



SonicWall Gen 7 NSa Series

Die SonicWall Network Security Appliance (NSa)-Next-Generation-Firewalls (NGFWs) der 7. Generation (Gen 7) bieten mittleren bis großen Unternehmen eine erstklassige Performance und die niedrigsten Total Cost of Ownership in ihrer Klasse.

Mit umfassenden Sicherheitsfeatures wie Intrusion-Prevention, VPN, Anwendungskontrolle, Malware-Analyse, URL-Filtering und IP-Reputationsdiensten schützen sie den Netzwerkrand zuverlässig vor hoch entwickelten Bedrohungen, ohne Engpässe zu verursachen.

HIGHLIGHTS

- Formfaktor: 1 HE
- Mehrere 1-GbE- und 10-GbE-Schnittstellen
- Multi-Gigabit-Durchsatzraten bei der Bedrohungs- und Malware-Analyse
- Enterprise-Internet-Edge-fähig
- Unterstützung der letzten (7.) SonicOS-Generation
- Sichere SD-WAN-Funktionen
- Intuitive Verwaltung über eine einzige Konsole
- TLS-1.3-Unterstützung
- Erstklassiges Preis-Leistungs-Verhältnis
- Schnelle DPI-Performance
- Niedrigste TCO in ihrer Klasse
- Hohe Portdichte für ein effizientes Netzwerk
- SonicWall-Switch, SonicWave-Access-Point und Capture-Client-Integration
- Redundante Stromversorgung



Überblick über die technischen Daten der Gen 7 NSa Series. **Alle technischen Daten anzeigen »**

Threat-Prevention-Durchsatz

3,5 GBit/s

Verbindungen

2 Millionen

Ports

Mehrere 10-GbE-Ports

Finden Sie die richtige SonicWall-Lösung für Ihr Unternehmen

sonicwall.com/products

Die Lösung kommt mit einer hohen Portdichte einschließlich mehreren 1-GbE- und 10-GbE-Ports und sorgt durch Hochverfügbarkeit, Clustering und zwei Stromversorgungen für eine hohe Netzwerk- und Hardware-Redundanz.

Die SonicWall Network Security Appliance (NSa)-Next-Generation-Firewalls (NGFWs) der 7. Generation (Gen 7) bieten mittleren bis großen Unternehmen eine erstklassige Performance und die niedrigsten Total Cost of Ownership in ihrer Klasse.

Mit umfassenden Sicherheitsfeatures wie Intrusion-Prevention, VPN, Anwendungskontrolle, Malware-Analyse, URL-Filtering und IP-Reputationsdiensten schützen sie den Netzwerkrand zuverlässig vor hoch entwickelten Bedrohungen, ohne Engpässe zu verursachen.

Die Gen 7 NSa Series wurde von Grund auf mit brandneuen Hardwarekomponenten entwickelt, die selbst bei verschlüsseltem Netzwerkverkehr einen Threat-Prevention-Durchsatz von mehreren Gigabit erlauben. Die Lösung kommt mit einer hohen Portdichte einschließlich mehreren 1-GbE- und 10-GbE-Ports und sorgt durch Hochverfügbarkeit, Clustering und zwei Stromversorgungen für eine hohe Netzwerk- und Hardware-Redundanz.

Generation 7 – SonicOS 7.0 und Sicherheitsservices

Die Gen 7 NSa Series läuft auf SonicOS 7.0, einem neuen Betriebssystem, das von Grund auf mit besonderem Augenmerk auf eine moderne Benutzerschnittstelle, intuitive Workflows und einen nutzerzentrierten Designansatz konzipiert wurde. SonicOS 7.0 bietet mehrere Features, mit denen sich die Workflows im Unternehmen vereinfachen lassen. Dank einer simplen Regelkonfiguration, einer vollautomatischen Implementierung und einer flexiblen Verwaltung können Unternehmen ihre Sicherheits- und operative Effizienz verbessern.

Die Gen 7 NSa Series unterstützt erweiterte Netzwerkfunktionen wie SD-WAN, dynamisches Routing, Clustering auf den Schichten 4 bis 7 sowie High-Speed-VPN-Funktionalität. Neben Firewall- und Switch-Funktionen bietet die Appliance eine einzige Konsole, um sowohl Switches als auch Access-Points zu verwalten.



