
STORMSHIELD
ZINTEGROWANY SYSTEM
OCHRONY SIECI KLASY
NEXT GENERATION FIREWALL I UTM

FIREWALL ZINTEGROWANY Z IPS · FILTR URL · ANTYWIRUS · SSL PROXY · SANDBOXING W CHMURZE · GEOLOKALIZACJA · KONTROLA APLIKACJI I URZĄDZEŃ MOBILNYCH · IPSEC VPN · SSL VPN · AUTOMATYCZNY BACKUP KONFIGURACJI · POLSKIE WSPARCIE TECHNICZNE · CENTRALNE ZARZĄDZANIE · RAPORTOWANIE · POLSKI INTERFEJS UŻYTKOWNIKA

STORMSHIELD

KOMPLETNA OCHRONA TWOJEJ SIECI FIRMOWEJ

STORMSHIELD

Firma STORMSHIELD (wcześniej NETASQ) istnieje od 1998 roku i od kilku lat jest członkiem Airbus Group (dawniej European Aeronautic Defence and Space Company - EADS) – koncernu lotniczo-zbrojeniowego. W 2014 roku, wtedy jeszcze firma NETASQ, połączyła się z firmą Arkoon. Produkty NETASQ UTM (Unifed Threat Management) bardzo szybko podbiły rynek europejski, dzięki zastosowaniu unikatowej architektury ASQ (Active Security Qualification), analizującej przesyłane pakiety na poziomie jądra systemu operacyjnego. Dzięki temu produkty STORMSHIELD od lat słyną z wysokiej wydajności i skutecznej ochrony. Innowacyjne podejście sprawiło również, że obecny w rozwiązaniach tego producenta system IPS nie tylko blokuje niebezpieczny ruch, ale również usuwa szkodliwą zawartość z kodu HTML i dostarcza użytkownikom bezpieczne strony WWW.

Rozwiązania STORMSHIELD chronią około 1900 polskich organizacji, w tym m.in. 900 firm, 800 instytucji państwowych, 120 placówek szkolnych oraz 100 placówek medycznych.

UNIKATOWA ARCHITEKTURA SYSTEMU

Elementem wyróżniającym rozwiązania STORMSHIELD jest integracja zapory sieciowej (Stateful Inspection Firewall) z modułem IPS (Intrusion Prevention System) na poziomie jądra systemu operacyjnego. Tak głęboka integracja dwóch kluczowych modułów pozwala na uzyskanie wysokiej wydajności podczas analizy całego pakietu, a więc jego nagłówka i zawartości. W ten sposób urządzenia STORMSHIELD spełniają dwa najważniejsze oczekiwania klientów – skutecznie eliminują niebezpieczny ruch oraz zapewniają wysoką wydajność skanowania.

JAK DZIAŁA IPS DLA HTTP?

Próbę wizyty na zainfekowanej stronie WWW standardowy IPS po prostu zablokuje. IPS dostępny w urządzeniach STORMSHIELD, rozpozna zagrożenia w kodzie HTML, usunie je i dostarczy użytkownikowi bezpieczną witrynę.

OPATENTOWANA TECHNOLOGIA WYKRYWANIA ZAGROŻEŃ

Do wykrywania i blokowania włamań rozwiązania STORMSHIELD wykorzystują unikatową technologię Active Security Qualification (ASQ), która dzięki analizie protokołowej, połączonej z zaawansowaną heurystyką, pozwala na wykrywanie zagrożeń niezależnie od sygnatur (ochrona proaktywna). W ten sposób sieć jest chroniona przed najnowszymi zagrożeniami, dla których sygnatury jeszcze nie powstały, gwarantując ochronę komunikacji sieciowej.

ZBIERANIE LOGÓW NA URZĄDZENIACH

Urządzenia STORMSHIELD posiadają dysk służący do zbierania i przechowywania logów. W mniejszych modelach STORMSHIELD istnieje możliwość bezpośredniego zapisywania logów na karty SD oraz SDHC. To szczególnie przydatna funkcjonalność dla klientów korzystających z najniższych modeli, które nie posiadają wbudowanego dysku twardego.

