Funcions del Barracuda Spam Firewall

[Filtrat d'entrada/sortida i prevenció de fuita de dades](#)
[Protecció contra spam](#)
[Protecció contra virus](#)
[Barracuda Central](#)
[Protecció contra atacas de denegació de servei (DoS)](#)
[Correu electrònica en cua](#)
[Filtrat previ d'spam i virus](#)
[Xifrat](#)
[Filtrat de sortida](#)
[Administració central basada en el núvol](#)
[Preguntes freqüents](#)

Filtrat d'entrada/sortida i prevenció de fuita de dades

Barracuda Spam Firewall gestiona tot el trànsit d'entrada i sortida per protegir les organitzacions enfront d'amenaces originades per correus electrònics i fuites de dades.

Com a solució de gestió de correu electrònic completa, les organitzacions poden xifrar els missatges i aprofitar el núvol per posar el correu electrònic en cua si els servidors de correu deixen d'estar disponibles.

Protecció contra spam

Amb un llarg historial en la protecció antispam, Barracuda Networks segueix sent líder en identificació i bloqueig d'spam. Un complet conjunt de capes de seguretat garanteix que les organitzacions mantinguin la seva productivitat davant de la constant evolució de les amenaces. Barracuda Spam Firewall aprofita Barracuda Central per identificar correu electrònic de spammers coneguts i determinar si els dominis incorporats al correu electrònic dirigeixen a dominis d'spam o malware coneguts. Aprofita moltes de les mateixes tècniques líders del sector que es troben en Barracuda Spam Firewall, que protegeixen contra els intents d'incorporar text dins de les imatges amb la intenció d'ocultar contingut als filtres de correu brossa tradicionals.

Protecció contra virus

Com que els atacs de virus cada vegada són més sofisticats i complexos, la infraestructura de correu electrònic requereix protecció antivirus avançada. El potencial per a la destrucció i l'alliberament d'informació o l'alteració d'una xarxa afecta greument la productivitat i pot comportar pèrdues econòmiques.
Barracuda Spam Firewall escaneja el correu electrònic i els arxius entrants utilitzant tres potents

capes de tecnologia d'escaneig de virus. També descomprimeix els arxius per oferir una protecció completa. Mitjançant Energize Updates, s'actualitzen potents definicions de virus automàticament per mantenir la protecció més actualitzada contra virus transmesos per correu electrònic.
Per proporcionar protecció davant correu electrònic intern corrupte, un plug-in de Microsoft Exchange permet a les organitzacions protegir-se contra la propagació de virus que no accedeixen a la passarel·la de correu electrònic. Les definicions de virus també s'actualitzen amb regularitat per a garantir la protecció més actualitzada.

Barracuda Central

Tots els productes de Barracuda compten amb el suport de Barracuda Central, un centre d'operacions de seguretat avançat 24 x 7 que treballa contínuament per supervisar i bloquejar les amenaces d'Internet més recents. Barracuda Central reuneix dades de més de 150.000 punts de tot el món i els analitza per desenvolupar defenses, regles i signatures. A mesura que van sorgint noves amenaces, Barracuda Central actua ràpidament per respondre a brots primerencs i proporciona les últimes definicions mitjançant Barracuda Energize Updates. Aquestes actualitzacions no requereixen administració en absolut i garanteixen que Barracuda Spam Firewall proporcioni una protecció completa i precisa contra les últimes amenaces d'Internet.

Protecció contra atacs de denegació de servei (DoS)

No tots els atacs estan orientats a aconseguir que els usuaris enviïn el seu número de targeta de crèdit, que facin clic en un enllaç maliciós o a implantar un virus. Sovint, l'objectiu de l'atac està orientat a desactivar una xarxa o reduir la seva eficàcia. Com a servei basat en el núvol, Barracuda Spam Firewall permet detenir els spammers abans que sobrecarreguin un servidor de correu electrònic.

