DATENBLATT

SonicWall-Gen-8-Firewalls der Mittelklasse: NS*a* Series

Erstklassiger Bedrohungsschutz für verteilte Unternehmen und Firmenstandorte

Die neuesten SonicWall-Next-Generation-Firewalls (NGFWs) für das mittlere Segment – Network Security appliance (NS*a*) Series – bieten mittleren und großen Unternehmen eine erstklassige Performance bei der Bedrohungsabwehr und überzeugen mit den niedrigsten Gesamtbetriebskosten ihrer Klasse. Die Firewalls bilden die Grundlage der Sicherheitslösung, die neben Zero-Trust-Funktionen, flexibler Lizenzierung mit optionalen verwalteten Firewall-Services und integrierter Cybergarantie zur Risikominimierung auch ein vereinfachtes zentralisiertes Firewall-Management bietet.

Mit umfassenden Sicherheitsfeatures wie Intrusion-Prevention, VPN, Anwendungskontrolle, Malware-Analyse, URL-Filterung sowie DNS-Sicherheits-, Geo-IP- und Botnet-Services schützen die Gen-8-Firewalls den Netzwerkrand zuverlässig vor hoch entwickelten Bedrohungen, ohne Engpässe zu verursachen.



NS*a* 2800



NS*a* 3800



NS*a* 4800



NS*a* 5800

Überblick über die technischen Daten der Gen 8 NS*a* Series.

Alle technischen Daten anzeigen »

Bis zu 7 GBit/s	Bis zu 30 GBit/s	Bis zu 8 Millionen
Threat-Prevention-Durchsatz	Firewall-Durchsatz	Verbindungen

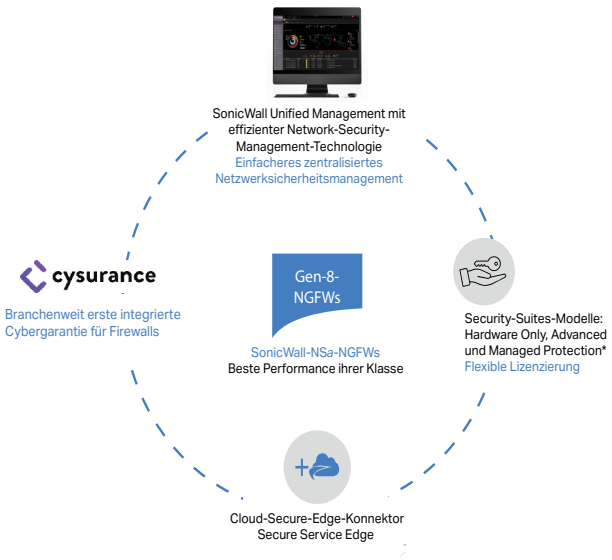
HIGHLIGHTS

- Formfaktor: 1 HE (rackfähig)
- 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)
- Erstklassiges Preis-Leistungs-Verhältnis
- Erweiterbarer Speicher
- Erweiterte DNS-Filterung
- Reputationsbasierter Content Filtering Service (CFS 5.0)
- Vereinfachtes zentralisiertes SaaS- und On-Premises-Management via Network Security Manager
- Wi-Fi-6-Firewall-Management
- Unterstützung für SonicWall Unified Management
- Enterprise-Internet-Edge-fähig
- Sichere SD-WAN-Funktionen
- TLS-1.3-Unterstützung
- Einfachere Lizenzierung einschließlich der Security-Suite-Optionen Hardware Only, Advanced und Managed Protection
- Unterstützt durch das SonicWall-Capture-Labs-Threat-Research-Team
- SonicWall-Switch-, SonicWave-Access-Point- und Capture-Client-Integration
- Unterstützung für Cloud-Secure-Edge-Konnektor
- Integrierte Cysurance-Garantie von bis zu 200.000 USD im Rahmen der Service-Suites

sonicwall.com

SONICWALL®

Die Gen-8-NS*a*-Firewalls bieten eine starke Sicherheit im Rahmen einer umfassenden Lösung, die Bedrohungsschutz, zentrale Verwaltung, Berichte und Analysen, Sicherheits- und verwaltete Serviceoptionen, die Integration von Secure Service Edge (SSE) und eine Cybergarantie umfasst.



