



STORMSHIELD

NETWORK SECURITY

STORMSHIELD SN310

UTM / Next Generation Firewall dla małych sieci



HA

MOŻLIWOŚĆ
BUDOWANIA URZĄDZEŃ
W KLASTRZE HA

4 Gbps

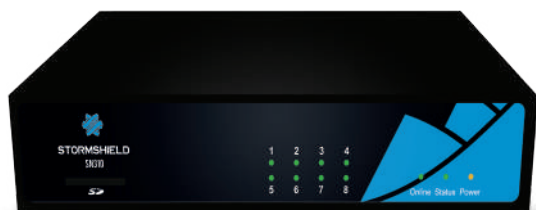
PRZEPUSTOWOŚĆ
FIREWALL

600 Mbps

PRZEPUSTOWOŚĆ
IPSEC VPN

8 portów

INTERFEJSY ETHERNET
10/100/1000



Wysoka dostępność

Dzięki funkcji wysokiej dostępności usługi działają nieprzerwanie, nawet w przypadku awarii urządzenia.



Bezpieczne strefy w Twojej sieci

- Segmentacja sieci: tryb transparentny (mostek) / tryb routera / tryb hybrydowy
- 8 portów dla lepszej elastyczności i szczegółowości przy określaniu polityki filtrowania
- Odseparowanie podłączonych urządzeń (IoT i BYOD)



Ciągłości działania

- Możliwość budowania klastrów HA
- Redundantne łącza dostępowe
- Optymalizacja przepływu ruchu sieciowego



Łatwe wdrożenie

- Intuicyjny interfejs graficzny
- Kreator konfiguracji



COMMON
CRITERIA



COMMON
CRITERIA



EU
RESTRICTED



NATO
OTAN
RESTRICTED

NEXT GENERATION UTM
& FIREWALL

MAŁE SIECI

WWW.STORMSHIELD.PL

SPECYFIKACJA TECHNICZNA

WYDAJNOŚĆ*

Przepustowość Firewall (1518 bajtów UDP)	4 Gbps
Przepustowość IPS (1518 bajtów UDP)	2.4 Gbps
Przepustowość IPS (plik HTTP 1MB)	1.2 Gbps
Przepustowość Antywirus	495 Mbps

VPN*

Przepustowość IPSec - AES-GCM	175 Mbps
Przepustowość IPSec - AES256/SHA2	600 Mbps
Maks. liczba tuneli IPSec VPN	100
Maks. liczba SSL VPN (tryb Portal)	50
Liczba jednoczesnych klientów SSL VPN	20

POŁĄCZENIA SIECIOWE

Liczba jednoczesnych sesji	300 000
Nowe sesje na sekundę	18 000
Maksymalna liczba dostawców internetu/zapasowych	64/64

INTERFEJSY SIECIOWE

Interfejsy Ethernet 10/100/1000	8
---------------------------------	---

SYSTEM

Maksymalna liczba reguł filtrowania	8 192
Maksymalna liczba tras statycznych	512
Maksymalna liczba tras dynamicznych	10 000

REDUNDANCJA

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

SPRZĘT

Dysk lokalny	Karta pamięci SD**
MTBF w 25°C (lata)	25.2
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 15.1W 0.13
Poziom głośności	bez wentylatora (chłodzenie pasywne)
Rozpraszanie ciepła (maks., BTU/h)	65
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, SD-WAN.

ZARZĄDZANIE

Interfejsy 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, pamięć zewnętrzna (wymagana karta SD).

.....
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.