# Hermes: Mail Firewall Appliance

## Hermes: Mail Firewall Appliance

P. Pérez, B. Pérez y P. Sancho


### Resumen

**Hermes** es una solución software para estafeta de correo electrónico con funciones de cortafuegos y antispam. Incluye soporte para el encaminamiento de mensajes, dominios virtuales, control de virus y spam. Dispone de un interfaz gráfico, para que su configuración sea fácil, que permite el acceso a todos los mecanismos de control y protección necesarios, así como a las estadísticas sobre el servicio. Esta solución se presenta como distribución Linux basada en Debian con licencia GPL y puede descargarse en http://hermes.unizar.es/descargas.


**Palabras clave:** relay, antispam, antivirus, mail, GPL.


### Summary

**Hermes** is a software solution for electronic mail relay with firewall and antiSpam functions. It includes: messages routing, virtual domains and control of virus and Spam. It has a graphical interfaz so that their configuration is simple and it allows access to all the necessary control and protection mechanisms, as well as to the statistics on the service. This solution is a Linux distribution based on Debian with license GPL and can be downloaded from http://hermes.unizar.es/descargas.


**Keywords:** relay, antispam, antivirus, relay, GPL

Hermes es una solución software para estafeta de correo electrónico con funciones de cortafuegos y antispam

## 1.- Características

A continuación describimos algunas de las características que posee:

- Solución completa pero abierta y estándar.
- Su instalación no requiere la dedicación de personal especializado en correo electrónico, dando así respuesta a las necesidades de seguridad en el servicio de correo a organizaciones medianas y pequeñas que no disponen de personal técnico especializado. Facilita la escalabilidad del sistema con recursos proporcionados para poder responder también a las necesidades de una organización grande.
- Compatibilidad con la infraestructura de correo electrónico existente en la organización para servidor de buzones y gestión de usuarios.
- Minimiza las tareas de administración y configuración del sistema.
- Securiza completamente el sistema y cada uno de sus componentes.
- Dispone de un sistema de monitorización completo y estándar.
- Integra exclusivamente componentes software libre, los módulos implementados se han desarrollado bajo licencia GPL y son actualizables a través de Internet.
- El desarrollo del proyecto **Hermes** se materializa en una distribución temática, en soporte CR-ROM, cuya instalación y configuración en un hardware dimensionado adecuadamente, permite la puesta en servicio de un auténtico firewall de correo electrónico.

Su instalación no requiere la dedicación de personal especializado en correo electrónico, dando así respuesta a las necesidades de seguridad en el correo a organizaciones medianas y pequeñas que no disponen de este tipo de personal

## 2.- Módulos que integran Hermes

### 2.1.- Sistema Operativo

Hermes es una distribución basada en Debian Sarge especialmente ensamblada para el cometido de *firewall* de correo electrónico. En esta distribución se incluyen todos los paquetes necesarios, así como los asistentes para la instalación y configuración ajustados para la tarea a desempeñar, sin que sean necesarios conocimientos especiales sobre el sistema operativo.

### 2.2.- Software de MTA (Mail Transfer Agent)

La principal tarea a realizar por el sistema es la de encaminar el correo entre la organización y el exterior, así como entre los distintos servidores internos. Para esta tarea hemos optado por Sendmail. La utilización de Sendmail aquí es totalmente compatible con el uso de otra software de MTA en los servidores de correo internos.

La principal tarea a realizar por el sistema es la de encaminar el correo entre la organización y el exterior, así como entre los distintos servidores internos

El software de MTA dará respuesta a las tareas de:

- Encaminamiento de mensajes entre los servidores internos y entre estos y el exterior
- Gestión de colas de mensajes, descargando a los servidores internos
- Comunicación con los sistemas antivirus y antispam
- Gestión de dominios y direcciones virtuales
- Opcionalmente, autenticación de los mensajes enviados por los usuarios de las distintas organizaciones
- Generación del fichero de log

La configuración inicial, los parámetros de funcionamiento y las tareas de administración (arranque y parada, monitorización, gestión de colas, etc.) son accesibles desde el entorno web de administración.

El servidor SMTP incluye autenticación mediante la extensión SMTP AUTH y soporte para acceso a LDAP.

### 2.3.- Antivirus y Antispam

Las tareas de antivirus y antispam se encomiendan a la utilidad Criba desarrollada por la Universidad de Zaragoza

Estas tareas se encomiendan a la utilidad Criba (con el antivirus Clamav y el analizador de contenidos SpamAssassin). Criba ha sido desarrollada por la Universidad de Zaragoza (http://webmail.unizar.es/desarrollo/criba) y se está utilizando de forma satisfactoria en varias universidades.

