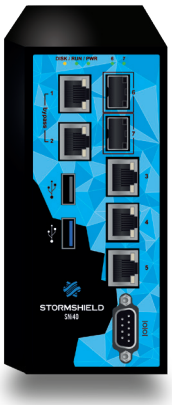
STORMSHIELD

NETZWERKSICHERHEIT

STORMSHIELD **SNi40**

Firewall für die Industrie

4,8 Gbit/s	1,2 Gbit/s	10	5 Ports
FIREWALL-DURCHSATZ	VPN IPSEC-DURCHSATZ	INDUSTRIE-PROTOKOLLE	10/100/1000 SCHNITTSTELLEN



CSPN
INDUSTRIELLE FIREWALL

Ein auf Ihre Umgebung angepasstes Produkt

Erhöhen Sie Ihre Sicherheit mit einer Appliance, die speziell zum Schutz von PLC (Programmierbare Logiksteuerung) entwickelt wurde. Verbessern Sie die Gesamtsicherheit mit einer Vielzahl von Appliances, die sowohl Ihre OT- als auch IT/OT-Konvergenzanforderungen erfüllen.

Schutz ohne Beeinträchtigung

- Sicherheit geht vor - mit Hochverfügbarkeit oder einem Sicherheitsmodus
- Erkennung und Absicherung der wichtigsten Hersteller aus dem Industrieumfeld (Schneider Electric, Siemens, Rockwell...)

Vereinfachte Integration

- Leicht zu installieren durch einen einfachen Setup-Prozess
- Ein einziges Produkt mit einer einzigen integrierten Administration - unabhängig vom Schutzbereich (OT oder IT)

Verwalten Sie Ihre Infrastruktur

- Verfügbare Liste mit den aktiven Geräten in Ihrem Netzwerk
- Echtzeit-Kontrolle von bestehenden Sitzungen

TECHNISCHE DATEN

DURCHSATZ*	
Firewall-Durchsatz (UDP 1518 Byte)	4,8 Gbit/s
Firewall-Durchsatz (IMIX**)	2,9 Gbit/s
IPS-Durchsatz (UDP 1518 Byte)	3,3 Gbit/s
IPS-Durchsatz (1 Mbit HTTP-Dateien)	1,8 Gbit/s
Latenz (max.)	10 ms

VPN*	
IPSec-Durchsatz - AES-GCM	1,2 Gbit/s
Max. Anzahl von VPN-Tunnels IPSec	500
Max. Anzahl von VPN-Clients SSL (Portalmodus)	75
Anzahl von gleichzeitigen VPN-Clients SSL	100

NETZWERK-KONNEKTIVITÄT	
Gleichzeitige Sitzungen	500.000
Neue Sitzungen pro Sekunde	20.000
Anzahl von Haupt-Gateways (max.)/Backup (max.)	64/64

KONNEKTIVITÄT	
Schnittstellen 10/100/1000 Kupfer	5
Steckplätze 1 Gbit/s SFP	0-2
Serieller Port	1
USB-Ports	1 USB 2.0, 1 USB 3.0

PROTOKOLLE - DEEP PACKET INSPECTION (DPI)

Protokolle: Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, SOFBUS / LACBUS, IEC 60870-5-104, IEC 61850 (MMS, Goose und SV), S7+ und IT

REDUNDANZ	
Hohe Verfügbarkeit (Aktiv/Passiv)	✔
Bypass	✔

HARDWARE	
Speicher	32 GB SSD
Log-Partition	>20 GB SSD
MTBF bei 25 °C (Jahre)	26,6
Installation	Rail DIN (Breite 35 mm, Norm EN 50022)
Höhe x Breite x Tiefe (mm)	165 x 80 x 145
Gewicht	1,40 kg
Redundante Stromversorgung (DC)	12-36 VDC 5-1,67 A
Stromaufnahme (W) (Leerlauf) DC bei +25 °C	15,5
Stromverbrauch (W) (volle Leistung, max.) DC bei +25 °C	19,5
Gebläse	-
Wärmeabstrahlung (max., BTU/h)	66,54
Betriebstemperatur	-40 °C bis +75 °C (-40 °F bis 167 °F)
Relative Luftfeuchte im Betrieb (ohne Kondensation)	0 % bis 90 %
Schutzgrad durch das Gehäuse (IP-Code)	IP30
Lagertemperatur	-40 °C bis +85 °C (-40 °F bis +185 °F)
Relative Luftfeuchtigkeit für die Lagerung (ohne Kondensation)	5 % bis 95 %