Correo electrònic en cua

Barracuda Spam Firewall garanteix que es pugui seguir enviant correu electrònic fins i tot quan es produeixin fallades del servidor de correu electrònic o pèrdues de la connectivitat. En cas d'interrupcions en les pròpies instal·lacions, el correu electrònic es pot posar en cua en Cloud Protection Layer durant un màxim de 96 hores. També es pot especificar un destí alternatiu per al lliurament si el lliurament a la destinació principal falla.
Durant les interrupcions de servei del servidor de correu electrònic, el correu electrònic de tots els servidors de correu resulta visible per mitjà de Cloud Protection Layer. Des del registre de missatges, es pot veure l'estat de tots els correus electrònics en cua i si el correu s'ha tornat a lliurar.

Filtrat previ d'spam i virus

Barracuda Spam Firewall està integrat amb un servei basat en el núvol que filtra prèviament el correu electrònic abans de lliurar-lo al Barracuda Spam Firewall local. Cloud Protection Layer s'actualitza contínuament amb definicions en temps real amb actualitzacions de Barracuda Central. L'elasticitat de la infraestructura de núvol global de Barracuda proporciona la flexibilitat necessària per gestionar pics de correu electrònic durant períodes específics del dia i durant atacs de denegació de servei.

Cloud Protection Layer garanteix que la infraestructura de seguretat de correu electrònic de l'organització s'adapti a l'augment del volum de correu electrònic i de la mida dels arxius adjunts, així com al creixement de les empreses. Aprofitant l'ample de banda i la potència de càlcul del CPL, les organitzacions poden ampliar fàcilment la seva solució de seguretat de correu electrònic.

Xifrat

Barracuda Spam Firewall ofereix diverses funcions de xifrat. Està totalment integrat amb un servei de xifrat de correu electrònic basat en el núvol per al correu electrònic sortint. El correu electrònic que compleix amb la política o que està marcat per al xifrat mitjançant Barracuda Outlook Add-in s'envia per mitjà de TLS a Barracuda Message Center.

Barracuda Message Center utilitza AES amb claus de 256 bits per xifrar el correu electrònic. Per xifrar trànsit el trànsit de correu electrònic entre llocs per Internet, Barracuda Spam Firewall Message Transport Agent admet SMTP sobre TLS. Es pot utilitzar entre Barracuda Spam Firewall o altres servidors de correu electrònic que admetin SMTP sobre TLS.

Barracuda Spam Firewall ofereix diverses funcions de xifrat. Està totalment integrat amb un servei de xifrat de correu electrònic basat en núvol per al correu electrònic sortint. El correu electrònic que compleix amb la política o que està marcat per al xifrat mitjançant Barracuda Outlook Add-in s'envia per mitjà de TLS a Barracuda Message Center.

Filtrat de sortida

El filtrat de sortida evita la inclusió de les organitzacions en llistes de bloqueig d'spam i impedeix la sortida de dades confidencials de l'organització per correu electrònic. Sense saber-ho, els empleats poden propiciar que els sistemes interns es converteixin en una font per l'spam de botnet. Utilitzant un subconjunt de les seves capes de defensa, el filtrat de sortida de Barracuda Spam Firewall deté el correu brossa i els virus de sortida. També permet als administradors aplicar polítiques de contingut per a la prevenció de pèrdua de dades (DLP) i per complir altres estàndards de contingut en el correu electrònic de sortida. Es poden utilitzar filtres predefinits i polítiques personalitzades per

detectar dades confidencials i bloquejar o xifrar correu electrònic.

Administració central basada en el núvol

Barracuda Spam Firewall està integrat amb el portal d'administració basat en la web Barracuda Cloud Control (BCC), que aprofita la infraestructura de núvol global de Barracuda per permetre a les organitzacions administrar centralment tots els seus dispositius mitjançant una interfície "d'un sol panell". Els administradors obtenen una visió global de tots els seus dispositius o serveis i, a més, poden administrar centralment les polítiques i la configuració. La interfície simple facilita a les organitzacions petites i mitjanes la implementació i administració del servei amb una despesa de TI mínim.

