



STORMSHIELD



DLA SIECI ŚREDNICH I DUŻYCH

ZADBAJ O BEZPIECZEŃSTWO SIECI FIRMOWEJ

Stormshield SN510

BEZPIECZEŃSTWO SIECI | BEZPIECZEŃSTWO DANYCH

Stormshield SN510

IDEALNE ROZWIĄZANIE DLA ŚREDNICH I DUŻYCH SIECI.



ŁATWA INTEGRACJA Z INFRASTRUKTURĄ SIECIOWĄ

Dzięki zaawansowanym funkcjom sieciowym, urządzenie dostosowuje się do infrastruktury bezproblemowo i jej nie obciążają.



WBUDOWANY DYSK TWARDY NA POTRZEBY ZBIERANIA LOGÓW

Dzięki wbudowanemu dyski twardego urządzenie zbiera i przechowuje logi ruchu sieciowego.



BEZPIECZNA KOMUNIKACJA UŻYTKOWNIKÓW MOBILNYCH

Dzięki zastosowanemu SSL VPN zgodnego z wszystkimi systemami operacyjnymi (Android, Apple, Windows) STORMSHIELD zapewnia użytkownikom mobilnym bezpieczny dostęp do zasobów w sieci firmowej.



OPTYMALIZACJA ŁĄCZY INTERNETOWYCH

Dzięki zastosowaniu HTTP Proxy cache spada zużycie łączy internetowych.

ŚREDNIE I DUŻE SIECI

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.

Wykrywanie podatności sieci

Otrzymuj informacje o nieaktualnych bądź niebezpiecznych aplikacjach pracujących w Twojej sieci firmowej i eliminuj wykryte podatności, zapewniając swojej sieci firmowej najwyższy poziom ochrony.

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 agent, SSL, SPNEGO), uwierzytelnianie wielu użytkowników w trybie cookies (Citrix-TSE), globalna / lokalna polityka bezpieczeństwa.

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), wykrywanie niezidentyfikowanych dotychczas zagrożeń różnego typu poprzez sandboxing, dekodowanie i kontrola ruchu szyfrowanego SSL, ochrona VoIP (SIP), dostosowanie polityki filtrowania do zdarzeń bezpieczeństwa lub wykrywanie luk w zabezpieczeniach.

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, internal LDAP directory - wewnętrzna baza LDAP, routing oparty na regułach (PBR), zarządzanie QoS, DHCP klient / relay / serwer, klient NTP, DNS proxy, HTTP proxy cache, HA, redundancja łącza WAN, LACP, Spanning-tree protocol (RSTP/MSTP).

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 2.x.

* Test przeprowadzony w warunkach laboratoryjnych dla oprogramowania w wersji 2.1. Wyniki mogą różnić się w zależności od warunków testowych oraz wersji oprogramowania.

** Opcjonalnie

Specyfikacja techniczna

WYDAJNOŚĆ*

Firewall	5 Gbps
Firewall + IPS (1518-bajtowa ramka danych)	3 Gbps
Firewall + IPS (pliki HTTP 1 MB)	1.7 Gbps
Antywirus	850 Mbps

VPN*

Przepustowość IPsec AES 128	1 Gbps
Przepustowość IPsec AES 256	780 Mbps
Liczba tuneli IPsec	500
Liczba klientów SSL VPN (tryb Portal)	75
Liczba tuneli SSL VPN	100

POŁĄCZENIA SIECIOWE

Liczba równoczesnych sesji	500,000
Nowe sesje / sekundę	20,000
Maksymalna liczba dostawców internetu	64
Liczba interfejsów wirtualnych (Agg, Dialup, ethernet, loopback, VLAN, pptp, ...)	350

PARAMETRY SPRZĘTOWE

Interfejsy Ethernet 10/100/1000	12
---------------------------------	----

SYSTEM

Maksymalna liczba reguł firewall	8,192
Maksymalna liczba tras statycznych	2,048
Maksymalna liczba tras dynamicznych	10,000

REDUNDANCJA

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

SPRZĘT

Pamięć wewnętrzna	320 GB
Dodatkowa pamięć	>300 GB
MTBF (lata)	14,5
Wysokość x Szerokość x Głębokość (mm)	44.45 x 440 x 310
Waga	4,25 kg
Opakowanie: Wysokość x Szerokość x Głębokość (mm)	142 x 590 x 443
Waga z opakowaniem	6,2 kg
Zasilanie (AC)	100-240V 60-50Hz 3-1.5A
Pobór energii	230V 50Hz 34W 0,21A
Liczba wentylatorów	2
Poziom głośności	55db
Rozpraszanie ciepła	130 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 nieznanego 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 | handel@dagma.pl

WWW.STORMSHIELD.PL