

SonicWall Gen 7 NSsp Series

Dank ihrer hohen Portdichte sowie Schnittstellen mit Multi-Gigabit-Geschwindigkeit können die Next-Generation-Firewalls der SonicWall Network Security services platform™ (NSsp) mehrere Millionen Verbindungen auf Zero-Day und andere raffinierte Bedrohungen prüfen. Für große Unternehmen, Hochschuleinrichtungen, Behörden und MSSPs konzipiert, sind diese Firewalls in der Lage, Angriffe in Echtzeit und ohne Abstriche bei der Performance abzuwehren. Sie zeichnen sich durch eine hohe Zuverlässigkeit aus und ermöglichen Organisationen einen unterbrechungsfreien Netzwerkbetrieb.

HIGHLIGHTS

SonicWall NSsp Series

- Hohe Portdichte
- 100-GbE-Ports
- Integration mit lokalen und cloudbasierten Sandboxes
- Verwaltung über eine einzige Konsole
- Threat-Prevention-Durchsatz von > 80 GBit/s
- Redundante Stromversorgung
- Firewall-Inspection-Durchsatz von bis zu 100 GBit/s
- TLS-1.3-Unterstützung
- Unterstützung mehrerer Millionen gleichzeitiger TLS-Verbindungen
- Niedrige Gesamtbetriebskosten



Überblick über die technischen Daten der NSsp Series.
[Alle technischen Daten anzeigen »](#)

100-GbE

Ports

Bis zu 100 GBit/s

Firewall-Inspection-Durchsatz

80 Mio.

Max. Anzahl von Verbindungen (NSsp 15700)

Erfahren Sie mehr über die
SonicWall Gen 7 NSsp Series:

sonicwall.com/NSsp

Firewalls der Enterprise-Klasse

In wachsenden Unternehmen steigt auch die Zahl verwalteter und unverwalteter Geräte, Netzwerke, Cloud-Workloads, SaaS-Anwendungen, Nutzer, Internetgeschwindigkeiten und verschlüsselter Verbindungen. Wenn eine Firewall diese Entwicklung nicht unterstützt, wird sie schnell zum Problem. Dabei sollte eine Firewall vor allem zur Stabilität beitragen und nicht zu einer Schwachstelle werden.

Die SonicWall NSsp-Firewalls verfügen über mehrere 100-/40-/25-/10-G-Schnittstellen, sodass Sie einige Millionen verschlüsselte und unverschlüsselte gleichzeitige Verbindungen mithilfe überragender Threat-Prevention-Technologie verarbeiten können. Weil mehr als 70 Prozent aller Sitzungen heute verschlüsselt sind, ist es für die Produktivität und Informationssicherheit extrem wichtig,

eine Firewall zu haben, die diesen Datenverkehr ohne Beeinträchtigung der Benutzererfahrung verarbeiten und prüfen kann.

Mit dem Unified-Policy-Konzept der NSsp können Organisationen einfach und intuitiv Zugriffs- und Sicherheitsrichtlinien über eine einzige Oberfläche erstellen.

Vereinfachtes Management und Reporting

Der SonicWall Network Security Manager ermöglicht eine kontinuierliche Verwaltung und Überwachung der Netzwerkaktivitäten sowie das zugehörige Reporting. Über ein intuitives Dashboard lassen sich Firewall-Prozesse zentral verwalten und historische Berichte bereitstellen. Dank der einfachen Implementierung, Einrichtung und Verwaltung können Organisationen ihre Gesamtbetriebskosten senken und von einem schnellen ROI profitieren.