Hardware

Mit ihren brandneuen Hardwarekomponenten kommen die Gen-8-Appliances der NS*a* Series selbst bei verschlüsseltem Traffic auf einen Threat-Prevention-Durchsatz von mehreren Gigabit. Die Firewall-Lösungen kommen mit einer hohen Portdichte und sorgen durch Hochverfügbarkeit und zwei Stromversorgungen für eine hohe Netzwerk- und Hardware-Redundanz.

Architektur

Die Gen 8 NS*a* Series läuft auf SonicOS 8, einem neuen Betriebssystem mit einer modernen Benutzeroberfläche, intuitiven Workflows und einem nutzerzentrierten Designansatz. SonicOS 8 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 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 bieten die Appliances die Möglichkeit, Switches und Access-Points über eine einzige Konsole zu verwalten.

Bedrohungsschutz und Sicherheitsservices

Speziell konzipiert, um die hoch entwickelten Cyberangriffe von heute und morgen abzuwehren, erlaubt die Gen 8 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 sowie die patentierten Technologien 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 besonders gut getarnter und gefährlicher Malware einschließlich Zero-Day- und verschlüsselter Bedrohungen.

Um Ihre individuellen Anforderungen zu erfüllen, können Sie zwischen den einfachen Lizenzierungsoptionen Hardware Only, Advanced (APSS) und Managed Protection Security Suite (MPSS) wählen. MPSS ergänzt die vorhandenen Ressourcen um verwaltete Firewall-Services.

Die Integration mit dem Konnektor für Cloud Secure Edge ermöglicht einen sicheren Zugriff auf private Anwendungen hinter den Firewalls. Der Zugriff auf Anwendungen durch Nutzer und Geräte erfolgt nach einem Zero-Trust-Framework.

Cybergarantie

Um den Schaden und die Kosten von Sicherheitsvorfällen zu minimieren, Compliance-Anforderungen zu erfüllen und ein sicheres Gefühl zu vermitteln, kommt Ihre Security-Suite mit einer integrierten Cybergarantie.

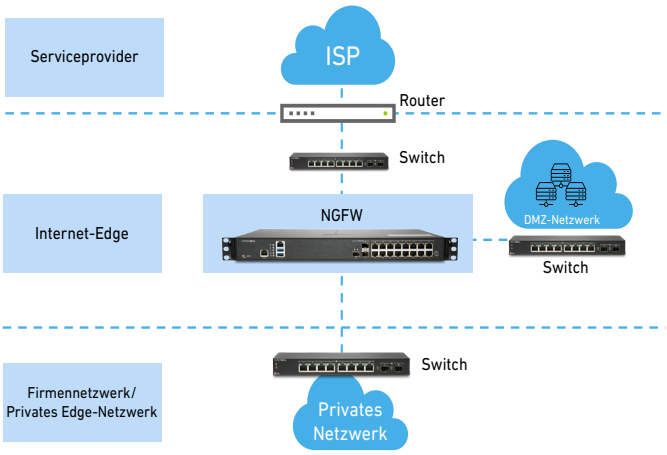
Implementierungsoptionen

Die Gen 8 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 8 NS*a* Series private Netzwerke vor bösartigem Netzwerkverkehr aus dem Internet. Auf diese Weise können Sie:

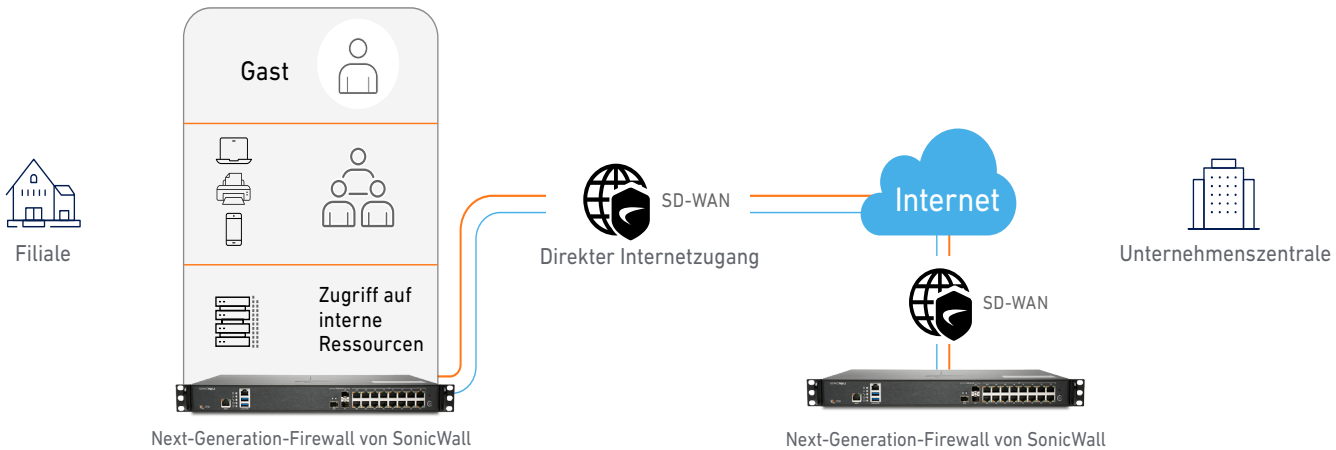
- von einer bewährten NGFW-Lösung mit der höchsten Performance ihrer Klasse profitieren
- umfassende Einblicke gewinnen und den verschlüsselten Verkehr einschließlich TLS 1.3 durchsuchen, um schwer zu fassende Bedrohungen aus dem Internet ohne Abstriche bei der Performance zu blockieren
- Ihr Unternehmen mit integrierten Sicherheitsfunktionen wie Malware-Analyse, Cloud-App-Sicherheit, URL-Filterung und Reputationsdiensten schützen
- Platz und Geld mit einer integrierten NGFW-Lösung einschließlich hoch entwickelter Sicherheits- und Netzwerkfunktionen sparen
- 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 8 NS*a* Series ideal für mittlere und verteilte Unternehmen. Mit dieser Implementierungsoption können Organisationen:

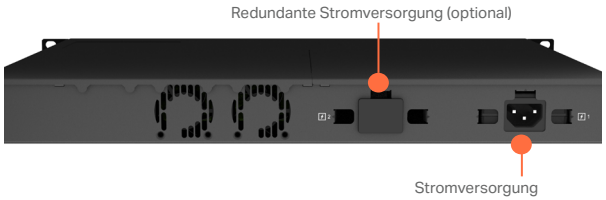
- eine zukunftssichere Lösung für einen umfassenden Schutz in einer dynamischen Bedrohungslandschaft sicherstellen und dabei von einer leistungsstarken Multi-Gigabit-Performance bei der Bedrohungsanalyse profitieren
- ihren Filialen einen direkten und sicheren Internetzugriff bereitstellen, anstatt ein 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



