Analisis, diseño e implementación de una solución anti spam para la Empresa Ecuaonline

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por el Sr. DAVID MONCAYO FERNÁNDEZ DE CÓRDOVA, CANDIDATO A INGENIERO EN SISTEMAS E INFORMÁTICA como requerimiento para a la obtención del título de INGENIERO EN SISTEMAS E INFORMÁTICA

_____

Fecha

_____

ING. CRISTÓBAL ESPINOSA

PROFESOR DIRECTOR

DEDICATORIA

El siguiente trabajo va dedicado con mucho amor y cariño a mis padres quienes me han acompañado en cado momento de mi vida, siempre han estado ahí para darme su apoyo, a mis hermanas a quienes quiero mucho, a Cris quien siempre ha sabido ayudarme y comprenderme, Miah quien me dio la fuerza para dedicarme y esforzarme en cada momento durante el trascurso del proyecto.

David Moncayo Fernández de Córdova

AGRADECIMIENTOS

Quiero agradecer en primer lugar a mi familia, en especial a mis padres quienes siempre han buscado mi bienestar.

Agradezco también a la gente que trabaja dentro Ecuaonline S.A., a mi director de tesis el Ing. Cristóbal Espinosa por la guía que durante la elaboración del proyecto.

El desarrollo de este trabajo no hubiera sido posible sin la ayuda de Cristina Vallejo, quien siempre me apoyo para que este proyecto se lleve a cabo.

David Moncayo Fernández de Córdova

ÍNDICE DE CONTENIDOS

LISTADO DE TABLAS

LISTADO DE FIGURAS

LISTADO DE ANEXOS

NOMENCLATURA

Ancho de banda digital: Cantidad de datos que se pueden transmitir en un periodo de tiempo, similar a una tubería, a mayor ancho de banda en una conexión, mayor información puede pasar a través de ella.

Encriptación: Es el procedimiento que se usa para ocultar información mediante el uso de una clave.

E- mail: Servicio de red que permite enviar y recibir mensajes rápidamente, denominados cartas electrónicas.

E- Mail Hosting Service: Servicio que se da principalmente a exigentes usuarios de correo electrónico de pequeñas y medianas empresas por parte de un proveedor de servicios.

Spam: Se conoce como Spam al correo electrónico no solicitado y de tipo masivo.

Hoax: Es hacer creer a un grupo de personas de que algo que es falso es real a través de una noticia, por medios masivos como el caso de Internet.

Phishing: Es un delito informático en donde se busca adquirir información confidencial como claves de tarjetas de crédito entre otros, haciéndose pasar por una empresa o institución de confianza

SMTP (Simple mail transfer Protocol): Protocolo de red basado en texto para el intercambio de correo entre computadores u otro tipo de dispositivos.

SSL (Secure Sockets Layer): Protocolo de Capa de Conexión Segura, proporciona seguridad, autenticación y privacidad a la información entre extremos sobre Internet con el uso de criptografía.

Relay: Consiste en permitir a un servidor de correo transmitir correos electrónicos de sus usuarios a otros servidores de correo en la Internet.

Open Relay: Son servidores que permiten que se envié a través de ellos correo sin ningún tipo de restricción**.**

Smart host: Es un tipo de retransmisión de correo que permite a un servidor SMTP enviar correo a través de un intermediario con su debida autenticación, como es SMTP-AUTH o POP antes que SMTP.

Dominio: Es un nombre base que agrupa a un conjunto de equipos o dispositivos, permite proporcionar nombres más fácilmente recordables que una dirección IP.

DNS (Domain Name System): Es una base de datos distribuida y jerárquica que almacena información correspondiente a los nombres de dominio, su uso más común

es la asignación de nombres de dominio a una IP y la definición de los servicios que brindan los servidores.

Zonas: Son porciones de nombre de dominio que almacenan los datos, donde se publican los datos y los nombres de los servicios.

Registros: Están hechos en base a lo que se conoce como resource records o RR´s, y tienen un tipo asociado.

SPF (Sender Policy Framework): es una identificación para evitar la falsificación de direcciones, mediante el uso de un registro DNS, garantizando que se envié el correo por servidores SMTP autorizados.

MX (Mail eXchange Record): Es un registro utilizado para el intercambio de correo, donde se especifica cómo debe ser encaminado un correo, apunta a los servidores encargados de transmitir un correo electrónico.

Spamassassin: Es un filtro anti- spam que puede integrarse con un servidor de correo, el filtrado lo realiza a través de pruebas heurísticas, cabeceras de correo y verificación del cuerpo de correo**.**

Router: Es un dispositivo de red capaza de aprender no solo la dirección de origen y destino, sino también las rutas que deben seguir los paquetes para llegar a su destino

Switch: Es un dispositivo que permite la interconexión de redes de computadores y que opera en la capa de enlace de datos. Su función es interconectar dos o más segmentos de red.

ISP (Internet Service Provider): Es una empresa dedicada a conectar a sus usuarios a Internet, así como servicios relacionados como alojamiento web, correo entre otros.

Listas Negras: son listas que buscan discriminar de alguna forma con respecto a los que no están en la lista.

Listas de acceso: Concepto de seguridad informática que se utiliza para separar los privilegios de los usuarios.

Virus informáticos: Tiene por objeto alterar el funcionamiento de un computador.

POP (Post Office Protocol): Es un protocolo que se utiliza para descargar los correos electrónicos desde un servidor de correo.

IMAP (Internet Message Access Protocol): Es un protocolo de red de acceso a mensajes electrónicos que se encuentran almacenados en un servidor, permite descargar los correos al computador bajo demanda.

LDAP (Lightweight Directory Access Protocol): Es un protocolo a nivel de la capa de aplicación que permite el acceso un directorio distribuido en donde los usuarios pueden acceder a cierta información dentro de una red. Almacena información de autenticación, recursos de una red, datos de contacto de usuarios entre otros.

Prevención de Intrusos: Es un dispositivo que ejerce control de acceso a una red para proteger a los sistemas computacionales de ataques y abusos

Bayesianos: Es un clasificador probabilístico que se basa en aplicar el Teorema de Bayes, para detectar mensajes de correo electrónico basura.

BIND (Berkeley Internet Name Domain o Berkeley Internet Name Daemon): Es el servidor de DNS más usado en sistemas Unix.

LACNIC (Latin American and Caribbean Internet Addresses Registry): Es el Registro Regional de Internet para América Latina y el Caribe. Administra las Direcciones IP versión 4 y versión 6, números de Sistemas Autónomos, DNS Reverso y recursos de la región

Mailbox: Casilla postal para tráfico de correo electrónico.

FQDN (Fully Qualified Domain Name): Es un nombre que se compone por el nombre de la computadora y el nombre de dominio asociado a ese equipo.

RFC (Request For Comments): Son una serie de notas sobre Internet, cada una de ellas de manera individual constituye un documento y es una propuesta para el uso de un protocolo en Internet.

Autenticación: Es el proceso de verificar la identidad digital de un remitente, como es una petición para conectarse hacia un servidor por ejemplo.

Servidor: Es un ordenador que suministra información a otros, a través de una red.

Certificado digital: Es un documento digital emitido por una unidad certificadora garantiza la relación entre una entidad con su clave pública.

Clave Pública: Es una clave que se puede entregar a cualquier persona.

RESUMEN

El tráfico que genera el correo basura (SPAM) dentro de la red, ocasiona gran pérdida de tiempo y consumo de recursos; además por este medio se transmiten otras amenazas como virus, gusanos entre otros. Ante este problema el presente documento muestra la implementación de una solución integral para el proveedor de servicio de internet (ISP), en busca de mejorar la calidad de servicios a los clientes, y evitar que desde la red del proveedor también se genere SPAM.

Para llevarlo a cabo se implemento un servidor DNS secundario así como la reconfiguración en los registros de las zonas en el servidor DNS primario, además se implemento el uso del registro (SPF), para evitar la falsificación de direcciones de correo electrónico, por otra parte se genero la retransmisión (relay), desde el servidor de correo actual hacia el servidor anti– spam implementado; existe mayor control en el uso del protocolo SMTP a través de listas de acceso en la salida a internet para los clientes. Los resultados muestran que en el primer mes se redujo alrededor de quince correos por minuto considerados como SPAM.

CAPÍTULO I

INTRODUCCIÓN

1. Prólogo

El crecimiento de las redes a nivel mundial, el uso de servicios como el correo electrónico y el tipo de información que se intercambia a través del mismo obliga a tener control sobre todo porque muchas veces por este medio puede enviarse y recibirse correo no deseado o virus que afectan directamente al usuario haciéndose esto recurrente y causando más de una molestia, generando pérdidas de tiempo y gran consumo de recursos en lo que ancho de banda se refiere.

Siendo así el Spam representa tanto para clientes como la empresa que provee el servicio incrementos en los costos de telecomunicaciones, almacenamiento de la información e inversión de tiempo en lo que a recurso humano se refiere, además de que se presentan problemas adicionales como virus o spyware[1] en las estaciones de trabajo de los empleados.

Ecuaonline en la actualidad cuenta con un servidor de correo donde no se filtra efectivamente el correo y no se controla el tráfico de correo saliente de la red del proveedor permitiendo que existan problemas con lo que es generación de Spam a través del servidor ya que cualquiera puede enviar correo a través del mismo, lo

[1] Spyware: aplicaciones que recopilan información sobre una persona u organización, su uso más común es recopilar información de usuario para distribuirlo a empresas publicitarias.

que se conoce como Open Relay[2]. Por otra parte dentro de la red del proveedor no existe ningún tipo de control en el tráfico tanto de entrada como de salida de correo electrónico por lo que se puede enviar correo libremente generando grandes inconvenientes.

1.1. E- mail

Es un servicio de red que permite enviar y recibir mensajes rápidamente, denominados cartas electrónicas, mediante el uso del protocolo SMTP[3], por dicho medio se puede no solo enviar mensajes de texto sino también toda variedad de documentos digitales.

1.2. SPAM

Correo basura o sms basura, se considera a los correos no solicitados y de tipo masivo. También se conoce como Spam a los virus y paginas filtradas como propagandas, entretenimiento, etc. Involucra enviar correos idénticos o casi idénticos a un gran número de direcciones de correo.

[2] Open Relay: Servidores de correo que permiten el envío de correo a través de ellos sin restricción.

[3] SMTP: Simple mail transfer Protocol, protocolo de red basado en texto para el intercambio de correo entre computadores u otro tipo de dispositivos.

1.3. Objetivos

1.3.1. Objetivo General

Implementar una solución Anti Spam para la empresa Ecuaonline, mediante uso de filtro de contenido y distintas soluciones encaminadas a la eliminación del correo basura en la red de la empresa.

1.3.2. Objetivos Específicos

- Diseñar una solución que sea perdurable y escalable que permita adaptarse al uso de nuevas protecciones para brindar seguridades de envió y recepción de correo.
- Analizar las ventajas y desventajas que se tiene con los cambios dentro de la estructura actual del servidor de correo y de la red con los puertos destinados a envió y recepción de correo.
- Implementar mecanismos de eliminación de correo no deseado para las compañías así como cortar el envío y recepción de virus a través del correo.
- Realizar un control del tráfico SMTP de la red, para eliminar el correo electrónico que se genera desde y hacia esta.

1.4. Planteamiento del problema

El correo es una parte importante del servicio que da un ISP[4], las pérdidas ocasionadas cuando los clientes no pueden enviar correos hacia distintas partes del mundo o el no saber si los correos electrónicos llegan a sus destinatarios obligan a los clientes al ver que en ocasiones los problemas sobrepasan la capacidad de su administrador de correo, dominio o internet, tengan que buscar otro proveedor.

El recibir correo indeseado o que no es de interés para una empresa y la pérdida de tiempo que ocasiona el tener que eliminar dichos correos, y es más que las direcciones IP públicas y sus redes sean marcadas bajo lista negra ocasionan más de un dolor de cabeza tanto para el usuario y el proveedor.

En lo que va del año en curso hasta la presente han existido grandes oleadas de SPAM a través del correo, los controles en sitios como café net que son parte de los clientes que maneja la compañía, que muchas veces no ocupan servicio de correo pero sin embargo a través del puerto 25 están causando que las IP que a los mismos se les asignan este en listas negras obligan a tomar decisiones por parte de la compañía que provee el servicio. Por dicha razón el proveedor está buscando las mejoras alternativas a implementar para eliminar dicho problema ya que existe mal uso del servicio.

[4] ISP: Internet Service Provider, se conoce como provedor de servicios de internet a la empresa dedicada a conectar a Internet a los usuarios de su red, ofrece también servicios como alojamiento web, registro de dominios, servicio de correo electrónico, entre otros.

1.5. Alcance

A pesar de que el proveedor ya cuenta con ciertos mecanismos de control con respecto a lo que es envío y recepción de correo, dichos controles no son del todo efectivos ya que se genera grandes cantidades de correo no deseado dentro de la red del proveedor.

