



# STORMSHIELD

NETWORK SECURITY

# STORMSHIELD SN210

UTM / Next Generation Firewall dla małych sieci



2 Gbps

PRZEPUSTOWOŚĆ  
FIREWALL

350 Mbps

PRZEPUSTOWOŚĆ  
IPSEC VPN

400 Mbps

PRZEPUSTOWOŚĆ  
ANTYWIRUS

2+6 portów

INTERFEJSY ETHERNET  
10/100/1000



## Wybierz najlepsze narzędzie do kompleksowego zabezpieczenia swojej sieci firmowej

Najbardziej wszechstronne funkcje bezpieczeństwa na rynku: system zapobiegania włamaniom (IPS), firewall, kontrola aplikacji, VPN, audyt podatności, antywirus, antyspam, filtrowanie stron internetowych itp.



### Bezpieczne strefy w Twojej sieci

- Segmentacja sieci: tryb transparentny (bridge) / tryb router'a / tryb hybrydowy
- Odseparowanie podłączonych urządzeń (IoT i BYOD)



### Ciągłości działania

- Redundantne łącza dostępowe
- Optymalizacja przepływu ruchu sieciowego



### Łatwe wdrożenie

- Intuicyjny interfejs graficzny
- Kreator konfiguracji



COMMON  
CRITERIA



COMMON  
CRITERIA



EU  
RESTRICTED



NATO  
RESTRICTED

NEXT GENERATION UTM  
& FIREWALL

MAŁE SIECI

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

# SPECYFIKACJA TECHNICZNA

## WYDAJNOŚĆ\*

Przepustowość Firewall (1518 bajtów UDP)	2 Gbps
Przepustowość IPS (1518 bajtów UDP)	1.6 Gbps
Przepustowość IPS (plik HTTP 1MB)	800 Mbps
Przepustowość Antywirus	400 Mbps

## VPN\*

Przepustowość IPSec - AES-GCM	140 Mbps
Przepustowość IPSec - AES256/SHA2	350 Mbps
Maks. liczba tuneli IPSec VPN	50
Maks. liczba SSL VPN (tryb Portal)	20
Liczba jednoczesnych połączeń klientów SSL VPN	20

## POŁĄCZENIA SIECIOWE

Liczba jednoczesnych sesji	200 000
Nowe sesje na sekundę	15 000
Maksymalna liczba bram głównych/zapasowych	64/64

## INTERFEJSY SIECIOWE

Interfejsy Ethernet 10/100/1000	2+6 switch
---------------------------------	------------

## SYSTEM

Maksymalna liczba reguł filtrowania	4 096
Maksymalna liczba tras statycznych	512
Maksymalna liczba tras dynamicznych	10 000

## REDUNDANCJA

High Availability (Active/Passive)	-
------------------------------------	---

## SPRZĘT

Pamięć lokalna	Karta SD**
Partycja na logi	Tak
MTBF w 25°C (lata)	20.6
Wielkość urządzenia	1U (<1/2 19")
Wysokość x szerokość x głębokość (mm)	46 x 210 x 195
Waga	1 kg (2.2 lbs)
Opakowanie: Wysokość x Szerokość x Głębokość (mm)	90 x 360 x 290
Waga z opakowaniem	2 kg (4.41 lbs)
Zasilanie (AC)	100-240V 60-50Hz 1.3-0.75A
Pobór energii elektrycznej (maks.)	230V 50Hz 1.1W 0.1A
Poziom głośności	chłodzenie pasywne 0 dBA
Rozpraszanie ciepła (maks., BTU/h)	45
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% @ 60°C

## CERTYFIKACJA

Zgodność

CE/FCC/CB

# FUNKCJONALNOŚCI

## PEŁNA KONTROLA SIECI

Firewall/IPS/IDS, 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 kwarentanna w przypadku ataku, antyspam i anty-phishing, reputacja na bazie analizy heurystycznej, wbudowane oprogramowanie antywirusowe (HTTP, SMTP, POP3, FTP), deszyfracja i inspekcja ruchu SSL, ochrona VoIP (SIP), dostosowanie polityki filtrowania do zdarzeń bezpieczeństwa, 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, HA, 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 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.

\*\* Opcjonalnie.