novática
CEPIS UPGRADE Revista de la Asociación de Técnicos de Informática

Novática, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de **ATI** (Asociación de Técnicos de Informática), organización que edita también la revista **REICIS** (Revista Española de Innovación, Calidad e Ingeniería del Software). ***Novática*** edita asimismo **UP**GRADE, revista digital de **CEPIS** (*Council of European Professional Informatics Societies*), en lengua inglesa, y es miembro fundador de **UP**ENET (**UP**GRADE *European* ***NET****work*).

<http://www.ati.es/novatica/>
<http://www.ati.es/reicis/>
<http://www.upgrade-cepis.org/>

ATI es miembro fundador de **CEPIS** (*Council of European Professional Informatics Societies*) y es representante de España en **IFIP** (*International Federation for Information Processing*); tiene un acuerdo de colaboración con **ACM** (*Association for Computing Machinery*), así como acuerdos de vinculación o colaboración con **AdaSpain**, **AI2**, **ASTIC**, **RITSI** e **Hispalinux**, junto a la que participa en **ProInnova**.

Coordinación Editorial, Redacción Central y Redacción ATI Madrid
Padilla 66, 3º, dcha., 28006 Madrid
Tlfn.914029391; fax.913093685 <novatica@ati.es>
Composición, Edición y Redacción ATI Valencia
Av. del Reino de Valencia 23, 46005 Valencia
Tlfn./fax 963330392 <secreval@ati.es>
Administración y Redacción ATI Cataluña
Vía Laietana 46, ppal. 1ª, 08003 Barcelona
Tlfn.934125235; fax 934127713 <secregen@ati.es>
Redacción ATI Aragón
Lagasca 9, 3-B, 50006 Zaragoza.
Tlfn./fax 976235181 <secreara@ati.es>
Redacción ATI Andalucía <secreand@ati.es>
Redacción ATI Galicia <secregal@ati.es>
Suscripción y Ventas <http://www.ati.es/novatica/interes.html>, ATI Cataluña, ATI Madrid
Publicidad
Padilla 66, 3º, dcha., 28006 Madrid
Tlnf.914029391; fax.913093685 <novatica@ati.es>
Imprenta: Derra S.A., Juan de Austria 66, 08005 Barcelona.
Depósito legal: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Portada: Viento en popa - Concha Arias Pérez / © ATI
Diseño: Fernando Agresta / © ATI 2003

Nº 200, julio-agosto 2009, año XXXV

sumario

Monografía del próximo número:
"Presente y futuro de la Informática en Europa"

Certificación RACEv2 del Servicio de Correo Electrónico del Centro Astronómico Hispano-Alemán de Calar Alto

Enrique de Guindos Carretero
Centro Astronómico Hispano-Alemán A.I.E. de Almería, Departamento de Informática; socio senior de ATI

<guindos@caha.es>

Resumen: *el servicio de correo electrónico de cualquier empresa es algo vital para su buen funcionamiento. Aplicando unos criterios de calidad y seguridad a este sistema, no sólo prestaremos un mejor servicio a nuestros usuarios, sino que también contribuiremos a mejorar y avanzar en las comunicaciones electrónicas globales.*

Palabras clave: *correo electrónico, Postfix, RACE, RedIRIS, relay, spam, SPF, submission, webmail.*

1. Introducción

Hablar a estas alturas de la necesidad de tener un sistema de correo electrónico eficaz y seguro en cualquier empresa, resulta algo obvio. Sin embargo, no resulta menos claro el hecho de que todavía muchas compañías, aún disponiendo de correo electrónico propio, no dedican a él el suficiente tiempo y medios para darle la necesaria seguridad y calidad.

La iniciativa RACEv2 [2] de RedIRIS [1], la red Académica y de Investigación Española (ver **figura 1**), define una serie de criterios y normas que deberían cumplir los servidores de correo electrónico para ofrecer un servicio seguro y de calidad. Esta iniciativa, además, realiza las auditorías necesarias para constatar que los servidores que optan al certificado de calidad que otorga RACEv2, cumplen con dichos criterios. En este sentido, una institución que obtenga la certificación RACEv2, se convierte inmediatamente en evaluadora de futuros centros que soliciten dicha catalogación. El Centro Astronómico Hispano-Alemán de Calar Alto, tras conseguir su certificado, ha participado en la evaluación de la Universidad de Las Palmas de Gran Canaria.

El presente artículo pretende hacer comprender a todo el mundo la importancia que tiene, hablando del servicio de correo electrónico, un servidor bien configurado y con unas medidas mínimas de seguridad y calidad. La iniciativa RACEv2 ha sido propuesta dentro de la Red Académica y de Investigación, pero sus principios deberían trascender a cualquier empresa que preste servicios de correo electrónico, tanto si pertenece a dicha red como si se trata del ámbito privado. En [2], se pueden ver los criterios que se deben seguir para conseguir unos resultados mínimos de seguridad y calidad.