Speziell konzipiert, um die hoch entwickelten Cyberangriffe von heute und morgen abzuwehren, erlaubt die Gen 7 NSa Series Zugriff auf die erweiterten Firewall-Sicherheitsservices von SonicWall, sodass Sie Ihre gesamte IT-Infrastruktur zuverlässig schützen können. Lösungen und Services wie Cloud Application Security, Capture Advanced Threat Protection (ATP), cloudbasiertes Sandboxing, Real-Time Deep Memory Inspection (RTDMI™) und Reassembly-Free Deep Packet Inspection (RFDPI) – für sämtlichen Traffic einschließlich TLS 1.3 – bieten einen umfassenden Gateway-Schutz vor den am besten getarnten und gefährlichsten Malware-Angriffen einschließlich Zero-Day- und verschlüsselten Bedrohungen.

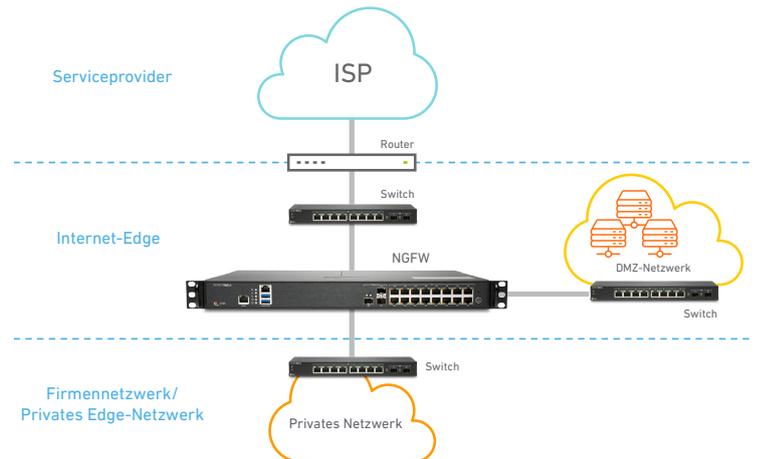
Implementierungsoptionen

Die Gen 7 NSa Series bietet im Wesentlichen zwei Implementierungsoptionen für mittlere und verteilte Unternehmen:

Internet-Edge-Implementierung

Bei dieser standardmäßigen Implementierungsoption schützt die NGFW der Gen 7 NSa Series private Netzwerke vor böartigem Netzwerkverkehr aus dem Internet. Auf diese Weise können Sie:

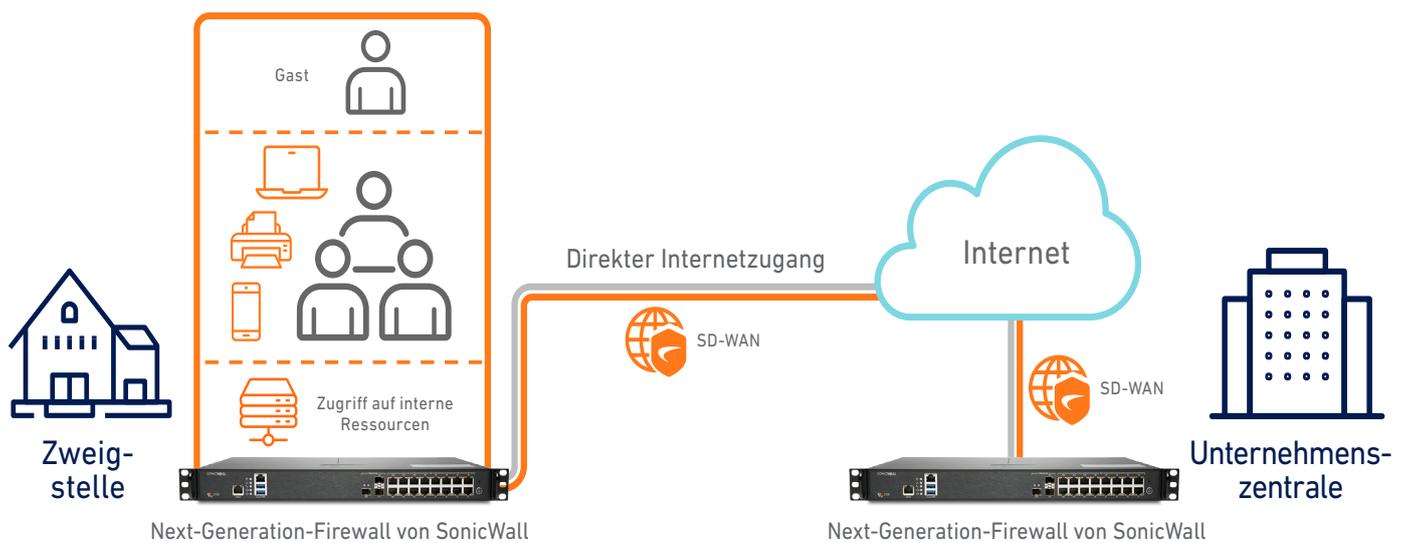
- von einer bewährten NGFW-Lösung mit der höchsten Performance und Portdichte (einschließlich 10-GbE-Konnektivität) in ihrer Klasse profitieren
- umfassende Einblicke gewinnen und den verschlüsselten Verkehr einschließlich TLS 1.3 durchsuchen, um schwer zu fassende Bedrohungen aus dem Internet ohne Abstriche bei der Performance zu blockieren.
- Ihr Unternehmen mit integrierten Sicherheitsfunktionen wie Malware-Analyse, Cloud-App-Sicherheit, URL-Filtering und Reputationsdiensten schützen
- Platz und Geld sparen, während Sie von einer integrierten NGFW-Lösung mit hoch entwickelten Sicherheits- und Netzwerkfunktionen profitieren
- durch eine einzige intuitive Benutzeroberfläche für eine zentrale Verwaltung die Komplexität reduzieren und die Effizienz maximieren



