Hermes I Mail Firewall Appliance

Solución para estafeta de correo electrónico con funciones de cortafuegos y control de virus y spam

Versión 1.0.36

Presentación

El servicio de correo electrónico de las organizaciones (sean grandes instituciones o pequeñas empresas) se ha convertido en una infraestructura básica para su buen funcionamiento. No solo es un servicio imprescindible, sino también complejo.

En los últimos años hemos asistido a la conversión del correo electrónico en una puerta abierta a la entrada de virus, gusanos y basura en general en las organizaciones. Esta situación degrada el servicio de correo, hace perder tiempo y dinero, obliga a dedicar cada vez mas recursos y pone en entredicho la buena imagen de la organización. Un servicio de correo mal administrado se convertirá seguramente en un problema de seguridad para la organización

En este momento la instalación, configuración y mantenimiento de un servicio de correo de calidad requiere recursos dedicados y sobretodo personal especializado.

Hermes nació, fruto de la colaboración entre la ***Universidad de Zaragoza*** y el ***Gobierno de Aragón***, como una solución software pensada y desarrollada para dar respuesta a la necesidad de poner en marcha un estafeta que actúe de pasarela y cortafuegos entre los servidores de correo de la organización y el resto de la Internet.

En su versión actual (**1.0.xx**) se presenta como un paquete debian que al aplicarse sobre una plataforma preinstalada con un S.O. Debian Etch, añade todos los modulo necesarios y los configura para que el sistema pueda actuar como un firewall de correo electrónico. También configura el S.O.base para asegurarlo y optimizar su funcionamiento, así como para dotarlo de todas las herramientas necesarias para monitorizar el sistema y poder administrarlo de forma cómoda

Todos los componentes de Hermes están basado en software libre y el resultado final esta liberado con **licencia GPL**

Hermes incluye toda la experiencia acumulada por el Servicio de Correo de la Universidad de Zaragoza y en gran medida toda la experiencia destilada del foro IRIS-MAIL que promueve **RedIris** y en el que participan todas las instituciones de la red académica española.

Por ello se ha tenido especial interés en que una instalación basada en hermes cumpla con los requisitos de calidad establecidos en el proyecto **RACE** (wwr.rediris.es/race) y facilita la utilización de iniciativas surgidas del foro **ABUSE** (http://www.rediris.es/abuses/) para el mantenimiento de listas blancas de organizaciones reconocidas, así como la participación en la red de sensores de spam y virus desplegada por **INTECO** (www.inteco.es)

Uso de Hermes

Hermes es una solución para la ***relay de correo*** de la organización. Por ello permite actuar como filtro para la mensajería que entra en la organización así como para encaminar el correo que se genera dentro de la misma.

No es un gestor de correo y por ello no esta pensado para gestionar los buzones de los usuarios. Al independizar los procesos de filtrado y encaminamiento de los mensajes es **compatible** con cualquier plataforma de correo.

En la actualidad la disponibilidad del servicio de correo es critica para cualquier organización. Por ello, Hermes esta pensado para funcionar en un sistema de **alta disponibilidad** y balanceo de carga, donde dos o mas sistemas pueden actuar de forma solidaria para ofrecer el servicio.

En la versión actual, Hermes no incluye un sistema propio para la gestión de las cuarentenas, apoyándose para ello en algunos desarrollos complementarios adaptados a instalaciones basadas en ***Dovecot*** y en ***SUN Java System Mesaging Server***. En una próxima versión, Hermes incluirá soporte completo para la gestión de cuarentenas de usuario. Esto facilitará su integración con cualquier sistema de correo.

Sistema Operativo

El proceso de instalación de hermes esta pensado para intervenir son una instalación base de un sistema **Linux Debian** (versión Etch), aunque podría instalarse sin demasiada dificultad sobre otros sistemas como Solaris o BSD.

La instalación y posterior configuración de Hermes incluye en el sistema todas los paquetes, librerías y scripts necesarios, y configura todos los módulos para ajustarlos a las tareas de relay.

El administrador podrá añadir al sistema cualquier otro software que necesite (agentes para la realización de copias, por ejemplo) , siempre que no interfieran con las herramientas utilizadas por Hermes.

Para agilizar las consultas al dns, el sistema incluye un servidor de dns (**bind**) en modo caché.

Alta disponibilidad y Balanceo de Carga

Cuando todo el trafico de correo de la organización pasa por un único punto debemos plantearnos el uso de una plataforma de alta disponibilidad. Hermes incluye soporte para facilitar su uso en un escenario de este tipo.

