



STORMSHIELD

NETZWERKSICHERHEIT

STORMSHIELD SNI20

Industrie-Firewall



2,4 Gbit/s

LEISTUNG
DER FIREWALL

10 ms

LATENZ
(MAXIMAL)

DPI

INDUSTRIELLE
PROTOKOLLE

NAT

INTEGRATION IN
INDUSTRIENETZWERKE



An Ihre Umgebung angepasste Lösung

Durch die Kombination von einzigartiger und transparenter Netzwerkintegration (Routing und NAT) und modernen Sicherheitsfunktionen lässt sich die SNI20 integrieren, ohne die bestehende Betriebsinfrastruktur ändern zu müssen.



Integration in industrielle Umfelder

- Operationsspielraum (Cluster, Bypass und Stromversorgung)
- Kraftwerke (IEC 61850-3)
- Geeignet für widrige Betriebsumfelder (DIN-Schiene, IP30)
- Optimierte Beschaffungskosten für groß angelegte Einsätze



Sicherheit in Echtzeit

- Sichere Fernwartung Ihrer Maschinen und SPSen (VPN SSL / IPsec)
- Fernsteuerung Ihrer verteilten Prozesse
- Segmentierung nach Zonen ohne Änderung Ihres Systems
- Sichern von Operationen (DPI, IPS, Filterung)

UTM UND FIREWALL
DER NEUEN GENERATION

BETRIEBSSYSTEME MIT STRENGEN
INDUSTRIEANFORDERUNGEN

WWW.STORMSHIELD.COM

TECHNISCHE DATEN

LEISTUNG*

Firewall Übertragungsrate (UDP 1518 Byte)	2,4 Gbit/s
Firewall Übertragungsrate (IMIX**)	1,4 Gbit/s
IPS-Übertragungsrate (UDP 1518 Byte)	1,6 Gbit/s
IPS Übertragungsrate (1 MB Datei HTTP)	900 Mbit
Latenz (max.)	10 ms

VPN*

Übertragungsrate IPSec - AES-GCM	600 Mbit
Max. Anzahl IPSec-VPN-Tunnel	100
Max. Anzahl SSL VPN (im Portalbetrieb)	50
Anzahl gleichzeitiger SSL-VPN-Clients	20

NETZWERKVERBINDUNG

Anzahl gleichzeitiger Sitzungen	500.000
Anzahl neuer Sitzungen/Sek.	20.000
Anzahl zentraler Knotenpunkte (max.)/Backup (max.)	64/64

KONNEKTIVITÄT

Schnittstellen (Kupfer) 10/100/1000	2-4
SFP-Steckplätze (Kupfer/Faser) 1 Gbit/s	0-2
Verwaltung	1 serielle Schnittstelle und 2 USB 3.0

INDUSTRIELLE PROTOKOLLE – DEEP PACKET INSPECTION (DPI)

Protokolle: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BAC-net/IP, PROFINET, IEC 60870-5-104, IEC 61850-3 und IT

REDUNDANZ

Hochverfügbarkeit (aktiv/passiv)	✓
Bypass	Optional

HARDWARE

Speicher	SD-Karte
MTBF bei 25 °C (in Jahren)	35,1
Installation	DIN-Schiene (35 mm breit, Norm EN 50022)
Höhe x Breite x Tiefe (mm)	210 x 60 x 155
Gewicht	1,75 kg (3,86 lbs)
Höhe x Breite x Tiefe, verpackt (mm)	190 x 270 x 235
Verpackungsgewicht	2,46 kg (5,42 lbs)
Redundante Stromversorgung (CC)	2x 12-48 VDC 3-0,75 A
Leistungsaufnahme (Leerlauf) CC bei +25 °C	15
Leistungsaufnahme (Vollast, max.) CC bei 25 °C	19
Lüfter	-
Wärmeableitung (max., BTU/Std.)	64,83
Betriebstemperatur	-40° bis +70 °C (-40° bis +158 °F)
Relative Feuchte in Betrieb (ohne Kondensierung)	0 % bis 95 %
Geräteschutzgrad (IP-Code)	IP30
Lagertemperatur	-40° bis +85 °C (-40° bis +185 °F)
Relative Lagerfeuchte (nicht kondensierend)	0 % bis 95 %

