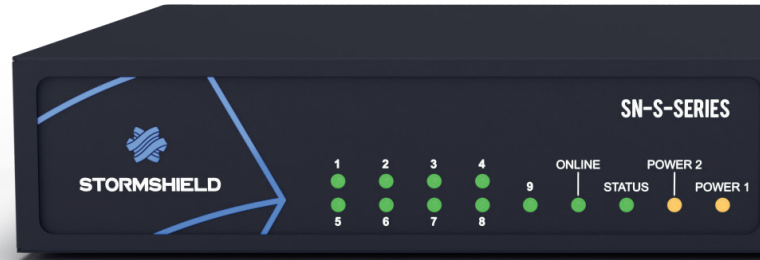




STORMSHIELD

NETWORK SECURITY

STORMSHIELD SN-S-SERIES-320



Hält mit Ihrem Wachstum Schritt

SD-WAN

KONNEKTIVITÄT

8 GBit/s

LEISTUNG FÜR
FIREWALLS

2 GBit/s

LEISTUNG FÜR
IPSEC-VPN

Resilienz

DOPPELTE
STROMVERSORGUNG



Sichere Kommunikation

Mit Glasfaser- (1 GBit) und Kupferverbindungen (2,5 GBit) für mehr Leistung fügt sich die SN-S-Series-320 nahtlos in ihre bestehende Infrastruktur ein und sorgt so für einen reibungslosen Schutz Ihrer Netzwerkverbindungen.



Geschäftskontinuität

- Hohe Verfügbarkeit
- Redundante Stromversorgung*
- LACP



Optimale Zuverlässigkeit

- Sichere Verschlüsselung dank TPM-Chip
- IPsec-VPN und Intrusion-Prevention-System
- Integrierter microSD-Steckplatz



Höhere Leistung

- Verwaltung von WAN- und SD-WAN-Verbindungen
- Firewall Durchsatz von 8 GBit/s
- 1 Glasfaseranschluss (1 GBit) und 8 Kupferanschlüsse (2,5 GBit)

*optional

UTM & FIREWALL
DER NÄCHSTEN GENERATION

KLEINUNTERNEHMEN, AGENTUREN &
REMOTE-STANDORTE

WWW.STORMSHIELD.COM

TECHNISCHE DATEN

LEISTUNG*

Firewall-Durchsatz (UDP 1518 Bytes)	8 GBit/s
IPS-Durchsatz (UDP 1518 Bytes)	4 GBit/s
IPS-Durchsatz (1 MB HTTP)	2 GBit/s
Antivirus-Durchsatz	1 GBit/s

VPN*

IPSec-Durchsatz - AES-GCM	2 GBit/s
Max. Anzahl IPSec-VPN-Tunnel	100
Anzahl der SSL-VPN-Clients im Portalmodus	100
Anzahl der gleichzeitigen SSL-VPN-Clients	100

NETZWERKKONNEKTIVITÄT

Max. Anzahl gleichzeitiger Sitzungen	400.000
Anzahl neuer Sitzungen pro Sek.	25.000
(max.) Anzahl der Hauptgateways/Backup (max.)	64/64

KONNEKTIVITÄT

100/1000/2500-Schnittstellen	8
1-GBit-Schnittstellen, Glasfaser	1 ¹

SYSTEM

Anzahl der Filterregeln (empfohlen/Sonderkonfiguration)	2.048/8.192
Max. Anzahl statischer Routen	512
Max. Anzahl dynamischer Routen	10.000

REDUNDANZ

Hohe Verfügbarkeit (Aktiv/Passiv)	✓
Redundante Stromversorgung (optional)	Externe

HARDWARE

Speicherung	✓
Protokollpartition	microSD-Karte
TPM-Chip	✓
MTBF bei 25°C (in Jahren)	36,5
Abmessungen	1U - (< 1/2 19 Zoll)
Höhe (mit/ohne Gummifüße) x Breite x Tiefe (mm)	46/42 x 210 x 205
Gewicht	1,664 kg
Stromversorgung (AC)	100–240 V 60–50 Hz 1,3–0,75 A
Verbrauch (max.)	230 V 50 Hz 29 W 0,57 A
Geräuschpegel	Ohne Lüfter
Wärmeableitung (max, BTU/h)	70
Betriebstemperatur	5° bis 40° C (41° bis 104° F)
Relative Luftfeuchtigkeit im Betrieb (nicht kondensierend)	20 % bis 90 % bei 40° C
Lagertemperatur	-30° C bis +65° C (-22° F bis +149° F)
Relative Luftfeuchtigkeit bei der Lagerung (nicht kondensierend)	5 % bis 95 % bei 60° C

ZERTIFIZIERUNGEN

Konformität	CE/FCC/CB
-------------	-----------

Kein Vertragsdokument. Die genannten Funktionen sind in Version 4.x enthalten.

