Universidad Central de Venezuela
Facultad de Ciencias
Escuela de Computación
Laboratorio de Comunicación y Redes

Diseño e Implementación de un Servicio de E-mail Aunado a Técnicas Antispam y Basado en Software de Dominio Público

Trabajo Especial de Grado
presentado ante la ilustre
Universidad Central de Venezuela
por los bachilleres:

Eugenio Alberto Blanco Pérez
C.I.: 10.886.786
E-mail: eugeblan1669@yahoo.es

William José Cedeño Hernández
C.I.: 8.995.347
E-mail: williamcedeno@cantv.net

para optar al título de Licenciado en Computación

Tutor: Prof. Eric Gamess

Caracas, Diciembre 2009

Universidad Central de Venezuela
Facultad de Ciencias
Escuela de Computación

ACTA DEL VEREDICTO

Quienes suscriben, Miembros del Jurado designado por el Consejo de Escuela de Computación, para examinar el Trabajo Especial de Grado, presentado por los Bachilleres Eugenio Alberto Blanco Pérez, C.I. 10.886.786 y William José Cedeño Hernández, C.I. 8.995.347, con el título "**Diseño e Implementación de un Servicio de E-mail Aunado a Técnicas Antispam y Basado en Software de Dominio Público**", a los fines de cumplir con el requisito legal para optar al título de Licenciado en Computación, dejan constancia de lo siguiente:

Leído el trabajo por cada uno de los Miembros del Jurado, éstos fijaron el día 14 de Diciembre de 2009, para que sus autores lo defendieran en forma pública en el "Auditorio de la Facultad de Ciencias" lo cual estos realizaron mediante una exposición oral de su contenido, y luego respondieron satisfactoriamente a las preguntas que fueron formuladas por el Jurado, todo ello conforme a lo dispuesto en la Ley de Universidades y demás normativas vigentes de la Universidad Central de Venezuela. Finalizada la defensa pública del Trabajo Especial de Grado, el jurado decidió APROBARLO.

En fe de lo cual se levanta la presente acta, en Caracas el 16 de Diciembre de 2009, dejándose también constancia de que actuó como Coordinador del Jurado el Profesor Tutor Eric Gamess.

Prof. Eric Gamess
(Tutor)

Prof. María Elena Villapol
(Jurado Principal)

Prof. Karima D. Velásquez C.
(Jurado Principal)

Resumen

Título:
Diseño e Implementación de un Servicio de E-mail Aunado a Técnicas Antispam y Basado en Software de Dominio Público.

Autores:
Eugenio Alberto Blanco Pérez
William José Cedeño Hernández

Tutor:
Prof. Eric Gamess

El presente Trabajo Especial de Grado está enfocado hacia la implementación de un sistema de correo electrónico conjugado con técnicas y herramientas para el control de spam basado en software de dominio público. El objetivo del trabajo es proponer una solución que permita a cualquier persona u organismo implementar un sistema de correo electrónico con un eficaz manejo de mensajes no deseados.

El proyecto está compuesto por un proceso de investigación, instalación y configuración de los componentes necesarios para implementar una plataforma de correo electrónico con control de spam. La solución antispam se basa en spamassassin, el cual es un software de código abierto que implementa funcionalidades necesarias para el control del spam. Como caso de estudio se seleccionó a la Asamblea Nacional, en la cual se efectuó reingeniería total de la plataforma de correo, quedando establecido Zimbra Messaging and Collaboration Suite 5.0 como plataforma de mensajería y colaboración. Esta suite usa como background el sistema operativo Debian Etch release 4. Todos estos sistemas se integraron para proporcionar un servicio de correo libre de spam en concordancia con los lineamientos del decreto Nº 3.390.

Con la implementación de la plataforma de correo electrónico con control de spam, se logró obtener una solución que proporciona beneficios adicionales (antivirus, firewall, etc.) que brinda más y mejores opciones a los usuarios y administradores. De igual forma se obtuvo una plataforma fácilmente escalable en cuanto a servicios y funcionalidades, además de ser extensible, ya que esta solución se podría implementar en otros entes públicos y privados.

Palabras Claves: E-mail, Debian, Zimbra, Postfix, spam, spammer, spamassassin.

Tabla de Contenido

Índice de Figuras

Índice de Tablas

Introducción

En un mundo tan desarrollado como el actual, los recursos de información son tan amplios que van más allá de la imaginación. Son muchas las organizaciones que cuentan con un número considerable de computadoras en operación y que utilizan herramientas soportadas por las redes digitales. Una de las herramientas más utilizadas hoy en día es el correo electrónico, que es el abanderado de los servicios de Internet. Este servicio representa, dentro de los procesos de casi cualquier empresa, el canal para el flujo de datos, por lo que tiene una importancia relevante.

Sin embargo, al igual que otros servicios de Internet, puede ser vulnerable a los ataques de hackers. Uno de los ataques más constantes contra este servicio es el spam, que consume el tiempo de los usuarios, ya que deben identificar y eliminar el correo no deseado. Ante este problema, el propósito de este trabajo es presentar alternativas basadas en el uso de software libre o software de dominio público para disminuir este flagelo.

Las iniciativas de fomentar el uso de software libre habrán alcanzado el éxito cuando logren que el principal motivo para aceptar o rechazar cualquier tipo de software, sea cubrir con la función que se necesita. Cuando los programadores pueden leer, modificar y redistribuir el código fuente de un programa, éste evoluciona. Así, el esquema de desarrollo del software libre garantiza que exista una revisión robusta del código, además de mejoras y adaptaciones a un contexto particular.

Considerando que el modelo de negocios alrededor del código abierto está basado en los servicios de valor agregado, más allá de las implicaciones económicas, apostar por el software libre es apostar por un modelo de desarrollo basado en la libre transmisión del conocimiento, frente al modelo de apropiación y control de dicho conocimiento que promueven los monopolios del software.

En el presente Trabajo Especial de Grado se describen los aspectos más importantes para la implementación de una infraestructura para el manejo de correos electrónicos, aunado a técnicas y herramientas para el control de spam.

A manera de orientar al lector en el seguimiento y comprensión, el presente trabajo se encuentra estructurado por capítulos, como es especificado a continuación:

- **Capítulo 1:** En este capítulo se hace una descripción de la problemática existente con el servicio de correo electrónico ante el flagelo del spam.
- **Capítulo 2:** Contiene documentación sobre las técnicas más comunes de control para mensajes no deseados.
- **Capítulo 3:** En este capítulo se describe la metodología utilizada para el desarrollo del trabajo, se especifican las fases de análisis, diseño, implementación y pruebas. Se analizan las herramientas de software de dominio público para la gestión de correo electrónico y control de spam.

- **Capítulo 4:** Este capítulo presenta algunos trabajos relacionados con el tema central del documento.
- **Capítulo 5:** Este capítulo contiene las conclusiones que se emiten sobre el trabajo de investigación, así como las recomendaciones y adecuaciones necesarias, encontradas en el desarrollo del TEG.

1. El Problema

1.1 Planteamiento del problema

Una de las herramientas de comunicación más importante con la que cuentan las organizaciones en la actualidad es el correo electrónico, pero cuando este servicio se ve vulnerado por el flagelo del spam, se hace cuesta arriba su operatividad y atractiva utilización. Por otra parte, los entes públicos enfrentan un problema de directrices ya que por mandato presidencial [6] se debe tratar de canalizar la plataforma tecnológica hacia el uso de software de dominio público.

En base a lo anteriormente expuesto, se plantea la implementación de una solución para el manejo del correo electrónico aunado a herramientas para el control de mensajes no deseados, utilizando como base tecnológica el software de dominio público.

1.2 Objetivo general

Diseñar e implementar una plataforma de correo electrónico que controle el spam de manera dinámica.

1.3 Objetivos específicos

- Conocer la problemática generada por el spam.
- Documentar las técnicas actuales de defensa contra el flagelo del spam.
- Conceptualizar y diseñar una adecuada infraestructura que permita la gestión de correos electrónicos cumpliendo con requisitos mínimos de robustez y seguridad.
- Implementar un control de virus y spywares.
- Analizar, evaluar e instrumentar el funcionamiento de una suite integral para manejo de correo electrónico y control de spam.

1.4 Justificación

El estado venezolano estableció, mediante decreto N° 3.390, que la administración pública deberá emplear prioritariamente software libre [6] desarrollado con estándares abiertos en sus sistemas, proyectos y servicios informáticos. Por esto, todos los órganos y entes de la administración pública han iniciado un proceso progresivo de migración hacia el software libre. La Asamblea Nacional está buscando alternativas óptimas acordes con el decreto, pero sin poner en riesgo la función de legislar.

Ahora bien, el servicio de correo electrónico se ha visto vulnerado por el flagelo del spam; por ello se deben buscar herramientas que controlen de manera eficiente y acertada los mensajes no solicitados. Debido a la naturaleza volátil del concepto spam, resulta importante contar con herramientas capaces de adquirir

dinámicamente conocimientos sobre el dominio, descartando aquellas que con el paso del tiempo se vuelvan obsoletas.

No es menospreciable la reducción de costos asociada al reemplazo de tecnologías comerciales con tecnologías basadas en software de dominio público. Este ahorro puede ser utilizado en la formación profesional o en la investigación.

1.5 Alcance

Para la realización de este Trabajo Especial de Grado se propone el diseño, el desarrollo y la implementación de una infraestructura para el manejo de correos basado en protocolos estándares y tecnologías abiertas (Debian GNU/Linux[1] y Postfix[2]), haciendo hincapié en el control efectivo y dinámico del spam.

[1] http://www.debian.org
[2] http://www.postfix.org

2. Marco Teórico

2.1 Definiendo el problema del spam

El spam es un flagelo que afecta a millones de usuarios del correo electrónico, que llena los buzones de cantidad de basura informativa no solicitada y de poco valor.

2.1.1Historia del término

El origen de la palabra spam tiene raíces norteamericanas con unas curiosas derivaciones socioculturales que datan de 1937, cuando la empresa charcutera norteamericana Hormel Foods lanzó una carne en lata originalmente llamada *Hormel's Spiced Ham* (ver Figura 2.1). El gran éxito del invento lo convirtió con el tiempo en una marca genérica, tan conocida que hasta el mismo fabricante le recortó el nombre, dejándolo con sólo cuatro letras: “SPAM”. El spam alimentó a los soldados rusos y británicos en la Segunda Guerra Mundial, y fue comercializado en todo el mundo en 1957. En los años 60 se hizo aún más popular, gracias a la innovadora anilla de apertura automática, que ahorraba al consumidor el uso del abrelatas [4].

Figura 2.1: Lata de Spam

Fue entonces cuando los Monty Python[3] empezaron a hacer burla de la carne en lata. La divertidísima costumbre de gritar la palabra SPAM, en diversos tonos y volúmenes, se trasladó metafóricamente al correo electrónico no solicitado que perturba la comunicación normal en Internet. En un famoso sketch de 1969, (Flying Circus), los comediantes británicos representaban a un grupo de

[3] Grupo británico de humoristas que sintetizaron el humor de los años 60 y 70.

hambrientos vikingos, atendidos por camareras que les ofrecían “huevo y panceta; huevo, salchichas y panceta; huevo y spam; huevo, panceta, salchichas y spam; spam, panceta, salchichas y spam; spam, huevo, spam, spam, panceta y spam; salchichas, spam, spam, panceta, spam, tomate y spam”. La escena acababa con los vikingos cantando a coro, “spam, spam, spam, spam. ¡rico spam! ¡maravilloso spam! spam, spa-a-a-a-a-am, spa-a-a-a-a-am, spam. ¡rico spam! ¡rico spam! ¡rico spam! ¡rico spam! ¡rico spam! spam, spam, spam, spam” [4].

Como la canción, el spam es una repetición sinfín de texto de muy poco valor o ninguno que, aplicado a los mensajes electrónicos, se refiere a los mensajes enviados de forma masiva y dirigidos a personas que, en principio, no desean recibirlos.

2.1.2 ¿Qué es el spam y cómo se identifica?

El spam es el hecho de enviar mensajes no solicitados y en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada está basada en el correo electrónico. Otras tecnologías de Internet que han sido objeto de spam son: grupos de noticias, motores de búsqueda y blogs[4]. El spam también puede tener como objetivo los teléfonos móviles (a través de mensajes de texto) y los sistemas de mensajería instantánea.

Definiendo el problema

Existe una alta probabilidad que un usuario de correo electrónico haya recibido spam recientemente, es decir, un mensaje no deseado enviado a su buzón. Si el usuario es nuevo en el uso de tecnologías en Internet, probablemente ha visto sólo unos pocos de estos mensajes que molestan. Si ha estado usando Internet por más tiempo, podría recibir una docena o más de estos mensajes cada día, y si administra una red, podría ser bombardeado con centenares o miles de estos mensajes.

La Figura 2.2 tiene todos los elementos de un mensaje propio de spam:

- El mensaje viene de un negocio con el que no se tiene ninguna relación.
- Fue enviado desde una dirección electrónica (*charles7713@yahoo.com*) que es ficticia, o se creó solamente con el propósito de enviar mensajes de spam y la cual ya debe haber sido anulada o desechada.
- El mensaje anuncia un servicio que es ilegítimo y sombrío.
- El mensaje no identifica claramente a la persona o grupo que lo ha enviado.
- Las solicitudes de eliminación que fueron enviadas a la dirección listada en la parte inferior, *webmaster@tiffiny.com*, fueron ignoradas.

[4] Un weblog, también llamado blog o bitácora, es un sitio web donde se recopilan cronológicamente mensajes de uno o varios autores, sobre una temática o a modo de diario personal, siempre conservando el autor la libertad de plasmar lo que considere pertinente.

- La compañía que hace la publicidad no se conoce bien y no está tratando de establecer una reputación o buscando un consumidor fiel.

```
Received: (from mail@localhost)
     by apache.vineyard.net (8.8.5/8.8.5) id LAA01663
     for <simsong@vineyard.net>; Sat, 16 May 1998 11:57:57 -0400 (EDT)
From: charles7713@yahoo.com
Message-Id: <199805161557.LAA01663@apache.vineyard.net>
Received: from 209-142-2-72.stk.inreach.net(209.142.2.72)
     by apache.vineyard.net via smap/slg (Vl.3) id smaOO1626; Sat May
16 11:57:27 1998 Date: Sat, 16 May 1998 05:18:34
To: <simsong@vineyard.net>
Subject: Search Engines, 400 for 5.75 (1)

  * * * LIMITED TIME SPECIAL OFFER * * *

For Only $5.75 (1) We Will Submit Your Web Site To Over 400 of the
Net's Hottest Search Engines, Directories & Indexes.

If you're site isn't listed in the Search Engines, how can people find
you to buy your products or services?

Visit Our Web Site to Learn More:
http://www.tiffiny.com/sitesubmissions
Thank You

The price for this service is $69 prepaid which covers the cost of
submitting your site every three months for an entire year.  We have
shown the price of $5,75 to show how inexpensive this program really
is when the overall cost is annualized. Minimum 12 month term and full
prepayment required.
====================================

Name removal requests.
Send to:
TO:   webmaster@tiffiny.com
SUB:  remove
```

Figura 2.2: Mensaje típico de spam

Un usuario que recibe spam, experimenta distintas emociones. Al principio estaría probablemente desconcertado. Pudo haberse preguntado. *¿Qué es este mensaje?, ¿de dónde vino?, ¿dónde consiguieron estas personas mi nombre?* Una vez que la confusión pasó y recibió el segundo o tercer correo basura, pudo haberse enfadado. Quizás escribió correos para quejarse, dirigidos a quien le envió el spam, y se enfadó más cuando sus quejas rebotaron debido a que el spammer había enmascarado su dirección de e-mail. Finalmente, pudo enojarse una vez más, debido a que empezó a recibir spam diariamente. Al leer su correo electrónico, su fuente de diversión o información se convirtió en un proceso de consumo de tiempo, deshaciéndose de correos no deseados sin un final a la vista.

Los spammers comprenden que es en vano enviar e-mails que no van a leerse, así que acuden cada vez más a nuevas y engañosas técnicas para conseguir que el usuario lea su correo antes de que lo elimine. Algunos trucos se diseñan para parecer como si el mensaje vino de un nuevo compañero comercial (ver Figura 2.3):

```
From: Bob Brown <bob@gdi4.gdi.net>
Subject: RE:To selected new clients
```

Figura 2.3: Técnica para envío de spam

O los spammers podrían intentar parecer como si él o ella es un viejo amigo (ver Figura 2.4):

```
From: Jane <jane234@yahoo.com>
Subject: Epale, ¿como te va?
```

Figura 2.4: Técnica para envío de spam

O también podrían intentar parecer como si el mensaje vino de usted (ver Figura 2.5):

```
From: Jason Sears <jason@netcom.com>
To: Jason Sears  <jason@netcom.com>
```

Figura 2.5: Técnica de envío de spam

Cuando los spammers se ponen más hábiles, se hace más difícil anular estos mensajes sin leerlos primero. Sin embargo, hay herramientas poderosas para luchar en contra del spam.

Taxonomía del spam

Hoy, las personas usan la palabra “spam” para definir casi cualquier tipo de mensaje de e-mail no deseado que reciben. Sin embargo, se usa el término para describir e-mails que se envían en volumen, sin tener en cuenta los deseos de los destinatarios.

Siendo por ello importante distinguir entre los diferentes tipos de mensajes no deseados, a continuación se explican algunos términos [4]:

- *E-mail comercial no solicitado (UCE):* es un mensaje del e-mail que se recibe sin pedirlo, anunciando un producto o servicio. Esto también se llama e-mail basura.
- *E-mail basura no solicitado (UBE):* se refiere a mensajes de e-mail que se envían en volumen a miles (o millones) de destinatarios. UBE puede ser comercial por naturaleza, en el caso que sea también un UCE. Pero también puede enviarse para otros propósitos, como propaganda o persecución política.
- *Mensajes de hacer dinero fácil (MMF):* a menudo en forma de esquemas de mercadeo multinivel o de cadena de cartas; son mensajes que le sugieren que se haga rico al enviar dinero al primer nombre en una lista, quitando ese nombre, agregando su nombre al final de la lista, y remitiéndoles el mensaje a otras personas.

2.1.3¿Qué hay de malo con el spam?

La mayoría de los mensajes de spam en Internet son anuncios de individuos y pequeños comercios que buscan una manera de hacer un cliente rápido. Normalmente, se envían mensajes de spam mediante el uso de técnicas sofisticadas, diseñadas para enmascarar los verdaderos remitentes de los mensajes. Y en cuanto a recolectar su dirección de e-mail, los spammers utilizan una variedad de técnicas para encontrarla, que serán descritas más adelante.

Durante los últimos años, varias empresas han experimentado con bultos de e-mails. Aunque las compañías se identifican claramente en los mensajes, estos bultos pueden causar los mismos problemas que el spam. Si estas compañías continúan sus experimentos y si a ellas se unen otras, se verá un aumento dramático en la cantidad de spam en la red.

Las personas que envían estos mensajes dicen que el e-mail es una forma de mercadeo electrónico directo, equivalente a anuncios en la radio o en el periódico. Pero hay diferencias importantes entre el spam electrónico y las técnicas de mercadeo convencionales, diferencias que pudieran destruir la utilidad del Internet si el spam no es detenido.

El spam desperdicia dos de los recursos más preciosos: el ancho de banda y el tiempo de los administradores de red, como también desperdicia el tiempo de los usuarios alrededor del planeta.

Ante esto, es importante preguntarse: ¿cuánto spam existe a nuestro alrededor? Aunque es difícil hablar de números exactos, informes muestran que hay mucho, y que el problema está empeorando:

- Según América Online, una tercera parte de los mensajes de e-mail que recibe de Internet en cualquier día, es spam [4].
- Según el primer estudio académico de spam, a través de Lorrie Faith Cranor en los Laboratorios de Investigación de AT&T y Brian A. LaMacchia en Microsoft, entre el 5% y 15% del e-mail recibido por el citado Laboratorio de Investigación de AT&T y el Laboratorio de Investigación de Bell, era spam [10].

Estos números no cuentan la historia entera. Aunque muestran que hay mucho spam en Internet hoy, no explican por qué es una amenaza. De hecho, si el único problema con el spam fuera el puro volumen, se podría hacer argumentos igualmente apremiantes sobre el número de anuncios en el diario, anuncios en la televisión y en la radio, e incluso las carteleras en metros y en autobuses. Nadie está diciendo que la publicidad está a punto de acabar con el periodismo. De hecho, la mayoría de los periódicos, revistas, incluso los entes gubernamentales, recurren en anunciar a terceros para financiarse.

Pero hay que definir: ¿Cuál es la diferencia entre el spam y la publicidad? La respuesta a esta pregunta no queda en la tecnología, pero sí en la economía.

La diferencia fundamental entre el spam y otras formas de publicidad tiene que ver con el costo y el precio de quien lo paga [4].

El bajo costo del spam

Un anuncio en un periódico o enviar un catálogo a miles de personas tiene un costo, dependiendo del tamaño del catálogo, la calidad de la impresión y el tipo de correo que se use. Enviar un e-mail requiere de una computadora conectada a Internet y una línea telefónica, y con esto un spammer puede enviar muchísimos e-mail rápidamente por un costo relativamente económico.

El sentido común dice que no hay ninguna razón para enviar un anuncio a alguien que no puede comprar el producto; es decir, no hay ninguna razón para gastar el dinero en anunciar comida de perro a los dueños de un gato. Pero los spammers no tienen ninguna motivación para clasificar y destinar sus mensajes, porque el costo de mandar mensajes electrónicos es muy bajo.

El alto costo del spam

El spam puede ser barato al enviarlo, pero el e-mail en volumen llega a buzones de usuarios, donde su administración encarece los costos. Esto de “simplemente pulse el botón borrar”, no es una solución buena al problema del spam.

Bajo las circunstancias normales, las computadoras no pueden apreciar la diferencia entre los mensajes que son spam y los mensajes normales e importantes. Cada mensaje en forma independiente que sea o no spam, se trata con cuidado y rápidamente es llevado por las computadoras a su destino o destinos apropiados.

Un spammer puede tardar sólo cinco o diez minutos en programar su computadora para enviar un millón de mensajes durante el transcurso de un fin de semana. Es cierto que cada uno de estos mensajes puede anularse con sólo pulsar el botón del ratón, que toma sólo tres o cuatro segundos: unos segundos para determinar que el mensaje es realmente un spam, más un segundo en pulsar el botón “borrar”. Pero esos segundos se suman rápidamente: un millón de personas pulsando el botón “borrar”, corresponde a un mes de actividad humana gastada, o visto de otra manera: si tiene en un día seis mensajes del spam, el usuario está gastando dos horas cada año anulando spams. Lo cual significa que los administradores del servicio de correo pagan por el spam con su tiempo.

A pesar de que el sistema de correo electrónico fue diseñado para hacer difícil la pérdida de mensajes, cuando una computadora no puede entregar un mensaje al destinatario, hace su mejor esfuerzo para devolver ese mensaje al remitente [13]. Si no puede enviarle el mensaje al remitente, lo envía al administrador de correos como si las direcciones de e-mail del remitente y del destinatario fuesen inválidas.

Por esta razón, la naturaleza del buen significado del software de correo de Internet llega a ser una gran responsabilidad cuando los spammers entran en el cuadro. En un correo por volumen, cualquiera de los centenares de miles de direcciones de e-mail podría ser inválida. Bajo circunstancias normales, estos mensajes de e-mail serían devueltos al remitente, pero el spammer no quiere estos rebotes. Para evitar esto, los spammers envían a menudo mensajes con direcciones de retornos inválidos. El resultado es que los mensajes de e-mail terminan en los buzones de administradores de correos de Internet.

2.2 ¿Cómo controlar el correo basura?

Actualmente existen muchas técnicas y recomendaciones para controlar el spam. A través de este capítulo, se señalan diferentes técnicas que permiten tanto a los usuarios como a los administradores luchar contra este flagelo.

2.2.1 Técnicas para usuarios

Dentro de las técnicas que mayormente destacan por ser implementadas por los usuarios, se encuentran las que a continuación se señalan, las mismas consideran tres enfoques para detener el spam:

- Cuidar la divulgación de la dirección del correo.
- Filtrar el correo basura, esto se refiere a la necesidad de filtrar el e-mail entrante para quitar el spam.
- Responder al correo basura, para lo cual se debe rastrear al spammer y quejarse con el responsable del acceso a Internet del spammer.

Tal como se menciona, estas tácticas no son exclusivas entre sí, el usuario puede aprovecharse de los tres métodos para reducir el correo basura que recibe y ayudar a hacer que el spam sea improductivo.

Cuidando la dirección de correo

Una manera de prevenir la recepción de e-mail basura es mantener las direcciones de e-mail fuera del alcance de los spammers. Después de todo, nadie puede enviar correos sin la dirección de e-mail del usuario.

Los spammers construyen una lista de envío, coleccionando direcciones legítimas que aparecen en páginas web, grupos de noticias, etc. En este sentido, para prevenir el spam, el usuario debe ocultar o puede enmascarar sus direcciones de e-mail cada vez que aparezcan en un lugar público. También se enmascaran las direcciones de e-mail en los chats y en los directorios de miembros de ISP. Si el ISP que le provee el servicio opera con tales directorios, el usuario puede pedir que su nombre sea removido del directorio para prevenir que sea coleccionado por un spammer.

Otra manera eficaz de proteger la dirección de e-mail, es usar una cuenta como “importante” y darla a la familia, los amigos, los contactos comerciales y otros cuyo correo quiera recibir, y además abrir una segunda cuenta “insignificante” la

cual se usará siempre que se subscriba a una lista de envío o para propósitos públicos.

Como puede observarse, existen mecanismos que los usuarios pueden emplear para proteger su e-mail del spam, que cada vez busca diversas formas de invadirlo tales como las se que aprecian a continuación:

Troyanos y ordenadores zombis

Recientemente se ha empezado a utilizar una técnica mucho más perniciosa: la creación de virus troyanos que se expanden masivamente por computadoras no protegidas (sin firewall, antivirus, etc.). Así, las computadoras infectadas son utilizadas por el *spammer* como "ordenadores zombis [5]", que envían spam controlado por el software troyano. Esto puede causar perjuicios al usuario que ignora haber sido infectado (que no tiene por qué notar nada extraño) al ser identificado como *spammer* por los servidores a los que envía spam sin saberlo, lo que conduce a que no se le deje acceder a determinadas páginas o servicios.

Listas de correo

En este caso, los spammers también han sido capaces de reunir direcciones de e-mail de listas de correo de Internet. Muchas listas de envío son tratadas por programas que pueden manejar tareas diarias, como agregar nuevos miembros y envíos programados. Si el usuario se subscribe a listas de envío populares, está en riesgo de los spammers que coleccionan direcciones preguntando al servidor de la lista.

Los programas de listas de correo normalmente ofrecen la opción de desactivar a quienes las envían. Si el usuario está en una lista de envío, debe instarle al administrador de la lista que lo desactive [2].

Correos de grupos de noticias

Cuando el usuario tiene sólo una cuenta de correo electrónico y desea enviar correos a un grupo de noticias, es más difícil proteger la dirección de e-mail. Sin embargo, existen dos estrategias normalmente usadas: re-mailers anónimos y direcciones enmascaradas.

Los re-mailers anónimos

Un re-mailer anónimo permite enviar e-mail anónimamente [4]. El correo que se envía a través del servicio es reescrito para quitar la dirección de e-mail y otras informaciones de envío. Un problema con el re-mailer anónimo es que el usuario es justo eso, un anónimo. En algunos grupos de noticias, los lectores ignoran los correos anónimos porque son usados a menudo por spammers.

Las direcciones enmascaradas

Este enfoque está dirigido al envío de correo con una dirección enmascarada, para lo cual se debe reemplazar la dirección de e-mail origen con una dirección inválida, pero que la verdadera dirección pueda ser determinada fácilmente por un ser humano.

Entre las pautas sugeridas para una dirección enmascarada, están las siguientes:

- Informar a las personas cómo desenmascarar la dirección en alguna parte del mensaje.
- Hacer el enmascaramiento obvio para los humanos, pero que no llegue a ser más fácil para los sistemas detectores de e-mail usado por los spammers.
- No maquillar nombres de dominio. Alguien puede registrar ese dominio y entonces recibirían todo el spam enviado a la dirección enmascarada.
- Asegurarse de enmascarar el nombre del dominio. No modificar el usuario o buzón simplemente. Si el usuario usa un buzón inválido pero un nombre del dominio válido, estará obligando al servidor de correo a procesar correo basura entrante y determinar que sea un usuario desconocido.

Los canales

Este es otro enfoque para minimizar el spam, que consiste en crear una dirección e-mail especial que sólo se usará durante un tiempo limitado. Esta técnica fue propuesta por Robert Hall, investigador de AT&T Labs, como parte de un sistema llamado canales de e-mail [4]. El sistema de Hall permite crear e-mails diferentes para personas con propósitos diferentes a través de un canal público que seguiría tarjetas comerciales, otro canal para comunicaciones privadas, otro canal para el envío de la red y de esta manera tener software que automáticamente filtre el e-mail entrante destinado para los diferentes canales.

Siendo importante acotar que los canales usados para el envío de correo por la red pueden anularse después de unas semanas, mucho tiempo para recibir contestaciones legítimas, poco tiempo para el spam.

Páginas web

Otro de los medios a través de los cuales los spammers recolectan frecuentemente direcciones de e-mails, son las páginas web. Si el usuario mantiene páginas web es muy importante proteger la dirección.

Pero en algunos casos, mantener la dirección escondida en la web es más difícil que mantenerla en la red. Normalmente el usuario quiere que la página web incluya la dirección de correo, para que las personas puedan contactarlo. Pero, ¿si debe esconder la dirección? En este caso, hay algunas tácticas que pueden ser utilizadas:

- Enmascarar la dirección, como si estuviera en un grupo de noticias.
- Colocar partes de las direcciones de e-mail o hostname en negrillas o cursiva, muchos colectores no descifran el código de formato HTML de las direcciones reales y se confunden.
- Insertar un 20% (espacio) antes de la dirección de e-mail, ya que esto hace que el enlace trabaje bien para los web browsers, pero la mayoría de los colectores de dirección consideran estas direcciones de e-mail como inválidas.
- Crear una imagen gráfica que incluya la dirección de e-mail y despliegue la imagen en la página.
- Coleccionar los comentarios y otros mensajes usando una forma y una escritura de CGI, en lugar de un URL “mailto”.

Listas opt-out

En el mercado directo del mundo las compañías de lista-envío y tele-mercadeo han desarrollado un sistema llamado opt-out [4], que permite a los usuarios decidir si quieran recibir publicidad voluntariamente. La forma en que estas listas trabajan es simple: Si no se quiere recibir e-mail o las llamadas de teléfono, se escribe una carta al DMA (Direct Marketing Association´s). El DMA da esta información a las compañías de mercadeo directo quienes usan esta base para envío a sus clientes.

Viendo el éxito de DMA, muchos spammers han intentado emularlo. Hoy muchos envíos de correo electrónicos tienen una pequeña nota al fondo (ver Figura 2.6):

```
To unsubscribe to “Pure Power Marketing Tips” please reply to this
message and type in unsubscribe in subject line.
```

Figura 2.6: Nota al fondo de mensaje spam

Si los spammers remueven al usuario de la lista, es actualmente cuestionable. Muchos mensajes del spam se envían de direcciones fraudulentas a las que no pueden contestarse. En otros casos, los spammers coleccionan direcciones de personas que han pedido ser quitadas y venden a otros spammers las listas de dirección como “confirmadas”.

Las listas opt-out podrían parecer una solución al problema de e-mail no solicitado, en función de que los spammers usen las listas correctamente y no abusen de ellas para recoger direcciones del e-mail.

Filtrando el correo basura

Una sugerencia común para tratar con e-mail no deseado es “sólo pulsar el botón suprimir” para anularlos del buzón, después de que el usuario ha determinado que no está interesado en el contenido. Esta táctica tiene la ventaja de ser simple y no requiere de ningún software especial.

Pero, desgraciadamente, pulsar el botón “suprimir” tiene muchas desventajas. El e-mail basura todavía interrumpe el tren de pensamiento y el usuario debe pasar tiempo determinando cuales mensajes son no deseados. Si recibe muchos mensajes de e-mail no deseados, ellos pueden llenar el buzón, impidiendo recibir mensajes importantes. Un mejor enfoque sería tener la computadora configurada para anular el spam automáticamente, antes de revisarlos.

Filtros

Un filtro es un juego de instrucciones para el tratamiento de un e-mail. Por ejemplo, un filtro de correo podría incluir las siguientes instrucciones:

- Si el correo es de *mom@home.org*, salvar en el buzón familiar.
- Si el correo es de *dracula@monster.com*, borrarlo.
- Por otra parte, dejarlo en el buzón entrante.

La flexibilidad del filtro depende del software que lo hace. La mayoría de los filtros pueden archivar mensajes en los buzones, pueden anular mensajes o pueden dejarlos intactos. Algunos pueden activar programas externos y pueden pasar los mensajes a esos programas. Todos los filtros pueden tomar decisiones basadas en títulos del mensaje, algunos también pueden examinar el cuerpo del mensaje.

Existen muchos programas para filtrar e-mails, dentro de los que destacan el cliente de correo de Eudora Pro, Microsoft Outlook Express y el Netscape Messenger. En sistemas Unix, el paquete de correo *elm* incluye una utilidad de filtros llamada *filter*, pero un programa más complejo y poderoso llamado *procmail* [12] se ha vuelto el estándar para los trabajos serios de filtros. Con estos programas es normal que el usuario escoja que filtros aplicar al e-mail entrante; cada usuario puede tener un juego diferente de filtros.

En tal sentido, los filtros de e-mail verifican un mensaje entrante contra cada instrucción en orden, y se detiene cuando el mensaje coincide con una de las instrucciones. Esto hace crítico el orden de las instrucciones de filtrado. Por ejemplo, este filtro, mientras parece correcto, borrará mensajes de *mom* (remitente) con la palabra *money*:

- Borrar los mensajes con el título money.
- Salvar los mensajes de *mom* en el buzón familiar.
- Dejar el resto en el buzón de entrada.

Por eso, un mejor filtro sería:

- Salvar los mensajes de *mom* en el buzón familiar.
- Borrar los mensajes con el título money.
- Dejar el resto en el buzón de entrada.

Para ello, el usuario debe ser muy cuidadoso con los filtros que automáticamente borren mensajes. Con este ejemplo, se mostró que es fácil borrar accidentalmente mensajes que realmente se desean.

Otras estrategias de filtrado

Cuando se filtra para reducir la cantidad de correo basura, una táctica obvia es enfocarse en el remitente del mensaje e intentar evitar mensajes enviados por los spammers.

En este caso se mencionan dos enfoques básicos que permiten filtrar e-mails por la dirección del remitente del mensaje:

- Con el enfoque “rechazar los villanos, permita a otros”, se usan filtros para anular mensajes de spammers conocidos. Se asumen mensajes de los remitentes desconocidos como buenos y se les permite atravesar el filtro. El usuario no sabrá si debe agregar los remitentes desconocidos a la lista de villanos, hasta que ellos le envíen un mensaje no deseado.
- Con el enfoque “permitir a los amigos, rechazar a los otros”, los filtros sólo permiten mensajes de las direcciones preseleccionadas y anulan a todos los otros que no lo están. Este enfoque es hostil a los extraños; sólo las personas a quienes se ha decidido que se desea recibir sus mensajes podrán alcanzarlo.

Por otro lado, hay que tomar en cuenta que debido a que la segunda estrategia hace la comunicación más difícil, algunas variaciones pueden ser más útiles. Con el *procmail*, en lugar de anular mensajes de los remitentes desconocidos, el usuario podría hacer rebotar los mensajes a sus remitentes junto con una solicitud de contraseña del filtro, y aceptar mensajes de cualquiera de los amigos o de aquellos que contengan la contraseña del filtro en el asunto. Como los spammers no se molestarán con leer los mensajes de rechazo, se debe personalizar el correo basura para incluir la contraseña del filtro. Todo esto proporciona buena protección contra el e-mail no deseado, mientras se permite la entrada a aquellos que realmente desean localizar al usuario.

Respondiendo al correo basura

En lo que respecta a esconder la dirección de correo, está muy lejos de ser 100% seguro. Sólo filtrando se evita el problema del spam y para detener al spam se debe detener al spammer.

Actualmente, la mayoría de los ISPs (CANTV, etc) tienen reglas que prohíben a sus clientes hacer spam. De acuerdo con esto, si se puede rastrear el sitio de donde se originó el spam se puede conseguir a menudo buenos resultados, quejándose con el administrador del sitio. El ISP del spammer puede no saber que sus computadoras están siendo usadas para enviar spam. El spam no se detendrá a menos que las víctimas se quejen. Por ello, informar a los ISPs acerca de los clientes que hacen spam es un servicio público; si todos asumen que alguien más pondrá la queja, el resultado es que nadie se queja.

En relación a lo expuesto, en esta sección se muestra cómo rastrear los correos basura, como identificar los ISPs y cómo quejarse eficazmente.

Trazando el correo basura

En la Figura 2.7 se ilustra el proceso de determinar la fuente de un mensaje de e-mail y luego se realiza un análisis del mensaje, como recibido por *chrism@pluto.solar.net*.

```
From you@earth.solar.net Sat May 9 12:40:45 1998
Received: from jupiter.solar.net (jupiter.solar.net [1.4.4.7]
    by pluto.solar.net (8.8.7/8.8.7) with SMTP id KAB00332
    for <chris@pluto.solar.net>; Sat, 9 May 1998 12:40:45 –0600
Received: from jupiter.solar.net (jupiter.solar.net [1.4.4.4]
    by jupiter.solar.net (8.8.8/8.8.8) with SMTP id MAA00395
    for <chris@jupiter.solar.net>; Sat, 9 May 1998 12:40:40 –0600
Date: Sat, 9 May 1998 12:40:30 –0600
From: you@earth.solar.net
To Chris <chris@jupiter.solar.net>
Subject: Steel Pulse concert date
Message-Id: 19980509124030.0113@earth.solar.net
X-Mailer: QUALCOM Windows Eudora Pro Version 4.0
X-UIDL: 179c97f481a775da1a8109409a00fe

Hi, Chris!

The next steel Pulse concert is on Friday. See you there!
```

Figura 2.7: Determinación de la fuente de un e-mail

¿Cómo sabe Chris quién le envió el mensaje? En el mensaje, hay varias indicaciones:

- El título "*From:*" lista *you@earth.solar.net* como el remitente. Para el e-mail legítimo esto es suficiente. Los remitentes legítimos quieren que el usuario sepa que ellos enviaron el mensaje, pero el valor del título "*From:*" puede ponerse fácilmente en cualquier dirección de correo válida o no.
- El título "*Message-Id*:" indica que el mensaje fue originado en *earth*.*solar*.*net.* Como la mayoría del software de correo agrega un *Message-Id* basado en el host que envía el mensaje, este título también normalmente apunta a donde el mensaje se originó. Pero, nuevamente, un spammer puede insertar fácilmente un *Message-Id* ficticio para enviarlo.
- Finalmente, los títulos "*Received:"* muestran que el correo viajó desde *earth*.*solar*.*net* a *jupiter*.*solar*.*net* y luego a *pluto*.*solar*.*net*. Como Chris tiene cuentas en *jupiter* y *pluto*, ella realmente sabe que el mensaje viajó como el primer título "*Received:"* indica. Es más, como el segundo título "*Received:"* fue agregado por *jupiter*, un organizador fidedigno, Chris sabe que *jupiter* recibió el mensaje de *earth*.*solar*.*net*

Sólo los títulos "*Received:"* agregados por organizadores fidedignos, son verdaderamente fiables para determinar la fuente de un mensaje, pero ellos no identifican al usuario que envió el mensaje. Sin embargo, ellos retroceden al sitio que los originó. Hay una variedad de trucos que los spammers usan para engañar sus títulos del mensaje y reducir la posibilidad de identificación.