Calar Alto logró la catalogación RACEv2 de Nivel Avanzado en agosto de 2008. Las instituciones que hasta la fecha han obtenido el certificado se pueden consultar en [3].

2. De dónde partíamos

Figura 1. Logotipo del proyecto RACE (Red Académica de Correo Electrónico) de RedIRIS.

A finales del siglo pasado, el correo electrónico en Calar Alto estaba en manos de Sendmail corriendo en un antiguo servidor SUN. Por aquel entonces, el *spam* no era un problema tan grave como actualmente, aunque empezaban las primeras quejas de los usuarios. Por entonces no teníamos ningún sistema *anti-spam* ni anti-virus en el servidor de correo y, realmente, se le prestaba poca atención a dicho servicio. Funcionaba, y sencillamente eso era suficiente para aquella época. El servicio que ofrecíamos se limitaba a un sencillo POP3 sin ningún tipo de seguridad, para que los usuarios pudiesen leer su correo desde lectores como Netscape, entre otros. Incluso había muchos usuarios que simplemente utilizaban el programa `mailx` como gestor de sus correos.

Esta situación cambió rápidamente. El primer problema fue el aumento progresivo del *spam* y de los virus de correo. También se incrementaron las peticiones para la creación de interfaces de *webmail* y nuevos servicios.

Tal y como estaba planteado el sistema en Calar Alto, era muy difícil atender todas las necesidades nuevas a partir de lo que había. La decisión que se adoptó fue la de empezar todo desde cero, intentando utilizar software con licencia libre para el proyecto.

Calar Alto es una institución pequeña. El número de usuarios de correo no excede de los 100. Por ello, tampoco se requerían grandes y complejos sistemas. Además, también hay que contar con que los recursos de personal que pudiesen dedicarse a construir todo desde la base, eran muy limitados.

3. A dónde queríamos llegar

Finalmente, y tras probar algunas posibles soluciones, se decidió atacar la nueva estructura partiendo del programa Postfix de Witese Venema [4] sobre un servidor Linux (actualmente funcionando en una máquina virtual).

Postfix es un agente de transporte de correo (MTA) muy seguro, consistente en varios componentes, cada uno de los cuales corren con privilegios bajos. Además, ninguno de ellos confía directamente en los datos de otro sin que previamente se hayan validado. El rendimiento, que también es muy bueno, no suponía un problema, ya que el total de correos manejados no es excesivamente grande, dada las dimensiones de nuestro centro.

Para finalizar, Postfix provee una interface de comandos compatible con Sendmail y una integración realmente sencilla de otros programas *anti-spam*, anti-virus o de identificación del remitente, entre otros. En la **figura 2** se ve un diagrama de bloques reducido (con las colas sombreadas):

4. No sólo de Postfix vive el correo

Postfix nos proporcionó la base de todo nuestro sistema de correo. Pero se necesitaban mecanismos que nos facilitasen herramientas para luchar contra el *spam* y los virus o que diesen valor añadido a los usuarios del servicio, como la aplicación de *webmail*. Todo ello mirado siempre desde la perspectiva de un sistema robusto y seguro.

Por todo ello, los primeros componentes que se integraron al nuevo sistema fueron el Spamassassin [5], como herramienta *anti-spam*, clamav [6] como antivirus (ambos controlados desde amavis-new [7]) y otros medios como SPF [8] para asegurar la integridad de remitentes. Se preparó, asimismo, el protocolo IMAP además del POP3 (siempre en sus versiones seguras) y el acceso a un sistema *webmail* (Squirrelmail [9]), también de forma segura.

En aquel tiempo, la primera iniciativa RACE de RedIRIS estaba ya funcionando. Debido a ello, en Calar Alto decidimos seguir sus directrices a la hora de configurar el nuevo servicio. En 2005, Calar Alto consiguió el Nivel Medio de dicha iniciativa. RACE tiene 3 niveles: Básico, Medio y Avanzado. No hay que entender el nivel Básico como un nivel bajo en calidad. El Nivel Básico asegura, por sí mismo, una calidad y seguridad en el servicio de correo importante. Los niveles Medio y Avanzado son catalogaciones con criterios de seguridad y calidad más elevados aún, por lo que para Calar Alto, una institución pequeña, conseguir el Nivel Medio suponía un gran avance.

