Barracuda Web Application Firewall

Web application firewall eliminuje útoky cílené na protokoly či na zranitelnosti webových aplikací a webových stránek. Poskytuje komplexní ochranu před útoky, které se zaměřují na krádež citlivých a důvěrných dat, útoky které omezují funkcionalitu daných webových aplikací "Denial of Service" (DoS) či se snaží určité webové stránky znehodnotit. Barracuda Web Application Firewall skenuje všechen webový provoz, aby mohl následně blokovat potencionální hrozby či aby zabránil úniku důležitých dat.

Ochrana před webovými útoky | Barracuda Web Application Firewall chrání webové aplikace, API a Backend mobilních aplikací proti řadě různých hrozeb. Ať už se jedná o útoky typu Zero-Day, Denial of Service (DoS), nebo útoky které zapříčiní únik důležitých dat či hrozbám z OWASP Top 10 na aplikační vrstvě. Umožňuje kontrolu provozu HTTP a HTTPS, aby mohl případně blokovat útoky které procházejí síťovými firewally před proniknutím do webové aplikace.

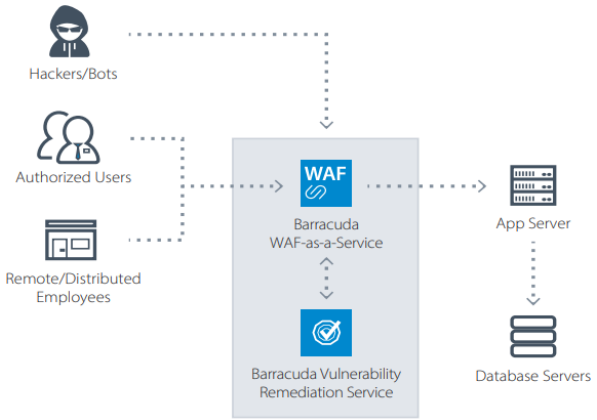
Řízení provozu a jeho akcelerace | Pro snížení administrativní zátěže spojené s ochranou webových stránek proti zranitelnosti aplikací, Barracuda Web Application Firewall automaticky přijímá aktualizace, které obsahují definice nejnovějších politik, bezpečnosti a útoků. Pro zvýšení výkonu celého řešení, Barracuda Web Application Firewall nabízí akcelerační funkce jako Load Balancing, SSL akceleraci a SSL Offload.

Reportování | Příprava reportů je rychlá a jednoduchá. V základní nabídce najdete možnost jejich automatické tvorby a doručení přes email. Reporty jsou formátovány dle PCI DSS standardu.

Pokročilé a snadné zabezpečení webové aplikace | Předem vytvořené bezpečnostní šablony, které jsou k dispozici v intuitivním webovém rozhraní, zajišťují okamžité zabezpečení bez nutnosti časově náročného nastavení. Díky integraci se skenery zranitelností a nástroji SIEM můžeme automatizovat hodnocení, monitoring a proces mitigace.

Barracuda WAF-as-a-Service

Barracuda Web Appliacation Firewall as a Service, tedy aplikační firewall jako služba je jedinečné řešení určené pro ochranu webových aplikací. Díky jednoduchému cloudovému nasazení je nyní zabezpečení webových aplikací na dosah pro organizace všech velikostí. Barracuda WAFaaS disponuje sadou předpřipravených konfiguračních pravidel – je tedy zajištěna rychlá a snadná implementace.



Ochrana dat | S rostoucími pravidly a regulacemi pro ochranu dat je stále obtížnější dosáhnout potřebné formální shody. Barracuda WAF-as-a-Service automaticky generuje detailní logy a umožňuje také generovat reporty, které prokážou soulad s danými předpisy. Krom máte k dispozici podrobný přehled o provozu aplikace a chování uživatelů, který lze využít pro další plánování.

Ochrana před DDoS útoky | Barracuda WAF-as-a-service zahrnuje ochranu napříč celým spektrem ochrany před L3 – L7 DDoS útoky. Chrání Vaše aplikace před výpadkem a z toho plynoucí nedostupnosti aplikací.