Implementierung für mittlere und verteilte Unternehmen

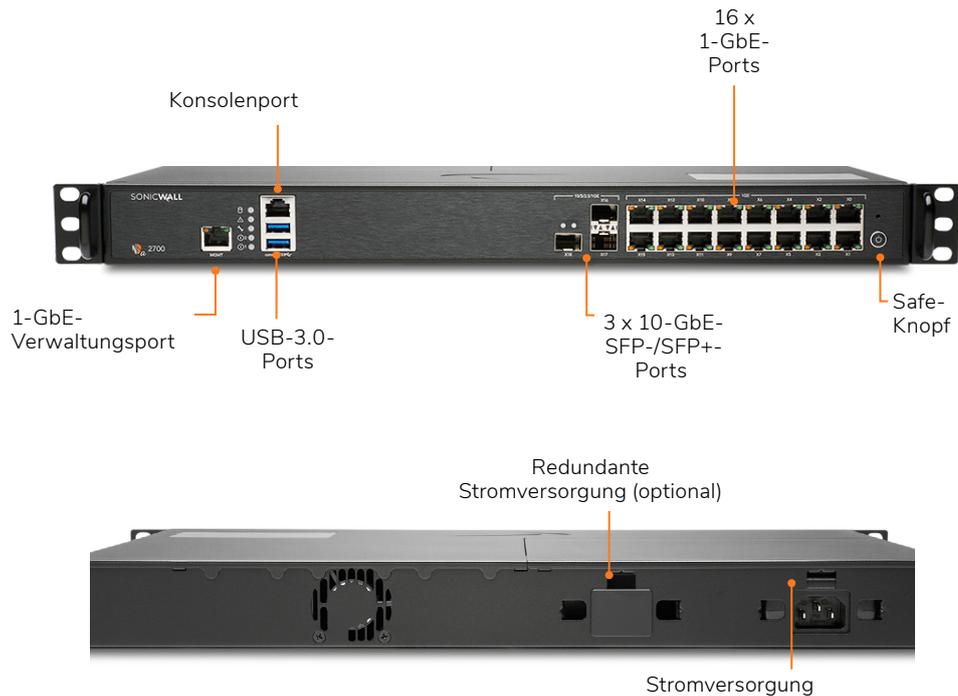
Dank ihrer SD-WAN-Unterstützung und ihrer zentralen Verwaltung eignet sich die SonicWall Gen 7 NSa Series ideal für mittlere und verteilte Unternehmen. Mit dieser Implementierungsoption können Organisationen:

- eine zukunftssichere Lösung für einen umfassenden Schutz in einer dynamischen Bedrohungslandschaft sicherstellen und dabei von einer leistungsstarken Multi-Gigabit-Performance bei der Bedrohungsanalyse profitieren
- Zweigniederlassungen einen direkten und sicheren Internetzugang bereitstellen, anstatt ein Backhaul über die Unternehmenszentrale durchzuführen
- ihren Zweigniederlassungen einen sicheren Zugriff auf interne Ressourcen in der Unternehmenszentrale oder in einer Public Cloud bieten und so die Anwendungslatenz deutlich verbessern
- Bedrohungen, die verschlüsselte Protokolle wie TLS 1.3 nutzen, automatisch blockieren und so ihre Netzwerke vor den raffiniertesten Angriffen schützen
- durch eine einzige intuitive Benutzeroberfläche für eine zentrale Verwaltung die Komplexität reduzieren und die Effizienz maximieren
- dank einer hohen Portdichte einschließlich 10-GbE-Konnektivität verteilte Netzwerke und Wide-Area-Netzwerke unterstützen

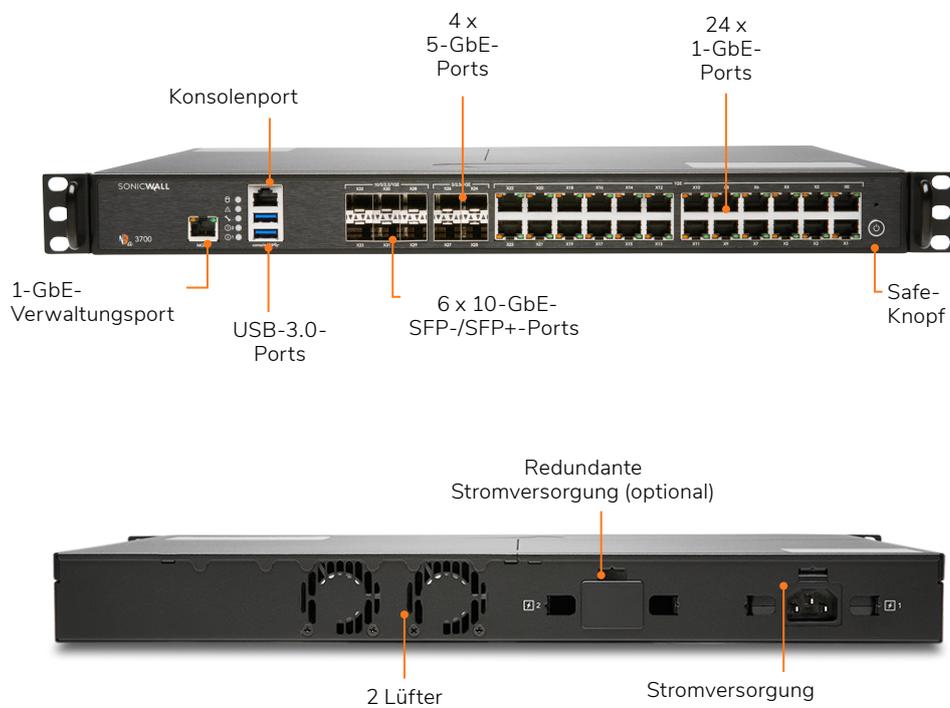


SonicWall Gen 7 NSa Series

NSa 2700



NSa 3700



Gen 7 NSa Series – technische Daten

Firewall	NSa 2700	NSa 3700
Betriebssystem	SonicOS 7.0	SonicOS 7.0.1
Schnittstellen	16 x 1-GbE, 3 x 10-GbE-SFP+, 2 USB 3.0, 1 Konsole, 1 Verwaltungsport	24 x 1-GbE, 6 x 10-GbE-SFP+, 4 x 5-GbE-SFP+, 2 USB 3.0, 1 Konsole, 1 Verwaltungsport
Speicher	64 GB M.2	128 GB M.2
Erweiterung	Erweiterungssteckplatz für Speicher (bis zu 256 GB)	Erweiterungssteckplatz für Speicher (bis zu 256 GB)
VLAN-Schnittstellen	256	256
Unterstützte Access-Points (max.)	32	32
Firewall-/VPN-Performance		
Firewall-Inspection-Durchsatz ¹	5,2 GBit/s	5,5 GBit/s
Threat-Prevention-Durchsatz ²	3,0 GBit/s	3,5 GBit/s
Application-Inspection-Durchsatz ²	3,6 GBit/s	4,2 GBit/s
IPS-Durchsatz ²	3,4 GBit/s	3,8 GBit/s
Anti-Malware-Inspection-Durchsatz ²	2,9 GBit/s	3,5 GBit/s
Durchsatz bei TLS-/SSL-Prüfung und -Entschlüsselung (DPI-SSL) ²	800 MBit/s	850 MBit/s
IPSec-VPN-Durchsatz ³	2,1 GBit/s	2,2 GBit/s
Verbindungen pro Sekunde	21.500	22.500
Max. Anzahl von Verbindungen (SPI)	1.500.000	2.000.000
Max. Anzahl von DPI-SSL-Verbindungen	125.000	150.000
Max. Anzahl von Verbindungen (DPI)	500.000	750.000
VPN		
Site-to-Site-VPN-Tunnel	2.000	3.000
IPSec-VPN-Clients (max.)	50 (1.000)	50 (1.000)
SSL-VPN-Lizenzen (max.)	2 (500)	2 (500)
Verschlüsselung/Authentifizierung	DES, 3DES, AES (128/192/256 Bit) / MD5, SHA-1, Suite B Cryptography	
Schlüsselaustausch	Diffie-Hellman-Gruppen 1, 2, 5, 14v	
Routenbasiertes VPN	RIP, OSPF, BGP	
Unterstützte Zertifikate	Verisign, Thawte, Cybertrust, RSA Keon, Entrust und Microsoft CA für SonicWall-to-SonicWall-VPN, SCEP	
VPN-Funktionen	Dead-Peer-Detection, DHCP über VPN, IPSec-NAT-Traversal, redundantes VPN-Gateway, routenbasiertes VPN	