Los trabajos que se realizarán, serán cambiar ciertos parámetros dentro de la configuración de los servidores DNS[5] de la compañía y los registros existentes de estos servidores actualizando zonas y documentando correctamente los cambios realizados dentro de dichos servidores. Cambios en la configuración del servidor de correo, sus dominios y sub dominios con el fin de parar el ingreso y salida de correo basura dentro de la red.

Analizar el uso de SPF[6] dentro de los registros en los servidores DNS con el fin de garantizar que los dominios de los distintos clientes que ocupan las IP de Ecuaonline no sean enlistados en los servidores a nivel mundial.

El proyecto comprende fases de análisis, diseño, varias pruebas e implementación, los dispositivos para realizar dicha reestructuración ya se encuentran dentro del proveedor, por lo cual no es tan difícil un análisis económico para su factibilidad.

[5] DNS: Domain Name System, es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio.

[6] SPF: Sender Policy Framework, protección contra la falsificación de direcciones para envío de correo, identifica a través de los servidores DNS a los servidores SMTP autorizados para transporte de correo.

1.6. Justificación

Con la implementación de filtros, sistemas de relay y smart host en servidores de correo y un firewall antes del servidor de correo se logrará que el proveedor brinde un mejor servicio a sus usuarios. Además con el control del tráfico SMTP se logrará un mejor rendimiento dentro de las empresas a las que ocupan el servicio de correo electrónico.

CAPÍTULO II

MARCO TEÓRICO

2. Introducción

2.1. E- mail

2.1.1. Modo de uso

Correo electrónico, o por sus siglas en ingles e- mail (electronic mail) permite a los usuarios enviar y recibir mensajes dentro del servicio que provee internet, con el uso del protocolo SMTP (simple mail transfer protocol) se puede enviar información de texto y cualquier tipo de documento digital, por su costo ha desplazado sin lugar a duda al correo ordinario.

En el año de 1961 en el MIT (Massachusetts Institute of Technology) se presento un sistema que permitía a varios usuarios ingresar desde terminales remotas para de esta manera guardar en disco información en una máquina central, en el año de 1975 se incorporo por parte de Ray Tomlinson el uso de la arroba @ debido a que esta no está presente en ningún nombre ni apellido de ninguna persona, la arroba se la lee como “at”, por consiguiente se expresa persona que se encuentra ubicada en tal dominio, que es lo que se pone después del signo arroba.

2.1.2. Funcionamiento

Para enviar un correo electrónico se requiere de mínimo estos tres componentes:

- Destinatario, una o más direcciones a las que va dirigido el mensaje.
- Asunto, una descripción corta con información sobre lo que verá en el mensaje.
- Cuerpo del mensaje, no tiene límite de tamaño y puede o no tener formato.

2.1.2.1. Ejemplo de envío de correo

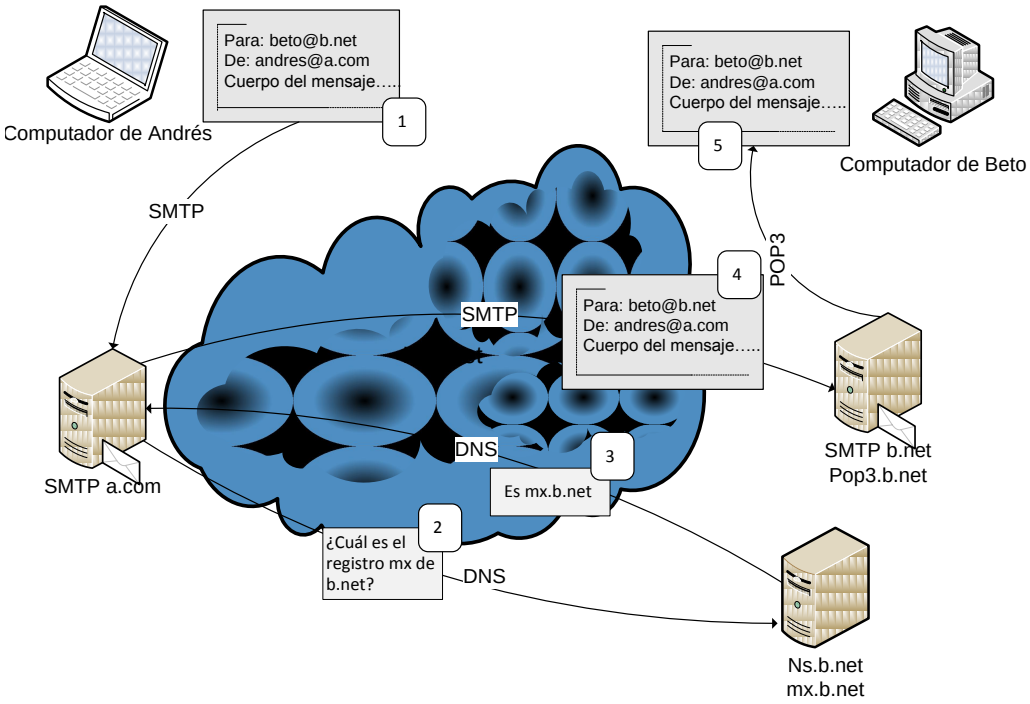


Figura 1: Funcionamiento envío de correo a través de protocolo SMTP

En el siguiente ejemplo Andrés con dirección de correo andres@a.com envía un correo a Beto beto@b.net, como se puede apreciar cada persona tiene un servidor distinto, para el envío se realizan los siguientes pasos:

1. Andrés redacta el correo y envía el correo a través de su programa cliente de correo electrónico, mismo que se contacta con el servidor de correo electrónico de Andrés median el uso del protocolo SMTP, que le trasfiere el correo y le da la orden de enviarlo hacia el destinatario.
2. El servidor SMTP determina que ha de entregar el correo a alguien del dominio b.net, pero no sabe con qué dispositivo se ha de contactar, por ello contacta a su servidor DNS usando el protocolo DNS. Que se encarga de preguntar quién es el encargado del dominio b.net, es decir le pregunta acerca del registro MX[7] asociado a este dominio.
3. El servidor de correo de Beto responde a través del nombre de dominio[8] del servidor de correo donde se encuentra el dominio b.net. Para este ejemplo es mx.b.net que es un servidor gestionado por el ISP (Proveedor de servicio de Internet).
4. El servidor SMTP de a.com ahora ya puede contactar con mx.b.net y trasferir el correo que quedará guardado en el servidor de correo de b.net. Se utiliza nuevamente el protocolo SMTP.

[7] Registro MX o Mail exchange record , es el registro para intercambio de correo, que especifica por donde debe ser encaminado un correo electrónico en internet.

[8] Dominio, es un nombre que agrupa a un conjunto de equipos proporcionando nombres en lugar de dirección IP , permitiendo a cualquier servicio de red moverse a un lugar diferente en la topología de internet.

5. Cuando el usuario Beto con dirección beto@b.net a través del cliente de correo. Se establece una conexión mediante el protocolo POP3 o IMAP, en este caso para el ejemplo mediante el uso del protocolo POP3 que baja el correo que fue almacenado en el servidor de correo de Beto.

2.2. DNS (Domain Name System)

Sistema de nombres de dominio, es una base de datos jerárquica y distribuida que almacena información sobre nombres de dominio de redes como internet. Uno de sus usos más comunes es el de traducir de nombres a direcciones IP y la localización de servidores de correo de cada dominio.

2.2.1. Concepto e instalación de dominios

El mapeo de direcciones de nombre de host está gestionado en NIC (Network Information Center), dentro de un archivo que es Hosts.txt, el cual es distribuido a los hosts mediante FTP, se utiliza un diseño de base de datos distribuida con recursos generalizados.

Quien realiza la distribución establece el valor para el tiempo de refresco y el receptor de dicha distribución es quien se encarga de realizar el refresco.

El servidor de nombre utiliza ficheros maestros donde se cargan las zonas con sus debidos registros y zonas.

2.2.2. Elementos de un DNS

- Espacio de nombres de dominio y registro de recursos.

  Son especificaciones para un árbol estructurado de espacio de nombres y los datos que se encuentran asociados a dichos nombres. Cuando se realiza una consulta esta menciona el nombre de dominio de interés y se describe la información solicitada.

- Servidores de nombres

  Son programas en donde se encuentra la estructura de un árbol de dominio; tiene además toda la información con respecto a los subconjuntos de espacio de dominio y punteros hacia otros servidores de nombre de dominio.

  Estos servidores conocen las partes del árbol ya que poseen información completa del mismo.

  Esta información autoritativa se almacena dentro de unidades llamadas zonas.

  - Servidores Primarios, son los únicos autorizados para un dominio y poseen la configuración del dominio.
  - Servidores Secundarios, funcionan como respaldo o distribuidores de carga, reciben periódicamente las actualizaciones que el servidor primario le envía.
  - Servidores de Cache, contiene una cache de direcciones, en primera instancia busca en su cache y de no ser así pregunta a un primario si lo tiene.

- Servidores de Forwarding, redirige las peticiones a otros servidores de nombres similar al caso anterior.

- Resolutores

  Son programas para extraer información de los servidores de nombre como respuesta a consultas que realizan los clientes.

2.2.3. Zonas

Cada dominio tiene asociada una zona DNS en donde se especifica la dirección o direcciones públicas con las extensiones del dominio como son subdominios, servidores de correo, alias, servidores de nombre. Debido a que todo el tráfico en internet es mediante direcciones IP se debe realizar una traducción del nombre mediante un servidor DNS, dicho servidor se encargará de traducir una IP asociada al dominio o cualquier aspecto relativo al dominio. Cada zona es una unidad más pequeña dentro de un servidor.

2.2.3.1. Zonas delanteras de operaciones de búsqueda

Se crea para realizar operaciones en la base de datos del DNS, resolviendo nombres a direcciones IP y a la información del recurso.

2.2.3.2. Zonas reversas de operaciones de búsqueda

Realiza la operación opuesta a las zonas delanteras de búsqueda, estas se las llena con los expedientes de la zona PTR, que sirven para señalar la pregunta

reversa de las operaciones de búsqueda al nombre de dominio apropiado. Esto es de gran utilidad en el caso del SMTP para que se mantenga un registro PTR, ya que los sitios de control de SPAM revisan la existencia de dicho registro.

2.2.4. Registros

Están hechos en base a lo que se conoce como resource records o RR´s, y tienen un tipo asociado. Cada campo dentro de un registro se lo separa mediante espacios debidamente tabulados.

Dominio, nombre del dominio al cual se aplica el registro.

TTL, time to live, tiempo de vida del RR, es posible dar un tiempo de vida cada registro en segundos, para que después de que se ocupe la información de este registro descarte la información al término de este periodo.

Clase, valor codificado de 16 bits, que sirve para identificar a una familia de protocolos. Utiliza las siguientes clases IN (sistema de internet) y CH (sistema caos).

Tipo, es un valor de 16 bit que especifica el tipo de recurso, y para que se usa dicho registro. Existen los siguientes tipos de registros:

- A, para asociar una dirección de máquina con una dirección IP. Solo debe existir uno por cada dirección IP. Ejemplo:

  casa IN A 190.56.19.148

- CNAME, identifica un nombre alternativo o alias a una máquina. Ejemplo:

  news IN CNAME casa

  www IN CNAME casa

- HINFO, identifica al CPU y el sistema operativo del host.

- TXT, proporcionan información de contacto al usuario. Ejemplo:

  servidor1.dominio.com. IN TXT “Administrador David”

- MX, identifica un servidor de correo para el dominio. A diferencia de otros registros este lleva un campo para identificar la preferencia de la máquina para el envió de correo. Ejemplo:

  fca.com.ec. MX 5 q1sc.ecuaonline.net.

- NS, servidor de nombres autoritativo para el dominio. Ejemplo:

  e1ns IN A 200.110.232.2

- PTR, identifica una dirección IP con un nombre de máquina. Se guarda dentro de un archivo para la resolución de zona reversa. Ejemplo:

  136 IN PTR prueba.com.

- SOA, identifica el comienzo de la zona autoritativa. Ejemplo:

  nano/var/cache/bind/zones/fca.com.ec

```
$TTL    43200
@       IN      SOA     ns.prueba.com. dmoncayo.prueba.com. (
                                2008052501  ; Serial
                                10800       ; Refresh
                                3600        ; Retry
                                604800      ; Expire
                                43200 )     ; Minimum
```

Los datos que se asocian a este registro son los siguientes:

- Origin, es el nombre primario para el dominio, generalmente es absoluto, y va con un punto al final.
- Contact, es el nombre de la persona responsable para el dominio y la dirección va separada por puntos.
- Serial, es el número que indica la versión de zona, y se modifica cada que se realiza un cambio en un día determinado y el valor estándar esta como año, mes, día y ID que incrementa según el número de modificación en el día que esta sea.
- Refresh, es un intervalo en segundos para que los servidores secundarios revisen la información del registro SOA. Usualmente es de una hora es decir 3600 segundos.
- Retry, es el tiempo que un servidor secundario espera cuando la conexión con el servidor primario ha fallado. Usualmente 10 minutos es decir 600 segundos.

