NETASQ | STORMSHIELD

ZINTEGROWANY SYSTEM OCHRONY SIECI

FUNKCJONALNOŚCI

Firewall zintegrowany z IPS | Filtr URL | Antywirus | IPSec i SSL VPN | Zarządzanie i dwa moduły raportujące w języku polskim | Polskie wsparcie techniczne | Kontrola aplikacji i urządzeń mobilnych Wsparcie IPv6 | Proxy | SSL Proxy | HTTP Proxy cache | Automatyczny backup konfiguracji

STORMSHIELD – NOWA SERIA URZĄDZEŃ UTM OD NETASQ

NETASQ | STORMSHIELD

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 wobec tego typu urządzeń – skutecznie eliminują niebezpieczny ruch oraz zapewniają wysoką wydajność skanowania.

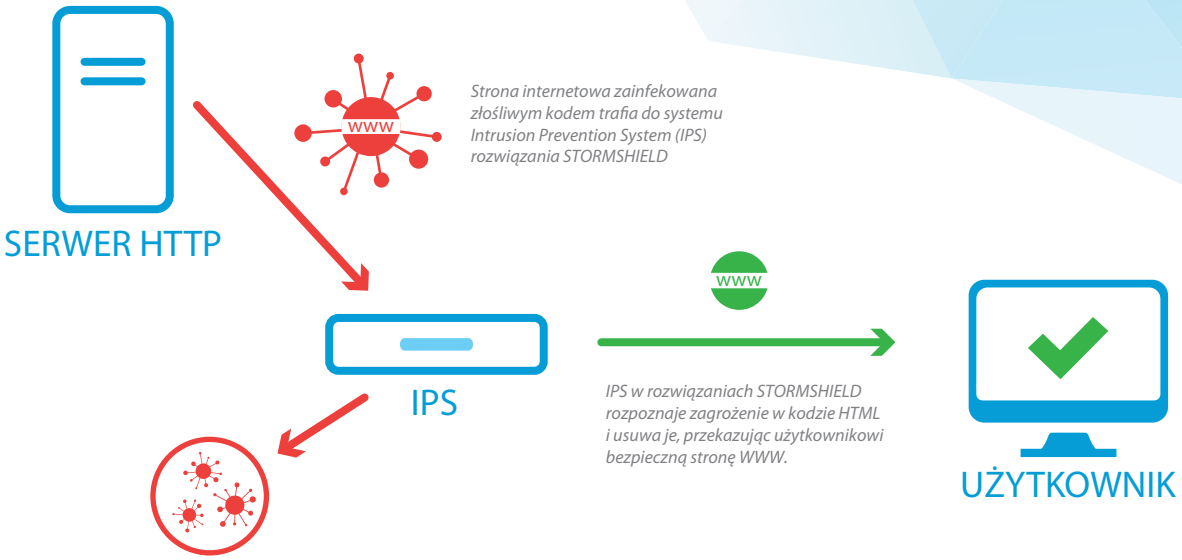
Opatentowana technologia wykrywania zagrożeń

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 pełną ochronę komunikacji sieciowej.

Obsługa kart SD

Rozwiązania STORMSHIELD dają możliwość bezpośredniego zapisywania logów na karty SD oraz SDHC o maksymalnej pojemności 32 GB. To szczególnie przydatna funkcjonalność dla klientów korzystających z modeli SN200 oraz SN300, które nie posiadają wbudowanego dysku twardego.

Jak działa system IPS w STORMSHIELD



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

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, SMTPS oraz FTPS. Sprawdzanie zakodowanych w SSL 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

