Barracuda

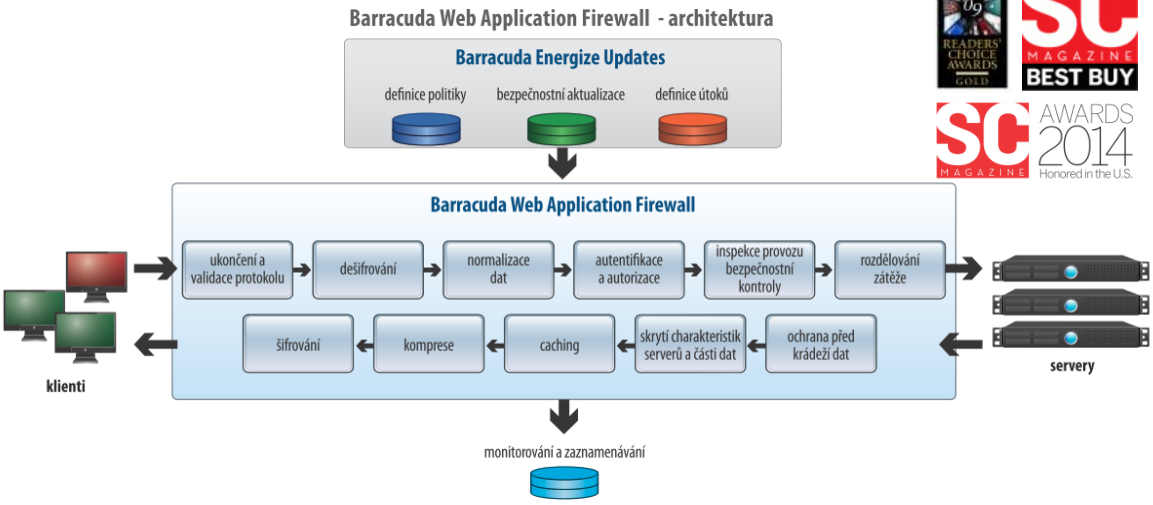
Barracuda Web Application Firewall

Rychlý rozvoj webových stránek a webových aplikací přináší mnoho nových možností pro interakci s uživateli. S tímto rozvojem bohužel také souvisí rapidní nárůst útoků, při kterých jsou využívána zranitelná nebo slabě chráněná místa aplikací nebo protokolů. Cílem těchto útoků je nejčastěji krádež citlivých dat (údaje o zákaznících, kreditních kartách atd.), poškození dobrého jména společností pozměňováním vzhledu jejich stránek nebo útoky typu denial of service. Proto společnost Barracuda přichází s řešením Web Application Firewall, které dokáže těmto útokům zabránit a eliminuje náklady související s odstraněním škod.

Zabezpečení pro webové stránky a webové servery na úrovni aplikační vrstvy

Barracuda Web Application Firewall provádí inspekci protokolů http, https a ftp určených pro webové aplikace a chrání je tak před útoky typu SQL Injections, cross-site scripting, session tampering a buffer overflows. Barracuda Web Application Firewall funguje jako obousměrná proxy brána a jde přes ni veškerý provoz (http/https) místo webového serveru. Dokáže blokovat útoky na server, skrýt jeho klíčové charakteristiky před hackery a zabránit úniku citlivých dat.

Barracuda Web Application Firewall zabraňuje útokům, které jsou spojené s manipulací s cookies a řídícími daty aplikací. Appliance analyzuje provoz a zvyšuje odolnost proti skrytým útokům tím, že normalizuje data, odstraňuje výplňkové znaky a dekóduje znakové sady. Barracuda Web Application Firewall je také plně integrován s Public-key Infrastructure (PKI) a umožňuje tak ověřování identity uživatelů, kteří využívají dané 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**.

Reporty. 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.

Řízení přístupu. Autentizace přes LDAP, RADIUS a další technologie posiluje politiky pro přístup k aplikacím dle uživatelů nebo skupin. Podporuje Single-Sign-On a dvou faktorovou autentizaci

Komplexní řešení. Firewall ležící na aplikační vrstvě a pokrývá bezpečnost webových aplikací, řídí přístup k nim a optimalizuje webový provoz.