- Expire, si un servidor secundario no puede verificar los cambios realizados en un primario, descarta la información de este en un tiempo generalmente de 42 días, 3600000 segundos.
- Mínimum, es el tiempo mínimo en los archivos que no especifican su TTL.

Datos, está relacionado con el tipo, y representa la información que se almacena.

2.3. Servicio DNS en Linux

En Linux el archivo de hosts se lo encuentra en etc/hosts, dicho archivo contiene nombres de máquinas con direcciones IP. El archivo host.conf permite indicar el orden de búsqueda para la resolución del DNS.

En la parte inferior se detalla un ejemplo de un fichero hosts. En el caso de uno de los DNS de Ecuaonline es el siguiente.

```
sudo nano /etc/hosts
127.0.0.1 localhost
127.0.1.1 q1ns q1ns.ecuaonline.net

# The following lines are desirable for IPv6 capable hosts
::1 ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

Figura 2: Configuración IP servidor DNS Primario

Quien gestiona el nombre de dominio en internet es IANA (Internet Assigned Naming Authority), los dominios genéricos de primer nivel son .com, .net, .org, .edu, entre otros y de ahí los correspondientes a los países como por ejemplo .ec. En el año 2000 se incluyeron 7 dominios nuevos de primer nivel .biz, .info, .name, .pro, .aero, .coop y .museum.

Todos los dominios se encuentran distribuidos en servidores raíz a nivel mundial, el archivo /var/named/named.ca contiene dicha lista de servidores raíz. Cuando se realiza una consulta DNS sobre el host www.paisacuarela.com.ec, inicialmente se pregunta a un servidor raíz por el servidor autorizado para la zona com.ec y devolverá la dirección IP del mismo, luego preguntamos al servidor por el host www, del subdominio paisacuarela para el ejemplo que nos dará posteriormente su IP.

Subdominios, delega una subsección de un dominio. Las peticiones que se realizan en DNS van desde arriba hacia abajo en el árbol. El servidor DNS en Linux ocupa el puerto 53 y el servidor es bind, por otra parte el fichero donde se almacena el cliente DNS es /etc/resolv.conf aquí se almacena la dirección IP del servidor DNS y el nombre del mismo.

2.3.1. Configuración de servidor DNS

Las zonas primarias se configuran en el /etc/named.conf y tienen la siguiente estructura:

- La directiva file indica el path o ubicación de almacenamiento de la zona, generalmente se lo localiza en /var/named.

  Tiene la siguiente estructura:

```
zone “nombre_del_dominio” IN {
        type master;
        file “nombre_path”;
};
```

Ejemplo con una zona delantera de operaciones de búsqueda

```
zone "dominio.com" IN {
        type master;
        file "zones/dominio.com";
};
```

El archivo zones/dominio.com, se encuentra en /var/named o /var/named/chroot/var/named.

Ejemplo con una zona reversa de operaciones de búsqueda

Se define una zona reversa para cada una de las redes utilizadas en el caso del ejemplo esta para la red 192.168.1.1 con máscara de 24 bits, para ello se toma la red en sentido inverso seguido del sufijo in-addr.arpa.

```
zone "1.168.192.in-addr.arpa" IN {
        type master;
        file "zones/1.168.192.db";
};
```

Las zonas secundarias se configuran en el /etc/named.conf

- Contiene una copia de seguridad de la zona primaria y en caso de que el servidor primario estuviese caído este responde con autoridad a una petición DNS

  Ejemplo con una zona delantera de operaciones de búsqueda

```
zone "dominio.com" IN {
        type slave;
        file "zones/dominio.com";
        masters { nombre_del_servidor_DNS_principal; };
};
```

Ejemplo con una zona reversa de operaciones de búsqueda

```
zone "1.168.192.in-addr.arpa" IN {
        type slave;
        file "zones/1.168.192.db";
        masters { nombre_del_servidor_DNS_principal; };
};
```

Zonas para servidor cache, se configuran en el /etc/named.conf

- Se configura un servidor DNS básico sin zonas primarias ni secundarias, contiene únicamente una lista de servidores raíz, y almacena en su cache las direcciones de las consultas DNS. En primera instancia pregunta a su cache de no ser así pregunta al servidor primario si lo tiene gracias a la lista de servidores raíz.

- El archivo /var/named/named.ca contiene la lista de servidores cache.

```
zone "." IN {
type hint;
file "named.ca";
};
```

2.4. Herramientas DNS

Los siguientes comandos permiten ver la forma para verificar los registros creados para un determinado dominio.

- Comando NSLOOKUP[9], para ver resolución de nombres a IP y viceversa.

  Ejemplos:

  Resolución directa Linux

  ecuaonline-admin@q1ns:~$ nslookup www.fopeca.com

  Server: 127.0.0.1

  Address: 127.0.0.1#53

  ** server can't find www.fopeca.com: NXDOMAIN

  Resolución inversa

  Linux

  ecuaonline-admin@q1ns:~$ nslookup 200.110.232.162

  Server: 127.0.0.1

  Address: 127.0.0.1#53

  162.232.110.200.in-addr.arpa name = mail.fopeca.com.

[9] NSLOOKUP, es un programa que se utiliza para determinar si el DNS esta resolviendo las IP y los nombres, funciona tanto en Unix como Windows.

Windows

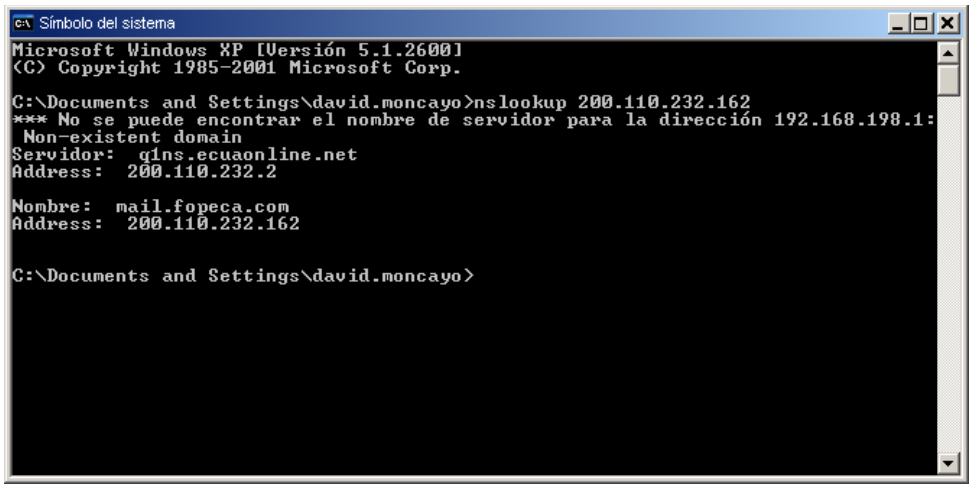


Figura 3: Commando nslookup, dirección IP

Además se puede realizar una consulta de otros registros de la siguiente manera, en Linux, se pone el comando nslookup seguido del registro que se desea consultar, así por ejemplo se puede ver el registro MX, de cualquier dominio.

A continuación se detalla un nslookup para consultar el registro MX:

ecuaonline-admin@q1ns:~$ nslookup -query=mx fca.com

Server: 127.0.0.1
Address: 127.0.0.1#53
Non-authoritative answer:
fca.com mail exchanger = 20 mail2.fca.com.
fca.com mail exchanger = 50 mx2.mailhop.org.
fca.com mail exchanger = 10 mail1.fca.com.
Authoritative answers can be found from:
fca.com nameserver = dns5.fca.com.
fca.com nameserver = dns2.fca.com.
fca.com nameserver = dns4.fca.com.
fca.com nameserver = dns6.fca.com.

fca.com nameserver = dns1.fca.com.

fca.com nameserver = dns3.fca.com.

mail1.fca.com internet address = 216.130.129.13

mail2.fca.com internet address = 68.156.14.5

dns5.fca.com internet address = 213.155.150.206

dns6.fca.com internet address = 203.62.195.76

De igual manera en Windows:

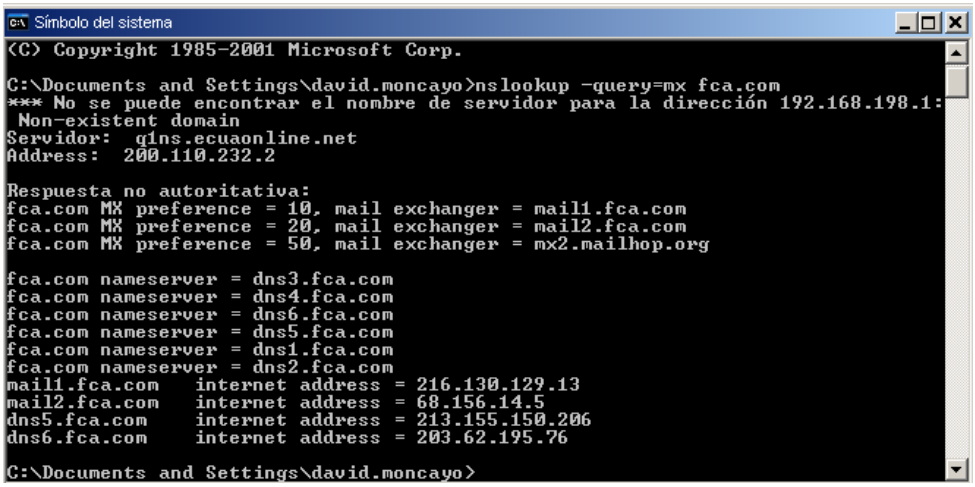


Figura 4: Comando nslookup para registros en Windows

- Comando dig[10], buscador de información de dominio.
  - Dig . ns, dirección de los trece servidores DNS a nivel mundial.

[10] Dig, es una herramienta de líneas de comandos que permite hacer consultas a un servidor DNS.

```
ecuaonline-admin@q1ns:~$ dig . ns

; <<>> DiG 9.4.2-P1 <<>> . ns
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30608
;; flags: qr rd ra; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 14

;; QUESTION SECTION:
;.                              IN      NS

;; ANSWER SECTION:
.                       177140  IN      NS      G.ROOT-SERVERS.NET.
.                       177140  IN      NS      I.ROOT-SERVERS.NET.
.                       177140  IN      NS      D.ROOT-SERVERS.NET.
.                       177140  IN      NS      J.ROOT-SERVERS.NET.
.                       177140  IN      NS      K.ROOT-SERVERS.NET.
.                       177140  IN      NS      B.ROOT-SERVERS.NET.
.                       177140  IN      NS      F.ROOT-SERVERS.NET.
.                       177140  IN      NS      L.ROOT-SERVERS.NET.
.                       177140  IN      NS      C.ROOT-SERVERS.NET.
.                       177140  IN      NS      A.ROOT-SERVERS.NET.
.                       177140  IN      NS      H.ROOT-SERVERS.NET.
.                       177140  IN      NS      E.ROOT-SERVERS.NET.
.                       177140  IN      NS      M.ROOT-SERVERS.NET.

;; ADDITIONAL SECTION:
H.ROOT-SERVERS.NET.     598146  IN      A       128.63.2.53
A.ROOT-SERVERS.NET.     128608  IN      A       198.41.0.4
M.ROOT-SERVERS.NET.     598146  IN      A       202.12.27.33
I.ROOT-SERVERS.NET.     598146  IN      A       192.36.148.17
G.ROOT-SERVERS.NET.     598146  IN      A       192.112.36.4
F.ROOT-SERVERS.NET.     598146  IN      A       192.5.5.241
D.ROOT-SERVERS.NET.     598146  IN      A       128.8.10.90
B.ROOT-SERVERS.NET.     598146  IN      A       192.228.79.201
K.ROOT-SERVERS.NET.     598146  IN      A       193.0.14.129
E.ROOT-SERVERS.NET.     598146  IN      A       192.203.230.10
J.ROOT-SERVERS.NET.     69085   IN      A       192.58.128.30
J.ROOT-SERVERS.NET.     69085   IN      AAAA    2001:503:c27::2:30
C.ROOT-SERVERS.NET.     598146  IN      A       192.33.4.12
L.ROOT-SERVERS.NET.     598146  IN      A       199.7.83.42

;; Query time: 9 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Oct 13 10:41:33 2008
;; MSG SIZE  rcvd: 464
```

Figura 5: Comando dig.ns

- Dig .net o .com, para conocer servidores que manejan los dominios.
- Dig dominio. NS, indica los servidores DNS del dominio.
- Dig dominio. MX(registro)

Se puede observar como despliega el comando dig el registro MX:

```
ecuaonline-admin@q1ns:~$ dig fca.com.ec. MX

; <<>> DiG 9.4.2-P1 <<>> fca.com.ec. MX
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46221
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 3

;; QUESTION SECTION:
;fca.com.ec.                    IN      MX

;; ANSWER SECTION:
fca.com.ec.             43200   IN      MX      5 q1sc.ecuaonline.net.

