Servidor de correo integral seguro

Integral Secure Mail Server

Miguel Ángel Poza

Resumen

Se ha conseguido desarrollar un sistema integral de protección del correo electrónico que no sólo mantiene el buzón de entrada libre de código malicioso, sino que también permite al usuario saturado por el Spam recuperar el control sobre su cuenta de correo. El sistema dispone además de un entorno de administración web fácilmente configurable incluso para usuarios con conocimientos básicos de correo electrónico.

Palabras clave: Spam, código malicioso, protección.

Summary

An integral system of protection of the electronic mail has been developed. It maintains the mailbox free of malicious code entrances and allows those users saturated by Spam regain the control on its electronic mail account. The system has also a module of Web Administration, easily formable even by users with basic knowledge on electronic mail.

Keywords: Spam, malicious code, protection.

1.- Introducción

El servicio de Internet que mayor implantación ha tenido en nuestra sociedad es el correo electrónico, además de ser uno de los más antiguos. No obstante, este servicio actualmente está en serio peligro; hace ya algunos años, los virus empezaron a aprovecharse de las ventajas que ofrecía el correo electrónico para su propagación y conseguir a través de él expandirse a millones de ordenadores en muy pocas horas. Pero surgió otro problema mayor y con mucha más fuerza, el Spam que no deja de ser un concepto clásico aplicado en un medio moderno, ¿quién no ha recibido publicidad en su buzón de casa?. El auge tan explosivo de la publicidad no deseada en Internet, está fundamentado en el bajo coste del envío de esta publicad. En estos momentos, las últimas informaciones indican que entre el 70% y el 80% del correo mundial es Spam.

El servicio de Internet que mayor implantación ha tenido en nuestra sociedad es el correo electrónico, además de ser uno de los más antiguos

Para los usuarios se ha convertido en un gran problema ya que en algunas cuentas se llegan a registrar más 500 mensajes diarios de Spam; este número de mensajes y un número mucho menor supone la inutilidad de esa cuenta, o la pérdida de muchas horas revisando los mensajes para finalmente clasificar 4 ó 5 correos como válidos. Para solucionar este problema existen muchas plataformas de clasificación automática de correos que afirman bloquear un porcentaje muy alto de los mensajes de Spam, pero todas ellas son costosas, difíciles de configurar y de usar y, con una carga de conocimientos técnicos que la hacen inaccesible a la mayoría de las empresas que normalmente no cuentan con profesionales informáticos especializados en el correo electrónico.

Para los usuarios la recepción masiva de correo no deseado se ha convertido en un gran problema

Para solucionar este problema hemos diseñado una appliance servidor de correo en castellano con todas las características exigibles, al cual le hemos añadido un sistema antispam, un sistema contra el código malicioso (virus, documentos adjuntos peligrosos, html mal intencionado, phising, activeX, etc....), es de fácil administración y utilización y requiere un mínimo mantenimiento para conseguir unas prestaciones notables.

2.- Características del sistema

A continuación pasamos a presentar las características principales de nuestro sistema, acompañadas de una pequeñísima exposición:

- Hardware ampliamente testeado y comprobado en los diversos escenarios, capaz de procesar más de 5.000 correos diarios en su configuración hardware más básica, sin contabilizar los correos que directamente se rechacen por destinatario inexistente.
- Instalable en hardware de alto rendimiento que unido a la capacidad de balanceado de carga, nos proporcionaría alcanzar el procesamiento de millones de correos diarios.
- Monitorización e históricos de monitorización del hardware y servicios del sistema.
- Desarrollo de las utilidades necesarias basadas en software libre.
- Adaptable a nuevas instalaciones donde realice la función de *servidor de correo integral*, proporcionando todas las funcionalidades de servidor de correo; o adaptable a instalaciones ya existentes donde la incorporación de nuestro servidor no implicará reconfiguraciones del sistema existente, al hacer de *servidor pasarela* intermedia entre Internet y el servidor de correo existente.