Si li interessa, pregunti per la resta de **productes Barracuda**:

Seguridad		Almacenamiento	Application Delivery	Infraestructura
Seguridad del Correo Electrónico Spam Firewall Email Security Service	**Seguridad de Red** Firewall NG Firewall SSL VPN	**De Protección de Datos** Backup	**Server Load Balancing** Load Balancer ADC Load Balancer FDC	**Telefonía IP** Phone System
Seguridad web Web Filter Web Security Service	**Seguridad de Aplicaciones Web** Web Application Firewall	**Archiving & Information Management** Message Archiver ArchiveOne PST Enterprise	**Link Load Balancing** Link Balancer	**Firma Electrónica** CudaSign
Video Vigilancia IP CudaEye	**Integrated Virtualization Platforms** Security Suite	**Sincronización de Archivos y Compartir** Copy	**Access Control** SSL VPN Web Application Firewall	

Preguntes freqüents sobre Barracuda Spam Firewall

Com protegeix Barracuda Spam Firewall enfront de les amenaces per correu electrònic?

Barracuda Spam Firewall, una solució de hardware i software integrada, utilitza un mètode multicapa per oferir la protecció de correu electrònic més completa que existeix enfront d'atacs d'spam, virus, suplantació, phishing i spyware. Un dels avantatges afegits de Barracuda Spam Firewall és el processament de cada correu electrònic per maximitzar el rendiment i la capacitat per filtrar milions de missatges al dia.
Darrere de les iniciatives líders en el sector de Predictive Sender Profiling i Barracuda Reial-Time Protection hi ha 12 capes de defensa explícites, que són les següents: protecció davant la denegació de servei i seguretat, controls de velocitat, anàlisi de reputació d'adreces IP, autenticació de remitents, verificació de destinataris, protecció davant virus, polítiques (regles especificades per l'usuari), anàlisi d'empremtes digitals, anàlisi d'intencions, anàlisi d'imatges, anàlisi bayesià i un motor de puntuació de regles de spam.

Com es filtra el correu electrònic?

Desplegat al perímetre de la xarxa, tot el correu electrònic entrant ha de passar a través de les 12 capes de defensa Barracuda Spam Firewall abans d'arribar al destinatari corresponent. Les capes de defensa s'agrupen en dues classes principals: gestió de connexions, que implica deixar anar les connexions de correu entrant abans de rebre missatges, i escaneig de correu, que analitza els missatges després de la seva recepció. Durant el procés de filtrat, els correus electrònics es verifiquen per detectar possibles atacs d'spam nous o coneguts, virus i infraccions de polítiques d'administrador. En base a les preferències de l'administrador i de l'usuari, el correu brossa es pot etiquetar, deixar en quarantena o bloquejar.

Per què s'ha d'etiquetar el correu electrònic? Què passa amb els correus electrònics etiquetats?

Etiquetar el correu electrònic beneficia les organitzacions ja que permet identificar fàcilment els

missatges que compleixen els criteris establerts. Els correus electrònics etiquetats es lliuren al destinatari amb una etiqueta personalitzada, com [BULK], que s'afegeix a l'assumpte del missatge.

Per què s'ha de deixar el correu electrònic en quarantena? Què passa amb els correus electrònics en quarantena?

Deixar els correus electrònics en quarantena és una mesura de seguretat que permet examinar els missatges qüestionables abans d'acceptar-los o rebutjar-los; generalment, un correu electrònic en quarantena es converteix en spam. Un administrador pot triar dos tipus de correu electrònic en quarantena: quarantena global o quarantena per usuari.
Quan es configura per la quarantena global, Barracuda Spam Firewall dirigeix tot el correu electrònic en quarantena a una bústia especificada per l'administrador. Quan es configura per la quarantena per usuari, Barracuda Spam Firewall emmagatzema el correu electrònic de forma local i informa periòdicament als usuaris sobre el seu correu electrònic en quarantena. Els usuaris poden optar per eliminar el correu electrònic en quarantena, reenviar-lo a les seves pròpies bústies o incloure en una llista blanca l'adreça del remitent per evitar que futurs correus electrònics del remitent es posin en quarantena. La quarantena per usuari està disponible amb els següents models de Barracuda Spam Firewall: 300, 400, 600, 800 i 900.