Para montar Hermes en modo AD tenemos varias alternativas:

- Poner dos máquinas Hermes configuradas de la misma manera y utilizando el *RoundRobin* de DNS. Esto puede servir para el uso de Hermes como relay pero es insuficiente cuando se usa como SMTP Sever.

- Poner dos maquinas Hermes configuradas de la misma manera, en una granja de equipos gestionados por un *balanceador de carga*. El la opción mas recomendable pero la mas cara

- Activar en Hermes el software de cluster que viene preconfigurado y que permite que 2 o mas máquinas trabajen en Alta Disponibilidad y Balanceo de Carga. Para implementar estas funcionalidades utiliza un combinación de *herartbeat* y *ldirector*. El funcionamiento en modo cluster es experimental.

En cualquiera de las tres situaciones, Hermes dispone de herramientas para sincronizar los ficheros de configuración entre los miembros del cluster, agrupar la información estadística y obtener su representación gráfica.

Configuración y Administración

Hermes dispone de un **interface gráfico**, accesible mediante web para la configuración del sistema, su monitorización y su actualización. En el entorno gráfico solamente se incluyen las

aquellas opciones que suelen modificarse; el resto se configura con valores "por defecto" aunque pueden ser cambiadas por el administrador modificando los ficheros de configuración.

El uso del entorno grafico es completamente compatible con el manejo directo de los ficheros de configuración. Los cambios desde el entorno grafico se reflejaran en los ficheros de configuración usados por las aplicaciones utilizadas y viceversa.

En el sistema pueden definirse **usuarios** a los que se les asignaran perfiles diferenciados con distinto nivel de acceso al sistema (admnitrador, operador, etc)

Seguridad del Sistema

Hermes es un sistema que por su cometido esta accesible desde Internet y por tanto es importante que disponga de las herramientas de seguridad suficientes como para impedir accesos ilícitos y detectar situaciones comprometidas. Para ello:

- Incluye ***Tripwire*** como sistema para el chequeo de la integridad del sistema. La política preestablecida permite detectar modificaciones sospechosas en ficheros importantes del sistema

- Usa ***iptables*** para controlar el acceso tcp al sistema y definir un firewall. Desde el entorno grafico puede modificarse la política de acceso de forma sencilla

- Dispone de herramientas para la realización de ***copias de seguridad*** del sistema mediante la utilización de un servidor FTP o utilizando discos locales. Pueden definirse distintas políticas de copias para los ficheros de configuración y para los de datos. Este mecanismo es compatible con otros sistemas de copias de seguridad corporativos.

- El **acceso al sistema** queda restringido al entorno grafico o al uso de ssh.

- La web de administración esta protegida por el uso de **SSL** en el servidor Apache. Inicialmente se utilizan certificados X509 autofirmados, pero puede utilizarse cualquier otro.

Monitorización y sistema de alarmas

Desde el entorno gráfico se tiene acceso a una colección completa de tablas de datos y gráficos que representan el rendimientos y evolución de sistema: cpu, memoria, discos, procesos, mensajes procesados, situación de las colas, etc.

Además, el sistema dispone de un agente encargado de realizar el chequeo automático de todos los módulos del sistema y enviar alarmas en caso de necesidad. Este sistema realiza mas de 50 test de forma periódica.

Toda esta información sobre el rendimiento del sistema y la ejecución de los tests es accesible desde el entorno web y también utilizando el protocolo **SNMP**. Para ello se ha definido un MIB particular que recoge toda la información del sistema. Las alarmas, si se producen se envían mediante correo electrónico.

MTA (Mail Transfer Agent)

Como sistema de gestión del correo, Hermes puede utilizar ***Sendmail*** o ***Postfix*** (experimental). El software de MTA se configura para que realice adecuadamente las funciones de encaminamiento de mensajes (*relay*) y de SMTP Server (*submit*).

El encaminamiento de mensajes pude configurarse para hacerlo por dominios, por usuarios (mediante el uso de LDAP) o por ambos.

En el transporte de mensajes se utiliza **SSL/TLS** si el otro extremo lo permite

Si se utiliza Sendmail como MTA, Hermes define **varias colas** de correo, con prioridades y políticas de reenvío diferentes.

Para el filtrado de mensajes, el software de mta se comunica mediante el uso de librerías Milter con la aplicación ***Criba***. Esta aplicación se encarga del chequeo de virus, detección de spam, control de flujo de mensajes, etc.