Una de las características del servidor de correo diseñado consiste en que el desarrollo de las utilidades necesarias se ha basado en software libre

- Administración web bajo https de todos los módulos con ayudas on-line de todas las herramientas que se ofrecen.
- Firewall personalizable e integrado con la solución, basado en la herramienta de filtrado de paquetes *Iptables*.
- Protocolos POP, IMAP, POPS e IMAPS.
- Servicio de *webmail* bajo https.
- Backup programable por el usuario con posibilidad de respaldo remoto del sistema, tanto de la configuración como de los archivos contenidos en el sistema.
- Módulo estadístico y de monitorización de las colas de correo. Desde este interfaz es posible generar multitud de informes gráficos sobre los correos tratados por el sistema, así como manipular los registros sobre los que se basan estas estadísticas. También ofrece la posibilidad de manipular los mensajes almacenados en la cuarentena, reenviando aquellos mensajes que hayan podido ser bloqueados.
- Antivirus y protección contra código malicioso (*phising*, ActiveX, html sospechoso, etc...) actualizable a través de Internet.
- Utilización simultanea de métodos heurísticos, listas negras y filtro bayesiano para la detección de spam.
- Actualizaciones automáticas del sistema desde repositorios de software validado.
- Eliminación de *bounces* con conectores a servidores de buzones, para rechazo de usuario inexistentes.
- Sistema de filtrado por buzón, administrable por cada uno de sus dueños. Por medio de este sistema los usuarios pueden incluir reglas personalizadas de filtrado y clasificación de correos que ejecutará el servidor independientemente del cliente de correo.
- Sistema de notificaciones de clasificación del correo personalizables por el usuario

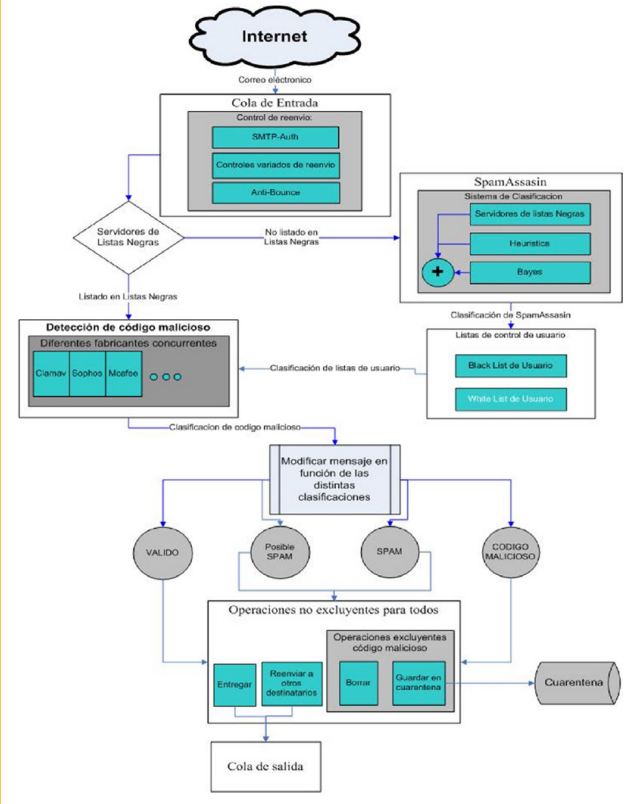
Para poder realizar una correcta configuración, el servidor diseñado posee un sencillo e intuitivo interfaz gráfico que proporciona todos lo medios necesarios, para realizar cualquier tipo de configuración con unos conocimientos básicos

Para poder realizar una correcta configuración, posee un sencillo e intuitivo interfaz gráfico que proporciona todos lo medios necesarios, para realizar cualquier tipo de configuración deseada con unos conocimientos básicos, de esta manera se ofrece la posibilidad de administrar este sistema desde cualquier parte del mundo con cualquier tipo de sistema electrónico que posea un navegador y casi por cualquier persona aunque no posea amplios conocimientos de informática.

