



STORMSHIELD

NETWORK SECURITY

STORMSHIELD SNI40

Zabezpieczenie dla sieci przemysłowych



4.8 Gbps

PRZEPUSTOWOŚĆ
FIREWALL

1.1 Gbps

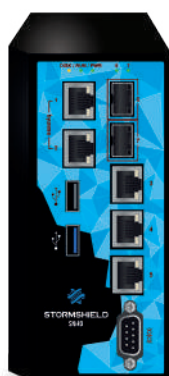
PRZEPUSTOWOŚĆ
IPSEC VPN

10+

PROTOKOŁY
PRZEMYSŁOWE

5 portów

INTERFEJSY ETHERNET
10/100/1000



CSPN
INDUSTRIAL FIREWALL

Zapewnienie bezpieczeństwa bez negatywnego wpływu na twoją działalność przemysłową

Dzięki prostej instalacji przy wdrożeniu, urządzenie zabezpieczające można łatwo zaimplementować w środowisku przemysłowym bez większego wpływu na jej działanie.



Urządzenie dostosowane do trudnego środowiska pracy

Urządzenie STORMSHIELD SNI40 zostało zaprojektowane w taki sposób, żeby zabezpieczyć sieci przemysłowe działające w trudnych warunkach, gdzie panuje niska lub wysoka temperatura, występują wstrząsy, jest pył czy pojawiają się zakłócenia elektromagnetyczne.



Monitorowanie pracy urządzeń w czasie rzeczywistym

Tak jak w przypadku wszystkich rozwiązań STORMSHIELD, model SNI40 umożliwia śledzenie działania urządzeń w czasie rzeczywistym.

NEXT GENERATION UTM
& FIREWALL

OCHRONA SIECI
PRZEMYSŁOWYCH

WWW.STORMSHIELD.PL

SPECYFIKACJA TECHNICZNA

WYDAJNOŚĆ*

Przepustowość Firewall (1518 bajtów UDP)	4.8 Gbps
Przepustowość IPS (IMIX**)	2.4 Gbps
Przepustowość IPS (1518 bajtów UDP)	2.9 Gbps
Przepustowość IPS (plik HTTP 1MB)	1.8 Gbps
Opóźnienie (Maksymalne)	10 ms

VPN*

Przepustowość IPsec - AES128/SHA1	1.1 Gbps
Przepustowość IPsec - AES256/SHA2	0.8 Gbps
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	20 000
Maksymalna liczba dostawców internetu/zapasowych	64/64

INTERFEJSY SIECIOWE

Interfejsy miedziane 10/100/1000	5
Gniazda SFP 1 Gb	0-2
Porty szeregowo	1
Porty USB	1 USB 2.0, 1 USB 3.0

PROTOKOŁY

Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, IEC-60870-5-104, OPC (DA/HDA/AE), BACnet/IP i protokoły IT

SPRZĘT

Pamięć wewnętrzna	32 GB SSD
Logi	> 20 GB SSD
MTBF w 25°C (lata)	26.6
Sposób instalacji	Szyna DIN (szerokość 35 mm, norma EN 50022)
Wysokość x szerokość x głębokość (mm)	165 x 80 x 145
Waga	1.40 kg (3.10 lbs)
Opakowanie: Wysokość x Szerokość x Głębokość (mm)	139 x 283 x 215
Waga z opakowaniem	2.10 kg (4.63 lbs)
Podwójne źródło zasilania (DC)	12-36VDC 5-1.67A
Zużycie (W) (Idle) DC @+25°C	15.5
Pobór mocy (W) (pełne obciążenie, maks.) (W) DC @+25°C	19.5
Liczba wentylatorów	-
Rozpraszanie ciepła (maks., BTU/h)	66.54
Temperatura pracy	-40° do +75°C (-40° do +167°F)
Wilgotność względna, podczas pracy (bez kondensacji)	0% do >90%
Klasa szczelności	IP30
Temperatura przechowywania	-40° do +85°C (-40° do +185°F)
Wilgotność względna przechowywania (bez kondensacji)	5% to 95%

CERTYFIKACJE

CE/FCC, IEC 60950-1, IEC 61000 (3-2, 3-3, 4-18, 6-2, 6-4), IEC 60068 (2-1, 2-2, 2-6, 2-13, 2-14, 2-27, 2-30, 2-78), EN 55024, EN 55032

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, 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, 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.

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 3.x.

* Test przeprowadzony w warunkach laboratoryjnych dla oprogramowania w wersji 3.x. Wyniki mogą się różnić w zależności od warunków testowych i wersji oprogramowania.