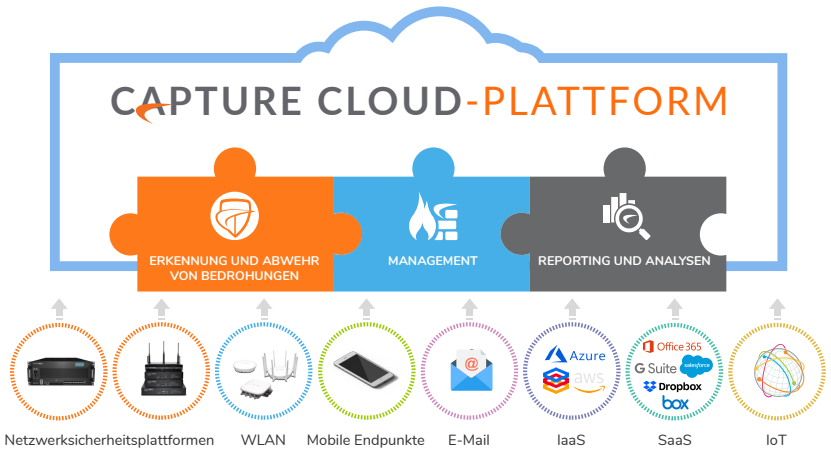
SONICWALL

SonicWall Network Security Virtual (NSv) Firewall Series

Sicherheit der nächsten Generation für öffentliche, private oder hybride Cloud-Umgebungen

Design, Implementierung und Einbindung moderner Netzwerkarchitekturen, wie Virtualisierung und Cloud, sind für viele Unternehmen weiterhin eine bahnbrechende Strategie. Die Virtualisierung von Rechenzentren, Migration in die Cloud oder eine Kombination davon bringen nachweislich große betriebliche und wirtschaftliche Vorteile. Doch leider gibt es innerhalb der virtuellen Umgebungen auch viele bereits umfassend dokumentierte Schwachstellen. Des Weiteren werden regelmäßig neue Schwachstellen aufgedeckt, die mit schwerwiegenden Folgen und Herausforderungen in Bezug auf die Sicherheit einhergehen. Zur Sicherstellung, dass Anwendungen und Dienste auf sichere, effiziente und skalierbare Weise bereitgestellt und die für alle Teile der virtuellen Struktur, inklusive Virtual Machines (VMs) schädlichen Bedrohungen bekämpft werden, müssen Anwendungen/ Workloads und Daten zur obersten Priorität gemacht werden.

Die SonicWall Network Security Virtual (NSv) Firewall Series hilft Security-Teams bei der Reduzierung dieser Arten von Sicherheitsrisiken und Schwachstellen, die eine schwerwiegende Unterbrechung von geschäftskritischen Diensten und Funktionen verursachen können. Die Next-Generation-Firewalls der NSv Series arbeiten mit zwei hoch entwickelten Sicherheitstechnologien, die einen erstklassigen Bedrohungsschutz bieten und Cyberkriminellen einen Schritt voraus sind. Die zum Patent angemeldete SonicWall Real-Time Deep Memory Inspection (RTDMI™)-Technologie verbessert unseren preisgekrönten Multi-Engine-Sandbox-Dienst Capture Advanced Threat Protection (ATP). Die RTDMI-Engine ist durch eine direkte Prüfung des Speichers in der Lage, massive Zero-Day-Bedrohungen sowie unbekannte Malware proaktiv aufzudecken und abzuwehren. Aufgrund der Echtzeitarchitektur ist die SonicWall RTDMI-Technologie sehr präzise, reduziert falsche Positivmeldungen und kann komplexe Angriffe selbst dann entschärfen, wenn die am stärksten geschützten Bereiche des Schadcodes weniger als 100 Nanosekunden sichtbar sind. Gemeinsam mit der patentierten* Reassembly-Free Deep Packet Inspection (RFDPI®)-Single-Pass-Engine von SonicWall lassen sich jedes einzelne Paket und jedes einzelne Byte durchleuchten. Dabei wird der ein- und ausgehende Datenverkehr direkt in der Firewall auf Bedrohungen geprüft.



*U.S. Patente 7.310.815; 7.600.257; 7.738.380; 7.835.361; 7.991.723

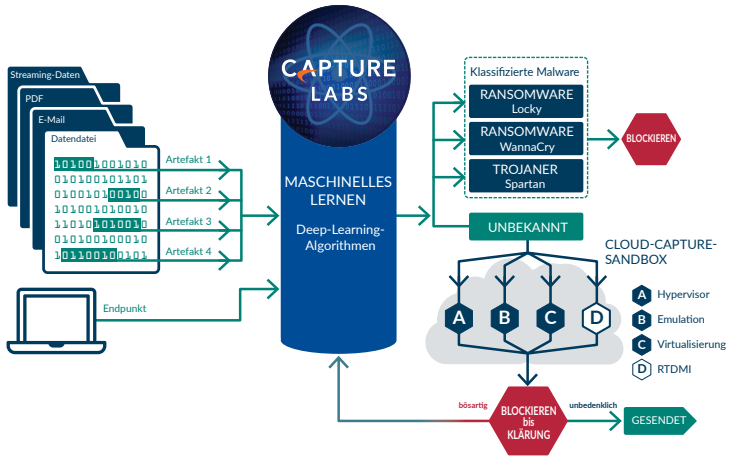
Vorteile

Öffentliche und private Cloud-Anwendungen

- Next-Gen-Firewall mit automatisierte Bedrohungserkennung und -verhinderung in Echtzeit
- Zum Patent angemeldete Real-Time Deep Memory Inspection-Technologie
- Patentierte Reassembly-Free Deep Packet Inspection-Technologie
- Komplette End-to-End-Transparenz und Kontrolle
- Application-Intelligence und Kontrolle
- Sicherheitssegmentierung und Sicherheitszonen
- Unterstützung für private Cloud-Plattformen (ESXi, Hyper-V) und öffentliche Cloud-Plattformen (AWS, Azure)
- BYOL- und PAYG-Lizenzen

Schutz von virtuellen Rechnern

- Schutz vor Zero-Day-Bedrohungen mit Capture ATP
- Vertraulichhaltung der Daten
- Sichere Kommunikation mit Verhinderung von Datenlecks
- Validierungs-, Inspektions- und Überwachungsmechanismen
- Sicherheit und Integrität des Systems
- Ausfallsicherheit und Verfügbarkeit virtueller Netzwerke



Die NSv Series nutzt innovative Deep-Learning-Technologien in der SonicWall Capture Cloud Plattform und bietet Organisationen genau die automatisierte Bedrohungserkennung und -verhinderung in Echtzeit, die sie brauchen. Diese Plattform bietet kleinen wie großen Organisationen eine Cloud-basierte Lösung für Bedrohungsschutz und Netzwerkverwaltung sowie Reporting und Analysen. Diese Plattform konsolidiert Bedrohungsinformationen aus mehreren Quellen, zum Beispiel aus Capture ATP sowie aus über 1 Million SonicWall Sensoren, die rund um den Globus verteilt sind. Die NSv Series nutzt neben integrierten Funktionen wie Intrusion-Prevention, Anti-Malware und Web-/URL-Filtering auch die SonicWall Capture Cloud Plattform, um selbst die gefährlichsten Bedrohungen am Gateway zu stoppen.

