



STORMSHIELD



DLA MAŁYCH FIRM

ZADBAJ O BEZPIECZEŃSTWO SIECI FIRMOWEJ

Stormshield SN160

BEZPIECZEŃSTWO SIECI | BEZPIECZEŃSTWO DANYCH

Stormshield SN160

IDEALNE ROZWIĄZANIE DLA MAŁYCH FIRM I NIEWIELKICH BIUR LUB ODDZIAŁÓW.



WYJĄTKOWO SKUTECZNA OCHRONA

SN160 zawiera wszystkie zabezpieczenia, niezbędne do skutecznej ochrony sieci w niewielkich firmach.



BEZPIECZNE POŁĄCZENIE Z FIRMA

Dzięki funkcji IPSec VPN i SSL VPN możliwe jest przydzielanie bezpiecznego dostępu do zasobów firmowych pracownikom, którzy znajdują się poza siedzibą firmy.



KONFIGURACJA W ZALEDWIE 3 MINUTY

Intuicyjny przewodnik poprowadzi Cię przez każdy etap instalacji i pozwoli optymalnie skonfigurować Twoje urządzenie w zaledwie kilka minut.

ODDZIAŁY, AGENCJE
ORAZ NIEWIELKIE BIURA

Zapewnij ciągłość działania swojej firmie

Różnorodność technologii zastosowana w urządzeniach STORMSHIELD pozwala skutecznie reagować nawet na najbardziej wyrafinowane ataki.

Oszczędzaj czas

Interfejs administracyjny STORMSHIELD został zaprojektowany tak, aby ergonomicznie i intuicyjnie pomóc w zapewnieniu bezpieczeństwa sieci firmowej szybko i bezbłędnie.

Kontroluj sposób wykorzystania sieci

Dzięki zaawansowanej funkcji filtrowania ruchu i zarządzania usługami, możesz sam zdefiniować, do jakich zasobów w Internecie będą mieli dostęp Twoi pracownicy.

.....

KONTROLA WYKORZYSTANIA SIECI

Firewall/IPS/IDS, firewall aplikacyjny, filtrowanie Microsoft Services, wykrywanie i kontrola wykorzystywanych urządzeń mobilnych, przegląd aplikacji (opcja), wykrywanie podatności (opcja), filtrowanie operacje o lokalizację (kraje, kontynenty), filtrowanie adresów URL (filtr chmurowy), transparentne uwierzytelnianie (Active Directory SSO agenta, SSL, SPNEGO), uwierzytelnianie wielu użytkowników w trybie cookies (Citrix-TSE), uwierzytelnianie w trybie gościa, filtrowanie zgodne z harmonogramem.

OCHRONA PRZED ZAGROŻENIAMI

Zapobieganie włamaniom, skanowanie protokołów, kontrola 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, interaktywne wykrywanie 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), dekodowanie i kontrola ruchu szyfrowanego SSL, ochrona VoIP (SIP).

POUFNOŚĆ

Site-to-site lub Client-to-site IPSec VPN, zdalny tunel SSL VPN w trybie Multi-OS (Windows, Android, iOS, itp.), centralnie 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, uwierzytelnianie w wielu domenach (w tym wewnętrzny LDAP), routing oparty na regułach (PBR), zarządzanie QoS, DHCP klient / relay / serwer, klient NTP, DNS proxy, HTTP proxy cache, IPFIX / NetFlow.

ZARZĄDZANIE

Przeglądarkowy interfejs zarządzania WEBGUI, obiektowe zarządzanie polityką filtrowania, licznik użycia reguł, analizator poprawności reguł, ponad 15 kreatorów instalacji, 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, automatyczne tworzenie kopii zapasowych konfiguracji.

Dokument nie jest umową. Wymienione funkcje dotyczą wersji oprogramowania 3.X.

* Test przeprowadzony w warunkach laboratoryjnych dla oprogramowania w wersji 3.1. Wyniki mogą różnić się w zależności od warunków testowych oraz wersji oprogramowania.