Unterstützte globale VPN-Client-Plattformen	Microsoft® Windows Vista (32/64 Bit), Windows 7 (32/64 Bit), Windows 8.0 (32/64 Bit), Windows 8.1 (32/64 Bit), Windows 10	
NetExtender	Microsoft Windows Vista (32/64 Bit), Windows 7, Windows 8.0 (32/64 Bit), Windows 8.1 (32/64 Bit), Mac OS X 10.4+, Linux FC3+/Ubuntu 7+/openSUSE	
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (Embedded)	
Sicherheitservices		
Deep Packet Inspection-Services	Gateway-Anti-Virus, Anti-Spyware, Intrusion-Prevention, DPI-SSL	
Content Filtering Service (CFS)	Prüfung nach HTTP-URL, HTTPS-IP, Schlüsselwörtern und Inhalt, umfassende Filterung anhand von Dateitypen wie ActiveX, Java, Cookies für Datenschutz, Freigabe- und Sperrlisten	
Comprehensive Anti-Spam Service	unterstützt	
Anwendungsvisualisierung	Ja	
Anwendungskontrolle	Ja	
Capture Advanced Threat Protection	Ja	
Netzwerk		
IP-Adressenzuweisung	Statisch (DHCP-, PPPoE-, L2TP- und PPTP-Client), interner DHCP-Server, DHCP-Relay	
NAT-Modi	1:1, 1:many, many:1, many:many, flexible NAT (überlappende IPs), PAT, transparenter Modus	
Routing-Protokolle	BGP4, OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing	
QoS	Bandbreitenpriorität, maximale Bandbreite, garantierte Bandbreite, DSCP-Markierung, 802.1e (WMM)	

Gen 7 NSa Series – technische Daten

Firewall	NSa 2700	NSa 3700
Authentifizierung	LDAP (mehrere Domains), XAUTH/RADIUS, SSO, Novell, interne Benutzerdatenbank, Terminaldienste, Citrix, Common Access Card (CAC)	
Lokale Benutzerdatenbank	250	
VoIP	Full H323-v1-5, SIP	
Standards	TCP/IP, UDP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3	
Zertifikate (ausstehend)	FIPS 140-2 (mit Suite B) Level 2, UC APL, VPNC, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-Virus, Common Criteria NDPP (Firewall und IPS)	
Common Access Card (CAC)	unterstützt	
Hochverfügbarkeit	Active/Passive mit Stateful-Synchronisierung	
Hardware		
Formfaktor	rackfähig (1 HE)	rackfähig (1 HE)
Stromversorgung	60 W	90 W
Maximaler Stromverbrauch (W)	21,5	36,3
Eingangsspannung	100–240 VAC, 50–60 Hz	100–240 VAC, 50–60 Hz
Gesamtwärmeabgabe	73,32 BTU	123,78 BTU
Abmessungen	43 x 32.5 x 4.5 cm	43 x 32.5 x 4.5 cm
Gewicht	4,0 kg	4,6 kg
WEEE-Gewicht	4,2 kg	4,8 kg
Versandgewicht	6,4 kg	7 kg
Umgebung (Betrieb/Lagerung)	0 bis 40 °C / -40 bis 70 °C	
Luftfeuchtigkeit	5–95 %, nicht kondensierend	
Richtlinien		
Erfüllt folgende Standards/Normen	FCC Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, MSIP/KCC Class A, UL, cUL, TUV/GS, CB, Mexico CoC nach UL, WEEE, REACH, ANATEL, BSMI	FCC Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, MSIP/KCC Class A, UL, cUL, TUV/GS, CB, Mexico CoC nach UL, WEEE, REACH, ANATEL, BSMI