ZERTIFIZIERUNGEN

CE/FCC/CB, EN 61000-6-2, EN 61000-6-4, IEC 61000-4-18, IEC 60068-2, IEC 61850-3, IEEE 1613, EN 50121-4, IEC 60529

FUNKTIONEN

NUTZUNGSKONTROLLE

Modus Firewall/IPS/IDS - Firewall basierend auf der Benutzeridentität - Ermittlung und Management der Anwendungen - Microsoft Services Firewall - Industrie-Firewall/IPS/IDS - Kontrolle der Industrieanwendung - Ermittlung und Kontrolle der Nutzung mobiler Geräte - Bestandsaufnahme der Anwendungen (Option) - Ermittlung von Sicherheitslücken (Option) - Geolokalisierung (Länder, Kontinente) - Dynamische Reputation der Geräte - URL-Filterung (eingebaut oder im Cloud-Modus) - transparente Authentifizierung (Agent SSO Active Directory, SSL, SPNEGO) - Authentifizierung von Mehrfach-Benutzern im Cookie-Modus (Citrix-TSE) - Authentifizierung im Gast- oder Patenschafts-Modus.

SCHUTZ VOR BEDROHUNGEN

Intrusion Prevention und Detection (IDP), Protokollanalyse und Compliance-Verifizierung, Anwendungsinspektion, Denial of Service (DoS)-Schutz, SQL-Injection-Schutz, Cross Site Scripting (XSS)-Schutz, Webcode- und Scripting-Schutz 2.0 Malware (clean and pass), Trojaner-Erkennung, Erkennung interaktiver Verbindungen (Botnet, Command&Control), Schutz vor Datenumgehung, Advanced Fragmentation Management, Automatische Angriffsreaktion (Benachrichtigung, Quarantäne, Blockierung, QoS, Dump), Entschlüsselung und SLL-Inspektion, VoIP-Schutz (SIP), Kollaborative Sicherheit: IP-Reputation.

GEHEIMHALTUNG

IPSEC VPN Standort zu Standort oder mobil, SSL-VPN-Fernzugriff im multi-OS Tunnelmodus (Windows, Android, iOS ...), SSL-VPN Agent mit zentralisierter Konfiguration (Windows), IPSEC-VPN-Support für Android/iPhone.

NETZWERK - INTEGRATION

IPv6 - NAT, PAT, transparente Modi (Bridge)/geführt/hybrid, Dynamisches Routing (RIP, OSPF, BGP), Management mehrfacher Links (Ausbalancierung, Umschaltung), internes oder externes PKI Management auf mehreren Ebenen, Multi-Domain Directories (u. a. internes LDAP), Explicit Proxy, Policy-basiertes Routing (PBR), Management der Servicequalität, Client/Relay/Server DHCP, Client NTP, Proxy Cache DNS, Proxy-Cache HTTP, LACP, Spanning Tree Protocol (STP).

MANAGEMENT

Internet Managementschnittstelle mit privater Navigation (DSGVO-konform), Objektorientierte Sicherheitsrichtlinien, kontextuelle Sicherheitsrichtlinien, Konfigurationshilfe in Echtzeit, Zähler für die Regelnutzung, mehrere Installationsassistenten, globale/lokale Sicherheitsrichtlinien, Integrierte Reporting- und Analysetools der Logs, Interaktive und individuell gestaltbare Berichte, Log-Übertragung an Syslog-Server UDP/TCP/TLS - SNMP Agent V1, V2, V3, IPFIX/NetFlow, automatisches Speichern der Konfigurationen, offene API, Skript-Registrierung.

Vertraglich unverbindliches Dokument. Zitiert werden die Funktionen der Version 4.x.

* Leistungsparameter der Version 4.x wurden im Labor und unter idealen Bedingungen gemessen. Die Ergebnisse können je nach Testbedingungen und Softwareversion schwanken.