Sus características principales son:

- Todos los mensajes se chequean antes de ser aceptados
- Para analizar los mensajes se utiliza el antivirus Clamav
- Permite definir acciones (rechazar, avisar, eliminar, etc.) según el virus
- Se hace un control de flujo por IP
- Pueden utilizarse una o varias Listas Negras para chequear la procedencia del mensaje
- Filtros Bayesianos y Heurísticos para analizar el contenidos (SpamAssassin)
- El spam se marca o rechaza según destinatario y de diferentes modos
- Se genera un completo fichero de log

## 2.4.- Sistema de explotación de estadísticas

Una de las herramientas más importantes para administrar adecuadamente un servicio de correo electrónico es disponer de información en tiempo real tanto sobre la evolución del tráfico como sobre los flujos de información o sobre el comportamiento del sistema en el momento de carga máxima, etc.. Solamente disponiendo de información estadística suficiente podremos dimensionar adecuadamente los recursos con el fin de poder prever las necesidades futuras.

Como fuente de información para las estadísticas se utilizará combinadamente la información de logs generada por el MTA y por los sistemas antivirus y antispam combinado con el sistema de representación gráfica RRDBtool.

## 2.5.- Monitorización

Se utiliza una combinación de herramientas desarrolladas explícitamente y utilidades incluidas en los paquetes que dan soporte a la alta disponibilidad (*ldirector* de *Ultra Monkey*).

La monitorización del sistema es accesible vía SNMP y para ello se utilizan las utilidades desarrolladas por el proyecto *Net-SNMP.*

## 2.6.- Interfaz de administración

El principal componente para que el sistema cumpla las características de *appliance* que se pretende, es disponer de un interfaz simple, homogéneo y suficiente para configurar y administrar cada uno de los componentes.

Se utiliza un interfaz web bajo https que permite el acceso a las tareas de administración, al sistema de monitorización y a las estadísticas. Para esto, el sistema incluye un servidor web *Apache*.

Este módulo se ha desarrollado íntegramente utilizando una combinación de HTML, Perl y PHP. Los CGIs actúan, ajustando los ficheros de configuración propios de cada módulo y deberán ser compatible con la modificación manual de los mismos.

Lo principal para que el sistema cumpla las características de appliance, es disponer de un interfaz simple, homogéneo y suficiente para configurar y administrar cada uno de los componentes

## 2.7.- Soporte a la Alta Disponibilidad

Uno de los requerimientos importantes del sistema es que pueda escalar hacia una arquitectura de alta disponibilidad y/o balanceo de carga a un coste razonable y sin la necesidad de utilizar elementos hardware externos al sistema.

El sistema incluye soporte a la alta disponibilidad mediante la utilización de *software de cluster* utilizando las herramientas desarrolladas por el proyecto *Ultra Monkey.* Todos los sistemas de monitorización y gestión están preparados para manejar un sistema de estas características.

## 2.8.- Copias de Seguridad

Por su versatilidad se ha optado por utilizar *rsync* para mantener un sistema de copias de seguridad barato y eficiente del sistema, sin necesidad de utilizar un hardware específico. Esto, además, facilitará las tareas de sincronización de archivos en caso de la utilización de varios equipos en modo cluster.

Por su versatilidad se ha optado por utilizar rsync para mantener un sistema de copias de seguridad barato y eficiente del sistema

## 2.9.- Soporte a TLS y certificación

Todas las comunicaciones entre el interior y el exterior (vía http, smtp, etc.) están securizadas mediante la utilización de TLS y certificados X509.

Los certificados necesarios para ello deben ser proporcionados por la organización aunque inicialmente se proporcionaran unos certificados provisionales firmados por la autoridad de certificación del proyecto.

**Hermes** ha sido desarrollado con un proyecto co-financiado por la Universidad de Zaragoza y el Gobierno de Aragón a través de la subvención otorgada por el Departamento de Ciencia, Tecnología y Universidad para actuaciones de promoción e implantación de tecnologías de la información en el año 2004. Las tareas de definición y coordinación del proyecto corresponden a personal del Área de Sistemas del Servicio de Informática y Comunicaciones de la Universidad de Zaragoza (Pascual Pérez, Borja Pérez, Pilar Sancho) y en el desarrollo del proyecto han colaborado David Sánchez y Jorge Bernal.

Se puede encontrar más información al respecto en: http://hermes.unizar.es

Todas las comunicaciones entre el interior y el exterior (vía http, smtp, etc.) están securizadas mediante la utilización de TLS y certificados X509

**Pascual Pérez,**
(pascual.perez@unizar.es),
**Borja Pérez,**
(borja@unizar.es),
**Pilar Sancho**
(pilar.sancho@unizar.es)
Servicio de Informática y Comunicaciones
UNIZAR