Die NSv lässt sich einfach in einer virtuellen Umgebung – in der Regel zwischen virtuellen Netzwerken (VNs) oder virtuellen privaten Clouds (VPCs) – implementieren und bereitstellen. Somit können Kommunikationen und Datenaustausch zwischen virtuellen Rechnern für die automatische Einbruchsverhinderung erfasst und gleichzeitig strenge Zugriffskontrollen für die Vertraulichhaltung der Daten, VM-Sicherheit und Integrität festgesetzt werden. Bedrohungen (wie Cross-VM-Angriffe oder Seitenkanalattacken, gängige Netzwerk-Eindringversuche sowie Anwendungs- und Protokollschwachstellen) werden durch die umfassenden Security Inspection Services[1] von SonicWall erfolgreich kaltgestellt. Jeder VM-Verkehr durchläuft mehrere Threat-Analysis-Engines, einschließlich Intrusion Prevention, Gateway Antivirus und Anti-Spyware, Cloud-Antivirus, Botnet-Filter, Anwendungskontrolle und Capture ATP Multi-Engine Sandboxing mit RTDMI-Technologie.

Sicherheitssegmentierung

Für eine maximal wirksame Abwehr von Advanced Persistent Threats (APTs) muss mittels Sicherheitssegmentierung ein integrierter Satz von dynamischen, durchsetzbaren Barrieren auf die komplexen Bedrohungen angewandt werden. Durch die in NSv integrierten segmentbasierten Sicherheitsfunktionen können ähnliche Schnittstellen in Gruppen zusammengefasst werden. Auf diese Gruppen können dann die gleichen Regeln angewandt werden, anstatt für jede Schnittstelle die gleiche Regel neu schreiben zu müssen. Durch die Anwendung von Sicherheitsregeln innerhalb des VN können Segmentierungen für die Zuteilung von Netzwerkressourcen zu verschiedenen Segmenten konfiguriert werden. Der Verkehr zwischen diesen Segmenten kann dann erlaubt oder eingeschränkt werden. Auf diese Weise lassen sich geschäftskritische interne Ressourcen streng kontrollieren.

NSv setzt die Segmentierungsein-schränkungen automatisch auf Basis dynamischer Kriterien, wie Anmeldedaten/Benutzer-ID, Geo-IP und Sicherheitslevel von mobilen Endpunkten, durch. Wenn erweiterte Sicherheit erforderlich ist, kann die NSv Firewall auch Multi-Gigabit-Switching in ihre Security-Segment-Regeln und Durchsetzung integrieren. Die Segmentregeln werden auf den Verkehr an die netzwerkweiten Switching-Punkte angewandt und die Durchsetzung der Sicherheitssegmentierung erfolgt global von einer zentralen Benutzerober-fläche aus.

Da die Wirksamkeit der Segmente von der zwischen ihnen durchgesetzten Sicherheit abhängt, setzt die NSv ein Intrusion-Prevention-System (IPS) ein, um ein- und ausgehenden Verkehr des VLAN-Segments zu scannen und so die Sicherheit für den internen Netzwerkverkehr zu verstärken. Dabei wird auf Basis durchsetzbarer Regeln für jedes Segment eine komplette Reihe von Sicherheitsdiensten an mehreren Schnittstellen angewandt.

Flexible Implementierungsszenarien

Mit Infrastruktur-Support für eine Hochverfügbarkeitsimplementierung erfüllt die NSv die SDDC (Software Defined Data Center)-Anforderungen an Skalierbarkeit und Verfügbarkeit. Somit werden Systemresilienz, Zuverlässigkeit der Dienste und regulatorische Konformität gewährleistet. Die NSv ist für einen weiten Bereich von öffentlichen, privaten und hybriden Implementierungsszenarien optimiert und kann bei Service-Level-Änderungen leicht angepasst werden, um sicherzustellen, dass VMs und deren Anwendungen/Workloads und Datenbestände verfügbar und geschützt sind. All das kann latenzfrei mit Multi-Gigabit-Geschwindigkeit durchgeführt werden.

Unternehmen erhalten somit alle Sicherheitsvorteile einer physischen Firewall und zugleich die betrieblichen und wirtschaftlichen Vorteile der Virtualisierung. Dazu gehören Systemskalierbarkeit, betriebliche Agilität, hohe Geschwindigkeit, einfache Verwaltung und Kostensenkung.

Die NSv Series ist in mehreren virtuellen Ausführungen und Konfigurationen erhältlich, um einem weiten Bereich von virtualisierten und Cloud-basierten Implementierungsszenarien zu entsprechen. Mit Multi-Gigabit-Bedrohungsschutz und Inspektion von verschlüsseltem Verkehr lässt sich die NSv Series bei erhöhtem Kapazitätsbedarf leicht anpassen, um die konstante Sicherheit des VN und VPC sicherzustellen. Zugleich wird dafür gesorgt, dass VMs und deren Anwendungen/Workloads und Datenbestände verfügbar und geschützt sind

Zentrale Verwaltung

NSv-Implementierungen können zentral verwaltet werden, entweder on-prem mit dem SonicWall Global Management System (GMS²) oder über das Capture Security Center², SonicWalls offene, skalierbare Cloud-Plattform für Verwaltung, Überwachung, Reporting und Analytics, die als wirtschaftliche SaaS-Lösung angeboten wird.

Das Capture Security Center bietet ultimative Transparenz, Agilität und Kapazität für die Verwaltung des gesamten virtuellen und physischen Firewall-Ökosystems mit größerer Klarheit, Präzision und Geschwindigkeit von einer zentralen Benutzerober-fläche aus.

Unified Policy-Engine mit SonicOS 7

Die SonicWall Unified Policy-Engine ermöglicht eine integrierte Verwaltung verschiedener Sicherheitsregeln von on-prem und virtuellen SonicWall Firewalls (ab NSv Series).

ZENTRALE VERWALTUNG

- Schaffen Sie eine einfache Lösung für umfassendes Sicherheitsmanagement, Analyseberichte und Compliance und vereinheitlichen Sie Ihr Netzwerksicherheitsprogramm.
- Automatisieren und stimmen Sie ihre Arbeitsabläufe ab, 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 prüfbarer Netzwerksicherheitsdaten anpassen und so spezifische Compliance-Vorgaben umsetzen.

RISIKOMANAGEMENT

- Handeln Sie schnell, fördern Sie Zusammenarbeit und Kommunikation und sorgen Sie für eine bessere Verfügbarkeit von Wissen im gemeinsamen Sicherheitsframework
- Treffen Sie fundierte Entscheidungen zu Sicherheitsregeln auf Basis zeitkritischer und konsolidierter Bedrohungsinformationen für eine effizientere Sicherheit.

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

Diese Engine kommt mit einer neuen Benutzeroberfläche, die einen völlig neuen Ansatz unterstützt – das UX-Design.

Damit ist eine intuitive Einrichtung kontextbezogener Sicherheitsregeln möglich, die durch Handlungsaufforderungen und einfaches Zeigen und Klicken optimal vereinfacht wird.

Auch optisch ist sie attraktiver als die klassische Benutzeroberfläche. Die Firewall ist in einer Ansicht überschaubar dargestellt, in der dem Benutzer Informationen über die Effektivität der verschiedenen Sicherheitsregeln präsentiert werden.

Hier kann der Benutzer auf nahtlose Weise vordefinierte Regeln für Gateway-Antivirus, Anti-Spyware, Content-Filtering, Intrusion-Prevention, Geo-IP-Filtering und Deep-Packet Inspektion von verschlüsseltem Verkehr bedarfsgerecht anpassen.

Mit der Unified Policy-Engine bietet SonicWall eine optimierte Benutzererfahrung mit weniger Konfigurationsfehlern und kürzeren Implementierungszeiten, was insgesamt zu einem besseren Sicherheitslevel beiträgt.

Flexible Lizenzierung

NSv unterstützt die Lizenzierungsoptionen „Bring Your Own License“ (BYOL) und „Pay As You Go“ (PAYG). Die BYOL-Lizenz für NSv kann direkt von SonicWall, einem Partner oder Wiederverkäufer bezogen werden. Die PAYG-Lizenz kann direkt vom AWS Marketplace bezogen werden. Diese Art von Lizenz basiert auf dem tatsächlichen Gebrauch, wobei die auf stündlicher oder jährlicher Basis basierende Zahlung nur für die tatsächlich genutzte Zeit erfolgt.