;; AUTHORITY SECTION:
fca.com.ec.             43200   IN      NS      q1ns.ecuaonline.net.
fca.com.ec.             43200   IN      NS      q2ns.ecuaonline.net.

;; ADDITIONAL SECTION:
q1sc.ecuaonline.net.    43200   IN      A       200.110.232.11
q1ns.ecuaonline.net.    43200   IN      A       200.110.232.2
q2ns.ecuaonline.net.    43200   IN      A       200.110.232.3

;; Query time: 2 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Oct 13 11:00:04 2008
;; MSG SIZE  rcvd: 149
```

Figura 6: Comando dig información registro MX

- Dig dominio. Traceroute, similar a tracert de TCP/IP

```
ecuaonline-admin@q1ns:~$ dig fca.com.ec traceroute

; <<>> DiG 9.4.2-P1 <<>> fca.com.ec traceroute
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24754
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;fca.com.ec.                IN      A

;; AUTHORITY SECTION:
fca.com.ec.           43200   IN      SOA     q1ns.ecuaonline.net. ifernandez.ecuaonline.net. 2008052501 10800 3600 604800 43200

;; Query time: 2 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Oct 13 11:42:33 2008
;; MSG SIZE  rcvd: 94

;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 30481
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;traceroute.                IN      A

;; AUTHORITY SECTION:
.                     6487    IN      SOA     A.ROOT-SERVERS.NET. NSTLD.VERISIGN-GRS.COM. 2008101300 1800 900 604800 86400

