



STORMSHIELD

SN-S-SERIES

220/320

Do 11,9 Gbps

PRZEPUSTOWOŚĆ FIREWALL

Do 4,8 Gbps

PRZEPUSTOWOŚĆ VPN

Jednolita ochrona

SME/SMI

NETWORK SECURITY



SKALOWALNA UJEDNOLICONA OCHRONA



Najlepsza ujednolicona ochrona

Ochrona infrastruktury, kontrola dostępu do aplikacji i zabezpieczenie przeglądania stron internetowych przez pracowników: to wszystko składa się na optymalną ochronę sieci małych i średnich firm.

Rozwiązanie SD WAN dla oddziałów zdalnych

Zautomatyzowane, bezpieczne połączenie dla Twojej rozproszonej infrastruktury zapewnia Twoim pracownikom zaufany dostęp do zasobów firmy.

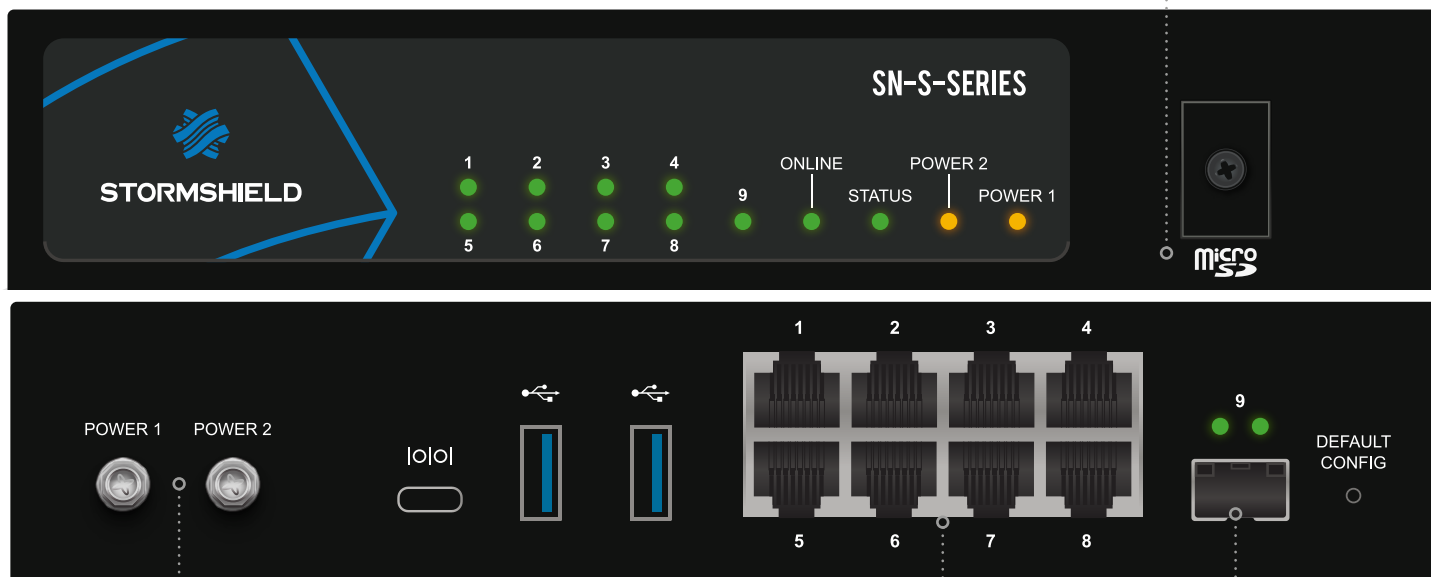
Rośnie wraz z twoimi potrzebami

Podnieś swoją platformę w ramach rozwoju, po prostu zmieniając licencję. Platforma SN-M-Series pozwala Ci przewidzieć Twoje potrzeby dotyczące wydajności.

DLA EUROPEJSKIEGO CYBERBEZPIECZEŃSTWA

Wybierając rozwiązania Stormshield, zyskujesz prawdziwą niezależność strategiczną i spokój ducha w wysoce napiętym kontekście geopolitycznym. W pełni opracowane we Francji, nasze oprogramowanie otrzymało certyfikat wiodących europejskich agencji cyberbezpieczeństwa, takich jak ANSSI (Francja) i CCN (Hiszpania), a także Standard Qualification.

Przechowywanie logów
Karta microSD



Redundantne
zasilanie

8 miedzianych
interfejsów
100/1000/2500

1 interfejs
światłowodowy
1 Gb

WAŻNE INFORMACJE



Interfejsy sieciowe

8

Interfejsy miedziane GbE



Ciągłość działania

Redundancja

Podwójne zasilanie (opcja)

SN-S-Series

220



Przepustowość

10 Gbps

Firewall



VPN

3,3 Gbps

Przepustowość IPSec

Zmiana
licencji

SN-S-Series

320



Przepustowość

11,9 Gbps

Firewall



VPN

4,8 Gbps

Przepustowość IPSec



FUNKCJONALNOŚCI

Dokument nie jest umową. Wymienione funkcje są dostępne w wersji 5.x.