Funktionen

SonicOS-Plattform
Die SonicOS-Architektur ist der Kern jeder physischen und virtuellen SonicWall Firewall, einschließlich der NSv und NSa Series, SuperMassive Series und TZ Series. Eine vollständige Liste aller Features und Fähigkeiten entnehmen Sie bitte dem Datenblatt zur SonicWall SonicOS-Plattform.

Automatische Abwehr von Bedrohungen[1]
Die NSv bietet umfassenden Schutz vor komplexen Bedrohungen, leistungsstarken Schutz vor Eindringversuchen und Malware sowie Cloud-basiertes Sandboxing.

Sicherheit rund um die Uhr[1]
Die NSv verhindert laterale Ausbreitungen von Bedrohungen und schützt den ein- und ausgehenden Verkehr. Updates bei neuen Bedrohungen werden automatisch per Push-Funktion an die Firewalls mit aktivierten Sicherheitsservices weitergeleitet und sind sofort wirksam, ohne dass Neustarts oder andere Unterbrechungen notwendig sind.

Zero-Day-Schutz[1]
Die NSv schützt vor Zero-Day-Angriffen durch ständige Updates zu den neuesten Exploit-Techniken und -Methoden, wobei Tausende verschiedener Exploits erfasst werden.

Threat API
Durch diese API erhält die NSv sämtliche Intelligence-Feeds von proprietären Anbietern, OEMs und Drittanbietern, die dann genutzt werden, um komplexe Bedrohungen wie Zero-Day-Angriffe, Insiderbedrohungen, Ransomware, Advanced Persistent Threats und Gefahren durch kompromittierte Zugangsdaten effektiv zu bekämpfen.

Schutz von Netzwerkzonen
Die NSv optimiert den Schutz vor internen Bedrohungen durch die Segmentierung des Netzwerks in mehrere Sicherheitszonen, wobei durch Intrusion-Prevention verhindert wird, dass sich Bedrohungen über Zonengrenzen hinaus ausbreiten. Durch die Erstellung von Zugriffsregeln und NAT-Richtlinien und deren Anwendung auf den durch verschiedene Schnittstellen passierenden Verkehr kann der interne oder externe Netzwerkzugriff auf Basis verschiedener Kriterien erlaubt oder verhindert werden.

Application Intelligence und Anwendungskontrolle[1]
Die NSv bietet granulare Kontrolle über den Netzwerkverkehr auf Benutzer-, E-Mail-Adressen-, Schedule- und IP-Subnet-Ebene und wendet dazu anwendungsspezifische Regeln an. Benutzerspezifische Anwendungen werden durch die Erstellung von Signaturen auf Basis bestimmter anwendungstypischer Parameter oder Muster kontrolliert. Der interne oder externe Netzwerkzugriff wird auf Basis verschiedener Kriterien erlaubt oder verweigert.

Schutz vor Datenlecks
Die NSv bietet auch die Möglichkeit, Datenstreams auf Schlüsselwörter zu scannen. Dadurch wird die Übertragung von bestimmten Dateinamen, Dateitypen, E-Mail-Anhängen, Arten von Anhängen, E-Mails mit bestimmten Betreffzeilen und E-Mails oder Anhängen mit bestimmten Schlüsselwörtern oder Byte-Mustern beschränkt.

Bandbreitenverwaltung auf Anwendungsebene
Die NSv kann aus verschiedenen Bandbreiteneinstellungen auswählen, um den Bandbreitenverbrauch einer Anwendung mit Paketmonitor-Nutzung zu reduzieren. Dadurch wird noch mehr Kontrolle über das Netzwerk ermöglicht.

[1] *Erfordert ein SonicWall Advanced Gateway Security Services (AGSS) Abo.*
[2] *SonicWall Global Management System und Capture Security Center erfordern separate Lizenzen oder Abos.*

Sichere Kommunikation
Die NSv gewährleistet einen sicheren Datenaustausch zwischen Gruppen virtueller Rechner, einschließlich Isolierung, Wahrung der Vertraulichkeit, Integrität und Kontrolle des Informationsflusses innerhalb dieser Netzwerke durch Segmentierung.

Zugriffskontrolle
Die NSv validiert, dass nur VMs, die bestimmte Bedingungen erfüllen, auf die Daten eines anderen virtuellen Rechners zugreifen können.

Benutzerauthentifizierung
Die NSv erstellt Regeln zur Kontrolle oder Einschränkung des Zugriffs auf VM und Workloads durch unbefugte Benutzer.

Vertraulichhaltung der Daten
Die NSv verhindert Datenklaus und unrechtmäßigen Zugriffen auf geschützte Daten und Dienste.

Ausfallsicherheit und Verfügbarkeit virtueller Netzwerke
Die NSv verhindert Ausfälle oder Leistungsabfälle bei Anwendungsdiensten und Kommunikationen.

Sicherheit und Integrität des Systems
Die NSv verhindert unbefugte Übernahmen von VM-Systemen und -Diensten.

Validierungs-, Inspektions- und Überwachungsmechanismen für den Netzwerkverkehr
Die NSv erkennt Unregelmäßigkeiten und böswillige Verhaltensweisen und wehrt Angriffe auf VM-Workloads ab.

Einbindungsoptionen
Die NSv kann auf einer Vielzahl virtualisierter und Cloud-Plattformen für verschiedene private/öffentliche Cloud-Sicherheitsanwendungen implementiert werden.

Flexible Lizenzierung
SonicWall bietet unbefristete und befristete Lizenzierungen. Bei der unbefristeten Lizenzierung müssen die Lizenzen für die Firewall und Sicherheitsdienste separat erworben werden. Das bedeutet, dass diese Lizenzen auch separat ablaufen. Bei befristeten Lizenzen sind Firewall- und Sicherheitsdienst-Lizenzen gebündelt und laufen deshalb zur gleichen Zeit ab. Für Cloud-Implementierungen sind sowohl unbefristete als auch befristete Lizenzen als „Bring Your Own License“ (BYOL) Lizenzmodell erhältlich.

SonicWalls befristete und unbefristete Lizenzierungen sorgen für mehr Flexibilität und Einfachheit, da sie für einzelne Artikel oder für gebündelte Firwewall-Software und Sicherheitsdienste erworben werden können. Sie sind sowohl für private Cloud-Angebote (ESXi und Hyper-V) als auch öffentliche Cloud-Angebote (AWS, Azure) verfügbar. Beim Ablauf eines Dienstabos wird die Benachrichtigung vor Ablauf der Lizenz zugestellt.

Befristete Lizenzmodelle sind in drei Ausführungen erhältlich – IPS/App Control Subscription, TotalSecure Subscription und TotalSecure Advanced Subscription – und gelten für ein Jahr. Je nach Angebotsschicht ist die NSv-Software gebündelt mit Intrusion Prevention System (IPS), Application Control, Support, Capture Security Center (CSC), Comprehensive Gateway Security Suite (CGSS) oder Advanced Gateway Security Suite (AGSS).

