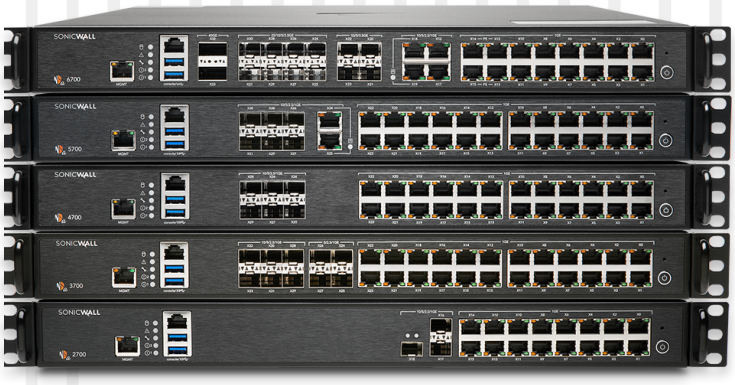
SonicWall Gen 7 NS*a* Series

Die SonicWall Network Security Appliance(NS*a*)-Next-Generation-Firewalls (NGFWs) der 7. Generation (Gen 7) bieten mittleren bis großen Unternehmen eine erstklassige Performance und die niedrigsten Gesamtbetriebskosten ihrer Klasse.

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



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

Bis zu 19 GBit/s	Bis zu 8 Millionen	40-/25-/10-/5-/2,5-/1-G
Threat-Prevention-Durchsatz	Verbindungen	Ports

HIGHLIGHTS

- Formfaktor: 1 HE
- Unterstützung für 40-/25-/10-/5-/2,5-/1-G-Ports
- Multi-Gigabit-Durchsatzraten bei der Bedrohungs- und Malware-Analyse
- Überragende TLS-Performance (Sessions und Durchsatz)
- Erweiterbarer Speicher
- DNS-Sicherheit
- Reputationsbasierter Content Filtering Service (CFS 5.0)
- Wi-Fi-6-Firewall-Management
- Integration von Network Access Control (NAC) mit Aruba ClearPass
- Enterprise-Internet-Edge-fähig
- Unterstützung der letzten (7.) SonicOS-Generation
- Sichere SD-WAN-Funktionen
- Intuitive Benutzeroberfläche mit zentraler Verwaltung
- TLS-1.3-Unterstützung
- Erstklassiges Preis-Leistungs-Verhältnis
- Unterstützt durch das SonicWall Capture Labs Threat Research-Team
- Hohe Portdichte für ein effizientes Netzwerk
- SonicWall-Switch, SonicWave-Access-Point und Capture-Client-Integration
- Redundante Stromversorgung

DATENBLATT

Die Lösung kommt mit einer hohen Portdichte einschließlich mehreren 40-GbE- und 10-GbE-Ports und sorgt durch Hochverfügbarkeit und zwei Stromversorgungen für eine hohe Netzwerk- und Hardware-Redundanz.

Die SonicWall Network Security Appliance(NS*a*)-Next-Generation-Firewalls (NGFWs) der 7. Generation (Gen 7) bieten mittleren bis großen Unternehmen eine erstklassige Performance und die niedrigsten Gesamtbetriebskosten ihrer Klasse.

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

Die Gen 7 NS*a* 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 40-GbE- und 10-GbE-Ports und sorgt durch Hochverfügbarkeit und zwei Stromversorgungen für eine hohe Netzwerk- und Hardware-Redundanz.

Generation 7 – SonicOS 7 und Sicherheitsservices

Die Gen 7 NS*a* 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 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 NS*a* Series unterstützt erweiterte Netzwerkfunktionen wie SD-WAN, dynamisches Routing, Hochverfügbarkeit 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 NS*a* 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, patentierte 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.