Ujednolicona ochrona

Optymalna ochrona sieci z **najbardziej kompleksowym zestawem funkcji bezpieczeństwa na rynku**: firewall, IPS, kontrola aplikacji, VPN, antywirus, antyspam, filtrowanie stron internetowych, itp.

Bezproblemowa integracja sieciowa

Różne tryby wdrożenia w Twojej sieci (router, transparentny i hybrydowy) należą do najbardziej elastycznych na rynku.

Zapewniają one bezproblemową integrację zapory z istniejącą architekturą sieciową.

SDWAN

Automatyczne zarządzanie połączeniami, dynamiczny wybór łącza i łatwe zarządzanie przepustowością **umożliwiają pracownikom dostęp do zasobów firmy.**

... oraz unikalne oprogramowanie

Stormshield oferuje unikalny, ergonomiczny interfejs do zarządzania swoim asortymentem produktów. To **obniża koszty operacyjne, ułatwia zarządzanie** zespołami IT i **oszczędza czas** firmy.

Więcej funkcjonalności

Kontrola użytkownika

Tryb Firewall/IPS/IDS • Reguły firewall w zależności od użytkownika • Wykrywanie i zarządzanie aplikacjami • Filtrowanie Microsoft Services • Przemysłowy Firewall/IPS/IDS • Kontrola aplikacji przemysłowych • Wykrywanie i kontrolowanie korzystania z terminali mobilnych • Geolokalizacja (kraje, kontynenty) • Dynamiczna reputacja hosta • URL Filtering • Transparentne uwierzytelnianie (Active Directory, SSO Agent, SSL) • Uwierzytelnianie VDI wielu użytkowników za pomocą dedykowanego agenta (Citrix, TSE) • Uwierzytelnianie w trybie gościa i polecenia • Usługi internetowe • Sprawdzanie hosta • Zero Trust Network Access (ZTNA)

Ochrona przed zagrożeniami

Wykrywanie i zapobieganie włamaniom (IPS) • Wykrywanie protokołów oraz sprawdzanie ich zgodności • Inspekcja aplikacji • Ochrona przed atakami DoS • Ochrona przed SQL injections • Ochrona przed Cross-Site Scripting (XSS) • Ochrona przed złośliwym kodem Web2.0 oraz skryptami • Wykrywanie trojanów • Wykrywanie połączeń interaktywnych (botnet, Command & Control) • Ochrona przed data evasion • Zaawansowane zarządzanie fragmentacją • Automatyczna reagowanie na ataki (powiadomienia, kwarantanna, blokada, QoS, zrzut ruchu) • Antyspam i antyphishing: analiza reputacji, silnik heurystyczny • Wbudowany antywirus (HTTP, SMTP, POP3, FTP) • Analiza i inspekcja ruchu szyfrowanego (SSL) • Ochrona VoIP (SIP) • Współpraca bezpieczeństwa: reputacja IP, Sanboxing oparty na chmurze na terenie Europy (opcja)

Poufność

Tunele IPsec VPN Site-to-site lub client-to-site • Odporność postkwantowa • Dostęp zdalny za pomocą SSL VPN dla wielu systemów (Windows, Android, iOS, itd.) • Agent SSL VPN z automatyczną opcją konfiguracji (Windows) • Wsparcie IPsec VPN dla Android/iPhone

Sieciowa - integracja

IPv6 • NAT, PAT, tryb transparentny (bridge)/routera/hybrydowy • Dynamiczny routing (RIP - OSPF - BGP) • Multicast • Zarządzanie wieloma łączami (równoważenie, failover) • Wielopoziomowe wewnętrzne lub zewnętrzne PKI • Uwierzytelnianie wielu domen (w tym wewnętrzny LDAP) • Routing oparty na regułach (PBR) • Zarządzenia QoS • Serwer/klient/relay DHCP • Klient NTP • DNS proxy-cache • HTTP proxy • Agregacja linków (LACP, tryb Broadcast oraz redundancja) • Spanning-tree management (RSTP/MSTP) • SD-WAN • Wieloskładnikowe uwierzytelniania (MFA)

Zarządzanie

Zarządzanie stronami Web • Interfejs webowy z anonimizacją logów (zgodność z RODO) • Obiektowe zarządzanie politykami • Kontekstowe reguły bezpieczeństwa • Analizator poprawności reguł • Licznik użycia reguł • Aktualizacje zabezpieczeń online lub offline • Globalna/Lokalna polityka bezpieczeństwa • Wbudowane narzędzia do raportowania i analizy logów • Interaktywne i konfigurowalne raporty • Wsparcie dla wielu serwerów syslog UDP/TCP/TLS • Agent SNMP v1, v2, v3 • IPFIX • Automatycznie konfigurowana kopia zapasowa • Open API • Nagrywanie skryptów • Klaster wysokiej dostępności (HA)