Filtrado de Mensajes. Políticas de aceptación/rechazo de mensajes

Permite establecer las condiciones para la aceptación o rechazo de los mensajes. Aunque algunas de estos mecanismos pueden definirse directamente en la MTA (Sendmail o postfix), es preferible hacerlo en el software de filtrado (criba) para que el tratamiento de los mensjas y la información resultante sea consistente. Los controles mas importantes son:

- El sistema esta configurado para impedir el ***open relay***.
- Para los mensajes internos (locales más autenticados) se hace un control sobre la ***validez del remite***.
- Se comprueba si el origen del mensaje esta incluido en una lista local de equipos que tienen prohibido el envío: **Local Black List**
- Se rechazan los mensajes que contienen alguna cabecera cuyo contenido responde a los patrones incluidos en el fichero de cabeceras a rechazar: ***Headers Filtres***
- Se rechazan los mensajes que sobrepasan el límite establecido para el flujo de mensajes por unidad de tiempo: ***Rate Control***
- Se chequea el tamaño de los mensajes y se rechazan los que lo sobrepasan. Los tamaños permitidos pueden definirse según el tipo de mensaje (local, autenticado y remoto): ***Size Control***
- Se controla el número de destinatarios de cada mensaje. Puede ser diferente según el tipo de mensaje: ***Max Rcpts***
- Para los mensajes de entrada, se comprueba la existencia real de cada destinatario. Esto permite rechazar en la relay los mensajes con destino desconocido: ***Users Unknows.*** Para esto puede utilizarse **LDAP** o ejecutar comandos **Mail To:**
- Se pueden configurar el sistema para impedir, o al menos dificultar, los ataques de directorio: ***Directory Harvest Attack***
- Se hace un análisis del contenido ***para detectar virus***. En caso afirmativo, el mensaje se descarta. Como antivirus se utiliza ***clamav***, actualizado cada 30 minutos.
- Detección y eliminación de “bounces ilicitos”: rebotes de mensajes que utilizan remites de la organización pero no han sigo originados en ella: **Bounces Verification**

Detección de Spam

El sistema antispam permite combinar algunas de las herramientas mas utilizadas para la identificación de correo basura, minimizando el riego de identificación errónea:

- Uso de **listas blancas** distribuidas mediante el DNS. De este tipo son las administradas por el Foro Abuse (mtawl y eswl).

- Uso de "**lista blanca por usuario**" que permite aceptar los mensajes procedentes de una lista de direcciones administrada por el destinatario.

- Aceptación de los mensajes enviados por **gestores de listas**.

- Uso de sistemas de reputación para el origen de los mensajes: **DNSBL** (SpamCop, SpamHaus, por ejemplo). Puede utilizarse una o varias.

- Utilización de **filtros bayesianos** para el análisis de contenidos. Para esto puede utilizarse ***SpamAssassin*** y/o ***Bogofilter***. Por rendimiento y precisión recomendamos el uso de Bogofilter.

- Análisis de contenidos para la localización de URL identificadas como sitios de alojamiento de spam: ***URIDNSBL***

- Chequeo de registros ***SPF***

- Análisis sobre el cumplimiento de los RFC (uso correcto del ***helo***, uso ***de resolución directa y/o inversa***, etc)

Para los mensajes identificados como spam por uno o varios de los métodos descritos, pueden definirse **acciones diferenciales por dominios o por usuarios**: rechazar el mensaje, marcarlo, enviarlo a cuarentena.

Para marcar los mensajes, Hermes incluye cabeceras especiales (***X-Spam_Hermes***) en los mensajes y también puede modificar el ***Subject*** para indicar la identificación.

Con este esquema y manteniendo actualizada la bases de datos de los filtros bayesianos, alcanzamos tasas de identificación correcta **superiores al 99%, con tasas de falsos positivos despreciables**.

Gestión de Cuarentenas

Aunque las tasas de falsos positivos son muy bajas, el riesgo que supone la pérdida de algunos mensajes hace imprescindible el uso de un sistema de cuarentenas que pueda gestionar el usuario.

En este momento, Hermes no incluye soporte interno para la gestión de cuarentenas. Por ello ahora estamos utilizando como espacio de cuarentenas una carpeta del buzón del usuario final junto con algunos filtros y unos scripts que facilitan al usuario la localización de falsos positivos, su recuperación y el mantenimiento de listas de excepciones particulares (listas blancas por destinatario.

Para los usuarios que solicitan el uso de cuarentenas, los mensajes identificados y marcados por el sistema de filtrado son depositados en una carpeta (spam) de su buzón de correo. En esta carpeta los mensajes permanecen un tiempo determinado y después se eliminan.

El usuario recibe diariamente un report con la lista de mensajes de spam enviados a la cuarentena y un procedimiento automático para la recuperación de mensajes.

En próximas versiones de Hermes, la gestión de cuarentenas estará integrada para conseguir un sistema mas independiente y mas cohesionado.