;; Query time: 2 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Oct 13 11:42:33 2008
;; MSG SIZE  rcvd: 103
```

Figura 7: comando dig, dominio tarceroute

Se interpreta la información que genera el comando dig de la siguiente manera:

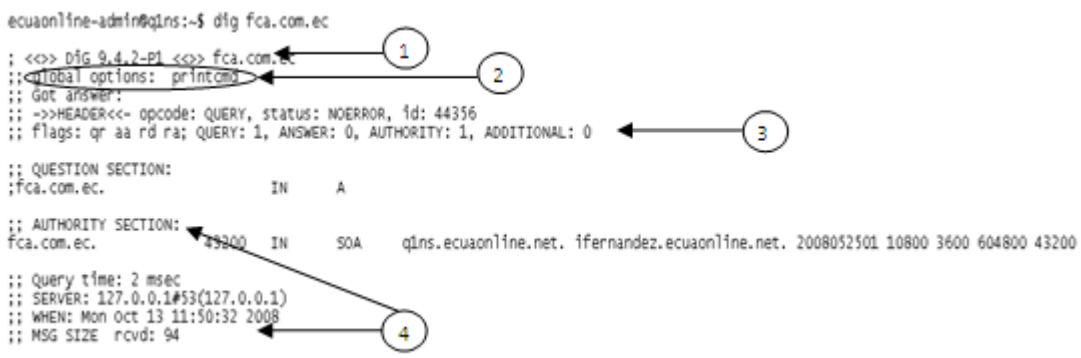


Figura 8: Interpretación información comando Dig

1. Las dos primeras líneas informan la versión del programa y el dominio que se está buscando.
2. La sección Got Answer, detalla la consulta recibida y si fue o no dada por una autoridad en DNS.
3. Es parte de la sección anterior y detalla la consulta y respuesta, y existen las siguientes banderas que tienen el siguiente significado:

    - Qr, query/response que diferencia consulta de respuesta
    - Rd, recursión desired modalidad de consulta que es replicada en ra.
    - Ra, recursión allowed significa que pedimos al servidor que si nos puede resolver la consulta por si mismo consulte a otro servidor.
    - AA, que la respuesta es de un servidor autorizado.
    - Tc, truncated response significa que la respuesta se ha fraccionado por ser de mayor tamaño del permitido.
    - AD Authentic Data y CD Checking Disabled.

4. Nos detalla la respuesta de nuestra consulta en si y los registros como SOA, A entre otros.

   Se puede usar en Windows también dentro de c:\windows\system32\drivers\etc\resolv.conf donde se puede ver esta información.

- Comando whois, entrega información sobre el registrante del dominio, es decir el propietario.
- Además existen sitios como www.dnsstuff.com, en donde se puede ver esta información como se muestra a continuación:

DNS Lookup

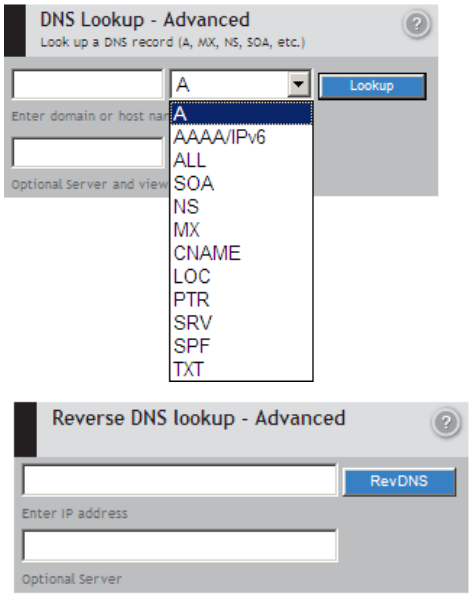


Figura 9: Consulta registros de un dominio a través de DNSSTUFF

Whois, para ver quién tiene la administración de un registro, y en donde fue comprado

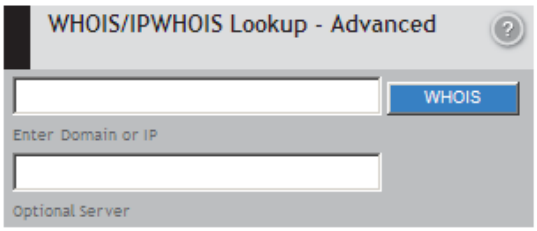


Figura 10: Consulta sobre Whois de un dominio

2.5. Mail Server

2.5.1. SMTP

Inicia en el año de 1982, con el primer sistema de intercambio de correo para ARPANET[11]. Es uno de los protocolos más utilizados y se basa en un modelo cliente servidor, la comunicación se la realiza en líneas de texto compuesto de caracteres ASCII entre el cliente y el servidor, y la respuesta de dicho servidor tiene un código numérico de tres dígitos. SMTP utiliza el puerto 25 en el conjunto de protocolos TCP/IP.

2.5.1.1. Funcionamiento SMTP

Un cliente SMTP contactará directamente con el Host del servidor de destino lo que se conoce como entrega punto a punto, el servidor de destino guardará el correo hasta que este haya sido copiado por el receptor del mismo.

Por otra parte existe también la posibilidad de intercambiar correo entre sistemas de correo locales y SMTP, dicho mecanismo se conoce como pasarelas o

[11] ARPANET, Advanced Research Projects Agency Network, creada como medio de comunicación para diferentes organismos y fue el inicio de Internet.

puentes de correo esto difiere de la entrega punto a punto, y además SMTP solo garantizará que la entrega sea fiable hasta la pasarela.

Pasos para la transacción de correo SMTP:

- El primer paso en el procedimiento es el comando MAIL, el <reverse-path> contiene el buzón de correo.

  <SP> MAIL FROM: <reverse-path> <CRLF>, este comando le dice al receptor SMTP que existe una nueva transacción de correo, si el receptor SMTP acepta la transacción y no existe errores devuelve la respuesta 250 OK.
- El segundo paso en el procedimiento es el comando RCPT RCPT <SP> A: <forward-path> <CRLF>, es la identificación del destinatario. Si se acepta el receptor envía un mensaje 250 OK, de no ser así envía una respuesta 550, este procedimiento puede repetirse varias veces.
- El tercer paso en el procedimiento con el comando DATA
- DATOS <CRLF>, de ser aceptado se envía la respuesta 354 y todas las líneas sucesivas son consideradas como el mensaje, al final el receptor SMTP envía una respuesta 250 OK.

  Con lo que el correo llegaría al respectivo buzón de los destinatarios donde el RCPT sea válido

En el siguiente ejemplo se muestra la transacción de correo con el uso de los comandos anteriores, tomando en cuenta que el host delta contacta directamente al gamma:

EMISOR: MAIL FROM: <david@delta.com>

RECEPTOR: 250 OK

EMISOR: RCPT A: <alejandro@gamma.com>

RECEPTOR: 250 OK

EMISOR: RCPT A: <jorge@gamma.com>

RECEPTOR: 550 Este usuario no existe aquí

EMISOR: RCPT A: <juan@gamma.com>

RECEPTOR: 250 OK

EMISOR: DATA

RECEPTOR: 354 Start mail de entrada; final con <CRLF>. <CRLF>

EMISOR: cuerpo del mensaje

EMISOR: <CRLF>. <CRLF>

RECEPTOR: 250 OK

El correo fue aceptado para los buzones de correo de Alejandro y Juan, en tanto que Jorge no tiene un buzón de correo en gamma.

Los mensajes tienen la siguiente estructura:

- Cabecera
- Cuerpo del mensaje

Cabecera

Puede verse como una línea lógica de caracteres ASCII, que se detalla en el RFC 822 con una sintaxis BNF[12], termina con una línea nula con la secuencia <CRLF>.

La cabecera es una lista de líneas de la forma field-name: field-values,

La columna 1 empieza con caracteres en blanco o tabulados, que se unen para formar un solo campo de forma canoníca.

Muchos campos importantes como el “para” y “de” son buzones y se los representa de la siguiente manera:

- correo@dominio.com
- El correo <correo@dominio.com>
- “El correo” <correo@dominio.com>

La cadena “El correo”, indica el propietario del buzón “correo@dominio.com”, el campo **<** y **>** delimitan la dirección de correo pero no forman parte de la misma, el cliente SMTP utiliza al DNS para determinar la dirección de destino del buzón.

Los campos más utilizados son:

To → receptores primarios del mensaje de correo

Cc → receptores secundarios del mensaje

From → identidad de quien emite el correo

[12] BNF, Backus-Naur form, que es una meta sintaxis para representar gramáticas libres de contexto tal como se hace en los lenguajes de computadora

Reply-to → buzón al que se deben enviar las respuestas y es añadido por el emisor.

Return path → ruta hacia el emisor y es añadida por el sistema que entrega el correo

Subject → es el asunto que tiene el mensaje, lo proporciona el usuario.

Cuerpo del mensaje

Todo lo que hay detrás de la línea nula es el mensaje como tal y está compuesto por caracteres ASCII, con valores menores a 128 decimales.

2.5.1.2. Modelo SMTP para intercambio de correo

El emisor SMTP establece comunicación en los dos sentidos con el receptor SMTP mismo que puede ser el destinatario final o un intermediario (pasarela de correo). Dicho emisor ha de generar comandos que serán replicados por el receptor.

Como se puede ver a continuación se ve la comunicación entre emisor y receptor SMTP

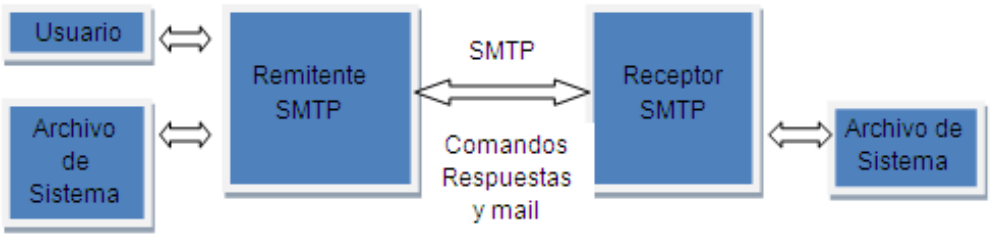


Figura 11: Modelo SMTP para intercambio de correo

Flujo de transacción de correo de SMTP

- El emisor SMTP establece conexión con el SMTP de destino, si se establece la conexión con el destinario se presenta la siguiente respuesta “220 Service ready”, y si el destinatario es incapaz de responder “421 Service not available”.
- Se envía un helo abreviatura de hello, de esta manera se verificará que se haya contactado con el servidor ya que el receptor devuelve su nombre de dominio.

  Si el emisor soporta extensiones definidas en el RFC 1615, puede sustituir el comando helo por ehlo, para ello el receptor debe deberá soportar dichas extensiones caso contrario devolverá el siguiente mensaje “500 Syntax error, command unrecognized”, si un receptor si soporta las extensiones manda el siguiente mensaje multi línea 250 OK.
- El emisor inicia la transacción por medio del comando MAIL, dicho comando posee la ruta de vuelta al emisor, además puede contener una lista de host de encaminamiento.
- Intercambio real de correo, consiste en darle al servidor SMTP el destino ya que puede haber más de un destinatario del correo lo que se hace enviando uno o más comandos RCPT TO: <forward- path>, que recibirá un mensaje de “250 Ok” si conoce el servidor el destino o caso contrario un mensaje de “550 no such user here”.
- Después de haber sido enviados los comandos “**rcpt”**, el emisor envía un comando DATA para notificar a quien va recibir el correo que se va a enviar el

contenido del mensaje, se recibe como respuesta a esto por parte del servidor "354 Start mail input, end with <CRLF>.<CRLF>"

- El cliente envía los datos línea a línea terminando con “<CRLF>.<CRLF>", de no existir inconvenientes el servidor responde con 250 OK
- Después de aquello puede ocurrir que quien envía no tenga más mensajes que enviar con lo que se cierra la conexión con el comando QUIT a lo que receptor responderá "221 Service closing transmission channel". Se pude presentar que el emisor no tenga mas mensajes para enviar sin embargo deba recibir correo por lo que mandará el comando TURN, los dos SMTP intercambiaran sus roles, y por último que el emisor deba enviar otro mensaje con lo que se volvería a enviar el comando MAIL.

El flujo que existe entre emisor y receptor es el siguiente:

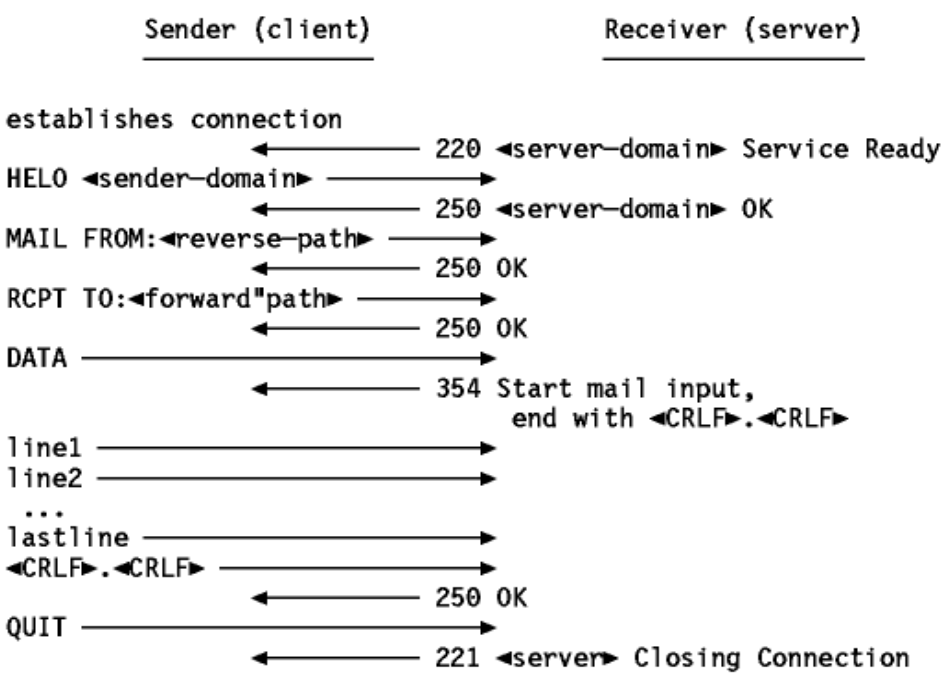


Figura 12: Flujo de transacción de correo SMTP[13]

2.5.2. Servidor de correo POP (Post Office Protocol).

Protocolo diseñado para recibir correo, de esta forma se descarga el correo desde un servidor de correo y es orientado a la conexión, los correos son descargados en las máquinas a menos que se guarde una copia en el servidor.

POP usa el término "maildrop" para referirse a un buzón gestionado por un servidor POP.

Autenticación de un usuario, es necesario que se identifique para que los usuarios puedan descargar el correo, por otro lado si el nombre de usuario y la contraseña suministrados coinciden con los del servidor, el usuario se autenticara y

[13] Tomado de http://ditec.um.es/laso/docs/tut-tcpip/3376c46.html#H536

pasara al estado de transacción, de no ser este el caso se rechazará la conexión hacia el servidor del que se requiere la descarga de correo.

2.5.3. IMAP (Internet Message Access Protocol).

Protocolo que sirve para recibir correo que se encuentra almacenado dentro del servidor, se diferencia de POP ya que funciona en dos modos orientado y no orientado a la conexión, lo que quiere decir que mientras la interfaz este activa se pueden descargar correos haciendo que la descarga sea más rápida, además los mensajes se descargan bajo demanda. Se guarda el mensaje dentro del servidor, hasta que el mismo haya sido eliminado directamente del servidor.

2.6. SPAM

Se conoce como SPAM a la práctica de enviar correo no solicitado de forma indiscriminada, generalmente se trata de publicidad de productos o servicios. La acción de enviar este tipo de correos electrónicos se conoce como spamming, nace el 5 de marzo de 1994 cuando una firma de abogados Canter y Siegel, hacen un anuncio de su firma legal se publico en USENET[14] con lo cual en ese entonces logró facturar 10.000 dólares debido a la cantidad de lectores que existieron.

Usualmente la mayoría de las direcciones de correo utilizadas para enviar este tipo de correo son falsas, para ello una de las soluciones es que el remitente firme sus mensajes mediante criptografía de clave pública o certificados digitales.

[14] USENET, Users Network, consiste en un sistema global de discusión en internet, donde los usuarios pueden leer o enviar mensajes sobre distintos grupos de noticias organizados de forma jerárquica.

Técnicas para envío de correo basura:

- Obtención de direcciones de correo, la mayoría de direcciones se las consigue a través robots o programas automáticos a través de internet, a continuación se presenta algunas de las formas para obtener la lista de direcciones de correo para envío de correo basura:

    - En las páginas web, ya que contiene las direcciones de su creador o de las personas que han visitado dicha página como es en el caso de los foros, etc.
    - En las cadenas de correo electrónico, generalmente no se las reenvía con copia oculta por lo que en un momento determinado puede tenerse una gran cantidad de direcciones de correo electrónico acumuladas de manera fácil.
    - Entrada ilegal en servidores de correo.
    - Por engaño y error, se generan de manera aleatoria direcciones de correo y se comprueba luego si llegaron los correos a los destinatarios, solo basta con conocer el dominio.

- Verificación de la recepción del correo, se envía correos con imágenes conocidas web bugs, de esta manera cuando se abre el correo uno solicita al servidor también la imagen, con lo que el spammer puede registrar que el correo ha sido abierto funciona como spyware. Otro método mas sencillo es

prometer que enviando un e-mail a una dirección se dejará de recibir este tipo de correos, por lo que este tipo de mensajes debe ser eliminado sin leerlo.

- Envío de correos, una vez que se tiene una lista de direcciones de correo extensa con direcciones válidas se envía correo por medio de programas para ello, consumiendo ancho de banda de los receptores ocasionando pérdidas de dinero.