Cualquier título en un mensaje de e-mail puede ser inventado por el remitente. Los títulos pueden apuntar a una dirección de e-mail completamente ficticia o pueden sugerir las direcciones e-mail reales de un usuario.

Agregando títulos "Received:" ficticios

Debido a que los títulos "Received:" son a menudo las pistas más útiles para detectar la fuente de un mensaje no deseado, algunos spammers intentan esconder sus huellas agregando imitaciones de los títulos. No todos los títulos "Received:" agregados son obvios, pero uno inválido siempre es sospechoso.

Pistas obvias para títulos "Received:" forjados son: un formato inválido, hostnames inválidos, direcciones IP inválidas y fechas extremadamente incorrectas. El destinatario debería colocar una dirección de e-mail que el usuario reconozca; si no lo hace, el título probablemente sea forjado.

Si usted recibe el e-mail a través de un firewall, el sistema que remite puede agregar títulos "Received:" sospechosos. Así que se debe analizar un trozo de correo, para ver lo que se debe esperar.

Sitios de relevo

Otra manera en que los spammers tratan de esconder la fuente del spam está en utilizar un MTA (Mail Transport Agent) que pueda hacer relay en lugar del propio agente del spammer. Un sitio de relevo es fácil de reconocer por los títulos "*Received*:" (ver Figura 2.8).

```
Received: from relay.site.org (RELAY.SITE.ORG [128.250.200.51])
       by araw.uic.edu (8.8.8/8.8.8) with ESMTP id PAA25824
       for <alanz@araw.uic.edu>; Mon, 23 Feb 1998 15:41:43 –0600 (CDT)
Received: from spammer.evil.com (SPAMMER.EVIL.COM [129.23.99.26])
       by relay.site.org (8.8.5/8.8.5) with ESMTP id PAA176000
       for alanz@araw.uic.edu; Mon, 23 Feb 1998 15:37:15 –0600 (CDT)
```

Figura 2.8: Sitios de relevo

Haciendo una revisión, se observa que araw.uic.edu recibió el mensaje de relay.site.org. Se deduce que este título es exacto, además que *relay.site.org* recibió el mensaje de *spammer.evil.com. Entonces:* o *relay* está siendo usada como un relevo por *spammer.evil.com,* o si el segundo título "*Received*:" es ficticio, el spam vino de *relay.site.org*. De cualquier modo, se debe informar al administrador de *relay.site.org* para que sepa de este mensaje.

Hay muchos usos legítimos para relevar e-mails. En organizaciones donde los usuarios tienen PC que no tienen MTA propio, el e-mail del PC es relevado por un servidor del correo central, esto debe permitirle al PC relevar mensajes.

La página web de seguridad *http://maps.vix.com/tsi,* contiene una herramienta en línea, que los administradores de sistema pueden usar para chequear el MTA y asegurarse que ellos no relevarán mensajes.

Encontrando a los responsables

Usando estas técnicas se puede identificar el sitio donde se originó el spam, así como los sitios donde se anunciaron y sitios que están usándose como relevos.

Verificando sitios con nslookup de DNS

Primero, el usuario tiene que separar los sitios reales de los sitios farsantes. Los spammers forjan a menudo títulos para que ellos parezcan estar enviando correo de sitios ficticios. La manera más fácil de decir si un sitio es un host de Internet genuino, es realizar una búsqueda de DNS de su hostname. En la Figura 2.9 se muestra el resultado de una búsqueda del servidor web del Williams College, *web.williams.edu*, usando *nslookup* [5].

```
Non-authoritative answer:
web.williams.edu        internet address = 137.165.4.29
Authoritative answer:
Williams.EDU    nameserver = lee.williams.EDU
Williams.EDU    nameserver = lenox.williams.EDU
Williams.EDU    nameserver = nic.near.net
lee.williams.EDU      internet address = 137.165.4.2
lenox.williams.EDU    internet address = 137.165.4.21
nic.near.net    internet address = 192.52.71.4
```

Figura 2.9: Búsqueda de un servidor web

Además de listar las direcciones de Internet del sitio (así se demuestra que es un host real), *nslookup* muestra información sobre los servidores que tienen autoridad sobre el dominio[5]. Si se busca al host de un spammer, sabiendo quién proporciona el servicio del nombre, puede sugerir quién proporciona el servicio de Internet al spammer.

En dos casos no se verá la dirección de IP del sitio. Primero, puede ser que el nombre del host buscado no sea el nombre real, sino un nombre alternativo. Para el nombre real en la Figura 2.10 se muestra el resultado de búsqueda de *www.williams.edu.*

```
www.williams.edu canonical name = web.williams.edu
```

Figura 2.10: Resultado de búsqueda

Esto permite saber que el nombre real del host es web.williams.edu. Una búsqueda de DNS de ese nombre (nombre canónico), deberá devolver la información de las direcciones IP.

[5] Es posible tener que poner opciones en su programa de búsqueda para conseguir mostrar los nombres de servidores y otra información DNS asociada con un hostname.

Otra posibilidad, es que el host que se está buscando no maneje su propio e-mail, sino que otro host llamado *mail exchanger* o *MX* lo maneja (ver Figura 2.11).

```
sjdm.org  preference = 10, mail exchanger = mail.sjdm.org
```

Figura 2.11: Manejo de e-mail

El correo enviado a sjdm.org realmente es manejado por mail.sjdm.org. Una búsqueda de DNS a ese nombre debería devolver la dirección IP.

Investigando dominios con whois

Si se tiene problemas para encontrar el host en el DNS, la otra posibilidad que existe es buscar al nombre del dominio en el registro de InterNIC[6].

En la Figura 2.12 se presenta un ejemplo de una búsqueda whois [5] para *asambleanacional.gob.ve*.

```
Servidor Whois de NIC-Venezuela (.VE)
Este servidor contiene informacion autoritativa exclusivamente de
dominios .VE
Cualquier consulta sobre este servicio, puede hacerla al correo
electronico whois@nic.ve
Titular:
   Asamblea Nacional (asambleanacional.gob.ve-dom)
      informatica@an.gob.ve
      Asamblea Nacional
      Edif. José Maria Vargas, Esquina De Pajarito Piso 1
      Caracas, Distrito  Capital  VE
      0212-4096306/6310/6304

   Nombre de Dominio: asambleanacional.gob.ve

   Contacto Administrativo:
      Azdruval Figueroa (asambleanacional.gob.ve-adm)
      azdruvalfigueroa@an.gob.ve
      Asamblea Nacional
      Edif. Jose Maria Vargas, Esquina De Pajarito Piso 2
      Caracas, Distrito  Capital  VE
      0212-4096305

   Contacto Técnico:
      Carlos Palacio (asambleanacional.gob.ve-tec)
      carlospalacios@an.gob.ve
      Asamblea Nacional
      Edif. José Maria Vargas, Esquina De Pajarito Piso 3
      Caracas, Distrito  Capital  VE
      0212-4096317

   Contacto de Cobranza:
      azdruval Figueroa  (asambleanacional.gob.ve-bil)
        azdruvalfigueroa@an.gob.ve
      Asamblea Nacional
```

[6] http://www.internic.net

```
      Edif. José Maria Vargas, Esquina De Pajarito Piso 4
      Caracas, Distrito  Capital  VE
      0212-4096306/6310/6304

   Ultima Actualización: 2007-08-23 20:15:31
   Fecha de Creación: 2007-08-23 13:11:35

   Estatus del dominio: ACTIVO

   Servidor(es) de Nombres de Dominio:
   - dns1.asambleanacional.gob.ve
   - dns.reacciun.ve
NIC-Venezuela - CNTI
http://www.nic.ve
```

Figura 2.12: Búsqueda con whois

Además de demostrar que *asambleanacional.gob.ve* es un nombre de dominio registrado, se obtienen las direcciones e-mails de las personas responsables para el dominio.

Administradores de correos

En este caso, las personas listadas como contactos de DNS pueden ser responsables para asignar hostnames dentro del dominio, pero pueden no ser los administradores del sistema para las computadoras con esos hostnames. Por ejemplo, Carlos Palacio (el administrador de DNS), asigna nombres a todos los hosts de *asambleanacional.gob.ve*, pero posiblemente no maneja la computadora www.*asambleanacional.gob.ve* realmente.

Por ello, cualquier sitio que recibe e-mails debe tener una dirección de administrador de correos que entrega correos a la persona responsable del sitio de e-mail. Casi todos los ISPs tendrán estas direcciones y muchos también tienen una dirección para informar sobre el abuso de sus servicios. Si se envía un correo al administrador de correos y rebota, se puede usar la información de contacto DNS para avisar a alguien asociado con el dominio.

Identificando proveedores de servicio con traceroute

Si el spammer ha registrado su propio dominio y resuelve sus propios nombres de servidores, todos los whois avisarán que la información puede ser dirigida al spammer. Una manera de hacer una buena suposición sobre quién está proporcionando servicio de Internet al sitio desde donde se origina el spam, es ver la ruta por donde viajan los datos al sitio. La compañía que posee el último enrutador antes del sitio del spammer, puede estar proporcionando el servicio de Internet a éste.

En este sentido, el programa *traceroute* (Unix) [5] o *tracert.exe* (DOS/Windows), proporciona una tabla referente a cómo viajan los datos a través de la red para alcanzar el sistema remoto. Es útil para aprender sobre la estructura del

Internet, diagnosticando conexiones fallidas u otros problemas y determinando quién proporciona servicio de Internet a un sitio que hace spam.

2.2.2Técnicas para administradores

Cuando se está prestando un servicio de Internet a otros, el spam debe ser de particular preocupación. No sólo puede que sus usuarios reciban correos no deseados, sino que sus usuarios podrían estarlo enviando o un spammer podría intentar usar su sitio para enmascarar la fuente de sus mensajes. Si el usuario es el administrador de correo de la organización, tendrá que tratar con los efectos de mensajes no deseados en el sistema de correo.

Escoger políticas y definir las reglas de uso del servicio

Una de las decisiones más importantes que se debe tomar como administrador de sistemas de correo o ISP, es elegir cuáles son las políticas a utilizar. Para hacer dicha elección se deben realizar las siguientes preguntas:

- ¿Cuál es la filosofía de seguridad?, ¿cuánto tiempo se está dispuesto a gastar para proteger el sistema de ser blanco de un spam?
- ¿Cómo se quiere tratar con el spam que pudiera enviarse a los usuarios del sistema?
- ¿Cómo se quiere tratar con las quejas contra los usuarios? Si las quejas demuestran ser ciertas, ¿qué acción se deben tomar contra los usuarios?
- ¿Cómo se quiere diseminar información sobre las políticas y asegurar que los usuarios estén de acuerdo con ellas?

Filosofía de seguridad

Cuando los usuarios empiezan a recibir spam o cuando un spammer enmascara la fuente del spam sugiriendo que se originó en su sitio, la reacción dependerá en parte de cuánto tiempo y energía el administrador puede gastar para proteger su sitio, educar a sus usuarios o rastrear a los abusadores. El tiempo y personal disponible determinará si el administrador puede cazar activamente a los spammers, quejarse a sus proveedores, demandar a los spammers, etc.

Si el administrador dispone de poco tiempo, el mejor uso del tiempo puede ser establecer controles fuertes desde el inicio. Si por otro lado, tiene los recursos para ayudar a sus usuarios a perseguir spammers, es mucho mejor.

Spam a sus usuarios

En cuanto a este aspecto, existen tres enfoques básicos que están relacionados con el spam:

- Identificar a los spammers y bloquearlos a nivel del sistema: con este enfoque también se corre el riesgo de bloquear accidentalmente mensajes legítimos y arriesgarse al enojo de sus usuarios.

- Proveer las herramientas a sus usuarios, pero no envolverlos activamente: cada usuario escoge cómo tratar su propio correo.
- Utilizar un enfoque híbrido: quizás se bloquee al spam obvio a nivel de sistema y se provea las herramientas a los usuarios para usar algunos filtros, o se mantengan filtros que cualquier usuario puede escoger.

Cualquiera que sea el enfoque que se escoja, se debe estar claro con los usuarios. Si los usuarios firman por el servicio esperando recibir sus correos o noticias puras, ellos no pueden estar contentos si está bloqueando el spam. Por otro lado, si ellos piensan que el servicio los protege de spam y no es así, se desagradarán también.

Spam por sus usuarios

¿Qué proceso seguirá el administrador si recibe una queja que alega que uno de sus usuarios ha estado enviando correo basura no solicitado?, ¿tendrá los registros lógicos con lo cuales determine cuándo el usuario envió los mensajes?, ¿cuántos mensajes fueron enviados y a quien?, ¿se pedirá una explicación al usuario?, ¿se cerrará la cuenta del usuario hasta que se resuelva la situación?

Si la queja demuestra ser bien fundada: ¿qué acción tomará contra el usuario?, ¿se proporcionará una advertencia?, ¿se cancelará la cuenta del usuario o se buscará acciones legales contra el mismo?

Diseminando la información de la política

Con respecto a cómo el administrador permitirá a sus usuarios saber sobre las políticas de uso del servicio, para ello existe un enfoque ideal que está relacionado con la formulación de una política contra el spamming como parte de la AUP (Acceptable Use Policy) de su sistema. Este es un documento que describe lo que constituye el uso aceptable e inaceptable del servicio, y cómo se debe responder al uso inaceptable. El AUP puede constituir un contrato legal entre el administrador y el usuario.

Por esta razón, un AUP bien escrito contra el spam debe contener como mínimo:

- Una descripción específica de lo que constituye el uso inaceptable de e-mail. La descripción debe dirigirse a los tipos de spam, cuando sea aplicable.
- Si se proporciona un servicio de Internet a otro ISP, debe contener una declaración clara, donde se manifieste que el administrador es responsable para distintas acciones con sus propios clientes.
- Una declaración de las acciones que se tomarán contra los usuarios que se comprometan en prácticas inaceptables. En tal caso, los administradores deben poder suspender el acceso de un usuario sin la

aprobación de los superiores; también debe indicar el administrador las acciones típicas de la política que puede tomar, pero sin limitarlas.
- Una declaración acerca de si bloqueará al spam al nivel del sistema.
- Una dirección de contacto o número de teléfono para los usuarios que tengan preguntas sobre la política.

En atención a lo antes señalado, es un paso importante el formular y dar fuerza a un AUP para impedir que el sistema se convierta en un asilo para spammers.

Bloquear el spam entrante

Existen diferentes enfoques para bloquear al spam a nivel de sistema. Algunos confían en modelos de búsqueda heurísticos para determinar si un mensaje dado podría ser spam, otros se enfocan en identificar y bloquear spammers conocidos, o los sitios de origen del spam.

En el agente de transporte de correo

El lugar más obvio para bloquear el spam entrante es en el MTA, debido a que el MTA tiene una copia completa del mensaje y tiene acceso a toda la información pertinente que ayudaría a decidir si el mensaje es spam.

En este sentido, la mayoría de los MTAs de Internet proporcionan maneras de bloquear spam y que se lleven a cabo, pero a menudo estos bloqueos requieren considerables conocimientos de los funcionamientos del MTA.

Por eso, cuando se está bloqueando el spam en el MTA, una decisión importante tiene que ver con la clasificación del spam. En tal caso, existen cuatro enfoques principales que se deben tomar en cuenta:

- *Aceptar y dejar el mensaje:* con este enfoque, el MTA acepta el mensaje del spammer y entonces lo anula o lo archiva en alguna parte insignificante (por ejemplo, para quejarse). Esta no es una buena opción, porque consume recursos del sistema que procesa los mensajes.
- *Aceptar y rebotar el mensaje:* con este enfoque, el MTA acepta el mensaje del spammer y lo pasa a un filtro que devuelve un mensaje al spammer. Este enfoque le exige al sistema procesar los mensajes, pero desgraciadamente muchos spammers falsifican la información de dirección de retorno, así que el mensaje probablemente será enviado a un lugar inexistente.
- *Rebotar el mensaje con un error permanente:* con este enfoque, el MTA informa al sitio original durante la transacción de SMTP, que el mensaje se rechaza y no debe ser reenviado. El remitente normalmente recibe una notificación de que su mensaje fue rechazado. Ésta es la respuesta más común y más eficaz contra el spam bloqueado por el MTA.
- *Rebotar el mensaje con un error temporal:* con este enfoque, el MTA informa al sitio original que el mensaje no puede entregarse debido a un

problema temporal. El sitio original continuará intentando la entrega, regularmente, por algún período.

Cualquiera que sea la opción que se escoja, está basada en los recursos del sistema y sus propias preferencias. En esto radica la utilidad de mezclar estas opciones. Hay también otras, menos comunes: podría mantener al spam sospechoso para la revisión posterior o podría entregarlo con un título especial que indica que el mensaje puede ser spam, permitiéndoles a sus usuarios filtrar basándose en ese título.

Bloquear a los hosts no resolubles

Los spammers forjan a menudo sus direcciones *"From:"* para impedir que las quejas vuelvan a ellos o a sus proveedores. Algunos spammers usan direcciones forjadas con dominios inválidos. Debido a que los e-mail legítimos siempre deben incluir una dirección de e-mail de remitente válido, se pueden bloquear muchos mensajes no deseados, negándose a aceptar e-mails que vienen de un dominio que no esta registrado en el Servicio de Nombres de Dominio.

Pero, bloquear los mensajes de dominios que no se pueden encontrar en los DNS[7] representa un problema; el dominio puede ser uno real, todavía irresoluble debido a fallas del DNS. De acuerdo con esto, muchos administradores prefieren devolverle un error temporal al remitente, en lugar de uno permanente.

Bloquear los spammers conocidos

Si se tiene una lista de sitios y usuarios que fueron reconocidos como spammers, se podría rechazar cualquier e-mail de esas fuentes. La mayoría de los MTAs proporcionan una manera de inspeccionar la dirección del correo entrante contra una "lista de infractores", y rechazar así correos de dominios o spammers. Algunos de los sitios más conocidos son los siguientes:

- http://www.mindspying.com/cgi-bin/spamlist.pl
- http://www.znet.com/spammers.txt
- http://www.wsrcc.com/spam/spamlist.txt
- http://www.e-scrub.com/cgi-bin/blacklists.cgi

Además, cuando se recibe spam en el sistema se puede agregar el spammer a una lista propia de infractores. En lugar de usar la configuración del MTA para rechazar los hosts infractores se puede impedir que se conecten al puerto SMTP, usando filtros TCP. Esto controla si un host puede o no acceder a un puerto dado en el sistema.

[7] Otra posibilidad es que la dirección no sea una verdadera dirección de Internet, sino una dirección UUCP o algún otro tipo de dirección de la red.

Utilizar el RBL

Una variación sofisticada de listas de spammers, en cuanto al RBL (Realtime Blackhole List), es un servidor de nombres que tiene registros de DNS para sitios considerados como spammers, relevos de spam, o los proveedores de servicio de spam.

Si el MTA utilizado puede tomar decisiones sobre sitios remitentes buscándolos en el DNS, se puede verificar el RBL y bloquear cualquier mensaje de sitios que tienen archivos allí. En muchos MTAs, realizar una búsqueda de DNS puede ser más rápido que investigar una lista de spammers; también es posible configurar el servidor de nombre local, para reflejar una copia del RBL para aun hacer más rápidas las búsquedas[8].

El RBL probablemente se equivoca al bloquear a muchos en lugar de pocos. Por ejemplo, el RBL lista sitios que se usan como relevos del spam, hasta que el relevo abierto se apague (o hasta que pasen de 20 a 30 días sin cualquier incidente de relevo). Por otro lado, el RBL es probablemente más moderno que cualquier otra lista, y los cambios en el RBL son al instante y transparentemente distribuidos gracias al uso del DNS.

En el router

También el RBL puede usarse para bloquear sitios de spam en el enrutador de la red. Si el enrutador puede comunicarse usando BGP (Border Gateway Protocol) [13], los MAPSs (Mail Abuse Prevention Systems) pueden configurar el enrutador para que le diga los sitios de spam, para que el enrutador pueda dirigir paquetes de spam listado en el RBL a una dirección “Black Hole”[9].

Una mayor ventaja de bloquear el spam en el enrutador, es que el mismo representa un punto de ahogo para los datos. Se puede, con un sólo cambio del enrutador, mantener alejadas las conexiones de los hosts listados en el RBL. Esto lo aleja de tener que configurar cada sistema que recibe e-mail para hacer que busque en el RBL.

Parar el spam saliente

Proteger los usuarios de spam entrante es importante, pero el problema del spam no se acabará hasta que los spammers se detengan. Al principio se discutieron las AUPs; aquí se examinarán algunas tácticas y técnicas que pueden mantener alejados a los spammers, previniendo a sus usuarios del spam.

[8] Cuando el RBL cambia, el servidor de nombre local se notifica para poner al día su copia.
[9] Una dirección donde el spam no puede escapar.

Evitar ser atacado

Los spammers pueden enviar e-mail basura utilizando su servidor de correo como relevo.

No permitir que el servidor sea utilizado como relevo

Si un spammer puede usar su servidor de correo como relevo [1] puede enviar spam que no puede ser devuelto a él; peor, el spam se devolverá a su sitio y el administrador recibirá quejas de eso. Esto significa que si su servidor de correo permite ser relevado, puede hacer que sea agregado al RBL (como se discutió antes) lo cual causará que muchos otros sitios rechacen e-mails de este sitio.

Por esta razón, el enfoque básico para prevenir el relevo es configurar el servidor de correo para que acepte sólo e-mails que sean enviados por alguien a su sitio o se dirija a alguien en su sitio.

Manteniendo un ojo en los usuarios

Finalmente, aquí están algunas formas con las cuales se puede monitorear a los usuarios para asegurarse que ellos no están haciendo spam en el sitio.

Guardar archivos log efectivos

El administrador que proporciona un servicio en línea a usuarios debe guardar traza de la actividad que ellos realizan. Esta traza puede ser evidencia importante si un usuario está haciendo spam desde el sitio.

De permitir conexiones remotas los módems, demonios PPP, o demonios SLIP, deben ser configurados para registrar la fecha, el tiempo de cada conexión o desconexión, la identidad del usuario que marca y la dirección IP que se asignó a la conexión.

Si los usuarios se conectan a las cuentas locales, el demonio del login debe registrar la fecha, tiempo y el username de cada conexión. En sistemas Unix, se puede habilitar cuentas del sistema para que se pueda repasar órdenes que los usuarios han tecleado, si se necesita investigar una queja de spam, siendo recomendable, por ello, establecer una política de retención de archivos para los accesos de conexión y trazas del servidor de correo. Se debe guardar las trazas de por lo menos una semana o, con suerte, por lo menos un mes, si se tienen los recursos para hacerlo.

Ejecutar un servidor IDENT

Cuando un cliente se conecta a un servidor, el servidor siempre sabe la dirección IP del cliente. Bajo algunas condiciones, el servidor puede determinar también al usuario específico que comenzó la conexión. El RFC 1413 [14] describe el protocolo IDENT, una manera para que los servidores pidan el nombre del usuario que ejecuta el proceso que controla la conexión.

Si uno de los usuarios empieza el spam, sus mensajes pueden permitirle a otro administrador de sistema que rastree el mensaje del usuario y proporcionarle la mejor evidencia para confrontar al usuario.

Cuando uno de los usuarios se conecta a un sitio remoto, ese sitio puede identificar el número del puerto de la conexión y puede pedir el nombre del usuario al servidor IDENT.

Técnicas activas

Hay una variedad de técnicas que pueden ser usadas para descubrir y detener a los usuarios de enviar spam. La detención del spam activo da mucho que hacer en la actualidad.

La manera más fácil de detener el spam activamente es establecer un límite para el número de mensajes de e-mail que cada usuario puede enviar en un solo día. Entonces, simplemente se debe controlar el número de mensajes de e-mails que cada usuario envía y suspender la cuenta (o la habilidad para enviar correo) cuando este límite se excede.

Otra manera simple para impedir a los usuarios enviar spam a través de los servidores de correo que permiten relevar, es bloquear el acceso a esas máquinas. Simplemente se bloquean todas las conexiones TCP/IP salientes que se originen en direcciones IP asociadas con la conexión de los usuarios, con un destino de puerto 25 para cualquier host en el Internet.

Alternativamente, se puede supervisar los usuarios directamente usando un programa como *tcpdump* [5]. Tcpdump monitorea cada paquete de TCP/IP enviado a una red de área local. Si se pone una computadora a correr *tcpdump* entre los usuarios conectados y la conexión de Internet saliente, es posible supervisar cada paquete que envían y reciben los usuarios. Usando un filtro, se puede tener el informe de cada conexión TCP saliente que se origina en el sitio y tiene un destino al puerto 25 en un host remoto.

3. Marco Metodológico y Propuesta

Para el logro de los objetivos planteados en el capítulo 1, es necesario definir una metodología de trabajo que permita la conceptualización rápida de una propuesta eficiente al problema planteado. A continuación, se presenta la especificación de la metodología utilizada y otros detalles importantes que fueron tomados en cuenta para el desarrollo e implementación de la solución.

3.1 Recolección de la información

La primera fase contemplada en la metodología para el diseño e implementación de un servicio de e-mail con herramientas antispam y basado en software de dominio público, es la recolección de información sobre el estado actual de la plataforma de correo electrónico.

La recolección de esta información fue llevada a cabo a partir de entrevistas al personal que administra la plataforma de servidores de la Asamblea Nacional, así como la recopilación de documentos sobre normas y procedimientos del área de servidores y conocimientos propios del servicio. A continuación, se presentan las especificaciones de la plataforma de correo electrónico.

3.1.1 ¿Cómo funciona el servicio actualmente?

Para hablar sobre el funcionamiento actual del servicio de correo electrónico, se muestra en la Figura 3.1 el diseño actual o topología de conexión implementada.

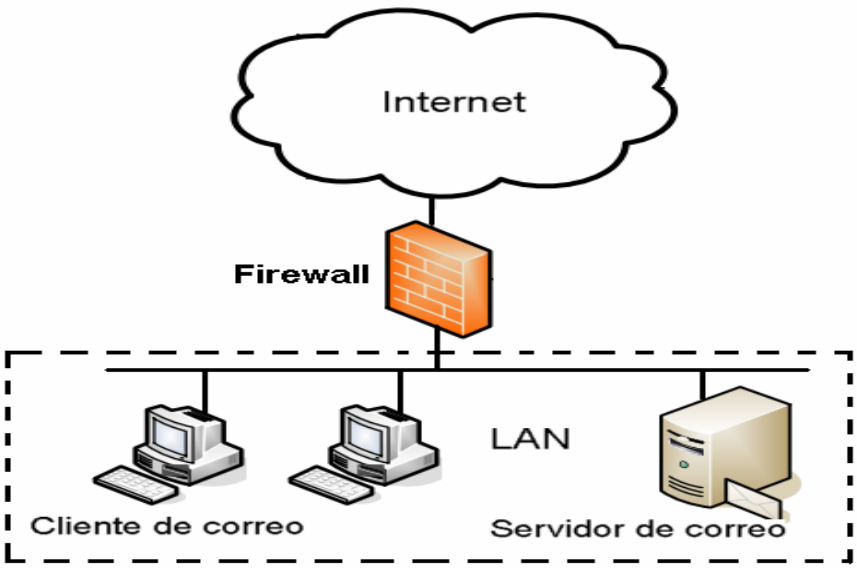

Figura 3.1: Topología actual del servicio de correo

Actualmente se cuenta con un servidor de correo electrónico que está ubicado en la LAN [13]. En el mismo equipo se almacena la información de los usuarios, buzones y demás componentes inherentes al servicio de correo electrónico.

El acceso desde la LAN no tiene ningún tipo de restricciones ni filtros. Este servicio es accedido desde Internet a través de un mapeo de direcciones efectuado por el firewall.

Se realizan respaldos completos cada mes e incrementales cada día[10], que luego son llevados a cintas y resguardados bajo normas y procedimientos establecidos.

El diseño o topología actual presenta una gran debilidad, ya que todos los equipos se encuentran dentro del mismo segmento de red y cualquier falla o vulnerabilidad de seguridad existente en alguno de estos equipos puede comprometer o poner en riesgo al servidor de correo.

3.1.2 Políticas de uso actual del servicio

Estas son algunas de las políticas de uso actual para el servicio de correo electrónico.

De la información

- La Dirección de Tecnología de Información de la Asamblea Nacional, podrá denegar el acceso a los servicios de correo electrónico e inspeccionar, monitorear y cancelar una cuenta de correo cuando hayan sospechas fundadas de violación de las normas internas de la Institución, o cuando existan requerimientos legales en base a la Ley Especial contra Delitos Informáticos.
- Todos los directores o jefes de área deben enviar una comunicación a la Dirección de Informática de la Asamblea Nacional, notificando el egreso de su personal para así eliminar la cuenta de correo.
- La vigencia de la cuenta comprende el período que inicia el primer día de trabajo y finaliza el día en que la Dirección General de Desarrollo Humano de la Asamblea Nacional notifica a la Dirección de Tecnología de Información el fin del compromiso contractual del empleado.
- En ningún caso el servicio de correo electrónico garantiza la entrega de un mensaje. Numerosas circunstancias pueden impedir la recepción de un mensaje (límite de almacenamiento en el buzón del usuario receptor, rechazo de mensajes por virus, direcciones mal formadas, etc.).

De la asignación de cuentas de usuarios

- Los nombres jerárquicos para las cuentas de usuario serán formados por el nombre seguido del apellido: williamcedeno.
- Si un nombre común se repite, se deberá tomar las siguientes políticas:
  - Ø Primer nombre, seguido del primer apellido: williamcedeno.
  - Ø Primer nombre, inicial del segundo nombre, seguido del primer apellido: williamjcedeno.

[10] http://www.monografias.com/trabajos14/respaldoinfo/respaldoinfo.shtml

  - Ø Primer nombre, seguido del primer apellido e inicial del segundo apellido: williamcedenoh.
  - Ø Primer nombre, inicial del segundo nombre, seguido del primer apellido e inicial del segundo apellido: williamjcedenoh
  - Ø Primer nombre, seguido del primer apellido y un dígito diferenciador consecutivo (1, 2, 3, etc): williamcedeno1
- El Nombre Común (CN) no debe superar los 20 caracteres.
- En caso de combinaciones que terminen formando palabras no éticas, deberá procederse a un cambio del identificador de usuario.
- Las dependencias como comisiones y direcciones tendrán un correo asignado con el siguiente formato:
  - Ø c.p_nombre@an.gob.ve. Comisión Permanente.
  - Ø c.m_nombre@an.gob.ve. Comisión Mixta.
  - Ø c.e_nombre@an.gob.ve. Comisión Especial.
  - Ø dir_ nombre@an.gob.ve. Dirección.
- Los nombres de usuarios que posean la letra Ñ será sustituida por la N.
- Los nombres con tildes son sustituidos por el mismo caracter sin la tilde.
- Los enlaces como Hernán de León estarán unidos (e.g. hernandeleon).

De la creación de cuentas

Una cuenta de correo electrónico permite el envío y recepción de mensajes y está asociada a una dirección única tanto en el ámbito de la Asamblea Nacional como de Internet:

- Todo usuario de la red de datos de la Asamblea Nacional tendrá asignada una cuenta de correo electrónico.
- Todos los usuarios de correo tendrán tanto correo interno como correo externo.
- Las cuentas de correo de la institución sólo responderán al dominio an.gob.ve.
- Cada usuario podrá descargar localmente sus correos.
- Se permitirá acceso tanto por el cliente de correo como vía web mail.
- Las cuentas de correo electrónico son intransferibles, sólo debe utilizarla el propietario de la cuenta.

Administración

- La Dirección de Tecnología de Información de la Asamblea Nacional, no hará monitoreos de forma rutinaria o inspecciones de los buzones sin el consentimiento del propietario del buzón, a menos que amerite por causas mayores una auditoría.
- El password debe ser creado para contener al menos ocho caracteres y debe ser cambiado por el usuario una vez realizado su primer acceso.
- Se debe garantizar los respaldos, tanto de los archivos de configuración como de las bases de datos.

- Todos los correos que ingresen serán revisados automáticamente para determinar la presencia de virus, de acuerdo con las políticas de protección antivirus establecidas.

Eliminación o suspensión de cuentas

- Cuando el usuario enviase a foros de discusión (listas de distribución y/o newsgroups) mensajes que comprometan la reputación de la Asamblea Nacional o violen la ley.
- Cuando finaliza la relación contractual del usuario con la Asamblea Nacional.
- A solicitud expresa del usuario.
- Inactividad de la cuenta: ningún mensaje leído/enviado durante un período de tiempo superior a 6 meses.

Usuario

- Todo usuario del correo tiene la responsabilidad de utilizarlo de forma eficiente, efectiva y ética, siguiendo el patrón esperado en cualquier comunicación escrita tradicional (memorandos, cartas externas, etc.).
- El usuario del correo electrónico debe asegurarse de:
  - Ø Dirigir cada mensaje al (los) destinatario(s) correcto(s).
  - Ø Enviar los mensajes a aquellas personas que realmente necesitan estar informadas y no a todas las personas que conoce.
  - Ø Evitar el envío de mensajes internamente con muchos archivos adjuntos.
  - Ø Hacer un uso adecuado del lenguaje en los correos electrónicos.

Seguridad

- El usuario debe bloquear su sesión antes de levantarse de su puesto de trabajo, para evitar que otra persona utilice su correo sin su consentimiento.
- El password de la cuenta de correo es intransferible, debe ser memorizado o guardardo en un lugar seguro por el usuario.
- La contraseña debe ser cambiada por el usuario cada cierto período de tiempo o cuando sospeche que está en peligro.
- La contraseña del usuario debe ser entre 8 y 11 caracteres alfanuméricos, tratando de no asociar el password con la cédula, nombre u otra característica que identifique al usuario.
- Está prohibido y será sancionado enviar mensajes con direcciones no asignadas por los responsables de la asignación de las cuentas de la Institución y, en general, está prohibido falsificar las cabeceras de correo electrónico saliente.
- Está prohibido facilitar y/o ofrecer la cuenta y buzón a personas no autorizadas.
- No están permitidos los mecanismos y sistemas que intenten ocultar la

identidad del emisor de correo.

Envíos masivos

Para la difusión de información deben respetarse las siguientes directrices:

- En ningún caso se podrá utilizar el servicio para la distribución de información ajena a las finalidades de la Asamblea Nacional.
- No se debe utilizar el servicio de forma indiscriminada, ya que el exceso de información puede llegar a ser negativo.
- En los mensajes se debe evitar incluir archivos binarios o documentos de tamaño elevado para evitar la degradación del servicio de correo y el llenado involuntario de los buzones de los usuarios.

Del manejo de la información

- Queda terminantemente prohibido el intercambio de información propietaria, confidencial o privilegiada, fuera de los límites de la organización o del grupo de trabajo para el cual la misma es de interés.
- Queda terminantemente prohibida la creación o intercambio de mensajes ofensivos, obscenos o que contengan amenazas. Si se recibe un mensaje con este tipo de contenido, el incidente deberá ser notificado a la Dirección de Tecnología de Información de la Asamblea Nacional, a través de correo electrónico soporte@an.gob.ve.
- Los usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de acceso o cuenta de correo que proporciona la Asamblea Nacional.
- Si se sospecha que la cuenta está siendo utilizada por una tercera persona, hay que avisar inmediatamente a la Dirección de Tecnología de Información o a la cuenta de correo electrónico soporte@an.gob.ve

Acuerdo de servicio

- El usuario reconoce y acepta que el servicio puede tener fallas, ser interrumpido, tener trastornos, entre otros.
- El usuario se compromete a seguir las normas y políticas establecidas por la Dirección de Tecnología de Información en el uso y manejo del correo electrónico y se sometera a cada una de ellas, con sus respectivas penalidades.

3.1.3 Estadísticas de uso actual

Existen creadas al menos tres mil (3000) cuentas de usuarios que corresponden a las nóminas de obreros, empleados, contratados y alto nivel.

De un universo aproximado de tres mil (3000) usuarios, en general hacen uso del servicio de correo regularmente unos 400 usuarios para intercambio de informacion institucional, y el restante lo utiliza pocas veces con mínimo consumo en sus buzones.

Este universo de usuario pronto será incrementado en un 100% aproximadamente, cuando la nómina de jubilados permita hacer consultas seguras vía web, lo que generará mayor demanda del servicio.

El espacio utilizado por el universo actual de usuarios es cercano a 240 GB de informacion, lo que representa un promedio (240 GB / 3000) de 80 MB por persona, y si se lleva contra los usuarios (240 GB / 400) de gran uso sería de 600 MB por persona. Estos valores serán de gran utilidad para el diseño conceptual de la solucion.

3.1.4 Componentes de software y hardware utilizados

En cuanto al software utilizado actualmente, se puede mencionar haciendo referencia a la forma en que es tratado el correo por los componentes del servicio:

- El servidor de correo está instalado bajo el sistema operativo Debian.
- El MTA utilizado es POSTFIX conjugado con MySQL para el tratamiento y configuración de las cuentas de correo.
- Para el manejo de listas se cuenta con el aplicativo Mailman[11] que se administra en forma independiente.
- El servicio de correo dispone de los protocolos IMAP y POP para que los clientes puedan descargar o sincronizar sus mensajes con cualquier cliente de correo local.
- Se hace uso del aplicativo Horde[12] para prestar el servicio vía web seguro (https).
- Por lo general, los usuarios utilizan como cliente de correo las aplicaciones Outlook y Outlook Express, ya que la mayoría de las estaciones de trabajo cuentan con el sistema operativo Microsoft Windows XP y la suite de Microsoft Office.