NSv Series – Systemdaten

FIREWALL ALLGEMEIN	NSv 10	NSv 25	NSv 50	NSv 100
Betriebssystem	SonicOS[1]			
Unterstützte Hypervisors	VMware ESXi v5.5 / v6.0 / v6.5 / v6.7, Microsoft Hyper-V Win 2012 / 2016, KVM Ubuntu 16.04 / CentOS 7			
Unterstützte Public-Cloud-Plattformen (Instanz Typ)	AWS (c5.groß), Azure (Std D2 v2)			
Lizenzierung	BYOL, PAYG[2]			
Maximal unterstützte vCPUs	2	2	2	2
Schnittstellenzahl (ESXi/Hyper-V/KVM)	8/8/8	8/8/8	8/8/8	8/8/8
Max Mgmt/DataPlane-Kerne	1/1	1/1	1/1	1/1
Min. Arbeitsspeicher[3]	4 GB	4 GB	4 GB	4 GB
Max. Arbeitsspeicher[4]	6 GB	6 GB	6 GB	6 GB
Unterstützte IP/Knoten	10	25	50	100
Mindestspeicherplatz	60 GB			
SSO-Benutzer	25	50	100	100
Logging	Analyzer, lokale Logdatei, Syslog			
Hochverfügbarkeit	Active/Passive			
FIREWALL/VPN-PERFORMANCE[6]	**NSv 10**	**NSv 25**	**NSv 50**	**NSv 100**
Firewall Inspection-Durchsatz	2 GBit/s	2,5 GBit/s	3 GBit/s	3,5 GBit/s
Voller 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	1100 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)	2.500	6.250	12.500	25.000
Maximale Anzahl von Verbindungen (DPI)	2.500	6.250	12.500	25.000
TLS/SSL DPI-Verbindungen	500	1.000	2.000	4.000
VPN	**NSv 10**	**NSv 25**	**NSv 50**	**NSv 100**
Site-to-Site-VPN-Tunnel	10	10	25	50
IPSec-VPN-Clients	10(10)	10(10)	10(25)	10(25)
SSL-VPN-Clients enthalten[7]	2	2	2	2
SSL-VPN-Clients (max.)[7]	50	50	50	50
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			
NETZWERK	**NSv 10**	**NSv 25**	**NSv 50**	**NSv 100**
IP-Adressenzuweisung	Statisch, DHCP, interner DHCP-Server, DHCP-Relais			
NAT-Modi	1:1, many:1, 1:many, flexible NAT (überlappende IPs), PAT			
Max VLAN	25	25	50	50
Routing-Protokolle4	BGP, OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing			
QoS	Bandbreitenpriorität, maximale Bandbreite, garantierte Bandbreite, DSCP-Markierung, 802.1p			
Authentifizierung	XAUTH/ RADIUS, Active Directory, SSO, LDAP, Novell, interne Benutzerdatenbank, Terminaldienste, Citrix			
VoIP	SIP			
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, L2TP, PPTP, RADIUS			
Max. SD-WAN-Gruppen	12	12	18	32
Max. SD-WAN-Mitglieder pro Produkt	24	24	36	64

NSv Series – Systemdaten (Fortsetzung)

FIREWALL ALLGEMEIN	NSv 200	NSv 300	NSv 400	NSv 800	NSv 1600
Betriebssystem	SonicOS[1]				
Unterstützte Hypervisors	VMware ESXi v5.5 / v6.0 / v6.5 / v6.7, Microsoft Hyper-V, KVM Ubuntu 16.04 / CentOS 7				
Unterstützte Public-Cloud-Plattformen (Instanz Typ)	AWS (c5.groß), Azure (Std D2 v2)	nicht zutr.	AWS (c5.xgroß), Azure (Std D3 v2)	AWS (c5.2xgroß), Azure (Std D4 v2)	AWS (c5.4xgroß), Azure (Std D5 v2)
Lizenzierung	BYOL, PAYG[2]				
Maximal unterstützte vCPUs	2	3	4	8	16
Schnittstellenzahl (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-Kerne	1/1	1/2	1/3	1/7	1/15
Min. Arbeitsspeicher[3]	6 GB	6 GB	8 GB	10 GB	12 GB
Max. Arbeitsspeicher[4]	6 GB	8 GB	10 GB	14 GB	18 GB
Unterstützte IP/Knoten	Unbegrenzt	Unbegrenzt	Unbegrenzt	Unbegrenzt	Unbegrenzt
Mindestspeicherplatz	60 GB				
SSO-Benutzer	500	5.000	10.000	15.000	20.000
Logging	Analyzer, lokale Logdatei, Syslog				
Hochverfügbarkeit	Active/Passive[5]				
FIREWALL/VPN-PERFORMANCE[6]	**NSv 200**	**NSv 300**	**NSv 400**	**NSv 800**	**NSv 1600**
Firewall Inspection-Durchsatz	4,1 GBit/s	5,9 GBit/s	7,8 GBit/s	13,9 GBit/s	17,2 GBIT/S
Voller 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	1M	1.5M	3M	4M
Maximale Anzahl von Verbindungen (DPI)	125.000	500.000	1.5M	2M	2.5M
TLS/SSL DPI-Verbindungen	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-Tunnel	75	100	6000	10.000	25.000
IPSec-VPN-Clients (max.)	50(1000)	50(1000)	2000(4000)	2000(6000)	2000(10.000)
SSL-VPN-Clients enthalten[7]	2	2	2	2	2
SSL-VPN-Clients (max.)[7]	100	150	200	300	400
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				
NETZWERK	**NSv 200**	**NSv 300**	**NSv 400**	**NSv 800**	**NSv 1600**
IP-Adressenzuweisung	Statisch, DHCP, interner DHCP-Server, DHCP-Relais				
NAT-Modi	1:1, many:1, 1:many, flexible NAT (überlappende IPs), PAT				
Max. VLAN[8]	128	128	128	128	128
Routing-Protokolle4	BGP, OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing				
QoS	Bandbreitenpriorität, maximale Bandbreite, garantierte Bandbreite, DSCP-Markierung, 802.1p				
Authentifizierung	XAUTH/ RADIUS, Active Directory, SSO, LDAP, Novell, interne Benutzerdatenbank, Terminaldienste, Citrix				
VoIP	SIP				
Standards	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, L2TP, PPTP, RADIUS				
Max. SD-WAN-Gruppen	38	38	70	102	102
Max. SD-WAN-Mitglieder pro Produkt	76	76	140	204	204

[1]*Unterstützt derzeit SonicOS 6.5.4.*
[2]*PAYG ist derzeit nur für AWS erhältlich.*
[3]*Arbeitsspeicher mit Jumbo-Frame deaktiviert.*
[4]*Arbeitsspeicher mit Jumbo-Frame aktiviert. Für Jumbo-Frames ist zusätzlicher Arbeitsspeicher erforderlich. Jumbo-Frames werden von Azure und AWS nicht unterstützt.*
[5]*Hochverfügbarkeit erhältlich fürdie VMware ESXi-Plattform und Microsoft Hyper-V, plus HA wird von Azure und AWS nicht unterstützt.*
[6]*Veröffentlichte Leistungszahlen sind von den Spezifikationen abhängig. Die tatsächliche Leistung kann je nach verwendeter Hardware, Netzwerkbedingungen, Firewallkonfiguration und aktivierten Diensten unterschiedlich sein. Leistung und Kapazität können ebenfalls unterschiedlich sein, da sie von der zugrunde liegenden Virtualisierungsinfrastruktur abhängig sind. Wir empfehlen zusätzliche Prüfungen innerhalb Ihrer Umgebung, um sicherzustellen, dass Leistung und Kapazität Ihre Anforderungen erfüllen. Leistungswerte wurden unter Verwendung eines Intel Xeon W Prozessors (W-2195 2,3GHz, 4,3GHz Turbo, 24,75M Cache) mit SonicOSv 6.5.0.2 und VMware vSphere 6.5 gemessen.*
[7]*Eine höhere SSL VPN-Zahl ist erst ab SonicOS 6.5.4.4-44v-21-723 Firmware erhältlich.*
[8]*VLAN-Schnittstellen werden von Azure und AWS nicht unterstützt*
Testmethoden: Die maximale Firewall-Leistung wurde auf Basis von RFC 2544 getestet. Full DPI/Gateway-AV/Anti-Spyware-/IPS-Durchsatz wurden mit dem Spirent WebAvalanche HTTP-Leistungstest sowie Ixia-Testtools nach Branchenstandard gemessen.
Tests erfolgten mit unterschiedlichen Datenströmen zwischen mehreren Portpaaren. Der VPN-Durchsatz wurde gemäß RFC 2544 unter Verwendung von UDP-Datenverkehr mit einer Paketgröße von 1418 Byte gemessen. Änderungen hinsichtlich technischer Daten und Funktionen vorbehalten.