En 2008 surge la segunda versión de RACE:

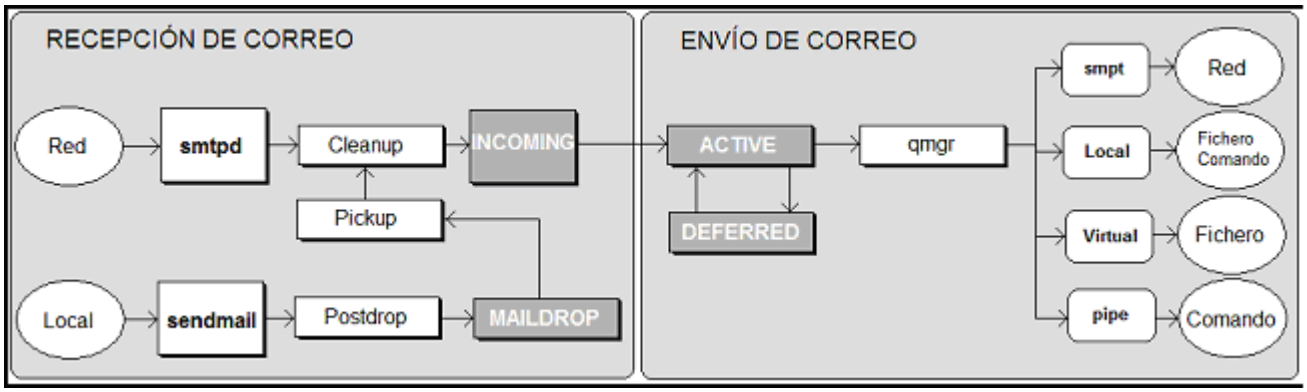

Figura 2. Esquema básico del funcionamiento de Postfix.

RACEv2. Es entonces cuando en Calar Alto decidimos dar el salto para buscar el Nivel Avanzado, cosa que logramos en agosto de ese año. En los párrafos siguientes pasaré a describir los puntos principales aplicados para lograr dicha catalogación.

5. RACEv2 en Calar Alto

Todos los criterios propuestos por RedIRIS se pueden ver en [2]. Presento aquí algunos de los que hemos observado en Calar Alto para ofrecer un mejor servicio de correo electrónico:

5.1. Reglas *anti-relay*

En principio, sólo se deben aceptar correos destinados a la organización o a los dominios delegados. En nuestro caso, el único dominio que disponemos es `caha.es`. El problema de permitir *relay*[1] no autorizados en el correo electrónico propicia la expansión del *spam*, ya que una estafeta mal configurada en cuanto al *relay*, se suele utilizar como salto para el envío masivo de *spam*. Las siguientes líneas del fichero `main.cf`, muestran estas reglas y algunos de los controles más importantes que se realizan y que veremos a continuación:

```
smtpd_recipient_restrictions =
permit_mynetworks,
 permit_sasl_authenticated,
 reject_unknown_sender_domain,
 reject_unauth_destination,
 check_sender_access hash:/etc/
postfix/LISTAS/ca-Xlist,
 check_client_access hash:/etc/
postfix/LISTAS/mtawl,
 reject_unknown_client_hostname,
reject_unknown_reverse_client_hostname,
reject_rbl_client strong.dnsbl.
rediris.es,
reject_rbl_client zen.spamhaus.org,
reject_rbl_client bl.spamcop.net,
check_policy_service unix:private/
policy,
 permit
```

5.2. Resolución inversa de MTAs

Empieza a ser común que los servidores bien configurados rechacen correos que vengan de un servidor sin resolución inversa. Por ello, el nuestro también debe estar bien configurado para evitar rechazos. Como vemos en la figura 3, nuestro servidor tiene resolución directa e inversa.

5.3. Control de acceso al puerto 25 en entrada

En Calar Alto disponemos de una única estafeta que concentra todo el tráfico de entrada y salida de correo electrónico. Cualquier ordenador que quiera enviar correos desde Calar Alto, debe tener como servidor de correo sólo el que está autorizado. Nadie puede configurar su propio servidor para mandar correo directamente fuera de Calar Alto. Igualmente, el único servidor autorizado para recibir correo desde el exterior es el servidor de correo. Nadie más puede recibir directamente correo desde el exterior

5.4. Criterios de SPF, tanto la definición dentro de nuestro DNS como el chequeo del correo entrante

SPF (*Sender Policy Framework* [8]) es un estándar abierto para evitar la falsificación de la dirección del remitente. Por un lado, el emisor especifica en el DNS (*Domain Name System*) qué servidores están autorizados a enviar correo para ese dominio. Por otro lado, el receptor chequea que el correo que llega de un dominio, lo haga desde una de esas máquinas autorizadas. Por lo tanto, es un proceso que puede ser utilizado para comprobar que lo que llega es legítimo, pero también para demostrar que quien manda correo está legitimado a hacerlo. Obviamente, si no se declara en un dominio un registro SPF en el DNS, el destinatario, aunque quiera, no podrá comprobar si llega desde donde debe. En nuestro caso, tenemos implementado un SPF completo, es decir: en nuestro DNS existe una entrada declarando la legitimidad de nuestro MX, como la que sigue:

```
TXT  "v=spf1  mx  -all"
```