** Opcjonalnie

Specyfikacja techniczna

WYDAJNOŚĆ*

| | |
|--|----------|
| Firewall | 1 Gbps |
| Firewall + IPS (1518-bajtowa ramka danych) | 800 Mbps |
| Firewall + IPS (pliki HTTP 1 MB) | 400 Mbps |
| Antywirus | 100 Mbps |

VPN*

| | |
|---------------------------------------|----------|
| Przepustowość IPSec AES 128 | 200 Mbps |
| Przepustowość IPSec AES 256 | 200 Mbps |
| Liczba tuneli IPSec | 50 |
| Liczba klientów SSL VPN (tryb Portal) | 20 |
| Liczba tuneli SSL VPN | 5 |

POŁĄCZENIA SIECIOWE

| | |
|--|---------|
| Liczba równoczesnych sesji | 150,000 |
| Nowe sesje / sekundę | 6,000 |
| Maksymalna liczba dostawców internetu | 64 |
| Liczba interfejsów wirtualnych (VLAN, Dialup itp.) | 100 |

PARAMETRY SPRZĘTOWE

| | |
|---------------------------------|---------------------|
| Interfejsy Ethernet 10/100/1000 | 1+ 4 porty (switch) |
|---------------------------------|---------------------|

SYSTEM

| | |
|-------------------------------------|-------|
| Maksymalna liczba reguł firewall | 4,096 |
| Maksymalna liczba tras statycznych | 512 |
| Maksymalna liczba tras dynamicznych | 1,000 |

REDUNDANCJA

| | |
|------------------------------------|---|
| High Availability (Active/Passive) | - |
|------------------------------------|---|

SPRZĘT

| | |
|--|--------------------------------------|
| Pamięć wewnętrzna | Karta SD** |
| MTBF (lata) | 24.9 |
| Wysokość x Szerokość x Głębokość (mm) | 45 x 176 x 107 |
| Waga | 0.55 kg |
| Opakowanie: Wysokość x Szerokość x Głębokość (mm) | 78 x 320 x 200 |
| Waga z opakowaniem | 1.2 kg |
| Zasilanie (AC) | 100-240V 60-50Hz 1.5-0.8A |
| Pobór energii | 230V 50Hz 8.4W 0.07A |
| Poziom głośności | bez wentylatora (chłodzenie pasywne) |
| Rozpraszanie ciepła | 35 (max, BTU/h) |
| Temperatura pracy | 5° - 40°C |
| Wilgotność względna, operacyjna (bez kondensacji) | 20% - 90% @ 40°C |
| Temperatura przechowywania | -30° - 65°C |
| Wilgotność względna przechowywania (bez kondensacji) | 5% - 95% @ 60°C |



AUDYT PODATNOŚCI STORMSHIELD

Uzbrój się w intuicyjne i wyjątkowo skuteczne narzędzie, pozwalające wykrywać potencjalne luki i podatności w sieci firmowej.

Audyt podatności

Na podstawie informacji filtrowanych przez urządzenie Stormshield, wykrywane są podatności, które mogą zagrozić Twojej sieci firmowej. W razie wykrycia luki otrzymasz powiadomienie o podatności.

Raportowanie

Audyt podatności oferuje gotowy zestaw raportów oraz dostęp do konsoli, w której w czasie rzeczywistym będziesz mógł śledzić stan bezpieczeństwa swojej sieci firmowej.



ROZSZERZONA KONTROLA DOSTĘPU DO SIECI

Monitoruj w jaki sposób Twoi pracownicy korzystają z Internetu i optymalizuj przepustowość firmowego łącza, korzystając m.in. z zaawansowanego filtra URL.

Ochrona przed zagrożeniami

Rozwiązania Stormshield weryfikują poziom ryzyka różnych witryn i blokują niebezpieczną zawartość na stronach WWW, zanim zostanie ona udostępniona lub wyświetlona pracownikowi.



OCHRONA ANTYWIRUSA

Urządzenia Stormshield dają możliwość wykorzystania do ochrony antywirusowej oprogramowania firmy Kaspersky. Program ten działa nie tylko w oparciu o bazy sygnatur wirusów, ale również w oparciu o analizę heurystyczną.

Sandboxing bazujący na chmurze

Dostępna w rozwiązaniach Stormshield usługa Breach Fighter wykrywa różnego typu ataki. Ochrona odbywa się poprzez analizę nieznanych obiektów w wyizolowanym, wirtualnym środowisku. Usługa ta może być w łatwy sposób zintegrowana z już istniejącą polityką bezpieczeństwa.



STORMSHIELD

Dystrybucja 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