KONTROLA RUCHU SZYFROWANEGO SSL

Urządzenia STORMSHIELD pozwalają na kontrolę ruchu szyfrowanego za pomocą protokołu SSL. Rozwiązanie działa jako serwer proxy SSL, umożliwiając kontrolę ruchu HTTPS, POP3S oraz SMTPS. Sprawdzanie zaszyfrowanych za pomocą SSL/TLS danych odbywa się po uprzednim zdeszyfrowaniu transmisji. Jeśli przesyłane informacje są bezpieczne, STORMSHIELD ponownie szyfruje dane, podpisuje je własnym certyfikatem i przesyła do użytkownika.

BEZPIECZNA KOMUNIKACJA VPN

Wszystkie urządzenia STORMSHIELD pozwalają na szyfrowanie komunikacji pomiędzy lokalizacjami z użyciem tuneli IPSec, które są konfigurowane z użyciem prostego, graficznego kreatora. Połączenia VPN dla użytkowników mobilnych mogą być budowane z wykorzystaniem protokołu IPSec lub SSL VPN z wykorzystaniem darmowego klienta lub np. aplikacji OpenVPN. Dla klientów wymagających zabezpieczenia ciągłości komunikacji na wypadek awarii łącza, każde urządzenie wyposażono w funkcję VPN failover, dzięki której tunel automatycznie zestawi się na zapasowym łączu, gwarantując nieprzerwaną komunikację.

DWA FILTRY URL

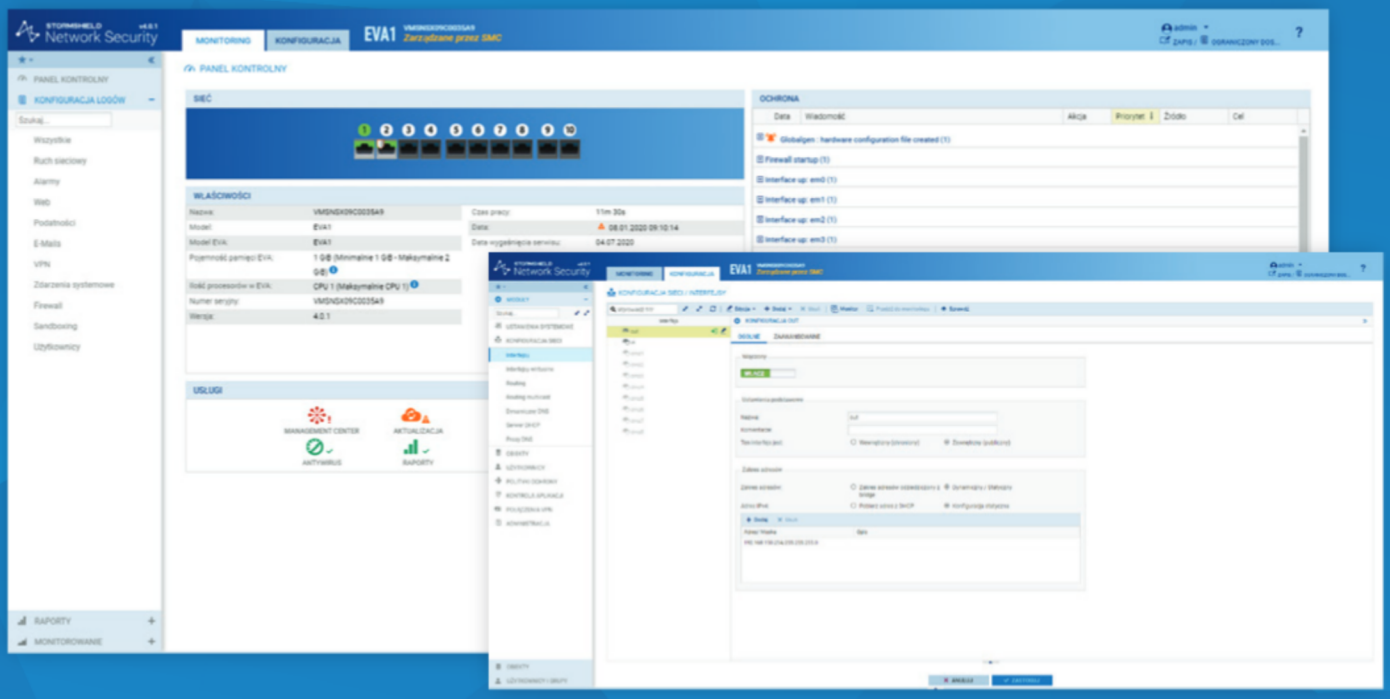
Rozwiązania STORMSHIELD udostępniają dwa filtry URL, pozwalające blokować użytkownikom sieci firmowej dostęp do wybranych stron internetowych (również tych dostępnych przez HTTPS).