En cuanto al hardware en las estaciones de trabajo, se utiliza una variedad de computadoras de distinto rendimiento, desde un Pentium IV de 1,8 GHz, 256 MB de RAM, 40 GB de disco IDE, hasta un Quad Core de 3,2 GHz con 2 GB de RAM, 250 GB de disco SATA, equipadas con unidades de CD o DVD, puertos USB y demás periféricos básicos para su funcionamiento.

En la Tabla 3.1 se muestra el equipamiento de hardware que se utiliza a nivel de servidor. La Figura 3.2 muestra el equipo.

Figura 3.2: Servidor HP ProLiant DL360G5

[11] http://www.gnu.org/software/mailman/docs.html
[12] http://www.horde.org

Descripción del producto	HP ProLiant DL360 G5 High Efficiency - Quad-Core Xeon L5420 2.5 GHz
Factor de forma	Se puede montar en bastidor - 1U
Dimensiones (Ancho x Profundidad x Altura)	42.6 cm x 70.5 cm x 4.3 cm
Peso	12.5 kg
Procesador	1 x Intel Quad-Core Xeon L5420 / 2.5 GHz (Quad-Core)
Memoria caché	12 MB L2
Caché por procesador	12 MB (2 x 6 MB)
Memoria RAM	4 GB (instalados) / 32 GB (máx.) - DDR2 SDRAM - Código de corrección de errores (ECC) avanzado - 667 MHz - PC2-5300
Controlador de almacenamiento	RAID (Serial ATA-150 / SAS) - PCI Express x4 (Smart Array P400i); IDE (IDE/ATA)
Bahías de almacenamiento de servidor	Hot-swap
Disco duro	6 x 72 GB SAS.
Controlador gráfico	ATI ES1000 - 32 MB
Conexión de redes	Adaptador de red - PCI Express x4 - Ethernet, Fast Ethernet, Gigabit Ethernet - Puertos Ethernet : 2 x Gigabit Ethernet
Alimentación	CA 120/230 V (50/60 Hz)
Redundancia de alimentación	2 fuentes redundantes de 700w
Garantía del fabricante	3 años de garantía (in situ)

Tabla 3.1: Especificaciones HP ProLiant DL360G5

3.2 Análisis del servicio existente

Este análisis es de suma importancia ya que en él se refleja las fallas de percepción humana, que son la crítica real de un servicio.

3.2.1 Fallas de acceso

Muchos factores pueden impedir la utilización de un servicio. En el caso de estudio en la Asamblea Nacional, se presentan eventualmente fallas de conectividad con el sistema de correo electrónico. A pesar que no se le pueden atribuir estas fallas al propio sistema de correo electrónico, los usuarios no discriminan a la hora de quejarse del servicio. Es quizás por ello uno de los factores que refleja la baja demanda del mismo.

3.2.2 Falta de publicidad del servicio

La finalidad de las técnicas de publicidad son las de poder seguir argumentando e influir sobre el público, de forma constante, aunque no se encuentre el vendedor presente o éste no exista. En el caso de estudio, estas técnicas de publicidad no se efectuaron bajo un patrón contundente y constante, lo que generó un bajo nivel de aceptación del producto (correo electrónico).

3.2.3 Poco agradable al ojo humano

Cuántas veces se utiliza lo que no llama la atención o lo que no está de moda, este concepto es también manejado en el caso de los servicios digitales. El aplicativo Horde no es muy vistoso en comparación con otros de su índole (Hotmail, Gmail, etc.) aunque se pudiera cambiar el diseño agregando algunos plugins.

3.2.4 Proceso tedioso y lento de carga

El sistema de correo actual requiere autenticarse dos veces, lo que hace tedioso el acceso inicial al sistema. Cada pantalla de tratamiento del correo se tarda para cargar, tornando lenta su utilización.

3.3 Conceptualizar y diseñar una propuesta

En esta fase se mostrará la propuesta de solución para el nuevo servicio de correo electrónico con tratamiento de spam basado en software de dominio público.

3.3.1 Topología de conexión y flujo de datos

En la Figura 3.3 se detalla la topología de conexión que se pretende implementar. La misma obedece a las mejores prácticas de seguridad en cuanto a servicios públicos.

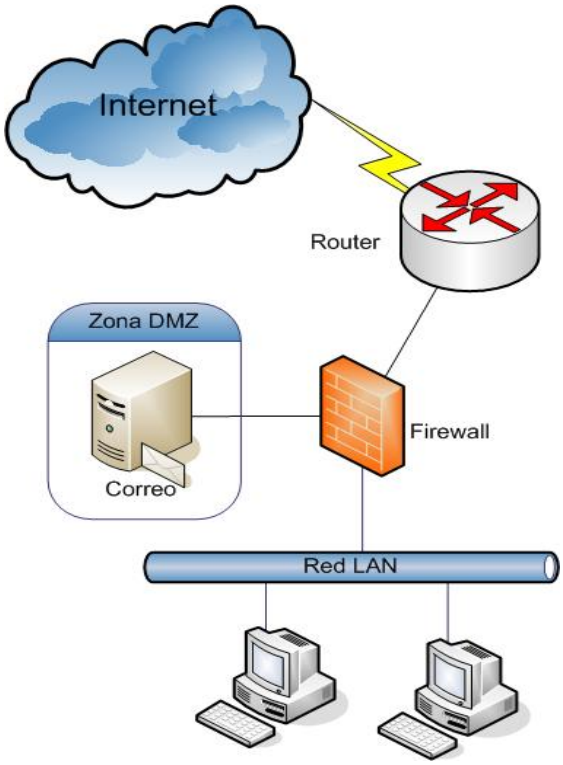

Figura 3.3: Topología de conexión propuesta

Los usuarios podrán acceder al servicio desde cualquier equipo conectado en la red LAN o vía remota, desde cualquier equipo conectado a Internet (incluso desde teléfonos móviles). A través del portal web que ofrece el servicio podrán efectuar el tratamiento de los mensajes que llegan al buzón electrónico y demás bondades que ofrece la solución, o en su defecto podrán instalar y configurar un agente de correo (MUA) de su preferencia.

3.3.2 Políticas de uso del servicio

Se propone la reforma de las políticas de uso para el servicio de correo electrónico, las cuales se describen a continuación.

Políticas y normas de uso del servicio de correo electrónico

Estas políticas aplican a todos los usuarios de mensajería de la Asamblea Nacional, que en lo sucesivo será llamada la Institución.

La Dirección de Tecnología de Información de la Asamblea Nacional, en la presente publicación, establece las políticas que se deberán adoptar para el uso de correo electrónico en las distintas unidades organizativas de la Institución. A su vez, se mencionan los términos y condiciones para el manejo y administración del correo electrónico, así como lo referente a toda transacción de información que haga uso del servicio de correo electrónico.

El objetivo de estas políticas es asegurar, establecer y proveer un modelo uniforme con los estándares básicos adecuados, que sirva de guía para el diseño, desarrollo, integración, manejo y administración apropiada del servicio de correo electrónico, así como salvaguardar la integridad de la correspondencia e información a ser transferida a través de los medios electrónicos de la Institución.

Nota: Cualquiera de las normativas y políticas antes expuestas pueden ser sujetas a cambio, cuando la Dirección de Tecnología de Información de la Asamblea Nacional considere necesario.

Aspectos generales

De la información

- El correo electrónico es una herramienta para el intercambio de información entre personas, no es una herramienta de difusión de información.
- La Dirección de Tecnología de Información de la Asamblea Nacional se compromete en la aplicación de la Ley Especial contra Delitos Informáticos en los artículos referentes al servicio de correo electrónico.
- En ningún caso, el servicio de correo electrónico garantiza la entrega de un mensaje bajo circunstancias como: virus, tamaño del mensaje, direcciones mal formadas, etc., que pueden impedir la recepción de un mensaje.

- Todo correo enviado desde los servidores de la institución llevarán el siguiente aviso legal:

> *Este mensaje es privado y confidencial, y está dirigido exclusivamente a su(s) destinatario(s). Si usted ha recibido este mensaje por error, debe abstenerse de distribuirlo, copiarlo o usarlo en cualquier sentido. Asimismo, le agradecemos comunicarlo al remitente y a la dirección soporte@an.gob.ve y borrar el mensaje y cualquier documento adjunto.*

Administración

- El tamaño máximo para el envío y recepción de un mensaje de correo electrónico será de 10 MB.
- La contraseña debe ser creada para contener al menos ocho caracteres y debe ser cambiada por el usuario una vez realizado su primer acceso.
- Los usuarios serán catalogados según el tipo de relación nominal con la Institución, lo cual enmarca la clasificación de las cuentas para asociar las clases de servicio (COS) de cada una. Por ende, los buzones tendrán una capacidad oscilatoria entre 100 MB y 5000 MB.
- En la medida que las circunstancias lo permitan se garantiza el respaldo de los archivos de configuración como de las bases de datos.
- Todos los mensajes que ingresen al servidor de correos serán revisados automáticamente para determinar la presencia de virus y el filtrado de clasificación de spam, de acuerdo con las políticas de protección establecidas podrán ser eliminados o colocados en cuarentena.
- Se podrá denegar el acceso a los servicios de correo electrónico e inspeccionar, monitorear y cancelar una cuenta de correo, cuando hayan sospechas fundadas de violación de las normas internas de la Institución, o cuando existan requerimientos legales.

De la creación de cuentas

- Para la creación de cuentas se deberá contar con la siguiente información referente al usuario: nombres y apellidos, cédula de identidad, tipo de empleado, teléfono de oficina, teléfono móvil o de habitación y ubicación física laboral.
- Las cuentas existentes permanecerán sin alteraciones de formación.
- Los nombres utilizados para la creación de cuentas de usuario deberán ser generados bajo el siguiente patrón: concatenación de nombre + punto + apellido + los 3 dígitos finales de la cédula (e.g. william.cedeno347).
- Las dependencias como comisiones permanenetes, mixtas, direcciones y otros entes dependientes de la Institución tendrán una cuenta de correo conceptualizado bajo el siguiente formato:
  - Ø cp.enlace@an.gob.ve (Comisión Permanente).
  - Ø cm.desarrollo@an.gob.ve (Comisión Mixta).
  - Ø dir.informatica@an.gob.ve (Dirección).

- Ø div.soporte@an.gob.ve (División).
- Los nombres de usuarios que posean la letra Ñ, deberá ser sustituida en la cuenta por la letra N.
- Los nombres con tildes son sustituidos en la cuenta por el mismo caracter sin la tilde.
- Los nombres como Hernán de León estarán unidos (e.g. hernan.deleon123).
- Los nombres de cuentas no deben superar los 20 caracteres y deben ser escritos en minúsculas.

De las cuentas

- Todo empleado, obrero, contratado, pensionado, jubilado, en comisión de servicio, o en algún estatus que refleje su vinculación salarial con la Institución, tendrá asignada una cuenta de correo electrónico intransferible.
- Cada unidad administrativa podrá tener asociada una cuenta de correo electrónico si así lo solicitase.
- La Dirección de Tecnología de la Información podrá efectuar actualizaciones y depuraciones periódicas de las cuentas, basadas en movimientos de personal.
- Toda cuenta de correo que permanezca inactiva por más de ciento ochenta (180) días será desactivada.
- La vigencia de la cuenta comprende el período que inicia con el primer día de trabajo y finaliza el día en que la Dirección General de Desarrollo Humano de la Asamblea Nacional notifica el finiquito de la relación con el empleado.
- Se eliminará una cuenta de correo cuando se comete una falta grave a las políticas de uso del correo.

Son responsabilidad del usuario

Redacción y envío

- Todo usuario del correo tiene la responsabilidad de utilizarlo de forma eficiente, efectiva y ética, siguiendo el patrón esperado en cualquier comunicación escrita tradicional (memorandos, cartas externas, etc.).
- El usuario del correo electrónico debe asegurarse de:
  - Ø Dirigir cada mensaje al (los) destinatario(s) correcto(s).
  - Ø Enviar los mensajes a aquellas personas que realmente necesitan estar informadas y no a todas las personas que conoce.
- Evitar el envío de mensajes internamente con muchos archivos adjuntos. Si necesita compartir información deberá utilizar los directorios compartidos destinados para tal fin en los servidores de archivo.

- Queda terminantemente prohibida la propagación de “cadenas”, publicidad o cualquier otro tipo de información no solicitada (spam) a través del uso del correo electrónico de la institución.

Seguridad

- El usuario debe bloquear su sesión antes de levantarse de su puesto de trabajo, para evitar que otra persona utilice su correo sin su consentimiento.
- La contraseña de la cuenta de correo es intransferible, el usuario debe memorizarla o guardarla en un lugar seguro y debe superar los ocho (8) caracteres.
- La contraseña debe ser cambiada periódicamente o cuando se sospeche que está en riesgo.

Del manejo de la información

- Queda terminantemente prohibido el intercambio de información propietaria, confidencial o privilegiada fuera de los límites de la Institución o del grupo de trabajo, para el cual la misma es de interés.
- Cada usuario podrá descargar localmente sus correos con el cliente de su preferencia. La Dirección de Tecnología de Información de la Asamblea Nacional recomienda el uso de la herramienta Thunderbird.
- Queda terminantemente prohibida la creación o intercambio de mensajes ofensivos, obscenos o que contengan amenazas. Si se recibe un mensaje con este tipo de contenido, el incidente deberá ser notificado a la Dirección de Tecnología de la Información a través del correo electrónico soporte@an.gob.ve.
- Los usuarios son completamente responsables de todas las actividades realizadas con su cuenta de correo.
- Si se sospecha que la cuenta está siendo utilizada por una tercera persona, se debe avisar inmediatamente a la Dirección de Tecnología de la Información o a la cuenta de correo electrónico soporte@an.gob.ve.
- Estará penalizado con la cancelación del buzón, el envío a foros de discusión (listas de distribución y/o newsgroups) de mensajes que comprometan la reputación de la Institución o violen la ley.
- No se permite el envío ni la recepción, a través del correo electrónico de la organización, de archivos con extensiones descritas en la Tabla 3.2.

*.vbs	*.bmp	*.psd	*.wav	*.voc	*.js	*.msc	*.mp3
*.mpeg	*.midi	*.msvideo	*.exe	*.dll	*.jse	*.msi	*.tar
*.mde	*.sh	*.arj	*.pif	*.src	*.lnk	*.mst	*.clsid
*.asd	*.asf	*.asx	*.bas	*.bat	*.mdb	*.ocx	*.chm
*.cmd	*.com	*.hlp	*.hto	*.inf	*.isp	*.mht	

Tabla 3.2: Extensiones de archivos

Acuerdo de servicio

- El usuario reconoce y acepta que el servicio puede tener fallas, ser interrumpido, sufrir variaciones, entre otros.
- El usuario se compromete a seguir las normas y políticas establecidas por la Dirección de Tecnología de la Información en el uso y manejo del correo electrónico, y se someterá a cada una de ellas con sus respectivas penalidades.

3.3.3 Estrategia de publicidad

No basta con establecer normas de uso para lograr los cambios de hábito en los usuarios o controlar la utilización del producto en sí, hay que motivar al usuario y generar la necesidad sobre el servicio. Por esto se debe acompañar el lanzamiento de un servicio o impulsar su uso con mecanismos de publicidad e instrumentos que generen la necesidad de utilización.

Como instrumentos de publicidad se proponen:

- La creación de pendones para colocarlos en las entradas de las sedes.
- La publicidad del servicio en la Intranet de la Asamblea Nacional.
- La generación de trípticos inherentes al servicio en conjunto a un proceso de entregas del mismo.
- La colocación de un stand de atención personalizada donde se puedan captar nuevos usuarios y explicar las bondades de la nueva plataforma.
- La utilización de los fondos de pantalla de los PCs para impulsar el servicio.

Como mecanismos que generen necesidad de uso estarían:

- Autenticación a través de la cuenta de correo para ver los recibos de pagos por la Intranet.
- Autenticación a través de la cuenta de correo, para poder publicar clasificados en la Intranet.
- Autenticación a través de la cuenta de correo para poder enviar mensajes SMS por la Intranet.
- Autenticación a través de la cuenta de correo para poder opinar en los foros de noticia de la Intranet.
- Envío a las cuentas de correo institucional de los cortes de cuentas de la caja de ahorro.
- Envío a las cuentas de correo institucional el talón de pago quincenal.

Con varios mecanismos e instrumentos que se dispongan, el impacto de uso debe aumentar significativamente.

3.3.4 Propuesta de solución

Enmarcado en las bondades de los servicios de correo más publicitados como Gmail, Yahoo y Hotmail, entre otros, se propone un conjunto de herramientas

que faciliten la administración y que, sobre todo, sea de impacto visual al usuario, sin dejar a un lado el concepto de software abierto y que cumpla con la necesidad de prevenir el spam.

Existe en el mercado una solución integral que cumple con todas estas características y mucho más; ésta se trata de Zimbra Collaboration Suite, que es multiplataforma y permite:

- Mensajería instantánea.
- Acceso con dispositivos móviles.
- Etiquetado de mensajes.
- Calendarios compartidos.
- Documentos compartidos.

Más allá de las propias funcionalidades en sí, proporciona mucha interactividad y posibilidades mediante la integración y combinación de distintas capas de información.

Con estas herramientas dentro del mismo portal de correo electrónico, se incrementa la productividad y el trabajo es más amigable y simple.

3.4 Selección del hardware y software a utilizar

En el mundo del software libre se puede encontrar un abanico de herramientas muy amplio para el propósito de este trabajo. Sin embargo, se debe decidir muy bien a la hora de escoger la que mejor se adapte a nuestras necesidades.

3.4.1 Sistema operativo

Linux es un núcleo de un sistema operativo creado por Linus Torwalds, quien nació en Finlandia el 28 de diciembre 1969 y estudió en la Universidad de Helsinki [8]. Desarrolló Linux porque deseaba disponer de un SO Unix en su PC. Linus quiso compartir el código para que cualquiera pudiera usarlo y contribuir a su desarrollo. Dado que en GNU ya habían desarrollado muchas herramientas para Unix con la misma filosofía de software libre, pronto se unió los dos proyectos en un SO (Sistema Operativo) GNU/Linux totalmente libre. Pero, dentro de las tantas herramientas que se desarrollaron, las más importantes aportadas por GNU fueron dos: el intérprete de comandos (bash) y el compilador de C (gcc).

Tipos de licencias libres

La licencia más utilizada en Linux es la licencia GPL de GNU. Sin embargo, hay otras licencias igualmente aceptables bajo el término de software libre [8]. Existiendo una serie de términos que rodean a este tipo de software libre, se describen a continuación algunos de ellos:

- *Libertad de distribución:* Se refiere a la libertad de comercializar el software sin que sea necesario pagar derechos de ningún tipo.

- *Código libre:* Se considera que el código es libre cuando las fuentes son de dominio público.
- *Integridad de las fuentes:* Recomienda no restringir los derechos de modificación del código fuente, aunque se aceptan algunas fórmulas que restringen la forma de efectuar ciertas modificaciones.
- *No discriminación para grupos o personas:* La licencia no considera distinción alguna para ningún tipo de persona o grupo.
- *No discriminación para actividad o propósito:* Es decir, no se distingue entre uso comercial, doméstico, educativo, etc.
- *Distribución de la licencia:* La licencia afectará a las sucesivas distribuciones de los programas de forma automática sin necesidad de trámite alguno.
- *La licencia no debe contaminar otros programas:* La licencia no debe imponer restricción alguna a otros programas. Por ejemplo, no sería admisible obligar a que el programa sólo se pueda redistribuir en un medio que no contenga software comercial.
- *Ejemplos de licencias libres:* GPL, BSD y Artistic.

Cada licencia tiene sus peculiaridades. Por ejemplo, si se desarrollan aplicaciones haciendo uso de fuentes protegidas bajo la licencia GPL, se estará asumiendo para todo el desarrollo la condición de GPL. En cambio se podría desarrollar software propietario derivado de fuentes bajo licencia BSD. La GPL se ha hecho muy popular; porque protege el legado del software libre para que continúe como tal.

¿Qué es Linux/GNU?

Quizás el usuario ha leído que Linux significa Linux Is Not UniX, pero en realidad Linux es un núcleo de SO tipo Unix. Su compatibilidad Posix (Portable Operating System Interface, la X de Unix) es alta. El SO se complementa con una serie de aplicaciones desarrolladas por el grupo GNU. Tanto estas aplicaciones como el núcleo, son software libre. GNU/Linux es un SO tipo Unix, Multiusuario, Multitarea, Multiprocesador, Multiplataforma, Multilingüe, nacido en la red de redes Internet.

Unix se originó en los laboratorios Bell AT&T a comienzos de 1970, y el MsDos tomó muchas ideas de este SO, pero sus planteamientos eran mucho más modestos y sólo se intentó implantar imitaciones de unas cuantas buenas ideas de Unix: El sistema en árbol de directorios, la redirección de entrada-salida y la estructura de un comando, por ejemplo. Unix ha mantenido la compatibilidad con versiones anteriores sin ningún problema. Tradicionalmente los SO Unix se han caracterizado por ser poco intuitivos de cara al usuario. Esto está cambiando rápidamente, porque Linux está ofreciendo cada vez entornos más intuitivos para la utilización, como resultado del acercamiento progresivo de Linux hacia el usuario doméstico. De todas formas, existe una barrera de tipo cultural que conviene tener presente, por ejemplo, muchos usuarios hoy en día

saben lo que significa *'format a:*', **a:** es el nombre de una unidad de disquete en MsDos o en Windows, pero en Linux no existen unidades lógicas; en Linux se debería hablar de sistemas de archivos en lugar de unidades lógicas, que es un concepto muy distinto.

Linux es un núcleo de un SO, y para que sea completo hay que acompañarlo de una serie de utilidades, dotarlo de una estructura de directorios, así como de archivos de configuración y scripts para distintas tareas. Todas estas cosas juntas y bien organizadas proporcionan una distribución adecuada. Tomando en cuenta que algunas distribuciones incluyen software propio, otras en cambio sólo incorporan software GPL o similar. Considerando que cada distribución tiene sus propias características que la hacen más o menos adecuada para ciertos usos, uno de los aspectos más importantes de las distribuciones es el sistema de actualización de paquetes que permite actualizar el SO a cada nueva versión, teniendo en cuenta las dependencias entre unos paquetes y otros. En este sentido, las aplicaciones en formato binario pueden funcionar en una distribución, y en cambio no funcionar en otra. Sin embargo, partiendo de las fuentes de una aplicación, casi siempre basta con recompilar la aplicación para obtener un binario que funcione en esa distribución. Esto se debe al uso de librerías dinámicas que pueden variar de una distribución a otra. Para obtener un binario que funcione en cualquier distribución, se puede compilar una aplicación estáticamente, lo cual hace que el ejecutable sea de mayor tamaño. Estos problemas están en vías de solución, ya que las diferentes distribuciones están haciendo esfuerzos de estandarización para que cualquier aplicación pueda funcionar en cualquier distribución de Linux.

Comparación de distribuciones open source

Recomendar una distribución Linux, es como orientar a alguien sobre religión (probablemente se han encontrado con una guerra de opiniones sobre distribuciones). En este caso, las opiniones personales pueden variar, pero los hechos son mucho más difíciles de disputar.

Más aun, si se considera que existen alrededor de 400 distribuciones de Linux, de las cuales se han descontinuado 50 oficialmente, o el sitio web de la distribución (o información del producto) simplemente desapareció, o se puso inactivo (no han liberado una nueva versión hace más de 2 años y sus sitios web no muestran desarrollo en curso); éstas son: Aleader, Antomic, Ares, la Colmena, el Azul, el Punto Azul, BYO, Caldera/SCO, Corel, DemoLinux, Dynasoft, el Águila, Eridani, EvilEntity, Feliz, HP Secure, Immunix, JAMD, JBLinux, Kondara, LASER5, LGIS, LinuxInstall.org, LinuxPPC, LRs, Luminux, Madeinlinux, Merdeka, MUMi, Aseado, N-ix, OEone, el Oso polar, la Oficina Roja, Shabdix, Slackintosh, SmartPeer, los Espectros, la Estampida, la Tormenta, SuperRescue, TrX, Unido, el uOS, Virtual, Virux, Brujería, WinBi y Zeus.

¿Dónde se hace la distribución y en qué está basada?

Con el fin de conocer dónde se hacen las distribuciones, es importante señalar que casi un cuarto de ellas comienzan en EE.UU., pero también son muy activos Alemania, Canadá, Francia y Japón. Así, en Debian, aunque la idea vino de EE.UU., la distribución se ha vuelto un proyecto verdaderamente global, con menos de la mitad de los diseñadores de Debian, localizada en los Estados Unidos. Sin embargo, se debe comprender que la mayoría de las distribuciones son modificaciones de versiones de Red Hat o Debian nada más. En algunos casos, estas distribuciones modificadas pueden justificarse; una distribución que ofrece un sitio que dé apoyo para un mercado e idioma específico, es un buen ejemplo. Algunas distribuciones como Mandrágora, Conectiva y PLD eran originalmente basados en Red Hat, aunque ellos han desarrollado subsecuentemente en las distribuciones sus propios derechos, y hay otras distribuciones basadas en ellos ahora. En cuanto a Suse, se ha señalado que está basado originalmente en una distribución alemana llamada Jurix que ya no se mantiene actualmente.

¿Qué es lo libre de la distribución?

Esto es una parte polémica. La idea inicial era mostrar qué productos son libres en ambos sentidos de la palabra, es decir, libremente disponibles para descargar y libremente disponibles bajo GPL. La primera parte es fácil, una distribución puede descargarse o no, ya que existen distribuciones que tienen los árboles de desarrollo completamente abiertos y alguien fácilmente puede meterse dentro y puede ver lo que está pasando. La segunda parte es más difícil, ya que existen distribuciones que no proporcionan el acceso a la rama de desarrollo, entonces no se puede obtener el código fuente de sus descargas, no permitiendo liberar nada de su propio trabajo bajo GPL.

Popularidad de la distribución

DistroWatch[13] mantiene un ranking de visitas a los sitios de las distribuciones individuales (en el sitio principal, así como en los espejos) y el nivel de popularidad medida diariamente (ver Tabla 3.3).

Distribución	Hit por día
Ubuntu	2718
Suse	1828
Mandriva	1528
Fedora	1260
MEPIS	961
Damn Small	880
Debian	796

Tabla 3.3: Popularidad de las distribuciones

[13] http://distrowatch.com

Descripción de algunas distribuciones

Mandriva

Mandriva Linux (anteriormente Mandrakelinux), es una distribución que ha experimentado un enorme crecimiento de popularidad desde la primera versión en julio de 1998. Los diseñadores tomaron la distribución de Red Hat, cambiaron el escritorio predefinido a KDE y agregaron un instalador de fácil uso; mientras rompían el mito de que Linux es duro instalar. Mandriva Linux ha madurado para volverse una distribución popular entre nuevos usuarios que buscan un sistema operativo alternativo. El desarrollo de Mandriva es completamente abierto y transparente; cuando una nueva versión está entrando en una fase beta, instantáneamente se acepta como la primera beta y se publica. Como intercambio, los usuarios probablemente notarán más “bugs” y quizás menos estabilidad que con otras distribuciones. Muchas personas encuentran este intercambio aceptable en sus escritorios, ellos consiguen el último software y la caída de la aplicación ocasional, es algo con que ellos pueden vivir. El resultado de este tipo de desarrollo es una distribución de Linux muy moderna.

> *Pros:* Las utilidades de configuración son gráficas de fácil uso y las particiones NTFS pueden redimensionarse.
>
> *Contras:* Algunos releases tienen bugs y sólo están disponibles inicialmente a los miembros de MandrivaClub.
>
> Empaquetamiento: urpmi (RPM)
>
> *Descarga:* La instalación por FTP está disponible inmediatamente después de liberar el release y las imágenes ISO después de varias semanas.

Fedora

Fedora está relacionada con el nombre Red Hat, que para muchos personifica a Linux, probablemente la compañía mejor conocida en el ámbito Linux. Fundada en 1995 por Bob Young y Marc Swing, recientemente Red Hat Inc. ha mostrado signos de rentabilidad. Sin embargo, Red Hat 9 es la última versión en productos Linux de Red Hat y se reemplazó por Fedora Core a finales de 2003. Mientras Fedora es patrocinada oficialmente por Red Hat, ésta se desarrolla con la participación de la comunidad, tiene corta vida y sirve principalmente como base de comprobación para Red Hat.

¿Qué tiene de especial Red Hat y Fedora? Pues es una curiosa mezcla de conservar los paquetes estables de las principales versiones, reunidos en base a conocimientos intensivos y desarrollos internos. Los paquetes no son los más modernos; una vez que una versión beta se anuncia, las versiones del paquete están listas, salvo las actualizaciones de seguridad. El resultado es una prueba extensiva y la distribución es estable. Esto ha permitido que Red Hat tenga

éxito, convirtiéndose en una distribución de Linux dominante en los servidores alrededor del mundo.

Otra razón para el éxito de Red Hat, es la variedad de servicios populares ofrecidos por la compañía. Los paquetes de software son fáciles de poner al día vía red de Red Hat, un libre almacén de software y valiosa información. Un inmenso rango de servicios está disponible. Existe la seguridad de un apoyo excelente por el personal de soporte muy experimentado. La compañía ha desarrollado un programa de certificación, el RHCE (Red Hat Certified Engineer) y los exámenes están ahora disponibles en la mayoría de las partes del mundo.

Como se señaló anteriormente, es actualmente la distribución más ampliamente difundida (aunque eso no significa que sea la mejor), debido a que ofrece un entorno amigable que facilita la instalación e incorpora software propietario de gran calidad. El sistema de paquetes 'RPM' es muy bueno, y actualmente es utilizado por un gran número de distribuciones.

Pros: Ampliamente usado, apoyo excelente de la comunidad.

Contras: Corta vida del producto, pobre apoyo multimedia, transición de Red Hat a Fedora.

Empaquetamiento: RPM.

Descarga: Gratuita.

Suse

Suse es una distribución comercial alemana que ha tenido un crecimiento espectacular. Ofrece un entorno muy amigable que facilita mucho la instalación; seguramente es la más fácil de instalar y de mantener. Tiene capacidad de auto detección de hardware, incorpora abundante software propietario de gran calidad. En general, se puede decir que es muy completa y muy recomendable para cualquiera que no tenga muchos conocimientos de Linux.

Suse es otra compañía con el enfoque de escritorio. La distribución ha recibido las revisiones positivas para el instalador y la configuración de YaST, desarrollado por los propios diseñadores de Suse. La documentación que viene con el producto embalado, ha sido etiquetada como la más completa. La distribución ha logrado una porción del mercado sustancial en Europa y América del Norte, pero no se comercializa en Asia y otras partes del mundo. Suse fue adquirido por Novell en el 2003.

El desarrollo de Suse está completamente a puertas cerradas y ninguna versión beta pública se mantiene en prueba. La compañía tiene una política de no constituir el software disponible libre hasta 1 ó 2 meses después de que las versiones están en las tiendas.

Pros: Atención profesional al detalle, herramientas de configuración YaST fácil de usar.

Contras: Disponible sólo a través de revendedores del software o por FTP normalmente 1 a 3 meses después del release.

Empaquetamiento: YaST (RPM).

Descarga: Históricamente, Suse no proporcionó las imágenes de ISO para descargar, pero esto ha cambiado con la versión 9.1. La edición Profesional de Suse Linux está disponible para la instalación vía FTP.

Debian

Debian GNU/Linux comenzó en 1993. Es un proyecto completamente no comercial, quizás el más puro formulario de los ideales que empezaron el movimiento del software libre. Cientos de diseñadores voluntarios del mundo contribuyen al proyecto que se maneja bien y de forma estricta, asegurando una distribución de calidad conocido como Debian.

Existen tres ramas durante el proceso de desarrollo: “stable”, “testing” y “instable”. Cuando una nueva versión de un paquete aparece, se pone en la rama inestable para comprobación; si pasa, el paquete se mueve a la rama de la comprobación donde sufre pruebas rigurosas que duran muchos meses. Esta rama se declara sólo estable después de una comprobación muy completa. Como resultado de esto, la distribución es posiblemente la más estable y fiable; aunque no la más moderna. Mientras la rama estable es perfecta para el uso en la misión de los servidores críticos, muchos usuarios prefieren ejecutar la comprobación más moderna o las ramas inestables en sus computadoras personales.

Debian tiene mala reputación por ser difícil de instalar, a menos que el usuario tenga conocimiento íntimo sobre el hardware de la computadora. Compensando este fracaso, tiene “apt-get” y “aptitude”, un instalador conveniente para los paquetes de Debian. Muchos usuarios sólo lo necesitan una vez; en cuanto Debian está en marcha, todas las actualizaciones futuras de cualquier tipo pueden lograrse vía la utilidad apt-get (o aptitude).

Debian es una distribución totalmente libre, desarrollada por un grupo muy numeroso de colaboradores en el más puro espíritu de Linux. La calidad es extraordinaria, se trata de una distribución muy seria que trabaja por el placer de hacer las cosas bien hechas, sin presiones comerciales de ningún tipo; pero que resulta más adecuada para usuarios con conocimientos previos, ya que el grado de facilidad de uso en especial para los novatos deja bastante que desear si se compara con algunas distribuciones comerciales. Los usuarios típicos de Debian son aquellos que tienen como mínimo algún conocimiento técnico y que tampoco tienen reparos a la hora de investigar un poco las cosas. El idioma sobre el cual trabaja es el inglés y el grupo con el cual se coordina Debian; por ejemplo, los bugs deben ser reportados en inglés. También se

caracteriza por la seguridad y la rapidez en la detección y corrección de errores, siendo éstos sus puntos fuertes. Asimismo, soporta un enorme número de paquetes; es una distribución tremendamente flexible y el sistema de mantenimiento de paquetes 'dpkg' es de mucha utilidad:

Pros: 100% libre, excelente sitio web y recursos de la comunidad, bien probado, instalación del software con apt-get.

Contras: El instalador arcaico, la versión estable tiende a estar obsoleta.

Empaquetamiento: APT (DEB).

Descarga: Gratuita.

Ubuntu

Ubuntu ha atacado el escenario de distribuciones Linux como ningún otro. Primeramente, parece haber observado todas las otras distribuciones, aprender de sus errores y combinar los mejores rasgos en un producto superior. Acelerando el ciclo de release, con mirror actualizados, gran cantidad de documentación, incluso los CD libres y de fácil obtención en cualquier parte del mundo. El proyecto es consolidado por Mark Shuttleworth, empresario surafricano, quien hizo una fortuna cuando vendió su compañía Thawte Consulting a Verisign, en US$575 millones a finales de 1999. Él también fundó varias iniciativas de fuentes educativas y abiertas alrededor de Suráfrica, incluyendo Go Open Source.

En cuanto al aspecto técnico, Ubuntu está basado en Debian Sid (la rama inestable), pero con los paquetes más modernos. La distribución se diseña para ser usada en los escritorios y servidores, con un camino de actualización apoyado de Debian 3.0 (Woody). Uno de sus rasgos más interesantes, es el hecho que la cuenta de administrador (root) es por defecto inválida; al primer usuario registrado después de la instalación, se le conceden los privilegios del administrador a través del orden “sudo”. Esta medida podría parecer una molestia al principio, pero debe ser tomada en cuenta ya que anima las buenas prácticas de seguridad.

Pros: La gran comunidad de diseñadores y usuarios; el ciclo del release y período de apoyo.

Contras: Los apoyadores de Ubuntu no han construido un modelo comercial viable todavía alrededor de la distribución.

Empaquetamiento: APT (DEB).

Descarga: Gratuita.

Knoppix

Knoppix es desarrollado por Klaus Knopper, en Alemania. Se puede asegurar que Knoppix, basado en Debian, ha levantado la barra de normas a un nuevo nivel; sobre todo con el descubrimiento del hardware automático que la hace

envidiable, igualmente por la sencillez, la selección enorme del software, la técnica de descompresión rápida y la habilidad de instalarlo en un disco duro. Esto ha convertido a Knoppix en una herramienta indispensable. También puede usarse como disco de emergencia, como una herramienta para demostrar Linux a aquellos que no lo han visto, o como una herramienta para probar una nueva computadora antes de la compra. Incluso puede usarse como una distribución de Linux para las tareas del cada día.

Pros: El autodescubrimiento del hardware es excelente, corre directamente del CD sin la instalación del disco duro. Puede usarse como una herramienta de recuperación.

Contras: El bajo rendimiento si se ejecuta desde el CD.

Empaquetamiento: APT (DEB).

Descarga: Gratuita.

FreeBSD

Aunque BSD (un descendiente directo de Unix) no es Linux, los dos sistemas operativos tienen mucho en común: ellos son libres, en ambos sentidos de la palabra; usan muchas de las mismas aplicaciones de fuentes abiertas.

FreeBSD tiene una historia larga y turbulenta, que data antes de la versión 1.0, que se liberó en noviembre de 1993. El proceso de desarrollo tiene lugar en dos ramas coexistentes: estable (la rama de la producción) y actual (la nueva rama de tecnología); éstos pueden compararse aproximadamente al estable de Debian y las ramas inestables.

Aunque FreeBSD tiene una reputación bien merecida, por el alto rendimiento y estabilidad, puede usarse como un sistema del escritorio, así como de servidor. La instalación no es difícil en comparación con la instalación de Slackware Linux. Si se viene del mundo de Linux, será agradable saber que la inmensa mayoría de aplicaciones de fuentes abiertas ya se las ha venido conociendo y disfrutando (por ejemplo XFree86, KDE, el GNOME, Apache, e incluso algún software no libre, como el driver NVIDIA o el navegador Ópera) y también trabajan en FreeBSD.

Pros: Es rápido y muy estable; tiene documentación excelente y la disponibilidad de puertos por compilar las aplicaciones del software localmente.

Contras: Tiende a estar detrás de Linux, cuando necesita soporte para nuevo hardware, tiene la disponibilidad limitada de aplicaciones comerciales.

Empaquetamiento: Los paquetes binarios y los fuente (TBZ).

Descarga: Gratuita.

Análisis de la escogencia de la distribución

Quizás las razones por las cuales se seleccionó el sistema operativo base, se deba más a la facilidad de implementación de los MTAs a evaluar que a otros aspectos.