Implementierung

Next-Generation-Firewall (NGFW)

- Verwaltung über eine zentrale Konsole
- NSsp Series ist fest in den Rest des SonicWall-Lösungsökosystems integriert
- Ein umfassender Einblick in die Aktivitäten von Anwendungen, Geräten und Benutzern im Netzwerk ermöglicht es, angemessene Richtlinien umzusetzen sowie Bedrohungen und Bandbreiten-Engpässe zu beseitigen
- Integration mit Capture ATP mit RTDMI für cloudbasiertes Sandboxing oder Capture Security Appliance für lokale Malware-Erkennung

Deep Packet Inspection-Prüfung des SSL-/TLS-Verkehrs (DPI-SSL) zur Erkennung verborgener Bedrohungen

- Die NSsp prüft mehrere Millionen gleichzeitige TLS-/SSL- und SSH-verschlüsselte Verbindungen unabhängig von Port oder Protokoll
- Ein- und Ausschlussregeln ermöglichen eine Personalisierung basierend auf bestimmten unternehmensspezifischen Compliance-Anforderungen und/oder rechtlichen Vorgaben
- Unterstützung von TLS-Cipher-Suites bis hin zu TLS 1.3

Netzwerk und Segmentierung

- Betrieb über mehrere segmentierte Netzwerke, Clouds oder Servicedefinitionen hinweg; mit eindeutigen Templates, Gerätegruppen und Richtlinien für mehrere Geräte und Nutzer

- MSSPs können zudem mehrere Kunden mit einer Clean Pipe sowie eindeutigen Richtlinien unterstützen

Multi-Instance-Firewall (nur bei der NSsp 15700)

- Bei Multi-Instance handelt es sich um die nächste Generation von Multi-Tenancy
- Jeder Nutzer wird mit dedizierten Rechenressourcen isoliert, um einen Ressourcenmangel zu vermeiden
- Umfasst physische und logische Ports/Nutzer
- Unterstützung von unabhängigen Benutzerregeln und unabhängigem Konfigurationsmanagement
- Unterstützung von Versionsunabhängigkeit und Hochverfügbarkeit für Nutzer

Wire-Modus-Funktion

- Bypass-Modus für die schnelle und relativ unterbrechungsfreie Einbindung von Firewall-Hardware in ein Netzwerk
- Inspect-Modus zur Erweiterung des Bypass-Modus ohne funktionelle Veränderung des risikoarmen, latenzfreien Paketpfads
- Secure-Modus für die aktive Zwischenschaltung der Multi-Core-Prozessoren der Firewall in den Paketverarbeitungspfad
- Tap-Modus für die Aufnahme eines gespiegelten Paket-Streams über einen einzigen Switch-Port an der Firewall, sodass keine physische Zwischeneinfügung nötig ist

Schutz vor hoch entwickelten Bedrohungen

- SonicWall Capture Advanced Threat Protection™ (ATP) wird von mehr als 150.000 Kunden weltweit in einer Vielzahl von Lösungen eingesetzt und hilft ihnen, über 1.200 neue Malware-Formen pro Tag zu identifizieren und zu stoppen
- Die NSsp Series lässt sich in die Capture Security Appliance integrieren, um unbekannte Bedrohungen mit lokalem Sandboxing auf Basis von Real-Time Deep Memory Inspection™ (RTDMI) zu erkennen und aufzuhalten

Capture Cloud Platform

- Die Capture Cloud Platform von SonicWall bietet kleinen wie großen Organisationen eine cloudbasierte Lösung für Bedrohungsschutz und Netzwerkverwaltung sowie Reporting und Analysen

Content-Filtering-Services

- Die aufgerufenen Websites werden gegen eine umfangreiche Cloud-Datenbank mit Millionen bewerteter URLs, IP-Adressen und Websites abgeglichen
- Erstellung und Anwendung von Regeln, um den Zugriff auf Sites basierend auf der Nutzer- oder Gruppenidentität bzw. nach Tageszeit für über 50 vordefinierte Kategorien zu erlauben oder zu verweigern