Pierwszy filtr URL jest dedykowany dla polskich użytkowników sieci i jest efektem ścisłej współpracy producenta z polskim dystrybutorem. Baza stron internetowych dla tego filtra powstała na podstawie analizy aktywności w Internecie pracowników polskich firm. Filtr dostarcza ponad 50 kategorii tematycznych, według których klasyfikowane są strony. Jeśli jakiejś strony brakuje w klasyfikacji, można ją zgłosić za pomocą specjalnie przygotowanej zakładki na stronie www.stormshield.pl. Zgłoszona w ten sposób strona zostanie sprawdzona i dodana do filtra.

Drugą opcją filtrowania jest chmurowy URL Filtering, zawierający 65 kategorii - razem to ponad 100 mln adresów URL. Zaletą tego filtra jest przeniesienie procesu weryfikacji danego adresu WWW z urządzenia do chmury, niemal całkowicie eliminując wpływ na wydajność rozwiązania STORMSHIELD.

POLITYKI BEZPIECZEŃSTWA W ZALEŻNOŚCI OD UŻYTKOWNIKÓW

Dzięki integracji urządzenia STORMSHIELD z bazami użytkowników Active Directory, LDAP lub wieloma równocześnie, możliwe jest tworzenie polityk bezpieczeństwa z uwzględnieniem użytkowników i grup. Jeśli w sieci firmowej nie ma jeszcze takiej bazy użytkowników, można ją stworzyć z wykorzystaniem urządzenia STORMSHIELD (baza LDAP na urządzeniu).



Interfejs został podzielony na dwie zakładki - Monitoring oraz Konfiguracja. Zaletą takiego podziału interfejsu jest możliwość przełączania się pomiędzy zakładkami, bez utraty stanu obecnej pracy.

ZARZĄDZANIE W JĘZYKU POLSKIM

Każde urządzenie STORMSHIELD konfigurowane jest przez konsolę administracyjną w języku polskim dostępną poprzez przeglądarkę internetową. Polski interfejs użytkownika już od 10 lat doceniają administratorzy sieci w polskich instytucjach i firmach. Dzięki temu, administrowanie rozwiązaniami STORMSHIELD możliwe jest także za pomocą urządzeń mobilnych.