La evaluación se hará sobre un servidor de tecnología media, esto hace que no requieran drivers de última generación; por lo tanto, cualquier escogencia de SO podrá manipular el conjunto de dispositivos del que está compuesto el equipo. Cabe destacar que a la hora de la implementación pueda descartarse la selección, debido a la tecnología escogida.

En el proceso de evaluación e inclusive en el supuesto proceso de producción, este servidor deberá prestar sólo el servicio de correo y ningún otro, lo que hace que se eliminen los paquetes adicionales innecesarios, rompiendo con algunas entradas en el esquema de comparación.

Para brindar la continuidad operativa de un servicio crítico como éste, se hace hincapié en la robustez del soporte técnico del sistema operativo y afines.

Es posible que la facilidad de implementación no sea el criterio de mayor relevancia en la comparación, por lo que no se recomienda usar una distribución por el facilismo de la instalación, antes es preferible ahondar más a la hora de configurar bajo un sistema operativo con mejores cualidades.

Por otra parte, se debe mantener alejado de las distribuciones que apuntan a alianzas con monopolios; ya que, es muy probable que dentro de poco, por razones comerciales, ya no estén en su totalidad con el GNU.

Si la confianza en la distribución es tal, no se requiere modificar o auditar el código fuente; y no hay por qué preocuparse por obtener el mismo. Por el contrario, antes de cualquier elección, el usuario debe ubicar el código fuente del sistema operativo y los paquetes que se instalen.

Por consiguiente, tomando en consideración los análisis efectuados anteriormente sobre las principales distribuciones, Debian ha sido seleccionado como la distribución que mejor se adapta a los requerimientos actuales y potencialmente reales. A tal efecto, de ahora en adelante se utilizará esta distribución como herramienta de apoyo.

3.4.2 Servidor de correo

Se podría decir que el correo electrónico ha sido el padre de Internet; antes incluso de existir el concepto de Red Local, existían en el mundo Unix una serie de utilidades para transferencia de datos entre máquinas a través de modem. Es el venerable y todavía ampliamente usado UUCP (acrónimo de Unix-to-Unix-CoPy). Básicamente, no era sino una serie de utilidades que permitían transferir archivos entre dos máquinas y ordenar la ejecución remota de diversas aplicaciones. En paralelo con estos programas, todos los sistemas incluían una

utilidad para intercambiar mensajes entre los diversos usuarios de un sistema. Esta utilidad se denominaba “mail”.

No tardó mucho en surgir la idea de que los intercambios de mensajes pudieran producirse entre diversas máquinas, aprovechando los programas existentes “mail” y “uucp”. En este momento surgió la necesidad de establecer un mecanismo para saber de dónde venían los mensajes, a dónde iban, cómo y por dónde debían encaminarse. La solución a este problema fue un nuevo programa delivermail que todavía aparece en algunas distribuciones de Unix.

Con la aparición de ARPANet y las primeras redes locales, la complejidad del sistema de correo, del encaminamiento y los problemas añadidos de gestión de listas, modos de conexión entre máquinas y diferentes sistemas “Unix”, hacen que delivermail crezca en complejidad. Finalmente, en 1980 se publican los primeros tópicos sobre lo que será la futura Internet y aparece el primer RFC sobre un protocolo específico para transferencia de correo electrónico: el SMTP (Simple Mail Transfer Protocol).

Esto es el comienzo de la aparición de los servidores de correo basados en SMTP, que da pie a toda la gamma de componentes que hoy día sirven como herramientas en tan preciado servicio.

Sendmail

Reseña

Sendmail es un programa de distribución gratuita, creado y actualmente revisado por Eric Allman; es uno de los programas de transporte de correo más utilizados y que mejor se integran en sistemas Unix. La legendaria reputación de que sendmail es difícil de comprender, duro de configurar y plagado de agujeros de seguridad se está quedando poco a poco en leyenda. Sendmail posee un archivo de configuración /etc/sendmail.cf, de sintaxis casi críptica, pensado para un rápido procesamiento por el programa, no por el usuario. Diversas utilidades de configuración mediante macros facilitan al administrador del sistema la tarea de configurar. Aunque actúa principalmente como MTA, también puede ser utilizado como MUA [13], aunque no posee interfaz de usuario.

Funciones

Como agente de usuario, sendmail lee por defecto de la entrada estándar hasta encontrar un EOF o una línea que contenga únicamente un punto (“.”). En ese momento manda una copia de ese mensaje a cada una las direcciones destino (que se le habrán pasado previamente en la línea de comandos). Él mismo determinará la ruta a seguir (consultando el DNS si fuera necesario), basándose en el contenido de la dirección destinataria.

La utilización de Sendmail como demonio en el sistema permite enviar y recibir correo SMTP. Para ello, sendmail se queda como proceso residente

escuchando el puerto 25, admitiendo y realizando conexiones SMTP cuando sea necesario (es decir, actúa como un Agente de Transporte de Correo). Cuando reciba una petición de conexión, creará un proceso hijo que se encargará de ello, mientras el proceso padre seguirá escuchando el puerto 25.

Cuando el envío de un e-mail no puede alcanzar su destino, porque rechazan la conexión, este debe ser almacenado en una cola de la máquina que manda el e-mail, para intentar de nuevo el envío más tarde. Para procesar la cola de correo, se utiliza el comando: sendmail –q <tiempo>, que procesa la cola de correo cada cierto tiempo.

El uso de alias en sendmail permite: tener nombres alternativos (nicknames) para usuarios individuales, envío de correo a otras máquinas, aunque la dirección sea local.

Qmail

Reseña

El Qmail fue desarrollado por Dan Bernstein, un profesor de matemáticas de la University of Illinois en Chicago. El Dr. Bernstein es bien conocido por el trabajo en el campo de la criptografía. El primer lanzamiento público de Qmail, versión beta 0.70, tuvo lugar el 24 de enero de 1996. La primera versión gamma, 0.90, se lanzó el 1 de agosto de 1996. La versión 1.0, el primer lanzamiento general, se anunció el 20 de febrero de 1997.

Funciones

- Adaptación automática a la variante de Unix: no es necesario trasladar la aplicación.
- Configuración automática para cada máquina.
- Reducción al mínimo del código que se ejecuta con setuid y como root.
- División en cinco sistemas de confianza: seguridad en profundidad.
- Registro opcional de hash unívoca para cada mensaje, del contenido completo del mensaje.
- Cumple con los RFC 821, RFC 1123, RFC 1651, RFC 1652 y RFC 1854.
- Transmite mensajes con codificación 8-bit.
- Retransmisión y reescritura de mensajes para clientes autorizados.
- Tratamiento instantáneo de los mensajes que se agregan a la cola.
- División del directorio de la cola (no hay ralentización cuando la cola aumenta).
- Limpieza automática de colas de correo.
- Alta capacidad de nombres para la máquina local y dominios virtuales.
- La transmisión a un servidor que no responde se detiene o acelera automáticamente.
- Encaminamiento artificial: smarthost, localnet, mailertable.
- Programa de entrega de correo controlado por el usuario: Procmail.

Paquetes relacionados

Qmail sigue la filosofía clásica de Unix, cada programa debe llevar a cabo una función sencilla y bien definida. Las funciones complejas deben construirse a partir de una cadena de funciones simples, realizadas por programas individuales y enlazadas en una «tubería» o *pipe* que las redirecciona. La alternativa es construir herramientas cada vez más complejas que reinventan casi toda la funcionalidad de las herramientas más sencillas.

No es sorprendente que Qmail en sí, no haga algunas de las cosas que a todos les gustaría que hiciese. En ese momento entran en juego algunos de los complementos escritos para Qmail. Por supuesto, muchas de las herramientas estándar Unix pueden actuar como módulos de Qmail.

Licencia

El copyright de Qmail pertenece a su autor, Dan Bernstein, y no se distribuye con una declaración de derechos del usuario. Se puede usar Qmail con cualquier finalidad, y puede redistribuir libremente distribuciones de código fuente de Qmail, pero sin modificaciones; puede certificar distribuciones binarias var-qmail, y puede redistribuir parches para Qmail. Pero no puede distribuir código fuente de qmail modificado o distribuciones de binarios que no sean var-qmail.

Debido a la restrictiva licencia de qmail con respecto a la distribución de paquetes precompilados, Qmail se instala generalmente a partir de una distribución del código fuente.

Postfix

Reseña

Postfix es un agente de transporte de correo electrónico bastante reciente que se suma a la lista de alternativas de MTAs. En el diseño, tienen mucha prioridad factores como la seguridad, la eficiencia, la facilidad de configuración y administración, junto con la compatibilidad con otros sistemas de correo.

Siendo el correo electrónico hoy día una herramienta de trabajo vital en multitud de entornos de trabajo, sustituir los sistemas actuales por otro nuevo es una decisión muy delicada. Se debe garantizar que la migración se va a producir sin inconvenientes para los usuarios, y con el mínimo tiempo de parada del servicio. Con Postfix, esto es fácil de conseguir.

Wietse Venema, diseñador de la herramienta, es un programador respetado como pocos. Autor de programas tan conocidos como los TCP Wrappers, SATAN, The Coroner Toolkit, sus versiones de portmap y rpcbind, es un experto en seguridad informática [9].

Por último, pero no menos importante, hay que decir que el código fuente de Postfix (por supuesto de dominio público) es un ejemplo de diseño, claridad y

documentación, lo cual facilita el mantenimiento, así como la incorporación de nuevas capacidades, corrección de errores, etc.

Funciones

Diseño modular

El sistema Postfix está compuesto de varios procesos que se comunican entre sí, aparte de varias utilidades que puede usar el administrador para influir en el sistema u obtener información de él. Este diseño, junto con el archivo *master.cf* que permite configurarlos, tiene algunas ventajas.

Cada proceso se ejecuta con los mínimos permisos necesarios para realizar la tarea. Se puede activar la emisión de más información de depuración, de forma independiente para cada programa. Esto es realmente útil para resolver problemas. Se pueden insertar procesos externos entre ciertas partes del sistema, lo cual es muy útil para antivirus, filtrados, etc.

Por ejemplo, se puede lanzar un servidor SMTPD adicional en otro puerto o sobre otra IP, con distintas opciones de configuración de acceso.

Seguridad

Seguridad frente a ataques contra el servidor, y también contra el uso inadecuado. Postfix soporta directamente el uso de listas negras, es relativamente difícil configurarlo como relay abierto. Si se juega mucho con las opciones de restricciones de acceso, hay que tener cuidado con las que se ponen y en qué orden. Se puede acabar dejando puertas abiertas, o por el contrario tener un "*bunker*" inutilizable. Afortunadamente, este tipo de opciones tienen nombres muy descriptivos y están bien documentadas, por lo que es fácil hacerlo bien. Se puede instalar Postfix de forma que corra en modo 'chroot', lo que proporciona aún más seguridad.

Configuración

La facilidad de configuración de Postfix, es quizá el factor que más atrae a muchos administradores. Cuando se conoce un poco, no sólo es sencillo escribir un archivo de configuración para casi cualquier situación (máquinas 'dial-up', servidores centrales, relays, etc.). Más aún, a la vista de una configuración que se presente es igual de fácil entender el funcionamiento que se pretende con ella. Existen multitud de parámetros que se pueden cambiar (todos ellos con nombres coherentes a su función), pero la inmensa mayoría sólo hay que modificarlos en casos excepcionales. De hecho, la práctica habitual cuando se solicita ayuda, es aportar simplemente la salida del comando *'postconf -n'* que da en unas pocas líneas los parámetros de configuración a los que el administrador ha asignado valores distintos de los que tienen por defecto.

Restricciones de acceso

Postfix, recién instalado (definiendo el valor de mydomain) aceptaría un mensaje, si el cliente de la conexión SMTP tiene una IP perteneciente a la misma subred que el servidor, sea cual sea el destino del mensaje.

El mensaje se acepta, si es que la dirección de destino del mensaje (RCPT TO) es de la misma máquina (user@$myhostname o user). En caso contrario se rechaza. Siendo la principal idea de que por defecto Postfix aceptará correo de máquinas en las que confía o que vaya dirigido a direcciones de determinados dominios permitidos o dirigidos a direcciones de mydestination.

Filtrado por contenido

Todas estas comprobaciones las hace el servidor SMTPD, antes de pasar a la fase DATA del protocolo. Si se decide rechazar el mensaje, se hace en este punto. Si se permite pasar a la fase DATA, aún se puede hacer otras comprobaciones cuando se termina de recibir el mensaje, y antes de aceptarlo. Si se pasan todas las pruebas, el mensaje es depositado por el servidor SMTPD en una cola de Postfix. Aún existe otra forma de inspeccionarlo antes de la entrega, mediante el mecanismo de 'filtrado de contenido', que se puede usar para pasar un antivirus. La idea es que los mensajes se pueden enviar a un proceso externo antes de ser entregados, y éste permitir el envío (reinyectándoselo a Postfix, por lo que puede incluso modificar el mensaje) o denegar su entrega, pudiendo en este caso enviar un mensaje de error al remitente.

Manipulación de direcciones

Postfix no tiene un lenguaje de reescritura de direcciones. En lugar de esto, se procede a pasar por una serie de fases gobernadas por tablas, un mecanismo que tiene mucha potencia. Una vez que un mensaje ha pasado los controles del servidor SMTPD o ha sido enviado localmente, las direcciones de origen y destino son asignadas y adaptadas a la forma cualificada (ver Figura 3.4).

```
usuario          -> usuario@$myorigin
usuario@maquina -> usuario@maquina.$mydomain
```

Figura 3.4: Modificación de direcciones

Ahora ya están todas las direcciones en un formato adecuado. Antes de decidir cómo hay que entregar el mensaje, éste pasa por varias fases. El siguiente paso consiste en aplicar las tablas canónicas, si se han definido. Estas tablas definen la reescritura de direcciones en las cabeceras, existiendo para ello tres (3) posibilidades (ver Figura 3.5):

```
sender_canonical_maps
recipient_canonical_maps
canonical_maps
```

Figura 3.5: Posibilidades de reescritura de direcciones

Asimismo, estas tablas se usan para convertir direcciones con nombres de usuarios internos al tipo nombre.apellido, o para adaptar direcciones de sistemas de correo propietarios.

Además, hay que tener en cuenta algunos aspectos al usar estas tablas:

Si se modifican las direcciones destino y éste es local, habrá que definir un mecanismo para que el correo pueda ser entregado a la cuenta adecuada.

Si se modifican las direcciones origen, se puede decir lo mismo para el caso de las posibles respuestas al mensaje.

La tabla *aliases* es normalmente la mejor forma para convertir de nuevo las direcciones tipo nombre.apellido a cuentas locales reales.

Tras la aplicación de las tablas canónicas, viene el enmascaramiento de nombres de máquinas. Esto se aplica a todas las direcciones excepto a la de destino. Se trata de ocultar detalles internos, sin afectar al enrutamiento del correo (ver Figura 3.6).

```
masquerade_domains      ¿Qué nombres de dominio enmascarar?
masquerade_exceptions   ¿Cuentas que no se enmascaran (root, etc)?
masquerade_classes      ¿Direcciones que se enmascaran?
```

Figura 3.6: Parámetros

El orden de los valores del primer parámetro es importante. Para cada dirección a la que se va a aplicar el enmascaramiento se recorre la lista de valores de *masquerade_domains* y lo compara con el dominio de la dirección. Cuando uno de estos valores coincide con la parte final del dominio de la dirección, se elimina lo que pueda haber a la izquierda y se detiene el proceso.

A continuación se aplica la tabla virtual, si se ha definido. Esta tabla es un poco especial, en el sentido de que el servidor SMTPD también la consulta para aceptar correo destinado a direcciones declaradas en ella. El sentido principal de esta tabla, es que nuestro sistema pueda aceptar correo destinado a direcciones que no aparentan ser de nuestro dominio, como es típico en el caso de un ISP que recoge correo para los dominios que alberga, de ahí su nombre.

Enrutamiento del correo

Una vez aplicados todos los pasos anteriores, el mensaje queda en su forma definitiva. Ahora hay que decidir a dónde mandarlo. ¿Es para un buzón local? ¿Hay que enviarlo a otra máquina? Lo primero que se hace ahora es consultar otra tabla; en este caso la *transport*. Aquí, se busca el dominio de la dirección destino. Si está definido, el resultado de la consulta debe ser un par *agente de transporte: destino,* donde uno de los dos es opcional. Si no se pone el agente, se asume smtp. Si no se pone el segundo, se asume el dominio destino. El *agente de* transporte debe estar definido en el archivo *master.cf.*

Un caso típico del uso de transport es cuando se filtra la entrada de correo en el cortafuego, de forma que una sola máquina reciba correo para toda una

organización. Si debe recibir el correo dirigido a las máquinas internas, será el MX de éstas, y se configura para que lo acepte (mediante relay_domains). Pero a la hora de entregarlo a la máquina final, Postfix siempre busca el MX de la dirección destino, que es nuestra propia máquina, lo que crearía un bucle. Para ello se debe especificar en transport que el correo va directamente a esas máquinas.

Entrega local

Este es el caso cuando el dominio de la dirección destino se encontró en la tabla transport con resultado local o no se encontró pero se considera local según el método descrito arriba. Ahora se usa el transporte definido en la variable local_transport, que por defecto vale local, que indica el propio agente de entrega local de Postfix. Otros transportes para entrega local son lmtp o virtual (este último es distinto de la tabla del mismo nombre, aunque tiene relación), o incluso software externo, como Cyrus.

Si se usa el transporte local (y sólo si se usa éste), se consulta la tabla de aliases y el archivo *.forward*. Si éstos no indican que haya que redirigir el mensaje, éste se entrega al transporte definido en *mailbox_transport*, que puede ser lmtp, cyrus, etc. Si ese parámetro no está definido (por defecto no lo está) lo normal es añadir el mensaje al buzón de entrada del usuario (típicamente /var/mail/usuario). Pero esta conducta se puede cambiar mediante unos parámetros (ver Tabla 3.4):

Parámetro	Descripción
`mailbox_command`	Un comando externo que se encargue de eso. Típicamente Procmail.
`mailbox_command_maps`	Lo mismo que el anterior pero con mapas que permiten indicar programas diferentes para cada cuenta. Este parámetro tiene mayor precedencia que el anterior.
`home_mailbox`	Se mira si no está definido el anterior. Es el archivo relativo al directorio HOME del usuario donde añadir el mensaje. Si termina por el carácter '/' eso indica que se use el formato Maildir, originario de qmail.

Tabla 3.4: Ejemplos de parámetros para entrega local

Para cuentas de correo, que no se corresponden con cuentas reales en el sistema, se puede usar software externo, definiendo el correspondiente transporte en el archivo *master.cf* (como en el caso de cyrus) o usar el transporte virtual que proporciona el propio Postfix. Existen otra serie de parámetros (fallback_transport, luser_relay) para tratar los casos de correo dirigido a usuarios inexistentes, aunque, también es posible que no llegue a darse este caso configurando el servidor para que sólo acepte correo dirigido a

usuarios válidos; lo que evita el correspondiente mensaje de rebote. Para eso se usa el parámetro local_recipient_maps.

Entrega remota

Este es el caso si la entrega no es local. Si el dominio de la dirección se encontró en la tabla transport, se usa el transporte indicado en dicha tabla. En caso contrario, si tiene valor el parámetro relayhost, el mail se entrega a esa máquina; si no, se busca en DNS el MX para el dominio de la dirección destino y se entrega a él. Si no existe MX, se entrega a la máquina destino.

El transporte por defecto (default_transport) y el que se usará prácticamente siempre, es SMTP, pudiéndose definir en el archivo master.cf otros transportes que sean SMTP, pero que usen otro puerto, o limitados en cuanto al número de envíos simultáneos, la frecuencia con que se arranca el proceso, etc.

Otro transporte interesante es LMTP. Aunque se usa para entrega local, los buzones pueden estar en la misma máquina donde se ejecuta Postfix o en una distinta. En el primer caso, la comunicación entre Postfix y el servidor LMTP (como Cyrus) puede ser por sockets Unix o TCP. En el segundo caso, será por TCP.

Direcciones virtuales

Postfix tiene un soporte excelente para dominios y/o direcciones virtuales. El uso típico de esta característica, es aceptar correo para direcciones que aparentemente no corresponden a nuestro servidor. Por ejemplo, el servidor de correo de un ISP, mailhost.isp.com debe aceptar correo para direcciones de todos los dominios a los que da servicio. Una universidad puede haber registrado un dominio específico para algún proyecto de investigación, sea proyecto.org y habrá colocado como MX de ese dominio al servidor de correo de la universidad. Éste debe recibir correo dirigido a ese dominio, sea para entregarlo a una cuenta local o para redirigirlo a un servidor interno.

La forma de configurar esto en Postfix es muy sencilla, basta con uno o varios archivos que se declaran con la directiva virtual_maps. Este archivo, como todos los que se usan en Postfix, consta de líneas con dos partes: una con la que emparejar la dirección (en este caso la del 'envelope recipient') y otra con la dirección resultado; es decir, a donde hay que enviar el mensaje. Este archivo es un poco especial porque no sólo se consulta a la hora de decidir dónde enviar un mensaje que ya se ha aceptado, sino que el propio servidor SMTPD lo consulta para saber que debe aceptar el correo dirigido a esas direcciones. Esta comprobación se hará siempre que en las restricciones de acceso se encuentren las reglas: check_relay_domains, permit_auth_destination o reject_unauth_destination.

Selección del MTA

Por su parte, la selección del MTA es muy parecida a la escogencia de la distribución de Linux a utilizar. Siendo el postfix, el que ofreció más ventajas a la hora de compilar e instalar, por varias razones:

- Puede ser un reemplazo parcial o total de sendmail, o cualquier otro MTA.
- El compilarlo es relativamente simple.
- La integración con el sistema es rápida y sólo requiere que se agregue un usuario y un grupo.
- La configuración se hace en un solo archivo de texto bastante explícito.

Básicamente la sencillez y facilidad de instalación y configuración, colocan a este MTA en una posición ventajosa a la hora de escoger una solución que cumpla con el decreto 3390 [6].

3.4.3 Herramientas antispam

Las herramientas Antispam encontradas y que están basadas en software de dominio público son pocas. Sin menospreciar sus bondades se exponen sus atributos y funcionamiento.

¿Qué es Procmail y para que sirve?

Procmail es un procesador de correo autónomo que se ejecutará al producirse la llegada de un nuevo mensaje. En ese momento Procmail será llamado automáticamente gracias al archivo *.forward* o a través del MTA, de tal modo que leerá el correo de la entrada estándar y abrirá el archivo *.procmailrc* que le indicará qué debe hacer con ese correo, en función de una serie de reglas previamente configuradas [12].

Las reglas de Procmail se ejecutan en función del mensaje en sí (tanto la cabecera como el cuerpo del mismo), y permitirán eliminar el spam (si no todo, al menos gran parte de él). Además, permite repartir los mensajes entre los diferentes usuarios de correo, pudiendo tener una sola dirección e-mail para todos los usuarios, pero utilizando algún campo especial para identificar a cada uno. También, se puede separar el correo de las listas de correo o por categorías, preparar auto-respuestas y muchas otras opciones.

Funcionamiento

Existen dos maneras de instalar Procmail. La primera de ellas es que sea utilizado por el MTA a la hora del reparto del correo, y la otra forma se realiza mediante un archivo de configuración de nombre *.forward* que contendrá la llamada a Procmail de forma que éste se ejecute a la llegada de nuevos mensajes al buzón del usuario.

Cuando es llamado de cualquiera de las dos formas, Procmail lee el mensaje de correo desde la entrada estándar. A continuación, abre y lee el archivo *.procmailrc*, examina las reglas contenidas en dicho archivo y decide el destino del mensaje (que puede ser devuelto, enviado a un usuario en concreto, auto respondido, borrado, etc.). Si el archivo *.procmailrc* no existe, el mensaje es depositado en el buzón habitual del usuario.

El conjunto de reglas de *.procmailrc* suelen ser de comprobación y búsqueda de cadenas de texto en el From (dirección de origen), Subject (tema del mensaje), Body (cuerpo del mensaje), así como en el resto de cabeceras del mismo. Como sencillo ejemplo, es posible especificarle al MTA que si en el cuerpo del mensaje se encuentran las palabras «gane» y «dinero» o similares, elimine el correo (probablemente se trate de un correo spam o correo basura), o que si en el Subject encuentra las palabras «clave» y «PGP», debe enviar al remitente de ese mensaje un texto con la clave PGP.

Configuración y ejemplo

En la Figura 3.7 se observa un ejemplo de *.procmailrc* antes de comentar las diferentes reglas que pueden usarse, así se puede analizar la manera de indicar a Procmail las acciones a realizar con cada tipo de mensaje:

```
MAILDIR=$/var/spool/mail
DEFAULT=$MAILDIR/juan
LOGFILE=$MAILDIR/log

:0:
* ^From.*juan
/home/juan/Mail/mensajes_juan

:0:
* ^From.*Josema
!jefe@de.josema

:0:
* ^From.*lista_de_correo@lista.com
/home/juan/Mail/lista_correo_1

:0
* ^Subject:.*prueba
/dev/null
```

Figura 3.7: Ejemplo de .procmailrc

Las tres primeras líneas especifican los directorios de correo (MAILDIR), el archivo de entrada de e-mails por defecto (DEFAULT) y un archivo donde Procmail indicará paso por paso todo lo que ha hecho en cada sesión (LOGFILE). En este sentido, a continuación se definen tres reglas (comenzando todas ellas por :0).

La primera de ellas especifica que todos los mensajes que contengan en la cabecera From la cadena “juan” serán dejados en el archivo *mensajes_juan*. De

esta manera, cuando llegue un e-mail From: juan@ctv.es, o From: juan@arrakis.es, éste será dejado en el archivo *mensajes_juan*.

Si la regla anterior no se cumple (es decir, no aparece la cadena “juan” en el campo From), se pasa a comprobar si se cumple la siguiente regla, que en este caso especifica que todos los mensajes provenientes de josema sean enviados a jefe@de.josema, acción realizada mediante el comando ! (admiración).

La penúltima regla permite separar el correo de una lista de correo a un archivo diferente del correo habitual (para así facilitar la lectura).

La última regla especifica que todos los mensajes que contengan la cadena “prueba” en el asunto (Subject), deben ir a para a /dev/null (algo así como la papelera de Linux). En caso de no cumplirse ninguna de las tres reglas, el mensaje irá a parar al archivo apuntado por $DEFAULT, usualmente /var/spool/mail, de forma que luego puedan ser recogidos por cualquier cliente de correo.

Spamassassin

Es un filtro inteligente del correo basado en scripts de Perl que utiliza una diversa gama de pruebas para identificar el correo basura. Además, spamassassin tiene una arquitectura modular que permite que otras tecnologías sean utilizadas conjuntamente contra el spam. Está diseñado para la fácil integración en cualquier sistema del correo. Spamassassin, es un proyecto de la fundación del software de Apache y se lanza bajo la licencia de Apache.

Funcionamiento

Cada mensaje que llega al servidor es analizado en busca de características comunes a un spam. Se utilizan reglas para comparar con los mensajes de correo en busca de palabras como “Mortgage”, “Viagra” o “Penis Enlargement”. Estas pruebas se aplican a las cabeceras y al contenido del correo para clasificarlo, usando métodos estadísticos avanzados. El resultado de filtrar los mensajes genera un puntaje que si supera determinado valor (5.0 por defecto) [3] es considerado un spam.

Cada vez que el puntaje sea más alto, el correo tiene más probabilidad de ser spam. A puntaje bajo, corresponde casi siempre un mensaje de correo que no es spam. Todo este proceso es añadido al mismo mensaje, en modo que el usuario pueda darse cuenta del por qué un determinado mensaje ha sido identificado como spam. Normalmente marca el mensaje con la cadena ** SPAM ** o [SPAM] en el asunto y explicando en el cuerpo por qué el correo recibido tiene aspecto de spam. El usuario decidirá que hacer con esos correos. Por ejemplo, puede decidir borrarlos directamente a nivel de servidor sin enterarse de su existencia.

Configuración

La configuración de spamassassin puede ser llevada a cabo de manera global o de manera individual, donde cada usuario define reglas de filtrado más estrictas o flexibles.

Cada regla en spamassassin posee un puntaje, valor que en caso de hacer match con dicha norma, es sumado al puntaje total del mensaje. El valor promedio para que un correo electrónico sea considerado spam también es configurable; finalmente, vale mencionar que para efectos prácticos, spamassassin posee puntajes predefinidos para todas sus reglas, que pueden ser modificadas.

FILTER MODE: Con esta configuración el mensaje es analizado; si se identifica como probable spam, se etiqueta en la línea del asunto y se envía al buzón del usuario. De esa manera, el usuario recibirá el mensaje y leyendo el asunto podrá identificar inmediatamente el spam.

DELETE MODE: El mensaje es analizado y si se identifica como probable spam, es eliminado directamente a nivel de servidor; el usuario nunca verá el mensaje. Hay que usar este modo con extremo cuidado porque podría perder mensajes importantes, sobre todo si configura un nivel de puntos muy bajo. Si bien spamassassin es un instrumento muy confiable en el 99% de los casos, no es perfecto y podría interpretar de manera equivocada algunos mensajes. En ese 1% podría estar algún mensaje importante.

REQUIRED POINTS (El umbral o línea de alerta): Los mensajes son analizados y de acuerdo con un par de valores (umbrales) pueden ser marcados como spam o borrados directamente. Por cada una de las más de 100 pruebas que spamassassin realiza para tratar de entender si el mensaje es o no spam, éste asigna un puntaje al mensaje. Siguiendo este concepto, si una vez realizadas todas las pruebas el mensaje pasa el umbral menor, éste será marcado como spam y si pasa el umbral mayor esta será eliminado.

BAYESIAN FILTERING: Habilitando estos filtros que hacen referencia a bases de datos presentes en Internet, spamassassin podrá identificar el spam sobre la base de palabras comunes que se encuentran en los mensajes spam ya identificados anteriormente.

LANGUAGE FILTERING: Con esta útil opción el usuario configura spamassassin para el idioma en que espera recibir los mensajes. De esa manera, cualquier mensaje que le llegue en otro lenguaje será marcado como spam.

Se pueden establecer variantes con las configuraciones anteriores.

3.4.4 Suite de colaboración integral

En poco tiempo, Zimbra se ha convertido en una solución de código abierto líder a nivel mundial tanto para empresas como para proveedores de servicio,

centros educativos y administraciones públicas. La clave de este éxito se basa en el uso de tecnologías de código abierto y protocolos de comunicación e intercambio de datos estándares ya consolidados, que han combinado de manera adecuada y completado con características que no estaban cubiertas pero que son claves para las empresas. Una completa documentación y un amplio abanico de comandos de consola específicos dotan a esta suite de enormes capacidades de integración con entornos existentes.

¿Qué es Zimbra Colaboration Suite?

La suite de colaboración Zimbra (Zimbra Collaboration Suite o ZCS) es un programa informático colaborativo o groupware creado por Zimbra Inc., compañía ubicada en San Mateo, California; posee tanto el componente de servidor como su respectivo cliente. Dos versiones de Zimbra están disponibles: una versión soportada por la comunidad de software de dominio público y una versión soportada comercialmente que contiene algunas mejoras propietarias.

El servidor ZCS expone una interfaz de programación de aplicaciones (API) SOAP para toda su funcionalidad y hace uso de proyectos de terceros como:

- Apache + Tomcat (servidor web).
- Clamav (antivirus).
- Spamassassin + DSpam (filtro de spam).
- Amavis-new (conector entre los antivirus y el servidor de correo).
- JDK (máquina Java).
- MySQL (servidor de base datos).
- OpenLDAP (servidor de directorio).
- Postfix (servidor de correo SMTP).
- Cyrus (servidor de correo POP/IMAP).

El cliente web ZCS es una interfaz de colaboración y administración completa que soporta correos electrónicos y calendarios a través de una impresionante interfaz web Ajax, que provee tips de sus objetos, ítems arrastrables, y menús que se expanden al hacer clic derecho. También incluye capacidades de búsqueda avanzada y permite relacionar fechas (por ejemplo si se arrastra el cursor sobre “mañana a las 6:00 p.m.” el sistema desplegará cualquier cita a esa hora). El calendario compartido en grupo también esta incluido.

ZCS es compatible con clientes propietarios tales como Microsoft Outlook, Novell Evolution y Apple Mail. También provee soporte de sincronización nativo de dos vías para muchos dispositivos móviles (Nokia E-Series, BlackBerry, Windows Mobile, etc).

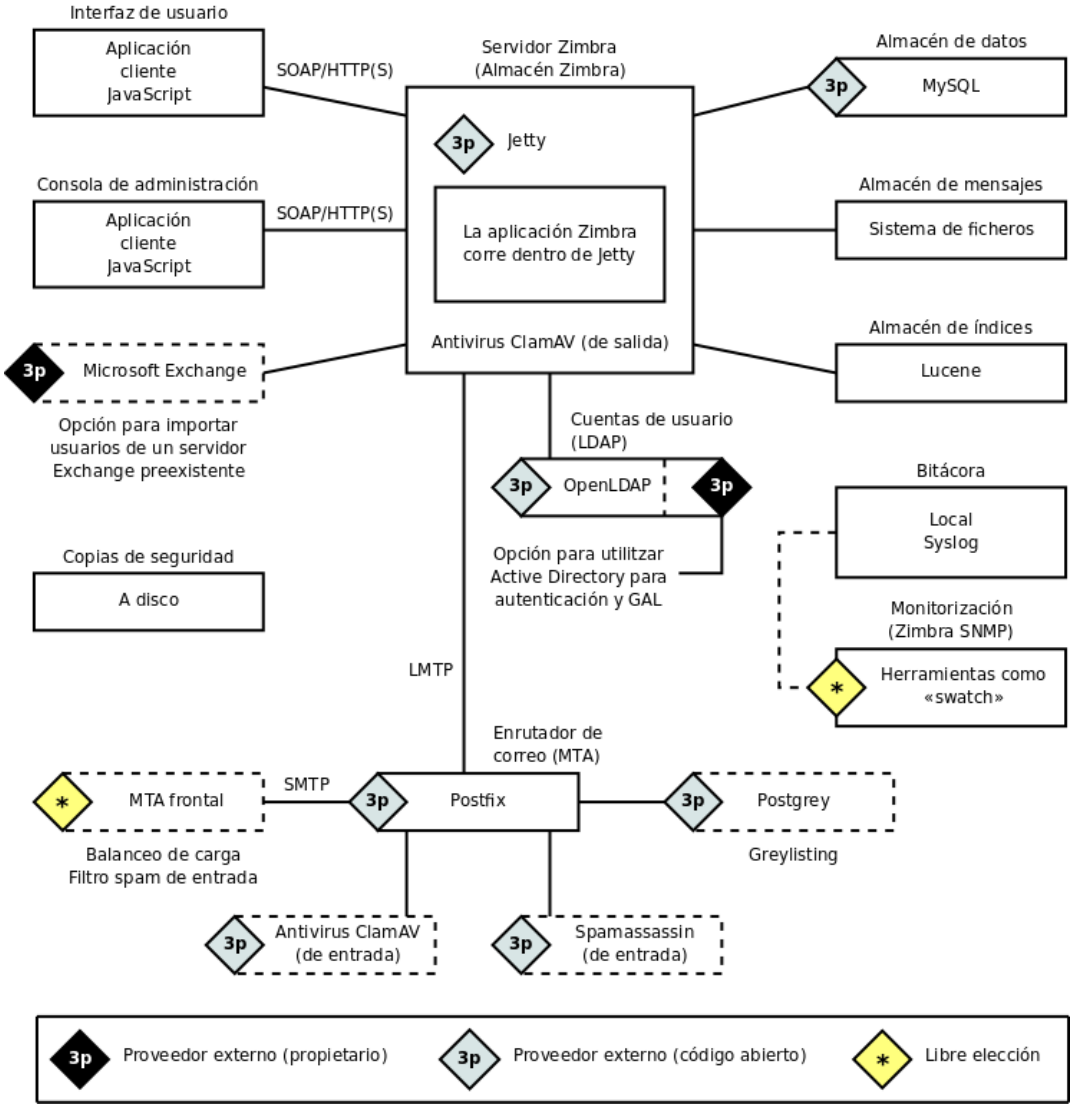

Figura 3.8: Arquitectura de servidor ZCS

Arquitectura

Zimbra está formada por un conjunto de componentes (ver Figura 3.8) que trabajan juntos para formar una solución completa. El núcleo del servidor está escrito en Java, utilizándose Jetty como servidor de aplicaciones.

El MTA (Postfix) enruta los mensajes de correo al servidor de Zimbra. Integrado a través de Postfix, Zimbra incorpora varios filtros de seguridad, como antivirus y antispam, entre otros. Asimismo, el MTA puede integrarse con otras tecnologías, como Postgrey para Greylisting o Spamhaus para DNSBL, u otras soluciones de seguridad comerciales, como los AV/AS de Barracuda Networks. Asimismo, soporta por defecto los protocolos principales de cifrado de canal, SSL y TLS.

Incluido en Zimbra hay diversos almacenes de datos para la información de los usuarios: OpenLDAP [7] proporciona la autenticación, MySQL guarda las preferencias y metadatos de los mensajes y el sistema de archivos guarda directamente los mensajes de correo.

Otro componente integrado en Zimbra es Lucene[14], un potente motor de indexación y búsquedas que permite a los usuarios y administradores buscar mensajes a través de múltiples carpetas de correo, tanto metadatos como contenidos en el cuerpo del mensaje.

Componentes de la arquitectura

La arquitectura del sistema está formada por los varios componentes.

Zimbra Core

Zimbra Core incluye las librerías, utilidades, herramientas de monitorización y archivos básicos de configuración.

Zimbra LDAP

Dada la variedad de servicios y aplicaciones asociadas a los servicios de que se disponen hoy en día, tener un directorio de usuarios basado en LDAP [7] es una necesidad. Zimbra utiliza por defecto OpenLDAP para almacenar y gestionar el almacén de usuarios, integrando el soporte para la replicación. Además, permite fácilmente su configuración para el uso de directorios LDAP externos, incluyendo Active Directory de Microsoft o eDirectory de Novell, entre otros.

Zimbra MTA

Uno de los componentes claves de cualquier solución de mensajería hoy en día el servidor de correo electrónico de Zimbra, que está formado, como es habitual, de diversas partes:

- Un MTA.
- Un almacén de buzones de correo accesible por IMAP4 y POP3, con soporte para cifrado del canal mediante (SSL).
- Unos filtros de contenidos (antivirus y antispam).

