Barracuda **Web Application Firewall**

Chroń aplikacje oraz dane przed zaawansowanymi zagrożeniami

Barracuda

- ☑ **Security**
- ☐ Storage
- ☐ Application Delivery

Barracuda Web Application Firewall **blokuje nawet najbardziej wyszukane rodzaje ataków** skierowanych na firmowe aplikacje sieciowe, mające dostęp do wrażliwych oraz poufnych danych.

Przewaga Barracudy

- Najnowocześniejsza ochrona oparta o architekturę Full Reverse-Proxy
- Ochrona współpracujących aplikacji webowych przed malware
- Wykorzystywanie informacji o reputacji IP do walki z atakami DDoS
- Brak licencjonowania opartego o liczbę użytkowników lub modułów
- Spełnia wymagania standardów wewnętrznego i zewnętrznego bezpieczeństwa (np. PCI DSS)
- Łatwa i szybka implementacja
- Bezpłatna wymiana sprzętu na nowy po czterech latach

O produkcie

- Kompleksowa ochrona przed zagrożeniami z listy top 10 OWASP
- Wbudowany caching, kompresja oraz grupowanie TCP zapewniają ochronę bez wpływu na wydajność
- Kontrola dostępu do aplikacji oparta na ID użytkownika
- Wbudowana ochrona przed utratą danych
- Certyfikat ICSA
- Load balancing

Nieustanna ochrona przed zagrożeniami

Barracuda Web Application Firewall zapewnia kompleksową ochronę przed utratą danych, atakami DDoS oraz wszelkimi znanymi podatnościami warstwy aplikacji. Dzięki automatycznym aktualizacjom, urządzenie zyskuje nowe funkcjonalności do walki z najnowszymi zagrożeniami, gdy tylko pojawiają się na horyzoncie.

Łatwy w obsłudze, za przystępną cenę

Wbudowane szablony zabezpieczeń oraz intuicyjny interfejs WWW zapewniają natychmiastową ochronę - bez konieczności żmudnej konfiguracji, czy nauki aplikacji. Integracja ze skanerami podatności oraz narzędziami SIEM (Security Incident and Event Manager) automatyzuje procesy diagnozowania, monitoringu oraz migracji.

Zarządzanie tożsamością i dostępem

Barracuda Web Application Firewall posiada rozbudowane możliwości autoryzacji oraz kontroli dostępu, co przekłada się na wysoki poziom bezpieczeństwa wrażliwych aplikacji oraz danych.

Ochrona serwerów, aplikacji oraz danych przed atakami sieciowymi

→ Kontrola ruchu przychodzącego pod kątem ataków na warstwę 7.

← Kontrola ruchu wychodzącego pod kątem wycieku danych

Implementując rozwiązanie Barracuda Web Application Firewall, daliśmy do zrozumienia naszym klientom oraz partnerom, że poważnie podchodzimy do bezpieczeństwa przechowywanych u nas danych. Dzięki temu nasi pracownicy mogą skupiać się przede wszystkim na zapewnianiu wysokiej jakości świadczonych przez naszą firmę usług.

Michael Fainshtein
Chief Technology Officer
CredoRax.

Specyfikacja techniczna

Ochrona aplikacji

- Ochrona przed zagrożeniami z listy top 10 OWASP
- Ochrona przed popularnymi atakami:
  - SQL Injection
  - Cross-site scripting
  - modyfikacja plików cookie lub formularzy
- Sprawdzanie danych formularzy
- Adaptacyjna ochrona
- Cloaking
- Kontrola odpowiedzi
- Ochrona przed wyciekiem danych na zewnątrz:
  - numery kart kredytowych
  - pasujących do wzorca (regex)
- Szczegółowe reguły dla wybranych elementów HTML
- Protokół kontroli granicznych
- Kontrola plików wgrywanych
- Ochrona przed atakami DDoS
- Reputacja IP klientów
- Lokalizacja GeoIP:
  - Anonymous Proxy