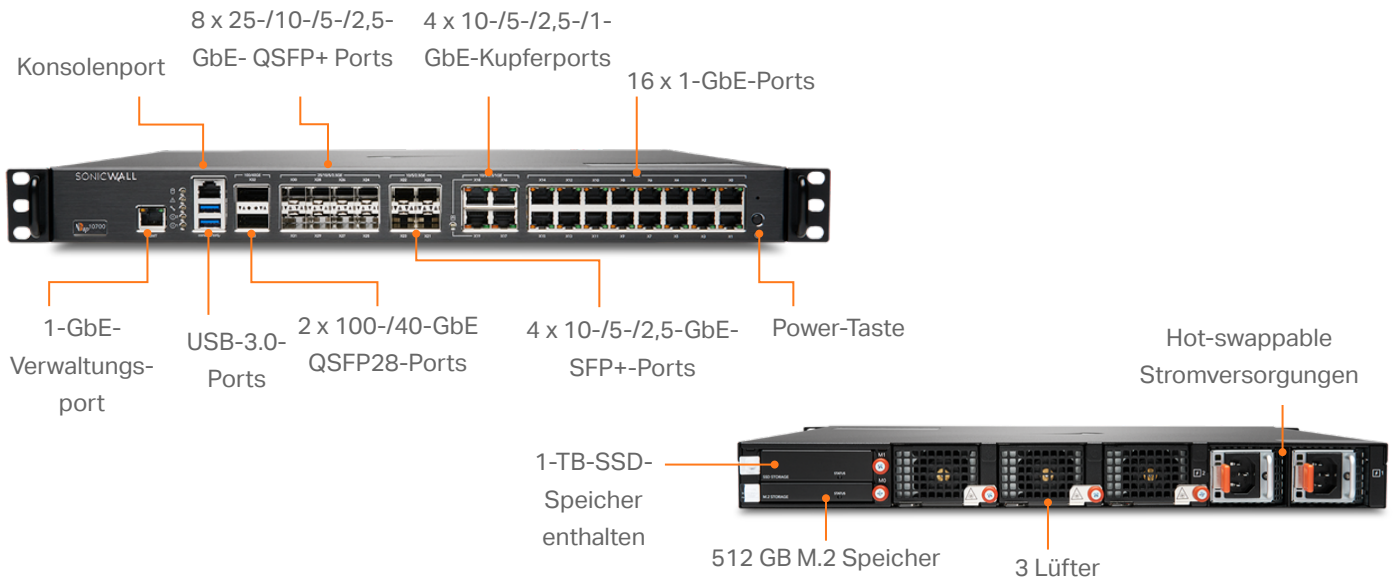
Intrusion-Prevention-System (IPS)

- Konfigurierbare, leistungsstarke Deep Packet Inspection-Engine für einen erweiterten Schutz der wichtigsten Netzwerkdienste wie Web, E-Mail, Dateiübertragung, Windows-Dienste und DNS
- Schutz vor Anwendungsschwachstellen sowie Würmern, Trojanern, Peer-to-Peer-Anwendungen, Spyware und Backdoor-Exploits
- Die flexible Programmierung von Signaturen ermöglicht einen proaktiven Schutz vor neu entdeckten Anwendungs- und Protokollschwachstellen
- Mit SonicWall IPS entfällt dank der branchenführenden Distributed Enforcement Architecture (DEA) von SonicWall die kosten- und zeitaufwendige Pflege und Aktualisierung von Signaturen für neue Attacken

