NETWORK SECURITY

# STORMSHIELD SN910

UTM / Next Generation Firewall
dla średnich i dużych sieci

**Interfejsy światłowodowe**
DOSTĘPNOŚĆ INTERFEJSÓW ŚWIATŁOWODOWYCH

**30 Gbps**
PRZEPUSTOWOŚĆ FIREWALL

**4.5 Gbps**
PRZEPUSTOWOŚĆ IPSEC VPN

**Modularność**
INTERFEJSY ETHERNETOWE I ŚWIATŁOWODOWE

COMMON CRITERIA EAL3+ | COMMON CRITERIA EAL4+ | EU RESTRICTED | NATO RESTRICTED

## Modularność

Moduł rozszerzenia sieci oferuje dużą elastyczność w konfiguracji. Możliwość rozbudowy pomiędzy interfejsami miedzianymi i światłowodowymi 1 GbE lub 10GbE pomaga w przewidywaniu zmian w infrastrukturze sieciowej.

### Wysoka wydajność

- Bardzo dobry stosunek wydajności do ceny w celu zabezpieczenia ruchu nowej generacji
- Synergia pomiędzy sprzętem i oprogramowaniem

### Ochrona prywatności

- IPSec VPN i zapobieganie włamaniom
- Zarządzanie dostępem

### Zgodność z obowiązującymi przepisami

- Dostęp do logów i raportów zgodny z RODO
- Wbudowany dysk twardy na logi

# SPECYFIKACJA TECHNICZNA

| | |
|---|---|
| **WYDAJNOŚĆ*** | |
| Przepustowość Firewall (1518 bajtów UDP) | **30 Gbps** |
| Przepustowość IPS (1518 bajtów UDP) | **15 Gbps** |
| Przepustowość IPS (plik HTTP 1MB) | **10 Gbps** |
| Przepustowość Antywirus | **2.9 Gbps** |
| **VPN*** | |
| Przepustowość IPSec - AES-GCM | **4.5 Gbps** |
| Przepustowość IPSec - AES256/SHA2 | **3 Gbps** |
| Maks. liczba tuneli IPSec VPN | **1 000** |
| Maks. liczba SSL VPN (tryb Portal) | **300** |
| Liczba jednoczesnych klientów SSL VPN | **150** |
| **POŁĄCZENIA SIECIOWE** | |
| Liczba jednoczesnych sesji | **1 500 000** |
| Nowe sesje na sekundę | **80 000** |
| Maksymalna liczba dostawców internetu/zapasowych | **64/64** |
| **INTERFEJSY SIECIOWE** | |
| Interfejsy Ethernet 10/100/1000 | **8-16** |
| Interfejsy miedziane 10Gb | **0-4** |
| Interfejsy światłowodowe 1 Gb | **2[1]-10** |
| Interfejsy światłowodowe 10 Gb | **0-4** |
| Opcjonalne moduły rozszerzeń:<br>(8 portów 10/100/1000 - 4 porty 10 Gb miedziane - 8 portów 1Gb światłowodowe - 4 porty 10Gb światłowodowe) | **1** |
| **SYSTEM** | |
| Maksymalna liczba reguł filtrowania | **32 768** |
| Maksymalna liczba tras statycznych | **5 120** |
| Maksymalna liczba tras dynamicznych | **10 000** |
| **REDUNDANCJA** | |
| High Availability (Active/Passive) | ✔ |
| **SPRZĘT** | |
| Dysk lokalny | **120 GB SSD** |
| MTBF w 25°C (lata) | **13.2** |
| Wielkość urządzenia | **1U -19"** |
| Wysokość x szerokość x głębokość (mm) | **44.45 x 440 x 310** |
| Waga | **5.1 kg (11.3 lbs)** |
| Zasilanie (AC) | **100-240V 60-50Hz 4-2A** |
| Pobór energii elektrycznej (maks.) | **230V 50Hz 72W 0.38A** |
| Wentylator | **3** |
| Poziom głośności | **50dbA** |
| Rozpraszanie ciepła (maks., BTU/h) | **334** |
| 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** |

[1] *Wymagane moduły SFP*

# 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.

**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.

**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.

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

*** Opcjonalnie.*