Wspierane protokoły

- HTTP/S 0.9/1.0/1.1
- FTP/S
- XML
- IPv4/IPv6

Uwierzytelnianie i autoryzacja

- LDAP/RADIUS/Lokalna baza danych użytkownika
- Certyfikaty klienta
- Single Sign-On
- RSA SecurID
- CA SiteMinder
- SMS Passcode

Logowanie, monitorowanie oraz raportowanie

- Logi systemowe
- Logi firewalla sieciowego
- Logi dostępu
- Logi audytu

Integracja SIEM

- ArcSight
- RSA enVision
- Splunk
- Symantec
- Custom

Dostępność aplikacji oraz akceleracja

- Wysoka dostępność (HA)
- SSL offloading
- Równoważenie obciążenia
- Routing na podstawie zawartości pakietów

Firewall XML

- Ochrona XML DOS
- Schematy i zagrożenia WSDL
- Kontrola zgodności pozycji WS-I

Sieć

- VLAN, NAT
- Listy kontroli dostępu (ACL)

Opcje wsparcia

Instant Replacement

- Jednostka zastępcza wysyłana następnego dnia roboczego
- Dodatkowe telefoniczne wsparcie techniczne producenta 24/7
- Bezpłatna wymiana sprzętu na nowy po czterech latach

Opcje sprzętu

- Zabezpieczający moduł sprzętowy FIPS 140-2 HSM
- Bypass na poziomie Ethernetu

Funkcje zarządzania

- Administracja oparta na rolach
- Wbudowany skaner podatności
- Wyjątki zaufanych hostów

POROWNANIE MODELI	360	460	660	860	960
POJEMNOŚĆ					
Ilość wspieranych serwerów	1-5	5-10	10-25	25-150	150-300
Przepustowość	25 Mbps	50 Mbps	200 Mbps	1 Gbps	4 Gbps
SPRZĘT					
Wielkość urządzenia	1U Mini	1U Mini	1U Fullsize	2U Fullsize	2U Fullsize
Wymiary (cm)	42,7 x 4,3 x 35,6	42,7 x 4,3 x 35,6	42,7 x 4,3 x 57,4	44,2 x 8,9 x 64,8	44,2 x 8,9 x 64,8
Waga (kg)	5,4	5,4	11,8	20,9	23,6
Ilość portów	2 x 10/100	2 x GbE	2 x GbE	2 x GbE	2 x 10GbE[1]
Port do zarządzania	1 x 10/100	1 x 10/100	1 x 10/100	1 x 10/100	1 x 10/100
Prąd zmienny (Amp)	1,2	1,4	1,8	4,1	5,4
Pamięć ECC			●	●	●
FEATURES					
Kontrola odpowiedzi	●	●	●	●	●
Ochrona przed wyciekiem danych	●	●	●	●	●
Kontrola plików wgrywanych	●	●	●	●	●
SSL Offloading	●	●	●	●	●
Uwierzytelnianie i autoryzacja	●	●	●	●	●
Wbudowany skaner podatności	●	●	●	●	●
Ochrona przed atakami DDoS	●	●	●	●	●
Sieciowy firewall	●	●	●	●	●
Wysoka dostępność (HA)	Active/Passive	Active/Passive	Active/Active	Active/Active	Active/Active
Caching i kompresja		●	●	●	●
Integracja z LDAP/RADIUS		●	●	●	●
Równoważenie obciążenia		●	●	●	●
Routing na podst. zawartości pakietów		●	●	●	●
Zaawansowany routing			●	●	●
Tryb uczenia się			●	●	●
Antywirus dla wgrywanych plików			●	●	●
XML Firewall			●	●	●

[1] Bypass na poziomie interfejsów (Fiber NIC/Ethernet)

Specyfikacje mogą ulec zmianie bez wcześniejszego powiadomienia

Dystrybucja rozwiązań Barracuda Networks w Polsce:
DAGMA Biuro Bezpieczeństwa IT | ul. Bażantów 4/2 | 40-668 Katowice | tel. 32 793 11 00 | faks 32 793 11 90 | www.barracuda.com.pl