Funciones del Barracuda Spam Firewall

Filtrado de entrada/salida y prevención de fuga de datos

Barracuda Spam Firewall gestiona todo el tráfico de entrada y salida para proteger a las organizaciones frente a amenazas originadas por correos electrónicos y fugas de datos.

Como solución de gestión de correo electrónico completa, las organizaciones pueden cifrar los mensajes y aprovechar la nube para poner el correo electrónico en cola si los servidores de correo dejan de estar disponibles.

Protección contra spam

Con un largo historial en la protección antispam, Barracuda Networks sigue siendo líder en identificación y bloqueo de spam. Un completo conjunto de capas de seguridad garantiza que las organizaciones mantengan su productividad frente a la constante evolución de las amenazas. Barracuda Spam Firewall aprovecha Barracuda Central para identificar correo electrónico de spammers conocidos y determinar si los dominios incorporados en el correo electrónico dirigen a dominios de spam o malware conocidos. Aprovecha muchas de las mismas técnicas líderes del sector que se encuentran en Barracuda Spam Firewall, que protegen contra los intentos de incorporar texto dentro de las imágenes con la intención de ocultar contenido a los filtros de spam tradicionales.

Protección contra virus

Puesto que los ataques de virus cada vez son más sofisticados y complejos, la infraestructura de correo electrónico requiere protección antivirus avanzada. El potencial para la destrucción y la liberación de información o la alteración de una red afecta gravemente a la productividad y puede conllevar pérdidas económicas.
Barracuda Spam Firewall escanea el correo electrónico y los archivos entrantes utilizando tres

potentes capas de tecnología de escaneo de virus. También descomprime los archivos para ofrecer una protección completa. Mediante Energize Updates, se actualizan potentes definiciones de virus automáticamente para mantener la protección más actualizada contra virus transmitidos por correo electrónico.
Para proporcionar protección frente a correo electrónico interno corrupto, un plug-in de Microsoft Exchange permite a las organizaciones protegerse contra la propagación de virus que no acceden a la pasarela de correo electrónico. Las definiciones de virus también se actualizan con regularidad para garantizar la protección más actualizada.

Barracuda Central

Todos los productos de Barracuda cuentan con el soporte de Barracuda Central, un centro de operaciones de seguridad avanzado 24 x 7 que trabaja continuamente para supervisar y bloquear las amenazas de Internet más recientes. Barracuda Central reúne datos de más de 150.000 puntos de todo el mundo y los analiza para desarrollar defensas, reglas y firmas. A medida que van surgiendo nuevas amenazas, Barracuda Central actúa rápidamente para responder a brotes tempranos y proporciona las últimas definiciones mediante Barracuda Energize Updates. Estas actualizaciones no requieren administración en absoluto y garantizan que Barracuda Spam Firewall proporcione una protección completa y precisa contra las últimas amenazas de Internet.

Protección contra ataques de denegación de servicio (DoS)

No todos los ataques están orientados a conseguir que los usuarios envíen su número de tarjeta de crédito, que hagan clic en un enlace malicioso o a implantar un virus. A menudo, el objetivo del ataque está orientado a inhabilitar una red o reducir su eficacia. Como servicio basado en la nube, Barracuda Spam Firewall permite detener a los spammers antes de que sobrecarguen un servidor de correo electrónico.

Correo electrónico en cola

Barracuda Spam Firewall garantiza que se pueda seguir enviando correo electrónico incluso cuando se produzcan fallos del servidor de correo electrónico o pérdidas de la conectividad. En caso de interrupciones en las propias instalaciones, el correo electrónico se puede poner en cola en Cloud Protection Layer durante un máximo de 96 horas. También se puede especificar un destino alternativo para la entrega si la entrega al destino principal falla.
Durante las interrupciones de servicio del servidor de correo electrónico, el correo electrónico de todos los servidores de correo resulta visible por medio de Cloud Protection Layer. Desde el registro de mensajes, se puede ver el estado de todos los correos electrónicos en cola y si el correo se ha vuelto a entregar.

Filtrado previo de spam y virus

Barracuda Spam Firewall está integrado con un servicio basado en la nube que filtra previamente el correo electrónico antes de entregarlo al Barracuda Spam Firewall local. Cloud Protection Layer se actualiza continuamente con definiciones en tiempo real con actualizaciones de Barracuda Central. La elasticidad de la infraestructura de nube global de Barracuda proporciona la flexibilidad necesaria para gestionar picos de correo electrónico durante períodos específicos del día y durante ataques de denegación de servicio.

