Barracuda Email Security Gateway

Elektronická pošta se stala nenahraditelnou součástí firemní komunikace. S tím souvisí také rozšiřující se spektrum hrozeb a útoků, jejichž nejčastějším cílem je získání důvěrných informací, zasílání nevyžádané pošty nebo šíření virů a jinak škodlivého softwaru. Emailovým serverům se nevyhýbají ani DoS/DDoS útoky.

Špička v oboru ochrany proti spamu | Díky dlouhodobým zkušenostem v oblasti antispamové ochrany je společnost Barracuda Networks lídrem v identifikaci a blokaci nevyžádané pošty. Komplexní soubor bezpečnostních technologií zajišťuje organizacím produktivitu, i když se hrozby neustále vyvíjí. Barracuda Email Security Gateway využívá Barracuda Central k identifikaci emailů od známých spamerů a určuje, zda odkazy v emailech patří distributorům spamu či malwaru. Další technikou je např. ochrana před pokusy skrýt text do obrázků za účelem ukrytí obsahu před tradičními filtry.

Silné stránky řešení

- > Různé možnosti nasazení: appliance, virtual appliance (VMware ESX a Workstation, Oracle VirtualBox, Citrix Xen a Microsoft Hyper-V), Azure, AWS, vCloud Air
- > Cloudový sandbox (od Lastline) pro inspekci podezřelých příloh v ceně
- > Volitelná cloudová před-filtrace zdarma
- > Volitelný druhý antivirový engine od Avira
- > Nativní „pull-based" šifrován a DLP zdarma
- > Zdarma Central Management – mimo on-appliance integrovaného GUI je možná správa i přes Barracuda Control Center, možnost spravovat veškeré lokality z jednoho místa.

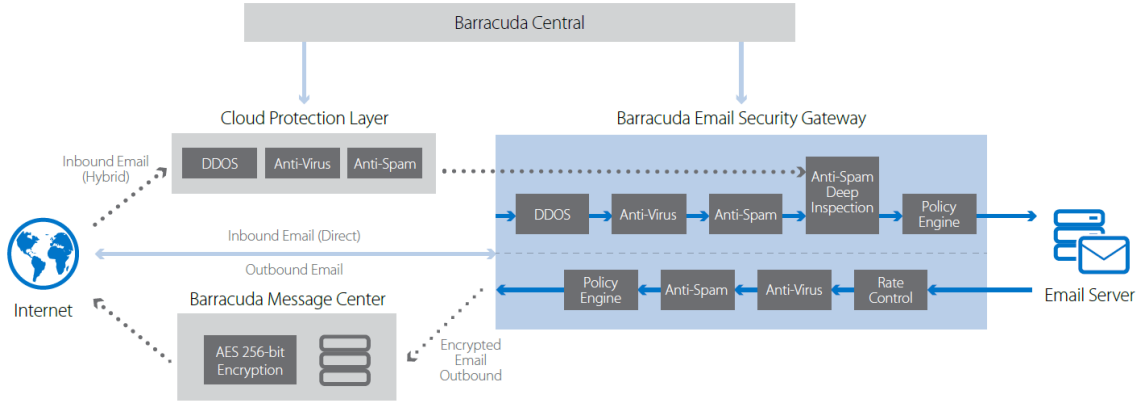
Ochrana před malwarem v emailu | Škodlivé kódy jsou neustále „zdokonalovány" a mají potenciál způsobovat citelné škody vč. finančních ztrát všem typům organizací. Proto je třeba mít sofistikovanou filtraci malware i na emailové bráně. Barracuda Email Security Gateway skenuje příchozí emaily a jejich přílohy s využitím tří nezávislých vrstev, resp. technologií. Součástí je kontrola archivů a neustálá aktualizace skrze „Energize Updates" k odhalování virů šířících se pomocí emailů.