Y, en el Postfix realizamos también un chequeo de SPF en correo entrante. En el fichero main.cf definimos la política:

```
check_policy_service
unix:private/policy
```

Mientras, en el `master.cf`, llamamos al programa de configuración e inicialización de SPF para el chequeo de los correos:

```
policy  unix - n n - - spawn
user=nobody  argv=/usr/bin/perl/
etc/postfix/smtpd-policy.pl
```

Con la declaración en el DNS nos aseguramos que el destinatario de un correo nuestro, si usa SPF en su servidor, pueda saber que llega desde un servidor autorizado para nuestro dominio. También podrá rechazar aquellos correos que digan venir desde **.caha.es** pero que no lo hagan desde nuestro servidor.

Con el uso del SPF junto con Postfix en la recepción, preguntamos por la legalidad del

```
C:\>nslookup caserv.caha.es
Servidor:  250.Red-80-58-61.staticIP.rima-tde.net
Address:  80.58.61.250

Respuesta no autoritativa:
Nombre:  caserv.caha.es
Address:  150.214.222.10


C:\>nslookup 150.214.222.10
Servidor:  250.Red-80-58-61.staticIP.rima-tde.net
Address:  80.58.61.250

Nombre:  caserv.caha.es
Address:  150.214.222.10
```

Figura 3. Resolución de la estafeta de Calar Alto.

servidor que envía un correo desde un dominio dado. En este caso, obviamente, sólo si el servidor remitente tiene una declaración similar a la nuestra en su DNS, podremos tomar las decisiones oportunas.

Creo que es necesario resaltar aquí la importancia de sistemas como el SPF escasamente implantados pero que, si lo estuvieran, evitarían mucho de los *spam* que se reciben a diario en nuestros buzones.

5.5. Uso de Lista Blanca de RedIRIS

Uno de los mayores problemas al que nos enfrentamos a la hora de filtrar correo malintencionado, es el de los falsos positivos, es decir, marcar como *spam* correo legítimo. La Lista Blanca de RedIRIS es un servicio que incluye las direcciones de estafetas de Instituciones como Universidades y otros centros de investigación, así como operadores que resultan de confianza. De esta forma, si un correo viene desde una de estas listas puede recibir una puntuación tal que evite que sea bloqueado por el sistema anti-*spam*. En nuestro caso, confiamos plenamente en las listas blancas de RedIRIS (puntuación de -99), evitando que un correo que llega desde una estafeta cuya IP aparezca en ellas sea filtrado de la siguiente forma en el fichero de configuración de Spamassassin:

```
header RCVD_IN_MTAWL_WHITELIST
eval:check_rbl('mtawlrev-
firsttrusted','mtawlrev.dnsbl.rediris.es')
describe RCVD_IN_ESWL_WHITELIST
Relay in mtawl whitelist
tflags RCVD_IN_MTAWL_WHITELIST
net
score RCVD_IN_ESWL_WHITELIST -
99
```

La Lista Blanca de RedIRIS es descargada tres veces al día. Asimismo, también hemos definido dentro de Postfix una lista blanca propia (ca-Xlist), para evitar filtrados de determinados sitios no cubiertos por la Lista Blanca de RedIRIS. Esto se puede ver en el listado del punto 5.1.

5.6. Acceso externo cifrado

Todo acceso a nuestro correo desde fuera de nuestra Institución se produce de forma cifrada. Los protocolos permitidos son sólo los seguros de POP3 (puerto 995) e IMAP (puerto 993). Todas las transacciones que se realizan con nuestro sistema de *webmail* van encriptadas.