Zimbra utiliza Amavis como filtro de contenidos y por defecto, SpamAssassin y ClamAV como filtros antispam y antivirus, respectivamente. De todos modos, es posible configurarlo para que utilice cualquier otro filtro antispam. El correo se recibe mediante SMTP, se enruta mediante una tabla de transportes y se entrega al almacén de correo haciendo uso del protocolo LMTP.

[14] http://lucene.apache.org

Zimbra Store

Zimbra Store, utilizando Jetty como contenedor de servlets, almacena el correo electrónico. Cada cuenta se configura en un servidor y esta cuenta está asociada con un buzón de correo que contiene todos los mensajes y archivos adjuntos. El servidor de buzones está formado por:

- El almacén de datos.
- El almacén de mensajes.
- El almacén de índices.
- Las utilidades de conversión de adjuntos a HTML.

Cada servidor de Zimbra tiene su propio almacén de datos, almacén de mensajes y almacén de índices para los buzones de ese servidor. En cuanto llega un correo, el servidor de Zimbra crea un nuevo proceso para indexar el mensaje. También se crea un hilo para la conversión de adjuntos a formato HTML, que a su vez es indexado por otro hilo.

El almacén de datos es una base de datos MySQL en la cual los identificadores de mensajes son enlazados con las cuentas de usuario. El almacén de datos relaciona el identificador del buzón con la cuenta de usuario a la que pertenece en el directorio LDAP. Esta base de datos contiene el conjunto de etiquetas definido por el usuario, las carpetas, las citas del calendario y los contactos de los usuarios, así como el estado de cada mensaje de correo (leídos, no leídos, etiquetas asociadas a cada mensaje y la carpeta en la cual reside el mensaje).

El almacén de mensajes guarda todos los mensajes y sus adjuntos en formato MIME. Los mensajes enviados a múltiples destinatarios dentro del mismo servidor sólo son almacenados una vez. La tecnología necesaria para indexar y buscar la proporciona Lucene y se mantienen índices sobre cada buzón.

Zimbra SNMP y Zimbra Logger

La instalación de ambos paquetes es opcional, pero muy recomendada. En cada servidor donde esté instalado, Zimbra SNMP recoge información periódica del estado del sistema. Además, utiliza Swatch[15] para analizar la salida del syslog y generar los traps de SNMP(Simple Network Managment Protocol).

Por su parte, Zimbra Logger instala herramientas de agregación de logs, informes y seguimiento de mensajes. Sin este paquete no se podrán utilizar las funcionalidades de seguimiento de mensajes y estadísticas del servidor de la consola gráfica de administración.

Instalaciones distribuidas (multiservidor)

Además de la solución de clustering con Red Hat Enterprise, Zimbra soporta una instalación distribuida (ver Figura 3.9) de cada uno de los dominios que

[15] http://swatch.sourceforge.net

hospede, centralizando la administración en una sola consola gráfica y ofreciendo un punto de entrada único a los usuarios.

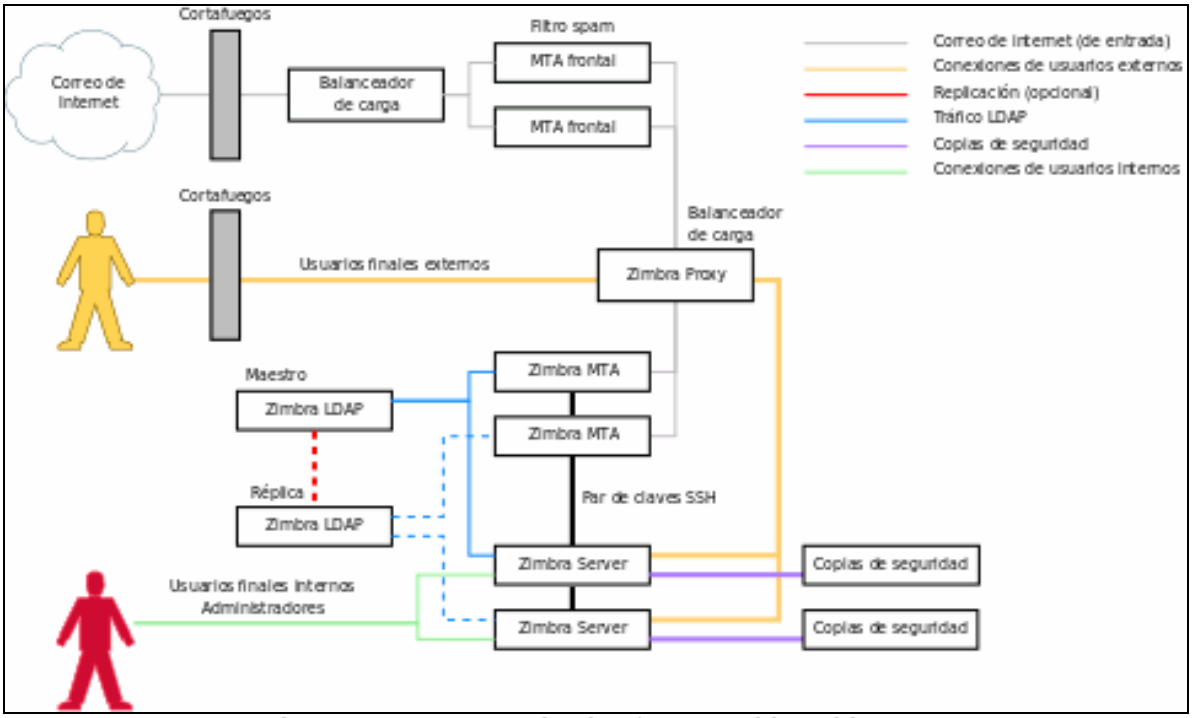

Figura 3.9: Esquema de plataforma multiservidor

Para lograrlo se instalan dos o más sistemas con Zimbra, todos con un subdominio diferente del mismo dominio. Uno de los servidores actúa como maestro y los demás como esclavos de éste. Durante la instalación que se empezará, como es lógico, por el maestro, se especifica en cada esclavo los datos del maestro que debe replicar. Las características principales de este tipo de instalación serían las siguientes:

- Gestión centralizada de las cuentas de los usuarios en el servidor maestro.
- Ejecución remota de comandos en los servidores esclavos mediante el uso de un par de claves SSH.
- Replicación del directorio LDAP del maestro a los esclavos. Esto permite mantener copias locales de las cuentas que cada nodo gestiona y el acceso al GAL (Global Address List) completo de usuarios.
- Monitorización del estado de todos los nodos a través de SNMP y presentación de los datos estadísticos en el maestro (en la consola gráfica de administración).
- Cada nodo tendrá su registro de DNS tipo A y tipo MX.
- Mediante la tabla de transportes de Postfix, el correo se enrutará al host pertinente.

- Mediante el uso del proxy de Zimbra (basado en Nginx y Memcached) se distribuirán las conexiones HTTP, IMAP y POP3 (y sus equivalentes sobre canal cifrado).

3.4.5 Descripción técnica del hardware seleccionado

Para la implementación final se dispone de un hardware bastante robusto de la casa Hewllet Packard, con dos procesadores Xeon, 8 GB RAM y ocho discos (146 GB c/u) en raid 5 + spare (ver Tabla 3.5). Este equipo (ver Figura 3.10) cuenta con garantía 3x3x3 y está conectado a dos UPS de 3 kVA c/u.

Ítem	Descripción
Producto	HP ProLiant DL380 G5 High Efficiency - Quad-Core Xeon E5430
Factor de forma	Se puede montar en bastidor - 2U
Dimensiones (Ancho x Profundidad x Altura)	8.59 cm x 44.54 cm x 66.07 cm
Peso	27.22 kg
Procesador	2 x Quad-Core Intel® Xeon® Processor E5430 (2.66 GHz, 1333 MHz FSB, 80W)
Memoria caché	12 MB L2
Caché por procesador	12 MB (2 x 6 MB)
Memoria RAM	8 GB (instalados) / 32 GB (máx.) - DDR2 SDRAM - Código de corrección de errores (ECC) avanzado - 667 MHz - PC2-5300
Controlador de almacenamiento	RAID (Serial ATA-150 / SAS) - PCI Express x4 (Smart Array P400i) ; IDE (IDE/ATA)
Bahías de almacenamiento de servidor	Hot-swap
Disco duro	8 x 145 GB SAS.
Controlador gráfico	ATI ES1000 - 32 MB
Conexión de redes	Adaptador de red - PCI Express x4 - Ethernet, Fast Ethernet, Gigabit Ethernet - Puertos Ethernet : 2 x Gigabit Ethernet
Alimentación	CA 120/230 V (50/60 Hz)
Redundancia de alimentación	2 fuentes redundantes de 850w
Garantía del fabricante	3 años de garantía (in situ)

Tabla 3.5: Hardware disponible para la implementación.

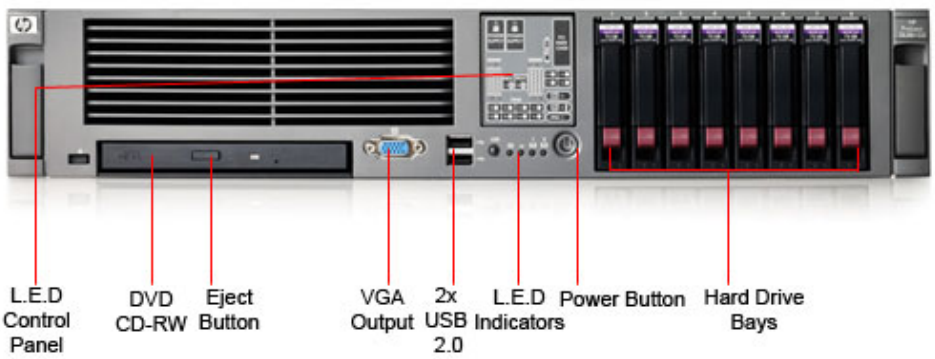

Figura 3.10: Servidor HP ProLiant DL380G5

3.5 Diseño del ambiente de pruebas

3.5.1 Esquema de pruebas

Para las pruebas (ver Figura 3.11) de la plataforma propuesta se pretende utilizar un equipo básico como servidor de ZCS, implementado bajo Debian Etch 4 con entorno gráfico y adicionalmente utilizas una estación de trabajo con Windows XP para enviar los distintos patrones de mensajes. Estos patrones darán pie al análisis y adecuación de los parámetros para obtener los conocimientos y afianzar las decisiones, observaciones y recomendaciones sobre el trabajo especial de grado.

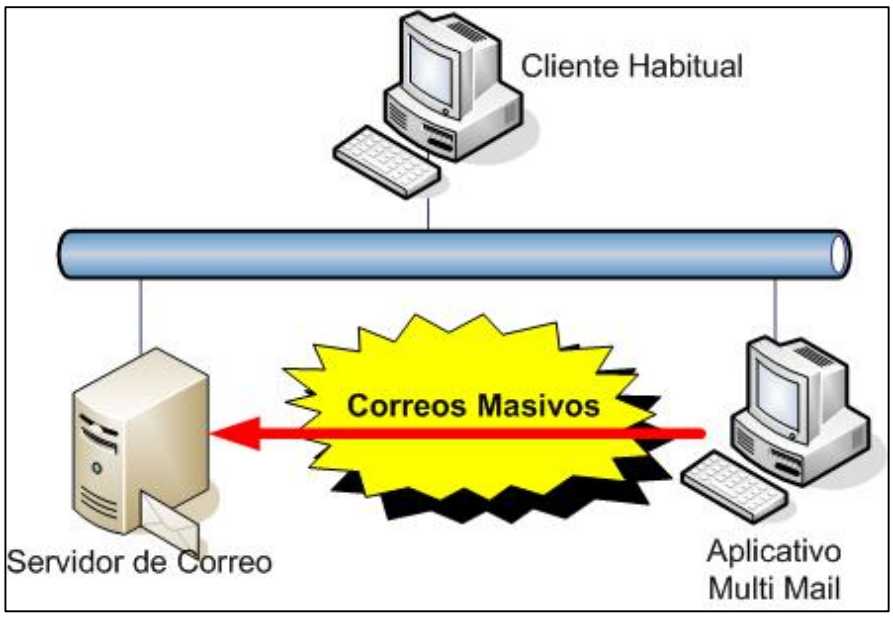

Figura 3.11: Topología de laboratorio de pruebas

3.5.2 Descripción de pruebas

Haciendo uso de los conocimientos teóricos y la forma como trabajan las herramientas de filtrado de la solución propuesta, se pretende bombardear y configurar la suite Zimbra para tomar las muestras que servirán para el análisis y recomendaciones de la implementación del producto.

Pruebas de detección de virus y código malicioso

Con esta prueba se pretende verificar la eficacia de los filtros de antivirus preconfigurado con la suite de Zimbra. Al enviar archivos adjuntos con firmas que presumen ser código malicioso se podrá detectar si la herramienta clamav puede detectar y erradicar estos mensajes.

Pruebas de envíos masivos o UBE

Muchos mensajes enviados desde el mismo origen pueden ser catalogados como spam, pero cuan rápido es el aprendizaje por parte de la solución. En estas pruebas se pretende evaluar la velocidad de convergencia en la detección de spam cuando se esta en presencia de múltiples envíos de correo basura.

Pruebas de envíos de mensajes MMF

Quizás la prueba más atrayente es la de valorizar el contenido del mensaje al compararlo con las reglas predefinidas del spamassassin. Con estas pruebas se observará la aplicación de las reglas y sus variantes, las cuales darán pie a los análisis posteriores en cuanto a la solución propuesta.

3.6 Proceso de implementación

En esta sección se explican los detalles de adecuación inicial para implementar la propuesta de solución.

3.6.1 Procesos de implantación de la solución propuesta

Como la suite de Zimbra viene integrada por ldap, postfix, spamassassin, clamav y otras herramientas de interés para la solución propuesta, la implementación se hará en forma integrada y completa.

Requerimiento de hardware para la suite de Zimbra

Los requerimientos de Zimbra Collaboration Suite en comparación con otros productos similares son bastante bajos. Para entornos de evaluación (hasta 50 cuentas) la siguiente configuración debería ser suficiente:

- CPU Intel/AMD de 32bits a 2.0. GHz o superior.
- Un (1) GB de RAM.
- Cinco (5) GB de espacio libre en disco para el software y los logs.
- Espacio adicional para el almacenamiento del correo y las bases de datos (depende del número de cuentas y de la cuota de disco asignada a cada una).

Instalación de Zimbra

Descripción de prerrequisitos y pasos para la instalación de la suite.

Adecuar el sistema operativo

Para la fase de evaluación se instalará el sistema operativo Debian Etch Release 4.0 con entorno gráfico para capturar las pantallas de instalación y hacer las pruebas de configuración. Para la implementación final del sistema operativo no se deberá usar entorno gráfico para mejorar el rendimiento del hardware.

El equipo usado para la instalación debe disponer de acceso a Internet o a un mirror de Debian [11]. Para el caso de estudio se configuró la IP *10.0.9.5*, como nombre de host se colocó *prueba* y se usó el nombre de dominio *tesis.net*

Paso #1: Revisar los servicios y puertos abiertos

En este paso se puede utilizar el analizador de puertos nmap [11] para verificar los servicios y puertos abiertos en el equipo de prueba. Se puede instalar con el comando *aptitude install nmap*. Al utilizar nmap con el comando nmap localhost en el equipo de pruebas, obteniéndose como salida el resultado de que no existe un posible conflicto de puertos (ver Figura 3.12), que regularmente se genera porque al instalar Debian en forma desatendida siempre se activa un agente de correo local que abrirá el puerto TCP 25 (Debian hace uso de exim4).

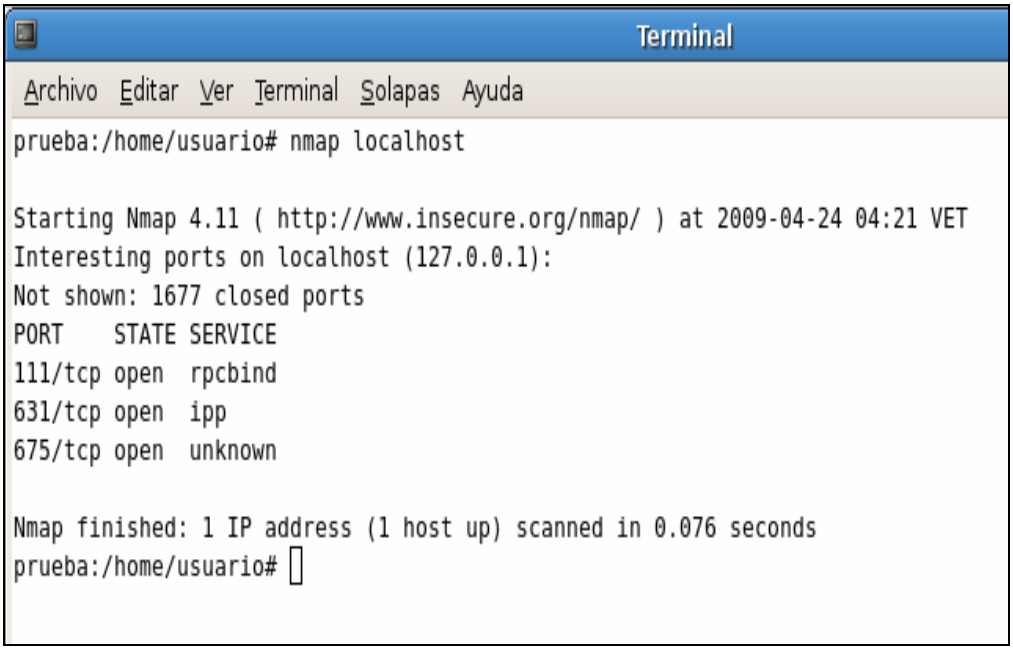

Figura 3.12: Chequeo de puertos

En caso de encontrar exim4 instalado se podrá desinstalar o eliminar ejecutando *aptitude remove exim4* y luego *aptitude purge exim4*.

Paso # 2: Adecuación de la resolución local de nombre.

Se debe modificar el archivo /etc/hosts (ver Figura 3.13) para adecuar el registro asociado a la máquina local de una forma que la suite de Zimbra establece para poder efectuar la instalación (para referencia, se comentan con # las líneas que vienen por defecto).

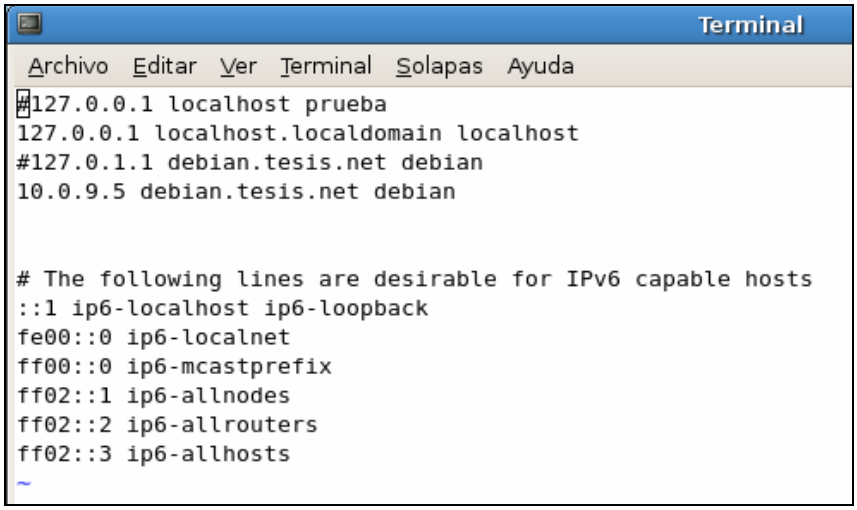

Figura 3.13: Modificación del archivo hosts

Se crearon nuevas entradas en el archivo y se agregaron la línea 2 y la línea 4.

Paso # 3: Instalación y configuración del DNS

En esta fase se montará un servicio de DNS local, necesario para resolver el nombre del dominio de prueba (tesis.net) y agregar el registro MX para el servidor de correo.

La herramienta que se utilizará es bind versión 9.0, y se podrá instalar ejecutando el comando *aptitude install bind9*. Una vez instalado se deberá modificar el archivo /etc/bind/name.conf.local (ver Figura 3.14), para crear la entrada de la nueva zona tesis.net y su inversa (la cual se mostrará aquí pero no es necesario para el laboratorio).

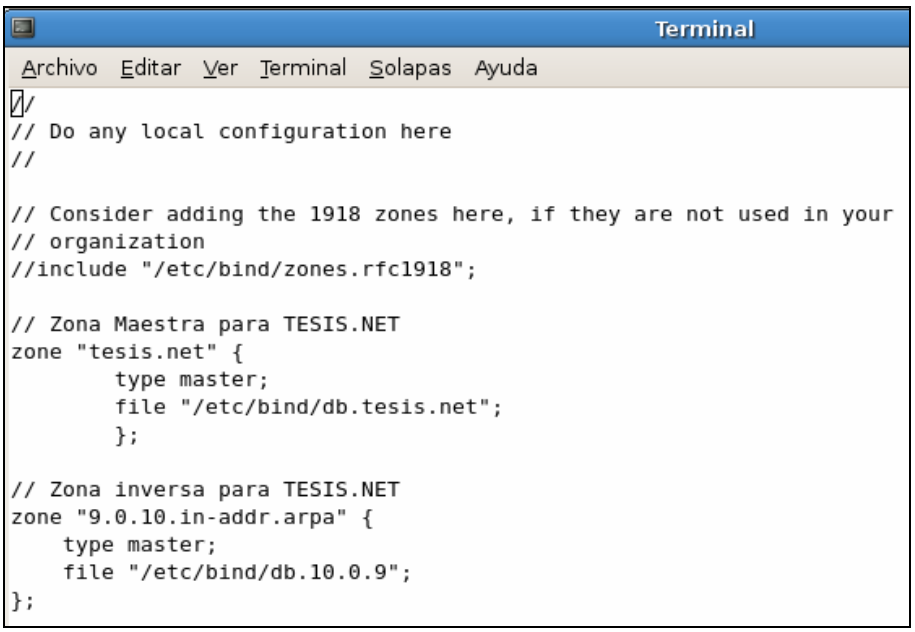

Figura 3.14: Insertar nueva zona y su inversa

Una vez realizado el cambio anterior se deberán crear los archivos que contendrán los registros de la zona directa tesis.net (contiene el registro MX) y los registros de la zona inversa. Para esto se ejecuta el comando *touch /etc/bind/db.tesis.net,* luego se edita el archivo y se adecua (ver Figura 3.15).

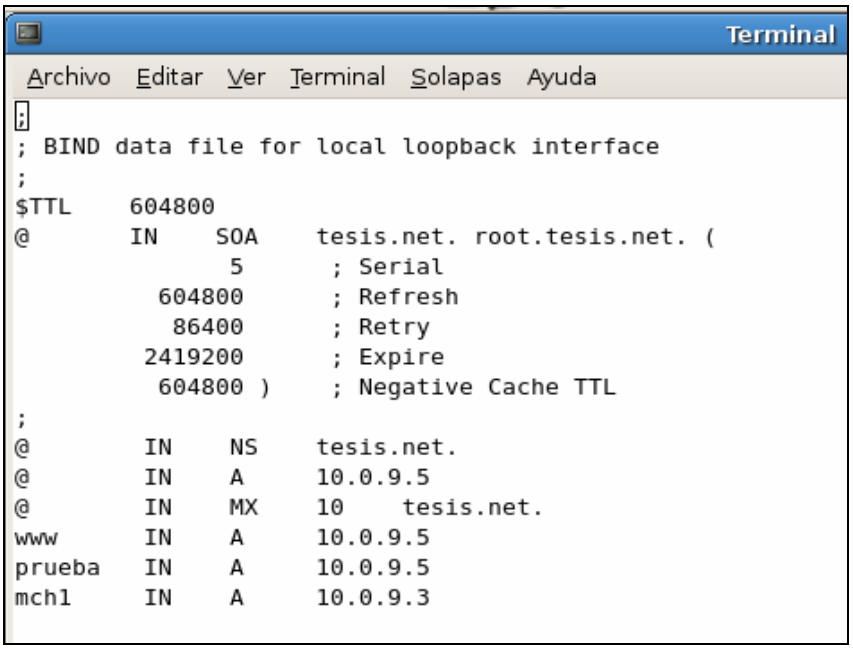

Figura 3.15: Registro de zona directa tesis.net

De la misma forma se crea un archivo para los registros de la zona inversa *touch /etc/bind/db.10.0.9*, se edita y se adecua (ver Figura 3.16).

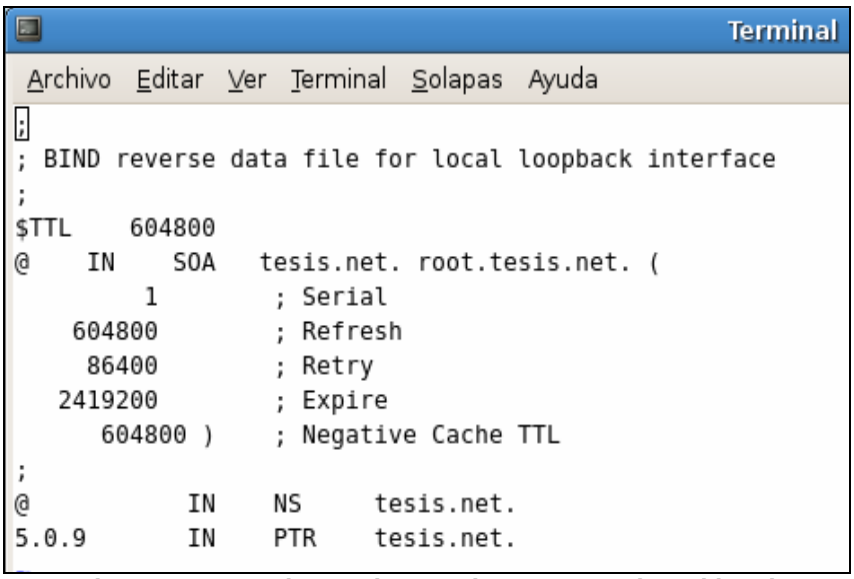

Figura 3.16: Registros de zona inversa para la red local

Paso # 4: Instalación de la suite Zimbra

Previamente descargado y copiado en la ruta /root se procede a la instalación del servidor de correo electrónico.

Como primera instancia se debe descomprimir el archivo con el comando *tar -xvzf /root/zcs-5.0.6_GA_2313.DEBIAN4.0.20080522112011.tar.gz,* luego se debe cambiar al directorio que se creó al descomprimir el archivo con el comando *cd /root/zcs-5.0.6_GA_2313.DEBIAN4.0.20080522112011.*

Una vez allí se debe ejecutar el comando *./install.sh* que es el instalador de Zimbra y que muestra información donde se indica que no existe ningún componente instalado previamente (ver Figura 3.17).

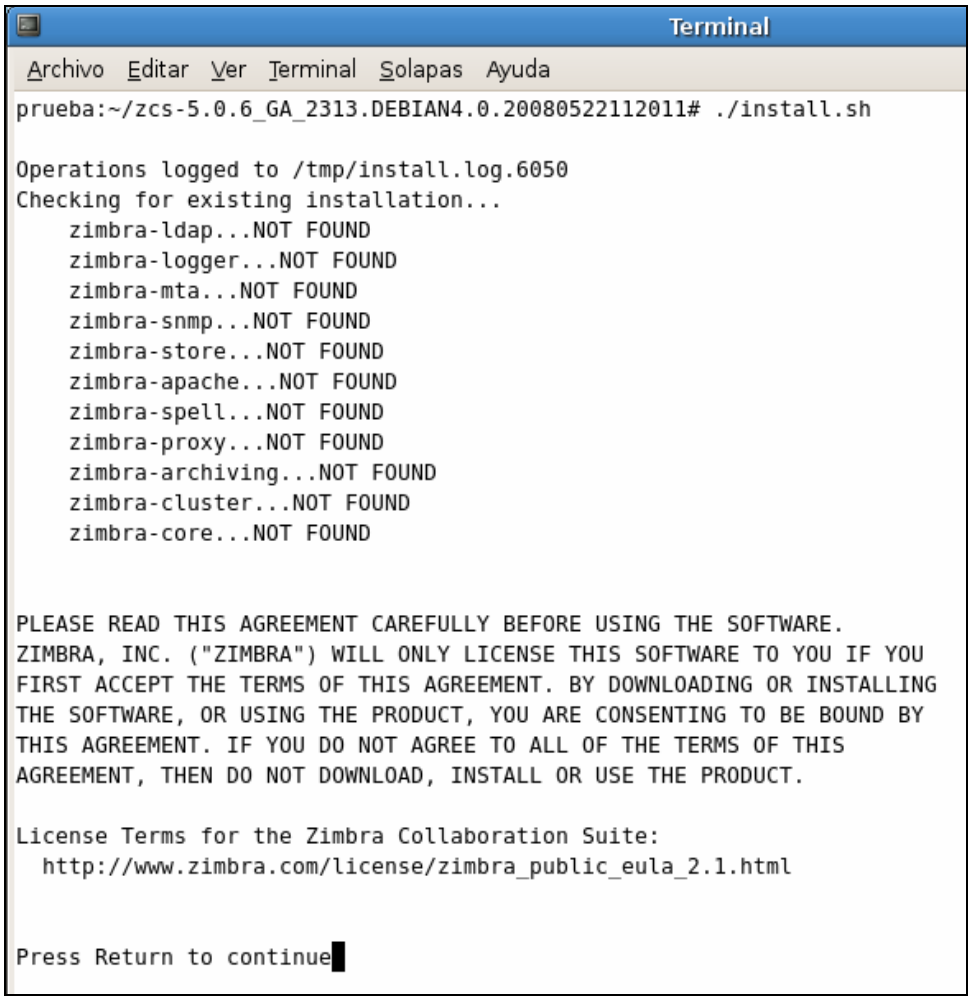

Figura 3.17: Chequeo de componentes instalados

Después de continuar con la instalación se genera un error (ver Figura 3.18) que se despliega por la necesidad de algunas dependencias.

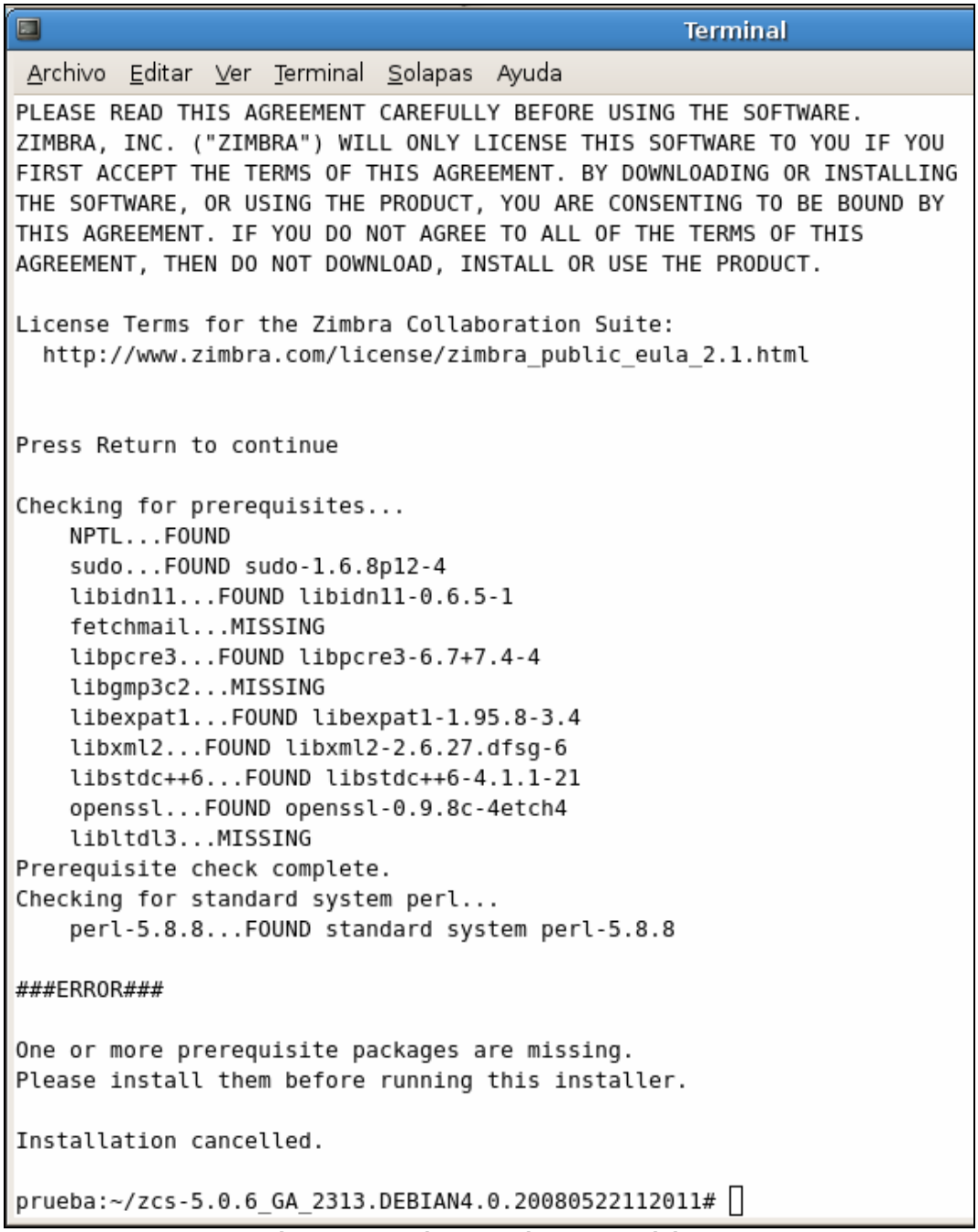

Figura 3.18: Chequeo de prerrequisitos

Como la instalación termina abruptamente, se pueden instalar las dependencias ejecutando *aptitude install fetchmail libgmp3c2 libltdl3* (ver Figura 3.19).

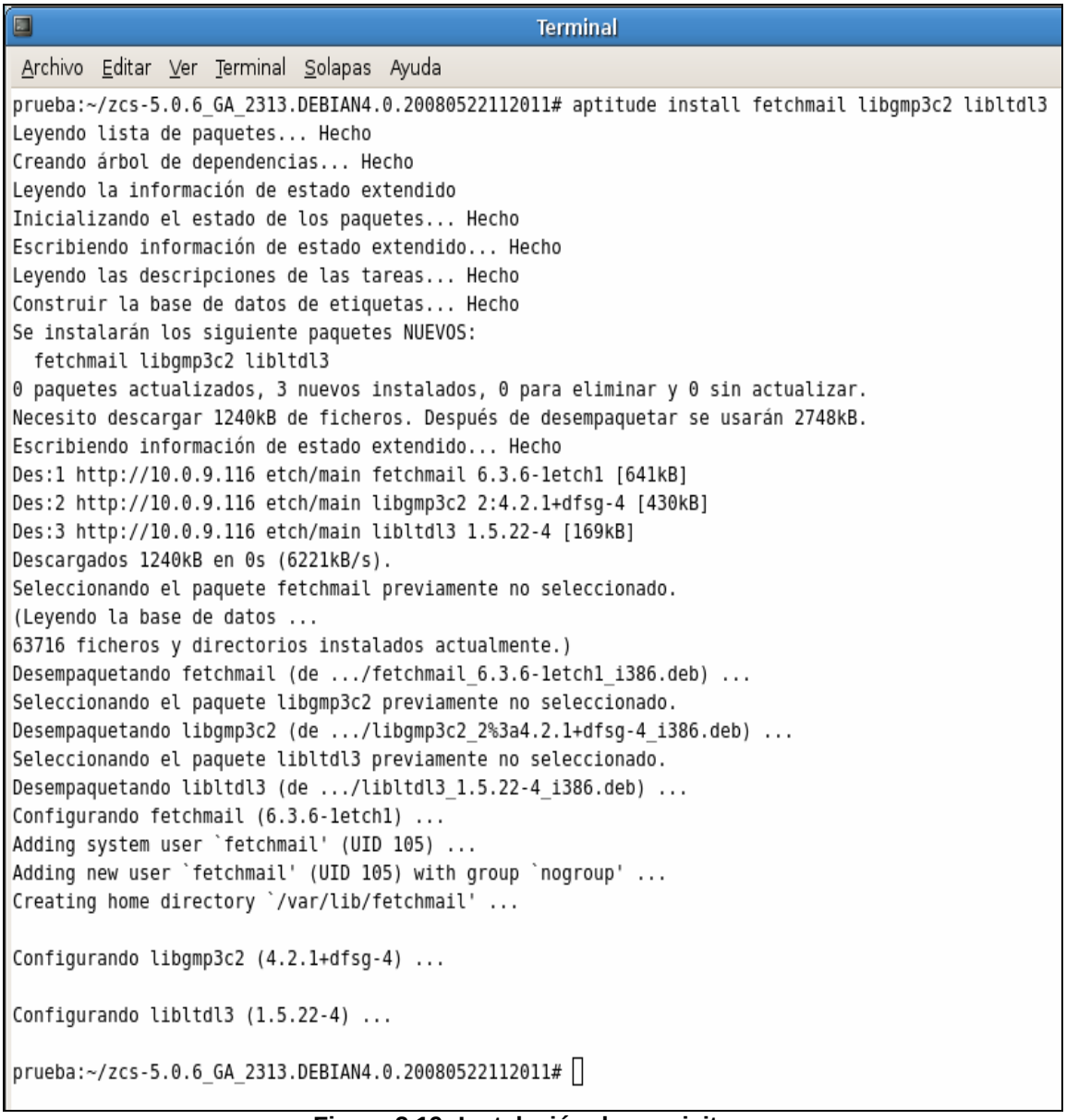

Figura 3.19: Instalación de requisitos

Una vez instaladas las dependencias se procede nuevamente a la instalación de la suite Zimbra con el comando *./install.sh* (ver Figura 3.17) y a continuación se mostrará el chequeo de las librerías necesarias para la instalación (ver Figura 3.20).

Figura 3.20: Nuevo chequeo de prerrequisitos

Seguido en la instalación se harán una serie de preguntas (ver Figura 3.21) a las cuales se deberá responder con la opción que se muestra por defecto, pudiéndose dar cambios en las respuestas en base a un modelo y topología previamente conceptualizado.