* Die Leistung wurde im Labor sowie unter idealen Bedingungen mittels Version 4.x gemessen.

Die Ergebnisse können je nach Testbedingungen und Softwareversion variieren.

¹ Transceiver erforderlich.

FUNKTIONEN

NUTZUNGSKONTROLLE

Firewall-/IPS-/IDS-Modus – Firewall auf Basis von Benutzerprofilen – Anwendungserkennung und -management – Microsoft Services-Firewall – Industrie-Firewall/IPS/IDS – Industrielle Anwendungskontrolle – Erkennung und Überwachung der Nutzung mobiler Endgeräte – Anwendungsinventarisierung (optional) – Schwachstellenerkundung (optional) – Geolokalisierung (Länder, Kontinente) – Dynamische Gerätereputation – URL-Filterung (integriert oder per Cloud) – Transparente Authentifizierung (SSO Active Directory Agent, SSL, SPNEGO) – Multi-User-Authentifizierung im Cookie-Modus (Citrix-TSE) – Authentifizierung im Gast- oder Sponsoring-Modus, Web-Services.

SCHUTZ VOR BEDROHUNGEN

Erkennung und Abwehr von Eindringlingen – Automatische Erkennung und Überprüfung der Protokollkonformität – Anwendungsinspektion – Schutz vor DoS-Angriffen (Denial of Service) – Schutz vor SQL-Injektionen – Schutz vor Cross-Site-Scripting (XSS) – Schutz vor Web-2.0-Malware – Trojanererkennung – Erkennung interaktiver Verbindungen (Botnet, Command & Control) – Schutz vor Extraktionsverfahren – Erweiterte Fragmentierungsverwaltung – Automatische Quarantäne bei Angriffen – Anti-Spam und Anti-Phishing: Reputationsanalyse, heuristische Engine – Integrierter Virenschutz (HTTP, SMTP, POP3, FTP) – SSL-Entschlüsselung und -Inspektion – VoIP-Schutz (SIP) – Kollaborative Sicherheit: IP-Reputation, in Europa gehostete Sandbox-Cloud (optional).

VERTRAULICHE KOMMUNIKATION

Site-to-Site- oder nomadisches IPSec-VPN – SSL-VPN-Remotenzugriff im Tunnelmodus für verschiedene Betriebssysteme (Windows, Android, iOS, ...) – SSL-VPN-Agent mit automatischer Konfiguration (Windows) – IPSec-VPN-Support für Android/iPhone.

NETZWERK & INTEGRATION

IPv6 – NAT, PAT, transparenter Modus (Bridge)/Router/Hybrid – Dynamisches Routing (RIP, OSPF, BGP) – Verwaltung mehrerer Links (Verteilung, Failover) – Verwaltung interner oder externer mehrstufiger PKI – Multi-Domain-Verzeichnisse (einschließlich internem LDAP) – Expliziter Proxy – Richtlinienbasiertes Routing (PBR) – Servicequalitätverwaltung – DHCP-Client/-Zeitlimit/-Server – NTP-Client – DNS-Cache-Proxy – HTTP-Proxy – LACP-Verwaltung – Spanning-Tree-Verwaltung (RSTP/MSTP) – SD-WAN, Multi-Faktor-Authentifizierung (MFA).

VERWALTUNG

Webbasierte Managementschnittstelle mit Datenschutzmodus (DSGVO-kompatibel) – Objektorientierte Sicherheitsrichtlinie – Kontextspezifische Sicherheitsrichtlinie – Konfigurationsunterstützung in Echtzeit – Nutzungszähler für Firewallregeln – Mehrere Installationsassistenten – Globale/lokale Sicherheitsrichtlinie – Integrierte Tools zur Berichterstellung und Protokollanalyse – Interaktive, anpassbare Berichte – Unterstützung mehrerer UDP-/TCP-/TLS-Syslog-Server – SNMP-Agent v1, v2, v3 – IPFIX – Automatisiertes Konfigurations-Backup – Offene API – Skriptaufzeichnung.