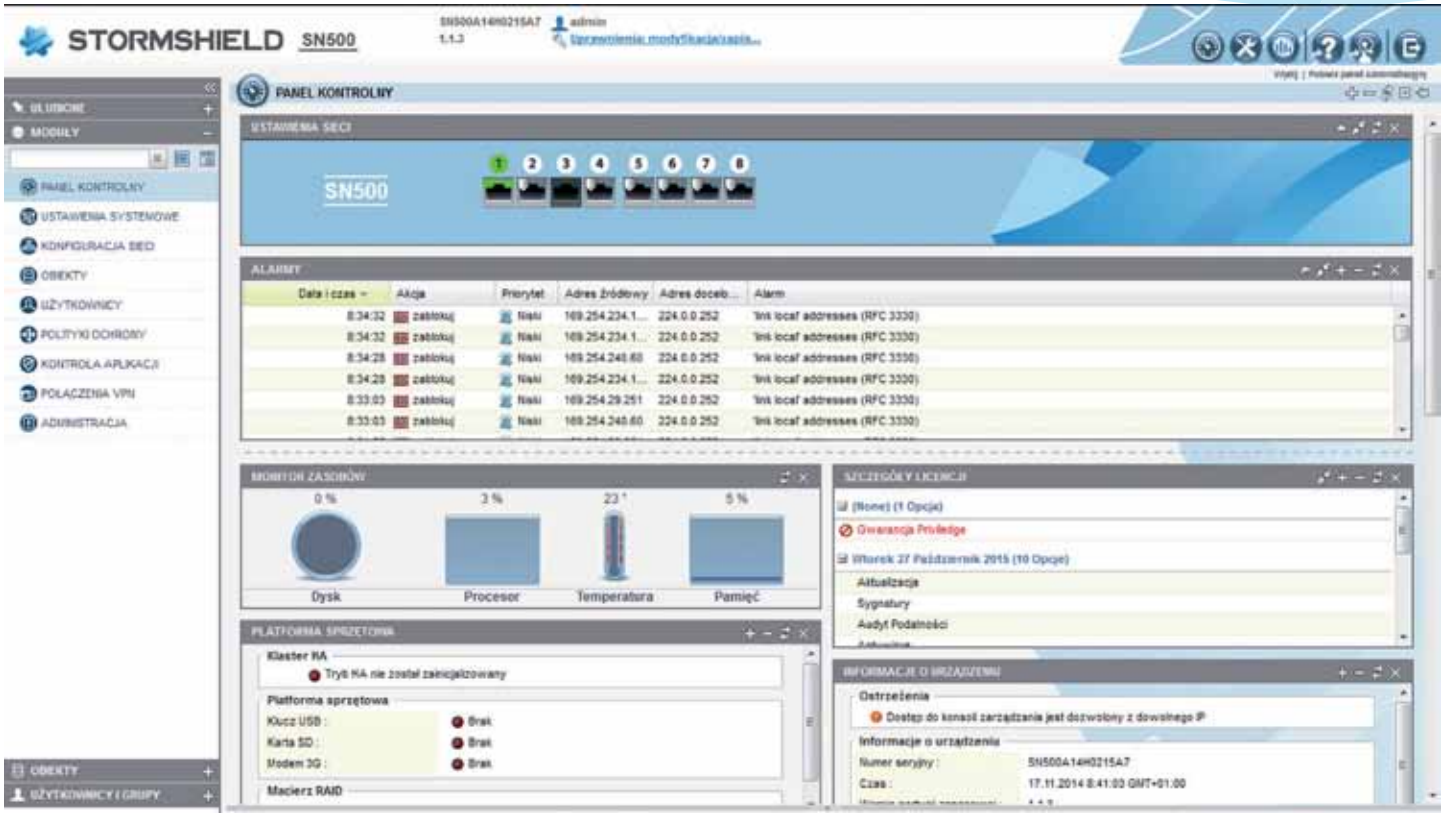
Wszystkie urządzenia STORMSHIELD pozwalają na szyfrowanie komunikacji pomiędzy lokalizacjami oraz zabezpieczanie zdalnego dostępu do zasobów firmy, protokołami IPSec VPN oraz SSL VPN. W wypadku SSL VPN użytkownik zyskuje dostęp do wszystkich usług i zasobów sieci za pomocą bezpłatnej aplikacji. Dla klientów 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 w kolejnym dniu roboczym.

Drugą opcją filtrowania jest rozszerzony filtr URL przechowywany w chmurze, 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.



Konsola zarządzająca urządzeniami STORMSHIELD dostępna jest w języku polskim z poziomu przeglądarki WWW. Wyświetlane treści można dowolnie organizować - poszczególne funkcjonalności mogą być przemieszczane metodą „przeciągnij i upuść". Ta sama metoda pozwala na szybką konfigurację zestawu reguł firewalla.

Zarządzanie w języku polskim

Każde urządzenie STORMSHIELD konfigurowane jest przez konsolę administracyjną w języku polskim, dostępną przez przeglądarkę internetową. Dzięki temu, administrowanie rozwiązaniami STORMSHIELD możliwe jest także za pomocą urządzeń mobilnych.

