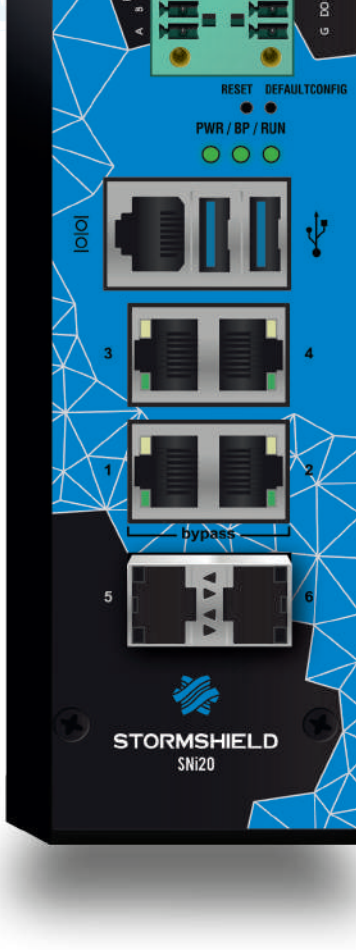
STORMSHIELD

NETWORK SECURITY

STORMSHIELD **SNi20**

Zabezpieczenie sieci przemysłowch

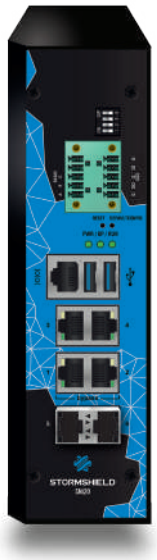


2.4 Gbps
PRZEPUSTOWOŚĆ FIREWALL

10 ms
MAKSYMALNE OPÓŹNIENIE

DPI
PROTOKOŁY PRZEMYSŁOWE (DEEP PACKET INSPECTION)

NAT
INTEGRACJA SIECI PRZEMYSŁOWYCH



Urządzenie dostosowane do Twojego środowiska

Dzięki połączeniu unikalnej i transparentnej integracji sieci (routing i NAT) z zaawansowanymi funkcjami bezpieczeństwa, integracja SNi20 odbywa się bez konieczności modyfikacji istniejącej infrastruktury sieciowej.

Integracja środowisk przemysłowych

- Tryby bezpieczeństwa - klaster HA, port bypass oraz redundantne zasilanie
- Przemysł energetyczny (IEC 61850-3)
- Urządzenie przystosowane do pracy w trudnych warunkach (szyna DIN, IP20)
- Optymalizacja kosztów (dzięki rozwiązaniom SNi40 i SNi20 jeszcze łatwiejsze dopasowanie urządzenia do wielkości sieci)

Bezpieczeństwo w czasie rzeczywistym

- Bezpieczne zdalne zarządzanie maszynami i sterownikami PLC (VPN SSL / IPsec)
- Zdalna kontrola nad rozproszonymi procesami
- Segmentacja na strefy bez zmiany infrastruktury
- Zabezpieczenie procesów OT (DPI, IPS, filtrowanie)

SPECYFIKACJA TECHNICZNA

WYDAJNOŚĆ*	
Przepustowość Firewall (1518 bajtów UDP)	**2.4 Gbps**
Przepustowość Firewall (IMIX**)	**1.4 Gbps**
Przepustowość IPS (1518 bajtów UDP)	**1.6 Gbps**
Przepustowość IPS (pliki 1 MB, HTTP)	**900 Mbps**
Opóźnienie (Maksymalne)	**10 ms**

VPN*	
Przepustowość IPSec - AES-GCM	**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	**500 000**
Nowe sesje na sekundę	**20 000**
Maksymalna liczba dostawców internetu/ bram zapasowych	**64/64**

INTERFEJSY SIECIOWE	
Interfejsy miedziane 10/100/1000	**2-4**
Gniazda SFP 1 Gb	**0-2**
Zarządzanie	**1 port szeregowy i 2 porty USB 3.0**

PROTOKOŁY - DEEP PACKET INSPECTION (DPI)

Modbus, UMAS, S7 200-300-400, EtherNet/IP, CIP, OPC UA, OPC (DA/HDA/AE), BACnet/IP, PROFINET, IEC 60870-5-104, IEC 61850-3 & IT

REDUNDANCJA	
High Availability (Active/Passive)	✔
Port bypass	Opcjonalnie

SPRZĘT	
Pamięć	**Karta SD**
MTBF w 25°C (lata)	**35,1**
Sposób instalacji	**Szyna DIN (szerokość 35 mm, norma EN 50022)**
Wysokość x szerokość x głębokość (mm)	**210 x 60 x 155**
Waga	**1.75 kg (3.86 lbs)**
Opakowanie: Wysokość x Szerokość x Głębokość (mm)	**190 x 270 x 235**
Waga z opakowaniem	**2.46 kg (5.42 lbs)**
Podwójne źródło zasilania (DC)	**2x12-48VDC 3-0.75A**
Zużycie (W) (Idle) DC @+25°C	**15**
Pobór mocy (W) (pełne obciążenie, maks.) (W) DC @+25°C	**19**
Liczba wentylatorów	**-**
Rozpraszanie ciepła (maks., BTU/h)	**64,83**
Temperatura pracy	**-40° do +70°C (-40° do +158°F)**
Wilgotność względna, podczas pracy (bez kondensacji)	**0% do 95%**
Klasa szczelności	**IP20**
Temperatura przechowywania	**-40° do +85°C (-40° do +185°F)**
Wilgotność względna, przechowywanie (bez kondensacji)	**0% do 95%**

CERTYFIKACJE

CE/FCC/CB, EN 61000-6-2, EN 61000-6-4, IEC 61000-4-18, IEC 60068-2, IEC 61850-3, IEEE 1613, EN 50121-4, IEC 60529

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 CrossSite 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.

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), zarządzanie wieloma łączami (równoważenie obciążenia, brama zapasowa), wielopoziomowe zarządzanie wewnętrznym lub zewnętrznym 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, wiele 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, IPFIX/NetFlow, automatyczne tworzenie kopii zapasowych konfiguracji, Open API.

.....

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.*