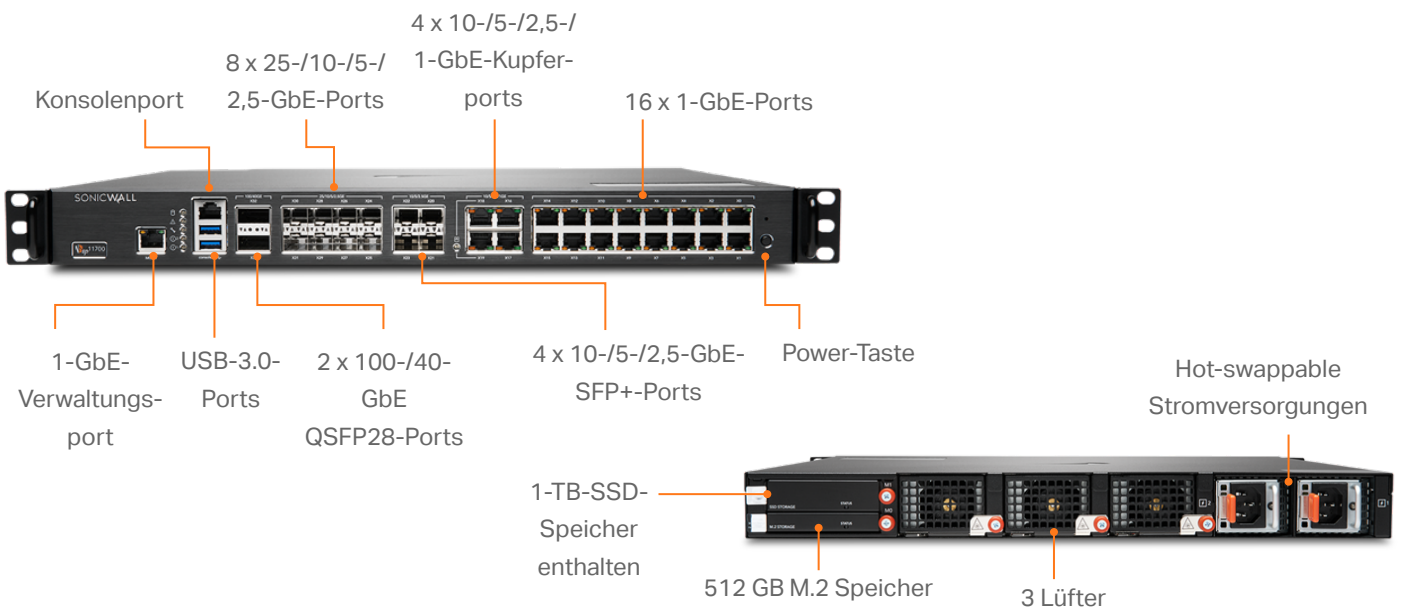
IoT und Anwendungskontrolle

- Die NSsp katalogisiert Tausende von Anwendungen mittels Anwendungskontrolle und überwacht deren Traffic auf ungewöhnliches Verhalten

