STORMSHIELD

SN-XS-SERIES

170

Do 8,5 Gbps
PRZEPUSTOWOŚĆ FIREWALL

Do 1,8 Gbps
PRZEPUSTOWOŚĆ VPN

SDWAN
MAŁE ODDZIAŁY

NETWORK SECURITY

UJEDNOLICONA OCHRONA, PASUJĄCA
DO WSZYSTKICH ŚRODOWISK

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 firm.

Rozwiązanie SD WAN dla oddziałów zdalnych

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

Łatwość wdrożenia

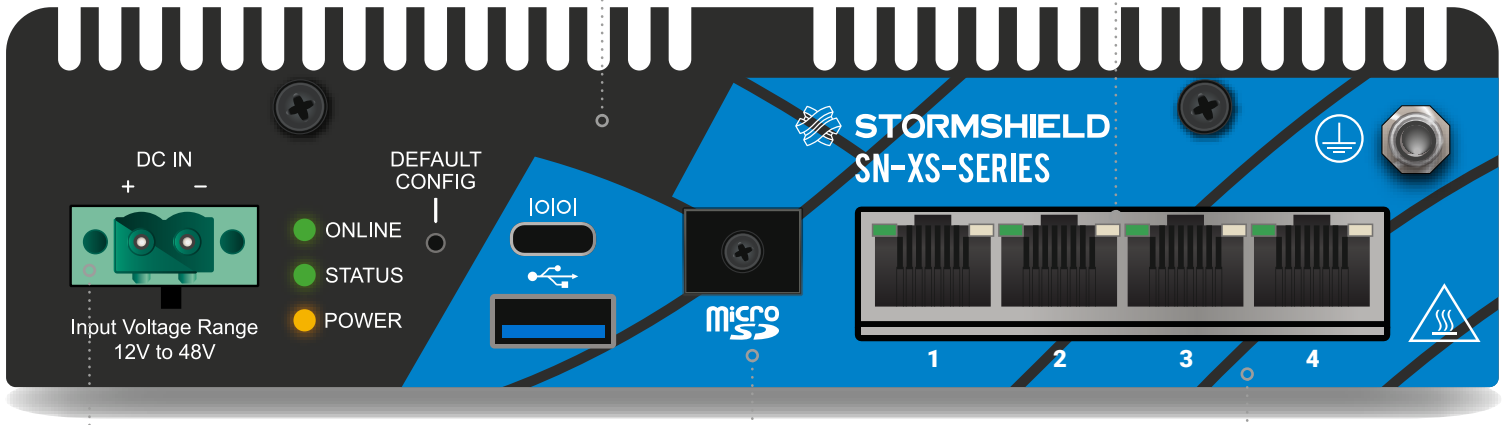
Różne tryby wdrożenia w Twojej sieci (router, transparentny i hybrydowy) należą do najbardziej elastycznych na rynku, zapewniając wysoką elastyczność w zakresie integrowania wielu urządzeń Stormshield, przy jednoczesnym zapewnieniu funkcji bezpieczeństwa.

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.

4 miedziane interfejsy
100/1000/2500

Kompaktowy
rozmiar



Zasilanie
220V - 48V

Przechowywanie logów
Karta microSD

Cicha praca
Bez wentylatorów

WAŻNE INFORMACJE

SN-XS-Series
170

Interfejsy
4
Miedziane interfejsy 2,5 GbE

Przepustowość
8,5 Gbps
Firewall

Przepustowość
2,5 Gbps
Firewall (IMIX)

Wytrzymały
Kompaktowy
Format

VPN
1,8 Gbps
Przepustowość IPSec

VPN
200
Przepustowość SSL

FUNKCJONALNOŚCI

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

SDWAN

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

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 istniejąca architekturą sieciową.**

... 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 użytkowania

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) • Uwierzytelniania 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 interaktywanych (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 opcja 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 anonimizacja 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)