KONTROLA APLIKACJI I URZĄDZEŃ

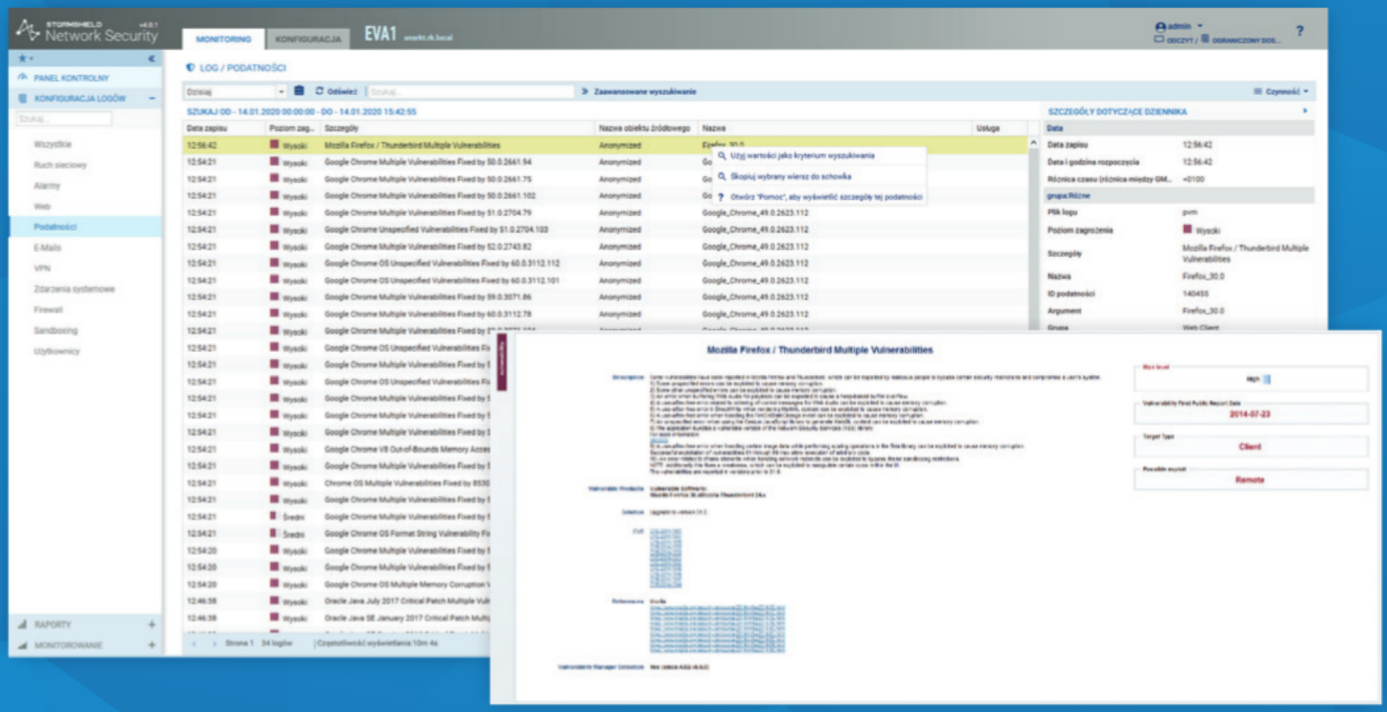
Urządzenia STORMSHIELD pozwalają administratorowi na pełną kontrolę korzystania z aplikacji sieciowych. Dzięki temu możliwe jest m.in. blokowanie niepożądanych w sieci firmowej komunikatorów internetowych (Skype, Gadu-Gadu) oraz aplikacji P2P obciążających łącze. Administrator ma także możliwość kontroli prywatnych urządzeń mobilnych pracowników, wykorzystywanych podczas pracy (tzw. BYOD).

PEŁNY MONITORING SIECI

Rozwiązania STORMSHIELD dają administratorowi możliwość pełnej kontroli chronionej sieci, a dzięki stale rozwijanemu interfejsowi graficznemu, możliwe jest uzyskanie szczegółowych informacji na temat aktywności sieciowych w czasie rzeczywistym. Dodatkowym ułatwieniem dla administratorów jest okno Log Line Details, które w prosty i przejrzysty sposób, pozwala na szczegółowe przeglądanie wszystkich zdarzeń.