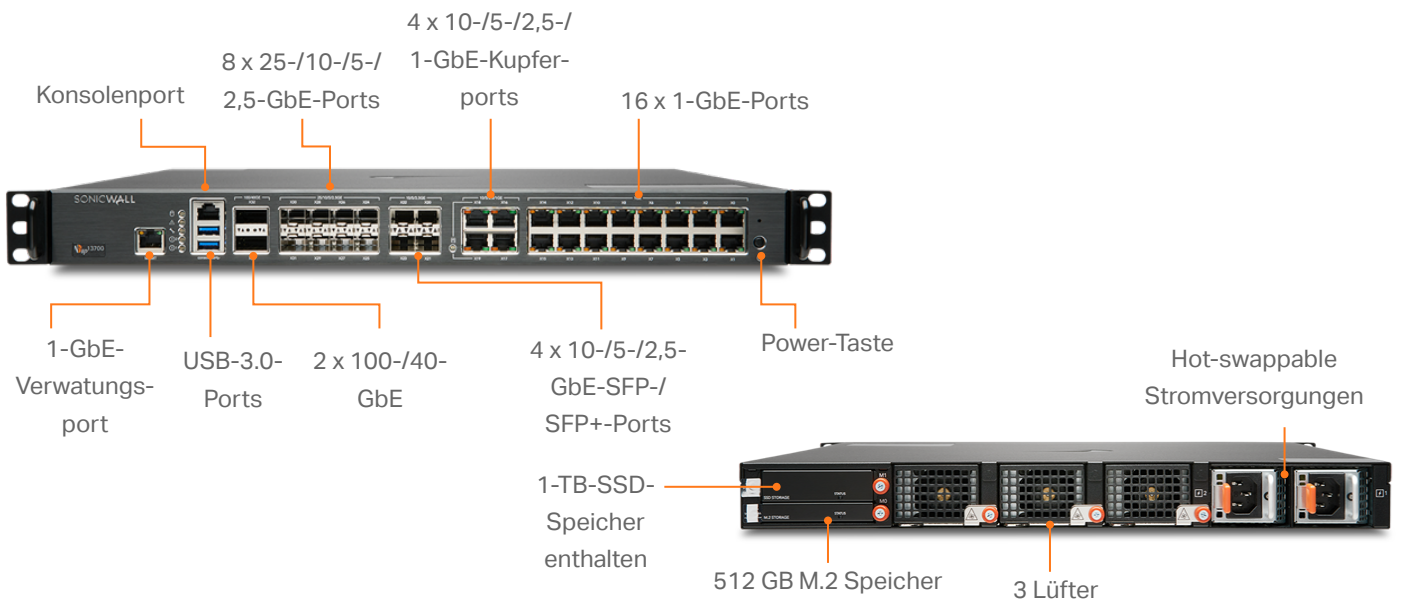
NSsp 10700



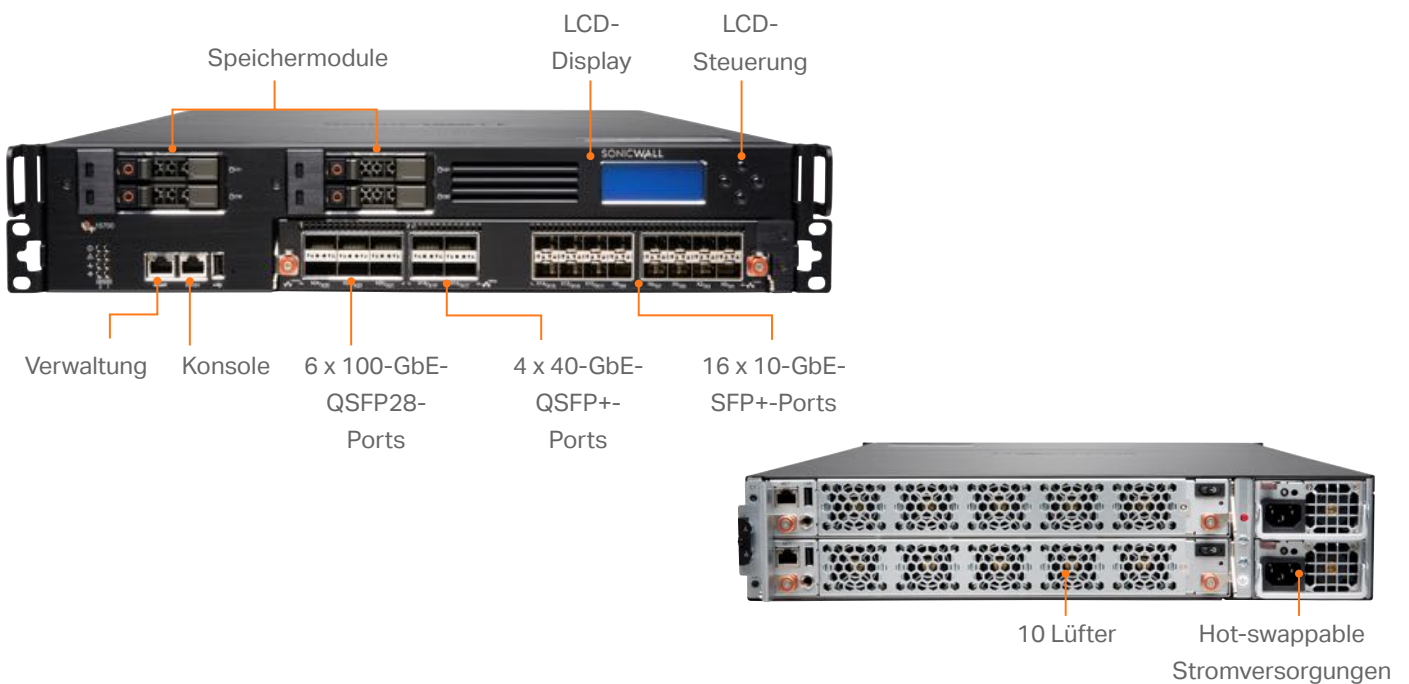
NSsp 11700



NSsp 13700



NSsp 15700



SonicWall NSsp Series – Systemdaten

Firewall allgemein	NSsp 10700	NSsp 11700	NSsp 13700	NSsp 15700
Betriebssystem	SonicOS 7.0.1	SonicOS 7.0.1	SonicOS 7.0.1	SonicOSX 7.0
Schnittstellen	2 x 100-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	2 x 100-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	2 x 100-/40-GbE-QSFP28, 8 x 25-/10-/5-/2,5-GbE- SFP28, 4 x 10-/5-/2,5-GbE-SFP+, 4 x 10-/5-/2,5-/1- GbE-Kupferport, 16 x 1-GbE, 2 USB 3.0, 1 Konsole, 1 Verwaltungsport	6 x 100-GbE-QSFP28, 4 x 40-GbE-QSFP+, 16 x 10-GbE-SFP+
Integrierter Speicher	1,5 TB	1,5 TB	1,5 TB	2 x 480-GB-SSD
Verwaltung	CLI, SSH, Web-UI, REST-APIs			
SSO-Benutzer	100.000			
Logging	Analyser, lokale Logdatei, Syslog, IPFIX, NetFlow			

Firewall-/VPN-Performance	NSsp 10700	NSsp 11700	NSsp 13700	NSsp 15700
Firewall-Inspection-Durchsatz ¹	42	47	60 GBit/s	105 GBit/s
Threat-Prevention-Durchsatz ²	27	35	45,5 GBit/s	82 GBit/s
