hypervisoren	VMware ESXi v5.5 / v6.0 / v6.5			
Maximal unterstützte Anzahl von vCPUs	2	2	2	2
Maximale Anzahl von Management-/ Data-Plane-Kernen	1/1	1/1	1/1	1/1
Mindestspeicher	4 GB	4 GB	4 GB	4 GB
Unterstützte IP/Nodes	10	25	50	100
Mindestspeicher	60 GB			
SSO-Benutzer	25	50	100	100
Logging	Analyzer, lokale Logdatei, Syslog			
Hochverfügbarkeit	Active/Passive			
Firewall-/VPN-Performance				
Firewall-Inspection-Durchsatz	2 GBit/s	2,5 GBit/s	3 GBit/s	3,5 GBit/s
Full-DPI-Durchsatz (GAV/GAS/IPS)	450 MBit/s	550 MBit/s	650 MBit/s	750 MBit/s
Application-Inspection-Durchsatz	1 GBit/s	1,25 GBit/s	1,5 GBit/s	1,75 GBit/s
IPS-Durchsatz	1 GBit/s	1,25 GBit/s	1,5 GBit/s	1,75 GBit/s
Anti-Malware-Inspection-Durchsatz	450 MBit/s	550 MBit/s	650 MBit/s	750 MBit/s
IMIX-Durchsatz	750 MBit/s	850 MBit/s	950 MBit/s	1.100 MBit/s
TLS-/SSL-DPI-Durchsatz	650 MBit/s	750 MBit/s	850 MBit/s	950 MBit/s
VPN-Durchsatz	500 MBit/s	550 MBit/s	600 MBit/s	650 MBit/s
Verbindungen pro Sekunde	1.800	5.000	8.000	10.000
Maximale Anzahl von Verbindungen (SPI)	10.000	50.000	125.000	150.000
Maximale Anzahl von Verbindungen (DPI)	10.000	50.000	100.000	125.000
TLS-/SSL-DPI-Verbindungen	500	1.000	2.000	4.000
VPN				
Site-to-Site-VPN-Tunnel	10	10	25	50
IPSec-VPN-Clients	10	10	25	25
SSL-VPN-NetExtender-Clients (max.)	2 (10)	2 (25)	2 (25)	2 (25)
Verschlüsselung/Authentifizierung	DES, 3DES, AES (128, 192, 256 Bit)/MD5, SHA-1, Suite B, Common Access Card (CAC)			
Schlüsselaustausch	Diffie-Hellman-Gruppen 1, 2, 5, 14v			
Routenbasiertes VPN	RIP, OSPF, BGP			
Networking				
IP-Adressenzuweisung	Statisch, DHCP, interner DHCP-Server, DHCP-Relay			
NAT-Modi	1:1, many:1, 1:many, flexible NAT (überlappende IPs), PAT			
VLAN-Schnittstellen	25	25	50	50
Routing-Protokolle	BGP, OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing			
QoS	Bandbreitenpriorität, max. Bandbreite, garantierte Bandbreite, DSCP-Marking, 802.1p			
Authentifizierung	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, interne Benutzerdatenbank, Terminaldienste, Citrix			
VoIP	Full H323-v1-5, SIP			
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, L2TP, PPTP, RADIUS			

NSv Series – Systemdaten (Fortsetzung)

