NETWORK SECURITY

STORMSHIELD SN1100



UTM / Next Generation Firewall
dla sieci korporacyjnych i data center

45 Gbps
PRZEPUSTOWOŚĆ FIREWALL

7.5 Gbps
PRZEPUSTOWOŚĆ VPN

10 GbE
INTERFEJS ŚWIATŁOWODOWY

Integralność
INTERFEJSY ETHERNETOWE I ŚWIATŁOWODOWE



Modularność

Dzięki elastycznym opcjom konfiguracji, istnieje wiele sposobów na rozbudowę sieci. Możliwość rozbudowy o dodatkowe interfejsy ethernetowe i światłowodowe (1 GbE lub 10GbE) pozwala uwzględnić przyszłe zmiany w infrastrukturze.

Wydajność

- Najlepszy stosunek wydajności do ceny w zabezpieczaniu ruchu sieciowego
- Synergia pomiędzy sprzętem i oprogramowaniem

Gwarantowane bezpieczeństwo

- IPSec VPN i zapobieganie włamaniom
- Zarządzanie dostępem
- Zabezpieczanie kluczy VPN za pomocą sprzętowego modułu TPM

Niezawodność pracy

- Redundantne zasilanie*
- High availability (HA)

** opcjonalnie*

SPECYFIKACJA TECHNICZNA

WYDAJNOŚĆ*	
Przepustowość Firewall (1518 bajtów UDP)	**45 Gbps**
Przepustowość IPS (1518 bajtów UDP)	**18 Gbps**
Przepustowość IPS (plik HTTP 1MB)	**12 Gbps**
Przepustowość Antywirus	**4 Gbps**
VPN*	
Przepustowość IPSec - AES-GCM	**7,5 Gbps**
Przepustowość IPSec - AES256/SHA2	**4 Gbps**
Maks. liczba tuneli IPSec VPN	**2 000**
Maks. liczba SSL VPN (tryb Portal)	**500**
Liczba jednoczesnych połączeń klientów SSL VPN	**800**
POŁĄCZENIA SIECIOWE	
Maksymalna liczba jednoczesnych sesji	**1 800 000**
Liczba nowych sesji/sek.	**90 000**
Maksymalna liczba bram głównych/zapasowych	**64/64**
INTERFEJSY SIECIOWE	
Interfejsy Ethernet 10/100/1000	**8/24**
Interfejsy miedziane 10Gb	**0-8**
Interfejsy światłowodowe 1 Gb	**0-16**
Interfejsy światłowodowe 10 Gb	**2-10**
Opcjonalne moduły rozszerzeń: (8 portów 10/100/1000 - 4 porty 10 Gb miedziane - 8 portów 1Gb światłowodowe - 4 porty 10Gb światłowodowe)	**2**
SYSTEM	
Maksymalna liczba reguł filtrowania	**8 192 / 32 768**
Maksymalna liczba tras statycznych	**7 680**
Maksymalna liczba tras dynamicznych	**10 000**
REDUNDANCJA	
High Availability (Active/Passive)	✔
Redundantne zasilanie (z możliwością wymiany zasilacza bez przerywania pracy)	*Opcja*
SPRZĘT	
Pamięć lokalna	✔
Partycja na logi	**512 GB SSD**
Wielkość urządzenia	**1U -19”**
Wysokość x szerokość x głębokość (mm)	**44,45 x 440 x 540**
Waga (kg)	**8,11**
Zasilanie (AC)	**100-240V 60-50Hz 5A-3A**
Pobór energii elektrycznej (maks.)	**230V 50Hz 112W 0,57A**
Wentylatory	**3**
Poziom głośności	**65 dBA**
Rozpraszanie ciepła (maks., BTU/h)	**427**
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**

** Test przeprowadzony w warunkach laboratoryjnych dla oprogramowania w wersji 4.x. Wyniki mogą się różnić w zależności od warunków testowych i wersji oprogramowania.*

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.

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