Application-Inspection-Durchsatz ²	30	44	57 GBit/s	86 GBit/s
IPS-Durchsatz ²	28	37	48 GBit/s	76,5 GBit/s
Durchsatz bei TLS-/SSL-Prüfung und -Entschlüsselung (DPI-SSL) ²	10	11,5	16,5 GBit/s	21 GBit/s
VPN-Durchsatz ³	22,5	26,7	29 GBit/s	32 GBit/s
Verbindungen pro Sekunde	280.000	280.000	280.000	800.000
Max. Anzahl von Verbindungen (SPI)	15.000.000	20.000.000	25.000.000	80.000.000
Max. Anzahl von Verbindungen (DPI)	12.000.000	17.000.000	22.000.000	50.000.000
Max. Anzahl von Verbindungen (DPI-SSL)	1.500.000	1.750.000	2.000.000	3.000.000

VPN	NSsp 10700	NSsp 11700	NSsp 13700	NSsp 15700
Site-to-Site-VPN-Tunnel	6.000	12.000	12.000	25.000
IPSec-VPN-Clients (max.)	2000 (6000)	2000 (6000)	2.000 (6.000)	2.000 (10.000)
SSL-VPN-Lizenzen (max.)	2 (3000)			
Verschlüsselung/Authentifizierung	DES, 3DES, AES (128/192/256 Bit) / MD5, SHA (1.256.384.512) Suite B Cryptography		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			
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)			