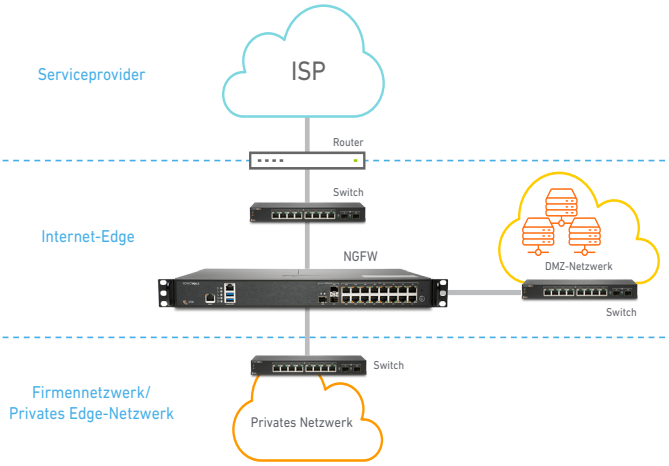
Implementierungsoptionen

Die Gen 7 NS*a* Series bietet im Wesentlichen zwei Implementierungsoptionen für mittlere und verteilte Unternehmen:

Internet-Edge-Implementierung

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

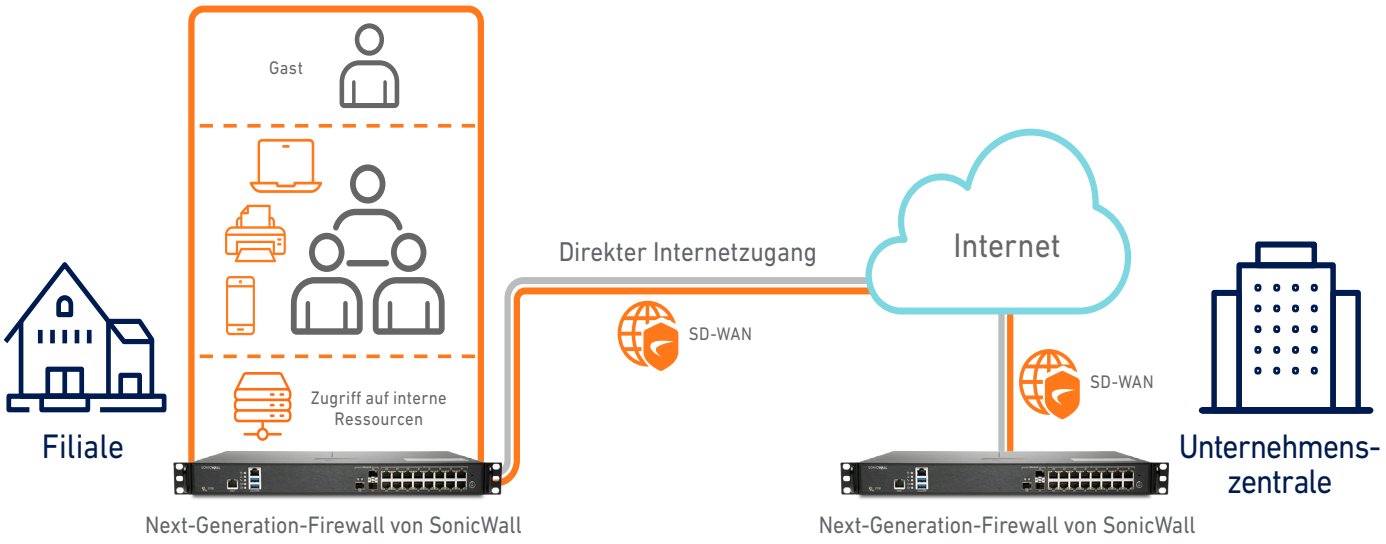
- von einer bewährten NGFW-Lösung mit der höchsten Performance und Portdichte (einschließlich 40-GbE- und 10-GbE-Konnektivität) ihrer Klasse profitieren
- umfassende Einblicke gewinnen und den verschlüsselten Verkehr einschließlich TLS 1.3 durchsuchen, um schwer zu fassende Bedrohungen aus dem Internet 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



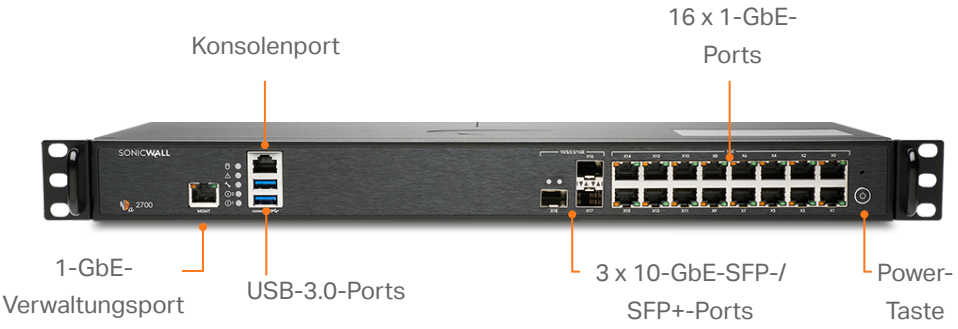
Implementierung für mittlere und verteilte Unternehmen