SANDBOXING W CHMURZE

Breach Fighter, usługa sandboxingu, która służy do ochrony przed niezidentyfikowanymi dotychczas zagrożeniami różnego typu. Ochrona odbywa się poprzez analizę nierozpoznanych wcześniej plików w odizolowanym, wirtualnym środowisku. Proces ten rozbudowuje skuteczność ochrony antywirusowej urządzenia, wspierając tradycyjną metodę detekcji złośliwych plików. Breach Fighter zwiększa możliwość wykrywania ataków w czasie rzeczywistym dzięki technologii opartej na behawioralnej analizie uruchamianego pliku.



Audyt Podatności działa na dwa sposoby – identyfikuje aplikacje, z których korzystają na co dzień użytkownicy sieci firmowej oraz wskazuje luki w tych aplikacjach, przyczyniając się do eliminowania podatności sieci firmowej na ataki.

AUDYT PODATNOŚCI WYKRYWA APLIKACJE SIECIOWE

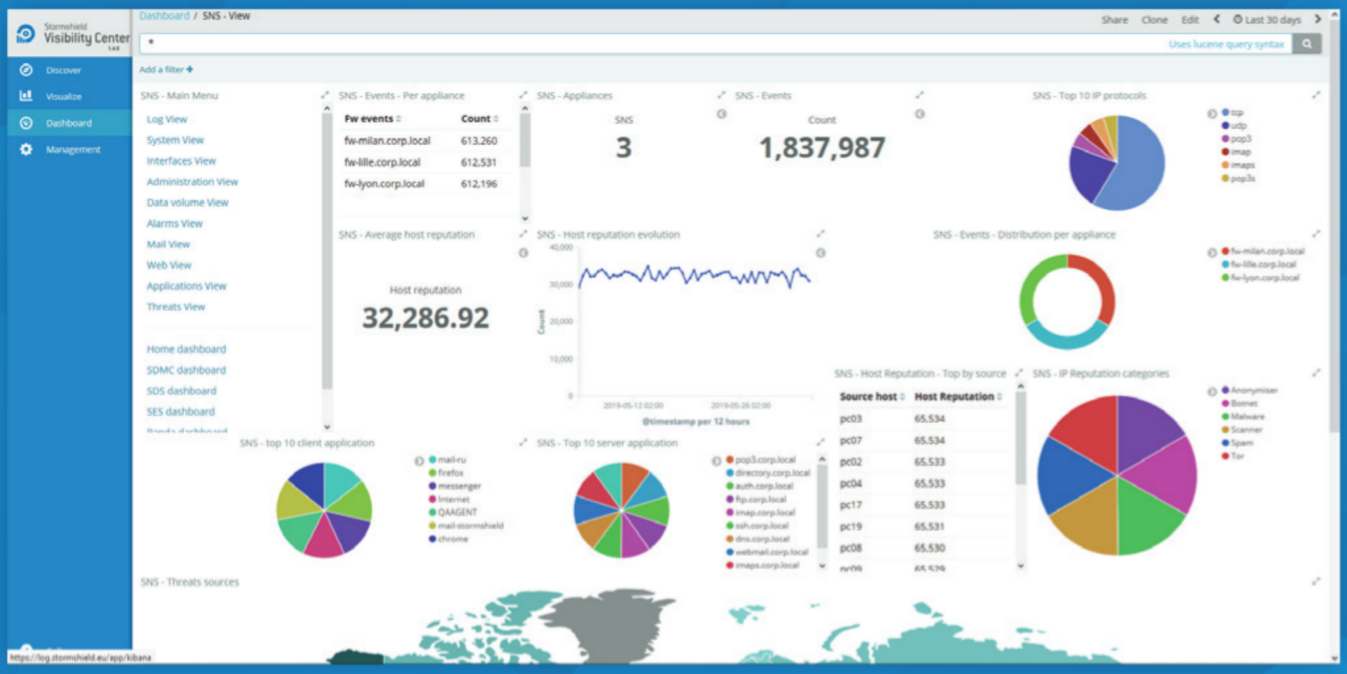
Audyt Podatności, dostępny w rozwiązaniach STORMSHIELD, prezentuje administratorowi szczegółową listę aplikacji sieciowych pracujących na stacjach roboczych, np. Google Desktop, Firefox, programy antywirusowe itp. Kliknięcie na wskazaną aplikację powoduje wyświetlenie wszystkich komputerów, na których dany program został zainstalowany, a także pozwala sprawdzić wersję konkretnej aplikacji i systemu pod jakim działa wybrana stacja.