1. Testmethoden: Die maximale Firewall-Leistung wurde auf Basis von RFC 2544 getestet. Die tatsächliche Leistung kann je nach Betriebsbedingungen bzw. aktivierten Diensten variieren.
2. Der Threat-Prevention-/Gateway-AV-/Anti-Spyware-/IPS-Durchsatz wurde mit dem Spirent WebAvalanche HTTP-Leistungstest sowie Ixia-Testtools nach Branchenstandard gemessen. Tests erfolgten mit unterschiedlichen Datenströmen zwischen mehreren Portpaaren. Threat-Prevention-Durchsatz bei aktiviertem Gateway-AV, Anti-Spyware und IPS sowie aktivierter Anwendungskontrolle gemessen.
3. Messung des VPN-Durchsatzes gemäß RFC 2544 bei UDP-Verkehr mit 1.280 Bytes pro Paket. Änderungen hinsichtlich technischer Daten, Funktionen und Verfügbarkeit vorbehalten.

PARTNER ENABLED SERVICES

Brauchen Sie Hilfe bei der Planung, Implementierung oder Optimierung Ihrer SonicWall-Lösung? Die SonicWall Advanced Services Partner unterstützen Sie mit erstklassigen Professional Services. Weitere Informationen:

www.sonicwall.com/PES

Die SonicOS-7.0-Funktionen im Überblick

Firewall

- Stateful Packet Inspection
- Reassembly-Free Deep Packet Inspection
- Schutz vor DDoS-Angriffen (UDP-/ICMP-/SYN-Flood)
- IPv4-/IPv6-Unterstützung
- Biometrische Authentifizierung für den Remote-Zugriff
- DNS-Proxy
- Umfassende API-Unterstützung
- SonicWall-Switch-Integration
- SD-WAN-Skalierbarkeit
- SD-WAN-Usability-Assistent¹
- SonicCoreX- und SonicOS-Containerisierung¹
- Skalierbarkeit von Verbindungen (SPI, DPI, DPI-SSL)
- Verbessertes Dashboard¹
- Optimierte Geräteansicht
- Überblick über den häufigsten Traffic und die häufigsten Nutzer
- Einblick in Bedrohungen
- Benachrichtigungszentrale

TLS-/SSL-/SSH-Entschlüsselung und -Prüfung

- TLS 1.3 mit verbesserter Sicherheit¹
- Deep Packet Inspection für TLS/SSL/SSH
- Ein-/Ausschluss von Objekten, Gruppen oder Hostnamen
- SSL-Steuerung
- Verbesserungen für DPI-SSL mit CFS
- Granulare DPI-SSL-Steuerung nach Zone oder Regel
- Capture Advanced Threat Protection²
- Real-Time Deep Memory Inspection
- Cloudbasierte Multi-Engine-Analyse
- Virtualisiertes Sandboxing
- Analyse auf Hypervisor-Ebene
- Umfassende Systemsimulation
- Prüfung unterschiedlichster Dateitypen
- Automatisierte und manuelle Dateiübermittlung
- Laufend aktualisierte Echtzeitinformationen zu Bedrohungen
- Blockieren der Bedrohung bis zur Klärung des Sicherheitsstatus
- Capture Client

Intrusion-Prevention²

- Signaturbasierte Scans
- Automatische Signatur-Updates
- Bidirektionale Prüfung
- Granulare IPS-Regeln

- GeolP-Durchsetzung
- Botnet-Filtering mit dynamischer Liste
- Abgleich regulärer Ausdrücke

Anti-Malware²

- Streambasierte Malware-Scans
- Virenschutz am Gateway
- Spyware-Schutz am Gateway
- Bidirektionale Prüfung
- Keine Einschränkung bei der Dateigröße
- Cloudbasierte Malware-Datenbank