STORMSHIELD

WYDAJNOŚĆ ¹	220	320
Przepustowość Firewall (UDP 1518 bytes)	10 Gbps	11,9 Gbps
Przepustowość Firewall (IMIX)	4 Gbps	5,7 Gbps
Przepustowość IPS (UDP 1518 bytes)	6 Gbps	9,9 Gbps
Przepustowość IPS (IMIX)	2 Gbps	3 Gbps
Ochrona przed zagrożeniami*	740 Mbps	1,1 Gbps

* Ochronę przed zagrożeniami mierzy się z włączonymi regułami Firewall, IPS, antywirus, reputacją IP, oraz zabezpieczeniami aplikacji internetowych, przy użyciu realistycznego ruchu (mix) oraz z włączonym logowaniem.

VPN	220	320
Przepustowość IPsec - AES-GCM (1464 byte UDP)	3,3 Gbps	4,8 Gbps
Przepustowość IPsec - AES-GCM (IMIX)	1,6 Gbps	2,7 Gbps
Maks. liczba tuneli IPsec VPN (1024 kbps na tunel)	300	400
Liczba jednoczesnych połączeń klientów SSL VPN	300	400

POŁĄCZENIA SIECIOWE	220	320
Liczba jednoczesnych sesji	300 000	400 000
Nowe sesje na sekundę	39 000	60 000
Maksymalna liczba bram głównych/zapasowych	64/64	64/64

INTERFEJSY SIECIOWE	220	320
Liczba interfejsów miedzianych	8	8
Liczba interfejsów światłowodowych**	1	1

** Wymaga transceiverów

SYSTEM	220	320
Maksymalna liczba reguł filtrowania (rekomendowana / specyficzna konf.)	2 048/8 192	2 048/8 192
Maksymalna liczba tras statycznych	512	512
Maksymalna liczba tras dynamicznych	10 000	10 000
High availability	Active-Passive	Active-Passive

¹ Test przeprowadzony w warunkach laboratoryjnych w warunkach idealnych dla wersji 5.x. Wyniki mogą się różnić w zależności od warunków testowych i wersji rozwiązania.

SPECYFIKACJA TECHNICZNA

SPRZĘT	220	320
Pamięć/Dysk lokalny	Tak	
Partycja na logi	Karta microSD	
MTBF w 25°C	36,5 lat	
Rozmiar	1U (<1/2 19")	
Wysokość x szerokość x głębokość (mm)	42 (47 z gumowymi nóżkami) x 210 x 205	
Waga	1,67 kg (3.68 lbs)	
Zasilanie	AC: 100-240V 60-50Hz 1,3-0,75A	
Redundantne zasilanie	Opcja	
Pobór energii elektrycznej (w spoczynku/średni/maksymalny w Wattach (W))	15/24/28	
Poziom hałasu	Chłodzenie pasywne (bez wentylatora)	
Rozpraszanie ciepła (w spoczynku/średnie/maksymalne w BTU/h)	51/82/95	
Warunki pracy	Temperatura: 0° do 40°C (32° do 104°F) Wilgotność: 0% do 90% @ 40°C (104°F)	
Warunki przechowywania	Temperatura: -30° do 65°C (-22° do 149 °F) Wilgotność: 5% do 95% @ 60°C (140°F)	

CERTYFIKACJA	220	320
Zgodność	CE/FCC/RCM/UKCA/CB	
Certyfikacja	EAL4+, Qualification Standard, Producto CCN Aprobado & Cualificado, IEC-62443-4-1	

PAKIETY LICENCYJNE

ESSENTIAL SECURITY PACK

Korporacje, które wybierają ten wariant poszukują jednolitej ochrony przed zagrożeniami przekazywanymi za pośrednictwem sieci WWW lub poczty elektronicznej, oraz chcą uważnie monitorować aktywności online ich użytkowników.

Z segmentacją sieciową, bezpiecznymi połączeniami, SD-WAN, IPS oraz Zero Trust Network Access (ZTNA), jest zapewniony niezbędny poziom zabezpieczeń.

PREMIUM SECURITY PACK

Ten pakiet koncentruje się na korporacjach o wysokich wymaganiach bezpieczeństwa, **zapewniając najlepszą technologię do przeciwdziałania nawet najbardziej wyrafinowanym atakom. Zaawansowany system antywirusowy z technologią emulacji oraz chmurowym URL filtrowaniem w oparciu o ponad 70 kategorii** podniesie Twoją ochronę do poziomu, który nie ma sobie równych na rynku.