Cloud Protection Layer garantiza que la infraestructura de seguridad de correo electrónico de la organización se adapte al aumento del volumen de correo electrónico y del tamaño de los archivos adjuntos, así como al crecimiento de las empresas. Aprovechando el ancho de banda y la potencia de cálculo del CPL, las organizaciones pueden ampliar fácilmente su solución de seguridad de correo electrónico.

Cifrado

Barracuda Spam Firewall ofrece diversas funciones de cifrado. Está totalmente integrado con un servicio de cifrado de correo electrónico basado en la nube para el correo electrónico saliente. El correo electrónico que cumple con la política o que está marcado para el cifrado mediante Barracuda Outlook Add-in se envía por medio de TLS a Barracuda Message Center.

Barracuda Message Center utiliza AES con claves de 256 bits para cifrar el correo electrónico. Para cifrar tráfico el tráfico de correo electrónico entre sitios por Internet, Barracuda Spam Firewall Message Transport Agent admite SMTP sobre TLS. Se puede utilizar entre Barracuda Spam Firewalls u otros servidores de correo electrónico que admitan SMTP sobre TLS.

Barracuda Spam Firewall ofrece diversas funciones de cifrado. Está totalmente integrado con un servicio de cifrado de correo electrónico basado en la nube para el correo electrónico saliente. El correo electrónico que cumple con la política o que está marcado para el cifrado mediante Barracuda Outlook Add-in se envía por medio de TLS a Barracuda Message Center.

Filtrado de salida

El filtrado de salida evita la inclusión de las organizaciones en listas de bloqueo de spam e impide la salida de datos confidenciales de la organización por correo electrónico. Sin saberlo, los empleados pueden propiciar que los sistemas internos se conviertan en una fuente para el spam de botnet. Utilizando un subconjunto de sus capas de defensa, el filtrado de salida de Barracuda Spam Firewall detiene el spam y los virus de salida. También permite a los administradores aplicar políticas de contenido para la prevención de pérdida de datos (DLP) y para cumplir otros estándares de contenido en el correo electrónico de salida. Se pueden utilizar filtros predefinidos y políticas

personalizadas para detectar datos confidenciales y bloquear o cifrar correo electrónico.

Administración central basada en la nube

Barracuda Spam Firewall está integrado con el portal de administración basado en la web Barracuda Cloud Control (BCC), que aprovecha la infraestructura de nube global de Barracuda para permitir a las organizaciones administrar centralmente todos sus dispositivos mediante una interfaz “de un solo panel”. Los administradores obtienen una visión global de todos sus dispositivos o servicios y, además, pueden administrar centralmente las políticas y la configuración. La interfaz simple facilita a las organizaciones pequeñas y medianas la implementación y administración del servicio con un gasto de TI mínimo.

Si le interesa, pregunte por el resto de **productos Barracuda**:

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

Preguntas frecuentes sobre Barracuda Spam Firewall

¿Cómo protege Barracuda Spam Firewall frente a las amenazas por correo electrónico?

Barracuda Spam Firewall, una solución de hardware y software integrada, utiliza un método multicapa para ofrecer la protección de correo electrónico más completa que existe frente a ataques de spam, virus, suplantación, phishing y spyware. Una de las ventajas añadidas de Barracuda Spam Firewall es el procesamiento de cada correo electrónico para maximizar el rendimiento y la capacidad para filtrar millones de mensajes al día.
Detrás de las iniciativas líderes en el sector de Predictive Sender Profiling y Barracuda Real-Time Protection hay 12 capas de defensa explícitas, que son las siguientes: protección ante la denegación de servicio y seguridad, controles de velocidad, análisis de reputación de direcciones IP, autenticación de remitentes, verificación de destinatarios, protección ante virus, políticas (reglas especificadas por el usuario), análisis de huellas digitales, análisis de intenciones, análisis de imágenes, análisis bayesiano y un motor de puntuación de reglas de spam.

¿Cómo se filtra el correo electrónico?

Desplegado en el perímetro de la red, todo el correo electrónico entrante debe pasar a través de las 12 capas de defensa de Barracuda Spam Firewall antes de llegar al destinatario correspondiente. Las capas de defensa se agrupan en dos clases principales: gestión de conexiones, que implica soltar las conexiones de correo entrante antes de recibir mensajes, y escaneo de correo, que analiza los mensajes tras su recepción. Durante el proceso de filtrado, los correos electrónicos se verifican para detectar posibles ataques de spam nuevos o conocidos, virus y infracciones de políticas de administrador. En base a las preferencias del administrador y del usuario, el spam se puede etiquetar, dejar en cuarentena o bloquear.

