

Hermes v2.0

Modulo de cuarentenas

La versión actual de Hermes no incluye soporte al uso de cuarentenas de usuario.

Tanto en Unizar como en DGA, la gestión de cuarentenas se delega a los servidores de buzones: se usa una carpeta (“spam”) del buzón del usuario para depositar los mensajes marcados.

Ahora, para la gestión de estas cuarentenas disponemos de varias utilidades que se encargan de generar los informes que se envían al usuario, gestionan la recuperación de mensajes y permite la actualización de listas blancas por usuario

Esto es cómodo para el usuario ya que en cualquier momento puede revisar esta carpeta y rescatar un mensajes pero tiene varios problemas:

- Carga al gestor de buzones con la tarea de recibir y archivar estos mensajes
- Consume espacio en los buzones
- Obliga a ajustar los programas de gestión de la cuarentena para que sean compatibles con el software de gestión de buzones.

En la nueva versión de Hermes, la gestión de cuarentenas iría integrada en el sistema, de manera que fuera independiente de los sistemas de gestión de buzones utilizado por las organizaciones.

Los mensajes de spam que haya identificado el sistema y que deban ponerse en cuarentena se derivaran a contenedores existentes en el mismo sistema, o a contenedores existentes en un sistema remoto. Esto permitiría centralizar las cuarentenas de varios sistemas de filtrado funcionando en modo cluster.

Para esto, debe incluirse en Hermes varios módulos:

- Soporte para la gestión de usuarios y alias mediante ldap
- interface web que permita al usuario revisar las cuarentenas y rescatar mensajes, así como definir las preferencias relativas a la acción sobre el spam, envío de informes, caducidad de los mensajes en cuarentena, listas blancas/negras de senders, etc.
- Los procedimientos de gestión de las cuarentenas deben ser compatibles con la posibilidad de utilizar un servidor remoto para las mismas o utilizar un sistema distribuido.

Funcionamiento de nuestra propuesta

Una vez analizado un mensaje entrante si es identificado como spam, el sistema consulta la acción programada según el dominio del destinatario. Las acciones pueden ser: rechazar, marcar, poner en cuarentena o hacer caso a las preferencias del destinatario.

Si la acción definida para el dominio o para el destinatario concreto es poner en cuarentena, el sistema redirigirá el mensaje hacia un “dominio de cuarentenas”.

Ejemplos:

- a) Mensaje XXX, identificado como spam y dirigido a varios destinatarios del dominio unizar.es. Como la preferencia establecida para el dominio unizar.es es “poner en cuarentena” el sistema reescribirá todas las direcciones de destino al dominio “cuarentena.unizar.es” (por ejemplo). En el sistema estará especificado el encaminamiento necesario para este nuevo destino. Podrá ser “localhost”, o un servidor remoto dedicado a la gestión de cuarentenas.
- b) Si la situación es que para el dominio unizar.es, las acciones sobre el spam dependen del usuario. El sistema consultará las preferencias de usuario y aplicará acciones diferenciadas a cada uno de ellos.

Tanto si el destino de los mensajes a poner en cuarentena es una maquina dedicada, como si el destino es localhost, necesitamos que se reconozca a los destinatarios como usuarios locales y que dispongan de un buzón de correo donde almacenar el spam. Para ellos utilizaremos las soluciones de “virtualización de usuarios”

La creación de las cuentas en el gestor de cuarentenas se hará en el momento de recibir el primer mensaje. Solo se crearan buzones para los usuarios válidos en el sistema destino.

Para hacer la comprobación de si los destinatarios son válidos lo ideal es tener acceso a un servidor LDAP de la organización. El uso de LDAP simplificaría también la gestión de alias. En caso de disponer de ldap se pueden hacer comprobaciones usando el protocolo SMTP y utilizando una tabla de alias suministrada por el administrador del servicio y mantener una base de datos local con los “nuevos usuarios del sistema”

Para depositar los mensajes en los buzones, como *mailer* se utilizará **maildrop** y como formato de buzones, **Maldir**. Esto nos permitirá utilizar con seguridad sistemas de almacenamiento tipo NAS si lo deseamos.

El contenido de los buzones de spam será accesible mediante la utilización de un servidor imap. Por tanto, en cada uno de los gestores de cuarentenas se instalará y configurará **dovecot**.

Los mensajes contenidos en los buzones de spam se “eliminarán” de manera periódica y automática, pudiendo configurarse el periodo de retención a nivel de administrador o de usuarios.

El usuario recibirá informes periódicos con los mensajes depositados en la cuarentena y dispondrá de herramientas simples para la recuperación de “falsos positivos”.