Audyt działa każdorazowo, gdy komputer lub serwer z sieci LAN generuje ruch, który jest sprawdzany przez urządzenie STORMSHIELD. Ruch taki jest filtrowany przez firewall i IPS, dzięki czemu identyfikowana jest aplikacja inicjującą dany ruch. Następnie taka aplikacja jest sprawdzana pod kątem znanych luk i podatności na ataki.

W podstawowej cenie urządzenia STORMSHIELD administrator otrzymuje dwa narzędzia do raportowania - STORMSHIELD Visibility Center oraz raporty TOP 10.

GEOLOKALIZACJA – FILTROWANIE OPARTE O LOKALIZACJĘ HOSTA

Dzięki funkcji geolokalizacji administrator wie nie tylko z jakimi źródłowymi i docelowymi adresami IP nawiązywane są połączenia, ale również, gdzie fizycznie znajdują się urządzenia, do których przypisane są te adresy. Geoobiekty pozwalają również na tworzenie polityk filtrowania według kraju czy kontynentu, powiązanego z adresem IP połączenia, co pozwala zablokować komunikację użytkowników z serwerami znajdującymi się w innych krajach czy kontynentach.



STORMSHIELD Visibility Center

RAPORTOWANIE (STORMSHIELD VISIBILITY CENTER)

STORMSHIELD Visibility Center to system gromadzenia i przeglądania logów, a także generowania raportów na podstawie zebranych danych. Narzędzie dostępne jest w postaci maszyny wirtualnej i pozwala na równoległe zbieranie logów z wielu urządzeń.

CENTRALNE ZARZĄDZANIE

Zarządzanie wieloma urządzeniami STORMSHIELD możliwe jest dzięki konsoli STORMSHIELD Management Center, posiadającej podobny interfejs użytkownika co każde urządzenie STORMSHIELD. Administrator może zarządzać wieloma urządzeniami wybierając interfejs w języku polskim. Dzięki temu administracja wieloma rozwiązaniami STORMSHIELD jest wyjątkowo intuicyjna i nie wymaga wertowania dodatkowej dokumentacji. Z pomocą konsoli administrator może uzyskać bezpośredni dostęp do swoich urządzeń, bez konieczności konfigurowania dostępu z zewnątrz, czy tworzenia dedykowanego połączenia VPN.

STORMSHIELD ELASTIC VIRTUAL APPLIANCE

Rozwiązania STORMSHIELD dostępne są zarówno w wersji sprzętowej jak i zwirtualizowanej (na platformach MS Hyper-V, VMWare, KVM, Citrix, Microsoft Azure oraz Amazon Web Services). Obie wersje stanowią identycznie skuteczne zabezpieczenie chronionej sieci i mogą być administrowane z poziomu przeglądarki internetowej. Co ważne, istnieje możliwość przenoszenia konfiguracji pomiędzy wersją sprzętową oraz zwirtualizowaną. STORMSHIELD Elastic Virtual Appliance zapewnia skuteczną ochronę zarówno pomiędzy maszynami wirtualnymi, jak i w fizycznej części sieci.

