



STORMSHIELD

NETWORK SECURITY

STORMSHIELD SN6100

UTM / Next Generation Firewall dla sieci korporacyjnych i data center



170 Gbps

PRZEPUSTOWOŚĆ
FIREWALL

20 Gbps

PRZEPUSTOWOŚĆ
VPN IPSEC

12.5 Gbps

PRZEPUSTOWOŚĆ
ANTYWIRUS

Modularność

INTERFEJSY ETHERNETOWE
I ŚWIATŁOWODOWE



⚡ Bardzo wysoka wydajność

Dzięki przepustowości nawet do 170 Gb/s, osiągniesz najwyższą możliwą wydajność.

🔌 Duża liczba interfejsów sieciowych

- Dostosuj liczbę/typ interfejsów do swojej sieci
- Dopasuj konfigurację do swoich potrzeb
- Stosuj równocześnie interfejsy miedziane i światłowodowe (1GbE, 10GbE lub 40GbE)
- Przewiduj zmiany w swojej infrastrukturze sieciowej

🔄 Niezawodność pracy

- High availability
- Dyski RAID
- Wymienne (Hot-swappable) redundantne zasilacze i wentylatory

📄 Zgodność z obowiązującymi przepisami

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



COMMON
CRITERIA



COMMON
CRITERIA



EU
RESTRICTED



NATO
RESTRICTED

NEXT GENERATION UTM
& FIREWALL

SIECI KORPORACYJNE
I DATA CENTER

WWW.STORMSHIELD.PL

SPECYFIKACJA TECHNICZNA

FUNKCJONALNOŚCI

WYDAJNOŚĆ*

Przepustowość Firewall (1518 bajtów UDP)	170 Gbps
Przepustowość Firewall (IMIX**)	53.3 Gbps
Przepustowość IPS (1518 bajtów UDP)	68Gbps
Przepustowość IPS (plik HTTP 1MB)	27 Gbps
Przepustowość Antywirus	12.5 Gbps

VPN*

Przepustowość IPsec - AES GCM	20 Gbps
Przepustowość IPsec - AES256/SHA2	12,3 Gbps
Maks. liczba tuneli IPsec VPN	10 000
Maks. liczba SSL VPN (tryb Portal)	2048
Liczba jednoczesnych klientów SSL VPN	500

POŁĄCZENIA SIECIOWE

Liczba jednoczesnych sesji	20 000 000
Nowe sesje na sekundę	250 000
Maksymalna liczba dostawców internetu/zapasowych	64/64

INTERFEJSY SIECIOWE

Interfejsy Ethernet 10/100/1000	8-64
Interfejsy miedziane 10Gb	0-32 ¹
Interfejsy światłowodowe 1 Gb	0-64 ¹
Interfejsy światłowodowe 10 Gb	2-34 ¹
Interfejsy światłowodowe 40 Gb	0-16 ¹
Opcjonalne moduły rozszerzeń: (8 portów 10/100/1000 - 4 porty 10 Gb miedziane - 8 portów 1Gb światłowodowe - 4 porty 10Gb światłowodowe - 2 porty 40Gb światłowodowe)	7

SYSTEM

Maksymalna liczba reguł filtrowania	32 768
Maksymalna liczba tras statycznych	10 240

REDUNDANCJA

High Availability (Active/Passive)	✓
Redundantne dyski SSD (RAID 1)	RAID 1
Redundantne zasilanie (z możliwością wymiany zasilacza bez przerywania pracy)	✓
Redundantna wentylacja (z możliwością wymiany wentylatora bez przerywania pracy)	✓

SPRZĘT

Dysk lokalny	512 GB SSD
Opcja Big Data (lokalny dysk twardej)	1 TB SSD
MTBF w 25°C (lata)	21.3
Wielkość urządzenia	2U - 19"
Wysokość x szerokość x głębokość (mm)	88.9 x 440 x 645
Waga	15.3 kg (33.73 lbs)
Zasilanie (AC)	100-240V 63-47Hz 9.4-4.72A
Zasilanie 48V (opcja)	48-60VDC 19.2-16A
Pobór energii elektrycznej (maks.)	230V 50Hz 557.4W 2.4A
Wentylator	4
Rozpraszanie ciepła (maks., BTU/h)	1915
Temperatura pracy	0° to 40°C (32° to 104°F)
Wilgotność względna, podczas pracy (bez kondensacji)	0% to 90% @ 40°C (104°F)
Temperatura przechowywania	-20° to 70°C (-4° to 158°F)
Wilgotność względna, przechowywanie (bez kondensacji)	5% to 95%

CERTYFIKACJA

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

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, analityczny 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.

** Rozmiar IP: 60% (48 bajtów) – 25% (494 bajtów) – 15% (1500 bajtów).

¹Zamiast 8 portów interfejsy 10/100/1000