NETWORK SECURITY

STORMSHIELD SN910

Kontinuität der Dienste für komplexe Netzarchitekturen

Glasfaser
ANSCHLUSSTECHNIK

30 Gbit
LEISTUNGEN FIREWALL

4,5 Gbit
LEISTUNGEN IPSEC

Modularität
SCHNITTSTELLEN KUPFER UND GLASFASER

COMMON CRITERIA

Modularität

Die Möglichkeit zur Netzwerkerweiterung bietet umfangreiche Konfigurierungsfreiheit. Dank der Modularität zwischen den Kupfer- und Glasfaserschnittstellen von 1 GbE bzw. 10 GBbE lassen sich die Entwicklungen Ihrer Infrastrukturen bequem vorausahnen.

Leistungen

- Bestes Preis-Leistungs-Verhältnis für Sicherheit im Datenverkehr der neuen Generation
- Synergieeffekte zwischen Hard- und Software

Garantierte Vertraulichkeit

- IPSEC VPN und Angriffsprävention
- Verwaltung der Zugänge

Kontextualisierte Sicherheitspolitik

- Schutz an Risikograd angepasst,
- Risiken werden pro Arbeitsrechner oder Server identifiziert,
- Interaktive Berichte zur Vereinfachung der Risikominderung

TECHNISCHE DATEN

LEISTUNGEN*	
Firewall Übertragungsrate (UDP 1518 Byte)	30 Gbit
IPS Übertragungsrate (UDP 1518 Byte)	15 Gbit
IPS Übertragungsrate (1 MB HTTP)	10 Gbit
Übertragungsrate Virenschutz	2,9 Gbit

VPN*	
Übertragungsrate IPSec - AES-GCM	4,5 Gbit
Übertragungsrate IPSec - AES256/SHA2	3 Gbit
Max. Anzahl IPSec-VPN-Tunnel	1.000
Anzahl SSL-VPN-Clients im Portalbetrieb	300
Anzahl gleichzeitiger SSL-VPN-Clients	150

NETZWERKVERBINDUNG	
Max. Anzahl gleichzeitiger Sitzungen	1.500.000
Anzahl neuer Sitzungen/Sek.	80.000
Anzahl zentraler Knotenpunkte (max.)/Backup (max.)	64/64

KONNEKTIVITÄT	
Schnittstellen 10/100/1000	8-16
10-GB-Kupfer-Schnittstellen	0-4
1-GB-Glasfaser-Schnittstellen	2[1]-10
10-GB-Glasfaser-Schnittstelle	0-4
Optionale Netzwerk-Erweiterungsmodule (8 Anschlüsse 10/100/1000 - 4 Anschlüsse 10 GB Kupfer - 8 Anschlüsse 1 GB Glasfaser - 4 Anschlüsse 10 GB Glasfaser)	1

SYSTEM	
Anzahl Filterregeln (Empholen / Maximal)	8.192 / 32.768
Max. Anzahl statischer Routen	5.120
Max. Anzahl dynamischer Routen	10.000

REDUNDANZ	
Hohe Verfügbarkeit (Aktiv/Passiv)	✔

HARDWARE	
Speicher	120 Go SSD
MTBF bei 25 °C (in Jahren)	13,2
Größe	1U - 19"
Höhe x Breite x Tiefe (mm)	44,45 x 440 x 310
Gewicht	5,1 kg (11,3 lbs)
Stromversorgung (AC)	100-240 V 60-50 Hz 4-2A
Verbrauch	230 V 50 Hz 72W 0,38A
Lüfter	3
Geräuschpegel	50 dbA
Wärmeableitung (max. BTU/Std.)	334
Betriebstemperatur	5° bis 40 °C (41° bis 104 °F)
Relative Feuchte in Betrieb (ohne Kondensierung)	20% bis 90% bei 40°C
Speichertemperatur	-30° bis 65 °C (-22° bis 149 °F)
Relative Speicherfeuchte (ohne Kondensierung)	5 % bis 95 % bei 60 °C

ZERTIFIZIERUNGEN	
Konformität	CE/FCC/CB

[1] *erfordert Transceiver*

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

FUNKTIONEN

NUTZUNGSKONTROLLE
Modus Firewall/IPS/IDS - Firewall basierend auf der Benutzeridentität - Ermittlung und Management der Anwendungen - Microsoft Services Firewall - Industrielle Firewall/IPS/IDS - Kontrolle der Industrieanwendung - Ermittlung und Kontrolle der Nutzung mobiler Geräte - Bestandsaufnahme der Anwendungen (Option) - Ermittlung von Schwachstellen (Option) - Geolokalisierung (Länder, Kontinente) - Dynamische Reputation der Geräte - URL-Filter (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, webservices.

SCHUTZ VOR BEDROHUNGEN
Angriffserkennung und -prävention - automatische Erkennung und Prüfung der Einhaltung von Protokollen - Anwendungsprüfung - Schutz vor Denial-Of-Service-Angriffen (DoS) - Schutz vor SQL-Injections - Schutz vor Cross Site Scripting (XSS) - Schutz vorschädlichen Web2.0 Codes und Skripten - Ermittlung von Trojanern - Ermittlung interaktiver Verbindungen (Botnet, Command&Control) - Schutz vor Data Evasion - Erweitertes Fragmentierungsmanagement - Automatische Quarantäne bei Angriffen - Antispam und Antiphishing: Analyse nach Reputation, heuristischer Scanner - integrierter Virenschutz (HTTP, SMTP, POP3, FTP), SSL-Entzifferung und Prüfung - VoIP-Schutz (SIP) - kollaborative Sicherheit: IP Reputation, in Europa gehostete Sandbox Cloud (Option).

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

NETZWERK - INTEGRATION
IPv6 - NAT, PAT, transparenter Modus (Bridge)/ geführt/hybrid - Dynamisches Routing (RIP, OSPF, BGP) - Management mehrfacher Links (Verteilung, 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 - HTTP proxy - LACP-Management - Spanning Tree Management (RSTP/ MSTP) - SD-WAN, Multifactor authentication (MFA).

MANAGEMENT
Internet Managementschnittstelle mit privatem Modus (vereinbar mit DSGVO) - Objektorientierte Sicherheitspolitik - kontextuelle Sicherheitspolitik - Konfigurationshilfe in Echtzeit - Zähler für die Nutzung der Firewall-Regeln - mehrere Installationsassistenten - globale/lokale Sicherheitspolitik - Integrierte Reporting- und Analysetools der Logs - Interaktive und individuell gestaltbare Berichte - Unterstützung mehrerer Syslog-Server UDP/TCP/TLS - SNMP Agent V1, V2, V3 - IPFIX - automatisches Speichern der Konfigurationen - offene API - Skript-Registrierung.

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