Netzwerk	NSsp 10700	NSsp 11700	NSsp 13700	NSsp 15700
Multi-Instance-Firewall	Nicht zutreffend	Nicht zutreffend	Nicht zutreffend	Max. Nutzerzahl pro Hardware: 12
IP-Adressenzuweisung	Statisch (DHCP-, PPPoE-, L2TP- und PPTP-Client), interner DHCP-Server, DHCP-Relay			
NAT-Modi	1:1, many:1, 1:many, flexible NAT (überlappende IP), PAT, transparenter Modus			
VLAN-Schnittstellen	1024			

SonicWall NSsp Series – Systemdaten

Netzwerk	NSsp 10700	NSsp 11700	NSsp 13700	NSsp 15700
Wire-Modus	–	–	–	Ja
Routing-Protokolle	BGP4, OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing	BGP4, OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing	BGP4, OSPF, RIPv1/v2, statische Routen, regelbasiertes Routing	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+, SSO, RADIUS Accounting, NTLM, interne Benutzerdatenbank, 2FA, Terminaldienste, Citrix, Common Access Card (CAC)		LDAP (mehrere Domains), XAUTH/RADIUS, SSO, Novell, interne Benutzerdatenbank, Terminaldienste, Citrix, Common Access Card (CAC)	
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			
Zertifizierungen (Änderungen möglich)	FIPS 140-2 (mit Suite B), UC APL, IPv6 (Phase 2), ICSA Network Firewall, ICSA Anti-Virus, Common Criteria NDPP (Firewall und IPS)		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)	
Hochverfügbarkeit	Active/Passive mit Stateful-Synchronisierung			
Hardware	NSsp 10700	NSsp 11700	NSsp 13700	NSsp 15700
Stromversorgung	2 x 350 W	2 x 350 W	2 x 350 W	2, redundant, 1.200 W
Lüfter	3 (auswechselbar)	3 (auswechselbar)	3 (auswechselbar)	10
Redundante Stromversorgung	100–240 VAC, 50–60 Hz			
Maximaler Stromverbrauch (W)	155,3	155,3	181,2	1135,0
Gesamtwärmeabgabe	529,57 BTU	529,57 BTU	617,89 BTU	3870,35 BTU
Formfaktor	Rackfähig (1 HE)	Rackfähig (1 HE)	Rackfähig (1 HE)	Rackfähig (2 HE)
Abmessungen	43 x 32,5 x 4,5 cm	43 x 32,5 x 4,5 cm	43 x 32,5 x 4,5 cm	68,6 x 43,8 x 8,8 cm
Gewicht	9,1 kg	9,1 kg	9,1 kg	26 kg
WEEE-Gewicht	11 kg	11 kg	11 kg	30,1 kg
Versandgewicht	14,9 kg	14,9 kg	14,9 kg	37,3 kg
Umgebungstemperatur (Betrieb/Lagerung)	0 bis 40 °C / -40 bis 70 °C			
Luftfeuchtigkeit	0 bis 90 % RH, nicht kondensierend	0 bis 90 % RH, nicht kondensierend	0 bis 90 % RH, nicht kondensierend	10 bis 95 %, nicht kondensierend
Richtlinien	NSsp 10700	NSsp 11700	NSsp 13700	NSsp 15700
Modellnummern (Zulassung)	1RK54-118	1RK54-119	1RK54-118	2RK05-0FE
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	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	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	FCC Class A, ICES Class A, CE (EMC Class A, LVD, RoHS), C-Tick, VCCI Class A, MSIP/KCC Class A, UL, cUL, TÜV/GS, CB, Mexico UL DGN Notification, 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 SonicOSX- und SonicOS-Features 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
- REST-APIs
- SonicWall-Switch-Integration

Einheitliche Sicherheitsrichtlinie

- Unified Policy umfasst Regeln für die Schichten 4 bis 7:
 - Quell-/Ziel-IP/Port/Service
 - Anwendungskontrolle
 - CFS/Web-Filtering
 - Durchsetzung von Single-Pass-Sicherheitsservices
 - IPS/GAV/AS/Capture ATP
- Regelmanagement:
 - Cloning
 - Shadow-Rule-Analyse
 - Zelleninterne Bearbeitung
 - Gruppenbearbeitung
- Verwaltung von Ansichten
 - Verwendete/Nicht verwendete Regeln
 - Aktive/Inaktive Regeln
 - Abschnitte