- Zombis y troyanos, en computadores que no tienen protección de cortafuegos son utilizados como zombis[15], de esta manera pueden tener acceso a los discos duros y a los correos electrónicos que llegan al ordenador. Por otra parte este empieza a enviar correo spam a otros computadores, por lo que este puede ser identificado como spammer en los servidores a los que manda este tipo de correo.
- Servidores de correo que permiten open relay, no necesitan un usuario y contraseña para enviar correo a través de ellos.

Existe también algo conocido como hoax, que es el intento por convencer a un grupo de personas de que algo falso es real por medio del uso de correo electrónico, cuyo fin mas que nada es a manera de broma para hacer quedar mal a alguien.

El hoax tiene los siguientes objetivos:

[15] Zombis, se conoce así a los dispositivos que tras haber sido afectados por virus son utilizados por terceros para ejecutar sus actividades sin autorización del usuario.

- Obtener direcciones de correo.
- Engañar al usuario para que acepte un archivo y revele información como contraseñas.
- Confundir a las personas para que cambien su opinión con respecto a alguien o algo.

2.6.1. Open Mail Relay

Se da cuando un servidor SMTP se encuentra configurado de manera que permite que cualquier persona pueda enviar correo en internet a través de él, en gran parte por usuarios desconocidos. Con el paso del tiempo la mayoría de servidores SMTP con Open Mail Relay han sido cerrados, o han sido bloqueados a través de las listas negras.

El principal problema es cuando se usa el MTA (agente de transporte de correo), para enviar correo basura.

2.6.2. Listas Negras

Son listas en donde se registran las direcciones IP que generan SPAM, se las clasifica de la siguiente manera:

RBL, Real Time Blackhole List, fue la primera que se uso, y contienen una base de datos de direcciones desde donde se genera el SPAM, son altamente efectivas y diariamente bloquean mas allá de 30.000 correos no deseados a diario.

DNSBL, DNS Black List, es un acuerdo entre servidores DNS para bloquear dominios que generan SPAM por medio de su IP que son almacenados dentro de una base de datos.

DRBL, Distributed Realtime Block List, difiere de DNSBL en la naturaleza de la distribución ya que permite a cada red que establezca su base de datos.

DNSWL, DNS White List, lista de direcciones que indica quien envía SPAM, puede ser rara vez, nunca etc.

RHSBL, Right Hand Side Blacklist, es similar a DNSBL, pero a diferencia de este tiene en cuenta el nombre de los dominios más no la IP.

URiBL, Uniform Resource Identifier Blacklist, sirve para identificar objetos como las imágenes, etc. que son incluidas los correos electrónicos que tratan de esta manera de hacer visitar un sitio web, enumera los nombres del dominio usados en URIs en vez de direcciones de correo electrónico.

2.7. Soluciones para evitar correo no deseado

Tomando en cuenta las sugerencias que se hacen en el RFC 2505 (Anti-Spam Recommendations for SMTP MTAs), el correo no deseado debe ser rechazado cuando se produce el dialogo entre servidores SMTP, lo que quiere decir que el correo no debería llegar al servidor de correo del receptor, y al emisor debería llegarle un mensaje de error.

Códigos de error SMTP:

- 5xx, (Fatal error), quiere decir que la trasferencia ha finalizado y que el correo regresa al emisor del correo
- 4xx, (Temporary error), quiere decir que la trasferencia se pone en cola hasta que pueda realizar en un periodo posterior.
- 2xx, quiere decir que el MTA es el encargado en dicho punto para que se cumpla el envió del correo.

Debe ser posible, obtener un recibido del correo para rastrear el camino, de donde se origino el correo electrónico pese a que los spammers utilizan falsos nombres, además debe ser posible registrar los sucesos anti-spam o anti-relay y rechazar correo de un host o un grupo de hosts.

Existen cuatro categorías dentro de lo que es técnicas anti- spam y son las siguientes:

- Las que requieren de una acción por parte del usuario.
- Las que se automatizan por parte del administrador de correo.
- Técnicas automatizadas para remitentes de correo.
- Las que realizan los investigadores y gente encargada de hacer cumplir la ley.

Cuando se requiere una acción por parte del usuario

Dirección munging, sirve para camuflar la dirección de correo real, impidiendo que los programas informáticos puedan acceder a la dirección de correo real, esto se usa usualmente en USENET.

Responder a correo SPAM, hay que evitar responder a este tipo de correos, es mas no leerlos para que el spammer no pueda saber si la dirección a la que envío el correo es válida o no y no se siga enviando este tipo de correos.

Deshabilitar HTML en el correo electrónico, visualizaciones de imágenes, HTML y URL, en los clientes de correo que no descargan directamente automáticamente imágenes y adjuntos, disminuyen el riesgo de este tipo de ataques.

Automatización por parte del administrador de correo

Autenticación y reputación, se trata de dar al correo electrónico suficiente información para que este sea verificable esto se lo realiza de la siguiente manera:

- Verificación de la IP del remitente, el correo cuenta con cuatro actores como son el autor del correo electrónico, el remitente del correo quien pone el correo en internet, el receptor quien recibe el correo, y por último los destinatarios del correo. De esta manera lo que se hace es verificar la dirección IP del remitente por parte del receptor, el problema con ello es que los spammers pueden hacer una copia del correo incluidas cabeceras y un verdadero cuerpo del mensaje para de esta manera parecer un correo autentico con el objetivo de hacer phishing y obtener información como nombres, contraseñas y números de tarjetas de crédito.

- Listas negras, se marca en listas a las direcciones IP de los remitentes de correo con el fin de marcar a la dirección o bloque de direcciones de donde se está generando el correo no deseado, el problema generalmente con este

mecanismo es que los proveedores de internet usualmente dan direcciones IP dinámicas.

- Control de usuarios, se puede bloquear el puerto 25 a cambio de ello usar el puerto 587 a través del MSA (mail submission agent), es un software que recibe el correo de MUA (Mail User Agent) y coopera con el MTA para la entrega del correo, uno de los beneficios es que al usar el MSA se pueden corregir errores en el formato del correo como son el message ID, fecha, o completar una dirección que no posee el nombre de dominio, generando un mensaje de error al autor del correo. Otro beneficio es que separa la funcionalidad del MTA y MSA haciendo más fácil al MTA denegar el relay, que consiste en rechazar la transmisión de cualquier correo cuya dirección no se encuentre como un remitente valido para un dominio. Por otra parte el MSA acepta correo de cualquier remitente en internet permitiendo solo a los autores de correo que este autenticados en el MSA.

- Autenticación de remitentes, cuando llega una solicitud para entregar un correo se envía una consulta a un servidor DNS mismo que revisa si tiene autoridad para el dominio en cuestión enviando una respuesta para autenticar dicho correo. Formas de autenticar SPF/ DKIM/ SenderID, que se detallan más adelante.

- Helo/ Ehlo control, una de las operaciones que puede reducir hasta en un 25% el spam por correo entrante consiste en la validación del FQDN[16]. De esta manera se debe negar las transmisiones que no presentan un HELO válido es decir que no es FQDN o una IP rodeada por corchetes.

    - No valido

        HELO localhost

        HELO 127.0.0.1

    - Validos

        HELO dominio.com

        HELO [127.0.0.1]

Se debe rechazar el correo cuando se envíe desde un host que no sea autenticado.

Negarse a recibir correo electrónico cuyo argumento HELO / EHLO no se resuelve en el DNS.

Revisiones de DNS Reverso, la mayoría de MTA utilizan FCrDNS (Forward confirmed reverse DNS), y si es in nombre de dominio válido ponen un recibido en el campo de cabecera del correo.

Reglas basadas en filtrado, cuando los correos no tienen asunto o hay palabras claves o expresiones en el asunto, el administrador de correo poner en el

[16] FQDN, Fully Qualified Domain Name, es el nombre de dominio que no tiene ambigüedad, especifica la ubicación exacta dentro del árbol jerárquico del DNS a través de un dominio de nivel superior a la raíz de dominio.

filtro de configuración para no recibir correos con asuntos tales como “Prueba” por ejemplo.

Remitentes apoyados por listas blancas, Hay un número de organizaciones que ofrecen IP blancas o etiquetas de licencia que puede ser colocado en correo electrónico mismas que tienen un costo que dan garantías a los beneficiarios de los sistemas que los mensajes marcados por lo tanto, no son spam.

Hibrido de filtrado, utiliza programas de open source SpamAssassin y Policyd-weight que usa varios test y técnicas de filtrado.

SMTP callback verification, dado que gran cantidad de correo SPAM se produce a través de direcciones no válidas, se procede a hacer una conexión con el servidor de correo del remitente como si se tratará de un rebote con la finalidad de revisar si la dirección existe o no dentro del servidor.

Técnicas automatizadas para remitentes de correo

Filtrado de salida, busca controlar el tráfico de una red, es decir determina el tipo de tráfico que sale de la red interna hacia redes externas, logrando que el tráfico solo salga de determinados servidores.

Bloqueo de puerto 25 en firewalls y routers, de esta manera los proveedores de internet pueden bloquear el tráfico SMTP a través del puerto 25 a usuarios caseros y lo que se hace es permitir que envíen correo a través de un smart host.

Intercepción al puerto 25, busca que todo el tráfico SMTP vaya dirigido hacia el servidor de correo.

Limitación de tasas de envío, de esta manera se busca que un usuario legítimo pueda enviar un determinado número de correos en un determinado tiempo para prevenir que los usuarios no se conviertan en zombis.

Técnicas para los investigadores y aplicación de la ley

En la actualidad se ha hecho imprescindible que exista una coordinación entre investigadores, empresas de servicios financieros, empresas que brindan el servicio de internet y regulaciones de ley, ya que en actualidad a través del correo SPAM se puede obtener datos privados de los usuarios como son números de tarjetas de crédito, suplantación de identidad, etc.

Honeypots, simula ser un servidor de correo que permite open relay, con la finalidad de que los spammers se conecten a él y de esta forma obtener datos que ayuden a obtener su identidad.

Spamtraps, es una clase de honeypot que como finalidad tiene cosechar correo basura con la finalidad de analizar los contenidos de los mensajes de esta manera poder eliminar el spam que llega desde direcciones al granel es decir de varias direcciones de modo masivo con el mismo tipo de contenido.

2.7.1. Cerrar Open Mail Relay

Esta opción bloquea la retrasmisión abierta través de SMTP, y exige a los usuarios que se autentiquen en su servidor, a menos que los mismos sean de confianza a través de su IP y la misma este marcada dentro del servidor de correo.

La lista de IPs de confianza muestran los rangos de direcciones IP que considere dignos de confianza. Conexiones SMTP de estas direcciones IP se le permitirá sin autenticación.

2.7.2. SPF

Viene de las siglas en ingles Sender Policy Framework, su función es evitar la falsificación de direcciones de correo electrónico, mediante un convenio de remitentes.

Identifica a través de los registros DNS cuales servidores SMTP de correo están autorizados para enviar correo.

Cuando se envía un correo desde un programa cliente de correo electrónico, este se conecta con el servidor de correo del remitente quien se encarga de contactar al servidor de correo del receptor, para que después el destinatario del correo descargue el correo desde el servidor de correo, el problema se presenta ya que es imposible autenticar a todos los servidores entre sí, lo que permite que cualquier servidor remitente pueda identificarse como el trasportista en origen de un nombre de dominio.

Además SPF se divide por un lado en la publicación de los datos en el registro TXT del servidor DNS y por otra parte debe tener el software integrado al MTA para que se pueda realizar consultas dentro de nuestro servidor.

2.7.2.1. Configuración

A continuación se muestra como se configura un registro SPF dentro del servidor DNS.

dominio.net. IN TXT "v=spf1 mx ~all"

Donde,

v → define cual es la versión que se uso de SPF en este caso spf versión 1.

mx → autoriza solo a las maquinas con la IP que se encuentra en los registros mx.

~all → hace que las máquinas que no están autorizadas no puedan acceder.

Un dominio que controla directamente todas sus máquinas (a diferencia de un proveedor de acceso a Internet de banda ancha o acceso telefónico) permite a todos sus servidores enviar correo. Por ejemplo, hotmail.com