Anwendungsidentifizierung²

- Anwendungskontrolle
- Bandbreitenverwaltung auf Anwendungsebene
- Erstellen personalisierbarer Anwendungssignaturen
- Schutz vor Datenlecks
- Erstellung von Anwendungsberichten über NetFlow/IPFIX
- Umfassende Anwendungs-signaturendatenbank

Visualisierung und Analyse des Datenverkehrs

- Benutzeraktivitäten
- Anwendung/Bandbreite/Bedrohung
- Cloudbasierte Analysen

Filterung von HTTP-/HTTPS-Webinhalten²

- URL-Filtering
- Proxy-Vermeidung
- Blockieren mithilfe von Schlüsselwörtern
- Regelbasierte Filterung (Ein-/Ausschluss)
- Einfügen des HTTP-Headers
- Bandbreitenverwaltung anhand von CFS-Ratingkategorien
- Einheitliches Richtlinienmodell mit Anwendungskontrolle
- Content Filtering Client

VPN

- Sicheres SD-WAN
- Auto-Provisioning für VPNs
- IPSec-VPN für Site-to-Site-Konnektivität
- Remote-Zugriff per SSL-VPN und IPSec-Client
- Redundantes VPN-Gateway
- Mobile Connect für iOS, Mac OS X, Windows, Chrome, Android und Kindle Fire
- Routenbasiertes VPN (OSPF, RIP, BGP)

Netzwerk

- PortShield
- Jumbo-Frames
- Path MTU Discovery
- Erweiterte Protokollierung
- VLAN-Trunking
- Portspiegelung (NSa 2650 und höher)
- Layer-2-QoS
- Portsicherheit
- Dynamisches Routing (RIP/OSPF/BGP)
- SonicWall Wireless Controller
- Regelbasiertes Routing (ToS/metrisch und ECMP)
- NAT
- DHCP-Server
- Bandbreitenverwaltung
- Hochverfügbarkeitsmodus A/P mit State-Sync
- Lastausgleich für ein- und ausgehenden Datenverkehr
- Hochverfügbarkeit – Active/Standby mit State-Sync
- L2-Bridge-, Wire-/Virtual Wire-, Tap-, NAT-Modus
- Asymmetrisches Routing
- Common Access Card (CAC)-Unterstützung

VoIP

- Granulare QoS-Kontrolle
- Bandbreitenverwaltung
- DPI für VoIP-Datenverkehr
- H.323-Gatekeeper- und SIP-Proxy-Unterstützung

Verwaltung, Überwachung und Unterstützung

- Unterstützung von Capture Security Appliance (CSa)
- Capture Threat Assessment (CTA) V2.0
- Neues Design oder Template
- Vergleich mit Branchen- bzw. weltweitem Durchschnitt
- Neue UI/UX, intuitives Feature-Layout¹
- Dashboard
- Geräteinformationen, Anwendungen, Bedrohungen
- Topology View
- Vereinfachte Erstellung und Verwaltung von Richtlinien
- Nutzungsstatistiken zu Regeln/Objekten¹
- Verwendet vs. nicht verwendet
- Aktiv vs. inaktiv
- Globale Suche nach statischen Daten
- Speicherunterstützung¹

Die SonicOS-7.0-Funktionen im Überblick (Fortsetzung)

- Interne und externe Speicherverwaltung¹
- WWAN-USB-Modem Unterstützung (5G/LTE/4G/3G)
- Network Security Manager (NSM)-Unterstützung
- Weboberfläche
- Befehlszeilenschnittstelle (CLI)
- Vollautomatische Registrierung und Bereitstellung
- Einfaches CSC-Reporting¹
- Unterstützung der mobilen SonicExpress-App
- SNMPv2/v3
- Zentralisierte Verwaltung und zentrales Reporting mit dem SonicWall Global Management System (GMS)²
- Logging
- NetFlow-/IPFIX-Export
- Cloudbasiertes Konfigurationsbackup
- BlueCoat Security Analytics Platform
- Anwendungs- und Bandbreitenvisualisierung
- IPv4- und IPv6-Verwaltung
- CD-Management-Anzeige
- Dell N-Series- und X-Series-Switch-Verwaltung mit hintereinandergeschalteten Switches