Funktionen

RFDPI-ENGINE	
Funktion	**Beschreibung**
Reassembly-Free Deep Packet Inspection (RFDPI)	Diese hochleistungsfähige, proprietäre und patentierte Prüf-Engine führt eine streambasierte bidirektionale Verkehrsanalyse durch, um Eindringversuche und Malware zu erkennen und den Anwendungsverkehr zu identifizieren – unabhängig vom Port und ganz ohne Zwischenspeicherung oder den Umweg über einen Proxy.
Bidirektionale Prüfung	Der ein- und ausgehende Datenverkehr wird gleichzeitig auf Bedrohungen geprüft, um zu verhindern, dass ein infizierter Computer das Netzwerk zum Verbreiten von Malware oder als Ausgangsplattform für Angriffe nutzt.
Streambasierte Prüfung	Da die Prüfung ohne Zwischenspeicherung und Proxys stattfindet, lassen sich Millionen gleichzeitiger Datenströme mit der DPI-Technologie bei minimalen Latenzzeiten scannen, ohne dabei das Datenvolumen oder die Dateigrößen einzuschränken. Dies funktioniert sowohl bei gängigen Protokollen als auch bei Raw-TCP-Streams.
Hohe Parallelität und Skalierbarkeit	Gemeinsam mit der Multicore-Architektur ermöglicht das einzigartige Design der RFDPI-Engine einen hohen DPI-Durchsatz sowie extrem hohe Geschwindigkeiten beim Aufbau neuer Sitzungen. Verkehrsspitzen in anspruchsvollen Netzwerken lassen sich so besser bewältigen.
Single-Pass-Inspection	Eine Single-Pass-DPI-Architektur prüft den Verkehr auf Malware und Eindringversuche und sorgt gleichzeitig für die Erkennung von Anwendungen. Dadurch werden DPI-bedingte Latenzzeiten drastisch verkürzt. Außerdem wird sichergestellt, dass sämtliche Informationen zu Bedrohungen innerhalb einer einheitlichen Architektur verarbeitet werden.

FIREWALL UND NETZWERK	
Funktion	**Beschreibung**
REST-APIs	Durch diese API erhält die Firewall sämtliche Intelligence-Feeds von proprietären Anbietern, OEMs und Drittanbietern. Diese nutzt diese, um komplexe Bedrohungen wie Zero-Day-Angriffe, Insiderbedrohungen, Ransomware, Advanced Persistent Threats und Gefahren durch kompromittierte Zugangsdaten effektiv zu bekämpfen.
Stateful Packet Inspection	Der gesamte Netzwerkverkehr wird inspiziert und analysiert. Darüber hinaus wird sichergestellt, dass die Firewall- Zugriffsregeln erfüllt werden.
Hochverfügbarkeit[1]	Die NSv Series unterstützt Active/Passive (A/P) mit State-Synchronisierung.
Schutz vor DDoS-/DoS-Angriffen	Dank SYN-Flood-Schutz lassen sich DoS-Angriffe mit Layer-3-SYN-Proxy- und Layer-2-SYN-Blacklisting-Technologien abwehren. Außerdem lässt sich das Netzwerk durch UDP-/ICMP-Flood-Schutz und Begrenzung der Verbindungsgeschwindigkeit vor DoS-/DDoS-Angriffen schützen.
IPv6-Unterstützung	Die Umstellung von IPv4 auf IPv6 (Internet Protocol Version 6) ist noch nicht abgeschlossen. Mit SonicOS unterstützt die Hardware Filtering- und Wire-Implementierungsmodi.
Flexible Implementierungsoptionen	Die NSv Series lässt sich in konventionellen NAT-, Layer-2-Bridge-, Wire- und Netzwerk-Tap-Modi implementieren.
WAN-Lastverteilung	Lastverteilung auf mehrere WAN-Schnittstellen mit Round Robin, Spillover oder prozentbasierten Methoden.
Verbesserte QoS (Quality of Service)	Garantierte Unterstützung kritischer Datenübertragung dank 802.1p und DSCP-Tagging sowie Remapping von VoIP-Datenverkehr im Netzwerk.
SIP-Proxy wird unterstützt	Blockieren von Spam-Anrufen, da alle eingehenden Anrufe vom SIP-Proxy autorisiert und authentifiziert werden müssen.
Biometrische Authentifizierung	Unterstützung von Authentifizierungsmethoden für Mobilgeräte, bei denen eine Duplizierung oder Weitergabe nicht ohne Weiteres möglich ist, wie z. B. bei der Fingerabdruckerkennung. So lässt sich die Identität des Nutzers auf sichere Weise prüfen, bevor ein Zugriff auf das Netzwerk gewährt wird.
Offene Authentifizierung und Social Login	Erlaubt Gastbenutzern das Einloggen mit ihren Anmeldedaten aus sozialen Netzwerken wie Facebook, Twitter oder Google+ und den Zugriff auf das Internet bzw. auf andere Gastservices über die WLAN-, LAN- oder DMZ-Zonen eines Hosts mit Passthrough-Authentifizierung.

VERWALTUNG UND REPORTING	
Funktion	**Beschreibung**
Cloud-basierte und lokale Verwaltung	Die SonicWall Appliances lassen sich über die Cloud durch das SonicWall Capture Security Center sowie lokal durch das SonicWall Global Management System (GMS) konfigurieren und verwalten.
Leistungsstarke Verwaltung einzelner Geräte	Eine intuitive webbasierte Oberfläche beschleunigt und vereinfacht die Konfiguration, erlaubt eine umfassende Befehlszeilenschnittstelle und bietet Support für SNMPv2/3.
Berichte zum IPFIX-/NetFlow-Datenstrom	Export von Analyse- und Nutzungsdaten zum Anwendungsverkehr mittels IPFIX- oder NetFlow-Protokollen, um die Echtzeitüberwachung bzw. historische Überwachung sowie die Berichterstellung mit Tools wie SonicWall Scrutinizer oder anderen Tools, die IPFIX und NetFlow mit Erweiterungen unterstützen, zu ermöglichen.

VIRTUAL PRIVATE NETWORKING (VPN)	
Funktion	**Beschreibung**
Auto-Provisioning für VPNs	Durch Automatisierung der Site-to-Site-VPN-Gateway-Erstausstattung zwischen den SonicWall Firewalls ist die Implementierung komplexer verteilter Firewalls ein Kinderspiel. Funktionen für Sicherheit und Konnektivität werden umgehend und automatisch ausgeführt.
IPSec-VPN für Site-to-Site-Konnektivität	Dank leistungsstarkem IPSec-VPN kann die NSv Series als VPN-Konzentrator für Tausende großer Standorte, Zweigniederlassungen oder Home-Offices eingesetzt werden.
Remote-Zugriff per SSL-VPN- oder IPSec-Client	Durch Einsatz der clientlosen SSL-VPN-Technologie oder eines leicht zu verwaltenden IPSec-Clients ist der unkomplizierte Zugriff auf E-Mails, Dateien, Rechner, Intranet-Sites und Anwendungen von zahlreichen unterschiedlichen Plattformen möglich.

[1]*Hochverfügbarkeit wird derzeit von Azure und AWS nicht unterstützt*

Redundantes VPN-Gateway	Mit mehreren WANs lässt sich ein primäres und sekundäres VPN konfigurieren, um ein einfaches automatisches Failover und Failback für alle VPN-Sitzungen zu ermöglichen.
Routenbasiertes VPN	Bei Ausfall eines temporären VPN-Tunnels wird der Datenverkehr reibungslos über alternative Verbindungen zwischen Endgeräten umgeleitet. Dieses dynamische Routing über VPN-Links sorgt für eine hohe Ausfallsicherheit.