OCHRONA SIECI PRZEMYSŁOWYCH

Rozwiązania STORMSHIELD zabezpieczają sieci informatyczne, ale również sieci przemysłowe. Modele SNi20 i SNi40 dedykowane sieciom przemysłowym są doskonale przystosowane do pracy w trudnych warunkach, gdzie panuje wysoka lub niska temperatura, występują wstrząsy, jest pył czy pojawiają się zakłócenia elektromagnetyczne. Urządzenia można zainstalować na szynie DIN. Dzięki funkcji Hardware Bypass urządzenia nie zablokują ruchu sieciowego i nie zakłócą działania sieci przemysłowej nawet w sytuacji własnej awarii lub zaników prądu. Urządzenia potrafią zabezpieczać protokoły przemysłowe: Modbus, S7, OPC UA, EtherNet/IP, IEC 60870-5-104, OPC CLASSIC (DA/HDA/AE), UMAS, oraz BACnet/IP.

OPCJE SERWISOWE STORMSHIELD

OCHRONA SIECI IT

	NGFW + IPS	IPSec + SSL VPN	Audyt Podatności	Antywirus	Filtr URL	Antyspam
Remote Office Security Pack SN160, SN160W, SN210, SN210W	✓	✓	✗	✗	✗	✗
Premium UTM Security Pack WSZYSTKIE MODELE	✓	✓	✓	✓ Kaspersky AV	✓ Chmurowy filtr URL 65 kategorii	✓
UTM Security Pack SN160, SN160W, SN210, SN210W, SN310, SN510, SN710, SN910, SN2000, SN3000, SN2100, SN3100	✓	✓	✗	✓ Clam AV	✓ Polski filtr URL 50 kategorii	✓
Enterprise Security Pack SN2000, SN3000, SN6000, SN2100, SN3100, SN6100	✓	✓	✓	✗	✗	✗

Cztery dostępne opcje serwisowe pozwalają dobrać funkcjonalności STORMSHIELD do potrzeb danej sieci firmowej.
Każdy z serwisów można w dowolnym momencie rozszerzyć, dokupując brakujące funkcjonalności.

OCHRONA SIECI PRZEMYSŁOWYCH

	NGFW + IPS	IPSec + SSL VPN	Audyt Podatności	Antywirus	Filtr URL	Antyspam
Industrial Security Pack SNi20, SNi40	✓	✓	✗	✗	✗	✗
Industrial Plus Security Pack SNi20, SNi40	✓	✓	✓	✗	✗	✗

Opcje serwisowe Industrial Pack przeznaczone są dla sieci przemysłowych i dostępne są dla modeli SNi20 i SNi40.
Serwisów Industrial Pack nie można rozszerzać o dodatkowe funkcjonalności.

SPECYFIKACJA ROZWIĄZAŃ SPRZĘTOWYCH

	MAŁE SIECI					SIECI PRZEMYSŁOWE	
	SN160	**SN210**	**SN310**	**SN160W**	**SN210W**	**SNi20**	**SNi40**
WYDAJNOŚĆ (Gbps)*							
Firewall	1	2	4	1	2	2,4	4,8
Firewall + IPS (1518-bajtowa ramka danych)	1	1,6	2,4	1	1,6	1,6	2,9
ŁĄCZNOŚĆ SIECIOWA							
Liczba jednoczesnych sesji	150 000	200 000	300 000	150 000	200 000	500 000	500 000
Nowe sesje / sekundę	7 500	15 000	18 000	7 500	15 000	20 000	20 000
802.1Q VLAN (Max)	64	64	64	64	64	64	64
VPN (Mbps)							
Przepustowość IPSec	200	350	600	200	350	600	1 100
Liczba tuneli IPSec VPN	50	50	100	50	50	100	500
Liczba tuneli SSL VPN (full)	5	20	20	5	20	50	100
HIGH AVAILABILITY (HA)							
Active / passive	-	-	✔	-	-	✔	-
ANTYWIRUS (Mbps)							
Przepustowość	260	400	495	260	400	-	-
SPRZĘT							
Interfejsy 10/100/1000	1 + 4 porty (switch)	2 + 6 portów (switch)	8	1 + 4 porty (switch)	2 + 6 portów (switch)	2 + 4	5
Protokół / Uwierzytelnianie	-	-	-	802.11 a/b/g/n WPA/WPA2	802.11 a/b/g/n WPA/WPA2	-	-
Pamięć wewnętrzna	karta SD**	karta SD**	karta SD**	karta SD**	karta SD**	karta SD**	32 GB SSD
Wielkość urządzenia (mm)	45x176 x107	46x210 x195	46x210 x195	45x176 x150	46x210 x240	210x60 x155	165x80 x145