Firewall allgemein	NSv 200	NSv 300	NSv 400	NSv 800	NSv 1600
Betriebssystem	SonicOS				
Supported Hypervisors	VMware ESXi v5.5 / v6.0 / v6.5				
Max Supported vCPUs	2	3	4	8	16
Maximale Anzahl von Management-/ Data-Plane-Kernen	1/1	1/2	1/3	1/7	1/15
Mindestspeicher	6 GB	8 GB	8 GB	10 GB	12 GB
Unterstützte IP/Nodes	Unbegrenzt	Unbegrenzt	Unbegrenzt	Unbegrenzt	Unbegrenzt
Minimum Storage	60 GB				
SSO-Benutzer	500	5.000	10.000	15.000	20.000
Logging	Analyzer, lokale Logdatei, Syslog				
Hochverfügbarkeit	Active/Passive				
Firewall-/VPN-Performance					
Firewall-Inspection-Durchsatz	4,1 GBit/s	5,9 GBit/s	7,8 GBit/s	13,9 GBit/s	17,2 GBit/s
Full-DPI-Durchsatz (GAV/GAS/IPS)	900 MBit/s	1,6 GBit/s	2,2 GBit/s	4,0 GBit/s	6,4 GBit/s
Application-Inspection-Durchsatz	2,3 GBit/s	3,4 GBit/s	4,1 GBit/s	5,5 GBit/s	6,4 GBit/s
IPS-Durchsatz	2,3 GBit/s	3,4 GBit/s	4,1 GBit/s	5,5 GBit/s	6,7 GBit/s
Anti-Malware-Inspection-Durchsatz	900 MBit/s	1,6 GBit/s	2,2 GBit/s	4,0 GBit/s	6,6 GBit/s
IMIX-Durchsatz	1,5 GBit/s	2,3 GBit/s	2,8 GBit/s	4,2 GBit/s	5,3 GBit/s
TLS-/SSL-DPI-Durchsatz	1,1 GBit/s	1,2 GBit/s	1,8 GBit/s	3,4 GBit/s	5,1 GBit/s
VPN-Durchsatz	750 MBit/s	1,4 GBit/s	1,9 GBit/s	4,2 GBit/s	8,4 GBit/s
Verbindungen pro Sekunde	13.760	24.360	37.270	75.640	125.000
Maximale Anzahl von Verbindungen (SPI)	225.000	1 Mio.	1,5 Mio.	3 Mio.	4 Mio.
Maximale Anzahl von Verbindungen (DPI)	125.000	500.000	1,5 Mio.	2 Mio.	2,5 Mio.
TLS-/SSL-DPI-Verbindungen	8.000	12.000	20.000	30.000	50.000
VPN					
Site-to-Site-VPN-Tunnel	75	100	6.000	10.000	25.000
IPSec-VPN-Clients (max.)	50 (1.000)	50 (1.000)	2.000 (4.000)	2.000 (6.000)	2.000 (10.000)
SSL-VPN-NetExtender-Clients (max.)	2 (100)	2 (100)	2 (100)	2 (100)	2 (100)
Verschlüsselung/Authentifizierung	DES, 3DES, AES (128, 192, 256 Bit)/MD5, SHA-1, Suite B, Common Access Card (CAC)				
Schlüsselaustausch	Diffie-Hellman-Gruppen 1, 2, 5, 14v				
Routenbasiertes VPN	RIP, OSPF, BGP				
Networking					
IP-Adressenzuweisung	Statisch, DHCP, interner DHCP-Server, DHCP-Relay				
NAT-Modi	1:1, many:1, 1:many, flexible NAT (überlappende IPs), PAT				
VLAN-Schnittstellen	50	256	500	512	512
Routing-Protokolle	BGP, OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing				
QoS	Bandbreitenpriorität, max. Bandbreite, garantierte Bandbreite, DSCP-Marking, 802.1p				
Authentifizierung	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, interne Benutzerdatenbank, Terminaldienste, Citrix				
VoIP	Full H323-v1-5, SIP				
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, L2TP, PPTP, RADIUS				

[1] *Bei den aufgeführten Performancezahlen handelt es sich um die Höchstwerte. Die tatsächliche Performance kann je nach Hardware, Netzwerkbedingungen, Firewall-Konfiguration und aktivierten Diensten variieren. Performance und Kapazitäten können auch je nach Virtualisierungsinfrastruktur variieren. Wir empfehlen zusätzliche Tests innerhalb Ihrer Umgebung, um sicherzustellen, dass Ihre Performance- und Kapazitätsanforderungen erfüllt werden. Die Performancekennzahlen wurden unter Verwendung eines Intel-Xeon-W-Prozessors (W-2195 2,3 GHz, 4,3 GHz Turbo, 24,75 MB Cache) mit SonicOSv 6.5.0.2 und VMware vSphere 6.5 ermittelt.*

Testmethoden:
Maximalleistung auf Basis von RFC 2544 (für Firewall).
Messung des Full DPI-/GatewayAV-/Anti-Spyware-/IPS-Durchsatzes mittels Industriestandard HTTP-Performance-Test WebAvalanche von Spirent und Ixia-Test-Tools.
Tests erfolgten mit unterschiedlichen Datenströmen zwischen mehreren Portpaaren.
Der VPN-Durchsatz wurde gemäß RFC 2544 gemessen, unter Verwendung von UDP-Datenverkehr mit einer Paketgröße von 1.418 Byte. Änderungen hinsichtlich technischer Daten und Features vorbehalten.