Klíčové vlastnosti

Instant Replacement Service

- Zaslání náhradního HW do příštího pracovního dne
- 24/7 technická podpora
- Nový HW každé čtyři roky

Barracuda Energize Updates

- Standardní technická podpora
- Aktualizace firmware
- Automatická aktualizace definic

Správa – funkce

- Customizovatelná administrace založena na rolích
- Integrace skeneru zranitelností
- Customizovatelné šablony
- Interaktivní a naplánovatelné reporty

COMGUARD
communication security

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel. +420 513 035 400
info@comguard.cz | www.comguard.cz

COMGUARD

Barracuda

Barracuda Web Application Firewall

	Modelová řada					
Funkce a vlastnosti	360	460	660	86X Series	96X Series	106X Series
OWASP Top 10 Web Application Security Risks Protection	✓	✓	✓	✓	✓	✓
Geo-IP a IP reputace (včetně veřejné proxy)	✓	✓	✓	✓	✓	✓
File Upload Control	✓	✓	✓	✓	✓	✓
Outbound Data Theft Protection (Credit Cards, SSN etc.)	✓	✓	✓	✓	✓	✓
Website Cloaking	✓	✓	✓	✓	✓	✓
File Upload Control	✓	✓	✓	✓	✓	✓
File Upload Security (Anti-Virus and Advanced Threat Protection)	✗	✗	✓	✓	✓	✓
Rate Control	✗	✗	✓	✓	✓	✓
CAPTCHA Support (Internal, reCAPTCHA v2 & v3)	✓	✓	✓	✓	✓	✓
Brute Force Attack Protection	✓	✓	✓	✓	✓	✓
Advanced Bot Protection se strojovým učením založeným na cloudové bázi	✓	✓	✓	✓	✓	✓
Ochrana proti OWASP Top 10 API Security Risks	Částečně	Částečně	✓	✓	✓	✓
API Security (JSON)	✓	✓	✓	✓	✓	✓
API Security (XML)	✗	✗	✓	✓	✓	✓
API Discovery (JSON)	✓	✓	✓	✓	✓	✓
API Discovery (XML)	✗	✗	✓	✓	✓	✓
Application DDoS Protection	✓	✓	✓	✓	✓	✓
TLS/SSL Offloading	✓	✓	✓	✓	✓	✓
Load Balancing & Content Routing	✗	✓	✓	✓	✓	✓
Network HSM Support	✗	✗	✓	✓	✓	✓
Dynamic URL Encryption	✗	✗	✓	✓	✓	✓
HTTP/1.0, HTTP/1.1, HTTP/2.0, WebSocket, FTP/S & IPv6 Support	✓	✓	✓	✓	✓	✓
LDAP/Active Directory, RADIUS, Kerberos v5, SMS Passcodes, Okta support	✗	✓	✓	✓	✓	✓
SAML, Azure AD, Duo Support, RSA SecurID integration, OpenID Connect, JWT	✗	✗	✓	✓	✓	✓
Azure AD	✗	✗	✓	✓	✓	✓
Barracuda Vulnerability Remediation Service	✓	✓	✓	✓	✓	✓
Onboard logging [Web Firewall Logs, Access Logs, Audit Logs, Network Firewall Logs and System Logs)	✓	✓	✓	✓	✓	✓
Syslog Export	✓	✓	✓	✓	✓	✓
SIEM/SOAR Support (včetně: Splunk, ARCsight, Azure Sentinel, RSA enVision, IBM Qradar, Symantec, Sumologic, Loggly, Azure Event Hub a další)	✓	✓	✓	✓	✓	✓
VLAN and NAT Support	✓	✓	✓	✓	✓	✓
Network ACL's	✓	✓	✓	✓	✓	✓
Advanced Routing	✗	✗	✓	✓	✓	✓
Active-Passive High Availability	✓	✓	✓	✓	✓	✓
Active-Active High Availability	✗	✗	✓	✓	✓	✓
Advanced Bot Protection	✓	✓	✓	✓	✓	✓
Active DDoS Prevention	✓	✓	✓	✓	✓	✓
Advanced Threat Protection	✗	✗	✓	✓	✓	✓

Barracuda Web Application Firewall

Model

360
460
660
86X Series
96X Series
106X Series

COMGUARD
communication security

COMGUARD a.s.
Sochorova 38, CZ 616 00 Brno
tel. +420 513 035 400
info@comguard.cz | www.comguard.cz