Barracuda Central | Všechny produkty společnosti Barracuda Networks jsou podporovány z Barracuda Central, tj. pokročilého 24/7 Security Operation Centra neustále globálně monitorujícího nejnovější internetové hrozby z více než 250 000 zdrojů. Účelem je vytvářet pro zákazníky obranné mechanismy, pravidla a signatury prakticky v reálném čase, které jsou šířeny pomocí „Energize Updates". Tyto updaty nevyžadují žádnou interakci ze strany administrátorů a zaručují bezproblémovou přesnost a účinnost ochrany před internetovými hrozbami.

Ochrana před útoky typu Denial of Service (DoS/DDoS) | Ne všechny útoky jsou prováděny pomocí kódů snažících se získat přístup k datům, nebo získat jinou neoprávněnou výhodu. Často je útok zaměřen na kompromitaci či vyřazení služeb z provozu. Barracuda Email Security Gateway jakožto zařízení, které „sedí" před emailovým serverem, chrání tento před zahlcením a podobnými typy útoků.

Zabezpečení proti výpadkům emailových serverů | Barracuda Email Security Gateway zaručuje doručení emailu i v průběhu výpadku emailových serverů či ztrátě konektivity. V případě výpadků „on-premise" zařízení mohou být poštovní zprávy uchovávány v CPL (Cloud Protection Layer) po dobu až 96 hodin. Zároveň může být specifikována alternativní destinace pro doručení pro případ výpadku té primární. Během výpadku jsou všechny emaily přístupné pomocí CPL. Z logů pak administrátoři snadno vyčtou status takto uchovaných emailů, např. o jejich opětovném doručení.

Předsunutá volitelná filtrace v cloudu šetří výkon | Barracuda Email Security Gateway je integrován s cloudovou službou (Cloud Protection Layer), která provádí filtraci zpráv před jejich doručením na Barracuda Email Security Gateway. CPL je neustále aktualizována z Barracuda Central a navíc poskytuje flexibilní pokrývání špiček provozu i záložní řešení v době výpadků „on-premise" infrastruktury či DoS útoků. V neposlední řadě přináší CPL zákazníkům jistotu, že jejich bezpečnostní emailová infrastruktura je připravena na jakýkoli nárůst poštovního provozu.



BARRACUDA EMAIL SECURITY GATEWAY

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 EMAIL SECURITY GATEWAY

Šifrování | Barracuda Email Security Gateway nabízí vícero šifrovacích funkcí. Je plně integrován s cloudovou šifrovací službou pro odchozí emaily. Zprávy, které vyhovují politice, nebo jsou označeny pro zašifrování skrze Barracuda Outlook Add-in, jsou odeslány přes TLS do Barracuda Message Center, který využívá standard AES s délkou klíče 256 bitů. Pro šifrování zpráv mezi dvěma lokalitami v internetu, podporuje Barracuda Email Security Gateway Message Transport Agent protokol SMTP over TLS.

Filtrace odchozí pošty & DLP | Filtrace odchozího poštovního provozu preventivně chrání organizace před jejich zařazením na blokovací seznamy – black listy, ovládnutí jejich zařízení ze strany botnetů a chrání citlivá data obsažena v emailech před jejich kompromitací či únikem. Organizace tak může vynucovat své bezpečnostní politiky a zajišťovat shodu s regulatorními požadavky pomocí detekce a blokace citlivých dat v odchozím poštovním provozu či jejich zabezpečením pomocí šifrování.

Centrální správa v cloudu & reporting Barracuda Email Security Gateway je také integrován s webovým management portálem Barracuda Cloud Control (BCC). Díky tomu mají organizace přehled o všech lokalitách na jednom místě, ze kterého jsou také řízena a konfigurována. K dispozici je samozřejmě detailní monitorování emailů a automatická tvorba reportů dostupných přes webové rozhraní.

