NETWORK SECURITY

STORMSHIELD
SN-M-SERIES-920

Zachowaj ciągłość biznesową
w rozbudowanych architekturach sieciowych

Interfejsy światłowodowe
POŁĄCZENIE

36 Gbps
PRZEPUSTOWOŚĆ FIREWALL

6 Gbps
PRZEPUSTOWOŚĆ IPSEC VPN

Modularność
INTERFEJSY MIEDZIANE I ŚWIATŁOWODOWE

Modułowość

Możliwość rozbudowy sieci jest możliwa dzięki wielu elastycznym opcjom konfiguracji. Ta modułowość między miedzianymi i światłowodowymi interfejsami 1 GbE lub 10 GbE wspiera rozwój infrastruktury.

Ciągłości działania

- Możliwość tworzenia klastra high availability (HA)
- Redundantne zasilanie
- Integracja z szafami RACK w istniejącej infrastrukturze

Optymalna wydajność

- Pełna wydajność platformy SN-M-Series
- 36 Gb/s przepustowości firewalla
- Możliwość przejścia z modelu SN-M-Series-720 do SN-M-Series-920 bez konieczności wymiany urządzenia

Sprzęt typu „wszystko w jednym”

- VPN IPsec i zapobieganie włamaniom
- Ochrona stacji roboczych i serwerów
- Interaktywne raporty ułatwiające ograniczanie ryzyka

SPECYFIKACJA TECHNICZNA

WYDAJNOŚĆ*	
Przepustowość Firewall (1518 bajtów UDP)	**36 Gbps**
Przepustowość IPS (1518 bajtów UDP)	**16 Gbps**
Przepustowość IPS (plik HTTP 1MB)	**10 Gbps**
Przepustowość Antywirus	**3,5 Gbps**
VPN*	
Przepustowość IPSec - AES-GCM	**6 Gbps**
Maks. liczba tuneli IPSec VPN	**2 000**
Maks. liczba SSL VPN (tryb Portal)	**500**
Liczba jednoczesnych połączeń klientów SSL VPN	**500**
POŁĄCZENIA SIECIOWE	
Liczba jednoczesnych sesji	**1 500 000**
Nowe sesje na sekundę	**80 000**
Maksymalna liczba bram głównych/zapasowych	**64/64**
INTERFEJSY SIECIOWE	
Interfejsy Ethernet 100/1000/2500	**8-16**
Miedziane interfejsy 10 Gb	**0-4**
Interfejsy światłowodowe 1Gb	**0-8**
Interfejsy światłowodowe 10Gb	**2[1]-6**
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	**32 768**
Maksymalna liczba tras statycznych	**5 120**
Maksymalna liczba tras dynamicznych	**10 000**
REDUNDANCJA	
High availability (active/passive)	✔
Redundantne zasilanie	✔
SPRZĘT	
Pamięć lokalna	✔
Partycja na logi	**>200 GB**
MTBF w 25°C (lata)	**21.4**
Wielkość urządzenia	**1U -19"**
Wysokość x szerokość x głębokość (mm)	**44.45 x 440 x 343**
Waga	**4,93 kg (10.86 lbs)**
Zasilanie (AC)	**100-240 V 60-50 Hz 4-2 A**
Pobór energii elektrycznej (maks.)	**230 V 50 Hz 72 W 0.38 A**
Wentylator	**2**
Poziom głośności	**62 dBA**
Rozpraszanie ciepła (maks., BTU/h)	**270**
Temperatura pracy	**0° do 40 °C (32° do 104 °F)**
Wilgotność względna, podczas pracy (bez kondensacji)	**0% do 90% przy 40 °C**
Temperatura przechowywania	**-30° do 65 °C (-22° do 149 °F)**
Wilgotność względna, przechowywanie (bez kondensacji)	**5% do 95% przy 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.*