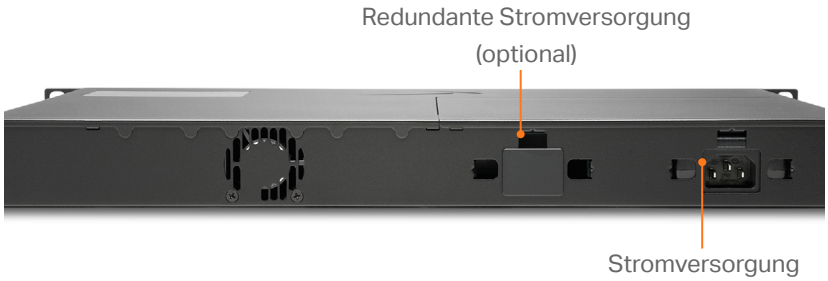
Dank ihrer SD-WAN-Unterstützung und ihrer zentralen Verwaltung eignet sich die SonicWall Gen 7 NS*a* Series ideal für mittlere und verteilte Unternehmen. Mit dieser Implementierungsoption können Organisationen:

- eine zukunftssichere Lösung für einen umfassenden Schutz in einer dynamischen Bedrohungslandschaft sicherstellen und dabei von einer leistungsstarken Multi-Gigabit-Performance bei der Bedrohungsanalyse profitieren
- ihren Filialen einen direkten und sicheren Internetzugriff bereitstellen, anstatt ein Backhaul über die Unternehmenszentrale durchzuführen
- ihren Filialen 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 40-GbE- und 10-GbE-Konnektivität verteilte Netzwerke und Wide-Area-Netzwerke unterstützen