Fehlersuche und Diagnose

- Erweiterte Paketüberwachung
- SSH-Terminal auf der Benutzeroberfläche

Wireless

- SonicWave-AP-Cloud-Management
- WIDS/WIPS
- Vermeidung unberechtigter APs
- Schnelles Roaming (802.11k/r/v)
- 802.11s-Mesh-Networking
- Automatische Kanalauswahl
- Analyse des HF-Spektrums
- Floor Plan View
- Topology View
- Bandsteering
- Beamforming
- AirTime-Fairness
- Bluetooth Low Energy
- MiFi-Extender
- Verbesserte Funkfrequenzen
- Zyklische Quote für Gastbenutzer

¹ Neues Feature, erhältlich für SonicOS 7.0

² Erfordert zusätzliches Abo

Erfahren Sie mehr über die SonicWall Gen 7 NSa Series

www.sonicwall.com/products/firewalls

Über SonicWall

SonicWall bietet grenzenlose Cybersicherheit für eine extrem dezentrale Arbeitswelt, in der jeder remote, mobil und potenziell gefährdet ist. Durch die Identifizierung unbekannter Bedrohungen, seine modernen Echtzeit-Überwachungsfunktionen und seine herausragende Wirtschaftlichkeit hilft SonicWall Unternehmen, Behörden und KMUs weltweit, die Cybersicherheitslücke zu schließen. Für weitere Informationen besuchen Sie uns auf www.sonicwall.com oder folgen Sie uns auf [Twitter](#), [LinkedIn](#), [Facebook](#) und [Instagram](#).



SonicWall, Inc.

1033 McCarthy Boulevard | Milpitas, Kalifornien 95035, USA

Weitere Informationen erhalten Sie auf unserer Website.

www.sonicwall.com

© 2021 SonicWall Inc. ALLE RECHTE VORBEHALTEN.

SonicWall ist eine Marke oder eingetragene Marke von SonicWall Inc. und/oder deren Tochtergesellschaften in den USA und/oder anderen Ländern. Alle anderen Marken und eingetragenen Marken sind Eigentum der jeweiligen Inhaber. Die Informationen in diesem Dokument werden in Verbindung mit den Produkten von SonicWall Inc. und/oder deren Tochtergesellschaften bereitgestellt. Sie erhalten durch dieses Dokument oder in Verbindung mit dem Verkauf von SonicWall-Produkten keine Lizenz (weder ausdrücklich noch stillschweigend, durch Rechtsverwirkung oder anderweitig) für geistige Eigentumsrechte. SONICWALL UND/ODER DESSEN TOCHTERGESELLSCHAFTEN ÜBERNEHMEN KEINE HAFTUNG UND KEINERLEI AUSDRÜCKLICHE, STILLSCHWEIGENDE ODER GESETZLICHE GEWÄHRLEISTUNG FÜR DEREN PRODUKTE, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG FÜR DIE HANDELSÜBLICHKEIT, DIE VERWENDUNGSFÄHIGKEIT FÜR EINEN BESTIMMTEN ZWECK UND DIE NICHTVERLETZUNG VON RECHTEN DRITTER, SOWEIT SIE NICHT IN DEN BESTIMMUNGEN DER LIZENZVEREINBARUNG FÜR DIESES PRODUKT NIEDERGELEGT SIND. SONICWALL UND/ODER DESSEN TOCHTERGESELLSCHAFTEN HAFTEN NICHT FÜR IRGENDWELCHE UNMITTELBAREN, MITTELBAREN, STRAFRECHTLICHEN, SPEZIELLEN, ZUFÄLLIGEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF SCHÄDEN AUS ENTGANGENEM GEWINN, GESCHÄFTSUNTERBRECHUNG ODER VERLUST VON INFORMATION), DIE AUS DER VERWENDUNG ODER DER UNMÖGLICHKEIT DER VERWENDUNG DIESES DOKUMENTS ENTSTEHEN, SELBST WENN SONICWALL UND/ODER DESSEN TOCHTERGESELLSCHAFTEN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDEN. SonicWall und/oder dessen Tochtergesellschaften übernehmen keine Gewährleistungen in Bezug auf die Genauigkeit oder Vollständigkeit dieses Dokuments und behalten sich das Recht vor, Spezifikationen und Produktbeschreibungen jederzeit ohne Vorankündigung zu ändern. SonicWall Inc. und/oder deren Tochtergesellschaften übernehmen keinerlei Verpflichtung, die in diesem Dokument enthaltenen Informationen zu aktualisieren.