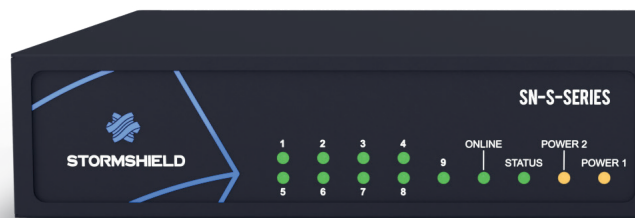




# STORMSHIELD

NETWORK SECURITY

## STORMSHIELD SN-S-SERIES-220



Ewolucja bezpieczeństwa

### SD-WAN

POŁĄCZENIE

### 4 Gbps

PRZEPUSTOWOŚĆ  
IPS I FIREWALL

### 1 Gbps

PRZEPUSTOWOŚĆ  
IPSEC VPN

### Wytrzymałość

PODWÓJNE  
ZASILANIE



### Możliwość dostosowania do Twoich potrzeb

Zaktualizuj swoją platformę, aby dopasować ją do zmian w organizacji, dzięki prostej zmianie licencji. SN-S Series-220 gwarantuje, że możesz być spokojny o odpowiednią wydajność i połączenie.



### Skalowalność

- 1 platforma sprzętowa dla 2 produktów
- Software'owa konwersja do SN-S serii 320
- Konwersja do SN-S serii 320 za pomocą oprogramowania
- Przepustowość zapory 4 Gb/s, skalowalna do 8 Gb/s



### Ciągłości działania

- HA (High availability)
- Redundantne zasilanie\*
- LACP



### Optymalny poziom poufności

- Ochrona z wykorzystaniem układu TPM
- IPsec VPN i zapobieganie włamaniom
- Zintegrowany port microSD



\*opcja

NEXT GENERATION UTM  
& FIREWALL

MAŁE FIRMY, AGENCJE  
I BIURA ZDALNE

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

# SPECYFIKACJA TECHNICZNA

## WYDAJNOŚĆ\*

Przepustowość Firewall (1518 bajtów UDP)	4 Gbps
Przepustowość IPS (1518 bajtów UDP)	2 Gbps
Przepustowość IPS (plik HTTP 1MB)	1 Gbps
Przepustowość Antywirus	500 Mbps

## VPN\*

Przepustowość IPsec - AES-GCM	1 Gbps
Maks. liczba tuneli IPsec VPN	100
Maks. liczba SSL VPN (tryb Portal)	50
Liczba jednoczesnych klientów SSL VPN	50

## POŁĄCZENIA SIECIOWE

Liczba jednoczesnych sesji	300,000
Nowe sesje na sekundę	20,000
Maksymalna liczba dostawców internetu/zapasowych	64/64

## INTERFEJSY SIECIOWE

Interfejsy Ethernet 10/100/1000	8
Interfejsy światłowodowe 1 Gb	1

## SYSTEM

Maksymalna liczba reguł filtrowania	2,048 / 8,192
Maksymalna liczba tras statycznych	512
Maksymalna liczba tras dynamicznych	10,000

## REDUNDANCJA

High availability (active/passive)	✓
Redundantne zasilanie	Zewnętrzne

## SPRZĘT

Dysk lokalny	✓
Partycja na logi	Za pomocą karty microSD
Układ TPM	✓
MTBF w 25°C (lata)	36,5
Wielkość urządzenia	1U - (<1/2 19")
Wysokość (z/bez gumowych nóżek) x Szerokość x Głębokość (mm)	46/42 x 210 x 205
Waga (kg)	1,664
Zasilanie (AC)	100-240V 60-50Hz 1.3-0.75A
Pobór energii elektrycznej (maks.)	230V 50Hz 29 W 0,57A
Poziom głośności	Bez wentylatora
Rozpraszanie ciepła (maks., BTU/h)	70
Temperatura pracy	5° to 40°C (41° to 104°F)
Wilgotność względna, podczas pracy (bez kondensacji)	20% to 90% @ 40°C
Temperatura przechowywania	-30° to 65°C (-22° to 149°F)
Wilgotność względna, przechowywanie (bez kondensacji)	5% to 95% at 60 °C

## CERTYFIKACJA

Zgodność	CE/FCC/CB
----------	-----------

# FUNKCJONALNOŚCI

## KONTROLA WYKORZYSTANIA SIECI

Firewall/IPS/IDS, firewall aplikacyjny, filtrowanie Microsoft Services, przemysłowy Firewall/IPS/IDS 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), uwierzytelnianie wielu użytkowników w trybie cookies (Citrix-TSE) - wiele metod uwierzytelniania gości, usługi internetowe.

## 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 kontrola ruchu SSL, ochrona VoIP (SIP), dostosowanie polityki filtrowania do zdarzeń bezpieczeństwa lub wykrywanie luk w zabezpieczeniach, wykrywanie niezidentyfikowanych dotychczas zagrożeń różnego typu, przy wykorzystaniu Sandboxingu w chmurze, którego datacenter są w Europie (opcja).

## 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), routing oparty na regułach (PBR), zarządzanie QoS, DHCP klient / relay / serwer, klient NTP, DNS proxy, HTTP proxy, HA, redundancja łączy WAN, LACP, wsparcie dla Spanning-tree protocol (RSTP/MSTP), SD-WAN. Uwierzytelnianie wieloskładnikowe (MFA).

## ZARZĄDZANIE

Interfejs webowy, anonimizacja logów, obiektowe zarządzanie politykami, licznik użycia reguł, analizator poprawności reguł, ponad 15 kreatorów konfiguracji, 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, automatyczne tworzenie kopii zapasowych konfiguracji.

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

<sup>†</sup> Wymaga transceiverów

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