5.7. Servicio Submission[2]

Tal y como dijimos más arriba, existe un control sobre el *relay*, de tal forma que no está permitido desde redes fuera de la nuestra. Sin embargo, la excepción existe para usuarios correctamente autentificados usando TLS [10]. De esta forma, un usuario de nuestro sistema puede enviar correos desde redes externas a Calar Alto, configurando correctamente su programa de correo para autentificarse ante nuestro servidor. En las **figuras 4** y **5** se aprecian los diagramas correspondientes al servicio de correo de Calar Alto. Como se puede ver, cualquier acceso de un usuario desde el exterior al sistema está encriptado. Internamente también se puede optar por una comunicación segura, si se desea, aunque en este aspecto aún dejamos libertad para que los usuarios decidan. Igualmente, controlamos quién está autorizado a enviar correos desde clientes externos:

```
smtpd_sender_login_maps = hash:/
etc/postfix/sasl_senders
smtpd_sender_restrictions =
hash:/etc/postfix/access
reject_authenticated_sender_login_mismatch
```

5.8. Servicio anti-virus y *anti-spam*

Ambos servicios se prestan desde Amavisnew, una interface de alto rendimiento entre Postfix y los revisores de contenidos (antivirus y *anti-spam*). En el propio fichero de configuración de Amavis (`/etc/amavisd.conf`), definimos el puerto de escucha del *daemon* de Amavis:

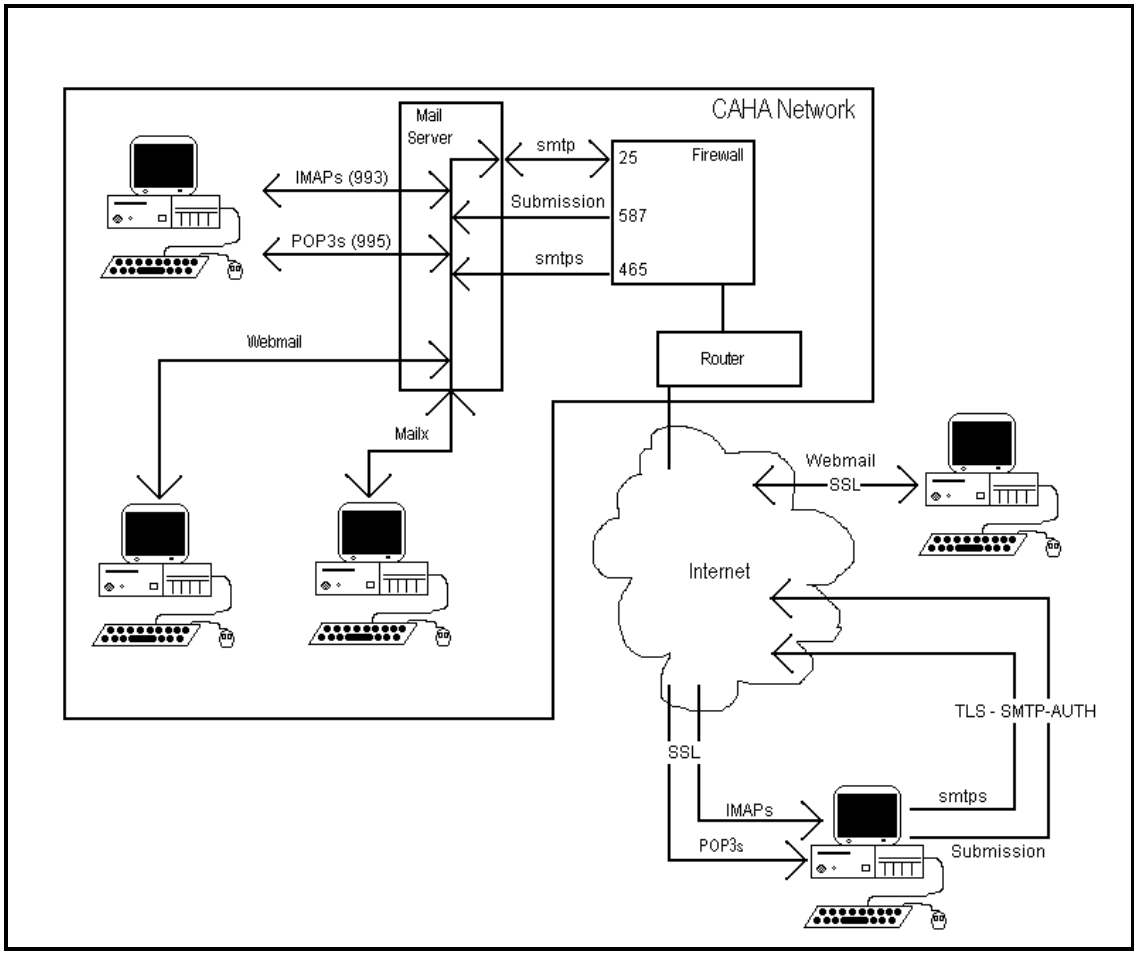

Figura 4. Esquema general del funcionamiento del correo en Calar Alto.