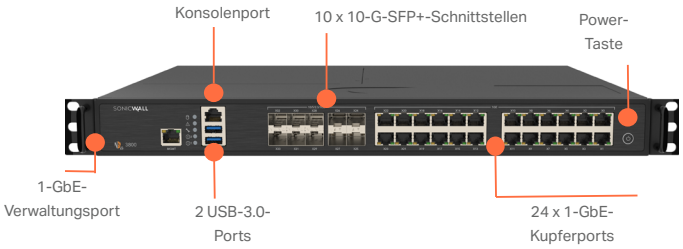
SonicWall Gen 8 NS*a* Series

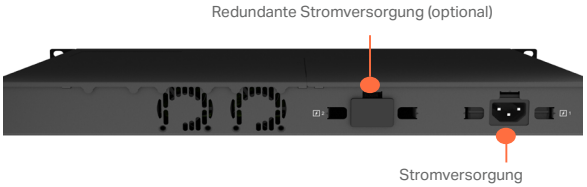
NS*a* 2800



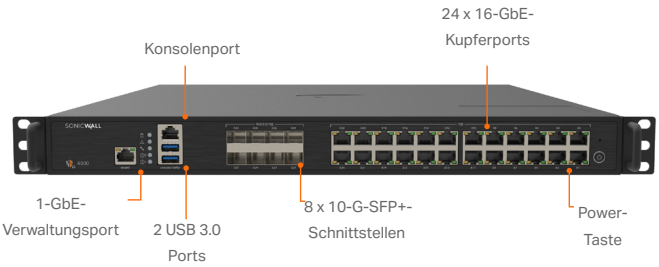


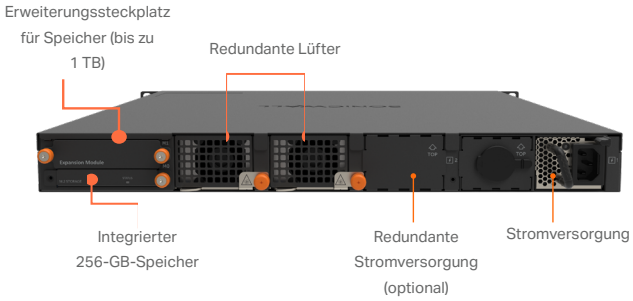
NS*a* 3800



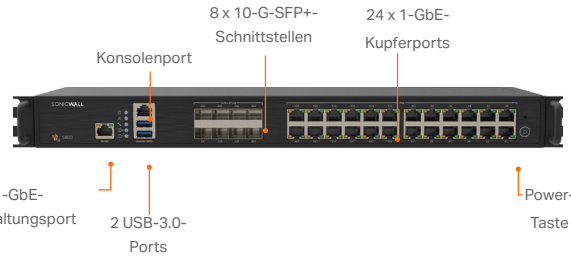


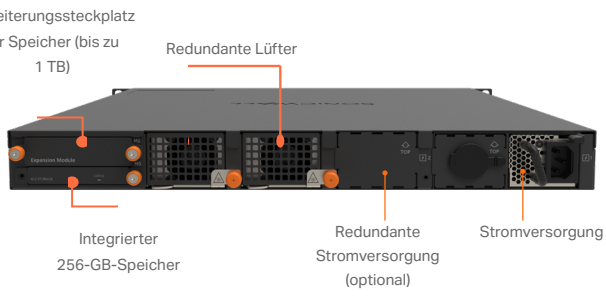
NS*a* 4800





NS*a* 5800





Gen 8 NS*a* Series – technische Daten

Firewall	**NS*a* 2800**	**NS*a* 3800**	**NS*a* 4800**	**NS*a* 5800**
Betriebssystem	SonicOS 8			
Schnittstellen	16 x 1-GbE, 3 x 10-G-SFP+, 2 USB 3.0, 1 Konsole, 1 Verwaltungsport	24 x 1-GbE, 10 x 10-G-SFP+, 2 USB 3.0, 1 Konsole, 1 Verwaltungsport	24 x 1-GbE-Kupferports, 8 x 10-G-SFP+, 1 Konsole (RJ45 zu DB9), 2 USB (Typ A)	24 x 1-GbE-Kupferports, 8 x 10-G-SFP+, 1 Konsole (RJ45 zu DB9), 2 USB (Typ A)
Speicher (Erweiterung)	128 GB (bis zu 512 GB)	256 GB (bis zu 512 GB)	256 GB (bis zu 1 TB)	256 GB (bis zu 1 TB)
Zentralisierte Verwaltung	Network Security Manager (NSM) 3.0 und höher, CLI, SSH, Web-UI, REST-APIs			
Logische VLAN- und Tunnel-Schnittstellen (max.)	256	256	512	512
SAML-Single-Sign-on-Nutzer[1]	40.000	40.000	50.000	50.000
Unterstützte Access-Points (max.)	512	512	512	512
Firewall-/VPN-Performance				
Firewall-Inspection-Durchsatz[2]	8 GBit/s	12 GBit/s	20 GBit/s	30 GBit/s
Threat-Prevention-Durchsatz[3]	6 GBit/s	8 GBit/s	13 GBit/s	24 GBit/s
Application-Inspection-Durchsatz[3]	7 GBit/s	9 GBit/s	13 GBit/s	24 GBit/s
IPS-Durchsatz[2]	7 GBit/s	8 GBit/s	13 GBit/s	24 GBit/s
Anti-Malware-Inspection-Durchsatz[3]	6 GBit/s	8 GBit/s	13 GBit/s	24 GBit/s
Durchsatz bei TLS-/SSL-Prüfung und -Entschlüsselung[3]	1,8 GBit/s	3 GBit/s	4,2 GBit/s	8 GBit/s
IPsec-VPN-Durchsatz[4]	5,5 GBit/s	8 GBit/s	10 GBit/s	21 GBit/s
Verbindungen pro Sekunde	50.000	90.000	140.000	240.000
Max. Anzahl von Verbindungen (SPI)	2.000.000	3.000.000	6.000.000	8.000.000
Max. Anzahl von Verbindungen (DPI)	1.000.000	1.200.000	3.000.000	5.000.000
Max. Anzahl von Verbindungen (TLS)	150.000	300.000	600.000	750.000
VPN und ZTNA				
Site-to-Site-VPN-Tunnel	2.000	3.000	4.000	6.000
IPsec-VPN-Clients (max.)	50 (1.000)	50 (1.000)	500 (3.000)	2.000 (4.000)
SSL-VPN-Lizenzen (max.)	2 (500)	2 (500)	2 (1.000)	2 (1.500)
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 10 und Windows 11			
NetExtender	Microsoft® Windows 10 und Windows 11, Linux			
Mobile Connect	Apple® iOS, Mac OS X, Google® Android™			
SonicWall Private Access auf Basis von Cloud Secure Edge[5]	Im „3 & Free"-Loyalty-Programm enthalten			
Sicherheitsservices				
Deep-Packet-Inspection-Services	Gateway-Anti-Virus, Anti-Spyware, Intrusion-Prevention, TLS-Entschlüsselung			
Content Filtering Service (CFS)	Reputationsbasierte URL-Filterung, Prüfung nach HTTP-URL, HTTPS-IP, Schlüsselwörtern und Inhalt, umfassende Filterung anhand von Dateitypen wie ActiveX, Java, Cookies für Datenschutz, Freigabe- und Sperrlisten			