¿Por qué se debe etiquetar el correo electrónico? ¿Qué ocurre con los correos electrónicos etiquetados?

Etiquetar el correo electrónico beneficia a las organizaciones ya que permite identificar fácilmente los mensajes que cumplen los criterios establecidos. Los correos electrónicos etiquetados se entregan al destinatario con una etiqueta personalizada, como [BULK], que se añade al asunto del

mensaje.

¿Por qué se debe dejar el correo electrónico en cuarentena? ¿Qué ocurre con los correos electrónicos en cuarentena?

Dejar los correos electrónicos en cuarentena es una medida de seguridad que permite examinar los mensajes cuestionables antes de aceptarlos o rechazarlos; generalmente, un correo electrónico en cuarentena se convierte en spam. Un administrador puede elegir dos tipos de correo electrónico en cuarentena: cuarentena global o cuarentena por usuario.
Cuando se configura para la cuarentena global, Barracuda Spam Firewall dirige todo el correo electrónico en cuarentena a un buzón especificado por el administrador. Cuando se configura para la cuarentena por usuario, Barracuda Spam Firewall almacena el correo electrónico de forma local e informa periódicamente a los usuarios sobre su correo electrónico en cuarentena. Los usuarios pueden optar por eliminar el correo electrónico en cuarentena, reenviarlo a sus propios buzones o incluir en una lista blanca la dirección del remitente para evitar que futuros correos electrónicos del remitente se pongan en cuarentena. La cuarentena por usuario está disponible con los siguientes modelos de Barracuda Spam Firewall: 300, 400, 600, 800 y 900.

¿Qué tecnologías se utilizan en Barracuda Spam Firewall?

Barracuda Spam Firewall utiliza una combinación de software de propiedad y software de código abierto. El sistema operativo Barracuda Spam Firewall se basa en un kernel de Linux estable y reforzado que ha pasado por un estricto escrutinio por parte de investigadores de seguridad. El robusto MTA puede gestionar un número elevado de conexiones SMTP y volúmenes elevados de entrega de correo. A partir del release 3.5 del firmware, Barracuda Spam Firewall MTA integra una función de registro de información que puede utilizarse junto con Barracuda Message Archiver.

Si utilizo Microsoft Exchange, ¿cómo me protegerá Barracuda Spam Firewall frente a ataques de “diccionario”?

Microsoft Exchange Accelerator, disponible en Barracuda Spam Firewall 300 y modelos superiores, utiliza el protocolo LDAP (Lightweight Dictionary Access Protocol) integrado en Exchange para verificar los destinatarios antes de entregar mensajes a Microsoft Exchange Server.

¿Qué nuevas tecnologías añade Barracuda Spam Firewall para combatir con las últimas campañas de spam?

Barracuda Networks ha anunciado varias iniciativas contra el spam:
Multi-Pass Optical Character Recognition Engine: el spam de imágenes generalmente incluye texto con imágenes con la intención de ocultar contenido omitiendo las capas de procesamiento de reglas de texto de los filtros de spam. &Con el motor OCR de varias pasadas y líder en el sector de Barracuda Networks, los cortafuegos Barracuda Spam Firewall hacen que los que trucos que utilizan los usuarios que envían spam para ocultar texto detrás de imágenes en color o desenfocadas sean inefectivos.

Predictive Sender Profiling: la solución Predictive Sender Profiling de Barracuda Networks investiga con más detalle los correos electrónicos enviados e indaga en la campaña para identificar posibles actividades anómalas del remitente, lo que permite a Barracuda Networks bloquear de forma efectiva el spam que generalmente no se puede detener mediante el análisis de reputación tradicional.

Barracuda Real-Time Protection: Barracuda Real-Time Protection utiliza un conjunto avanzado de tecnologías para bloquear de forma inmediata los virus y spyware más recientes, así como otros ataques de malware a medida que emergen. Gracias al uso de la vasta y diversa base de clientes de los cortafuegos de Barracuda Spam Firewall, Barracuda Networks lidera el sector en la detección de tendencias y en la respuesta las amenazas originadas por correo electrónico.

¿Cómo protege Barracuda Spam Firewall frente a las amenazas de virus?

Barracuda Spam Firewall proporciona una protección completa frente a las amenazas de virus a través de potentes capas. La primera capa consta de un reconocido motor de código abierto para el escaneo de virus. La segunda capa es un motor de virus de propiedad mantenido por Barracuda Central, un centro de operaciones de seguridad avanzado disponible de forma ininterrumpida que trabaja para supervisar y bloquear de forma continuada las últimas amenazas de Internet. La tercera capa es Barracuda Real-Time Protection, un conjunto de tecnologías avanzadas que permiten a los cortafuegos Barracuda Spam Firewall bloquear de forma inmediata los ataques más recientes de virus, spyware y otros ataques de malware a medida que emergen, sin tener que esperar a descargar una firma en Barracuda Spam Firewall.

