



# STORMSHIELD

NETWORK SECURITY

# STORMSHIELD SN160



Eine einheitliche Sicherheitslösung

1 Gbit

LEISTUNGEN  
FIREWALL

350 Mbit

LEISTUNGEN  
VPN IPSEC

100 Mbit

LEISTUNGEN  
VIRENSCHUTZ

1 + 4 Anschlüsse

SCHNITTSTELLEN  
10/100/1000



COMMON  
CRITERIA



COMMON  
CRITERIA



EU  
RESTRICTED



NATO  
RESTRICTED



## Die beste einheitliche Sicherheitslösung

Alle wichtigen Sicherheitsfunktionen des Markts für optimalen Schutz: Firewall, Angriffsprävention, Kontrolle von Anwendungen, VPN, Antivirus, Spam-Schutz, Cloud-basierter Web-Filter, Verwaltung von Schwachstellen usw.



## Garantierte Vertraulichkeit

- IPSEC VPN und Angriffsprävention
- Verwaltung der Zugänge



## All-in-one-Ausrüstung

- Firewall für Anwendungen, Angriffsprävention, VPN, Antivirus
- Spam-Schutz, Web-Filter, Verwaltung von Schwachstellen
- Erweitertes Reporting, Nachverfolgung von Benutzern



## Die Konfiguration wird zum Kinderspiel

- Intuitive grafische Benutzeroberfläche,
- Konfigurationsassistent

NEXT GENERATION UTM  
& FIREWALL

KLEINE UNTERNEHMEN, AGENTUREN  
REMOTE-STANDORTE UND  
SELBSTÄNDIGE

[WWW.STORMSHIELD.COM](http://WWW.STORMSHIELD.COM)

# TECHNISCHE DATEN

## LEISTUNGEN\*

Firewall Übertragungsrate (UDP 1518 Byte)	1 Gbit
IPS Übertragungsrate (UDP 1518 Byte)	800 Mbit
IPS Übertragungsrate (1 MB HTTP)	400 Mbit
Übertragungsrate Virenschutz	100 Mbit

## VPN\*

Übertragungsrate IPSec - AES128/SHA1	200 Mbit
Übertragungsrate IPSec - AES256/SHA2	200 Mbit
Max. Anzahl IPSec-VPN-Tunnel	50
Anzahl SSL-VPN-Clients im Portalbetrieb	20
Anzahl gleichzeitiger SSL-VPN-Clients	5

## NETZWERKVERBINDUNG

Max. Anzahl gleichzeitiger Sitzungen	150.000
Anzahl neuer Sitzungen/Sek.	6.000
Anzahl zentraler Knotenpunkte (max.)/Backup (max.)	64/64

## KONNEKTIVITÄT

Schnittstellen 10/100/1000	1 + 4 Anschlüsse (Switch)
----------------------------	---------------------------

## SYSTEM

Max. Anzahl Filterregeln	4.096
Max. Anzahl statischer Routen	512
Max. Anzahl dynamischer Routen	1.000

## REDUNDANZ

Hohe Verfügbarkeit (Aktiv/Passiv)	-
-----------------------------------	---

## HARDWARE

Speicher	Speicherung auf SD-Karte**
MTBF bei 25 °C (in Jahren)	24,9
Größe	1U (<1/2 19")
Höhe x Breite x Tiefe (mm)	45 x 176 x 107
Gewicht	0,55 kg (1,25 lbs)
Höhe x Breite x Tiefe verpackt (mm)	78 x 320 x 200
Verpackungsgewicht	1,2 kg (2,65 lbs)
Stromversorgung (AC)	100-240 V 60-50 Hz 1,5-0,8 A
Verbrauch	230 V 50 Hz 8,4 W 0,07 A
Geräuschpegel	Ohne Lüfter
Wärmeableitung (max. BTU/Std.)	35
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
-------------	-----------

\*Die Leistungen der Version 3.x wurden im Labor und unter idealen Bedingungen gemessen. Die Ergebnisse können je nach Testbedingungen und Softwareversion schwanken.

\*\*optional

# 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.

## 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 - Proxy-Cache HTTP

## 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/NetFlow - automatisches Speichern der Konfigurationen - externe Speicherung (optional) - offene API - Skript-Registrierung.

Vertraglich unverbindliches Dokument. Zitiert werden die Funktionen der Version 3.x.