



STORMSHIELD

NETWORK SECURITY

STORMSHIELD SN-XS-SERIES-170

Jedno zabezpieczenie dopasowane
do wszystkich środowisk

3 Gbps

PRZEPUSTOWOŚĆ
FIREWALL

SD-WAN

POŁĄCZENIE

1 Gbps

PRZEPUSTOWOŚĆ
IPSEC VPN

HA

WYSOKA
DOSTĘPNOŚĆ



Urządzenie typu all-in-one

Urządzenie dostosowujące się do wszystkich potrzeb twojej firmy wymagających solidnego rozwiązania. Oferuje ono zestaw najbardziej kompleksowych funkcji bezpieczeństwa na rynku zapewniając przy tym optymalną ochronę: firewall, IPS, kontrola aplikacji, VPN, antywirus, antyspam, chmurową bazę URL, itd.



Ciągłość działania

- Klaster HA (High availability)
- Redundantne łącze WAN



Poufność

- IPsec VPN, SSL VPN
- System zapobiegania włamaniom (IPS)
- Zarządzanie dostępem



Łatwa integracja

- Tryb transparentny (bridge)/routera
- Dostosowany do wszystkich środowisk (IT/OT)

NEXT GENERATION UTM
& FIREWALL

MAŁE SIECI

WWW.STORMSHIELD.PL

SPECYFIKACJA TECHNICZNA

WYDAJNOŚĆ*

Przepustowość Firewall (1518 bajtów UDP)	3 Gbps
Przepustowość Firewall (IMIX**)	2,5 Gbps
Przepustowość IPS (1518 bajtów UDP)	1 Gbps
Przepustowość IPS (plik HTTP 1MB)	800 Mbps
Przepustowość Antywirus (Threat Prevention)	300 Mbps

VPN*

Przepustowość IPsec - AES-GCM	1 Gbps
Przepustowość IPsec - AES256/SHA2 (IMIX)	740 Mbps
Maks. liczba tuneli IPsec VPN	50
Przepustowość SSL VPN	200 Mbps
Liczba jednoczesnych połączeń klientów SSL VPN	25

POŁĄCZENIA SIECIOWE

Liczba jednoczesnych sesji	150 000
Nowe sesje na sekundę	15 000
Maksymalna liczba bram głównych/zapasowych	64/64

INTERFEJSY SIECIOWE

Interfejsy Ethernet 100/1000/2500	4
-----------------------------------	---

SYSTEM

Maksymalna liczba reguł filtrowania	1 024/2 048
Maksymalna liczba tras statycznych	512
Maksymalna liczba tras dynamicznych	10 000

REDUNDANCJA

Klaster HA (active/passive)	✓
-----------------------------	---

SPRZĘT

Partycja na logi	Opcja karty SD
Układ TPM	✓
MTBF w 25°C (lata)	50,1
Montaż	Szafa rack, szafka, na ścianie lub szynie DIN (szerokość 35mm, standard EN 50022)
Rozmiar	Desktop 1U (<1/2 19")
Wysokość (z/bez nóżek) x szerokość x głębokość (mm)	42/46 x 165 x 139
Waga	1,16 kg (2.56 lbs)
Zasilanie (AC)	100-240V 60-50Hz 1,2A
Zasilanie (DC)	12-48VDC 3-0,75A
Pobór energii elektrycznej (maks. AC)	230V 50Hz 19,9W 0,23A
Pobór energii elektrycznej (maks. DC)	48V 19,1W 0,40A
Poziom głośności	Bez wentylatorów
Rozpraszanie ciepła (maks., BTU/h)	80
Temperatura pracy	-20° to 60°C (-4° to 140°F)
Wilgotność względna, podczas pracy (bez kondensacji)	0% to 95% @60°C (140°F)
Temperatura przechowywania	-40° to 85°C (-40° to 185°F)
Wilgotność względna, przechowywanie (bez kondensacji)	0% to 95% @60°C (140°F)

CERTYFIKACJA

Zgodność	CE/FCC/RCM/UKCA/IEC 61000-4-12/CB/IEC 60068-2/IEC 60529
----------	---

Zdjęcia w dokumencie mają charakter poglądowy.