¿Cómo bloquea Barracuda Spam Firewall las amenazas en tiempo real?

Los ingenieros de Barracuda Central trabajan diligentemente y de forma ininterrumpida para supervisar las amenazas de spam y virus de todo el mundo. Dado que los tiempos de respuesta son cruciales ante las amenazas en tiempo real, cuando se detecta una amenaza, Barracuda Spam Firewall utiliza uses Barracuda Real-Time Protection para mitigar estas amenazas porque emergen sin esperar nuevas actualizaciones.

¿Cuánto tiempo tendré que dedicar a la instalación y mantenimiento de Barracuda Spam Firewall?

Barracuda Spam Firewall está diseñado como solución fácil de instalar que requiere una sobrecarga administrativa mínima. Sin realizar ningún ajuste, Barracuda Spam Firewall ofrece un índice de precisión de detección de spam del 95% con un 0,01% de falsos positivos. Teniendo en cuenta las seis capas de defensa ajustadas automáticamente por Energize Updates, Barracuda Spam Firewall se mantiene actualizado fácilmente para garantizar la precisión del spam en curso.

¿Recibiré muchos falsos positivos con un Barracuda Spam Firewall?

Sin realizar ningún ajuste, Barracuda Spam Firewall está configurado para minimizar los falsos positivos, que suelen ser un 0,01% o menos, uno de los índices de falsos positivos más bajo del sector. Como ocurre con cualquier solución que permite la personalización de los usuarios, la devolución de falsos positivos de cada cliente variará en función de cómo ajuste el administrador la unidad (por ejemplo, un valor de puntuación de spam más estricto puede dar lugar a un número mayor de falsos positivos).

¿Qué incluye Energize Updates para Barracuda Spam Firewall?

La suscripción a Barracuda Energize Updates proporciona actualizaciones de las definiciones de spam y virus más recientes que bloquean nuevas campañas antes de que se conviertan en un brote. Los ingenieros de Barracuda Central actualizan constantemente las definiciones de spam y virus para poder ajustar de forma remota seis de las 12 capas de defensa, lo que permite minimizar el tiempo de administración. Energize Updates también ofrece acceso a soporte técnico, nuevos releases de firmware y la oportunidad de participar en el programa Barracuda Early Release Firmware.

¿Ofrece Barracuda Spam Firewall políticas por usuario?

Las políticas por usuario están disponibles en Barracuda Spam Firewall 300 y modelos superiores. Las políticas por usuario ofrecen a los usuarios la capacidad de definir sus propias políticas de puntuación individuales, base de datos bayesiana, lo que permite el uso de listas blancas y listas de bloqueo.

¿Puede Barracuda Spam Firewall filtrar los mensajes salientes?

Sí. Barracuda Spam Firewall filtra los mensajes salientes para detectar posibles virus y políticas de escaneo de spam básicas. Para el escaneo de salida avanzado, Barracuda Networks ofrece Barracuda Spam Firewall-Outbound, que incluye distintos flujos de trabajo para dejar en cuarentena el tráfico de correo electrónico de salida para que puedan revisarlo los auditores de políticas.

¿Cómo puedo bloquear o minimizar la cantidad de mensajes de rebote no válidos?

Los mensajes de rebote no válidos son informes de no entrega a direcciones de correo electrónico falsificadas. Para bloquear los mensajes de rebote no válidos, habilite la característica Invalid Bounce Suppression y traspase todo el correo electrónico saliente a través del dispositivo Barracuda Spam Firewall o Barracuda Spam Firewall-Outbound.

¿Permite Barracuda Spam Firewall a los administradores bloquear correo electrónico de otros países?

Sí. Barracuda Spam Firewall ofrece distintos métodos para bloquear correo electrónico de otros países:

1. En base a la búsqueda DNS inversa, los administradores bloquean los mensajes cuyo dominio de nivel superior se resuelve en el nombre de host de un país

2. En base al conjunto de caracteres declarado de un correo electrónico, los administradores bloquean mensajes que contienen un conjunto de idiomas específico.

3. Si bien Barracuda Networks no lo recomienda, los administradores crean políticas personalizadas para filtrar otros patrones en el asunto, la cabecera o el cuerpo de los mensajes para bloquear correo electrónico no deseado de otros países.