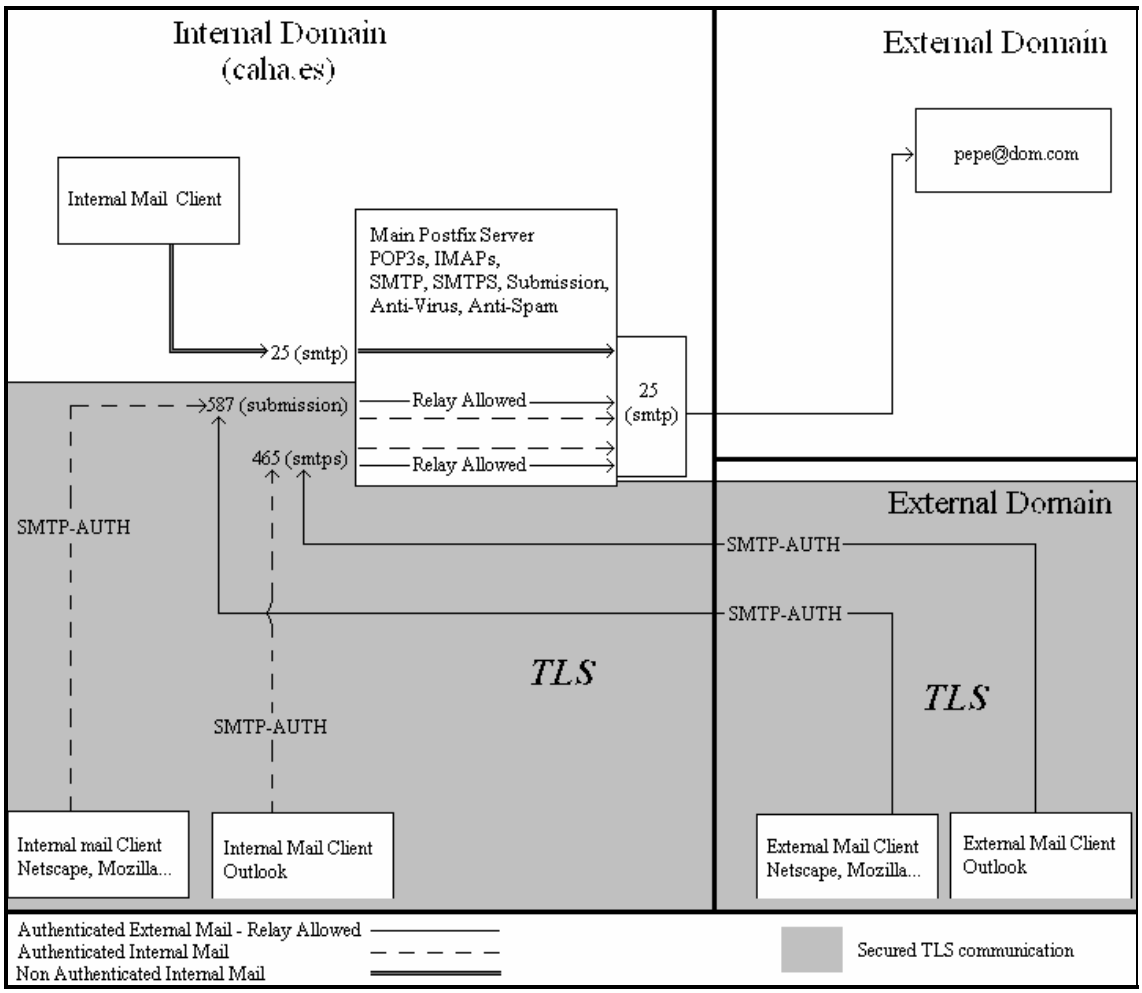

Figura 5. Control del *relay* para usuarios en redes externas a Calar Alto.

```
$inet_socket_port  =  10024;
```

En el fichero de configuración del postfix, `main.cf` se le da a conocer a postfix esta circunstancia, de tal forma que pueda pasarle los correos al filtro de contenidos para su análisis:

```
content_filter    =    smtp-
amavis:[127.0.0.1]:10024
```

La respuesta de Amavis, una vez aplicados los filtros *anti-spam* y anti-virus, la vamos a esperar en el puerto 10025, tal y como se especifica en el fichero `master.cf` de Postfix:

```
127.0.0.1:10025 inet n - n - - smtpd
```

En la **figura 6** se puede ver este proceso, en donde el *daemon* del filtro de contenidos (`amavisd`) recoge el correo, lo analiza con el *anti-spam* y anti-virus y devuelve su repuesta a la cola:

Como anti-virus principal estamos usando Clamav, con licencia GPL. Y como *anti-spam*, nos decantamos por Spamassassin.

En el caso de éste último, me gustaría reseñar que, aparte del sistema bayesiano de aprendizaje, nos ofrece una gran facilidad a la hora de crear nuestros propios tests y poder actuar de forma rápida ante un cambio en los patrones de *spam*.