Přehled klíčových funkcí a vlastností modelů

Bezpečnost
- Filtrování spamu a virů
- Cloudový Sandbox i předfiltrace
- Dva AV enginy
- Zabraňuje spoofingu i phishingu
- Ochrana proti DoS/DDoS
- Ochrana proti Directory harvest
- Filtrování odchozích emailů

Filtr spamu
- Rate control
- Analýza reputace IP
- Analýza otisku a obrazu
- Algoritmus přiřazení skóre dle pravidel
- Barracuda Anti-Fraud Intelligence

Pokročilé politiky řízení
- Filtrování dle IP a obsahu
- Kategorizace objemné pošty
- Šifrování obsahu
- Filtrování dle příjemce/odesílatele
- Podpora RBL a DNSBL
- Blokování dle klíčových slov
- Blokování dle sady znaků
- Data Loss Prevention
- Blokování reverzních DNS
- Blokování dle šablon a URL kategorií
- Politika TLS šifrování
- Sekundární autentizace

Autentizace odesílatele
- SFP a DomainKeys
- Emailreg.org
- Invalid bounce suppression

Filtrování virů
- Třívrstvá filtrace virů
- Integrovaný Exchange AV agent
- Kontrola archivů
- Blokování dle typu souborů
- Barracuda Anti-Virus Supercomputing Grid

Administrace
- Web GUI rozhraní i Cloud based centrální správa
- Administrace uživatelských účtů
- Reporty, grafy a statistiky
- LDAP rozhraní
- Podpora více domén
- Zabezpečená vzdálená administrace
- Delegování doménové správy
- Delegování role help desku
- Email spooling v cloudu
- Konfigurace obnovy do cloudu

Koncoví uživatelé
- Filtrování dle uživatelů
- Individuální přiřazení skóre spamu
- Osobní block list
- Uživatelská karanténa emailů + digest
- Integrace s Outlook/Lotus Notes
- Bayesovská analýza

Model	100*	200	300*	400*	600*	800*	900*	1000*
Kapacita								
Počet aktivních uživatelů	1-50	51-500	300-1000	1000-5000	3000-10000	8000-22000	15000-30000	25000-100000
Domény	10	50	250	500	5000	5000	5000	5000
Kapacita pro Message logy	8 GB	10 GB	12 GB	24 GB	72 GB	120 GB	240 GB	512 GB
Kapacita karantény			20 GB	60 GB	180 GB	360 GB	1 TB	2 TB
Hardware								
Velikost v racku	1U Mini	1U Mini	1U Mini	1U Mini	1U Fullsize	2U Fullsize	2U Fullsize	2U Fullsize
Ethernet rozhraní	1 x 10/100	1 x Gigabit	1 x Gigabit	1 x Gigabit	2 x Gigabit	2 x Gigabit	2 x Gigabit	2 x Gigabit
Red. diskové pole (RAID)				ano	Hot Swap	Hot Swap	Hot Swap	Hot Swap
ECC memory					ano	ano	ano	ano
Redundant. napájecí zdroj						Hot Swap	Hot Swap	Hot Swap
Vlastnosti								
Filtrace odchozí pošty	ano	ano	ano	ano	ano	ano	ano	ano
Šifrování emailů	ano	ano	ano	ano	ano	ano	ano	ano
Cloudová ochrana (CPL)	ano	ano	ano	ano	ano	ano	ano	ano
Akcelerátor MS Exchange/LDAP			ano	ano	ano	ano	ano	ano
Nastavení a karanténa dle uživatelů			ano	ano	ano	ano	ano	ano
Delegování help desku			ano	ano	ano	ano	ano	ano
Podpora Syslog			ano	ano	ano	ano	ano	ano
Clustering i Remote				ano	ano	ano	ano	ano
Nastavení dle domén				ano	ano	ano	ano	ano
Single Sign-On				ano	ano	ano	ano	ano
SNMP/API				ano	ano	ano	ano	ano
Upravitelné rozhraní					ano	ano	ano	ano
Score Settings dle uživ.					ano	ano	ano	ano
Delegovaná správa domén					ano	ano	ano	ano

*také jako virtuální appliance (VMware ESX & Workstation, Oracle VirtualBox, Citrix Xen a Microsoft Hyper-V)

COMGUARD security & networking

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