NSv Series – Bestellinformationen

Produkt	Artikelnummer
SonicWall NSv 10 Virtual Appliance Total Secure Advanced Edition (1 Jahr)	01-SSC-5875
SonicWall NSv 25 Virtual Appliance Total Secure Advanced Edition (1 Jahr)	01-SSC-5923
SonicWall NSv 50 Virtual Appliance Total Secure Advanced Edition (1 Jahr)	01-SSC-5926
SonicWall NSv 100 Virtual Appliance Total Secure Advanced Edition (1 Jahr)	01-SSC-5929
SonicWall NSv 200 Virtual Appliance Total Secure Advanced Edition (1 Jahr)	01-SSC-5950
SonicWall NSv 300 Virtual Appliance Total Secure Advanced Edition (1 Jahr)	01-SSC-5964
SonicWall NSv 400 Virtual Appliance Total Secure Advanced Edition (1 Jahr)	01-SSC-6084
SonicWall NSv 800 Virtual Appliance Total Secure Advanced Edition (1 Jahr)	01-SSC-6101
SonicWall NSv 1600 Virtual Appliance Total Secure Advanced Edition (1 Jahr)	01-SSC-6109
NSv 10 – Support und Sicherheitsabos	**Artikelnummer**
Advanced Gateway Security Suite-Bundle für NSv 10 Virtual Appliance (1 Jahr)	01-SSC-5008
24/7-Support für NSv 10 Virtual Appliance (1 Jahr)	01-SSC-4830
NSv 25 – Support und Sicherheitsabos	**Artikelnummer**
Advanced Gateway Security Suite-Bundle für NSv 25 Virtual Appliance (1 Jahr)	01-SSC-5165
24/7-Support für NSv 25 Virtual Appliance (1 Jahr)	01-SSC-5161
NSv 50 – Support und Sicherheitsabos	**Artikelnummer**
Advanced Gateway Security Suite-Bundle für NSv 50 Virtual Appliance (1 Jahr)	01-SSC-5194
24/7-Support für NSv 50 Virtual Appliance (1 Jahr)	01-SSC-5189
NSv 100 – Support und Sicherheitsabos	**Artikelnummer**
Advanced Gateway Security Suite-Bundle für NSv 100 Virtual Appliance (1 Jahr)	01-SSC-5219
24/7-Support für NSv 100 Virtual Appliance (1 Jahr)	01-SSC-5216
NSv 200 – Support und Sicherheitsabos	**Artikelnummer**
Advanced Gateway Security Suite-Bundle für NSv 200 Virtual Appliance (1 Jahr)	01-SSC-5306
Capture Advanced Threat Protection für NSv 200 Virtual Appliance (1 Jahr)	01-SSC-5309
Content Filtering Service Premium Business Edition für NSv 200 Virtual Appliance (1 Jahr)	01-SSC-5335
Gateway Anti-Malware, Intrusion Prevention And Application Control für NSv 200 Virtual Appliance (1 Jahr)	01-SSC-5364
24/7-Support für NSv 200 Virtual Appliance (1 Jahr)	01-SSC-5303
NSv 300 – Support und Sicherheitsabos	**Artikelnummer**
Advanced Gateway Security Suite-Bundle für NSv 300 Virtual Appliance (1 Jahr)	01-SSC-5584
Capture Advanced Threat Protection für NSv 300 Virtual Appliance (1 Jahr)	01-SSC-5587
Content Filtering Service Premium Business Edition für NSv 300 Virtual Appliance (1 Jahr)	01-SSC-5649
Gateway Anti-Malware, Intrusion Prevention And Application Control für NSv 300 Virtual Appliance (1 Jahr)	01-SSC-5671
24/7-Support für NSv 300 Virtual Appliance (1 Jahr)	01-SSC-5581
NSv 400 – Support und Sicherheitsabos	**Artikelnummer**
Advanced Gateway Security Suite-Bundle für NSv 400 Virtual Appliance (1 Jahr)	01-SSC-5681
Capture Advanced Threat Protection für NSv 400 Virtual Appliance (1 Jahr)	01-SSC-5684
Content Filtering Service Premium Business Edition für NSv 400 Virtual Appliance (1 Jahr)	01-SSC-5690
Gateway Anti-Malware, Intrusion Prevention And Application Control für NSv 400 Virtual Appliance (1 Jahr)	01-SSC-5693
24/7-Support für NSv 400 Virtual Appliance (1 Jahr)	01-SSC-5678
NSv 800 – Support und Sicherheitsabos	**Artikelnummer**
Advanced Gateway Security Suite-Bundle für NSv 800 Virtual Appliance (1 Jahr)	01-SSC-5737
Capture Advanced Threat Protection für NSv 800 Virtual Appliance (1 Jahr)	01-SSC-5748
Content Filtering Service Premium Business Edition für NSv 800 Virtual Appliance (1 Jahr)	01-SSC-5774
Gateway Anti-Malware, Intrusion Prevention And Application Control für NSv 800 Virtual Appliance (1 Jahr)	01-SSC-5777
24/7-Support für NSv 800 Virtual Appliance (1 Jahr)	01-SSC-5709
NSv 1600 – Support und Sicherheitsabos	**Artikelnummer**
Advanced Gateway Security Suite-Bundle für NSv 1600 Virtual Appliance (1 Jahr)	01-SSC-5787
Capture Advanced Threat Protection für NSv 1600 Virtual Appliance (1 Jahr)	01-SSC-5789
Content Filtering Service Premium Business Edition für NSv 1600 Virtual Appliance (1 Jahr)	01-SSC-5801
Gateway Anti-Malware, Intrusion Prevention And Application Control für NSv 1600 Virtual Appliance (1 Jahr)	01-SSC-5803
24/7-Support für NSv 1600 Virtual Appliance (1 Jahr)	01-SSC-5785

Über uns

Seit über 25 Jahren schützt SonicWall kleine, mittlere und große Unternehmen weltweit vor Cyberkriminalität. Mit unseren Produkten und Partnerschaften können wir eine Echtzeit-Cyberabwehrlösung für die individuellen Anforderungen von über 500.000 Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, Kalifornien 95035, USA
Weitere Information erhalten Sie auf unserer Website.
www.sonicwall.com

Datasheet-NSvVirtualFirewalls-US-VG-MKTG2648

SONICWALL®