Gen 8 NS*a* Series – technische Daten

Firewall	**NS*a* 2800**	**NS*a* 3800**	**NS*a* 4800**	**NS*a* 5800**
Comprehensive Anti-Spam Service	●	●	●	●
Anwendungsvisualisierung	●	●	●	●
Anwendungskontrolle	●	●	●	●
Capture Advanced Threat Protection	●	●	●	●
DNS-Filterung	●	●	●	●
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	BGP, 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+, SAML-SSO[1], Radius Accounting NTLM, interne Benutzerdatenbank, 2FA, Terminaldienste, Citrix, Common Access Card (CAC)			
Lokale Benutzerdatenbank	1.000	1.000	1.000	1.000
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	IPv6/USGv6			
Hochverfügbarkeit	Active/Passive mit Stateful-Synchronisierung			
Hardware				
Formfaktor	1 HE (rackfähig)			
Stromversorgung	90 W	150 W	450 W	450 W
Maximaler Stromverbrauch (W)	52,8	102,3	110,4	119,4
Eingangsleistung (AC)	100–240 VAC, 50–60 Hz	100–240 VAC, 50–60 Hz	100–240 VAC, 50–60 Hz	100–240 VAC, 50–60 Hz
Gesamtwärmeabgabe (BTU)	180,01	341	377,4	407,5
Abmessungen (in cm)	43 x 32,5 x 4,5 Versandmaße: 57,5 x 47,5 x 18,5	43 x 32,5 x 4,5 57,5 x 47,5 x 18,5	43 x 46 x 4,5 Versandmaße: 69,5 x 59,5 x 21	43 x 46 x 4,5 Versandmaße: 69,5 x 59,5 x 21
Gewicht	4,6 kg	4,6 kg	7,4 kg	7,4 kg
WEEE-Gewicht	4,8 kg	4,8 kg	9,3 kg	9,3 kg
Versandgewicht	7,2 kg	7,2 kg	13,2 kg	13,2 kg
Umgebungstemperatur (Betrieb/Lagerung)	0 bis +40 °C / -40 bis +70 °C		0 bis +40 °C / -40 bis +70 °C	0 bis +40 °C / -40 bis +70 °C
Luftfeuchtigkeit	5 bis 95 %, nicht kondensierend	5 bis 95 %, nicht kondensierend	5 bis 95 %, nicht kondensierend	5 bis 95 %, nicht kondensierend
Richtlinien				
Erfüllt folgende Standards/Normen (NS*a* 2800 und 3800)	FCC Klasse A, ICES Klasse A, CE (EMV, LVD, RoHS), UL, cUL, Mexiko: DGN-Mitteilung durch UL, ANATEL, WEEE, REACH, SCIP, RCM, MIC Terminal, VCCI Klasse A, KCC/MSIP, BSMI, MTCTE/TEC, CB			
Erfüllt folgende Standards/Normen (NS*a* 4800 und 5800)	FCC Klasse A, ICES Klasse A, CE (EMV, LVD, RoHS), UL, cUL, Mexiko: DGN-Mitteilung durch UL, ANATEL, WEEE, REACH, SCIP, RCM, VCCI Klasse A, KCC/MSIP, BSMI, MTCTE/TEC, CB			
Modellnummern (Zulassung)	1RK56-11C	1RK57-122	IRK58-123	1RK58-123

[1] SAML-Single-Sign-on ist für das demnächst erscheinende SonicOS-8.1-Release verfügbar.