Quines tecnologies s'utilitzen en Barracuda Spam Firewall?

Barracuda Spam Firewall utilitza una combinació de programari de propietat i programari de codi obert. El sistema operatiu Barracuda Spam Firewall es basa en un nucli de Linux estable i reforçat que ha passat per un estricte escrutini per part d'investigadors de seguretat. El robust MTA pot gestionar un nombre elevat de connexions SMTP i volums elevats de lliurament de correu. A partir de la versió 3.5 del firmware, Barracuda Spam Firewall MTA integra una funció de registre d'informació que es pot utilitzar juntament amb Barracuda Message Archiver.

Si utilitzo Microsoft Exchange, com em protegirà Barracuda Spam Firewall davant d'atacs de "diccionari"?

Microsoft Exchange Accelerator, disponible en Barracuda Spam Firewall 300 i models superiors,

utilitza el protocol LDAP (Lightweight Diccionari Access Protocol) integrat en Exchange per verificar els destinataris abans d'entregar missatges a Microsoft Exchange Server.

Quines noves tecnologies afegeix Barracuda Spam Firewall per combatre amb les últimes campanyes d'spam?

Barracuda Networks ha anunciat diverses iniciatives contra el correu brossa:
Multi-Pass Optical Character Recognition Engine: l'spam d'imatges generalment inclou text amb imatges amb la intenció d'ocultar contingut ometent les capes de processament de regles de text dels filtres de correu brossa. Amb el motor OCR de diverses passades i líder en el sector de Barracuda Networks, els tallafocs Barracuda Spam Firewall fan que els que trucs que utilitzen els usuaris que envien spam per ocultar text darrere d'imatges en color o desenfocades siguin inefectius.

Predictive Sender Profiling: la solució Predictive Sender Profiling de Barracuda Networks investiga amb més detall els correus electrònics enviats i indaga en la campanya per identificar possibles activitats anòmales del remitent, el que permet a Barracuda Networks bloquejar de forma efectiva l'spam que generalment no es pot aturar mitjançant l'anàlisi de reputació tradicional.

Barracuda Real-Time Protection: Barracuda Real-Time Protection utilitza un conjunt avançat de tecnologies per a bloquejar de forma immediata els virus i spyware més recents, així com altres atacs de malware a mesura que emergeixen. Gràcies a l'ús de la vasta i diversa base de clients dels tallafocs de Barracuda Spam Firewall, Barracuda Networks lidera el sector a la detecció de tendències i en la resposta les amenaces originades per correu electrònic.

Com protegeix Barracuda Spam Firewall enfront de les amenaces de virus?

Barracuda Spam Firewall proporciona una protecció completa enfront de les amenaces de virus a través de potents capes. La primera capa consta d'un reconegut motor de codi obert per a l'escaneig de virus. La segona capa és un motor de virus de propietat mantingut per Barracuda Central, un centre d'operacions de seguretat avançat disponible de forma ininterrompuda que treballa per supervisar i bloquejar de forma continuada les últimes amenaces d'Internet. La tercera capa és Barracuda Real-Time Protection, un conjunt de tecnologies avançades que permeten als tallafocs Barracuda Spam Firewall bloquejar de forma immediata els atacs més recents de virus, spyware i altres atacs de malware a mesura que emergeixen, sense haver d'esperar a descarregar una signatura en Barracuda Spam Firewall.

Com bloqueja Barracuda Spam Firewall les amenaces en temps real?