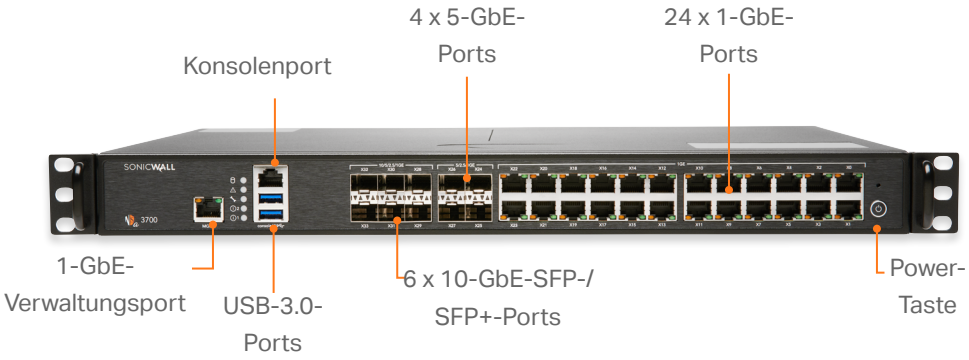


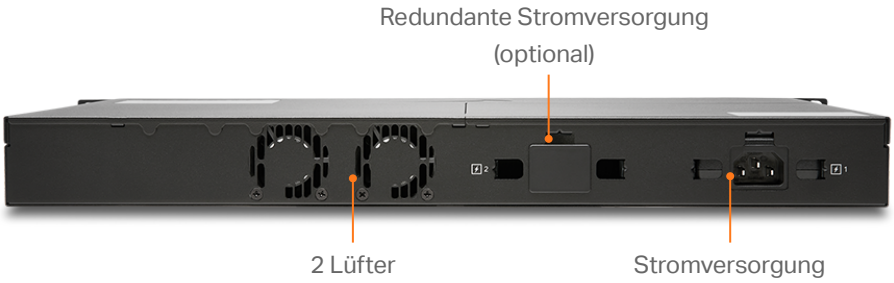
NS*a* 2700



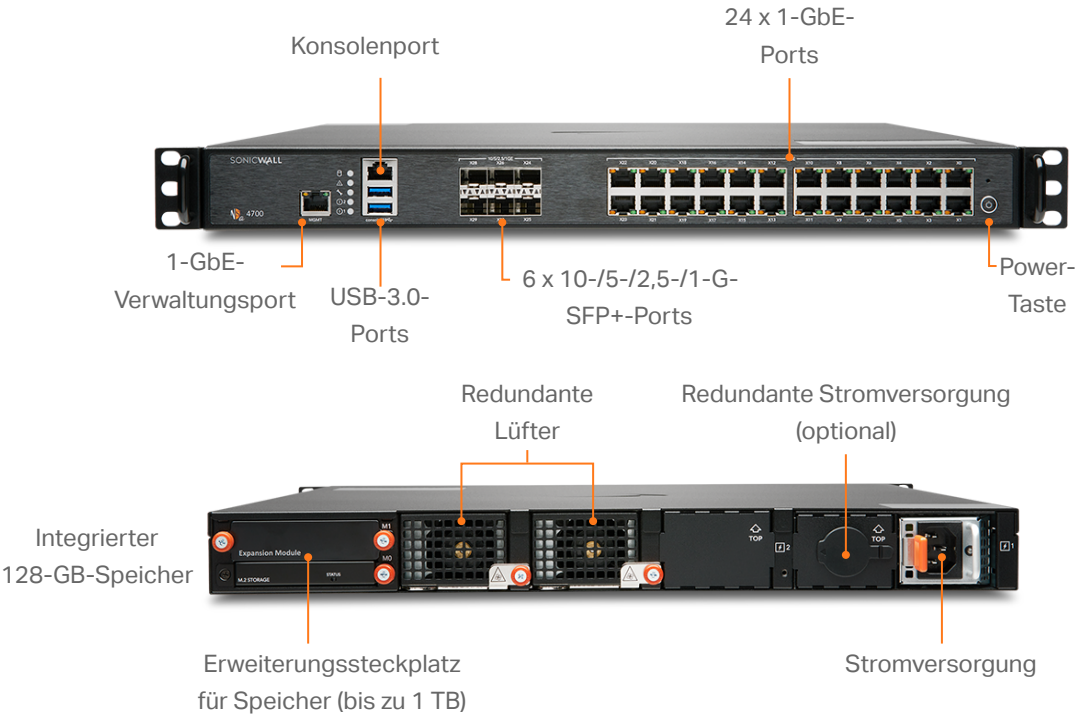


NS*a* 3700

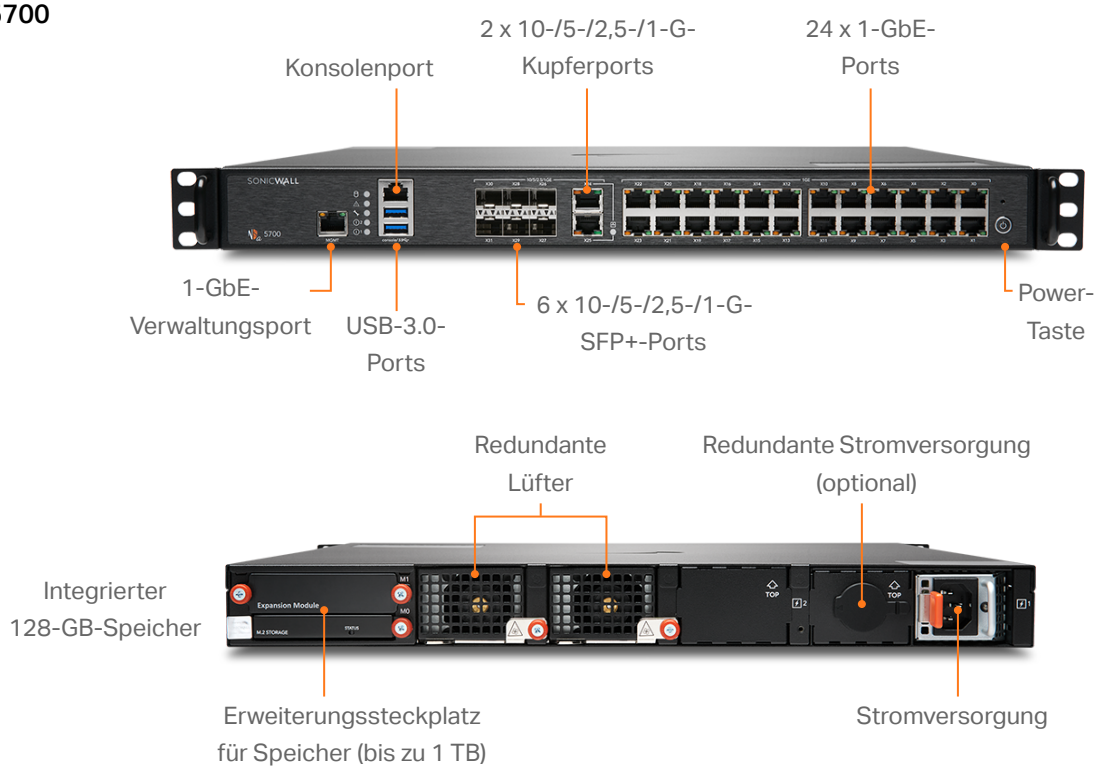




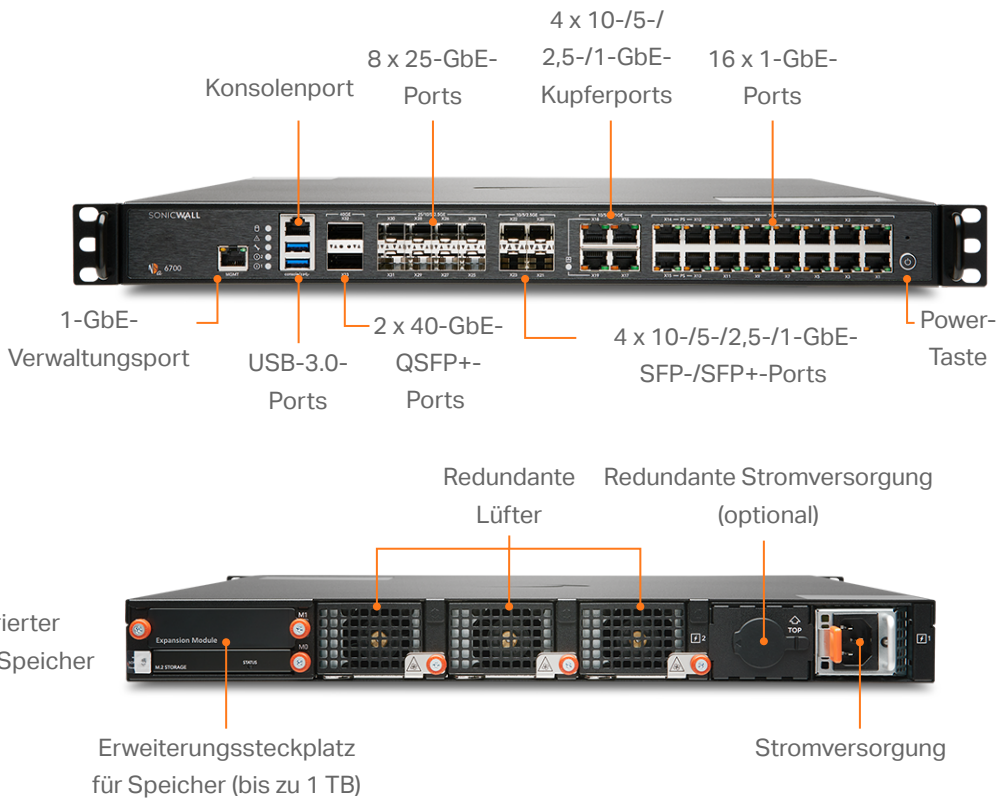
NS*a* 4700

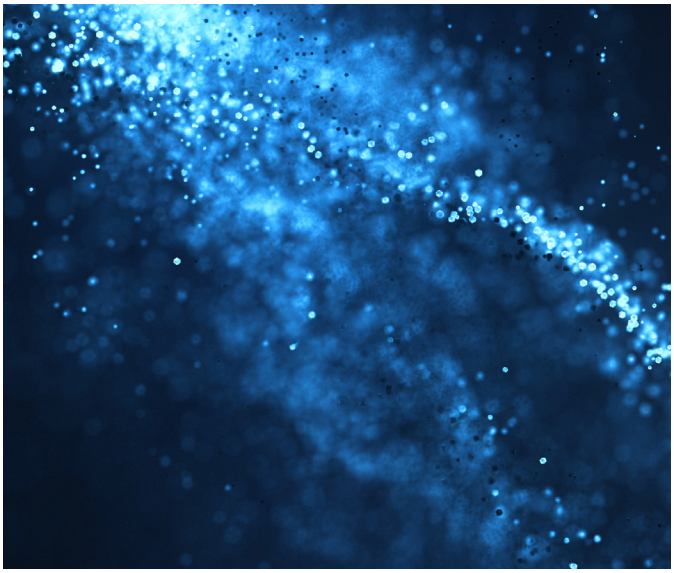


NS*a* 5700



NS*a* 6700





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

Gen 7 NS*a* Series – technische Daten

Firewall	NS*a* 2700	NS*a* 3700	NS*a* 4700	NS*a* 5700	NS*a* 6700
Betriebssystem	SonicOS 7				
Schnittstellen	16 x 1-GbE, 3 x 10-G-SFP+, 2 USB 3.0, 1 Konsole, 1 Verwaltungsport	24 x 1-GbE, 6 x 10-G-SFP+, 4 x 5-G-SFP+, 2 USB 3.0, 1 Konsole, 1 Verwaltungsport	6 x 10-/5-/2,5-/1-G-SFP+; 24 x 1-GbE-Kupferport 2 USB 3.0, 1 Konsole, 1 Verwaltungsport	6 x 10-/5-/2,5-/1-G-SFP+; 2 x 10-/5-/2,5-/1-G (Kupfer); 24 x 1-GbE-Kupferport 2 USB 3.0, 1 Konsole, 1 Verwaltungsport	2 x 40-G; 8 x 25-G, 4 x 10-/5-/2,5-/1-G-SFP+, 4 x 10-/5-/2,5-/1-G (Kupfer); 16 x 1-GbE (Kupfer) 2 USB 3.0, 1 Konsole, 1 Verwaltungsport