CONTENT- BZW. KONTEXTORIENTIERTE SICHERHEITSFUNKTIONEN	
Funktion	**Beschreibung**
Nachverfolgung der Benutzeraktivitäten	Bereitstellung von Informationen zur Benutzerkennung und -aktivität, die auf der nahtlosen SSO-Integration für AD/LDAP/Citrix1/Terminaldienste sowie umfassenden DPI-Daten basieren.
Identifizierung des Datenverkehrs nach Ländern mittels Geo-IP	Identifizierung und Kontrolle des Netzwerkverkehrs aus oder in bestimmte Länder. Schützt das Netzwerk vor Angriffen bzw. Sicherheitsbedrohungen bekannten oder verdächtigen Ursprungs. Zudem kann verdächtiger Verkehr, der vom Netzwerk ausgeht, analysiert werden. Möglichkeit, individuelle Länder- und Botnet-Listen zu erstellen, um einen nicht korrekten Landes- oder Botnet-Tag in Verbindung mit einer IP-Adresse zu überschreiben. Eliminiert unerwünschtes Filtering von IP-Adressen aufgrund einer Fehlklassifikation.
DPI-Filterung nach regulären Ausdrücken	Durch den Abgleich regulärer Ausdrücke lassen sich Inhalte, die ein Netzwerk passieren, identifizieren und kontrollieren und so Datenlecks verhindern. Es besteht die Möglichkeit, individuelle Länder- und Botnet-Listen zu erstellen, um einen nicht korrekten Landes- oder Botnet-Tag in Verbindung mit einer IP-Adresse zu überschreiben.

Breach-Prevention-Aboservices

CAPTURE ADVANCED THREAT PROTECTION	
Funktion	**Beschreibung**
Multi-Engine-Sandbox	Die Multi-Engine-Sandbox-Plattform mit virtualisiertem Sandboxing, umfassender Systemsimulation und einer Analysetechnologie auf Hypervisor-Ebene führt verdächtigen Code aus, analysiert dessen Verhalten und macht bösartige Aktivitäten transparent.
Real-Time Deep Memory Inspection (RTDMI)	Diese zum Patent angemeldete Cloud-basierte Technologie erkennt und blockiert Malware, die kein schädliches Verhalten zeigt und seine zerstörerische Kraft durch Verschlüsselung verbirgt. Weil die RTDMI Engine die Malware proaktiv zwingt, sich im Arbeitsspeicher zu enttarnen, erkennt und blockiert sie Massenmarkt- und Zero Day-Bedrohungen sowie unbekannte Malware.
Blockieren der Bedrohung bis zur Klärung des Sicherheitsstatus	Um zu verhindern, dass potenziell bösartige Dateien in das Netzwerk eindringen, können die zur Analyse in die Cloud gesendeten Dateien am Gateway festgesetzt werden, bis der Sicherheitsstatus geklärt ist.
Analyse unterschiedlichster Dateitypen und-größen	Der Service unterstützt die Analyse unterschiedlichster Dateitypen (entweder einzeln oder als Gruppe), darunter ausführbare Programme (PE), DLL, PDFs, MS-Office-Dokumente, Archive, JAR und APK sowie unterschiedliche Betriebssysteme wie Windows, Android, Mac OS X und Multi-Browser-Umgebungen.
Schnelle Implementierung von Signaturen	Wird eine Datei als bösartig identifiziert, so wird innerhalb von 48 Stunden eine Signatur auf Firewalls mit SonicWall Capture ATP-Abos aufgespielt und in die Gateway-Anti-Virus- und IPS-Signaturendatenbanken sowie URL-, IP- und Domain-Reputation-Datenbanken eingepflegt.
Capture Client	Capture Client ist eine einheitliche Client-Plattform mit mehreren Funktionen für die Endpunktsicherheit, darunter einem hoch entwickelten Malware-Schutz und einem umfassenden Einblick in den verschlüsselten Datenverkehr. Die Plattform bietet mehrschichtige Sicherheitstechnologien, umfassendes Reporting und einen zuverlässigen Endpunktschutz.

SCHUTZ VOR VERSCHLÜSSELTEN BEDROHUNGEN	
Funktion	**Beschreibung**
TLS-/SSL-Entschlüsselung und -Prüfung	Proxylose On-the-Fly-Entschlüsselung und -Prüfung von TLS-/SSL-Verkehr auf Malware, Eindringversuche und Datenlecks. Dabei werden Anwendungs-, URL- und Content-Kontrollregeln angewendet, um das Netzwerk vor Bedrohungen zu schützen, die im verschlüsselten Verkehr lauern. Dieser Service ist bei allen NSv Series-Modellen in den Sicherheitsabos inbegriffen.
SSH-Prüfung	Durch die Deep Packet Inspection-Prüfung von SSH-verschlüsseltem Verkehr (DPI-SSH) werden Daten, die über SSH-Tunnel übertragen werden, entschlüsselt und durchleuchtet, um Angriffe zu verhindern, die sich SSH zunutze machen.

INTRUSION PREVENTION	
Funktion	**Beschreibung**
Schutz durch Abwehrmechanismen	Ein eng integriertes Intrusion-Prevention-System (IPS) nutzt Signaturen und andere Abwehrmechanismen, um Paket-Payloads auf Schwachstellen und Exploits zu prüfen, und deckt dabei eine Vielzahl an Angriffen und Schwachstellen ab.
Automatische Signatur-Updates	Das SonicWall Threat Research-Team analysiert kontinuierlich Bedrohungen und sorgt für die ständige Aktualisierung einer umfassenden Liste an IPS-Abwehrmechanismen, die mehr als 50 Angriffskategorien abdeckt. Die neuen Updates sind sofort wirksam und erfordern weder einen Neustart noch sonstige Unterbrechungen.
IPS-Schutz innerhalb von Netzwerkzonen	Verbesserter Schutz vor internen Bedrohungen durch die Segmentierung des Netzwerks in mehrere Sicherheitszonen mit Intrusion-Prevention. Dies verhindert, dass sich Bedrohungen über Zonengrenzen hinaus ausbreiten.
Erkennen und Blockieren von Command-and-Control(CnC)-Aktivitäten durch Botnets	Erkennen und Blockieren von Command-and-Control-Verkehr, der von Bots im lokalen Netzwerk ausgeht und an IPs und Domänen geleitet wird, die nachweislich Malware verbreiten oder bekannte CnC-Punkte sind.
Protokollmissbrauch/-anomalien	Erkennen und Verhindern von Angriffen, die Protokolle missbrauchen, um unbemerkt am IPS vorbeizukommen.

Zero-Day-Schutz	Ständige Updates zu den neuesten Exploit-Techniken und -Methoden decken Tausende verschiedener Exploits ab und schützen das Netzwerk vor Zero-Day-Angriffen.
Umgehungsschutz	Umfassende Normalisierungs- und Entschlüsselungsmethoden sowie weitere Maßnahmen verhindern, dass Bedrohungen Umgehungstechniken auf den Schichten 2 bis 7 nutzen, um unerkannt in das Netzwerk einzudringen.

