



STORMSHIELD

NETWORK SECURITY

STORMSHIELD SN3100

UTM / Next Generation Firewall dla sieci korporacyjnych i data center



74 Gbps

PRZEPUSTOWOŚĆ
FIREWALL

15 Gbps

PRZEPUSTOWOŚĆ
VPN IPSEC

10 Gbps

PRZEPUSTOWOŚĆ
ANTYWIRUS

Modularność

INTERFEJSY ETHERNETOWE
I ŚWIATŁOWODOWE



⚡ Wydajność i bezpieczeństwo

Dzięki przepustowości nawet do 74 Gb/s, osiągniesz optymalną wydajność w swoim urządzeniu do ochrony sieci.



Możliwość rozbudowy

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



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

SPECYFIKACJA TECHNICZNA

FUNKCJONALNOŚCI

WYDAJNOŚĆ*

Przepustowość Firewall (1518 bajtów UDP)	74 Gbps
Przepustowość Firewall (IMIX**)	30.7 Gbps
Przepustowość IPS (1518 bajtów UDP)	55 Gbps
Przepustowość IPS (plik HTTP 1MB)	23 Gbps
Przepustowość Antywirus	10 Gbps

VPN*

Przepustowość IPsec - AES GCM	15 Gbps
Przepustowość IPsec - AES256/SHA2	8 Gbps
Maks. liczba tuneli IPsec VPN	5000
Maks. liczba SSL VPN (tryb Portal)	1024
Liczba jednoczesnych połączeń klientów SSL VPN	1000

POŁĄCZENIA SIECIOWE

Liczba jednoczesnych sesji	5 000 000
Nowe sesje na sekundę	175 000
Maksymalna liczba bram głównych/zapasowych	64/64

INTERFEJSY SIECIOWE

Interfejsy Ethernet 10/100/1000	2-26
Interfejsy miedziane 10Gb	0-12
Interfejsy światłowodowe 1 Gb	0-24
Interfejsy światłowodowe 10 Gb	0-12
Interfejsy światłowodowe 40 Gb	0-6
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)	3

SYSTEM

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

REDUNDANCJA

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

SPRZĘT

Pamięć lokalna	✓
Partycja na logi	>200GB
Opcja Big Data (lokalny dysk twardej)	1TB SSD
MTBF w 25°C (lata)	19.9
Wielkość urządzenia	1U - 19"
Wysokość x szerokość x głębokość (mm)	44.45 x 443 x 610
Waga	9,86 kg (21.74 lbs)
Zasilanie (AC)	100-240V 60-50Hz 5-3A
Zasilanie 48V (opcja)	36-72VDC 12-6A
Pobór energii elektrycznej (maks.)	230V 50Hz 141W 0.7A
Wentylator	3
Rozpraszanie ciepła (maks., BTU/h)	481
Temperatura pracy	0° do 40°C (32° do 104°F)
Wilgotność względna, podczas pracy (bez kondensacji)	0% do 95% @ 40°C (104°F)
Temperatura przechowywania	-30° do 65°C (-22° do 149°F)
Wilgotność względna, przechowywanie (bez kondensacji)	5% do 95% @ 60°C (140°F)

CERTYFIKACJA

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

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 kwarantanna w przypadku ataku, antyspam i antyphishing, 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, LACP, 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.

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