STORMSHIELD

NETWORK SECURITY

VON STORMSHIELD
SN-M-SERIES-520

Mehr Konnektivität für Ihr Unternehmen

SD-WAN	10 GBit/s	2,5 GBit/s	Modularität
KONNEKTIVITÄT	LEISTUNG FÜR FIREWALLS	LEISTUNG FÜR IPSEC-VPN	FÜR NETZWERK UND LEISTUNG

Mühelose Integration

Dank der erweiterten Netzwerkfunktionen und der Netzwerkmodularität passt sich SN-M-Series-520 nahtlos und ohne Beeinträchtigungen an Ihre Infrastruktur an.

Anpassungsfähigkeit und Modularität

- Kupfer- und Glasfaserschnittstellen (1 GbE, 2,5 GbE und 10 GbE) sowie Möglichkeiten zur Erweiterung Ihres Netzwerks
- Redundante Stromversorgung für Servicekontinuität
- Integration in bestehende Telekommunikations-Racks

Optimaler Schutz

- Sichere VPN-Verbindung dank TPM-Chip
- IPsec-VPN und Intrusion-Prevention-System
- Agentenverwaltung

Ausstattung aus einer Hand

- Verwaltung von WAN-Verknüpfungen – SD-WAN
- Hohe Verfügbarkeit
- Interaktive Berichte erleichtern die Risikominimierung.

TECHNISCHE SPEZIFIKATIONEN

LEISTUNG*	
Firewall-Durchsatz (UDP 1518 Bytes)	**10 GBit/s**
IPS-Durchsatz (UDP 1518 Bytes)	**5 GBit/s**
IPS-Durchsatz (1 MB HTTP)	**2,5 GBit/s**
Antivirus-Durchsatz	**1,3 GBit/s**
VPN*	
IPSec-Durchsatz - AES-GCM	**2,5 GBit/s**
Max. Anzahl IPSec-VPN-Tunnel	**1.000**
Anzahl der SSL-VPN-Clients im Portalmodus	**150**
Anzahl der gleichzeitigen SSL-VPN-Clients	**150**
NETZWERKKONNEKTIVITÄT	
Max. Anzahl gleichzeitiger Sitzungen	**600.000**
Anzahl neuer Sitzungen pro Sek.	**30.000**
(max.) Anzahl der Hauptgateways/Backup (max.)	**64/64**
KONNEKTIVITÄT	
2,5-GBit-Schnittstellen, Kupfer	**8-16**
10-GBit-Schnittstellen, Kupfer	**0-4**
1-GBit-Schnittstellen, Glasfaser	**2-10**[1]
10-GBit-Schnittstellen, Glasfaser (Dual speed)	**0-4**[1]
Optionale Netzwerkerweiterungsmodule (8x 1-GBit-Kupfer-Ports – 4x 10-GBit-Kupfer-Ports – 4x 1-GBit-Glasfaser-Ports – 8x 1-GBit-Glasfaser-Ports – 4x 10-GBit-Glasfaser-Ports)	**1**
SYSTEM	
Anzahl der Filterregeln (empfohlen/Sonder- konfiguration)	**4.096/16.384**
Max. Anzahl statischer Routen	**5.120**
Max. Anzahl dynamischer Routen	**10.000**
REDUNDANZ	
Hohe Verfügbarkeit (Aktiv/Passiv)	✔
Redundante Stromversorgung	**Doppelt integriert, nicht hot-swap-fähig**
HARDWARE	
Speicherung	✔
Protokollpartition	**> 200 GBit**
TPM-Chip	✔
MTBF bei 25°C (in Jahren)	**18**
Abmessungen	**1U – 19”**
Höhe x Breite x Tiefe (mm)	**44,45 x 440 x 343**
Gewicht	**4,17 kg**
Stromversorgung (AC)	**100–240 V 60–50 Hz 3–1,5 A**
Verbrauch	**54 W**
Lüfter	**2**
Geräuschpegel	**57 dBA**
Wärmeableitung (max, BTU/h)	**184**
Betriebstemperatur	**0 °C bis 40 °C (32 °F bis 104 °F)**
Relative Luftfeuchtigkeit im Betrieb (nicht kondensierend)	**0 % 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**

FUNKTIONEN

NUTZUNGSKONTROLLE
Firewall-/IPS-/IDS-Modus – Firewall auf Basis von Benutzerprofilen – Anwendungserkennung und -management – MicrosoftServices-Firewall – Industrie-Firewall/IPS/IDS – Industrielle Anwendungskontrolle – Erkennung und Überwachung der Nutzung mobiler Endgeräte – Anwendungsinventarisierung (optional) – Schwachstellenerkundung (optional) – Geolokalisierung (Länder, Kontinente) – Dynamische Geräterepuation – 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 Ausweichtechniken – 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-Remotezugriff 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.

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.*

Version 1.0 – Copyright Stormshield 2023