Speicher	64 GB M.2	128 GB M.2	128 GB	128 GB	256 GB M.2
Erweiterung	Erweiterungssteckplatz für Speicher (bis zu 256 GB)	Erweiterungssteckplatz für Speicher (bis zu 256 GB)	Erweiterungssteckplatz für Speicher (bis zu 1 TB)	Erweiterungssteckplatz für Speicher (bis zu 1 TB)	Erweiterungssteckplatz für Speicher (bis zu 1 TB)
Logische VLAN- und Tunnel-Schnittstellen (max.)	256	256	512	512	512
SSO-Benutzer	40000	40000	50000	50000	70000
Unterstützte Access-Points (max.)	512	512	512	512	512
Firewall-/VPN-Performance					
Firewall-Inspection-Durchsatz[1]	5,2 GBit/s	5,5 GBit/s	18 GBit/s	28 GBit/s	36 GBit/s
Threat-Prevention-Durchsatz[2]	3,0 GBit/s	3,5 GBit/s	9,5 GBit/s	15 GBit/s	19 GBit/s
Application-Inspection-Durchsatz[2]	3,6 GBit/s	4,2 GBit/s	11 GBit/s	18 GBit/s	20 GBit/s
IPS-Durchsatz[2]	3,4 GBit/s	3,8 GBit/s	10 GBit/s	17 GBit/s	20 GBit/s
Anti-Malware-Inspection-Durchsatz[2]	2,9 GBit/s	3,5 GBit/s	9,5 GBit/s	16 GBit/s	18,5 GBit/s
Durchsatz bei TLS-/SSL-Prüfung und -Entschlüsselung (DPI-SSL)[2]	800 MBit/s	850 MBit/s	5 GBit/s	7 GBit/s	9 GBit/s
IPSec-VPN-Durchsatz[3]	2,1 GBit/s	2,2 GBit/s	11 GBit/s	15 GBit/s	19 GBit/s
Verbindungen pro Sekunde	21000	22000	115000	228000	228000
Max. Anzahl von Verbindungen (SPI)	1500000	2000000	4000000	5000000	8000000
Max. Anzahl von DPI-SSL-Verbindungen	125000	150000	350000	350000	750000
Max. Anzahl von Verbindungen (DPI)	500000	750000	2000000	3500000	6000000
VPN					
Site-to-Site-VPN-Tunnel	2000	3000	4000	6000	6000
IPSec-VPN-Clients (max.)	50 (1000)	50 (1000)	500 (3000)	2000 (4000)	2000 (6000)
SSL-VPN-Lizenzen (max.)	2 (500)	2 (500)	2 (1000)	2 (1500)	2 (1500)
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	Windows 10		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	Windows 10 und Linux		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, Android, Kindle Fire, Chrome OS, Windows 10		Apple® iOS, Mac OS X, Google® Android™, Kindle Fire, Chrome, Windows 8.1 (Embedded)		
Sicherheitsservices					
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				