ZERTIFIZIERUNGEN

CE/FCC, IEC 60950-1, IEC 61000 (3-2, 3-3, 4-18, 6-2, 6-4), IEC 60068 (2-1, 2-2, 2-6, 2-13, 2-14, 2-27, 2-30, 2-78), EN 55024, EN 55032

EIGENSCHAFTEN

NUTZUNGSKONTROLLE

Firewall/IPS/IDS-Modus - Identitätsbasierte Firewall - Anwendungserkennung und -management - Microsoft Services Firewall - Industrielle Firewall/IPS/IDS - Industrielle Anwendungskontrolle - Erkennung und Kontrolle der Nutzung mobiler Endgeräte - Anwendungsinventar (Option) - Erkennung von Sicherheitslücken (Option) - Ortsbestimmung (Länder, Kontinente) - Dynamische Host-Reputation - Transparente Authentifizierung (Active Directory, SSO Agent, SSL, SPNEGO) - VDI Multi-User-Authentifizierung mit Agent (Citrix-TSE) - Gast- und Sponsoring-Modus-Authentifizierung, webservices.

SCHUTZ VOR SICHERHEITSRISIKEN

Intrusionserkennung und -schutz - Autodetektion und Konformitätsprüfung von Protokollen - Anwendungsinspektion - Schutz vor Denial-of-Service-Angriffen (DoS) - Schutz vor Einschleusung von SQL-Injection - Schutz vor Cross Site Scripting (XSS) - Schutz vor schädlichen Web2.0-Code und Skripten (Clean & Pass) - Trojanererkennung - Erkennung interaktiver Dienste (Botnets, Command&Control) - Schutz vor Ausweichtechniken - Schutz vor Protokoll- und Datenmanipulation - Erweitertes Management von Fragmenten - Automatische Reaktion auf Angriffe (Benachrichtigung, Quarantäne, Block, QoS, Dump) - SSL Entschlüsselung und -Inspektion - VoIP-Schutz (SIP) - Kollaborative Sicherheit: IP-Reputation.

VERTRAULICHKEIT

VPN IPSec Site-to-Site oder Nomade - Remotezugriff per VPN SSL im Tunnelmodus für Multi-OS (Windows, Android, IOS etc.) - Agent-VPN SSL mit automatischer Konfiguration (Windows) - VPN IPSec-Unterstützung Android/iPhone.

NETZWERK - INTEGRATION

IPv6, NAT, PAT, Transparentmodus (Bridge)/geroutet/hybrid - Dynamisches Routing (RIP - OSPF - BGP) - Multicast - Mehrfaches Link-Management (Balancing, Failover) - Verwaltung einer internen/externen PKI auf verschiedenen Ebenen, Multi-Domänen-Authentifizierung (Inklusive internem LDAP) - Policy-basiertes Routing (PBR) QuS-Management - DHCP-Client/Relay/Server - NTP-Client, - LACP, Spanning Tree Protocols (RSTP und MSTP), SD-WAN, Multifactor Authentication (MFA).

VERWALTUNG

Web-Management-Schnittstelle - Schnittstelle mit Privatmodus (EU-DSGVO) - objektorientierte Sicherheitspolitik - Kontextbezogene Sicherheitspolitik - Konfigurationsunterstützung in Echtzeit - Nutzungszähler - Sicherheitsaktualisierungen verbunden oder getrennt - Globale/lokale Sicherheitspolitik - Reporting- und Analysetools für eingebettete Protokolle - Interaktive und personalisierbare Berichte - Unterstützung für mehrere Syslog-Server UDP/TCP/TLS - SNMP v1, v2c, v3-Aagent - IPFIX - Automatisches Konfigurations-Backup - Offene API - Skriptaufzeichnung.

Unverbindliches Dokument. Die genannten Funktionen entsprechen denen von Version 4.x.

** Die Leistungsdaten gelten für die Version 4.x und wurden unter idealen Laborbedingungen ermittelt. Die Ergebnisse können je nach Testbedingungen und Programmversion abweichen.*