BARRACUDA WEB APPLICATION FIREWALL

MODEL
360
460
660
860
960

COMGUARD
security & networking

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

Barracuda

BARRACUDA WEB APPLICATION FIREWALL

MODEL
360
460
660
860
960

Přehled klíčových funkcí a vlastností modelů

Podporované webové protokoly
- HTTP/S 0.9/1.0/1.1
- FTP/S
- XML
- IPv6 Ready

Bezpečnost webových aplikací
- OWASP Top-Ten Protection
- Ochrana proti běžným útokům
  - SQL Injections
  - Injection příkazů OS
  - Cross-site scripting
  - Úprava cookies a formulářů
- Validace metadat polí formuláře
- Adaptivní zabezpečení
- Web site cloaking
- Řízení odpovědi
  - Blokování klienta
  - Zrušení spojení
  - Přesměrování
  - Nastavená odpověď
- Ochrana proti krádeži dat
  - Čísla platebních karet
  - Identifikační čísla sociálního zabezpečení
  - Srovnání se zadaným vzorkem (regex)
- Granulární politiky pro HTML prvky
- Kontrola omezení protokolu
- Řízení uploadu souborů
- Ochrana proti útokům hrubou silou
- Sledování session

Autentizace a autorizace
- LDAP/RADIUS/local/databáze uživatelů
- Klientské certifikáty
- Single Sign on

Záznamy, monitorování a hlášení
- Systém log
- Web Firewall log
- Access log
- Audit log

Dostupnost a akcelerace aplikací
- Vysoká dostupnost
- SSL Offloading
- Load Balancing
- Směrování dle obsahu

XML Firewall
- Ochrana XML DOS
- Schéma/WSDL enforcement
- Kontroly souladu WS-I

Systémové vlastnosti
- Grafické uživatelské rozhraní
- Správa založená na rolích
- Zabezpečená vzdálená správa
- Ethernet bypass
- Sdílené politiky
- Integrace s vulnerability skenem

Hardwarové vlastnosti

Konektory
- WAN/LAN/MGMT porty
- Sériový port DB9 pro konzulu

Model	360*	460*	660*	860	960
Kapacita					
Počet podporovaných serverů	1-5	5-10	10-25	25-150	150-300
Propustnost	25 Mbps	50Mbps	200Mbps	1Gbps	5Gbps
Počet http transakcí/sec	8000	15000	30000	90000	180000
Počet SSL transakcí/sec	2500	4000	12000	30000	50000
Hardware					
Met. Ethernet rozhraní	2 x 10/100	2 x Gigabit	2 x Gigabit	2 x Gigabit	2 x 10 Gigabit
Optické rozhraní				2 x Gigabit	2 x Gigabit
Vlastnosti					
Validace HTTP/HTTPS/FTP	ano	ano	ano	ano	ano
Ochrana proti běžným útokům	ano	ano	ano	ano	ano
Validace metadat formulářových polí	ano	ano	ano	ano	ano
Web site cloaking	ano	ano	ano	ano	ano
Řízení odezvy	ano	ano	ano	ano	ano
Ochrana proti krádeži síťových dat	ano	ano	ano	ano	ano
Granulární politiky pro prvky HTML	ano	ano	ano	ano	ano
Řízení nahrávání provozu	ano	ano	ano	ano	ano
Záznamy, monitorování a hlášení	ano	ano	ano	ano	ano
High Availability	Active/Passive	Active/Passive	Active/Active	Active/Active	Active/Active
SSL Offloading	ano	ano	ano	ano	ano
Autentizace a autorizace	ano	ano	ano	ano	ano
Integrace Vulnerability skenu	ano	ano	ano	ano	ano
Centralizovaný management	ano	ano	ano	ano	ano
Caching a komprese		ano	ano	ano	ano
Integrace s LDAP/RADIUS		ano	ano	ano	ano
Load Balancing		ano	ano	ano	ano
Směrování dle obsahu		ano	ano	ano	ano
Adaptive Profiling			ano	ano	ano
AV pro upload souborů			ano	ano	ano
XML Firewall			ano	ano	ano

*také jako virtuální appliance (WMware ESX/ESXi, VMware, Citrix XenServer, Microsoft Hyper-V a Oracle VirtualBox)

COMGUARD security & networking

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