Polityki bezpieczeństwa w zależności od użytkowników

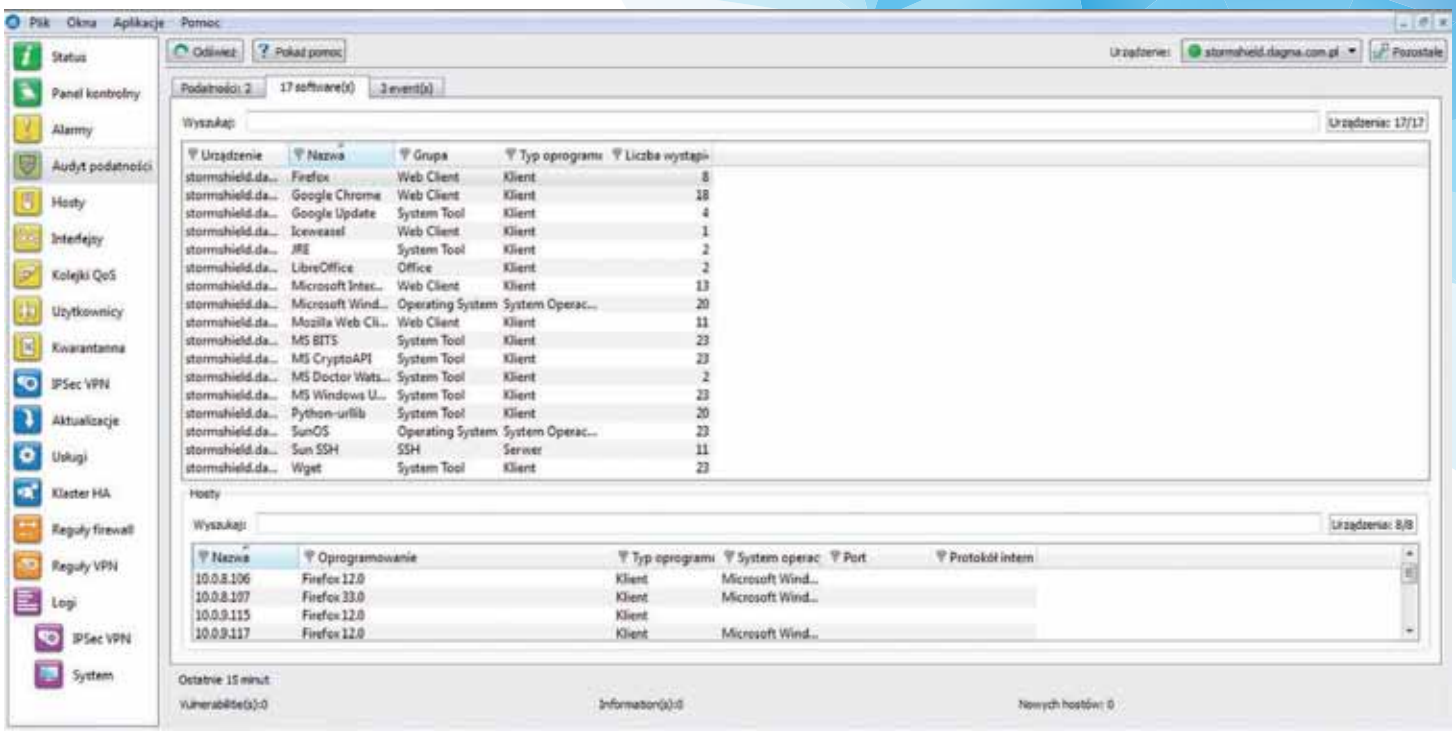
Dzięki integracji urządzenia STORMSHIELD z bazami użytkowników Active Directory lub LDAP, możliwe jest tworzenie polityk bezpieczeństwa z uwzględnieniem użytkowników i grup. Jeśli w sieci firmowej nie ma jeszcze takiej bazy użytkowników, można ją stworzyć z wykorzystaniem urządzenia STORMSHIELD (baza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

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) – wszystko dzięki modułowi, pozwalającemu na blokowanie dostępu do sieci firmowej z urządzeń mobilnych.

Pełny monitoring sieci

Rozwiązania STORMSHIELD dają administratorowi możliwość pełnej kontroli chronionej sieci. Dzięki aplikacji Real Time Monitor możliwe jest kontrolowanie wszystkich zdarzeń w czasie rzeczywistym. Narzędzie pozwala na śledzenie aktywności poszczególnych użytkowników sieci firmowej i kontrolę transmisji danych.
STORMSHIELD umożliwia administratorowi kontrolę wybranych aplikacji sieciowych, takich jak komunikatory internetowe, programy P2P, a także aplikacje dostępne w serwisie Facebook.