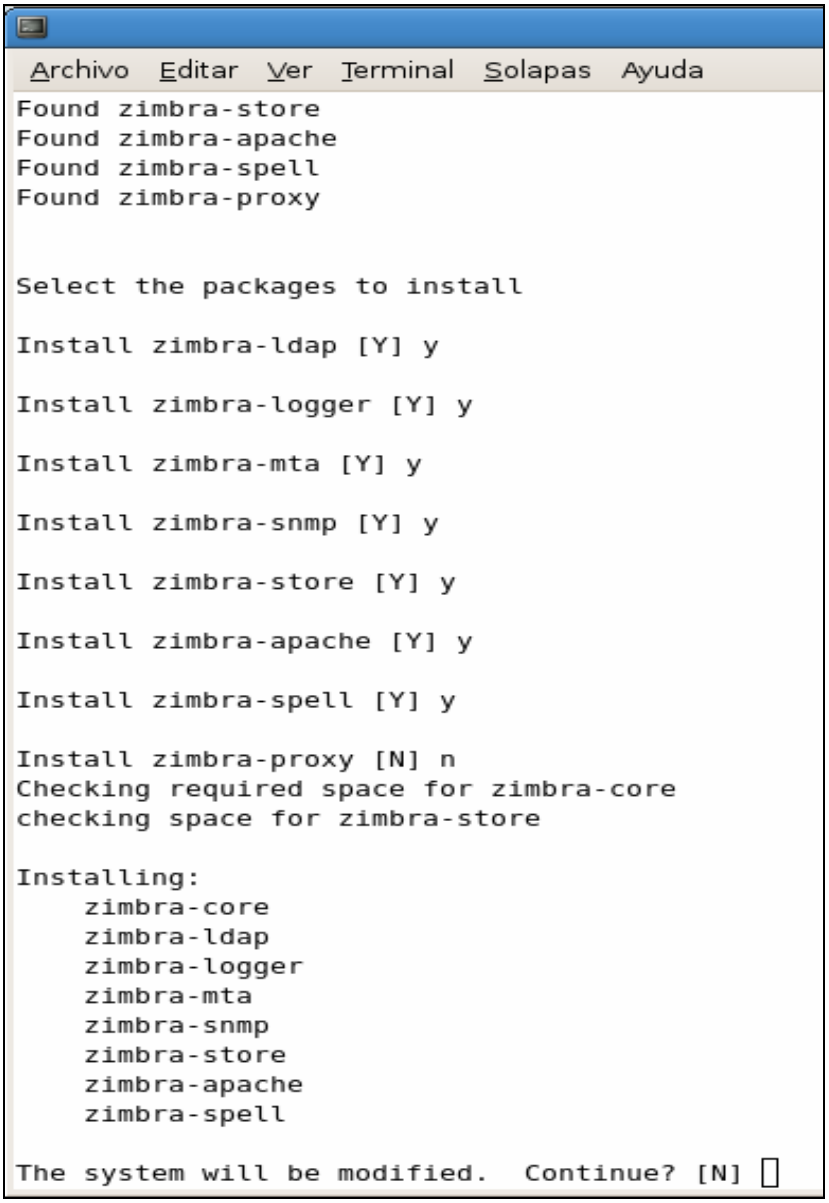

Figura 3.21: Selección de componentes a instalar

Aprobados los componentes a instalar, la instalación verifica la adecuación del dominio y el registro MX (ver Figura 3.22).

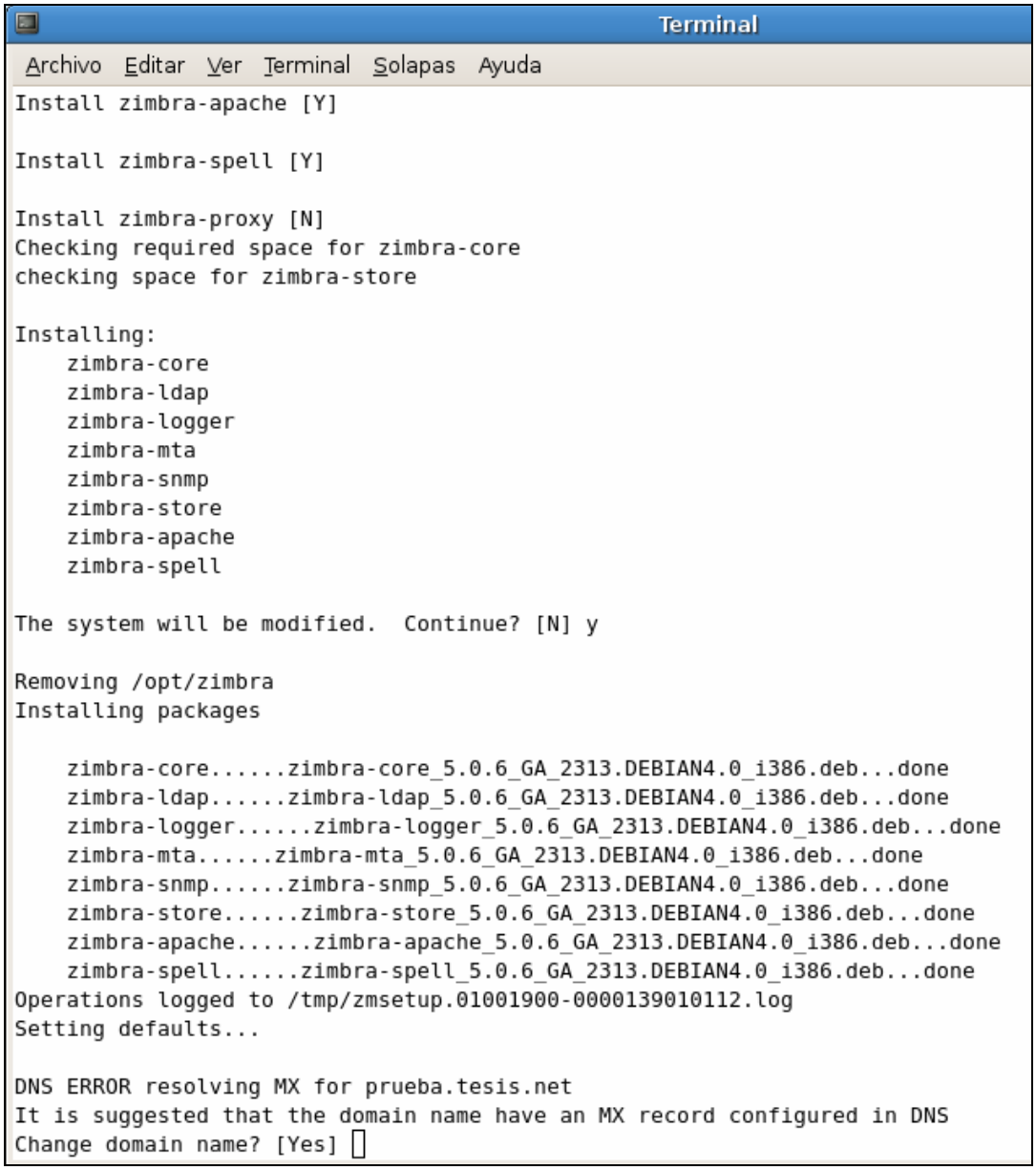

Figura 3.22: Falla de nombre de dominio

A continuación se muestra la información de la instalación de los paquetes seleccionados para habilitar en la suite de Zimbra (ver Figura 3.23).

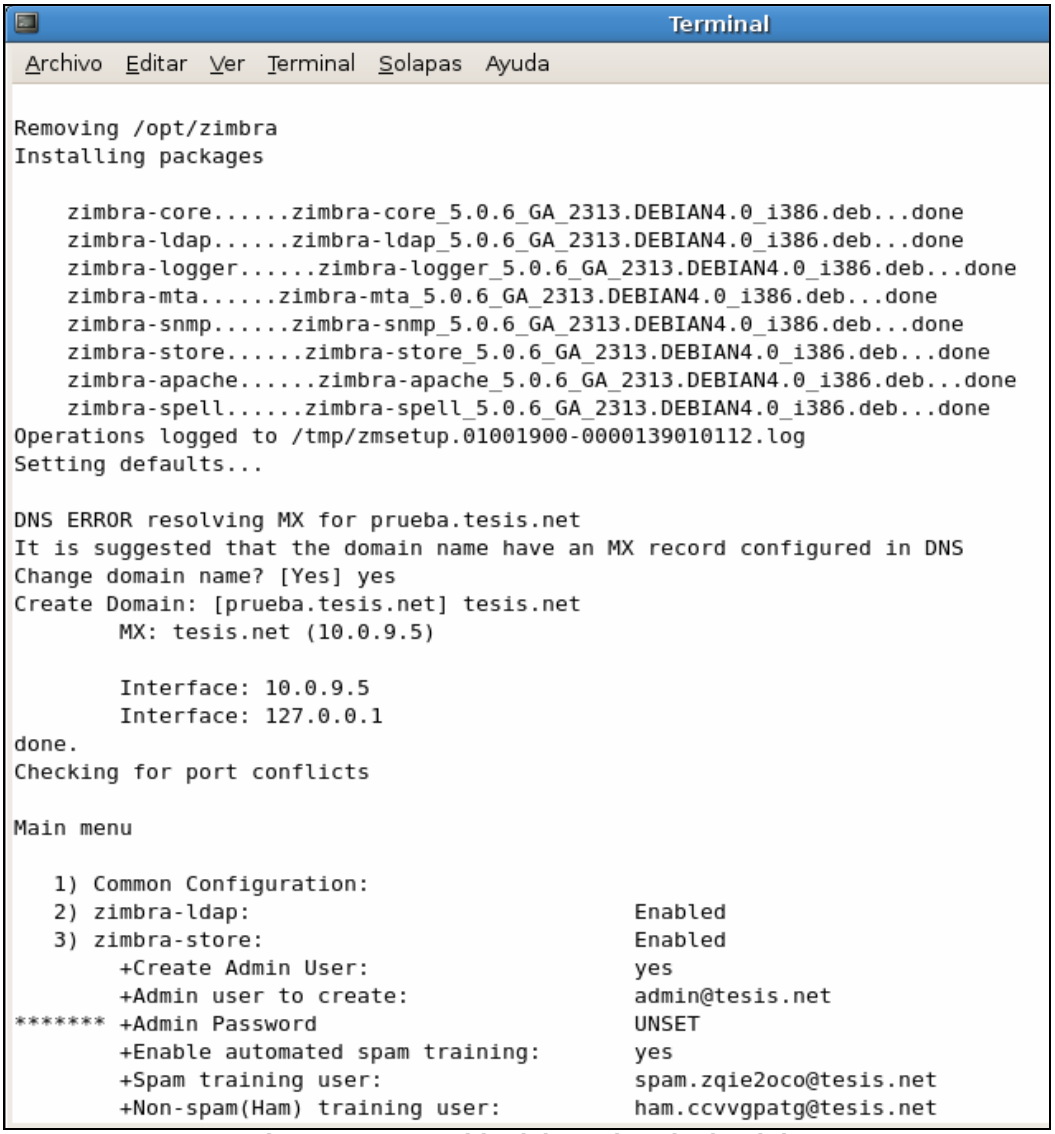

Figura 3.23: Cambio del nombre de dominio

Al continuar con la instalación se muestra un error al no encontrar el registro MX para el dominio prueba.tesis.net, lo cual es debido a que la instalación toma el nombre completo del host como nombre de dominio (ver Figura 3.23).

Para resolver esto se debe cambiar el nombre de domino a tesis.net y la instalación seguirá su curso, verificará la existencia del registro MX y el conflicto de puertos e indica que se debe cambiar lo que aparece con asteriscos (******) (ver Figura 3.24).

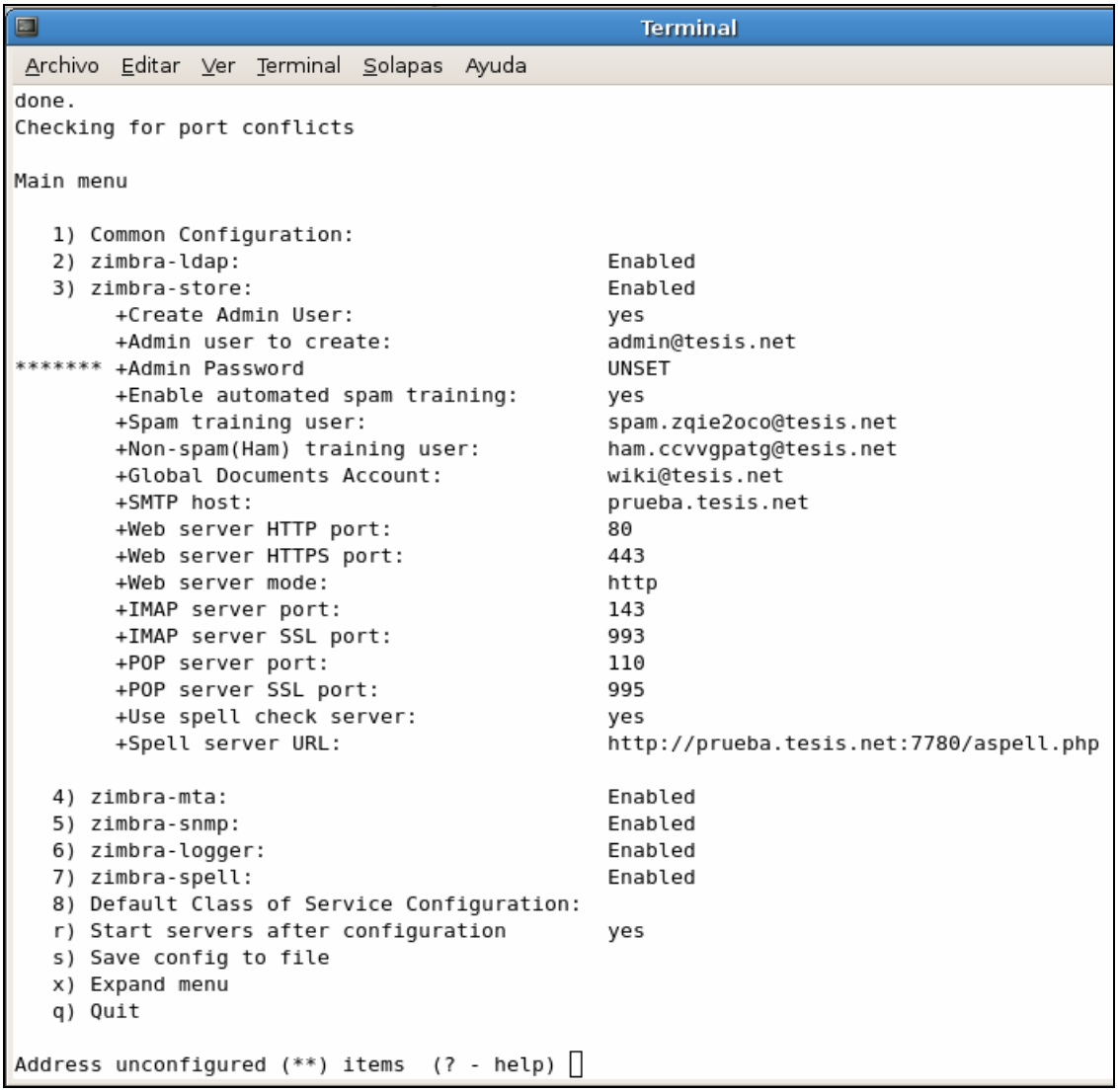

Figura 3.24: Menú de configuración

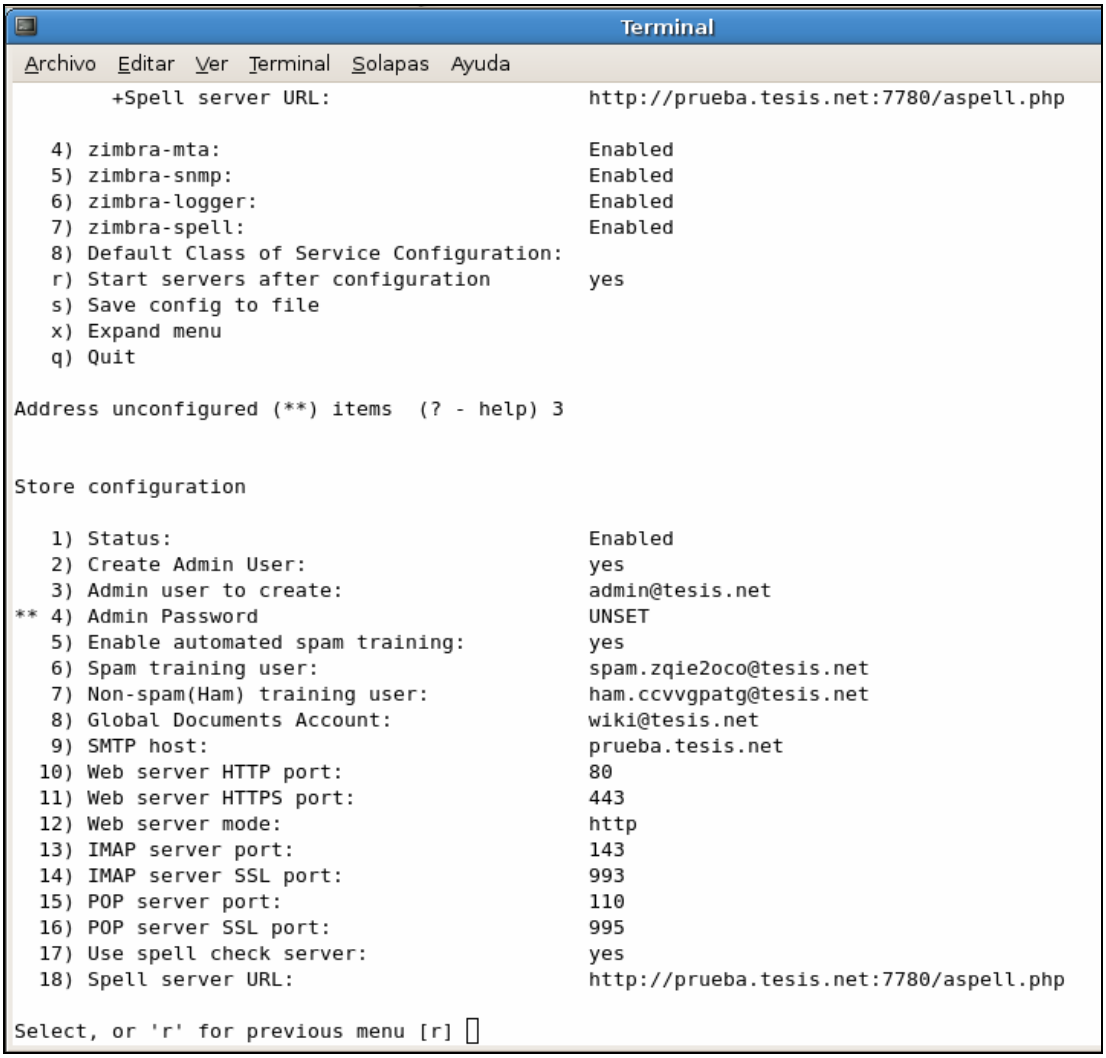

Figura 3.25: Selección del menú para cambio de password de administrador

Se accede a la opción 3 y luego a la opción 4 para cambiar el password de administrador (ver Figura 3.25).

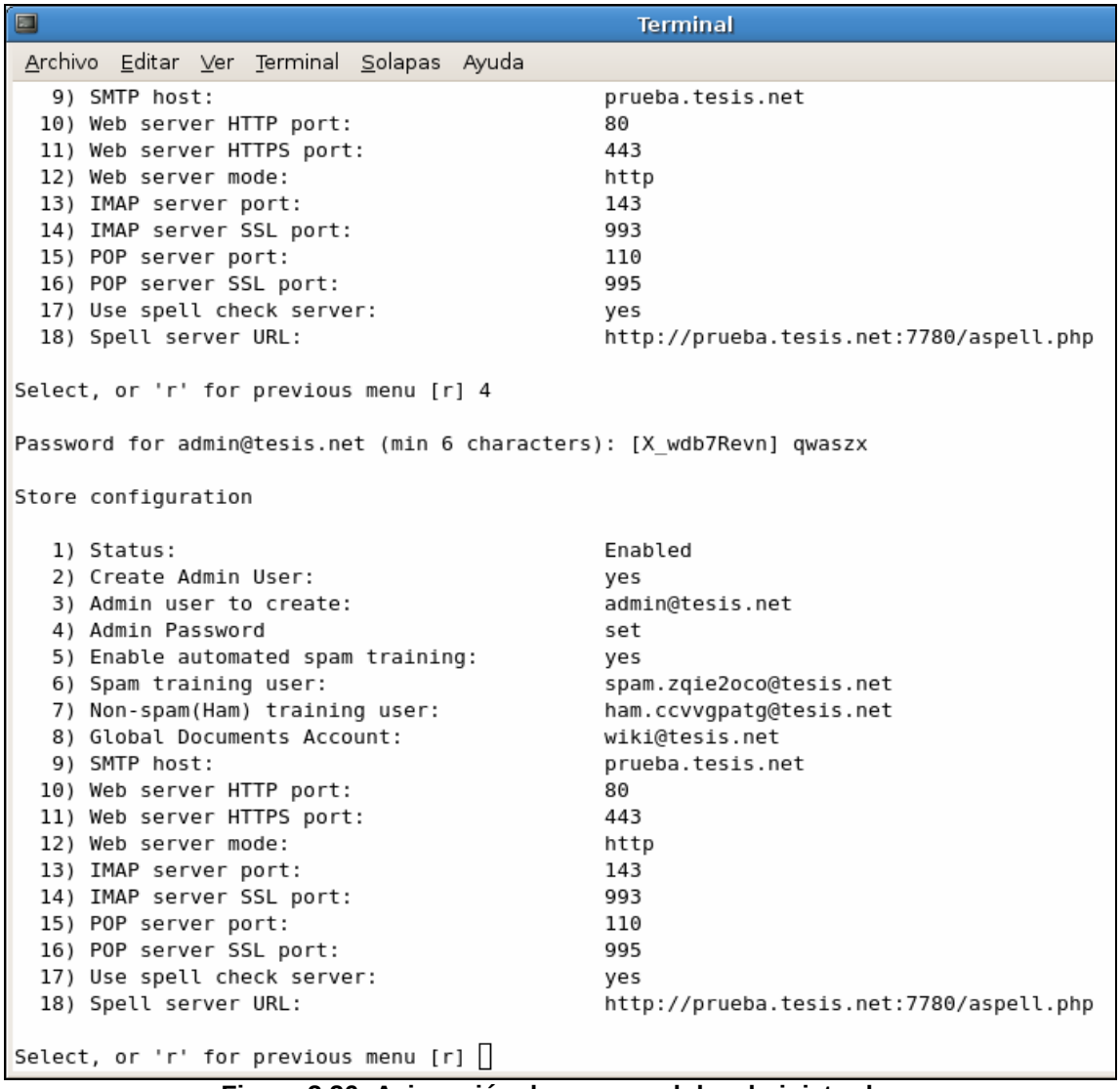

Figura 3.26: Asignación de password de administrador

Una vez asignado el password de administrador se retorna al menú principal (ver Figura 3.26).

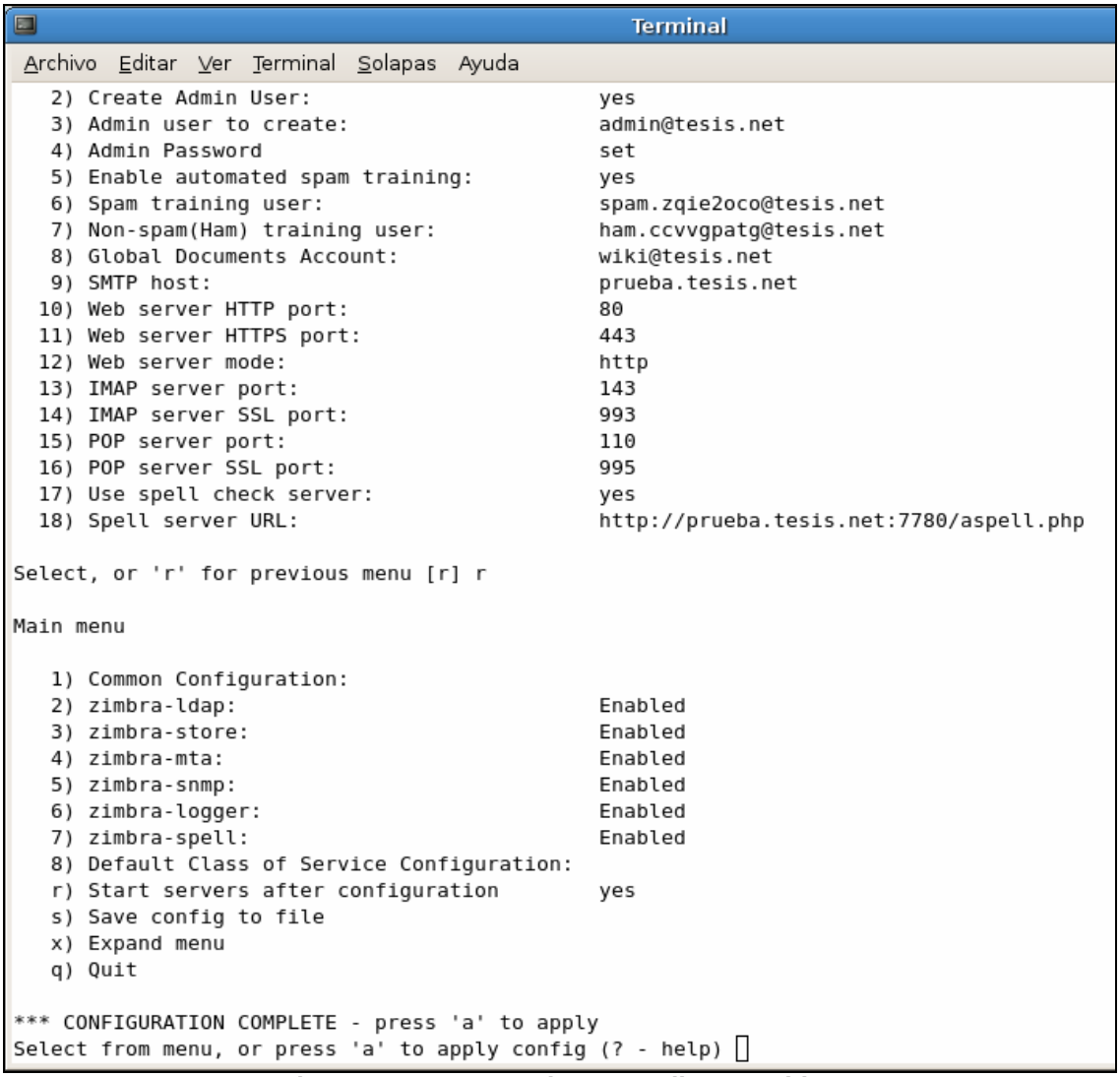

Figura 3.27: Esperando para aplicar cambios

Una vez completados los cambios en la configuración, se aplican los cambios, se salva la configuración y se procede a continuar la implementación (ver Figura 3.27).

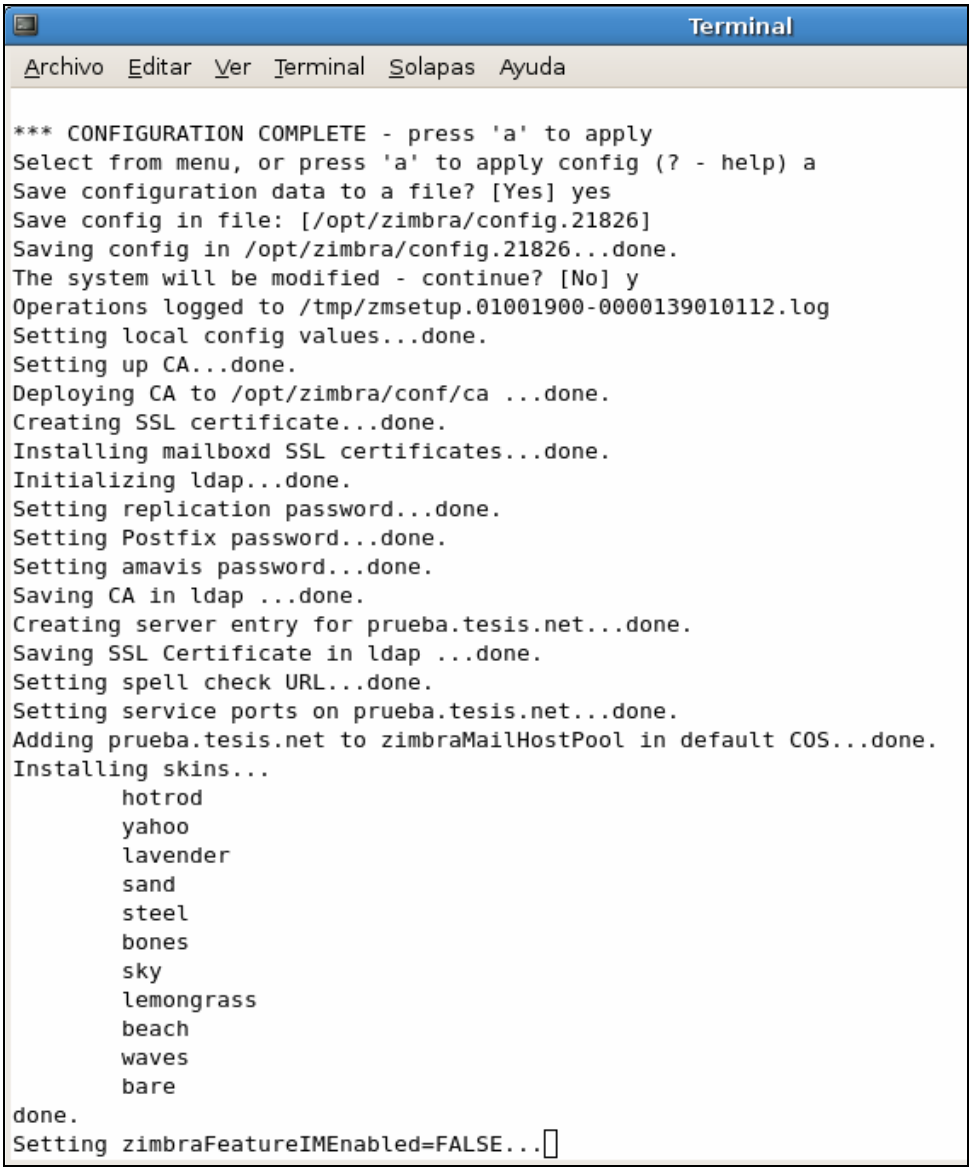

Figura 3.28: Aplicando cambio (parte 1)

El siguiente paso es la creación de los certificados digitales para cifrar las conexiones entre los componentes de la suite (ver Figura 3.28 y Figura 3.29).

Figura 3.29: Aplicando cambio (parte 2)

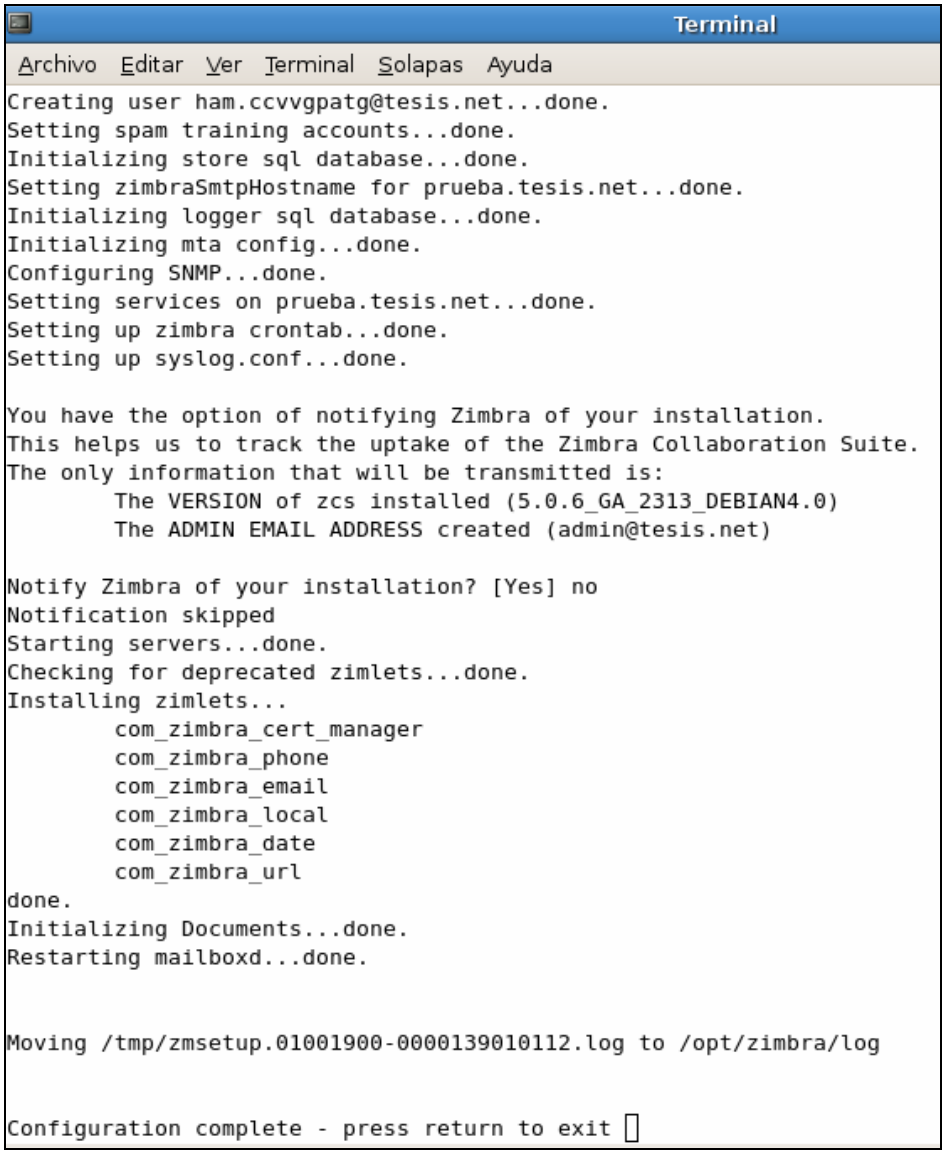

Figura 3.30: Instalación finalizada

Antes de finalizar la instalación se puede notificar a los creadores de Zimbra la implementación de la solución (ver Figura 3.30).

Una vez finalizada la instalación se procede a crear algunos usuarios de prueba, configurar algunos parámetros en la consola administrativa y efectuar pruebas de envío y recepción.

3.6.2 Archivos de configuración modificados

Mejorando el sistema antispam de Zimbra

Cuando un servidor está siendo bombardeado por spammers, se refleja gran cantidad de conexiones simultáneas. Muchas de esas conexiones fallan, porque no existen los usuarios de esas cuentas, pero aun así, estas conexiones existen y consumen recurso. Se puede configurar a postfix para que esto se reduzca significativamente iniciando sesión con el usuario Zimbra y ejecutando los comandos reflejados en la Figura 3.31 y luego se debe reiniciar el postfix.

```
postconf -e 'smtpd_hard_error_limit = 3'
postconf -e 'smtpd_soft_error_limit = 2'
```

Figura 3.31: Limitar número de conexiones con error

Estas instrucciones hacen que el servidor postfix deniegue las conexiones de clientes SMTP que tienen muchos errores[16].

Descartando e-mails enviados a direcciones invalidas

Se puede configurar a Zimbra para que rechace los correos a cuentas inexistentes, diciendo que la dirección no existe (mensaje de error 450), además de tomarse 5 segundos antes de aceptar otro comando del servidor que envía el mensaje con la dirección inválida, demorando de esta manera al spammer. Para lograrlo se debe añadir las líneas de la Figura 3.32 al archivo */opt/zimbra/conf/postfix_recipient_restrictions.cf* después de la primera línea (reject_non_fqdn_recipient) encontrada.

```
reject_unknown_recipient_domain
reject_unverified_recipient
```

Figura 3.32: Descartar direcciones inválidas

La primera línea bloquea mails de inexistentes dominios. Colocando esto antes, evita la sobrecarga innecesaria al probar mensajes cuyos dominios no existan. La segunda línea bloquea mails a direcciones cuyo destinatario no exista en el dominio de destino o no pueda ser alcanzada.

Muchas veces al colocar la segunda regla se tienen problemas al enviar mensajes ya que muchos servidores no permiten la verificación de las cuentas o como en caso de Yahoo que permite el envío a cualquier cuenta para después responder con un mensaje si es que la cuenta existe o no. Una forma de bloquear correos enviados al servidor a cuentas inexistentes es cambiar en */opt/zimbra/conf/zmmta.cf* el valor de *smtpd_reject_unlisted_recipients* a yes. Si se utiliza una versión de Zimbra posterior a 5.0.12 con alias de dominios, se debe configurar *postfix_enable_smtpd_policyd=yes* en lugar de lo anterior ya que esta no funciona. Luego se dede reiniciar el postfix.

De cualquier forma la primera regla es muy útil y funciona de maravilla bloqueando e-mail a dominios que no existen. Sin embargo las políticas de

[16] http://www.postfix.org/postconf.5.html#smtpd_soft_error_limit

verificación de direcciones del remitente/destinatario son sólo aplicables para servidores de bajo tráfico (menos de 2000 mails diarios), ya que su performance es pobre bajo alta carga, ya que tiene que verificar las direcciones cada vez que se trate de enviar un e-mail. La excesiva actividad de verificación de direcciones puede causar que un servidor sea puesto en una lista negra por algunos proveedores.

Asegurando zimbra contra virus en la red

Algo muy común que está pasando en las redes actuales, es que los PCs de usuarios son comúnmente infectados de virus o troyanos que se esconden en la red.

La mayoría de estos virus o troyanos se convierten en centros de envío de spam o tratan de infectar otras máquinas propagándose ellos mismos utilizando sus propios motores SMTP (servidores de correo) o utilizando los de la red.

Los más reciente spywares se instalan en los equipo y son usados por terceros para enviar correos spam a través del equipo infectado, usando el usuario y contraseña de correo en la máquina o por una vulnerabilidad típica y sencilla de todos los servidores de correo que permite enviar correo a cualquier máquina de la red a la que pertenece.

Por defecto, la mayoría de servidores de correo permiten el reenvío de correo a cualquier cliente SMTP que se encuentre en la misma red sin pedirle autenticación. Sólo los que ingresan de redes diferentes (Internet) se les pide autenticación. Esto en sí antes no significaba ningún problema, pero ahora con la proliferación de estos spywares y virus, hacen que el servidor de correo se convierta en centro de envio de spam.