FUNKCJONALNOŚCI

PEŁNA KONTROLA SIECI

Firewall/IPS/IDS, filtrowanie Microsoft Services, przemysłowy Firewall/IPS/IDS. Wyrwania i kontrola aplikacji. Filtrowanie Microsoft Services. Kontrola aplikacji przemysłowych. Wykrywanie i kontrola wykorzystywanych urządzeń mobilnych. Przegląd używanych w sieci aplikacji (opcja). Wykrywanie podatności (opcja). Filtrowanie oparte o geolokację (kraje, kontynenty). Dynamiczna reputacja hosta. Filtrowanie adresów URL (filtr chmurowy lub wbudowany). Transparentne uwierzytelnianie (Active Directory SSO agent, certyfikaty SSL, SPNEGO). Agentowe uwierzytelnianie wielu użytkowników (CitrixTSE). Wiele metod uwierzytelniania gości. Usługi internetowe. Sprawdzanie hostów zdalnych (ZTNA)

OCHRONA PRZED ZAGROŻENIAMI

Zapobieganie włamaniom, automatyczne wykrywanie i skanowanie protokołów, kontrola aplikacji, ochrona przed atakami Denial of Service (DoS), ochrona przed SQL injection, ochrona przed Cross-Site Scripting (XSS), ochrona przed złośliwym kodem Web2.0 i skryptami, wykrywanie trojanów, wykrywanie interaktywnych połączeń (botnety, Command & Control), zaawansowane zarządzanie fragmentacją, automatyczna kwarantanna w przypadku ataku, antyspam i antyphishing, reputacja na bazie analizy heurystycznej, wbudowane oprogramowanie antywirusowe (HTTP, SMTP, POP3, FTP), deszyfracja i inspekcja ruchu SSL, ochrona VoIP (SIP), wykrywanie podatności w sieci, wykrywanie niezidentyfikowanych dotychczas zagrożeń różnego typu przy wykorzystaniu Sandboxingu w chmurze, którego datacenter są w Europie.

POUFNOŚĆ

Site-to-site lub Client-to-site IPsec VPN, zdalny tunel SSL VPN w trybie Multi-OS (Windows, Android, iOS, itp.), automatycznie konfigurowany klient SSL VPN (Windows), wsparcie dla Android / iPhone IPsec VPN.

SIEĆ - INTEGRACJA

IPv6, NAT, PAT, tryb transparentny (bridge) / router / hybrydowy, dynamiczny routing (RIP, OSPF, BGP), wielopoziomowe wewnętrzne lub zewnętrzne zarządzanie PKI, integracja z wieloma bazami użytkowników (w tym wewnętrzna baza LDAP), policy-based routing (PBR), zarządzanie QoS, DHCP klient / relay / serwer, klient NTP, DNS proxy-cache, HTTP proxy, SD-WAN. Uwierzytelnianie wieloskładnikowe (MFA).

ZARZĄDZANIE

Interfejs webowy, anonimizacja logów, obiektowe zarządzanie politykami, licznik użycia reguł, analizator poprawności reguł, aktualizacje bezpieczeństwa, globalna / lokalna polityka bezpieczeństwa, wbudowane raportowanie i narzędzia do analizy, interaktywne i konfigurowalne raporty, wysyłanie logów do serwera syslog: UDP / TCP/ TLS - SNMP v1, v2, v3 agent - IPFIX/NetFlow - automatyczne tworzenie kopii zapasowych konfiguracji - Open API - nagrywanie skryptów.

Dokument nie jest umową. Wymienione funkcje dotyczą wersji 4.x.

* Test przeprowadzony w warunkach laboratoryjnych dla oprogramowania w wersji 4.x. Wyniki mogą się różnić w zależności od warunków testowych i wersji oprogramowania.

** Rozmiar IP: 60% (48 bajty) - 25% (494 bajty) - 15% (1500 bajtów).