NETZWERKSICHERHEIT

STORMSHIELD
SN-M-SERIES-920

Business Continuity für komplexe Architekturen

Glasfaser-
KONNEKTIVITÄT

36 GBit/s
LEISTUNG DER FIREWALL

6 GBit/s
LEISTUNG DER IPSEC-VPN

Modularität
KUPFER- UND GLASFASERSCHNITTSTELLEN

Modularität

Die Möglichkeiten zur Netzwerkerweiterung bieten eine sehr hohe Konfigurationsflexibilität. Diese Modularität zwischen Kupfer- und Glasfaserschnittstellen (1 GbE und 10 GbE) sorgt dafür, dass Sie Ihre Infrastruktur schrittweise weiterentwickeln können.

Servicekontinuität

- Hohe Verfügbarkeit
- Redundante Stromversorgung
- Integration in bestehende Netzwerk-Racks

Optimale Leistung

- Das volle Potenzial der SN-M-Series-Plattform
- Firewall-Durchsatz von 36 GBit/s
- Upgraden Sie Ihre SN-M-Series-720 mittels Software zur SN-M-Series-920

Ausstattung aus einer Hand

- Verwaltung von WAN-Verknüpfungen – SDWAN
- IPsec-VPN und Intrusion-Prevention-System
- Interaktive Berichte zur Unterstützung der Risikominimierung

TECHNISCHE SPEZIFIKATIONEN

LEISTUNG*	
Firewall-Durchsatz (UDP 1518 Bytes)	**36 GBit/s**
IPS-Durchsatz (UDP 1518 Bytes)	**16 GBit/s**
IPS-Durchsatz (1 MB HTTP)	**10 GBit/s**
Antivirus-Durchsatz	**3,5 GBit/s**
VPN*	
IPSec-Durchsatz - AES-GCM	**6 GBit/s**
Max. Anzahl IPSec-VPN-Tunnel	**2.000**
Anzahl der SSL-VPN-Clients im Portalmodus	**500**
Anzahl der gleichzeitigen SSL-VPN-Clients	**500**
NETZWERKKONNEKTIVITÄT	
Max. Anzahl gleichzeitiger Sitzungen	**1.500.000**
Anzahl neuer Sitzungen pro Sek.	**80.000**
(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	**0-8**
10-GBit-Schnittstellen, Glasfaser (Dual speed)	**2[1]-6**
Optionale Netzwerkerweiterungsmodule (8x 2,5-GBit-Port, Kupfer – 4x 10-GBit-Port, Kupfer – 8x 1-GBit-Port, Glasfaser – 4x 10-GBit-Port, Glasfaser)	**1**
SYSTEM	
Anzahl der Filterregeln (empfohlen/spezifische Konfiguration)	**8.192/32.768**
Max. Anzahl statischer Routen	**5.120**
Max. Anzahl dynamischer Routen	**10.000**
REDUNDANZ	
Hohe Verfügbarkeit (Aktiv/Passiv)	✔
Redundante Stromversorgung	**Doppelt integriert, nicht hot-swapfähig**
HARDWARE	
Speicherung	✔
Protokollpartition	**> 200 GB**
TPM-chip	✔
MTBF bei 25°C (in Jahren)	**21.5**
Abmessungen	**1U - 19 Zoll**
Höhe x Breite x Tiefe (mm)	**44,45 x 440 x 360**
Gewicht	**4,93 kg (10,86 lbs)**
Stromversorgung (AC)	**100–240 V 60–50 Hz 3-1.5A**
Stromverbrauch (max)	**230 V 50 Hz 93.2W 0.43A**
Lüfter	**3**
Geräuschpegel	**62 dBA**
Wärmeableitung (max, BTU/h)	**340**
Betriebstemperatur	**0° bis 40° C (32° bis 104° F)**
Relative Luftfeuchtigkeit im Betrieb (nicht kondensierend)	**0 % bis 95 % bei 40° C**
Lagertemperatur	**-30° bis 65° C (-22° bis 149° F)**
Relative Luftfeuchtigkeit bei der Lagerung (nicht kondensierend)	**5 % bis 95 % bei 60° C**
ZERTIFIZIERUNGEN	
Konformität	**CE/FCC/RCM/UKCA/CB**

[1] *Transceiver erforderlich*

** Die Leistung wurde im Labor sowie unter idealen Bedingungen mittels Version 4.x gemessen. Die Ergebnisse können je nach Testbedingungen und Softwareversion variieren.*

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-VDI Multi-User-Authentifizierung mit Agent (Citrix-TSE) – Authentifizierung im Gast- oder Sponsoring-Modus, webservices.

SCHUTZ VOR BEDROHUNGEN
Erkennung und Abwehr von Eindringlingen – Automatische Erkennung und Überprüfung der Protokollkonformität – Applikationskontrolle – 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-kontrolle – 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) – Multicast – 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, Multifactor Authentication (MFA).

VERWALTUNG
Webbasierte Managementschnittstelle mit Datenschutzmodus (DSGVO-kompatibel) – Objektorientierte Sicherheitsrichtlinie – Kontextspezifische Sicherheitsrichtlinie – Konfigurationsunterstützung in Echtzeit – Nutzungszähler für Firewallregeln – Sicherheitsaktualisierungen verbunden oder getrennt – 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.