STORMSHIELD

NETWORK SECURITY

STORMSHIELD **SNxr1200**

Do zabezpieczania krytycznych środowisk zarówno cywilnych jak i militarnych

IP67	ITAR FREE	2 kg	5 portów
KLASA SZCZELNOŚCI	UPROSZCZONY EXPORT	OBUDOWA Z ODLEWU	INTERFEJSY ETHERNET

Rozwiązanie stworzone do trudnych warunków

SNxr1200 to zapora nowej generacji przeznaczona do pracy w **trudnych warunkach**, zapewniająca potrzebny, wyższy poziom bezpieczeństwa, wykorzystywana szczególnie w misjach lotniczych, kosmicznych i wojskowych.

Bezpieczna komunikacja

- IPSec VPN zgodny z "**Restricted mode**"
- Zintegrowany system zapobiegania włamaniom (DPI i IPS)
- **Moduł TPM**

Ciągłość działania

- High availability
- Redundantne liki dostępu
- Zarządzanie ruchem

Gotowy do krytycznych środowisk

- **Złącza Micro MIL-DTL-38999**
- Zgodny ze standardem DO-160, MIL-STD-461 oraz MIL-STD-810

SPECYFIKACJA TECHNICZNA

PERFORMANCE*	
Przepustowość Firewall (1518 bajtów UDP)	**2.4 Gbps**
Przepustowość IPS (1518 bajtów UDP)	**1.6 Gbps**
Przepustowość IPS (pliki HTTP 1 MB)	**900 Mbps**
VPN*	
Przepustowość IPSec - AES-GCM	**600 Mbps**
Maks. liczba tuneli IPSec VPN	**100**
POŁĄCZENIA SIECIOWE	
Liczba jednoczesnych sesji	**500 000**
Nowe sesje na sekundę	**20 000**
ŁĄCZNOŚĆ	
Złącza w stanadardzie Micro MIL-DTL-38999	✔
Interfejsy Ethernet 10/100/1000 (poprzez złącza MIL-DTL-38999)	**5**
Interfejs szeregowy RS232 (poprzez złącza MIL-DTL-38999)	**1**
Interfejsy USB 2.0 (poprzez złącza MIL-DTL-38999)	**4**
REDUNDANCJA	
High Availability (Active/Passive)	✔
SPRZĘT	
Pamięć Karta SD	**128GB**
Partycja na logi > 100GB SSD	✔
Moduł TPM	✔
MTBF w 25 °C (lata, MIL-HDBK-217F. GB)	**9,1**
Wysokość x szerokość x głębokość (mm)	**67.5 x 140 x 205**
Waga	**2 kg (4.41 lbs)**
Zasilanie (CC)	**+28VDC (12VDC - 36VDC)**
Pobór mocy (W) (pełne obciążenie, maks.)	**30W**
Chłodzenie pasywne	✔
Rozpraszanie ciepła (maks., BTU/h)	**102.5**
Temperatura pracy (DO-160G, Section 4 / Cat A2)	**-40° do +71°C (-40° do +159.8°F)**
Temperatura przechowywania	**-40° do +85°C (-40°F do +185°F)**
Wilgotność (DO-160G, Sekcja 6 / kat. B)	**RH: 95±4% @ 65°C i RH: 85±4% @ 38°C**
Wilgotność (MIL-STD-810G Method 507.6 - rozdział 4.4, procedura I, kategoria B1)	**100%**
Wilgotność względna, przechowywanie (bez kondensacji)	**0%-95%**
Poziom ochrony zapewniany przez urządzenie (kod IP, IEC60529)	**IP67**
Wysokość (DO-160G Sekcja 4 / Kat A2)	**Wysokość robocza: +15 000m Test dekompresji: +8 000ft do +5 0000ft (+2 400m do +15 000m)**
Mgła solna (DO-160G sekcja 14 / Kat T)	**50% mgła solna po 96h**
Wstrząsy, wibracje i przyspieszenia (DO-160G Sekcja 7 / Kat B, Sekcja 8 / Kat U + MIL-STD-810E - Procedura II - Test Method 513 + MIL-STD-810G - Test Method 514.6 - Kat 20)	✔

CERTYFIKACJE

CE : EN55032/EN 55035 - SAFETY: EN62368-1
DO-160G / MIL-STD-461F / MIL-STD-810G

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), dynamicz-na 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 wykry-wanie 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 bezpie-czeństwa, 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.*