5.9. Otros sistemas para evitar correo no deseado

Además de Spamassassin, se emplean tres métodos más que impiden que determinados correos puedan siquiera entrar en el servidor para su revisión. Estos sistemas evitan un procesamiento innecesario de correos fraudulentos dentro del servidor:

a) Nolisting [11]: Cuando se tienen 2 o más registros MX definidos en el DNS y el emisor no recibe respuesta del primer MX, debe (según la RFC 2821) intentar por orden, al menos 2 de los MX definidos. Sin embargo, se ha observado que las conexiones desde sitios emisores de *spam* no siguen esta política, por lo que definir un registro MX que no responda pero tenga una mayor prioridad que el servidor verdadero que escucha, hace que decrezca el número de *spam* entrante. En nuestro caso, tenemos definido un MX que no responde con mayor prioridad que el real. En algunos casos (no es el nuestro), se puede emplear esta técnica en modo "sandwich". Esto consiste en poner el MX real entre dos que no responden.

b) Chequeos de DNS: En resoluciones directas e inversas, como se aprecia en las líneas del `main.cf` de la sección 5.1.

c) Listas Negras: La lista negra de RedIRIS (Strong [12]) así como las listas de Spamhaus [13] y Spamcop [14] son utilizadas para evitar la entrada de correo ilegítimo (listado de la sección 5.1).

5.10. Política de trazas (logs)

Conservamos los ficheros de trazas de transacciones durante un año, en formato comprimido. Se almacena sólo la información sobre transacciones, pero no información sensible. Estos ficheros están sincronizados horariamente mediante el protocolo NTP. La hora usada oficialmente en el observatorio es la Hora Universal (UT).

5.11. Control de flujo

En transacciones tanto internas como externas, utilizamos el servicio **Anvil** [15] de Postfix para controlar el número de correos enviados por unidad de tiempo. De esta forma presentamos una defensa contra clientes que realizan muchas conexiones o peticiones simultáneas al servidor en la unidad de tiempo especificada. Las líneas de configuración en `main.cf` son:

```
smtpd_client_connection_count_limit = 15
smtpd_client_connection_rate_limit = 70
smtpd_client_message_rate_limit = 450
```

No definimos la unidad de tiempo. De esta

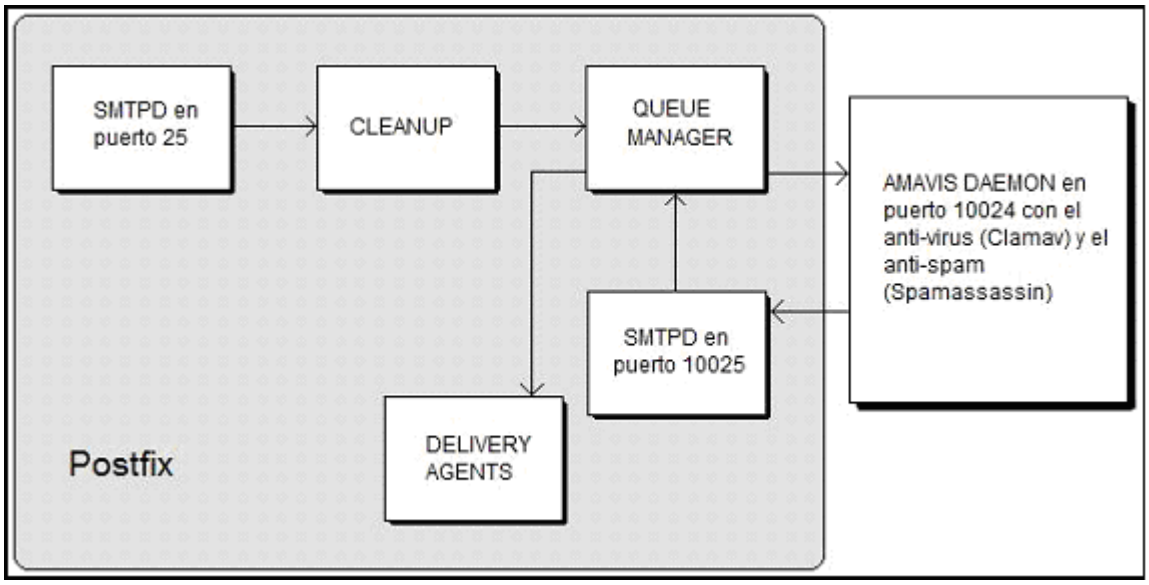

Figura 6. Funcionamiento conjunto del filtro de contenidos y de Postfix.

forma se toma 60s., que es el valor por defecto propio de Anvil.