Els enginyers de Barracuda Central treballen diligentment i de forma ininterrompuda per supervisar les amenaces d'spam i virus de tot el món. Atès que els temps de resposta són crucials davant les amenaces en temps real, quan es detecta una amenaça, Barracuda Spam Firewall utilitza Barracuda Real-Time Protection per mitigar aquestes amenaces perquè emergeixen sense esperar noves actualitzacions

Quant de temps hauré de dedicar a la instal·lació i manteniment de Barracuda Spam Firewall?

Barracuda Spam Firewall està dissenyat com a solució fàcil d'instal·lar que requereix una sobrecàrrega administrativa mínima. Sense fer cap ajust, Barracuda Spam Firewall ofereix un índex de precisió de detecció d'spam del 95% amb un 0,01% de falsos positius. Tenint en compte les sis capes de defensa ajustades automàticament per Energize Updates, Barracuda Spam Firewall es manté actualitzat fàcilment per garantir la precisió de l'spam en curs.

Rebré molts falsos positius amb un Barracuda Spam Firewall?

Sense fer cap ajust, Barracuda Spam Firewall està configurat per minimitzar els falsos positius, que solen ser un 0,01% o menys, un dels índexs de falsos positius més baix del sector. Com passa amb qualsevol solució que permet la personalització dels usuaris, la devolució de falsos positius de cada client variarà en funció de com ajusti l'administrador la unitat (per exemple, un valor de puntuació d'spam més estricte pot donar lloc a un nombre major de falsos positius).

Què inclou Energize Updates per Barracuda Spam Firewall?

La subscripció a Barracuda Energize Updates proporciona actualitzacions de les definicions d'spam i virus més recents que bloquegen noves campanyes abans que es converteixin en un brot. Els enginyers de Barracuda Central actualitzen constantment les definicions d'spam i virus per poder ajustar de forma remota sis de les 12 capes de defensa, el que permet minimitzar el temps

d'administració. Energize Updates també ofereix accés a suport tècnic, nous releases de firmware i l'oportunitat de participar en el programa Barracuda Early Release Firmware.

Ofereix Barracuda Spam Firewall polítiques per usuari?

Les polítiques per usuari estan disponibles a Barracuda Spam Firewall 300 i models superiors. Les polítiques per usuari ofereixen als usuaris la capacitat de definir les seves pròpies polítiques de puntuació individuals, base de dades bayesiana, el que permet l'ús de llistes blanques i llistes de bloqueig.

Pot Barracuda Spam Firewall filtrar els missatges de sortida?

Sí. Barracuda Spam Firewall filtra els missatges de sortida per detectar possibles virus i polítiques d'escaneig de spam bàsiques. Pel escaneig de sortida avançat, Barracuda Networks ofereix Barracuda Spam Firewall-Outbound, que inclou diferents fluxos de treball per deixar en quarantena el tràfic de correu electrònic de sortida perquè puguin revisar-lo els auditors de polítiques.

Com puc bloquejar o minimitzar la quantitat de missatges de rebot no vàlids?

Els missatges de rebot no vàlids són informes de no lliurament a adreces de correu electrònic falsificades. Per bloquejar els missatges de rebot no vàlids, habiliti la característica Invalid Bounce Suppression i traspassi tot el correu electrònic sortint a través del dispositiu Barracuda Spam Firewall o Barracuda Spam Firewall-Outbound.

Permet Barracuda Spam Firewall als administradors bloquejar correu electrònic d'altres països?

Sí. Barracuda Spam Firewall ofereix diferents mètodes per bloquejar correu electrònic d'altres països:

1. En base a la recerca DNS inversa, els administradors bloquegen els missatges dels quals el

domini de nivell superior es resol en el nom d'amfitrió d'un país

2. En base al conjunt de caràcters declarats d'un correu electrònic, els administradors bloquegen missatges que contenen un conjunt d'idiomes específic.

3. Si bé Barracuda Networks no ho recomana, els administradors creen polítiques personalitzades per filtrar altres patrons en l'assumpte, la capçalera o el cos dels missatges per bloquejar correu electrònic no desitjat d'altres països.