El usuario podrá acceder al contenido de las cuarentenas en cualquier momento, mediante la utilización de un interface web. Este interface le permitirá “rescatar” mensajes, cambiar sus preferencias o alimentar sus listas blancas/negras particulares.

Para el usuario, la localización física de las cuarentenas (un servidor dedicado o repartidas en cada una de las relays) será transparente. Si las cuarentenas están “repartidas”, el interface de acceso se encargará de recolectar los mensajes repartidos y presentarlos en una lista única.

La autenticación para el acceso al interface de usuario se delegará en el servidor POP/IMAP donde el usuario tienen su buzón de correo. Por ello el administrador del sistema establecerá el servidor a utilizar para cada dominio.

De manera regular, se eliminarán las cuarentenas correspondientes a usuarios que se han dado de baja.

Los mensajes rescatados de la cuarentena, tanto si se hace desde el **informe de spam** recibido, como si se hace desde el entorno de usuario, serán movidos al servidor de correo del usuario. En caso de que el usuario disponga de un servidor IMAP este movimiento es sencillo. Si solamente dispone de acceso POP, habrá que estudiar una solución.

Una vez montada toda la infraestructura y los módulos de gestión de las cuarentenas, es muy simple ofrecer un **servicio de backup** para los mensajes buenos. Esto permitiría al usuario recuperar cualquier mensaje perdido utilizando el mismo procedimiento que para rescatar mensajes de spam.

Opciones valoradas

Para el encaminamiento de los mensajes hacia el gestor de cuarentenas, su entrega en los espacios de cuarentena y el acceso a ellos hemos optado por utilizar herramientas existentes (mta+mailer+servidor imap). Esto evita desarrollar nuevas utilidades y hace el sistema mas versátil, permitiendo que sea el administrador el que decida donde almacenar el spam y como se accede.

Además esto facilita la integración de un **modulo de backup**

Se ha buscado una solución que elimine la necesidad de hacer una gestión de usuarios (altas, bajas, autenticaciones, etc) ya que esto aumentaría los costos de administración.

La posibilidad de que las cuarentenas se resuelvan en “localhost”, en vez de utilizar servidor dedicado facilita el despliegue del sistema en organizaciones pequeñas y medianas.

Para el acceso a los mensajes de cuarentena podríamos utilizar cualquier cliente webmail, en vez de desarrollar un interface propio. Pero esto confundiría al usuario, ya que *estaríamos matando moscas a cañonazos*, y no permitiría tener el spam “repartido” por varias maquinas. Además obligaría seguramente a tener que hacer una gestión de usuarios propia.

Una alternativa para la gestión de las cuarentenas es la utilización del modulo incluido con el software Amavis. Esta solución esta adaptada a su sistema de filtrado y se apoya en la utilización de una Base de datos. Esto nos obligaba a hacer ajustes en nuestro módulo de filtrado (criba) y a depender excesivamente de la disponibilidad de la Base de Datos. Por otra parte el desarrollo de un interface de usuario nos permite centralizar la gestión de las preferencias de usuario, las listas blancas/negras y el backup si se pone en servicio.

El funcionamiento del interface de gestión de usuarios será independiente del gestor de cuarentenas. Así podrá disponerse de él en el servidor web corporativo o en cada uno de los sistemas de filtrado.

Aspecto del sistema

Esta imagen da idea de cómo podría ser el interface del usuario:

Hermes User Manager

Backup Black List From White List From **Quarantine** Users Prefs Salir

From es Buscar Listado completo

|<< << 1 >> >>|

Quarantine for user pps@piedra.unizar.es (3230/3230)

rescatar	1	Mon, 09 Feb 2009 20:57:46 -0300	Abram Dennis	Please Check
rescatar	2	Tue, 10 Feb 2009 05:33:14 +0530	Cornelius Winkler	Your Female Needs More? Its Easy!
rescatar	3	Mon, 9 Feb 2009 22:03:12 -0300	John Peiers	Make Your Man's Carrot Grow
rescatar	4	Tue, 10 Feb 2009 02:36:29 +0200	Euro Dice Casino	Euro Dice Casino. 2,500 EUR Grats. ¿Qué Es Lo Que Espera?
rescatar	5	Mon, 09 Feb 2009 21:09:16 -0300	Aguia Cortaz	Brand Items And Dirty Cheap Price
rescatar	6	Mon, 9 Feb 2009 22:13:07 -0300 (PST)	Deloris Kincaid	Feel The Extreme Power Of Young Years On Your Side.
rescatar	7	Mon, 9 Feb 2009 21:13:13 -0300 (PST)	Britney Washington	Efficient Pills Preventing Ovulation Processes.
rescatar	8	Mon, 09 Feb 2009 20:13:43 -0500	Euro Casino	Venga Y Juegue En Euro Casino