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.

Wykrywanie podatności

Audyt Podatności to narzędzie, które pomaga administratorowi w kontroli aplikacji sieciowych, z których na co dzień korzystają użytkownicy. Narzędzie pomaga monitorować bezpieczeństwo samej sieci, poprzez wykrywanie i wskazywanie wersji oprogramowania, w którym wykryto luki, wrażliwości czy podatności na ataki. 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 inicjująca dany ruch. Następnie taka aplikacja jest sprawdzana pod kątem wykrytych luk i podatności na ataki.

Audyt Podatności – korzyści

- wykrywanie aplikacji sieciowych zainstalowanych na stacjach roboczych i serwerach
- wykrywanie aplikacji podatnych na ataki
- podpowiadanie niezbędnych działań
- brak wpływu na wydajność systemu
- brak konieczności instalowania agentów na stacjach

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 system pod jakim działa wybrana stacja.

Audyt Podatności wykrywa i prezentuje szczegółową listę aplikacji sieciowych m.in. Lotus Domino, Apple iTunes, Samba, Apache, MySQL, Mozilla Thunderbird, Skype i wiele innych.

Dwa moduły raportujące w standardzie

Urządzenia STORMSHIELD udostępniają dwa moduły z podstawowymi raportami z aktywności użytkowników w chronionej sieci. Pierwszy z nich jest dostępny z poziomu interfejsu urządzenia. Pozwala na korzystanie z 27 raportów TOP 10, tworzonych w oparciu o logi zapisywane na urządzeniu. Z poziomu wygenerowanego raportu możliwa jest zmiana reguł bezpośrednio na firewallu.

Drugi, Event Reporter Light, jest modułem raportującym, który umożliwia przeglądanie z poziomu przeglądarki WWW raportów nt. najczęściej odwiedzanych stron internetowych, generowanych alarmów systemu IPS oraz luk w aplikacjach sieciowych. Raporty można pobrać w postaci plików PDF i CSV.

STORMSHIELD Event Analyzer

To dodatkowe narzędzie, które dostarcza komplet informacji na temat stanu zabezpieczenia sieci, wykrytych infekcji, prób włamań do sieci, generowanego obciążenia czy identyfikacji niedozwolonych aplikacji sieciowych. Dzięki interaktywnym raportom STORMSHIELD Event Analyzer może informować, m.in. o średnim czasie spędzonym przez pracownika na poszczególnych stronach, najczęściej wpisywanych w wyszukiwarkach frazach czy ilości pobranych danych.

Dzięki STORMSHIELD Event Analyzer administrator może w łatwy sposób monitorować skuteczność ustalonych polityk bezpieczeństwa i generować raporty w oparciu o 200 zdefiniowanych przez producenta wzorów. Raporty powstają na podstawie logów przechowywanych w bazie Microsoft SQL i można je udostępniać za pośrednictwem usługi RSS.

W podstawowej cenie urządzenia STORMSHIELD administrator otrzymuje narzędzie do raportowania - Event Reporter Light oraz raporty TOP 10.

Opcje serwisowe **NETASQ STORMSHIELD**

	NGFW + IPS	IPSec + SSL VPN	Audyt Podatności	Antywirus	Filtr URL	Antyspam
Remote Office Security Pack SN150, SN200	✓	✓	✗	✗	✗	✗
Enterprise Security Pack SN2000, SN3000, SN6000	✓	✓	✓	✗	✗	✗
UTM Security Pack SN200, SN300, SN500, SN700, SN900, SN2000, SN3000	✓	✓	✗	✓ Clam AV	✓ Polski filtr URL 50 kategorii	✓
Premium UTM Security Pack WSZYSTKIE MODELE	✓	✓	✓	✓ Kaspersky AV	✓ Chmurowy filtr URL 65 kategorii	✓

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

STORMSHIELD Virtual Appliance

Rozwiązania STORMSHIELD dostępne są zarówno w wersji sprzętowej jak i zwirtualizowanej (na platformach VMware oraz Citrix). 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 Virtual Appliance zapewnia skuteczną ochronę zarówno pomiędzy maszynami wirtualnymi, jak i w fizycznej części sieci.