3.- Presentación funcional

Tras esta breve presentación de las características más reseñables, mostramos un esquema funcional del sistema:

ESQUEMA FUNCIONAL DEL SISTEMA



Cuando el sistema atiende una petición de reenvío o entrega de un correo a través del protocolo SMTP, se realizan una serie de comprobaciones para aceptar dicho correo, la más interesante de éstas es la de *anti-bounce*, con esta comprobación se consigue no aceptar los correos destinados a un dominio cuyo buzón no existe, hemos desarrollado más este sistema para conocer en todo momento los buzones existentes independientemente de la localización del servidor de buzones.

Una vez aceptado el mensaje, se procede a consultar si el emisor de dicho mensaje está incluido en los servidores de listas negras, si está incluido en múltiples listas es posible omitir el resto del análisis para acelerar el proceso y conseguir ahorrar recursos al sistema, excepto el de detección de código malicioso. Si no se confía tanto en las listas negras es posible forzar a realizar siempre el resto de análisis.

Cuando el sistema atiende una petición de reenvío o entrega de un correo a través del protocolo SMTP, se realizan una serie de comprobaciones para aceptar dicho correo

Una vez aceptado el mensaje, se procede a consultar si su emisor está incluido en los servidores de listas negras

El módulo de *spamassassin* aplica un compendio de métodos de detección de spam, tales como son las reglas de heurística, un sistema estadístico bayesiano, y un nuevo análisis de listas negras del propio *spamassasin*. Estos tres métodos se relacionan entre sí acumulando puntos, de manera que un mensaje se clasificará en función de esta puntuación, tratándose el mensaje dependiendo de los umbrales que sobrepase.

El emisor del mensaje volverá a ser contrastado con una serie de listas (no servidores de listas) que gestiona el administrador del sistema, la Blacklist contendrá cuentas de correo, dominios, subdominios o direcciones IP que el administrador desea clasificar como SPAM independientemente de los resultados anteriores y con Whitelist se obtendrá el resultado inverso, manteniendo a salvo cualquier mensaje procedente de las líneas incluidas en esta lista asegurando la entrega del mensaje en el buzón correspondiente.

El último módulo de clasificación es el de detección de código malicioso, se inspecciona tanto el cuerpo del mensaje como todos sus adjuntos así como la ocultación y manipulación de extensiones

de ficheros. Este módulo puede incorporar diversos motores de búsqueda de código malicioso. Además se podrán tomar decisiones en función del tipo de fichero o extensión del mismo. Este módulo tiene independencia sobre el resto imponiéndose los criterios que aquí se establezcan sobre el del resto de los análisis.

El siguiente módulo, recogerá todas las clasificaciones que se han asignado al mensaje para clasificarlo en alguna de las siguientes etiquetas: Válido, SPAM, Posible SPAM y Código Malicioso. Dependiendo de la clasificación que se haya asignado a ese mensaje se podrán ejecutar acciones diferentes en todas ellas –o si el administrador así lo desea– se realizarán las mismas acciones.

El módulo de operaciones, aplica al mensaje una o más operaciones que el administrador del sistema ha asignado a cada una de las etiquetas. Si un mensaje es detectado como contenido peligroso, únicamente podrá ser guardado en la cuarentena o borrado, nunca enviado, aunque con el resto de mensajes se podrán realizar las acciones o conjunto de acciones que el administrador haya seleccionado, pudiéndo realizarse varias simultáneas como por ejemplo enviar, guardar y reenviar a otro destinatario diferente.

Si un mensaje es detectado como contenido peligroso, únicamente podrá ser guardado en la cuarentena o borrado, nunca enviado

4.- Conclusiones

Como se puede comprobar es un proyecto que incluye gran cantidad de posibilidades de acción, pudiéndose adaptar a las necesidades de cualquier usuario. Otra de las ventajas que tiene es la posibilidad de cambiar a múltiples configuraciones de una forma rápida y sencilla, sin tener conocimientos específicos sobre correo electrónico. Aparte de su sencillez de administración también presenta un volumen de análisis diario muy extenso, pudiendo dar servicio a un gran número de instituciones.

Miguel Ángel Poza Sanz
(mikelpoza@ibercom.com)
Proyecto de fin de carrera
UPV/EHU