Barracuda **Web Application Firewall**

Chroń aplikacje i dane przed zaawansowanymi zagrożeniami

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

Barracuda Web Application Firewall **blokuje nieprzerwanie wydłużającą się listę nawet najbardziej wyszukanych rodzajów włamań i ataków**, skierowanych na firmowe aplikacje sieciowe, które mają dostęp do wrażliwych oraz poufnych danych.

Przewaga Barracudy

- Najnowocześniejsza ochrona oparta o architekturę Full Reverse-Proxy
- Ochrona współpracujących aplikacji webowych przed złośliwym oprogramowaniem
- Wykorzystywanie informacji o reputacji IP do walki z atakami DDoS
- Brak licencjonowania opartego o liczbę użytkowników lub modułów
- Pomaga organizacjom spełniać wymagania standardów wewnętrznego i zewnętrznego bezpieczeństwa, takich jak PCI DSS i HIPAA
- Skanowanie oparte na chmurze dzięki Barracuda Vulnerability Manager
- Automatyczne usuwanie luk zabezpieczeń

O produkcie

- Kompleksowa ochrona przed zewnętrznymi atakami, m.in. zagrożeniami z Top 10 OWASP
- Wbudowane buforowanie, kompresja oraz grupowanie TCP zapewniają ochronę bez wpływu na wydajność
- Kontrola dostępu do aplikacji sieciowych oparta na tożsamości użytkownika
- Wbudowana ochrona przed utratą danych
- Certyfikat ICSA

Nieustanna ochrona przed coraz nowszymi zagrożeniami

Barracuda Web Application Firewall zapewnia najlepszą 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. Natychmiast po pojawieniu się nowych zagrożeń urządzenie jest wyposażane w środki do ich blokowania.

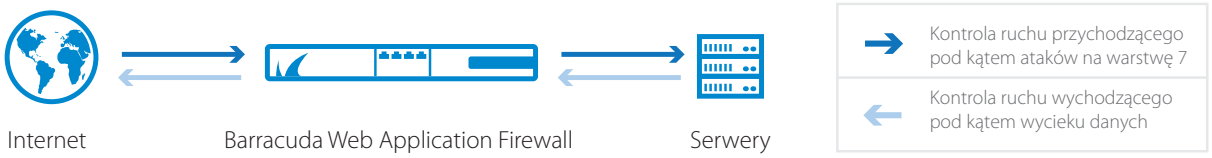
Zarządzanie tożsamością i dostępem

Barracuda Web Application Firewall ma rozbudowane możliwości autoryzacji oraz kontroli dostępu, co przekłada się na wysoki poziom bezpieczeństwa i prywatności dzięki ograniczaniu dostępu do wrażliwych aplikacji oraz danych tylko dla uwierzytelnionych użytkowników.

Łatwy w obsłudze, w przystępnej cenie

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

Ochrona serwerów, aplikacji oraz danych przed atakami sieciowymi.



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 nie muszą się martwić o bezpieczeństwo i mogą się skupiać przede wszystkim na zapewnianiu wysokiej jakości świadczonych usług.

Michael Fainshtein
Dyrektor ds. technologii
CredoRax.

Funkcje ochrony

Ochrona aplikacji sieciowych
- Ochrona przed zagrożeniami z listy top 10 OWASP
- Ochrona przed popularnymi atakami
  - SQL injection
  - cross-site scripting
  - modyfikacja plików cookie lub formularzy
- Sprawdzanie metadanych pól formularzy
- Adaptacyjna ochrona
- Maskowanie witryn WWW
- Kontrola odpowiedzi
- Kontrola ładunku JSON
- Ochrona przed wyciekiem danych na zewnątrz
  - numery kart kredytowych
  - własne numery pasujące do wzorca (wyrażenia regularne)
- Szczegółowe reguły dla wybranych elementów HTML
- Kontrola ograniczeń protokołu
- Kontrola wgrywania plików
- Lokalizacja Geo IP
  - Anonimowe proxy
- Blokowanie sieci TOR

Sieć
- VLAN, NAT
- Listy kontroli dostępu (ACL)

Obsługiwane protokoły sieciowe
- HTTP/S 0.9/1.0/1.1
- FTP/S
- XML
- IPv4/IPv6

Uwierzytelnianie i autoryzacja
- LDAP/RADIUS/Lokalna baza danych użytkowników
- SAML 2.0
- Certyfikaty klienta
- Jednokrotne logowanie
- Azure AD
- RSA SecurID
- CA SiteMinder
- SMS Passcode
- Kerberos v5
- Obsługa wielu domen