Specyfikacja rozwiązań wirtualnych

	Dla sieci					Dla chmury	
GŁÓWNE CECHY	V50	V100	V200	V500	VU	VS5	VS10
Chronione adresy IP	50	100	200	500	nielimitowane	5	10
Audyt podatności	opcjonalnie	opcjonalnie	opcjonalnie	opcjonalnie	opcjonalnie	✔	✔
Liczba jednoczesnych sesji	100 000	200 000	400 000	600 000	3 000 000	1 000 000	2 000 000
802.1Q VLANs (max)	128	128	128	128	512	512	512
Tunele IPSec VPN (max)	100	500	1 000	1 000	10 000	10 000	10 000
Równoczesne połączenia SSL VPN	20	35	70	175	500	500	500

Specyfikacja rozwiązań sprzętowych

	Małe firmy, agencje, filie			Firmy średniej wielkości, agencje				Duże firmy, centra danych		
	SN150	SN200 (odpowiednik U30S)	SN300 (odpowiednik U70S)	SN500 (odpowiednik U150S)	SN700 (odpowiednik U250S)	SN900 (odpowiednik U500S)	SN910	SN2000	SN3000	SN6000
WYDAJNOŚĆ (Gbps)*										
Firewall	0,4	0,6	0,8	1	2	4	20	25	50	80
Firewall + IPS (1518-bajtowa ramka danych)	0,2	0,5	0,7	1	2	3	12,5	9	14	18
Firewall + IPS (pliki HTTP 1 MB)	0,150	0,4	0,6	0,8	1,2	1,4	7	4	6	8
ŁĄCZNOŚĆ SIECIOWA										
Liczba jednoczesnych sesji	30 000	75 000	150 000	250 000	600 000	1 200 000	1 500 000	2 000 000	2 500 000	10 000 000
Nowe sesje / sekundę	2 500	15 000	18 000	20 000	22 000	25 000	60 000	90 000	120 000	180 000
802.1Q VLAN (Max)	64	64	64	256	256	512	512	512	1 024	1 024
Liczba ISP	4	4	4	8	8	8	12	8	12	12
VPN (Mbps)										
Przepustowość IPSec	80	250	300	500	650	800	4 000	3 000	4 500	6 000
HIGH AVAILABILITY (HA)										
Active / passive	-	-	✔	✔	✔	✔	✔	✔	✔	✔
ANTYWIRUS (Mbps)										
Przepustowość HTTP	30	125	150	200	250	300	1 800	3 000	3 250	3 300
SPRZĘT										
Interfejsy 10/100/1000	1 + 4 porty (switch)	1 + 2x2 porty (switch)	8	8	12	12	8-16	10-26	10-26	10-58
Światłowód 1GB lub 10GB (opcja)	-	-	-	-	-	2 x 1GB	6 x 1GB / 2 x 10GB	8	8	28
Pamięć wewnętrzna	-	karta SD**	karta SD**	120GB	120GB	120GB	120GB SSD	128GB SSD	128GB SSD	256GB SSD
Wielkość urządzenia (mm)	37x176x107	44,5x210x195	44,5x210x195	1U - 19"	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 SD oraz rozszerzenia licencji).

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 8-18, telefonicznie 32 259 11 89 lub pisząc na adres pomoc@stormshield.pl.

O firmie NETASQ – producencie STORMSHIELD

Rozwiązania STORMSHIELD tworzone są przez firmę NETASQ, która 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 NETASQ połączyła się z firmą Arkoon. Produkty Unified Threat Management (UTM) firmy NETASQ bardzo szybko podbiły rynek europejski, dzięki zastosowaniu unikatowej architektury ASQ (Active Security Qualification), analizującej przesyłane pakiety na poziomie jądra systemu operacyjnego. Dzięki temu produkty NETASQ 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. Na doświadczeniach i unikatowych rozwiązaniach firmy NETASQ bazują najnowsze urządzenia STORMSHIELD. Rozwiązaniami firmy NETASQ chronią swoje sieci m.in. Unia Europejska, NATO, Orange, Carrefour czy Renault.

Dystrybucja NETASQ STORMSHIELD w Polsce:
DAGMA Biuro Bezpieczeństwa IT | ul. Bażantów 4/2 | 40-668 Katowice
tel. 32 259 11 00 | faks 32 793 11 90
www.stormshield.pl