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

- TLS 1.3
- Deep Packet Inspection für TLS/SSL/SSH
- Ein-/Ausschluss von Objekten, Gruppen oder Hostnamen
- SSL-Steuerung
- Granulare DPI-SSL-Steuerung nach Zone oder Regel
- Entschlüsselungsrichtlinien für SSL/TLS und SSH

Capture Advanced Threat Protection¹

- Real-Time Deep Memory Inspection
- Cloubasierte 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-Integration

Intrusion-Prevention¹

- Signaturbasierte Scans
- Automatische Signatur-Updates
- Bidirektionale Prüfung
- Granulare IPS-Regeln
- Geo-IP-Durchsetzung
- Botnet-Filtering mit dynamischer Liste
- Abgleich regulärer Ausdrücke

Anti-Malware¹

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

Anwendungsidentifizierung¹

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

Visualisierung und Analyse des Datenverkehrs

- Benutzeraktivitäten
- Anwendung/Bandbreite/Bedrohung
- Cloubasierte Analysen

Filterung von HTTP-/HTTPS-Webinhalten¹

- URL-Filtering
- Proxy-Vermeidung
- Blockieren mithilfe von Schlüsselwörtern
- Regelbasierte Filterung (Ein-/Ausschluss)
- Einfügen des HTTP-Headers
- Bandbreitenverwaltung anhand von CFS-Rating-Kategorien
- Content Filtering Client

VPN

- 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

- Multi-Instance-Firewall (nur bei der NSsp 15700)
- PortShield
- Jumbo-Frames
- Path MTU Discovery
- Erweiterte Protokollierung
- VLAN-Trunking
- Portspiegelung
- Layer-2-QoS
- Portsicherheit
- Dynamisches Routing (RIP/OSPF/BGP)
- Regelbasiertes Routing (ToS/metrisch und ECMP)
- NAT
- DHCP-Server
- Bandbreitenverwaltung
- Link-Aggregation (statisch und dynamisch)
- Port-Redundanz
- Hochverfügbarkeitsmodus A/P mit State-Sync
- Lastausgleich für ein- und ausgehenden Datenverkehr
- Hochverfügbarkeit – Active/Standby mit State-Sync
- Wire-/Virtual-Wire-, Tap-, NAT-Modus
- Asymmetrisches Routing

VoIP

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

Verwaltung und Überwachung

- Weboberfläche
- Befehlszeilenschnittstelle (CLI)
- Vollautomatische Registrierung und Implementierung
- REST-API

Verwaltung und Überwachung (Fortsetzung)

- Unterstützung der mobilen SonicExpress-App
- SNMPv2/v3
- Zentrales Management und Reporting mit dem SonicWall Network Security Manager (NSM)¹
- Logging
- NetFlow-/IPFIX-Export
- Cloudbasiertes Konfigurationsbackup
- Anwendungs- und Bandbreitenvisualisierung
- IPv4- und IPv6-Verwaltung

¹ Erfordert zusätzliches Abo



Finden Sie die richtige SonicWall-Firewall für Ihr Unternehmen

www.sonicwall.com/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, moderne Echtzeit-Überwachungsfunktionen und eine herausragende Wirtschaftlichkeit hilft SonicWall Unternehmen, Behörden und KMUs weltweit, die Cybersicherheitslücke zu schließen. Besuchen Sie uns auf www.sonicwall.de oder folgen Sie uns auf [Twitter](#), [LinkedIn](#), [Facebook](#) und [Instagram](#), wenn Sie weitere Informationen wünschen.



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 HANDELSÜBLICHEIT, 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.

Datasheet-NSsp-A4-COG-5224

SONICWALL®