Para protegerse de este problema se debe configurar el servidor de correo para que siempre pida autenticación para el envio de correo y que sólo pueda hacer relay para su propia IP y para su interfaz loopback (127.0.0.x)

Zimbra se configura por defecto para que sea relay de su red local. Esto se debe cambiar a solo la dirección IP usada, lo cual se puede realizar por la consola de administración cambiando en el MTA, redes de confianza MTA, y cambiando la IP x.x.x.0/24 a x.x.x.x/32.

Con esto se evita que máquinas infectadas con virus usen un servidor para propagarse ellos mismos, o que lo puedan usar como centro de envío de spam.

Algo adicional que se debe hacer si es que se comparte una sola conexión a Internet, es por lo menos tener dos direcciones IP públicas: una para los usuarios y otra para el servidor de correo. Así se evitará que la IP del servidor sea marcada como spammer por culpa de algún virus dentro de la red.

3.6.3 Zona de descarga de software

El software utilizado en las pruebas de implementación fue descargado de los siguientes enlaces:

Zimbra: http://www.zimbra.com/community/downloads.html
Debian: http://www.debian.org/CD

Sin embargo, se puede conseguir descargar estas herramientas de otros enlaces realizando una búsqueda en Internet.

3.7 Proceso de pruebas

Esta sección del documento muestra información de las pruebas realizadas, que dieron pie a las observaciones y recomendaciones para la implementación de la solución.

3.7.1 Captura de pantallas que muestran el funcionamiento de la solución

Imágenes que reflejan la puesta en marcha de la plataforma en el servidor de laboratorio. Se presentarán imágenes de los distintos procesos de usuario y administración de la plataforma.

Figura 3.33: Pantalla de acceso a usuario

Al acceder al servicio se mostrará la pantalla de ingreso para usuarios, donde se le solicita el nombre de usuario y contraseña (ver Figura 3.33), adicionalmente al tipo de versión que se desea utilizar.

Al ingresar al sistema se muestran los controles estándares para el manejo de mensajes de correo electrónico y las herramientas adicionales de que dispone la suite de Zimbra.

Figura 3.34: Pantalla de acceso para administración

Para ingresar como administrador se debe hacer uso de la Consola de Administración. Como curiosidad no dispone de variedad en las versiones de uso (ver Figura 3.34). A esta consola se accede utilizando el puerto 7071 (por defecto). Como apariencia inicial para los administradores, se muestra el estado de cada servicio.

3.7.2 Procesos de usuario

El usuario puede crear sus propios filtros de mensajes y decidir que hacer con los mismos (ver Figura 3.35).

La suite de Zimbra permite a su vez realizar cambios con la opción de preferencias, la cual es de suma importancia para los ajustes propios que cada usuario pueda efectuar (ver Figura 3.36).

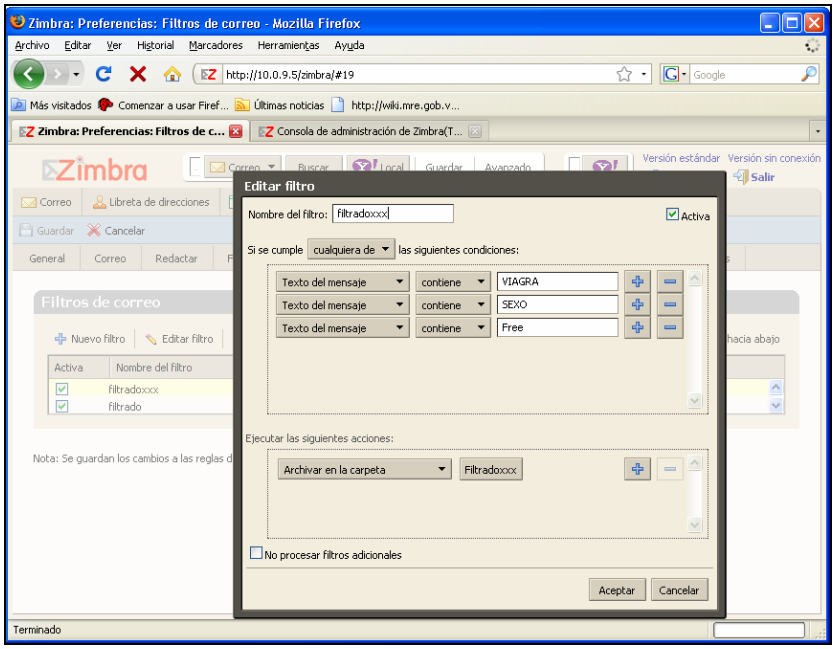

Figura 3.35: Adecuación de filtro según su contenido

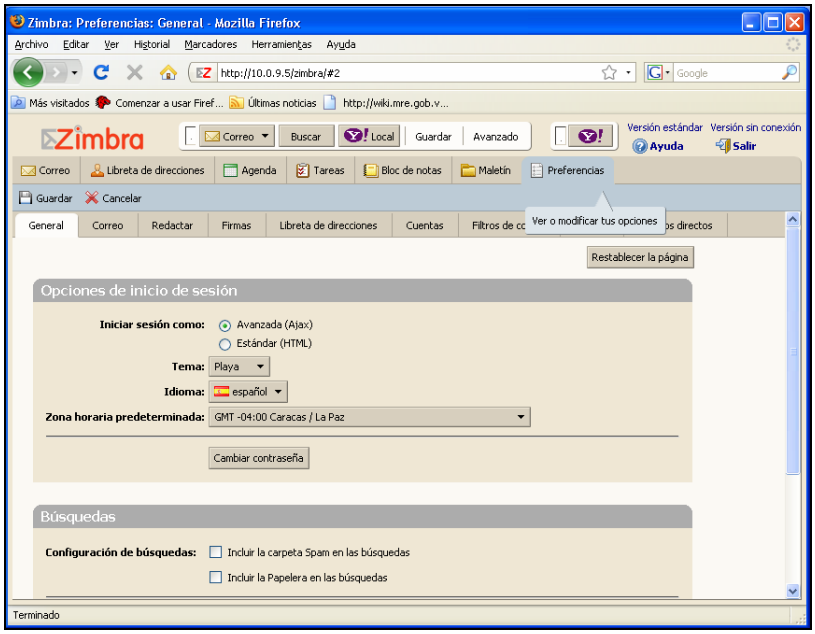

Figura 3.36: Opciones de preferencia

3.7.3 Procesos de administrador

Dentro de los procesos de adecuación de la plataforma (ver Figura 3.37 y Figura 3.38) se puede bloquear el envío y recepción de archivos adjuntos según su extensión, así como el uso de listas negras alternativas.

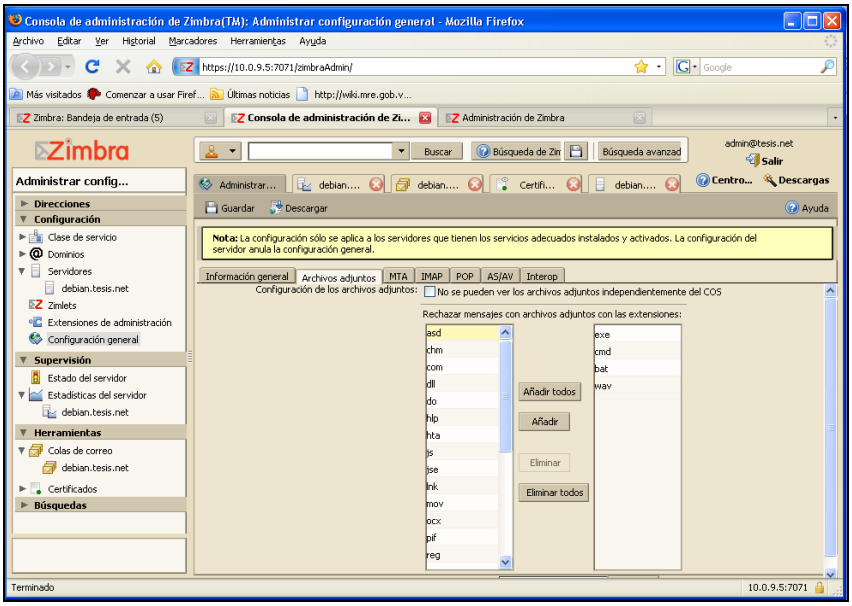

Figura 3.37: Bloqueo de adjuntos

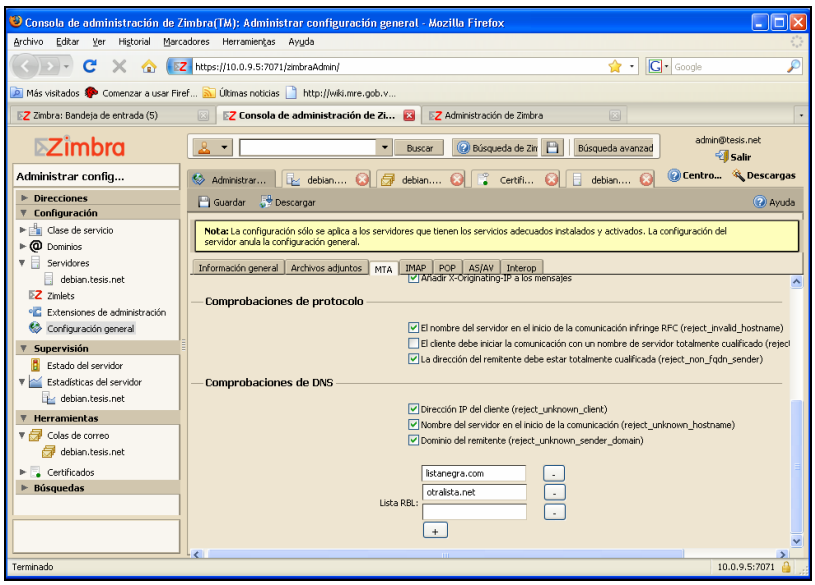

Figura 3.38: Parametrización de listas negras

3.7.4 Bombardeo de spam y virus a la solución

En esta sección se mostrará los resultados y los distintos análisis de las pruebas efectuadas a la plataforma de pruebas.

Herramienta de envío múltiple de e-mail

La herramienta utilizada para el envío masivo de mensajes al sistema de pruebas se llama Multi Mail (ver Figura 3.39), que permite agregar el cuerpo del mensaje en un archivo de texto y además permite adjuntar archivos en varios formatos.

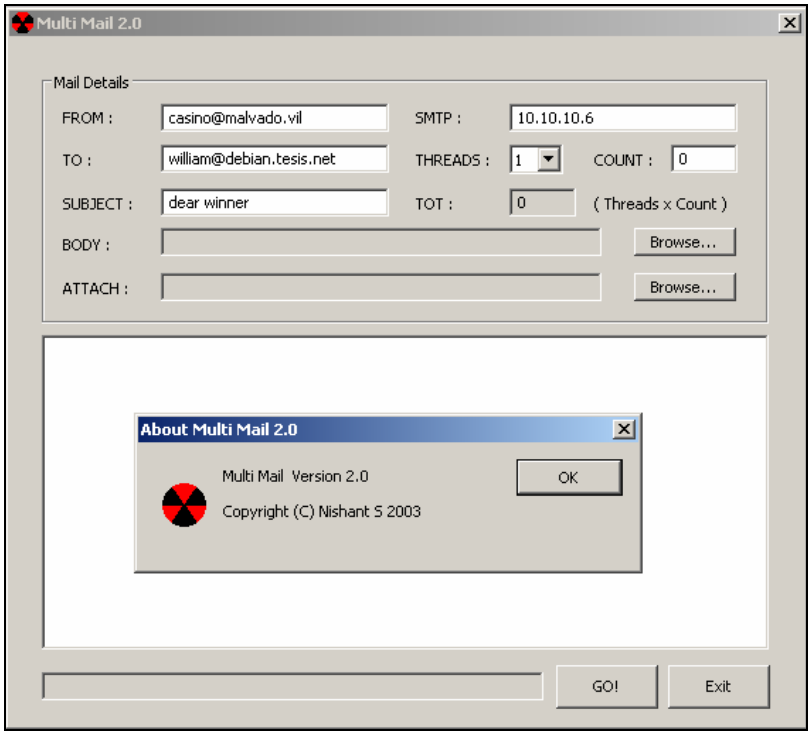

Figura 3.39: Herramienta de bombardeo de mensajes

Detección de mensajes con adjuntos de virus

Se envió un mensaje con la firma del virus eicar el cual fue detectado por la plataforma (ver Figura 3.40).

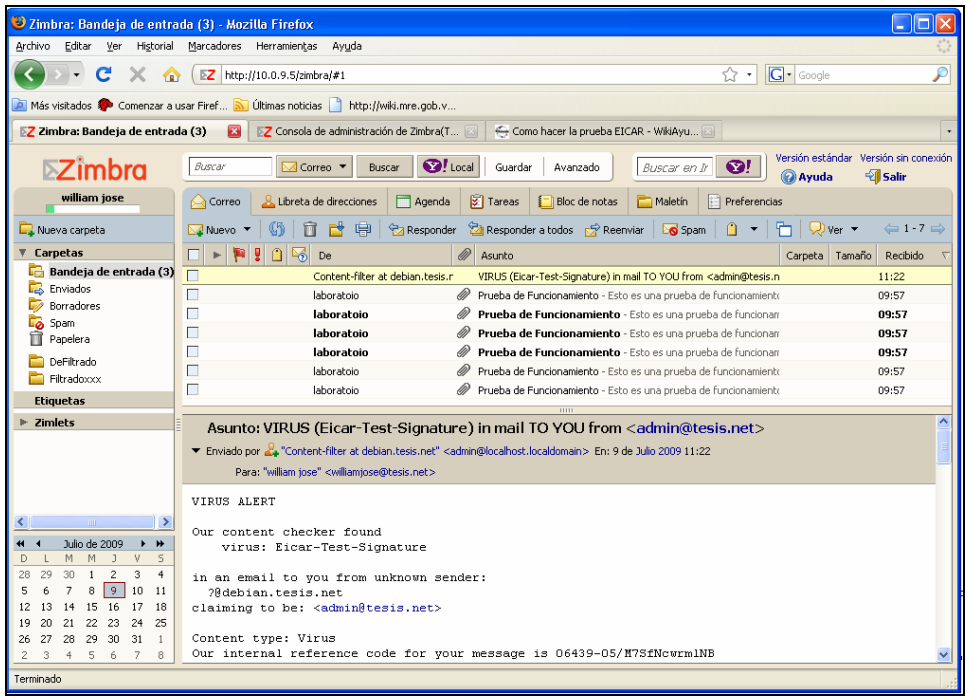

Figura 3.40: Detección de virus eicar

Enviando muchos mensajes y catalogándolos como spam

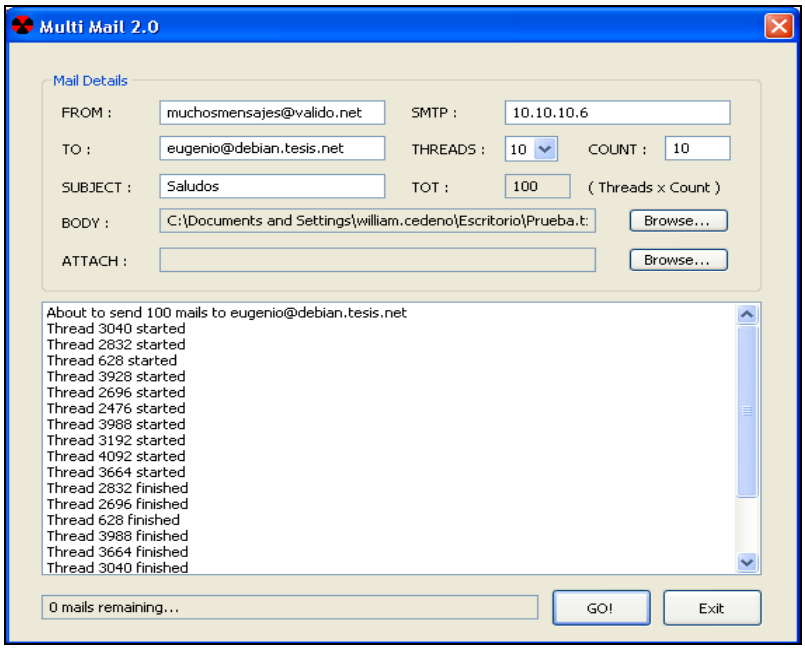

Figura 3.41: Envío de mensajes

Se enviaron 100 correos (ver Figura 3.41) a un usuario registrado, y se observó la puntuación dada a uno de esos mensajes (ver Figura 3.42) la cual resulto ser de 0,375 haciendo match con tres reglas antispam. La regla BAYES_50=0,001 produjo ese resultado porque aún no se han catalogado mensajes como spam.

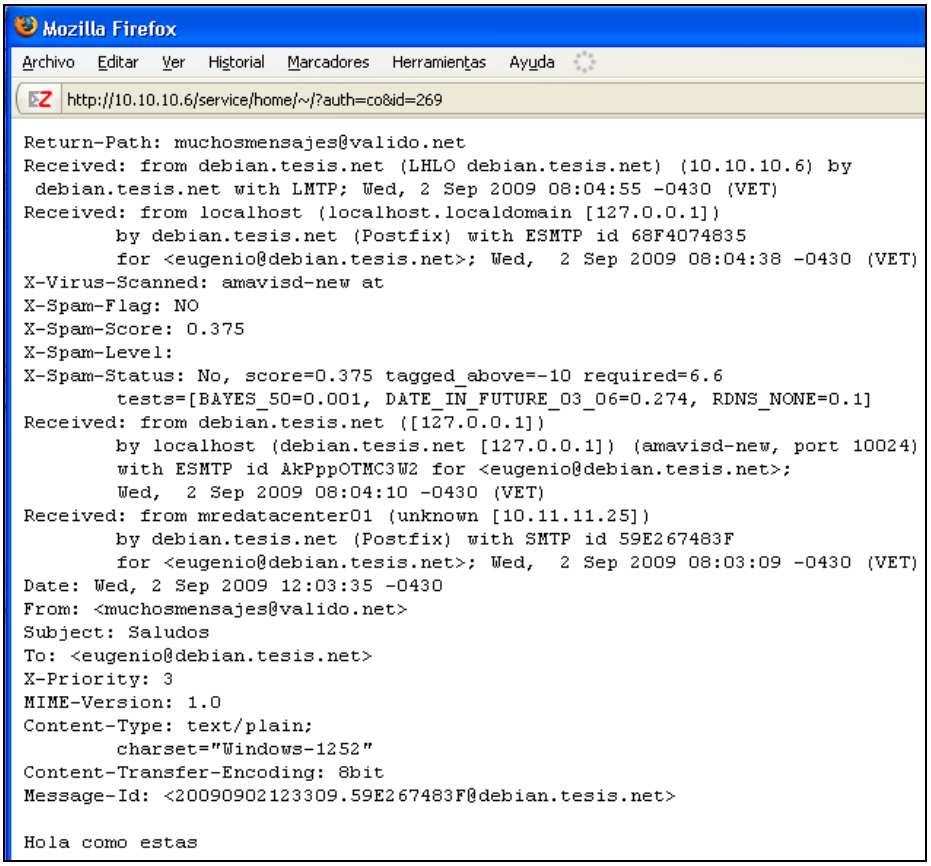

Figura 3.42: Cabecera de mensaje antes de ser catalogado spam

Luego se catalogaron como spam a 10 de estos mensajes y se ejecutó por consola el comando *zmtrainza* (ver Figura 3.43) bajo el usuario zimbra, lo cual generó la activación de los algoritmos de aprendizaje bayesiano.

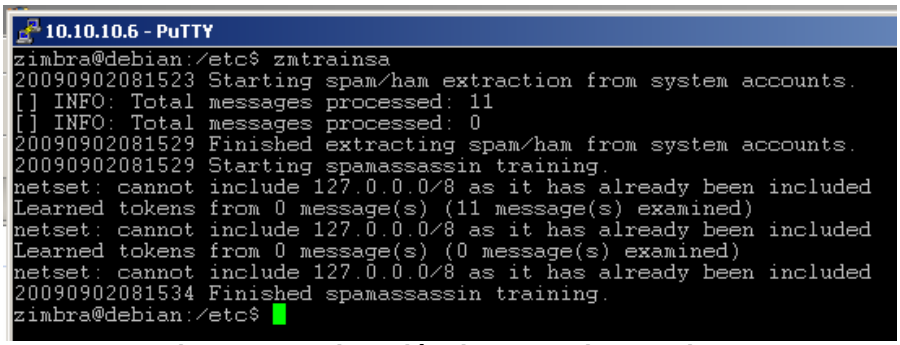

Figura 3.43: Ejecución de comando zmtrainza

Figura 3.44: Cabecera de mensaje catalogado como spam

Luego de haber ejecutado de forma manual el comando *zmtrainza*, (este se ejecuta en forma automática a una hora preestablecida), se enviaron nuevamente varios mensajes con el mismo cuerpo y el mismo remitente. Al observar la cabecera (ver Figura 3.44) de uno de estos mensajes, se observó que la regla BAYES_50 no existe pero sí la BAYES_99 que generó una puntuación bastante elevada (3,5).

Figura 3.45: Cabecera de mensaje catalogado como spam

Se enviaron nuevos mensajes sin modificar el cuerpo ni el remitente del mismo y al ser recibidos se catalogaron varios de ellos como spam. Se ejecutó nuevamente el comando *zmtrainza* y al realizar una revisión de la cabecera de uno de los mensajes se pudo observar que el puntaje subió de 2,3 a 3,012 (ver Figura 3.45). Pero hay que hacer la observación que la regla BAYES_99 no

varía pero la prueba AWL sí, pasando de -1,441 a -0,862 lo cual sí incide notablemente el valor del puntaje final. AWL (Auto White List) es una prueba que coloca automáticamente a la dirección del remitente en listas blancas y varía su puntaje si lo catalogan como spam.

Enviando mensajes con cuerpos de spam

Para esta prueba se editó un archivo de texto donde se agregaron palabras asociadas a un spam como "Mortgage", "Viagra" o "Penis Enlargement", además de colocar en el sujeto la palabra "Dear o Winner" y se enviaron 25 mensajes como se muestra en la Figura 3.46.

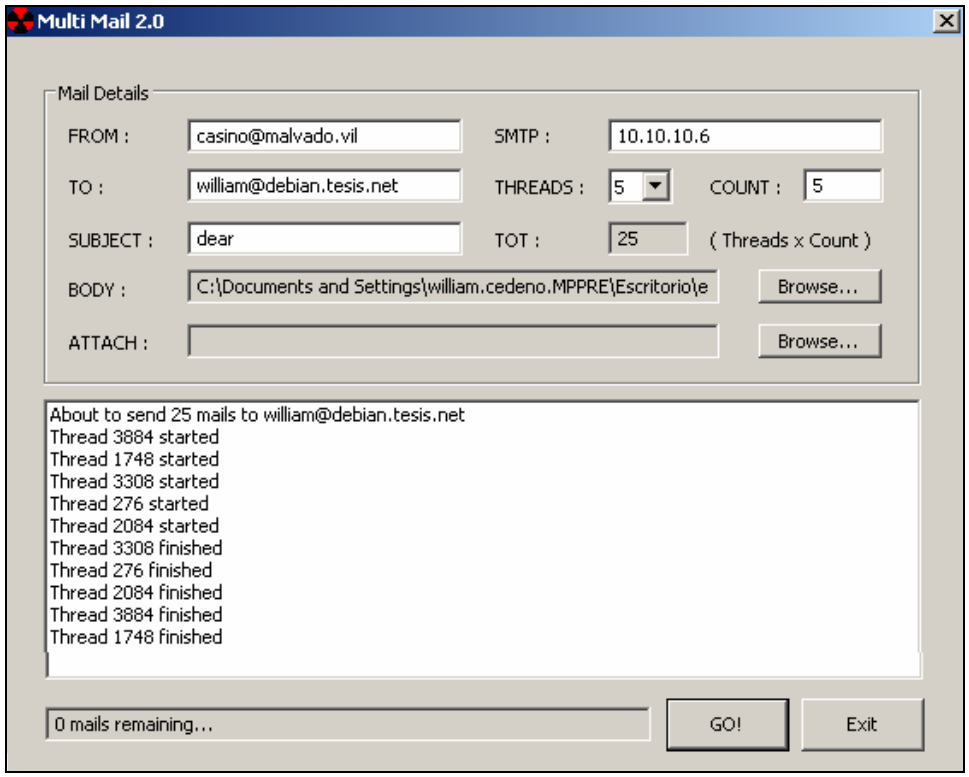

Figura 3.46: Envío de mensaje desde casino@malvado.vil

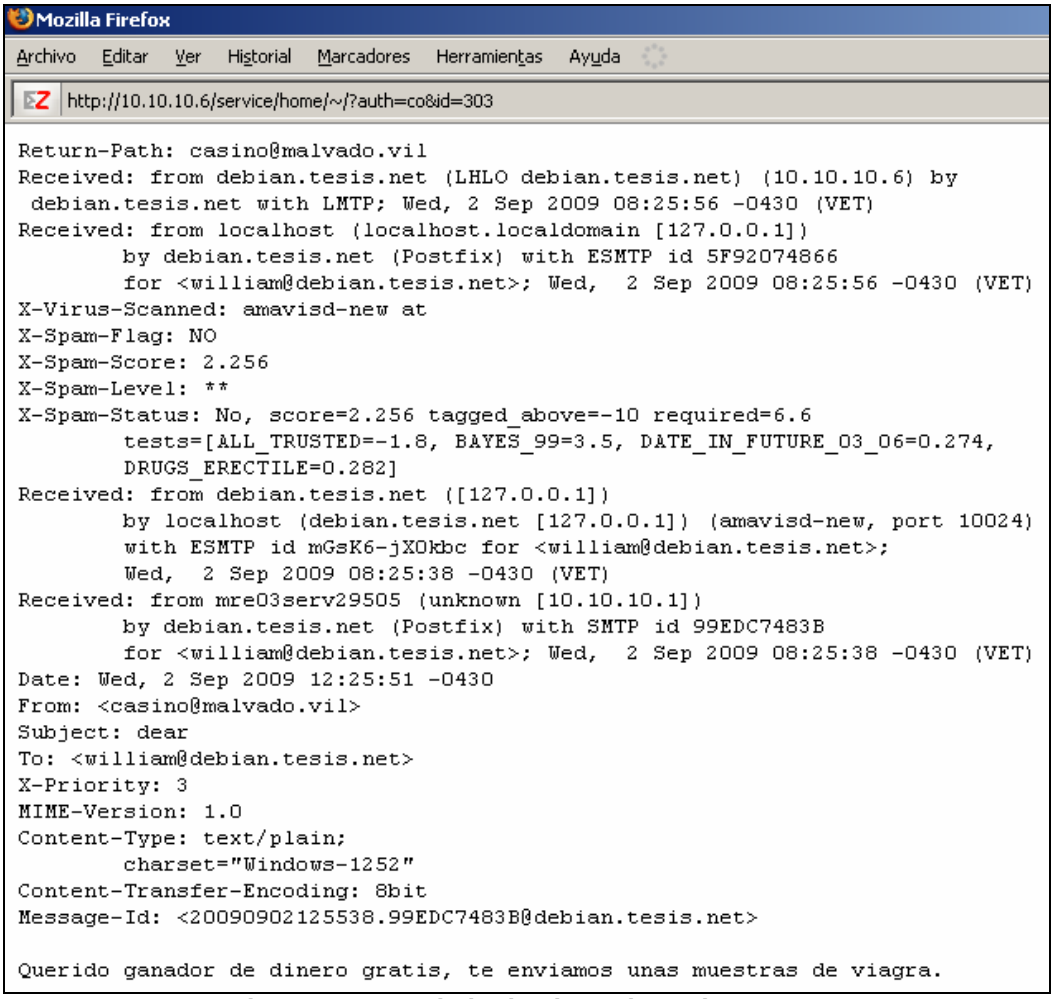

Figura 3.47: Enviado desde casino primera vez

Se observa que la suma (2,256) del peso asociado a los valores de las reglas no superan el umbral (required=6,6) para etiquetar el mensaje como spam (ver Figura 3.47), así que se catalogaron 15 de estos mensajes como spam, se agregaron más palabras que hacen tender el mensaje hacia un spam y se ejecutó el comando *zmtrainza*.

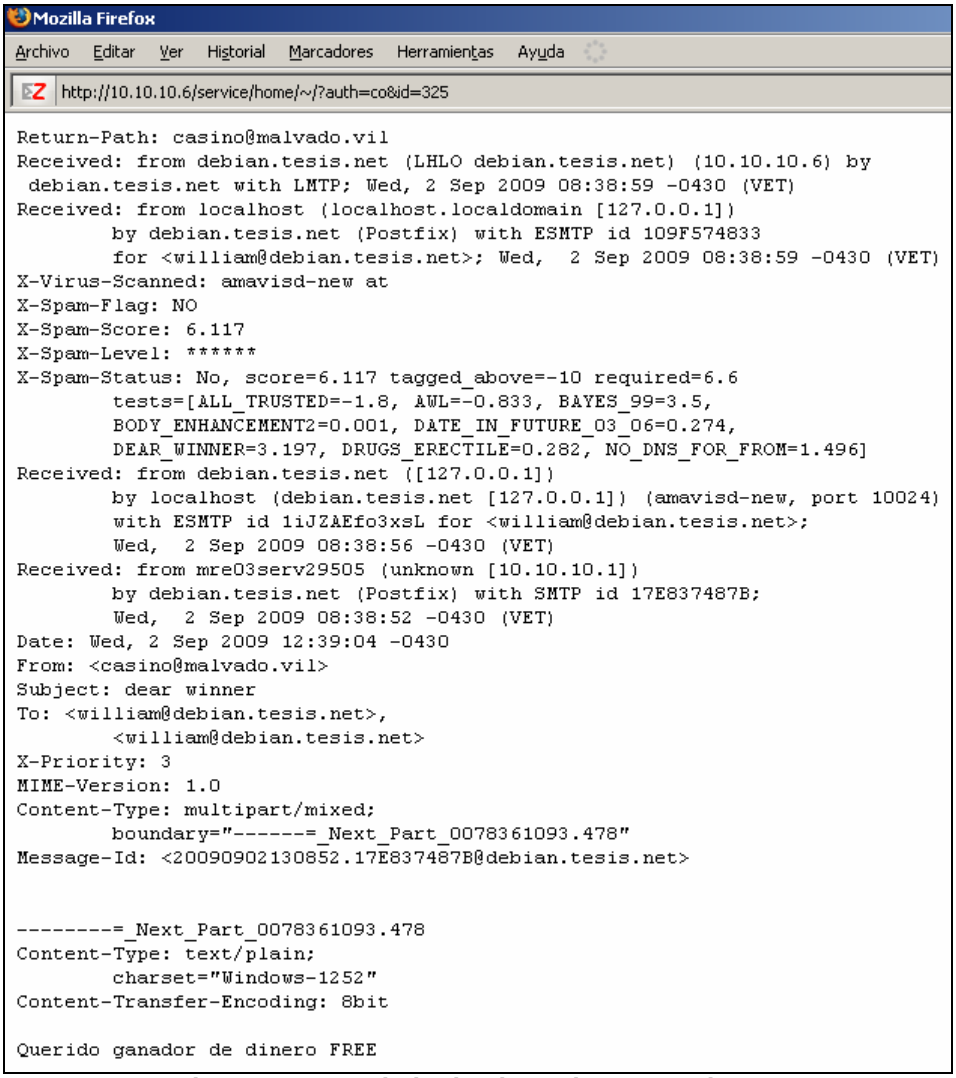

Figura 3.48: Enviado desde casino segunda vez

En esta parte se observa que la regla DEAR_WINNER=3,197 hace incrementar hasta 6,117 el valor asociado al mensaje, acercándolo al umbral cada vez más (ver Figura 3.48).

Para mostrar los cambios de un mensaje etiquetado como spam, se disminuyó el umbral de 6,6 a 5,5 (de 33 a 25 en consola gráfica de administrador) y se enviaron nuevos mensajes con el mismo cuerpo y el mismo sujeto.

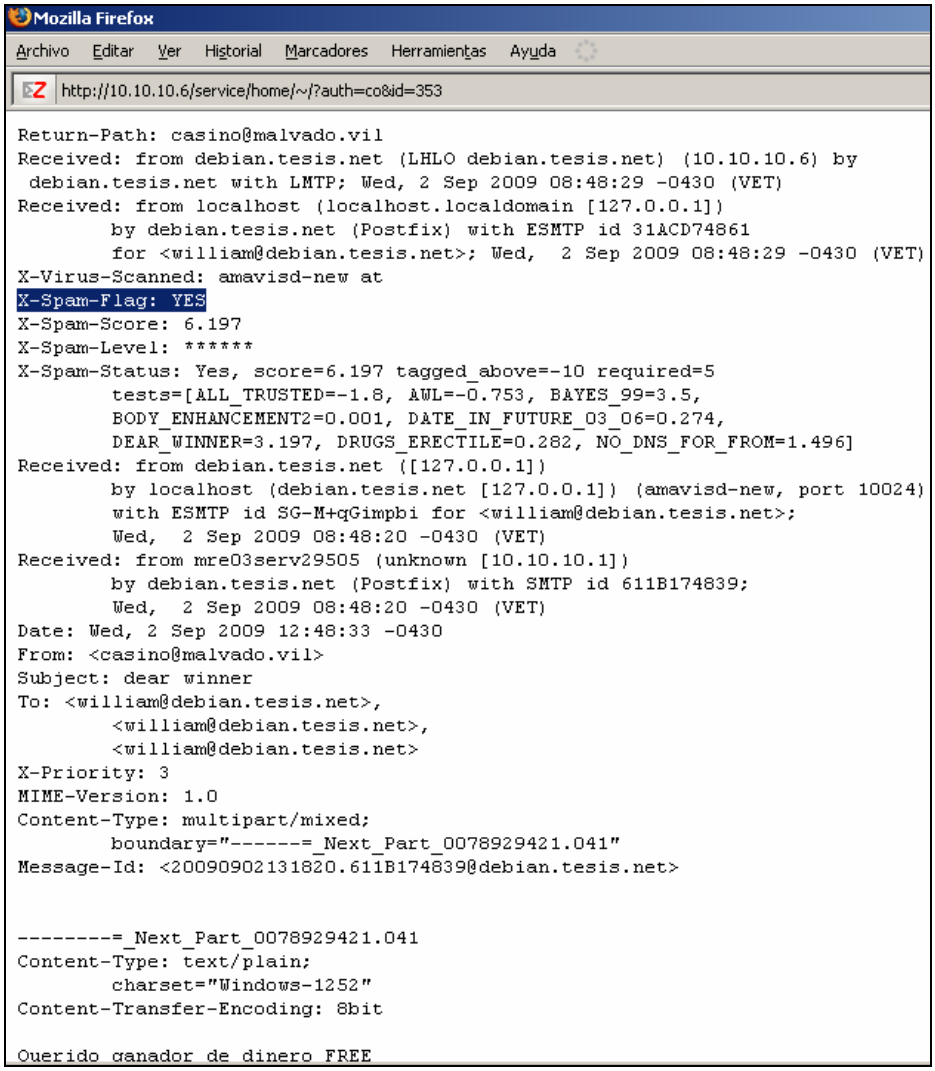

Figura 3.49: Mensaje etiquetado como spam

En esta ocasión se observa en la línea sombreada **X-Spam-Flag: YES** indicando que el mensaje presuntamente es un spam. Además este mensaje es llevado a la carpeta spam del buzón del usuario (ver Figura 3.49)

Mensajes catalogado por los usuarios como spam

Existe una cuenta de apoyo a la administración llamada spam.vtwptyvl donde se reciben todas las alertas de posibles spam hechas por los usuarios (ver Figura 3.50). El nombre de esta cuenta varía pero siempre comienza por spam.<aleatorio>

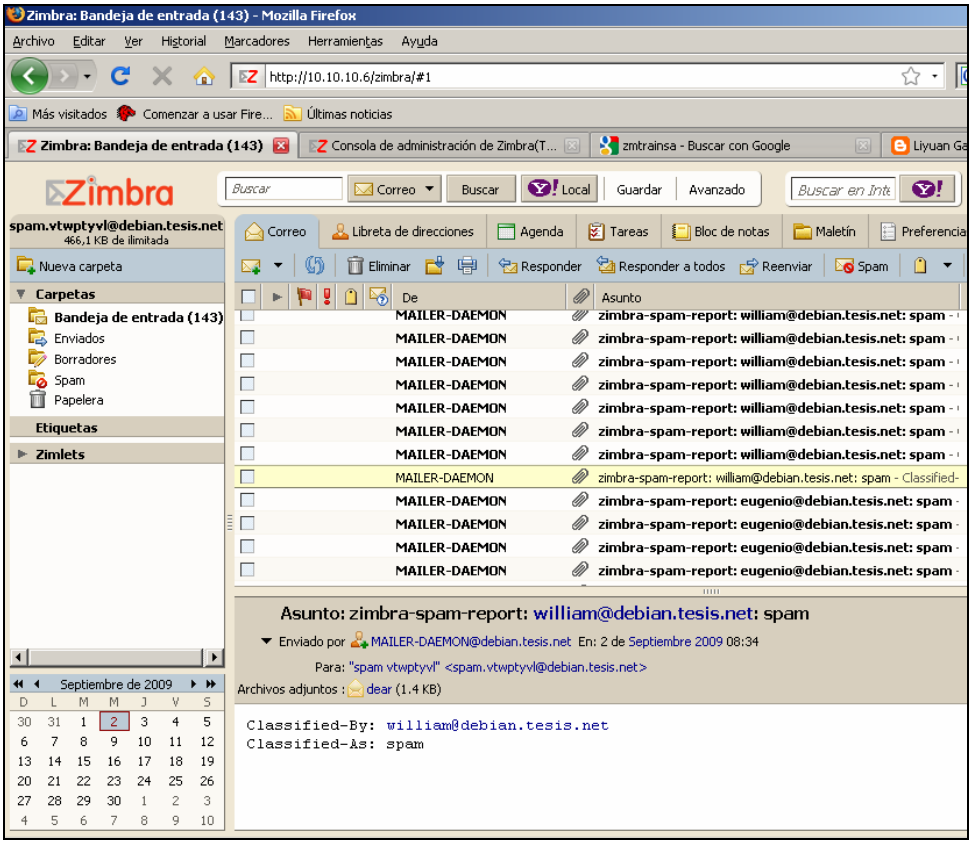

Figura 3.50: Buzón de la cuenta spam.vtwptyvl

3.8 Observaciones

Más que observaciones a la solución propuesta, en esta sección se pretende analizar ciertos ítems que dan comprensión a preguntas planteadas en una plataforma de esta índole.