Logowanie, monitorowanie i raportowanie
- Dzienniki systemowe
- Dzienniki zapory sieciowej
- Dzienniki dostępu
- Dzienniki audytu

Integracja SIEM
- ArcSight
- RSA enVision
- Splunk
- Symantec
- Własne rozwiązania użytkownika

Dostarczanie aplikacji i akceleracja
- Wysoki poziom dostępności
- SSL offloading
- Równoważenie obciążenia
- Routing na podstawie zawartości pakietów

Zapora sieciowa XML
- Ochrona przed XML DoS
- Wymuszanie schematów/WSDL
- Kontrola zgodności pozycji WS-I

Ochrona przed atakami DDoS
- Baza danych reputacji IP Barracuda
- Heurystyczny fingerprinting
- Zagrożenia związane z CAPTCHA
- Ochrona przed atakami Slow Client
- Węzły wyjściowe TOR

Opcje pomocy technicznej

Usługa natychmiastowej wymiany sprzętu
- Jednostka zastępcza wysyłana następnego dnia roboczego
- Pomoc techniczna 24x7
- Wymiana sprzętu na nowy po czterech latach

Opcje sprzętu
- Zabezpieczający moduł sprzętowy FIPS 140-2 HSM
- Opcjonalny bypass na poziomie Ethernetu

Funkcje zarządzania
- Administracja oparta na rolach z możliwością dostosowania przez użytkownika
- Wbudowany skaner podatności
- Wyjątki zaufanych hostów
- REST API
- Własne szablony użytkownika
- Interaktywne i zaplanowane raporty

PORÓWNANIE MODELI	360	460	660	860	960
POJEMNOŚĆ					
Liczba obsługiwanych serwerów zaplecza	1-5	5-10	10-25	25-150	150-300
Przepustowość	25 Mb/s	50 Mb/s	200 Mb/s	1 Gb/s	5 Gb/s
SPRZĘT					
Wielkość urządzenia	1U Mini	1U Mini	1U Fullsize	2U Fullsize	2U Fullsize
Wymiary (cm)	42,7 x 35,6 x 4,3	42,7 x 35,6 x 4,3	42,7x 57,4 x 4,3	44,2 x 64,8 x 8,9	44,2 x 64,8 x 8,9
Masa (kg)	5,4	5,4	11,8	20,9	23,6
Liczba portów	2 x 10/100	2 x GbE	2 x GbE	2 x GbE[1]	2 x 10GbE[1]
Port do zarządzania	1 x 10/100	1 x 10/100	1 x 10/100/1000	1 x 10/100/1000	1 x 10/100/1000
Prąd przemienny wejścia przy 230 V (A)	0,6	0,7	0,9	2,1	2,8
Zużycie energii (W)	144	168	216	492	648
Pamięć ECC			•	•	•
FUNKCJE					
Kontrola odpowiedzi	•	•	•	•	•
Ochrona przed wyciekiem danych na zewnątrz	•	•	•	•	•
Kontrola wgrywania plików	•	•	•	•	•
SSL offloading	•	•	•	•	•
Uwierzytelnianie i autoryzacja	•	•	•	•	•
Wbudowany skaner podatności	•	•	•	•	•
Ochrona przed atakami DDoS	•	•	•	•	•
Zapora sieciowa	•	•	•	•	•
Wysoki poziom dostępności	Aktywna/Pasywna	Aktywna/Pasywna	Aktywna/Aktywna	Aktywna/Aktywna	Aktywna/Aktywna
Buforowanie i kompresja		•	•	•	•
Integracja z LDAP/RADIUS		•	•	•	•
Równoważenie obciążenia		•	•	•	•
Routing na podstawie zawartości pakietów		•	•	•	•
Zaawansowany routing			•	•	•
Adaptacyjne profilowanie			•	•	•
Antywirus dla wgrywanych plików			•	•	•
Szyfrowanie URL			•	•	•
Zapora sieciowa XML			•	•	•

[1] Dostępne opcje bypassu na poziomie interfejsów (Fiber NIC/Ethernet).

Specyfikacje mogą ulec zmianie bez wcześniejszego powiadomienia.