SPECYFIKACJA TECHNICZNA

WYDAJNOŚĆ[1]	170
Przepustowość Firewall (UDP 1518 bytes / IMIX)	**8,5 Gbps**
Przepustowość Firewall (IMIX)	**2,4 Gbps**
Przepustowość IPS (UDP 1518 bytes)	**4 Gbps**
Przepustowość IPS (IMIX)	**1,1 Gbps**
Ochrona przed zagrożeniami*	**400 Mbps**

** 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	170
Przepustowość IPSec - AES-GCM (1464 byte UDP)	**1,8 Gbps**
Przepustowość IPSec - AES-GCM (IMIX)	**850 Mbps**
Maks. liczba tuneli IPSec VPN (1024 kbps na tunel)	**200**
Liczba jednoczesnych połączeń klientów SSL VPN	**200**

POŁĄCZENIA SIECIOWE	170
Liczba jednoczesnych sesji (TCP)	**150 000**
Nowe sesje na sekundę	**25 000**
Maksymalna liczba bram głównych/zapasowych	**64/64**

INTERFEJSY SIECIOWE	170
Liczba interfejsów miedzianych	**4**

SYSTEM	170
Maksymalna liczba reguł filtrowania (rekomendowana / specyficzna konf.)	**1 024 / 2 048**
Maksymalna liczba tras statycznych	**512**
Maksymalna liczba tras dynamicznych	**10 000**
High availability	**Active-Passive**

1 Wydajność mierzona jest w środowisku laboratoryjnym w idealnych warunkach dla wersji 5.x. Wyniki mogą się różnić w zależności od warunków testowych i wersji oprogramowania.

SPRZĘT	170
Partycja na logi	**Karta microSD**
MTBF w 25°C	**50,1 lat**
Montaż	**Szafa rack, szafka, na ścianie lub szynie DIN (szerokość 35mm, standard EN 50022)**
Rozmiar	**Desktop 1U (<1/2 19")**
Wysokość x szerokość x głębokość (mm)	**42 (46 z gumowymi nóżkami) x 165 x 139**
Waga	**1,16 kg (2.56 lbs)**
Zasilanie	**AC: 100-240V 60-50Hz 1.2A max DC: 12-48VDC 3-0,75A**
Pobór energii elektrycznej (w spoczynku/średnio/maksymalnie w Watach (W))	**9 / 10 / 19,9**
Poziom hałasu	**Chłodzenie pasywne (bez wentylatora)**
Rozpraszanie ciepła (w spoczynku/średnio maksymalnie w BTU/h)	**31 / 34 / 80**
Warunki pracy	Temperatura: **-20° do 60°C (-4° do 140°F)** Wilgotność: **0% do 95% @ 60°C (140°F)**
Warunki przechowywania	Temperatura: **-40° do 85°C (-40° do 185°F)** Wilgotność: **0% do 95% @ 60°C (140°F)**

CERTYFIKACJA	170
Zgodność	**CE/FCC/RCM/UKCA/ IEC 61000-4-12/CB/ IEC 60068-2**
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 filterningiem w oparciu o ponad 70 kategorii** podniesie Twoją ochronę do poziomu, który nie ma sobie równych na rynku.

	Essential Security Pack	Premium Security Pack
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

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 roboczego[1].

Spokój dla wszystkich
W ramach tej usługi możesz samodzielnie wymienić sprzęt po zdiagnozowaniu przez nasze wsparcie techniczne usterki[2].

[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.

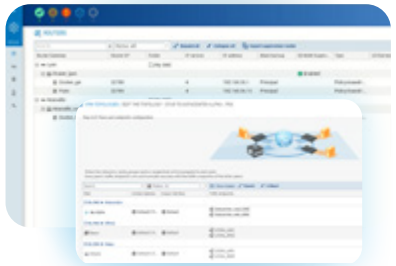
➔ breachfighter.stormshieldcs.eu

ZARZĄDZAJ 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