[2] Testmethoden: Die maximale Firewall-Leistung wurde auf Basis von RFC 2544 getestet. Die tatsächliche Leistung kann je nach Netzwerkbedingungen und aktivierten Diensten variieren.

[3] 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.

[4] 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.

[5] Im 3-Jahres-Bundle inbegriffen.

Die SonicOS-8-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 mit SonicWall-Wi-Fi-6-AP
- SD-WAN-Skalierbarkeit
- SD-WAN-Usability-Assistent
- Skalierbarkeit von Verbindungen (SPI, DPI, TLS)

Verbessertes Dashboard

- 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
- Deep Packet Inspection für TLS/SSL/SSH
- Ein-/Ausschluss von Objekten, Gruppen oder Hostnamen
- SSL-Steuerung
- Verbesserungen für TLS mit CFS
- Granulare DPI-SSL-Steuerung nach Zone oder Regel

Capture Advanced Threat Protection[1]

- Real-Time Deep Memory Inspection
- Cloudbasierte Multi-Engine-Analyse[1]
- Virtualisiertes Sandboxing
- Analyse auf Hypervisor-Ebene
- Umfassende Systemsimulation
- Prüfung unterschiedlichster Dateitypen
- Automatisierte und manuelle Dateiübermittlung
- Laufend aktualisierte Echtzeitinformationen zu Bedrohungen[1]
- Blockieren der Bedrohung bis zur Klärung des Sicherheitsstatus
- Capture Client[2]

Intrusion-Prevention[1]

- Signaturbasierte Scans
- Integration der Netzwerkzugriffskontrolle mit Aruba ClearPass
- Automatische Signatur-Updates
- Bidirektionale Prüfung
- Granulare IPS-Regeln
- Geo-IP-Durchsetzung
- Botnet-Filterung mit dynamischer Liste
- Abgleich regulärer Ausdrücke

Anti-Malware[1]

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

Anwendungsidentifizierung[1]

- 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 Webinhalten[1]

- 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 und ZTNA

- 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 und Android
- Routenbasiertes VPN (OSPF, RIP, BGP)
- Secure Private Access auf Basis von Cloud Secure Edge

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
- Dashboard
- Geräteinformationen, Anwendungen, Bedrohungen
- Topology View
- Vereinfachte Erstellung und Verwaltung von Richtlinien
- Nutzungsstatistiken zu Regeln/Objekten
- Verwendet vs. nicht verwendet
- Aktiv vs. inaktiv
- Globale Suche nach statischen Daten
- Speicherunterstützung

Die SonicOS-8.0-Funktionen im Überblick (Fortsetzung)

Verwaltung, Überwachung und Unterstützung (Fortsetzung)

- Interne und externe Speicherverwaltung
- WWAN-USB-Kartenunterstützung (5G/LTE/4G/3G)
- Unterstützung von Network Security Manager (NSM)
- SonicWall Unified Management und SonicWall AI for Monitoring and Insight (SAMI)
- Weboberfläche
- Befehlszeilenschnittstelle (CLI)
- Vollautomatische Registrierung und Implementierung
- Einfaches CSC-Reporting
- Unterstützung der mobilen SonicExpress-App
- SNMP V2/V3
- 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] Erfordert ein Security-Suite-Abo.

Erfahren Sie mehr über die SonicWall Gen 8 NS*a* Series

www.sonicwall.com/products/firewalls

SonicWall Inc.

1033 McCarthy Boulevard | Milpitas, Kalifornien 95035, USA | Weitere Informationen erhalten Sie auf unserer Website.

© 2025 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 Tochtergesellschaften von SonicWall Inc. übernehmen keinerlei Verpflichtung, die in diesem Dokument enthaltenen Informationen zu aktualisieren.