NETWORK SECURITY

STORMSHIELD SN710

UTM / Next Generation Firewall
dla średnich i dużych sieci

Interfejsy światłowodowe

DOSTĘPNOŚĆ INTERFEJSÓW ŚWIATŁOWODOWYCH

15 Gbps

PRZEPUSTOWOŚĆ FIREWALL

3 Gbps

PRZEPUSTOWOŚĆ IPSEC VPN

Modularność

INTERFEJSY ETHERNETOWE I ŚWIATŁOWODOWE

COMMON CRITERIA EAL3+

COMMON CRITERIA EAL4+

EU RESTRICTED

NATO OTAN RESTRICTED

Wydajność oraz modularność

Oferując wydajność na poziomie 15 Gb/s, model SN710 jest w stanie dostosować się do Twoich potrzeb dzięki modułowej budowie, która umożliwia rozbudowę liczby portów (do 16) oraz portów światłowodowych 10Gb.

Kontrola aplikacji

- Analiza dynamiczna
- Ograniczenie wykorzystywania niebezpiecznych lub niezwiązanych z pracą aplikacji
- Podejście jakościowe

Zgodność z przepisami

- Dostęp do logów i raportów jest zgodny z przepisami RODO
- Zbieranie logów
- Przechowywanie logów zgodne z obowiązującymi regulacjami

Urządzenie wielofunkcyjne

- Firewall aplikacyjny, zapobieganie włamaniom (IPS), VPN, antywirus
- Antyspam, filtrowanie stron internetowych, audyt podatności
- Zaawansowane raportowanie, monitorowanie użytkowników

SPECYFIKACJA TECHNICZNA

WYDAJNOŚĆ*	
Przepustowość Firewall (1518 bajtów UDP)	**15 Gbps**
Przepustowość IPS (1518 bajtów UDP)	**8 Gbps**
Przepustowość IPS (plik HTTP 1MB)	**3 Gbps**
Przepustowość Antywirus	**2 Gbps**
VPN*	
Przepustowość IPSec - AES-GCM	**3 Gbps**
Przepustowość IPSec - AES256/SHA2	**2 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	**1 000 000**
Nowe sesje na sekundę	**50 000**
Maksymalna liczba bram głównych/zapasowych	**64/64**
INTERFEJSY SIECIOWE	
Interfejsy Ethernet 10/100/1000	**8-16**
Miedziane interfejsy 10 Gb	**0-4**
Interfejsy światłowodowe 1 Gb	**0-8**
Interfejsy światłowodowe 10 Gb	**0-4**
Opcjonalne moduły rozszerzeń (8 portów 10/100/1000 — 4 porty miedziane 10Gb — 8 portów światłowodowych 1Gb — 4 porty światłowodowe 10Gb)	**1**
SYSTEM	
Maksymalna liczba reguł filtrowania	**16 384**
Maksymalna liczba tras statycznych	**2 048**
Maksymalna liczba tras dynamicznych	**10 000**
REDUNDANCJA	
High Availability (Active/Passive)	✔
SPRZĘT	
Pamięć lokalna	✔
Partycja na logi	**> 200 GB**
MTBF w 25°C (lata)	**15.1**
Wielkość urządzenia	**1U -19"**
Wysokość x szerokość x głębokość (mm)	**44.45 x 440 x 310**
Waga	**4.22 kg (9.3 lbs)**
Zasilanie (AC)	**100-240V 60-50Hz 3-1.5A**
Pobór energii elektrycznej (maks.)	**230V 50Hz 37W 0.23A**
Wentylator	**2**
Poziom głośności	**55 dbA**
Rozpraszanie ciepła (maks., BTU/h)	**145**
Temperatura pracy	**5° to 40°C (41° to 104°F)**
Wilgotność względna, podczas pracy (bez kondensacji)	**20% to 90% @ 40°C**
Temperatura przechowywania	**-30° to 65°C (-22° to 149°F)**
Wilgotność względna, przechowywanie (bez kondensacji)	**5% to 95% @ 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, inspekcja 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 kontrola 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.*

*** Opcjonalnie.*