BEDROHUNGSSCHUTZ

Funktion	Beschreibung
Malware-Schutz am Gateway	Die RFDPI-Engine prüft den gesamten Verkehr auf Viren, Trojaner, Keylogger und andere Malware in Dateien unbegrenzter Größe und über alle Ports und TCP-Streams hinweg.
Die Prüfung erfolgt sowohl in ein- als auch ausgehender Richtung sowie innerhalb von Zonen. Malware-Schutz durch Capture Cloud	Eine kontinuierlich aktualisierte Datenbank mit mehreren Millionen Bedrohungssignaturen auf den SonicWall Cloud-Servern ergänzt die lokalen Signaturendatenbanken und sorgt dafür, dass die RFDPI-Engine eine größtmögliche Anzahl an Bedrohungen abdeckt.
Sicherheitsupdates rund um die Uhr	Neue Updates zu Bedrohungen werden automatisch an Firewalls vor Ort mit aktivierten Sicherheitsservices weitergeleitet und sind sofort wirksam, ohne dass Neustarts nötig sind oder andere Unterbrechungen verursacht werden.
Bidirektionale Raw-TCP-Prüfung	Die RFDPI-Engine ist in der Lage, Raw-TCP-Streams bidirektional auf sämtlichen Ports zu prüfen. So lassen sich Angriffe verhindern, bei denen veraltete Sicherheitssysteme umgangen werden, die sich lediglich auf ein paar bekannte Ports konzentrieren.
Unterstützung zahlreicher Protokolle	Identifizierung gängiger Protokolle wie HTTP/S, FTP, SMTP, SMBv1/v2 und andere, bei denen Daten nicht in Raw-TCP-Paketen gesendet werden. Payloads werden für die Malware-Prüfung entschlüsselt, auch wenn sie keine bekannten Standardports nutzen.

APPLICATION-INTELLIGENCE UND KONTROLLE

Funktion	Beschreibung
Anwendungskontrolle	Die RFDPI-Engine nutzt eine kontinuierlich erweiterte Datenbank mit Tausenden von Anwendungssignaturen, um Anwendungen oder einzelne Anwendungsfunktionen zu identifizieren und zu kontrollieren. Dadurch lassen sich Netzwerksicherheit und -produktivität erhöhen.
Identifizierung benutzerdefinierter Anwendungen	Die Lösung erstellt Signaturen auf der Grundlage bestimmter Parameter oder Muster, die nur bei der Netzwerkkommunikation bestimmter Anwendungen vorkommen. So lassen sich benutzerdefinierte Anwendungen kontrollieren und eine erweiterte Kontrolle über das Netzwerk erreichen.
Bandbreitenverwaltung auf Anwendungsebene	Bandbreitenkapazität kann für kritische Anwendungen oder Anwendungskategorien granular zugewiesen und reguliert werden. Gleichzeitig lässt sich sämtlicher nicht notwendige Anwendungsverkehr unterbinden.
Granulare Kontrolle	Kontrolle von Anwendungen oder bestimmten Anwendungskomponenten auf der Grundlage von Zeitplänen, Benutzergruppen, Ausschlusslisten und einer Reihe von Aktivitäten mit voller SSO-Benutzeridentifizierung durch LDAP-/AD-/Terminaldienst-/Citrix-Integration.

CONTENT-FILTERING

Funktion	Beschreibung
Internes/Externes Content-Filtering	Über den Content Filtering Service und Content Filtering Client lassen sich Richtlinien zu Nutzungseinschränkungen effektiv durchsetzen und HTTP-/HTTPS-Websites mit anstößigen oder produktivitätsmindernden Informationen oder Bildern blockieren.
Enforced Content Filtering Client	Erweiterung der Richtliniendurchsetzung, um Internetinhalte für Windows-, Mac OS-, Android- und Chrome-Geräte außerhalb der Firewallgrenze zu blockieren.
Granulare Kontrolle	Inhalte lassen sich auf Basis der bereits vordefinierten Kategorien oder einer beliebigen Kombination an Kategorien blockieren. Die Filter können für eine bestimmte Tageszeit aktiviert werden, z. B. während Unterrichts- oder Geschäftszeiten, und auf einzelne Benutzer oder Gruppen beschränkt werden.
Web-Caching	URL-Bewertungen werden lokal auf der SonicWall Firewall zwischengespeichert, sodass jeder weitere Zugriff auf häufig besuchte Websites nur den Bruchteil einer Sekunde dauert.

DURCHSETZUNG VON VIREN- UND SPYWARE-SCHUTZ

Funktion	Beschreibung
Mehrstufiger Schutz	Die Firewall ist die erste Verteidigungsstufe am Netzwerkrand. Zusammen mit dem Endpunktschutz verhindert sie das Eindringen von Viren über Laptops, USB-Sticks und andere ungeschützte Systeme.
Option für automatisierte Durchsetzung	Es wird sichergestellt, dass auf jedem Computer, der auf das Netzwerk zugreift, geeignete Antivirensoftware und/oder DPI-SSL-Zertifikate installiert und aktiviert sind. Somit entfallen die Kosten, die typischerweise für die Verwaltung desktopbasierter Virenschutzlösungen entstehen.
Option für automatisierte Bereitstellung und Installation	Die Clients für Viren- und Spyware-Schutz werden automatisch und netzwerkweit auf jedem Rechner installiert und bereitgestellt, sodass der administrative Mehraufwand minimiert wird.
Virenschutz der nächsten Generation	Capture Client nutzt eine statische Artificial-Intelligence(AI)-Engine, um Bedrohungen zu identifizieren, bevor sie ausgeführt werden. Darüber hinaus ermöglicht Capture Client ein Rollback auf einen Zustand vor der Infizierung.
Spyware-Schutz	Der leistungsstarke Spyware-Schutz scannt den eingehenden Verkehr und blockiert die Installation zahlreicher Spyware-Programme auf Desktop-PCs und Laptops, bevor vertrauliche Daten übertragen werden können. Auf diese Weise werden die Sicherheit und die Performance von Desktops erhöht.

Die SonicOS-Funktionen im Überblick

Globale Kontrolle über

- Zentralisierte Kontrolle der IPv6-Sichtbarkeit
- Globale Deaktivierung der IPv6-Verkehrsabwicklung
- Deaktivierung der Standard-VPN-Richtlinien, Konfigurationsanzeigen und automatisch generierten Regeln

Anmeldung und Benutzersicherheit

- Benutzeraussperrung auf Basis von Anmeldeversuchen nach IP-Adressbereich
- Benutzeraussperrung von CLI
- Forcierte Passwortänderung beim ersten Anmelden
- Zwei-Faktor-Authentifizierung (TOTP) wird unterstützt
- Gastbenutzerrichtlinie mit Zero-Touch-Portal wird unterstützt
- Gastservice IPv6 wird unterstützt
- TACACS+ Abrechnung wird unterstützt
- Quotenkontrolle für alle Benutzer
- Dynamische Botnet-HTTP-Authentifizierung

Networking und System

- SD-WAN wird unterstützt
- DNS Security / DNS Sinkhole wird unterstützt
- FQDN over TCP DNS
- FQDN-Adressobjekte für NAT
- DHCPv6-Relais
- IPv6-Adressierungsmodus für H.323 VoIP Application Layer Gateway
- Multiple Control Plane (CP)-Kern wird unterstützt
- HTTP/HTTPS-Umleitung mit Data Plane Offload
- IP-Helper Offload zur Data Plane
- Firmware-Backup im lokalen Speicherplatz
- Hochverfügbarkeit-Verschlüsselung
- Hochverfügbarkeit-Firmware-Upload wird unterstützt
- Regelbasierte Routing-Optimierung der statischen und dynamischen Routen
- Performance/Durchsatz-Verbesserungen
- Watchdog-Funktion zur Überwachung des Firewall-Zustands
- Optimierte Skalierbarkeit für erweitertes Routing über VPN-nummerierte Tunnelschnittstellen
- Update H.323 Bibliotheken basierend auf OSS Noklava v10.5.0 ASN.1 Komplilierer
- Task-Thread-Priorität-Updates
- SSLVPN und Lesezeichen auf Data Plane