3.8.1 Modificar reglas y valores

Cuando existe la necesidad de escribir o modificar reglas de filtrado específicas o valores asociados a un regla para spamassassin, además de las que trae por defecto, se puede acceder al directorio /usr/share/spamassassin, en el cual hay una serie de archivos que empiezan por un número de dos dígitos (*10_misc.cf, 20_advance_fee.cf, 20_antiratware.cf*, etc). Estos archivos almacenan la configuración de las reglas de filtrado y el número del nombre del archivo indica el orden en que se aplicarán.

Para añadir nuevas reglas se crea un nuevo archivo, por ejemplo, "*90_reglas.cf*", y se añade contenido como el de la Figura 3.51.

```
body CASINO /casino|casion|online/i
describe CASINO casinos
score CASINO 7.0
```

Figura 3.51: Nueva regla spamassassin

Esta regla está compuesta por tres campos, que se describen como:

- *body*: Describe que palabras claves provocarán la identificación del correo como spam.
- *describe*: Establece una identificación de la regla.
- *score*: Indica la puntuación que debe darle al mensaje identificado.

También se observa que entre la palabra clave del inicio de línea y el valor, hay un identificador (en este caso: CASINO). Este identificador es el nombre de la regla. El empleo de este identificador se debe a que en el mismo archivo se pueden especificar varias reglas para identificar mensajes de distinta índole, por lo que la forma que tiene spamassassin de identificar cada regla es asignándole este nombre.

La línea que define la regla (body) contiene una expresión regular para identificar palabras clave (/casino|casion|online/i). Dichas expresiones tienen siempre la misma estructura (/<expresión regular>/i), donde <expresión regular> es la expresión regular diseñada para identificar un mensaje como spam. La “i” del final se coloca cuando se desee que la expresión regular no haga distinciones entre mayúsculas y minúsculas (*case insensitive*).

3.8.2 Modificación de umbrales

Zimbra trae una configuración por defecto en spamassassin que puede o no ser la adecuada. Para entender mejor estos parámetros, se observa un mensaje (ver Figura 3.52) que ha sido analizado por spamassassin.

```
X-Spam-Flag: YES
X-Spam-Score: 10.565
X-Spam-Level: **********
X-Spam-Status: Yes, score=10.565 tagged_above=-10 required=4
tests=[BAYES_99=3.5, FH_HOST_ALMOST_IP=1.751, RCVD_IN_PBL=0.905,
RCVD_IN_SORBS_DUL=0.877, RCVD_IN_XBL=2.033, URIBL_SBL=1.499]
```

Figura 3.52: Cabecera de mensaje

Este mail ha sido detectado como spam porque ha recibido una puntuación de 10,565. Dado que esta puntuación es mayor que required=4 se marca como spam. Las pruebas [17] que ha hecho spamassassin para detectar que esto es una spam son:

- BAYES_99.
- FH_HOST_ALMOST_IP.

[17] http://spamassassin.apache.org/tests_3_0_x.html

- RCVD_IN_PBL.
- RCVD_IN_SORBS_DUL.
- RCVD_IN_XBL.
- URIBL_SBL.

Si un correo es marcado (detectado) como spam existen cuatro (4) posibilidades:

- Usar el webmail del usuario, entrar a la carpeta (Basura o Junk o Spam), seleccionar el correo detectado como basura y pulsar sobre el botón “No basura”.
- Modificar los parámetros (ver Figura 3.53) generales para especificar la puntuación mínima para un spam, ejecutando “./zmprov gacf” o en la consola web de administración de zimbra. El SpamTag define cuando un correo es considerado spam y el SpamKill cuando debe eliminarse directamente. En el ejemplo anterior son necesarios 4 puntos para marcar el correo como spam. Este valor sale de: ZimbraSpamTagPercent (20% = 20 * 0,2) = 4. Por el otro lado se tiene que 15 son los puntos necesarios para eliminar el correo: ZimbraSpamKillPercent (75% = 75 * 0,2) = 15

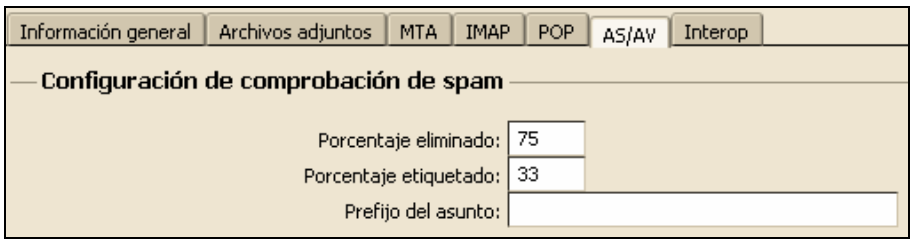

Figura 3.53: Parámetros de puntuación

- Modificar los valores para las diferentes pruebas que hace el spamassassin dependiendo de las necesidades. Para ello se necesita saber que valores cambiar y que es lo que hace esta prueba para recibir ese valor.
- Añadir al remitente a una lista blanca. Para ello hay que meter al dominio dentro del archivo */opt/zimbra/conf/spamassessin/60_whitelist.cf* añadiendo al final del archivo la línea “whitelist_from_rcvd *@*.dominio dominio” y reiniciar Zimbra (o reiniciar el Amavis).

3.8.3 Variar el lenguaje de la plataforma

Dentro del webmail del cliente existe la opción para cambiar el idioma de la interfaz de acuerdo con las preferencias del usuario; esto facilita el uso del sistema a usuarios que no dominen determinados idiomas y se pueden cambiar al de su origen. Si este usuario tiene privilegios de administrador el cambio de idioma afectará a su vez la interfaz de administración (sólo para ese usuario).

Para realizar este proceso se hace clic en preferencias para acceder a las opciones que permiten entre otras modificar el idioma (ver Figura 3.54).

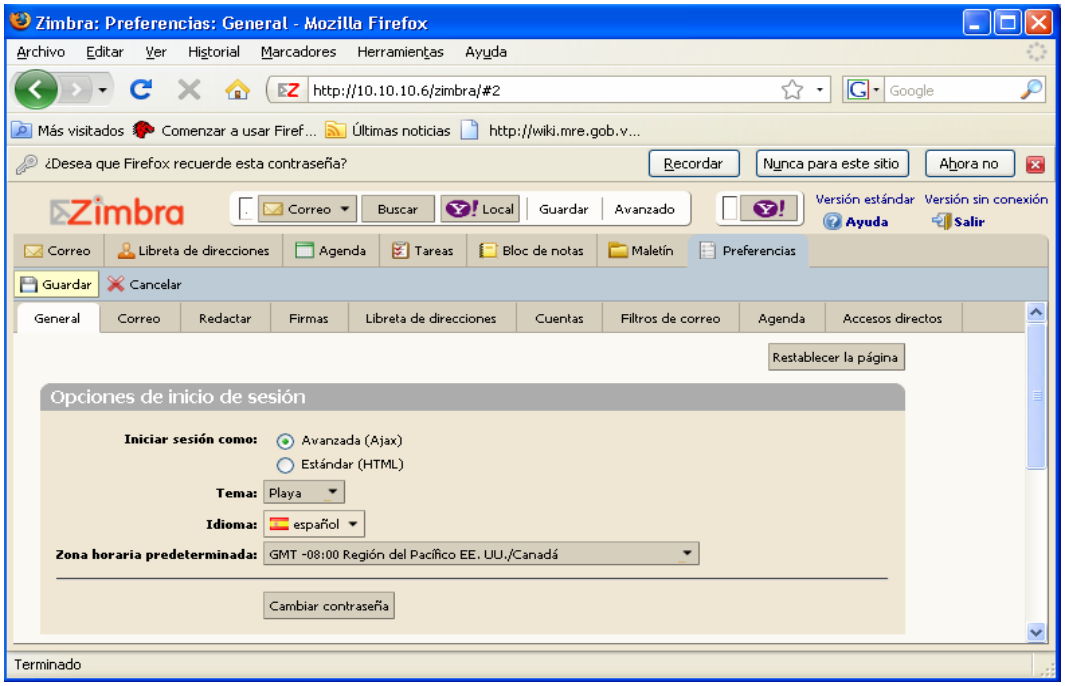

Figura 3.54: Opciones para preferencias de usuario

Luego se hace clic en el botón de idiomas y se despliega una lista de los idiomas disponibles en el sistema, se selecciona el idioma que se desee, se hace clic en guardar y listo (ver Figura 3.55).

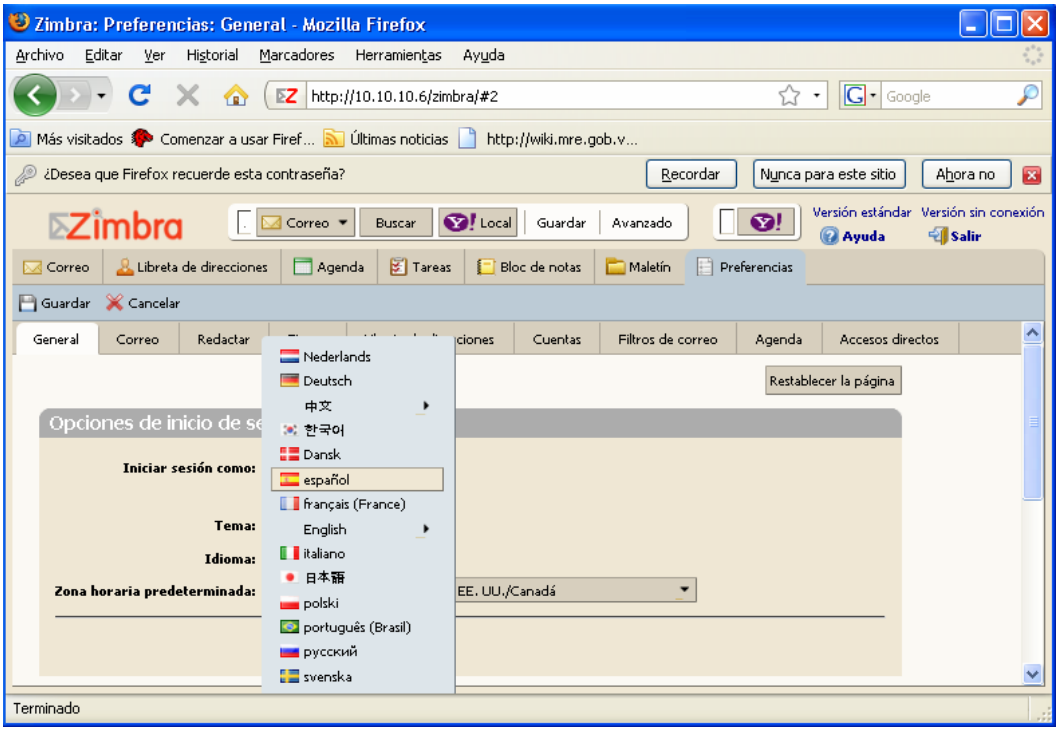

Figura 3.55: Selección y cambio del idioma

3.8.4 El usuario puede crear sus propios filtros

Además del filtro de mensajes que posee Zimbra, cada usuario del correo puede crear sus propios filtros para que sean marcados como spam sin necesidad de acudir al administrador del sistema, y así contribuye a combatir el spam.

3.8.5 Funciona en versiones particulares de Linux

La versión de servidor y cliente de código abierto Zimbra, está disponible en la mayoría de distribuciones de Linux como Red Hat Enterprise, Red Hat Fedora, Debian, openSuse, Ubuntu y para MacOS Tiger y Leopard. Sin embargo, para algunas distribuciones en particular no en tan trivial la implementación.

Para Windows y Apple, sólo está disponible la versión cliente llamada Zimbra Desktop, capaz de gestionar correos de la web al estilo del Outlook o del Thunderbird, con entornos gráficos más amigables y con la capacidad de sincronización con calendarios.

3.8.6 Variar la zona horaria por perfil de usuario

Cada región o país tiene asignada una zona horaria de acuerdo al tratado internacional en materia de husos horarios. Zimbra les permite a los usuarios configurar su cliente de correo de acuerdo con la región o país donde se encuentra, de manera de estar actualizado con la fecha y hora. Todo usuario puede acceder al cambio de zona horaria seleccionando preferencias (ver

Figura 3.54), hacer clic en la opción zona horaria predeterminada lo cual permite que se despliegue una lista de las zonas horarias oficiales a nivel mundial, y por último hacer clic en la zona horaria requerida (ver Figura 3.56)

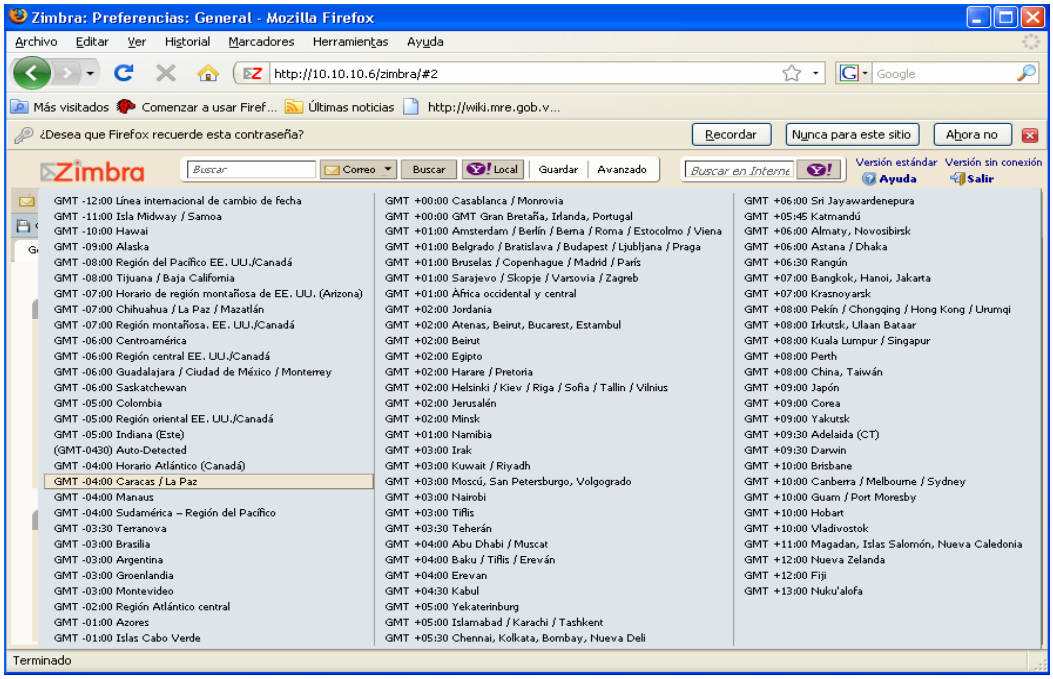

Figura 3.56: Selección de una zona horaria

3.8.7 El lenguaje de las reglas predeterminadas

Los archivos que almacenan las distintas reglas para determinar si un mensaje es spam o no, están diseñados con frases, palabras y términos en el idioma inglés, lo cual implica que se deben modificar para agregarles frases, palabras y términos en otros idiomas, para asegurar que cualquier mensaje spam en diferentes idiomas pueda ser detectado o simplemente se pueden crear nuevos archivos de reglas para el idioma que se desee, lo cual permite al spamassassin tener más opciones a la hora de analizar mensajes.

3.8.8 Existe una versión comercial

La comunidad de código libre desarrollo el proyecto Zimbra, con miras a suplir las necesidades del servicio de correo electrónico y con mejoras que lo hagan competitivo con las aplicaciones existentes Microsoft Exchange, Groupwise y Lotus Notes.

Este proyecto fue adquirido por Yahoo en el 2007 y a pesar de ser un código libre para la modificación, debe guiarse bajo los términos de su licencia. Existe una versión de la comunidad de código abierto (Open Source) y otra comercial (Zimbra Network) la cual incluye toda una serie de características añadidas respecto de la Open Source, como la alta disponibilidad mediante clustering y journaling a nivel de aplicación, las copias de seguridad incrementales y

completas con restauración detallada (hasta el nivel de un correo electrónico de una cuenta específica, todo desde la consola gráfica de administración) o el archivado de correos entrantes y salientes (para su posterior consulta o por requerimientos legales) mediante Zimbra Archiving and Discovery.

Otras características que también son exclusivas de su Network Edition son la gestión nativa de la jerarquía de almacenamiento, que le permite mover datos de una cierta antigüedad a otros volúmenes de datos para presentarlos en conjunto al usuario. Esto permite la clásica configuración de discos SCSI como almacenamiento principal y discos SATA (más lentos pero también más baratos) como almacenamiento secundario, o configuraciones con SAN (Storage Area Network) o NAS (Network Attached Storage) de ambos tipos de discos.

Respecto del soporte para múltiples dominios, en su versión Network Edition, Zimbra permite la personalización de los logos y textos para cada dominio, así como usuarios administradores diferentes para cada dominio (y usuarios superadministrador) para gestionar el servidor completo.

Gracias a Zimbra Mobile, ZCS consigue la conexión con dispositivos móviles sin cables (bien a través del carrier de telefonía, bien a través de Wi-Fi). Soporta los protocolos Active Sync de Windows y Palm, iSync de Apple y SyncML de Symbian. Otras herramientas como Sync4j/Funambol permiten expandir aun más este tipo de integraciones. Para BlackBerry, Zimbra proporciona un conector para BlackBerry Enterprise Server (BES) que se instala en el servidor y permite la afamada sincronización bidireccional a través del carrier de telefonía móvil.

Hablando de más integraciones, Zimbra proporciona sendos conectores para Outlook de Microsoft e iMail de Apple, con los que se consigue una integración completa y transparente con el servidor. Evolution también tiene un conector, en este caso gratuito.

Finalmente, mediante el uso de Verity, Zimbra Network Edition es capaz de convertir prácticamente cualquier adjunto de correo en HTML y mostrarlo en el mismo cliente web de correo. De este modo es posible evitar la dependencia en aplicaciones externas que pueden o no estar instaladas en el sistema.

3.8.9 Migración desde otras plataformas

La plataforma hace uso de los protocolos más comunes de entrega y recepción de mensaje como son:

- SMTP (Simple Mail Transfer Protocol): se utiliza para que dos servidores de correo intercambien mensajes.
- POP (Post Office Protocol): Se utiliza para obtener los mensajes guardados en el servidor y pasárselos al usuario.
- IMAP (Internet Message Access Protocol): También se usa para interacción del usuario con el servidor.

La migración de buzones desde otras plataformas a la suite de Zimbra es muy sencilla. A su vez en la página de Zimbra existe documentación y herramientas de apoyo para la migración de buzones de otras plataformas de correo electrónico.

3.8.10 Detección de spam vía imágenes

Los spammers además de utilizar texto para distribuir sus mensajes están haciendo uso de imágenes, lo cual hace que no sea fácil detectar si un mensaje es o no spam, si el contenido de la información forma parte de una imagen.

Dado este caso, se han desarrollado técnicas y aplicaciones para que spamassassin pueda ser capaz de analizar las imágenes contenidas en los mensajes, extraer el texto en caso de tenerlo y luego aplicar las reglas de filtrado a dicho texto para poder determinar si es spam o no.

Un ejemplo de estas aplicaciones son los plugins ImageInfo y FuzzyOCR; estas aplicaciones realizan un escaneo de la imagen y convierten en texto los distintos caracteres que se detecten en la imagen luego son guardados en un archivo de texto para ser analizado por spamassassin.

4. Trabajos Relacionados

4.1 Trabajo # 1

4.1.1 Identificación

Institución: Universidad Central de Venezuela, Facultad de Ciencias, Escuela de Computación

Tutor: Prof. Eric Gamess

Autor: Alejandro Enrique Brito Monedero

Titulo: Implementación de un Sistema para el Manejo de Correo Electrónico con Autenticación Centralizada Basada en Servicios de Directorio

Año de presentación: Caracas, Noviembre 2007

4.1.2 Objetivos y Resultados

El objetivo de este trabajo fue proponer una solución que permitiera tener un sistema de correo electrónico, tomando en cuenta criterios como el fácil acceso desde lugares remotos, la seguridad, el control centralizado de los usuarios y el filtrado de mensajes no deseados. La propuesta hace uso de las herramientas de Postfix, Dovecot y OpenLDAP, bajo software libre.

En este trabajo se hace hincapié en un servicio de directorio LDAP, que permita manejar de manera centralizada la autenticación de los usuarios. En comparación con la propuesta de este documento, tiene cierta similitud en la utilización de un servicio de directorio, así como del MTA utilizado. Pero no profundizan en el enfoque central de esta TEG acerca del tratamiento del spam. Sin embargo el producto de ambos conlleva a las mejores prácticas.

4.2 Trabajo # 2

4.2.1 Identificación

Institución: Universidad Central de Venezuela, Facultad de Ciencias, Escuela de Computación

Tutor: Prof. Carlos Alfonso Acosta

Autor: Br. Dedaniel Renaud Urribarrí

Titulo: Conjunto de Lineamientos para el Desarrollo de una Intranet Segura

Año de presentación: Caracas, Mayo 2004

4.2.2 Objetivos y Resultados

Este trabajo esta basado en un estudio extenso de las vulnerabilidades de las redes en todos sus niveles (desde la capa física hasta la capa de aplicación según el modelo OSI) y sobre todo de la tendencia actual de desarrollo de aplicaciones sobre Internet basado en intranets; proponiendo un conjunto de lineamientos generales para el diseño, desarrollo, implantación y administración de intranets seguras.

A pesar de que este trabajo no parece tener similitud alguna con esta TEG, se puede tomar el enfoque y lineamientos de seguridad propuestos en él, porque existen ataques, herramientas y técnicas que son empíricas y de uso común, ya que las usan tanto los especialistas como los hackers.

En este trabajo se demostró como una conjunción de elementos denominados políticas, estándares, lineamientos, reglas, técnicas y herramientas incrementan efectivamente el nivel de seguridad de una red. En la propuesta de esta TEG reflejada en el capítulo 3 se aprecia la importancia de las normas y políticas de uso del correo, así como la escogencia de una buena topología de conexión. Por esto se hace referencia a este trabajo como propuesta importante a la hora de implementar soluciones que requieran lineamientos y políticas de uso de los servicios.

4.3 Trabajo # 3

4.3.1 Identificación

Institución: Universidad EAFIT, Departamento de Informática y Sistemas, Medellín

Tutor: Prof. Juan Guillermo Lalinde Pulido

Autor: Diana Cristina López Toro, John Edgar Congote Calle

Titulo: Spam en el Correo Electrónico

Año de presentación: Medellín, 2006

4.3.2 Objetivos y Resultados

Dentro de los objetivos buscados por este trabajo están:

- Consultar los adelantos e innovaciones en el tema, que se han hecho hasta el momento en institutos y entidades competentes tales como IEEE, ACM, OCDE, entre otras.
- Conocer el funcionamiento de algunos programas diseñados en los últimos años para la detección de correo basura, así como establecer las principales características y diferencias entre ellos.

- Investigar y estudiar los fundamentos de las diferentes acciones legales que se están tomando en diferentes países para atacar el problema.
- Identificar cuales son aquellos puntos donde los spammers logran que sus ataques sean exitosos, para así poder detectar los aspectos en los que estamos fallando los usuarios y generar recomendaciones y sugerir buenas prácticas para evitar en la medida de lo posible ser víctimas del spam y enfrentar el problema.

Este trabajo toca un aspecto fundamental que fue expuesto en el marco teórico de esta TEG, el cual se refiere a la formación del usuario final en contra del spam. Sin embargo no existe una formula mágica para erradicar el problema, se requiere la persecución agresiva del spam en todos los frentes estudiados, tales como innovación tecnológica, cooperación con la industria, educación al usuario final del correo, una legislación efectiva, ejecución de la ley focalizada, etc.

Este trabajo puede dar pie al impulso para la implementación de una ley en materia de protección de datos dentro del contexto del combate contra el spam.

4.4 Trabajo # 4

4.4.1 Identificación

Institución: Centro de Investigación y de Estudios Avanzados del Instituto Politécnico Nacional de México, Departamento de Ingeniería Eléctrica, Sección de Computación.

Tutor: Dr. Arturo Díaz Pérez

Prof. Juan Guillermo Lalinde Pulido

Autor: Francisco Javier Alejandro Lagunes

Titulo: Sistema de análisis y filtraje de correo masivo no solicitado spam

Año de presentación: México, Julio 2005

4.4.2 Objetivos y Resultados

Este trabajo presenta el desarrollo de un filtro inteligente para la detección y eliminación de correo spam. Este filtro esta construido por un conjunto de reglas deterministas y heurísticas así como un análisis estadístico.

Las reglas deterministas rechazan correos cuyo emisor ha sido previamente identificado como fuente de correo spam. Pero aceptan inmediatamente correos cuya fuente ha sido validada por el usuario. Las reglas heurísticas analizan el tema y cuerpo de un mensaje mediante la identificación de palabras o frases consideradas como características de correo spam. Finalmente, el análisis estadístico, basado en el teorema de Bayes, calcula la probabilidad de que las frases de cierto tamaño de un cierto mensaje pertenezcan a un mensaje tipo

spam. Posteriormente se realiza un cálculo de probabilidad de que el correo sea spam.

Como se puede observar este trabajo tiene mucha similitud con el tema más importante de la TEG, a pesar de que no se hace una propuesta integral para el servicio de correo electrónico.

De temas como este se desprende la idea de proponer la creación de reglas de filtrado de spam en los distintos lenguajes y formas de expresión verbal existentes en el planeta, a pesar de que las mayores fuentes de envío de spam provienen de países de habla inglesa y países asiáticos.

5. Conclusiones

Contar con las políticas adecuadas desde el principio, es fundamental a la hora de prestar un servicio. Las normas y procedimientos son la base fundamental del buen funcionamiento de una organización.

Más allá de justificar en un decreto el uso de software de dominio público, se manifiesta cada vez más la robustez de Linux y las herramientas que en conjunto ayudan en la disminución del spam.

Lo que está claro es que el servicio de e-mail es muy útil y merece la pena utilizarlo, pero habría que replantearlo para adaptarlo a la problemática del correo basura. Sin embargo, el spam está costando a todos mucho tiempo y dinero, además de menguar la utilidad y credibilidad del servicio de correo electrónico como medio de comunicación entre personas.

Por otra parte, es importante señalar que existe una gran variedad de herramientas que apoyan la lucha contra el spam, pero es potestad del usuario final decidir la forma de usarlas. En las mejores prácticas de defensa contra el spam, se observan híbridos de técnicas y formas mixtas de erradicar el mismo. Allí es donde se debe hacer énfasis a la hora de configurar un servicio de correo.

Para esto existen una serie de técnicas, empezando desde las técnicas clásicas de filtrado, que son las que determinan la clase de los mensajes en base a los términos que contienen; pero este funcionamiento resulta poco adecuado en situaciones de ataque a filtros de correos spam mediante técnicas estadísticas o palabras dispersas. Por otro lado, al basar la clasificación en la presencia de términos, resulta más difícil identificar mensajes legítimos que contienen algunos términos frecuentes en mensajes spam. En el modelo propuesto, la determinación de la categoría de un mensaje se llevará a cabo en base a los correos más similares a uno dado.

Cabe destacar que los filtros antispam utilizan diversas técnicas como el análisis del título del mensaje, el contenido del mismo o el origen del mensaje, entre otras variables, para predecir si un mensaje es spam o no. De esta forma, un correo que en el título incluya la palabra “hipoteca” o “viagra” y el remitente sea anónimo o prototípico de un envío de spam, posiblemente cumpliría todas las reglas para ser borrado antes de llegar al buzón electrónico del destinatario.

Por ese motivo, los filtros antispam están muy relacionados con el idioma ya que necesitan analizar y relacionar palabras típicas del spam como viagra, dietas, hipotecas o hacerse rico y, por lo tanto, necesitan un desarrollo específico para cada idioma.

Aunque los filtros hasta el momento se han centrado en el inglés, el aumento de spam en otros idiomas está creando nuevas necesidades y nuevas oportunidades de negocio para las firmas dedicadas a su desarrollo.

El diseño modular de la herramienta de la propuesta basada en software de dominio público, genera mayor utilidad a la hora de detectar fallas, hacer mantenimiento, efectuar actualizaciones de paquetes, depurar funcionamiento y hacer entonación del sistema.

Como síntesis, se puede decir que este trabajo ha aportado un conjunto de indicaciones de gran importancia para la construcción de filtros antispam, junto con el desarrollo de un modelo que incorpora y saca partido de estas características.

- El software de dominio público permite implementar sistemas que pueden igualar o hasta superar soluciones propietarias equivalentes.
- El software de dominio público no necesita de hardware de última línea para poder implementar servicios con niveles de calidad aceptables, dando la posibilidad de ser escalados si las condiciones lo ameritan.
- Usar tecnologías libres permite la construcción de sistemas sumamente amplios y complejos, según sean las necesidades particulares.
- Se cumplieron con los objetivos del Trabajo Especial de Grado al seleccionarse y configurarse exitosamente los servidores SMTP, IMAP y LDAP para implementar el sistema de correos electrónicos integrado con servicios de directorio, lográndose satisfacer los requerimientos generales que presentan los organismos, siendo éstos: el envío y recepción de correos electrónicos, el acceso a los correos almacenados, la autenticación y manejo de la lista de contactos de manera centralizada, entre otros.

El proceso de pruebas de la solución propuesta, llevado a cabo bajo un ambiente diseñado previamente, representó una escala muy reducida de la solución real. Sin embargo, se pudo determinar que dicha solución puede ser reaplicada para diferentes ambientes a escalas mucho mayores, por lo cual se considera como una solución extensible a numerosas entes.

Siendo las palabras claves que resumen las ventajas de la solución antispam, las siguientes:

- Eficaz: el spam es bloqueado antes de la llegada al servidor de e-mail.
- Sencilla: instalada en poco tiempo, solución llave en mano de funcionamiento autónomo.
- Rentable: Reduce el tráfico de la red y la carga de los servidores de e-mail.
- Disponible: Varios servidores antispam redundantes, supervisados de forma permanente.
- Innovadora: Se vale de las más recientes tecnologías antispam, compaginando procedimientos estándares y métodos rápidos de análisis de los correos.
- Compatible: Independiente del servidor de e-mail. La solución antispam funciona directamente con el protocolo SMTP.

- Internacional: Programa antispam desarrollado para detectar el spam en varios idiomas.

El aporte brindado a través del desarrollo del Trabajo Especial de Grado, fue una propuesta para solucionar el problema de spam existente en la plataforma de correo de la Asamblea Nacional. Dicha solución, de acuerdo con los resultados obtenidos, se considera como efectiva y de alto rendimiento. La importancia se presencia en las características de la solución, donde posee bajos costos económicos, facilidad en la implantación y facilidades para mantenimiento y operación.

Referencias Bibliográficas

[1] A. McDonald. Spamassassin: a Practical Guide to Configuration, Customization and Integration. Packt Publishing. Septiembre 2004.

[2] A. Schwartz. Managing Mailing Lists. O'Reilly. Marzo 1998.

[3] A. Schwartz. Spamassassin. O´Reilly. Julio 2004.

[4] A. Schwartz and S. Garfinkel. Stopping Spam. O´Reilly. Octubre 1998.

[5] B. Hatch, J. Lee y G. Kurtz. Hackers en Linux. McGraw-Hill. Noviembre 2001.

[6] Decreto Nº 3.390. Publicado en la Gaceta Oficial de la República Bolivariana de Venezuela Nº 38.095. Diciembre 2004.

[7] G. Carter. LDAP System Administration. O´Reilly. Marzo 2003.

[8] J. Locke. Open Source Solutions For Small Business Problems. Charles River Media. Mayo 2004.

[9] K. Dent. POSTFIX: The Definitive Guide. O´Reilly. Diciembre 2003.

[10] L. Cranor and B. LaMacchia. Spam! Communications of the ACM, Vol. 41. Agosto 1998.

[11] T. Adelstein and B. Lubanovic. Linux System Administration. O´Reilly Media. Marzo 2007

[12] M. McCarthy. The Procmail Companion. Addison-Wesley. Mayo 2001.

[13] W. Stalling. Comunicaciones y Redes de Computadores. Prentice Hall. Mayo 2008.

[14] M. St. Johns. Identification Protocol IETF. RFC 1413. Febrero 1993.

Glosario de Acrónimos y Términos

A

ARPANet (Advanced Research Projects Administration Network): Red precursora de Internet nacida en 1968 y auspiciada por el Departamento de Defensa de Estados Unidos como plataforma de experimentación.

B

Blog: Es un sitio web (WEBLOG) personal donde se escriben periódicamente, como un diario on-line sobre distintos temas que le interesan al propietario. Cada escrito está ordenado cronológicamente y en general posee enlaces a otras páginas para ampliar el tema que se habla.

Browser: Es el programa que el usuario utiliza para acceder y visualizar a los servicios de Internet. Sinónimo de Browser es navegador.

Bug: Término aplicado a los errores descubiertos al ejecutar un programa informático.

C

CGI (Common Gateway Interface): Tecnología de la WWW que permite a un cliente (navegador web) solicitar datos de un programa ejecutado en un servidor web. CGI especifica un estándar para transferir datos entre el cliente y el programa.

Chat: Recurso en Internet que permite comunicarse en forma de texto con otros usuarios.

D

DNS (Domain Name System): Sistema de Nombres de Dominio. Conjunto de protocolos y servicios para la identificación/conversión de una dirección de Internet expresada en lenguaje natural por una dirección IP.

E

EOF (End Of File) indica el final de un archivo.

F

Filtrado bayesiano Enfoque estadístico para determinar si un correo electrónico es spam. Está basado en técnicas de inferencia de probabilidad aplicadas por el matemático inglés Thomas Bayes.

Firewall (Muro de Fuego - Cortafuego): Herramienta de seguridad que controla el tráfico de entrada/salida de una red.

FTP (File Transfer Protocol): Permite enviar o recibir cualquier tipo de archivos hacia o desde un servidor.

G

GNU: Es un acrónimo recursivo que significa “GNU No es Unix”. Proyecto iniciado por Richard Stallman con el objetivo de crear un sistema operativo completo libre: el sistema GNU.

GPL (General Public License): Licencia creada por la Free Software Foundation y orientada principalmente a los términos de distribución, modificación y uso de software libre.

H

Hacker: Término utilizado para llamar a una persona con grandes conocimientos en informática y telecomunicaciones y que los utiliza con un determinado objetivo. Este objetivo puede o no se maligno o ilegal. La acción de usar sus conocimientos se denomina hacking o hackeo.

Hash: Un hash es un valor numérico de longitud fija que identifica datos de forma unívoca. Los valores hash se utilizan para comprobar la integridad de los datos que se envían a través de canales no seguros.

HTML (Hyper Text Mark-up Language o Lenguaje de Marcas de Hipertexto): Lenguaje desarrollado por el CERN que sirve para modelar texto y agregarle funciones especiales (por ej. hipervínculos). Es la base para la creación de páginas web tradicionales.

I

INTERNIC (Internet Network Information Center): Organización que administra y gestiona los nombre de dominios de Internet desde EE.UU. Por lo general cada país tiene su NIC para administrar dominios propios.

ISO: Tipo de formato de imagen de CDs, DVDs, etc.

ISP (Internet Service Provider): Empresa que se encarga de conectar y dar servicio de Internet a sus usuarios por algún medio (cable, inalámbrico, satelital, celular, telefónico, etc.).

K

KDE (K Desktop Environment): KDE es un poderoso entorno de escritorio de fácil uso.

L

LAN (Local Area Network). LAN definición para redes de área local.

M

Mirror (Sitio espejo, sitio copia): Página o archivo que se encuentra almacenada en otro u otros servidores como respaldo al original.

MODEM (MOdulador-DEModulador): Periférico de entrada/salida, que puede ser interno o externo a una computadora, y sirve para a conectar una línea telefónica con la computadora. Se utiliza para acceder a Internet u otras redes, realizar llamadas, etc.

MTA (Mail Transport Agent): Agente para el transporte de correo electrónico.

MUA (Mail User Agent): Cliente de correo electrónico.

MX (Mail eXchange Record): Es un tipo de registro, un recurso DNS que especifica como debe ser encaminado un correo electrónico en Internet. Los registros MX apuntan a los servidores a los cuales enviar un correo electrónico, y a cual de ellos debería ser enviado en primer lugar, por prioridad.

N

Nslookup: Comando que averigua la dirección de una máquina e informaciones sobre dominios.

NTFS (New Technology File System): Es un sistema de archivos diseñado específicamente para Windows NT, y utilizado por las versiones recientes del sistema operativo Windows.

P

PPP (Point to Point Protocol): Protocolo de nivel de enlace para hacer conexión entre dos computadoras o nodos, utilizando cable serial, línea telefónica, teléfono celular, enlace de fibra óptica, etc.

R

Re-mailer: Servicio de Internet que, utilizando distintas técnicas, oculta la identidad del remitente de un correo electrónico.

RFC (Request For Comment): Documentos que se iniciaron en 1967 que describen los protocolos de Internet.

Router: Dispositivo hardware o software para interconexión de redes de computadoras que opera en la capa tres (nivel de red) del modelo OSI.

RPM (Red Hat Package Manager): Es también el nombre del programa que permite la instalación, actualización y eliminación de paquetes.

S

Script: Archivo que contiene instrucciones para el intérprete de comandos.

SLA (Service Level Agreement): Acuerdo de Nivel de Servicio.

SMTP (Simple Mail Transfer Protocol): Protocolo estándar para enviar e-mails.

SOAP (Simple Object Access Protocol): Protocolo de acceso a objetos simples. Define como dos objetos en diferentes procesos pueden comunicarse

T

TCP (Transmission Control Protocol) : Se trata del protocolo más usado de Internet.

Tcpdump: Herramienta en línea de comandos cuya utilidad principal es analizar el tráfico que circula por la red.

Traceroute: Herramienta de diagnóstico de redes que permite seguir la pista de los paquetes que van desde un host (punto de red) a otro.

U

UML (Unified Modeling Language): Popular lenguaje de modelado de sistemas de software. Se trata de un lenguaje gráfico para construir, documentar, visualizar y especificar un sistema de software.

URL: Se trata de una cadena de caracteres que identifica cada recurso disponible en la WWW.

W

Whois: Programa que permite a los usuarios hacer búsquedas en una base de datos sobre las personas y otras entidades de Internet, tales como dominios, redes y sistemas centrales.