5.12. Política de copias de seguridad de los buzones

Realizamos una copia diaria de los buzones sobre cinta. Además, una vez por semana se realiza una copia adicional, también en cinta, de la que existen 5 generaciones. Estas copias se guardan en cajas ignífiugas. Finalmente, cada 10 minutos sincronizamos los buzones sobre un disco en otra máquina que, además, se encuentra en un edificio diferente al servidor.

5.13. Documento descriptivo (DOCE)

En nuestra página web disponemos de una descripción detallada de nuestro correo electrónico para los usuarios [16].

5.14. Servicio de *webmail*

Tal y como se ha mencionado más arriba, todas las transacciones que se realizan con este sistema ocurren siempre encriptadas. Este servicio representa un valor añadido para todos aquellos usuarios que se encuentran fuera de nuestro Centro.

6. Conclusiones

En general, se han mostrado aquí muchos de los criterios que se cumplen en Calar Alto para garantizar la catalogación RACEv2. Pero no son los únicos. Entre otros, también cumplimos con criterios de control de destinatarios, tamaño máximo de mensajes, listas de correo, redirección de cuentas, etc. No se exponen en el presente artículo por la necesaria brevedad. Igualmente, aún queda mucho por hacer y mejorar. De hecho, la validez de la certificación RACEv2 es de dos años, lo que implica que debemos continuar este trabajo día a día para conseguir mantener la calidad requerida cara su posterior renovación. Es un reto más para el futuro.

Desde este artículo me gustaría llamar a la concienciación de aquellas instituciones que no prestan la suficiente atención a un servicio tan importante como es el correo electrónico. Con un esfuerzo común en seguir unas sencillas directrices, como las propuestas por RedIRIS y que en parte se muestran en este artículo, se podría disminuir en cierta medida el impacto negativo del *spam* y de los virus de correo, ofreciendo a la vez un servicio de mayor calidad. Cuantas más empresas e instituciones utilicen técnicas como las proporcionadas por SPF, vigilen sus *relays* o controlen efectivamente el puerto 25, más difícil se lo iremos poniendo a los *spammers*.

Calar Alto no es una institución grande y no se le puede adjudicar al correo electrónico personal dedicado. Por lo tanto, es éste un buen momento para agradecer a mis colaboradores su esfuerzo, sin el cual no hubiese sido posible conseguir el certificado. Hemos sido conscientes de que no solo para nuestros usuarios la seguridad y la calidad del servicio es muy importante, algo que resulta básico, sino que también lo es para poner nuestro granito de arena en la mejora del complejo mundo de las comunicaciones electrónicas.

Referencias

[1] RedIRIS. <http://www.rediris.es>.
[2] RedIRIS. *RACEv2: Red Avanzada de Correo Electrónico*. <http://www.rediris.es/race>.
[3] RedIRIS. *Directorio de Instituciones RACE*. <http://www.rediris.es/race/cata>.
[4] Postfix. <http://www.postfix.org>.
[5] SpamAssassin. <http://spamassassin.apache.org/>.
[6] ClamAV. <http://www.clamav.net/>.
[7] AMaVIS. <http://www.amavis.org>.
[8] SPF. <http://www.openspf.org>.
[9] Squirrelmail. <http://squirrelmail.org/>.
[10] Postfix. *Postfix TLS Support*. <http://www.postfix.org/TLS_README.html>.
[11] Nolisting. http://nolisting.org.
[12] RedIRIS. *Aspectos Técnicos del Servicio IRISRBL*. <http://www.rediris.es/irisrbl/irisbl.es.html>.
[13] Spamhaus. <http://www.spamhaus.org/>.
[14] Spamcop. <http://www.spamcop.net/>.
[15] Postfix. *Anvil*. <http://www.postfix.org/anvil.8.html>.
[16] Observatorio de Calar Alto. *Caha Mail Description Document*. <http://www.caha.es/caha-mail-description-document.html>

Libros de consulta

Kyle D. Dent. *Postfix: The definitive guide*. Ed. O'Reilly, 2003. ISBN-10: 0596002122.
Alan Schwartz. *Spamassassin. The Open Source Solution to Spam*. Ed. O'Reilly, 204. ISBN-10: 0596007078.

Notas

[1] En este artículo, usamos el término *relay* como sinónimo de "retransmisión de mensajes de correo electrónico" puesto que no existe un término suficientemente específico en castellano para expresar lo mismo. Así se hace también en los documentos internos del proyecto RACE.
[2] El término "Submission" se refiere aquí al acceso autenticado y cifrado a través del puerto 587 descrito en la RFC4409 <http://www.ietf.org/rfc/rfc4409.txt>.