Gen 7 NS*a* Series – technische Daten

Firewall	NS*a* 2700	NS*a* 3700	NS*a* 4700	NS*a* 5700	NS*a* 6700
Comprehensive Anti-Spam Service	unterstützt				
Anwendungsvisualisierung	Ja				
Anwendungskontrolle	Ja				
Capture Advanced Threat Protection	Ja				
Netzwerk					
IP-Adresszuweisung	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)				
Authentifizierung	LDAP (mehrere Domains), XAUTH/RADIUS, TACACS+, SSO, Radius Accounting NTLM, interne Benutzerdatenbank, 2FA, Terminaldienste, Citrix, Common Access Card (CAC)				
Lokale Benutzerdatenbank	1000	1000	2500	2500	3200
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				
FIPS 140-2-Konformität	Ja	Ja	Ausstehend	Ausstehend	Ausstehend
Zertifikate	ICSA Enterprise Firewall, ICSA Antivirus, IPv6/USGv6				
Zertifikate (in Bearbeitung)	Common Criteria NDPP (Firewall mit VPN und IPS)				
Common Access Card (CAC)	unterstützt				
Hochverfügbarkeit	Active/Passive mit Stateful-Synchronisierung				
Hardware					
Formfaktor	Rackfähig (1 HE)				
Lüfter	1	2	2 (auswechselbar)	2 (auswechselbar)	3 (auswechselbar)
Stromversorgung	60 W	90 W	350 W	350 W	350 W
Maximaler Stromverbrauch (W)	21,5	36,3	108,1	128,1	139,2
Redundante Stromversorgung	100–240 VAC, 50–60 Hz				
Gesamtwärmeabgabe	73,32 BTU	123,78 BTU	368,62 BTU	436,82 BTU	474,67 BTU
Abmessungen	43 x 32,5 x 4,5 cm	43 x 32,5 x 4,5 cm	43 x 46,5 x 4,5 cm	43 x 46,5 x 4,5 cm	43 x 46,5 x 4,5 cm
Gewicht	4,0 kg	4,6 kg	7,8 kg	7,8 kg	8,1 kg
WEEE-Gewicht	4,2 kg	4,8 kg	9,6 kg	9,6 kg	9,9 kg
Versandgewicht	6,4 kg	7 kg	13,5 kg	13,5 kg	13,8 kg
Umgebungstemperatur (Betrieb/ Lagerung)	0 bis 40 °C / -40 bis 70 °C				
Luftfeuchtigkeit	5 bis 95 %, nicht kondensierend	5 bis 95 %, nicht kondensierend	0 bis 90 % RH, nicht kondensierend	0 bis 90 % RH, nicht kondensierend	0 bis 90 % RH, nicht kondensierend
Richtlinien					
Modellnummern (Zulassung)	1RK51-109	1RK52-110	1RK53-115	1RK53-116	1RK54-118
Erfüllt folgende Standards/ Normen	FCC Class A, CE (EMC, LVD, RoHS), C-Tick, VCCI Class A, MSIP/KCC Class A, UL, cUL, TÜV/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 Netzwerkbedingungen und aktivierten Diensten variieren.

[2] Der Threat-Prevention-/Gateway-AV-/Anti-Spyware-/IPS-Durchsatz wurde mit Keysight-HTTP-Leistungstesttools nach Branchenstandard gemessen. Die Tests wurden mit mehreren Datenströmen über mehrere Portpaare durchgeführt. Der Threat-Prevention-Durchsatz wurde bei aktiviertem Gateway-AV, Anti-Spyware und IPS sowie aktivierter Anwendungskontrolle gemessen.

[3] Messung des VPN-Durchsatzes bei UDP-Verkehr mit 1.418 Bytes pro Paket und AESGMAC16-256-Verschlüsselung gemäß RFC 2544. Änderungen hinsichtlich technischer Daten, Funktionen und Verfügbarkeit vorbehalten.