Next-Generation Firewall

Firewall warstwy 7	✓	✓
Geolokalizacja	✓	✓
Usługii internetowe	✓	✓
Uwierzytelnienie użytkowników, MFA oraz SSO	✓	✓

SD-WAN i ZTNA

IPsec VPN	✓	✓
Szyfrowanie postkwantowe	✓	✓
SSL VPN	✓	✓
Ocena bezpieczeństwa urządzenia	✓	✓

Ochrona przed zagrożeniami

IPS/IDS	✓	✓
Zaufane certyfikaty publiczne	✓	✓
Antyspam	✓	✓
Threat intelligence (IP i domeny)	✓	✓
Chmurowa baza URL (filtrowanie url)	Opcja	✓
Antywirus	Opcja	✓
Breach Fighter (Sandboxing wykorzystujący AI)	Opcja	✓
Ochrona protokołów przemysłowych	Opcja	✓

Serwisy

Aktualizacja oprogramowania	✓	✓
Wymiana w razie awarii	✓	✓
Dostęp do standardowego wsparcia technicznego	✓	✓
Automatyczna kopia konfiguracji	✓	✓
Dostęp do wsparcia technicznego 24x7	Opcja	Opcja
Ekspresowa wymiana	Opcja	Opcja
Bezpieczny zwrot	Opcja	Opcja

Essential Security Pack

Premium Security Pack

WYMIANA SPRZĘTU

Wszystkie pakiety bezpieczeństwa obejmują wymianę sprzętu, aby zapewnić ciągłość działania w przypadku awarii. Urządzenie zostanie po prostu wymienione na podobny produkt. Dostępne są trzy poziomy tej usługi.

Standardowa wymiana

Twoje urządzenie zostanie wymienione po otrzymaniu przez nasze centrum obsługi klienta we Francji wadliwego urządzenia.

Ekspresowa wymiana

Twoje urządzenie zostanie wymienione z wyprzedzeniem. Gdy tylko nasze wsparcie zdiagnozuje awarie sprzętu, wyślemy produkt zastępczy, który otrzymasz następnego dnia roboczego¹.

Spokój dla wszystkich

W ramach tej usługi możesz samodzielnie wymienić sprzęt po zdiagnozowaniu przez nasze wsparcie techniczne usterki².

¹ Skontaktuj się z nami w sprawie kwalifikujących się krajów i miast. Dotyczy diagnozy postawionej przed godziną 13:00.

² Aby skorzystać z tej usługi należy wcześniej nabyć produkty zamienne.

DLA OPTYMALNEJ OCHRONY

Stormshield oferuje opcje, które pokryją Twoje dodatkowe potrzeby w zakresie cyberbezpieczeństwa.

Zneutralizuj najbardziej wyrafinowane zagrożenia dzięki Stormshield Network Advanced Antivirus.

Skorzystaj z zaawansowanego i niezawodnego rozwiązania filtrującego dzięki Stormshield Extended Web Control.

Rozszerz możliwości swojego domowego biura o niezwykle bezpieczny dostęp zdalny dzięki klientowi VPN Stormshield.

JAKIEŚ WĄTPLIWOŚCI DOTYCZĄCE ZAŁĄCZNIKÓW?



Przestań narażać bezpieczeństwo swojej infrastruktury na wątpliwe załączniki i przetestuj je za pomocą Stormshield Breach Fighter.

→ breachfighter.stormshieldcs.eu

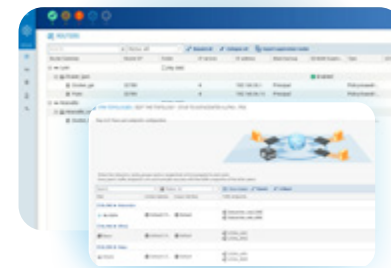
ZARZADZAJ BEZPIECZEŃSTWEM ZA POMOCĄ SKUTECZNYCH NARZĘDZI



Narzędzie do podejmowania decyzji

ze Stormshield Log Supervisor

Zoptymalizuj swoje zadania badawcze i reagowania na incydenty. Dzięki szybkiemu przeglądowi efektywności systemu będziesz mieć spokój ducha, wiedząc, że Twoje inwestycje w bezpieczeństwo są tego warte.



Zarządzanie dużymi infrastrukturami

ze Stormshield Management Center

Stormshield Management Center wymienia konfigurację zapór SNS i dane monitorujące w czasie rzeczywistym, jednocześnie zapewniając ich poufność i integralność. Jego intuicyjny interfejs graficzny minimalizuje błędy konfiguracji, a jego globalne zarządzanie zasadami bezpieczeństwa i filtrowania eliminuje powtarzające się zadania.

EUROPEJSKI WYBÓR W CYBERBEZPIECZEŃSTWIE

www.stormshield.pl