	ŚREDNIE SIECI			DUŻE SIECI		
	SN510	**SN710**	**SN910**	**SN2100**	**SN3100**	**SN6100**
WYDAJNOŚĆ (Gbps)*						
Firewall	8	15	30	60	74	170
IPS (1518 bajtów UDP)	3,3	8	15	35	55	68
IPS (plik HTTP 1MB)	1,7	3	10	20	23	27
ŁĄCZNOŚĆ SIECIOWA						
Liczba jednoczesnych sesji	500 000	1 000 000	1 500 000	2 500 000	5 000 000	20 000 000
Nowe sesje / sekundę	25 000	50 000	80 000	125 000	175 000	250 000
VPN (Mbps)						
Przepustowość IPSec	1 300	3 000	4 500	10 000	15 000	20 000
Liczba tuneli IPSec VPN	500	1 000	1 000	5 000	5 000	10 000
Liczba tuneli SSL VPN (full)	100	150	150	400	500	500
HIGH AVAILABILITY (HA)						
Active / passive	✔	✔	✔	✔	✔	✔
ANTYWIRUS (Mbps)						
Przepustowość	950	2 000	2 900	7 000	10 000	12 500
SPRZĘT						
Interfejsy 10/100/1000	12	8-16	8-16	2-26	2-26	8-64
Interfejsy miedziane 10 Gb	-	0-4	0-4	0-12	0-12	0-32
Światłowód 1 Gb / 10 Gb / 40 Gb	-	0-8 / 0-4 / -	2-10 / 0-4 / -	0-24 / 0-12 / 0-6	0-24 / 0-12 / 0-6	0-64 / 2-34 / 0-16
Pamięć wewnętrzna	> 200 GB	> 200 GB	120 GB	256 GB SSD	256 GB SSD	512 GB SSD
Wielkość urządzenia (mm)	1U - 19"	1U - 19"	1U - 19"	1U - 19"	1U - 19"	2U - 19"

** Test przeprowadzony w warunkach laboratoryjnych. Wyniki mogą różnić się w zależności od warunków testowych oraz wersji oprogramowania.*

*** Opcjonalnie (wymaga karty)* **** Rozmiar IP: 60% (48 bajtów) - 25% (494 bajtów) - 15% (1500 bajtów)*

POLSKA POMOC TECHNICZNA

Użytkownicy rozwiązań STORMSHIELD z aktywną licencją (serwisem) mogą bezpłatnie korzystać z pomocy technicznej w języku polskim. Pomoc świadczą wykwalifikowani inżynierowie, z którymi można kontaktować się w dni robocze, w godzinach 8:00 - 18:00, telefonicznie (32 259 11 89) lub pisząc na adres: pomoc@stormshield.pl.

CHCESZ DOWIEDZIEĆ SIĘ WIĘCEJ O TECHNOLOGII STORMSHIELD?

Wejdź na stronę **www.stormshield.pl**, aby:

- wypełnić formularz z prośbą o **bezpłatne wypożyczenie urządzenia do testów**
- **przetestować online demonstracyjną wersję** urządzenia
- zarejestrować się na **bezpłatną eKonferencję** prowadzoną przez inżyniera technicznego, który zdalnie przedstawi funkcjonalność STORMSHIELD

STORMSHIELD

Dystrybucja STORMSHIELD w Polsce:

DAGMA Bezpieczeństwo IT

ul. Bażantów 4/2 | 40-668 Katowice

tel. 32 259 11 00 | handel@dagma.pl

www.stormshield.pl