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
- Integration in SonicWall-Wi-Fi-6-AP
- SD-WAN-Skalierbarkeit
- SD-WAN-Usability-Assistent[1]
- Skalierbarkeit von Verbindungen (SPI, DPI, DPI-SSL)
- Verbessertes Dashboard[1]
- 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 Sicherheit[1]
- 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 Protection[2]
- Real-Time Deep Memory Inspection
- Cloudbasierte Multi-Engine-Analyse[2]
- Virtualisiertes Sandboxing
- Analyse auf Hypervisor-Ebene
- Umfassende Systemsimulation
- Prüfung unterschiedlichster Dateitypen
- Automatisierte und manuelle Dateiübermittlung
- Laufend aktualisierte Echtzeitinformationen zu Bedrohungen[2]
- Blockieren der Bedrohung bis zur Klärung des Sicherheitsstatus
- Capture Client[2]

Intrusion-Prevention[2]

- Signaturbasierte Scans
- Integration von Network Access Control (NAC) mit Aruba ClearPass
- Automatische Signatur-Updates
- Bidirektionale Prüfung
- Granulare IPS-Regeln
- Geo-IP-Durchsetzung
- Botnet-Filterung mit dynamischer Liste
- Abgleich regulärer Ausdrücke

Anti-Malware[2]

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

Anwendungsidentifizierung[2]

- Anwendungskontrolle
- Bandbreitenverwaltung auf Anwendungsebene
- Erstellung benutzerdefinierter Anwendungssignaturen
- Schutz vor Datenlecks
- Erstellung von Anwendungsberichten über NetFlow/IPFIX
- Umfassende Anwendungssignaturendatenbank

Visualisierung und Analyse des Datenverkehrs

- Benutzeraktivitäten
- Anwendung/Bandbreite/Bedrohung
- Cloudbasierte Analysen

Filterung von HTTP-/HTTPS-Webinhalten[2]

- URL-Filterung
- Proxy-Vermeidung
- Blockieren mithilfe von Schlüsselwörtern
- Reputationsbasierter Content Filtering Service (CFS 5.0)
- DNS-Filterung
- Regelbasierte Filterung (Ein-/Ausschluss)
- Einfügen des HTTP-Headers
- Bandbreitenverwaltung anhand von CFS-Rating-Kategorien
- 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 (SonicWall-Switch)
- 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
- Unterstützung von Common Access Card (CAC)

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 (CS*a*)
- Capture Threat Assessment (CTA) V2.0
- Neues Design oder Template
- Vergleich mit Branchen- bzw. weltweitem Durchschnitt
- Neue UI/UX, intuitives Feature-Layout[1]
- Dashboard
- Geräteinformationen, Anwendungen, Bedrohungen
- Topology View
- Vereinfachte Erstellung und Verwaltung von Richtlinien

Die SonicOS-7.0-Funktionen im Überblick (Fortsetzung)

- Nutzungsstatistiken zu Regeln/Objekten[1]
- Verwendet vs. nicht verwendet
- Aktiv vs. inaktiv
- Globale Suche nach statischen Daten
- Speicherunterstützung[1]

Verwaltung, Überwachung und Unterstützung (Fortsetzung)

- Interne und externe Speicherverwaltung[1]
- WWAN-USB-Kartenunterstützung (5G/LTE/4G/3G)
- Network Security Manager(NSM)-Unterstützung
- Weboberfläche
- Befehlszeilenschnittstelle (CLI)
- Vollautomatische Registrierung und Implementierung
- Einfaches CSC-Reporting[1]
- Unterstützung der mobilen SonicExpress-App
- SNMPv2/v3
- Zentrales Management und Reporting mit dem SonicWall Global Management System (GMS)[2]
- API für Berichte und Analysen
- Protokollierung
- 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- und -Firewall-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 ermöglicht eine stabile, skalierbare und nahtlose Cybersicherheit für eine extrem dezentrale Arbeitswelt, in der jeder remote, mobil und potenziell gefährdet ist. Durch die Identifizierung unbekannter Bedrohungen, moderne Echtzeit-Überwachungsfunktionen und eine herausragende Wirtschaftlichkeit hilft SonicWall großen Unternehmen, Behörden und KMUs weltweit, die Cybersicherheitslücke zu schließen. Weitere Informationen erhalten Sie unter www.sonicwall.de.

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

Datasheet-Gen7-NSa-JK-A4-9961