



STORMSHIELD

NETWORK SECURITY

STORMSHIELD SN-M-SERIES-520

Wsparcie dla rozwoju Twojego biznesu



SD-WAN

POŁĄCZENIE

10 Gbps

PRZEPUSTOWOŚĆ
FIREWALL

2.5 Gbps

PRZEPUSTOWOŚĆ
IPSEC VPN

Modularność

ZMIANY W SIECI
I WYDAJNOŚĆ

⚡ Bezproblemowa integracja

Dzięki zaawansowanym funkcjom sieciowym i modułowości, SN-M-Series-520 bezproblemowo dopasowuje się do Twojej infrastruktury bez wpływu na jej działanie.

📊 Zdolność adaptacji i modułowość

- Możliwość rozbudowy sieci za pomocą interfejsów miedzianych i światłowodowych (1 GbE, 2,5 GbE i 10 GbE)
- Ciągłość usług dzięki redundantnemu zasilaniu
- Integracja z szafami RACK w istniejącej infrastrukturze

🔒 Optymalne bezpieczeństwo

- Zabezpieczenie poświadczeń VPN za pomocą układu TPM
- IPsec VPN i zapobieganie włamaniom
- Zarządzanie dostępem



🔧 Sprzęt typu „wszystko w jednym”

- Zarządzanie łączem WAN - SD-WAN
- Możliwość tworzenia klastrów high availability (HA)



NEXT GENERATION UTM
& FIREWALL

ORGANIZACJE
ŚREDNIEJ WIELKOŚCI

WWW.STORMSHIELD.PL

SPECYFIKACJA TECHNICZNA

WYDAJNOŚĆ*

Przepustowość Firewall (1518 bajtów UDP)	10 Gbps
Przepustowość IPS (1518 bajtów UDP)	5 Gbps
Przepustowość IPS (plik HTTP 1MB)	2.5 Gbps
Przepustowość Antywirus	1.3 Gbps

VPN*

Przepustowość IPsec - AES-GCM	2.5 Gbps
Maks. liczba tuneli IPsec VPN	1 000
Maks. liczba SSL VPN (tryb Portal)	150
Liczba jednoczesnych połączeń klientów SSL VPN	150

POŁĄCZENIA SIECIOWE

Liczba jednoczesnych sesji	600 000
Nowe sesje na sekundę	30 000
Maksymalna liczba bram głównych/zapasowych	64/64

INTERFEJSY SIECIOWE

Interfejsy Ethernet 10/100/2 500 ²	8-16
Interfejsy miedziane 10 Gb	0-4
Interfejsy światłowodowe 1Gb	2-10 ¹
Interfejsy światłowodowe 10 Gb (Dual Speed)	0-4 ¹
Opcjonalne moduły rozszerzeń (8 portów 1 Gb miedzianych - 4 porty 10 Gb miedziane - 4 porty 1 Gb światłowodowe - 8 portów 1 Gb światłowodowych - 4 porty 10 Gb światłowodowe)	1

SYSTEM

Maksymalna liczba reguł filtrowania	4 096 / 16 384
Maksymalna liczba tras statycznych	5 120
Maksymalna liczba tras dynamicznych	10 000

REDUNDANCJA

High availability (active/passive)	✓
Redundantne zasilanie	✓

SPRZĘT

Pamięć lokalna	✓
Partycja na logi	> 200 Gb
Układ TPM	✓
MTBF w 25°C (lata)	18
Wielkość urządzenia	1U - 19"
Wysokość x szerokość x głębokość (mm)	44,45 x 440 x 343
Waga (kg)	4,17
Zasilanie (AC)	100-240 V 60-50 Hz 3-1.5 A
Pobór energii elektrycznej (maks.)	230V 50Hz 112W 0,57A
Wentylator	2
Poziom głośności	57 dBA
Rozpraszanie ciepła (maks., BTU/h)	184
Temperatura pracy	0° do 40 °C (32° do 104 °F)
Wilgotność względna, podczas pracy (bez kondensacji)	0% do 90% przy 40°C
Temperatura przechowywania	-30° do 65 °C (-22° do 149 °F)
Wilgotność względna, przechowywanie (bez kondensacji)	5% do 95% przy 60 °C

CERTYFIKACJA

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

FUNKCJONALNOŚCI

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.

¹ Wymaga transceiverów ² Prędkość do 2,5 Gb

¹ Wymaga transceiverów