



STORMSHIELD

NETWORK SECURITY

STORMSHIELD SN510

UTM / Next Generation Firewall
dla średnich i dużych sieci



8 Gbps

PRZEPUSTOWOŚĆ
FIREWALL

1.3 Gbps

PRZEPUSTOWOŚĆ
IPSEC VPN

950 Mbps

PRZEPUSTOWOŚĆ
ANTYWIRUS

12 portów

INTERFEJSY ETHERNET
10/100/1000



COMMON
CRITERIA



COMMON
CRITERIA



EU
RESTRICTED



NATO
RESTRICTED



Łatwa i bezproblemowa integracja

Kładąc nacisk na interoperacyjność i wykorzystując zaawansowane funkcje sieciowe, STORMSHIELD jest wyjątkowo łatwy do zintegrowania z istniejącą infrastrukturą.



Najlepsza marka w kategorii UTM i next gen firewall

- Nasi partnerzy są liderami w dziedzinie bezpieczeństwa IT
- Antywirus, antyspam, filtrowanie stron internetowych



Zgodność z przepisami

- Dostęp do logów i raportów jest zgodny z przepisami RODO
- Zbieranie logów
- Przechowywanie logów zgodne z obowiązującymi regulacjami



Bezpieczeństwo urządzeń mobilnych

- SSL VPN zgodny ze wszystkimi systemami operacyjnymi, m.in. Android, Apple, Windows
- Bezpieczny dostęp do wewnętrznych zasobów sieciowych dla urządzeń mobilnych

NEXT GENERATION UTM
& FIREWALL

ŚREDNIE I DUŻE SIECI

WWW.STORMSHIELD.PL

SPECYFIKACJA TECHNICZNA

WYDAJNOŚĆ*

Przepustowość Firewall (1518 bajtów UDP)	8 Gbps
Przepustowość IPS (1518 bajtów UDP)	3.3 Gbps
Przepustowość IPS (plik HTTP 1MB)	1.7 Gbps
Przepustowość Antywirus	950 Mbps

VPN*

Przepustowość IPsec - AES-GCM	1.3 Gbps
Przepustowość IPsec - AES256/SHA2	780 Mbps
Maks. liczba tuneli IPsec VPN	500
Maks. liczba SSL VPN (tryb Portal)	75
Liczba jednoczesnych klientów SSL VPN	100

POŁĄCZENIA SIECIOWE

Liczba jednoczesnych sesji	500 000
Nowe sesje na sekundę	25 000
Maksymalna liczba dostawców internetu/zapasowych	64/64

INTERFEJSY SIECIOWE

Interfejsy Ethernet 10/100/1000	12
---------------------------------	----

SYSTEM

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

REDUNDANCJA

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

SPRZĘT

Dysk lokalny	✓
Partycja na logi	> 200 GB
MTBF w 25°C (lata)	20.1
Wielkość urządzenia	1U - 19"
Wysokość x szerokość x głębokość (mm)	44.45 x 440 x 310
Waga	4.25 kg (9.4 lbs)
Opakowanie: Wysokość x Szerokość x Głębokość (mm)	142 x 590 x 443
Waga z opakowaniem	6.2 kg (13.7 lbs)
Zasilanie (AC)	100-240V 60-50Hz 3-1.5A
Pobór energii elektrycznej (maks.)	230V 50Hz 34W 0.21A
Wentylator	2
Poziom głośności	55dbA
Rozpraszanie ciepła (maks., BTU/h)	130
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

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.