Security Services

- Capture ATP blockieren der Bedrohung bis zur Klärung durch granulare Kontrolle
- Capture ATP-freundlicher Dateiname für nicht-HTTP-Protokolle
- CFS-Blockierung von individuellen YouTube-Videos
- Unterstützt HTTPS-Content-Filtering und DPI-SSL zusammen
- Next-Gen-Antivirus (SentinelOne) und DPI-SSL-Durchsetzung
- Verbesserte WAN DDOS-Schutzleistung

Regeln / Objekte

- Verbesserte Zugangsregeln
- App-basiertes Routing
- Dynamische Adressobjekte
- CFS-Regelausnahme
- Regelbasierte HTTPS-Content-Filtering-Objekte
- URI-Listengruppen in Content-Filtering-Objekten werden unterstützt
- Einfügung von CFS-Spezialkopfzeilen für HTTP-Anfragen
- UUID für Regeln und Objekte
- UUID für CFS-Regeln
- Quellen-MAC-Übersteuerung für NAT-Regeln

DPI-SSL / DPI-SSH

- DPI-SSL dynamische cloud-basierte Whitelist
- DPI-SSH-Blockierung von SSH-Port-Weiterleitungen
- DPI-SSH-Blockierung von X11-Weiterleitungen
- SSL-Entschlüsselungs-Port-Preservation in Packet-Mirror / Packet Capture
- DPI-SSL-granulare Kontrolle pro Zone
- Zugangsregeln basierend auf DPI-SSL-Kontrolle
- DPI-SSL-Client blockiert oder erlaubt abgelaufene CA-Zertifikate
- TLS-Zertifikatstatus mit Beantragung einer Verlängerung
- Unterstützung für lokale CRL
- Erweiterte DPI-SSL-Zertifikatverifizierung
- Unterstützung für ECDSA-bezogene Ciphers
- OpenSSL LTS Release-Unterstützung für Federal Zertifizierung

Protokollierung, Überwachung und Reporting

- Möglichkeit der Verifiziekrung, dass an einem bestimmten Paket eine DPI durchgeführt wurde
- Dateinamen- und URI-Protokollierung für App-Kontrolle
- Logon-Protokolle werden für Administrator angezeigt
- Konfigurationsaudit
- Protokollierung von NAT-Mapping für TCP-Verbindungen
- FTP-Unterstützung für Log-Automatisierung
- Capture Security Center (CSC) Reporting & Analytics-Unterstützung für NSv
- Capture ATP-Protokollierung der E-Mail-Absender/Empfänger
- Optimierung der Capture Threat Assessment Clients (SWARM v3)
- Funktion zum Rücksetzen der SFR (SWARM) statistischen Daten
- Option zum Wählen der Ausgabesprache für den SonicFlow Report

API

- SonicOS API Phase 1
- SonicOS API Authentifizerung wird unterstützt
- SonicOS API Phase 2
- LHM RESTful API

SonicOS Web Management UI

- SonicOS globale Suche
- Optimierte Nutzbarkeit für Content-Seiten
- Per-User client-seitig Speicherung der UI-Präferenen
- Pin-freundlicher Name für SonicOS Web Management-Anzeigen
- Refaktorisiertes SonicOS Web Interface-Layout

NSv Series – Bestellinformationen

PRODUKT	ESXI SKU	HYPER-V SKU	AZURE SKU	AWS SKU	KVM SKU
SonicWall NSv 10 Virtual Appliance TotalSecure Advanced Edition (1 Jahr)	01-SSC-5875	02-SSC-1387	02-SSC-3426	02-SSC-3452	02-SSC-3494
SonicWall NSv 25 Virtual Appliance TotalSecure Advanced Edition (1 Jahr)	01-SSC-5923	02-SSC-1395	02-SSC-3454	02-SSC-3464	02-SSC-3497
SonicWall NSv 50 Virtual Appliance TotalSecure Advanced Edition (1 Jahr)	01-SSC-5926	02-SSC-1399	02-SSC-3470	02-SSC-3474	02-SSC-3504
SonicWall NSv 100 Virtual Appliance TotalSecure Advanced Edition (1 Jahr)	01-SSC-5929	02-SSC-1405	02-SSC-3480	02-SSC-3489	02-SSC-3513
SonicWall NSv 200 Virtual Appliance TotalSecure Advanced Edition (1 Jahr)	01-SSC-5950	02-SSC-1412	02-SSC-0868	02-SSC-0906	02-SSC-3519
SonicWall NSv 300 Virtual Appliance TotalSecure Advanced Edition (1 Jahr)	01-SSC-5964	02-SSC-1420	—	—	02-SSC-3526
SonicWall NSv 400 Virtual Appliance TotalSecure Advanced Edition (1 Jahr)	01-SSC-6084	02-SSC-1427	02-SSC-0888	02-SSC-0912	02-SSC-3531
SonicWall NSv 800 Virtual Appliance TotalSecure Advanced Edition (1 Jahr)	01-SSC-6101	02-SSC-1429	02-SSC-0889	02-SSC-0914	02-SSC-3533
SonicWall NSv 1600 Virtual Appliance TotalSecure Advanced Edition (1 Jahr)	01-SSC-6109	02-SSC-1436	02-SSC-0895	02-SSC-0921	02-SSC-3540
PRODUKT	ESXI SKU	HYPER-V SKU	AZURE SKU	AWS SKU	KVM SKU
SonicWall NSv 10 Virtual Appliance TotalSecure Advanced Edition (3 Jahr)	01-SSC-5873	02-SSC-1386	02-SSC-3427	02-SSC-3453	02-SSC-3491
SonicWall NSv 25 Virtual Appliance TotalSecure Advanced Edition (3 Jahr)	01-SSC-5890	02-SSC-1397	02-SSC-3457	02-SSC-3465	02-SSC-3498
SonicWall NSv 50 Virtual Appliance TotalSecure Advanced Edition (3 Jahr)	01-SSC-5924	02-SSC-1398	02-SSC-3471	02-SSC-3472	02-SSC-3505
SonicWall NSv 100 Virtual Appliance TotalSecure Advanced Edition (3 Jahr)	01-SSC-5928	02-SSC-1404	02-SSC-3478	02-SSC-3486	02-SSC-3514
SonicWall NSv 200 Virtual Appliance TotalSecure Advanced Edition (3 Jahr)	01-SSC-5951	02-SSC-1411	02-SSC-0866	02-SSC-0903	02-SSC-3515
SonicWall NSv 300 Virtual Appliance TotalSecure Advanced Edition (3 Jahr)	01-SSC-5965	02-SSC-1419	—	—	02-SSC-3523
SonicWall NSv 400 Virtual Appliance TotalSecure Advanced Edition (3 Jahr)	01-SSC-6089	02-SSC-1426	02-SSC-0887	02-SSC-0911	02-SSC-3527
SonicWall NSv 800 Virtual Appliance TotalSecure Advanced Edition (3 Jahr)	01-SSC-6102	02-SSC-1428	02-SSC-0891	02-SSC-0913	02-SSC-3538
SonicWall NSv 1600 Virtual Appliance TotalSecure Advanced Edition (3 Jahr)	01-SSC-6108	02-SSC-1435	02-SSC-0897	02-SSC-0920	02-SSC-3542

**Für eine vollständige Liste der SKU wenden Sie sich bitte an Ihren lokalen SonicWall-Ansprechpartner*

Über SonicWall

SonicWall bietet Boundless Cybersecurity für das hyperverteilte Umfeld einer neuen Arbeitsrealität, in der jeder remote, mobil und ungeschützt ist. Indem SonicWall das Unbekannte kennt, Echtzeit-Transparenz und skalierbare Ökonomien ermöglicht, werden Cybersicherheitslücken bei Unternehmen, Regierungen und KMU weltweit geschlossen. Weitere Informationen finden Sie auf www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com

Datasheet-NSvVirtualFirewalls-US-VG-2088

SONICWALL®