"v=ptr-spf1~all"

ptr → permite a las máquinas bajo el dominio en este caso podría hacerse para dominio.net.

“v = spf1 ptr: dominio.net-all”

IP4 → direcciones IP versión cuatro.

IP6 → direcciones IP versión seis.

EXISTS → si el dominio indicado existe.

En el caso de dominio.net, se está especificando que el correo solo salga desde el servidor de correo, es decir lo que este conectado dentro de la red en la que esta el servidor, por lo que usuarios que se conectan desde fuera de dicha red utilicen deben utilizar métodos de autenticación para el envío a través del servidor, con su nombre de usuario y contraseña SASL[17].

Ejemplo:

ejemplo.com. INTXT “v=spf1 ip4:200.110.237.0/27 –all”

Como se puede ver en el ejemplo anterior, si se tuviese el servicio en el servidor de correo al recibir un correo se verifica en el return-path con un valor @ejemplo.com, en primera instancia se verificaría el registro, una vez que se obtiene el valor del registro TXT se vería si la IP de origen de dicho correo esta dentro del rango 200.110.237.0/27, de no ser así el correo debería ser rechazado.

2.7.3. SIDF

El Sender ID Framework, verifica que cada mensaje de correo electrónico originado en internet sea enviado desde donde dice serlo, esto se logra con el

[17] SASL, Simple authentication and security layer, es un framework para la autenticación y autorización de protocolos en internet. Entre los protocolos que usan SASL están IMAP, LDAP, POP3, SMTP y XMPP.

control del servidor que envía el correo en comparación a la lista de dominios que el propietario ha autorizado para que puedan enviar correo, esto se ve dentro del registro SPF.

A continuación se muestra el diagrama del funcionamiento de SIDF:

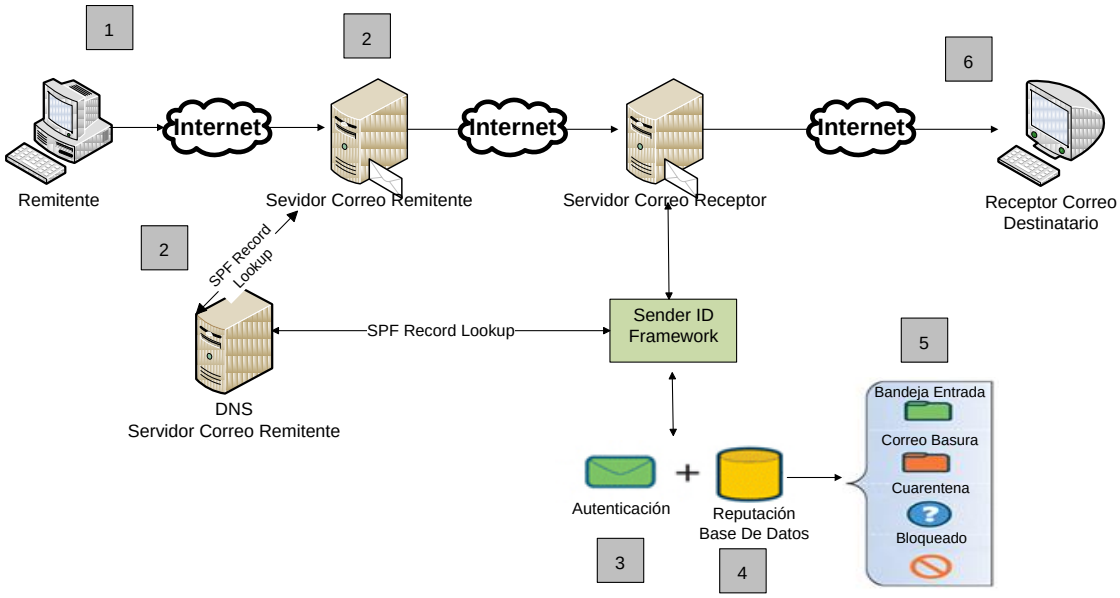


Figura 13: Funcionamiento SIDF (Sender ID Framework)

1. Un usuario envía un correo desde un cliente de correo o una interface web.
2. Se recibe el correo dentro del servidor de correo del remitente del correo, se verifica el registro SPF y autenticación del SMTP.
3. El MTA del servidor de correo del receptor comprueba que la dirección IP coincida con la que está autorizada para enviar correo al mencionado dominio.
4. Se verifica las IP y dominios dentro de la base de datos de reputación para veredicto de SIDF.

5. Basado en la sintaxis del registro SPF, si paso o no el veredicto de revisión, la reputación de quien envía el correo y filtro de contenido el MTA entrega el correo a la bandeja de entrada, bandeja de correo basura, pone en Cuarentena al mensaje de correo o lo bloquea.
6. El correo va a la bandeja de entrada y de correo no deseado dentro del cliente de correo del receptor del mensaje.

Una de las desventajas del SENDER ID es que no es un recurso abierto es decir que requiere licencia, al contrario de estándares abiertos de internet.

2.7.4. Firewall Anti Spam

Busca proteger del ingreso y salida de correo SPAM dentro de una red, algunos integran hardware y software. En otros casos solo se procede a comprar la aplicación, utilizan varias tecnologías a través de filtros para de esta manera proteger a los servidores de correo de ataques de spam, virus, spoofing, phishing y spyware.

Este tipo de firewall usa una serie de filtros y protecciones para el análisis de SPAM, de manera similar a como se muestra en las siguientes figuras.

Estructura tráfico correo entrante

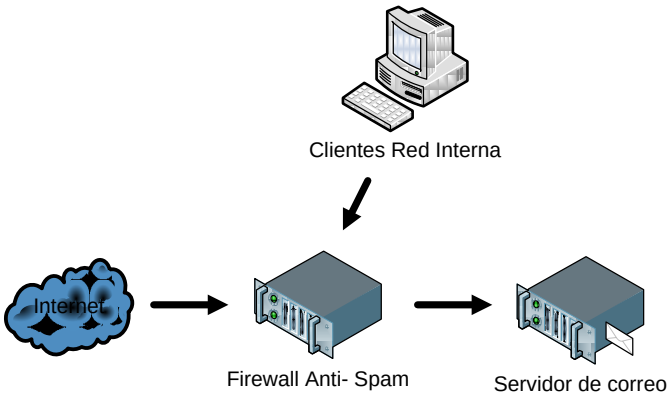


Figura 14: Estructura Correo electrónico entrante

Como se observa en la figura anterior los correos que llegan tanto de internet como dentro de la red donde se encuentra el servidor pasan por el firewall anti-spam, después de ello llegan al servidor de correo.

Arquitectura Firewall Anti- Spam para correo entrante

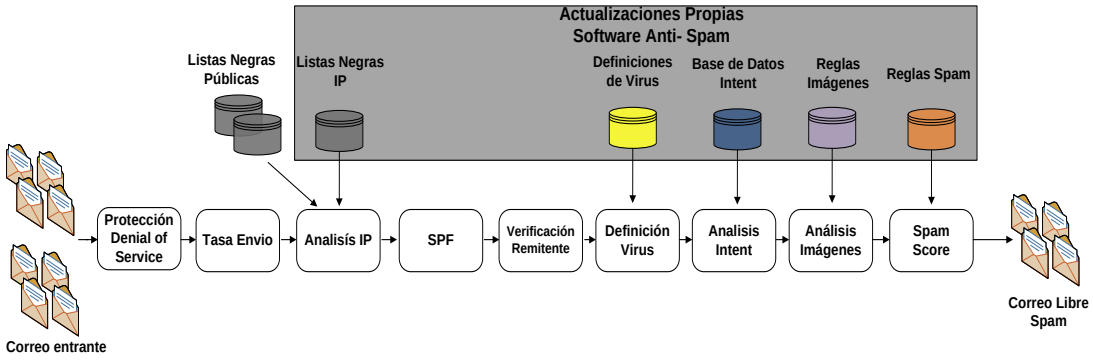


Figura 15: Arquitectura Anti- Spam correo electrónico entrante

Estructura tráfico correo saliente

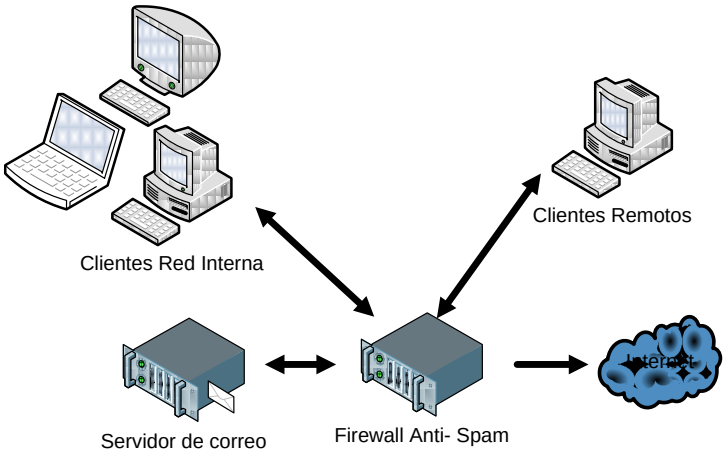


Figura 16: Estructura Correo electrónico saliente

Como se observa en la figura anterior los correos son enviados tantos desde clientes remotos como clientes locales así como desde el servidor de correo pasando por el firewall anti- spam, para ser entregado directamente a internet, al servidor de correo del remitente.

Arquitectura Firewall Anti- Spam para correo saliente

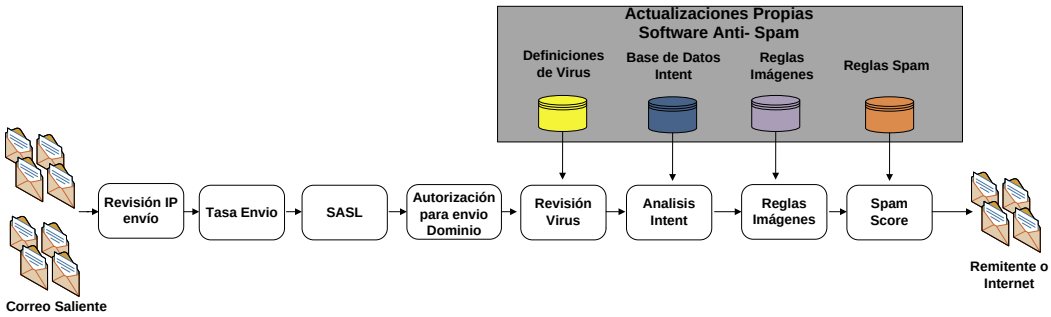


Figura 17: Arquitectura Anti- Spam correo electrónico saliente

Se específica algunos de los filtros y revisiones que realizan los servidores anti- spam que no fueron tratados en puntos anteriores, como parte de técnicas anti-spam.

Ataques por Denial of Service

Es un ataque que puede desactivar uno o más recursos dentro de una red como un enrutador o un servidor, haciendo que se produzca mayor consumo de ancho de banda.

Son paquetes elaborados de manera cuidadosa para de esta manera provocar un desbordamiento de búfer que desactiva un servidor y sus correspondientes servicios.

Análisis IP

Una vez que se realizan controles sobre las bases de datos encargadas de almacenar las direcciones IP, se procede a realizar un análisis de cada dirección.

Base de Datos propias del software anti- spam, es administrada por quien desarrolla la aplicación y se va actualizando con los reportes que generan cada uno de los firewall anti- spam instalados en otras partes del mundo, de esta manera se actualiza de manera constante la lista de remitentes válidos, así como los spammers conocidos dentro de los servidores centrales.

Exteriores a la base propia del software anti- spam, revisan las listas de bloqueo como Rbls o DNSBLs, hay organizaciones encargadas de actualizar dichas listas, por tanto permite al administrador del firewall definir una lista de servidores de

correo de confianza por su dirección IP. Además el administrador puede añadir nuevas direcciones IP.

Autenticación de autor de correo

Es una práctica común entre los spammers dar una dirección no válida de un dominio por lo que se realiza lo siguiente:

- Hacer cumplir que el remitente se especifique correctamente lo que quiere decir que cumpla las normas del RFC 821, que especifica que se debe poner nombres de dominio completo.
- Además es política que el remitente no este fuera de su infraestructura de correo electrónico.
- Marco de Políticas Remitente (SPF). SPF es una norma propuesta para evitar la suplantación de identidad.

Anti Virus

El análisis de virus precede a todas las técnicas de escaneo de correo, es decir revisa el correo aunque este se encuentre dentro de una lista blanca, y es bloqueado si un virus es detectado.

Análisis Intent

Todos los mensajes spam tienen una intención que es conseguir del usuario de una dirección de correo electrónico que viste una página web o llame a un número telefónico, de esta manera el software anti –spam busca identificar si estos datos son legítimos, es decir que se asocian a entidades legítimas.

Analiza la intención, realizando búsqueda de DNS contra URL conocidas en listas de bloqueo.

Análisis de imágenes

Hoy en día el spam por medio de imágenes representa alrededor de un tercio en el tráfico a través de internet.

El reconocimiento óptico de caracteres (OCR), de esta manera se analiza el texto que viene en conjunto con la imagen, además de analizar ciertas imágenes animadas que pudieran ser sospechosas.

Algoritmos Bayesianos

Es un algoritmo lingüístico, que analiza todo tipo de correo revisando los cuerpos de los mensajes y determinando si estos han sido recibidos en algún otro correo anterior comparando frases utilizadas, para verificar que no se trate de correo basura.

Puntuación de correo

Permite a los administradores configurar las puntuaciones de spam mundial, a través de varias puntuaciones que se miden de acuerdo a reglas.

CAPÍTULO III

ANÁLISIS DE SITUACIÓN ACTUAL DEL SERVIDOR DE CORREO Y SERVIDORES DNS DE ECUAONLINE

3. Situación actual del servidor de correo y servidores DNS de Ecuaonline.

3.1. Levantamiento de información

Servidor DNS: Ankaa

Solo se maneja un servidor DNS, que está registrado dentro de LACNIC como servidor autoritativo para las zonas reversas correspondientes a la red 200.110.232.0/21 asignada a la red de Ecuaonline. Este servidor es el servidor primario para los dominios de Ecuaonline.

Ocupa el sistema operativo base LINUX, distribución UBUNTU, Debian, en cuanto que al servidor DNS es BIND versión 9.3.2.

Los archivos de configuración están localizados en:

- /etc/bind/named.conf, este es el archivo principal de configuración de BIND
- /var/cache/bind/domains, dentro de este directorio se encuentran los archivos de zonas alojadas en el servidor
- /etc/bind, directorio de almacenamiento de claves de rndc.

Nombres registrados para el servidor:

- q1ns.ecuaonline.net

- q2ns.ecuaonline.net

Servidor de correo electrónico

El sistema de envió y recepción de correo actualmente tiene las siguientes características en cuanto al software:

- Sistema operativo Microsoft Windows 2003 server con Service Pack 1
- Servidor de Correo, Icewarp Merak Versión 8.0.3

El programa del servidor de correo se encuentra instalado en una partición del disco duro diferente a la del sistema, E:\Program Files\Merak, es decir no se encuentra en la misma partición que el sistema operativo.

Por otra parte el servidor de correo tiene un sistema Antivirus externo, que esta basado en el motor de McAfee, que se lo instala de manera manual. La versión que se encuentra instalada hasta el momento es la sdat5023 y las versiones actualizadas pueden ser encontradas en:

ftp://ftp.nai.com/pub/antivirus/superdat/intel/.

Se puede integrar con otros motores de antivirus, pero debe realizarse pruebas además este motor es gratuito.

El mecanismo Anti- spam está basado en Spamassassin, y el archivo de configuración lo mantiene el software del servidor de correo, la lista esta actualizada de manera manual.

Se puede crear el número que se necesite tanto de dominios como de cuentas, con los servicios POP, IMAP, IM, Groupware, SMTP, LDAP.

3.1.1. Diagrama actual del funcionamiento envío y recepción de correo

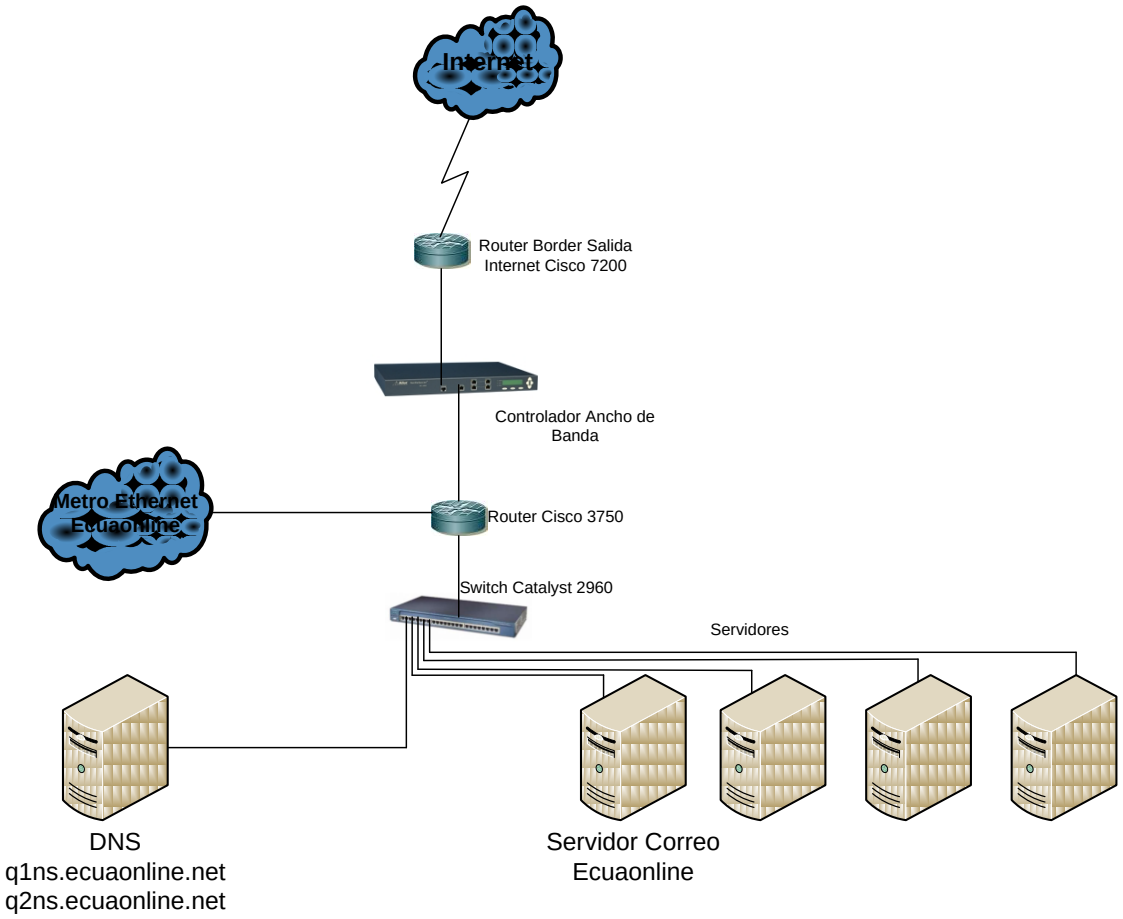


Figura 18: Situación actual funcionamiento de envío y recepción de correo dentro del proveedor

Como se puede ver en la figura 18, al momento solo se cuenta con un servidor DNS por lo que de existir problemas se debe poner un nuevo servidor, lo cual es un problema. Además de aquello el control Anti- Spam se realiza dentro del

servidor de correo, y los filtros que el mismo ocupa no son efectivos permitiendo el envío y recepción de correo no deseado.

Cualquier cliente puede hacer uso del protocolo SMTP para envío de correo desde cualquier ubicación causando problemas, ya que las las IP públicas pueden quedar marcadas dentro de listas negras por generación de spam.

3.1.2. Inventario de equipos en cuarto de servidores

Los siguientes son los equipos, con sus respectivas características que al momento operan dentro del cuarto de servidores de Ecuaonline S.A. que intervienen en funcionamiento del envío y recepción de correo electrónico.

Se detalla en la parte inferior los equipos que se encuentran dentro del cuarto de servidores de la empresa, así como la función que los mismos ocupan con respecto al funcionamiento de envío y recepción de correo electrónico.

Tabla 1: Inventario Equipos Cuarto Servidores del proveedor

Equipos Cuarto Servidores			
Router (Cisco)			
Marca	Modelo	Función	Características
Cisco	7200	Router de Border. Salida Internet.	4 interfaces FastEthernet, 256 MB ram, 256 MB flash SIMM,

			ios: disk0:c7200-is-mz.122-10g
Switch (Cisco)			
Marca	Modelo	Función	Características
Cisco	Catalyst 2950	Switch granja de servidores de Ecuaonline	24 puertos fast ethernet, 24 MB ram, 8 MB flash, ios: Lan *Base version* 12.1-22
Cisco	3750	Metro Ethernet, clientes y conexión a servidores.	Capa 3 24 interfaces Ethernet Gigabit, 128 MB ram, 16 MB flash, ios: c3750-advipservicesk9-mz.122-25.SEE.bin
Controlador de Ancho de Banda (Net Enforcer)			
Marca	Modelo	Función	Características
Allot Comunications	Net Enforcer AC - 402	Controlar el ancho de banda y la calidad de servicio	Memoria 512 MB Versión E5.5.3 Build 2
Servidores Linux			
Marca	Sistema Operativo	Función	Características
Clon	Ubuntu Linux BIND versión 9.3.2.	Servidor DNS (Domain Name System)	Pentium IV 1.8 GHz, 512 MB Ram, Disco duro 60 GB, 2 tarjetas ethernet 10/100 Mbps
Servidores Windows			
Marca	Sistema Operativo	Función	Características
Clon	Windows 2003 server	Servidor de correo electrónico para los clientes Ecuaonline	Pentium IV 1.8 GHz, 1024 MB Ram, Disco duro 160 GB, 2 tarjetas ethernet 10/100 Mbps

3.1.3. Recopilación de configuración de DNS y Mail server

3.1.3.1. Configuración de los registros y zonas dentro de servidores DNS.

Configuración del archivo principal de bind

Existe información descriptiva detallada de la siguiente manera:

Información sobre el nombre del servidor, y su IP asignada, así como de las personas que lo administran:

```
// DNS Server Name:          q1ns.ecuaonline.net
// Hostname:                       ankaa.ecuaonline.net
// Assigned IP Address:      200.110.232.2
//
// Maintained By:
//      - Ivan Fernandez
//      - Jorge Suarez
//
// Standard Zone Values
//     200xxxxx01   ; Serial yyyy/mm/dd/id
//          10800   ; Refresh (3 hours)
//           3600   ; Retry (1 hours)
//         604800   ; Expire (7 days)
//          43200 ) ; Negative Cache TTL (12 hours)
//
// Old Revisions Before Reconfiguration
//   - 02/01/2007: Changelog Started
//                 Full review of the configuration file
//                 Deleted old domains
//   - 16/01/2007: Added anniroses.com domain
```

Se detalla las fechas de creación y eliminación de una determinada zona, así como la persona que lo hizo.

Opciones de Control

Desde donde hay como controlar al servidor DNS

```
include "/etc/rndc.key";
//include "/etc/rndc.key-ns6";

acl "rndc-users" {
```

```
    200.110.232.0/27;
    201.219.12.0/28; // ! para negated
 };

controls {
       inet 127.0.0.1 allow { localhost; } keys { rndckey; };
//   inet * port 973 allow {"rndc-users";} keys {"rndc-remote";};
};
```

Opciones del servidor

```
options {
//       directory "/var/cache/bind"; // Debian Configuration
       directory "/var/named";
       dump-file "/var/named/data/cache_dump.db";
       statistics-file "/var/named/data/named_stats.txt";

//   forwarders {
//              192.26.92.30;
//              192.31.80.30;
//              200.110.232.2;
//       };

    recursive-clients 50000;
    listen-on-v6 { none; };
      auth-nxdomain no;    # conform to RFC1035
    allow-query { any; };
};
```

Zona Raíz de Internet

```
zone "." {
       type hint;
       file "domains/named.root";
};
```

Zona Primaria base

```
zone "ecuaonline.net" IN {
       type master;
       file "domains/ecuaonline.net";
       allow-update { none; };
       allow-query { any; };
};
```

Zonas reversas de operación de búsqueda

Se detalla en donde se almacenará la información de los registros de dichas zonas

```
zone "232.110.200.in-addr.arpa" IN {
        type master;
        file "domains/232.110.200.db";
        allow-update { none; };
        allow-query { any; };
};

zone "233.110.200.in-addr.arpa" IN {
        type master;
        file "domains/233.110.200.db";
        allow-update { none; };
        allow-query { any; };
};
```

Zonas directas de operación de búsqueda

Se encuentran divididas en clientes cuyo dominio se encuentran dentro de la red de Ecuaonline y servidores del proveedor.

```
zone "adrialpetro.com" IN {
        type master;
        file "domains/adrialpetro.com";
        allow-update { none; };
        allow-query { any; };
};

zone "anniroses.com" IN {
        type master;
        file "domains/anniroses.com";
        allow-update { none; };
        allow-query { any; };
};
```

Existe otro caso se presenta una descripción de cuando los clientes están dentro de la red de Ecuaonline pero ellos administran servidores de correo, web, ftp, o fuera de la red del proveedor.

```
zone "academiausa.edu.ec" IN {
    type master;
    file "domains/academiausa.edu.ec";
      allow-update { none; };
      allow-query { any; };
};

zone "g5corp.com" IN {
    type master;
    file "domains/g5corp.com";
      allow-update { none; };
      allow-query { any; };
};
```

Configuración de un archivo de una zona delantera de operaciones de búsqueda

Existen dos posibilidades, una de ellas es que el correo electrónico sea manejado por Ecuaonline, por lo tanto se detalla información sobre el servidor de correo en el registro MX, como se detalla a continuación.

```
$TTL    43200
@       IN      SOA     q1ns.ecuaonline.net. ifernandez.ecuaonline.net.  (
                              2007130401  ; Serial
                              10800       ; Refresh
                              3600        ; Retry
                              604800      ; Expire
                              43200 )     ; Minimum
; Name Servers Records.

        IN      NS      q1ns.ecuaonline.net.
        IN      NS      q2ns.ecuaonline.net.

; Mail exchange (MX records).

fca.com.ec.                     MX      5       mail.ecuaonline.net.
```

```
; Address (A) records.

mail                IN      A       200.110.232.4
```

Existe una segunda alternativa que el cliente maneje su propio servidor de correo y que dicho servidor este dentro de la red de Ecuaonline o que no lo esté. En la parte inferior se detalla el caso de que el servidor de correo este donde el cliente y dentro de la red del proveedor.

```
$TTL    43200
@       IN      SOA     q1ns.ecuaonline.net. ifernandez.ecuaonline.net.  (
                            2007130403  ; Serial
                            10800       ; Refresh
                            3600        ; Retry
                            604800      ; Expire
                            43200 )     ; Minimum
; Name Servers Records.

        IN      NS      q1ns.ecuaonline.net.
        IN      NS      q2ns.ecuaonline.net.

; Mail exchange (MX records).

      MX        05      mail.imbauto.com.ec.
      MX        10      mail2.imbauto.com.ec.
; Address (A) records.

mail        IN      A       200.110.239.11
mail2       IN      A       200.110.239.12
www         IN      A       200.110.239.11
```

Configuración de un archivo de una zona reversa de operaciones de búsqueda

A continuación se detalla una parte de la configuración la zona 232.110.200

```
$TTL    43200
```

```
@       IN      SOA     q1ns.ecuaonline.net. ifernandez.ecuaonline.net.  (
                                2007100703  ; Serial
                                10800       ; Refresh
                                3600        ; Retry
                                604800      ; Expire
                                43200 )     ; Minimum
; Name Servers Records.

        IN      NS      q1ns.ecuaonline.net.
        IN      NS      q2ns.ecuaonline.net.

; PTR Records

1               IN      PTR     athena.ecuaonline.net.
2               IN      PTR     q1ns.ecuaonline.net.
3               IN      PTR     q2ns.ecuaonline.net.
4               IN      PTR     q1ms.ecuaonline.net.
5               IN      PTR     q1ws.ecuaonline.net.
6               IN      PTR     servidores-uio.ecuaonline.net.
7               IN      PTR     servidores-uio.ecuaonline.net.
8               IN      PTR     www.ecuaonline.net.
9               IN      PTR     secure.ecuaonline.net.
10              IN      PTR     servidores-uio.ecuaonline.net.
11              IN      PTR     servidores-uio.ecuaonline.net.
12              IN      PTR     servidores-uio.ecuaonline.net.
13              IN      PTR     servidores-uio.ecuaonline.net.
14              IN      PTR     servidores-uio.ecuaonline.net.
15              IN      PTR     servidores-uio.ecuaonline.net.
16              IN      PTR     servidores-uio.ecuaonline.net.
17              IN      PTR     servidores-uio.ecuaonline.net.
18              IN      PTR     servidores-uio.ecuaonline.net.
19              IN      PTR     servidores-uio.ecuaonline.net.
20              IN      PTR     servidores-uio.ecuaonline.net.
21              IN      PTR     servidores-uio.ecuaonline.net.
22              IN      PTR     servidores-uio.ecuaonline.net.
23              IN      PTR     servidores-uio.ecuaonline.net.
24              IN      PTR     servidores-uio.ecuaonline.net.
25              IN      PTR     servidores-uio.ecuaonline.net.
26              IN      PTR     servidores-uio.ecuaonline.net.
27              IN      PTR     servidores-uio.ecuaonline.net.
28              IN      PTR     servidores-uio.ecuaonline.net.
29              IN      PTR     servidores-uio.ecuaonline.net.
30              IN      PTR     servidores-uio.ecuaonline.net.
31              IN      PTR     servidores-uio.ecuaonline.net.
32              IN      PTR     pool-uio1.ecuaonline.net.
33              IN      PTR     pool-uio1.ecuaonline.net.
34              IN      PTR     pool-uio1.ecuaonline.net.
35              IN      PTR     pool-uio1.ecuaonline.net.
```

3.1.3.2. Información configuración actual en el servidor de correo y de los dominios en el servidor

El servidor de correo posee el siguiente FQDN que es mail.ecuaonline.net, que es el nombre con el que ha sido registrado.

El servidor tiene la siguiente configuración en lo que al servicio SMTP se refiere:

El servidor no usa relay hacia ningún otro servidor y el tamaño máximo permitido para los correos en el envío es de 20 MB, con una capacidad de 100 MB para cada recipiente de los clientes quiere decir el número máximo de destinatarios del servidor período de sesiones permitidas en un mensaje saliente, usado para proteger su servidor de sobrecarga, todos los correos que no llegan a su destinatario llegan al usuario a través de un alias de reporte que es mailer-daemon.

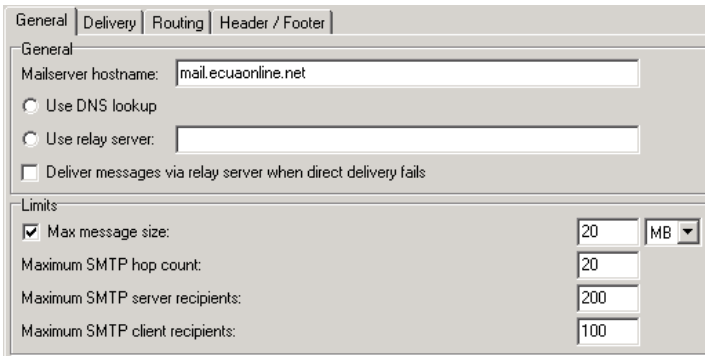


Figura 19: Configuración general de servidor de correo

Características de seguridad del servicio de correo

- El servidor permite la retrasmisión abierta (open relay), permitiendo el envío de correo desde cualquier locación, sin autenticación en lo que es envío de correo.

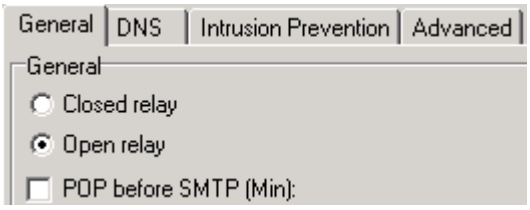


Figura 20: Configuración servidor para retransmisión abierta o cerrada

- Revisa en los siguientes servidores para ver si se encuentran en alguna lista negra:
    - dnsbl.sorbs.net
    - bl.spamcop.net
- Prevención de intrusos, bloque a los usuarios que sobrepasan las 100 conexiones por minuto, o que sus correos sobrepasen los 30 MB, bloqueándolos por un lapso de 25 minutos.
- Permite la retrasmisión únicamente si de donde se origina el correo es de un dominio local.
- En cuanto a filtros elimina correos que no tengan cabeceras.
- No tiene configuradas las redes o IP públicas de confianza, ya que se encuentra confifurado como open relay.

Características filtro Spam del servidor de correo

La lista de servidores para control de Spam de manera manual, SpamAssassin[18].

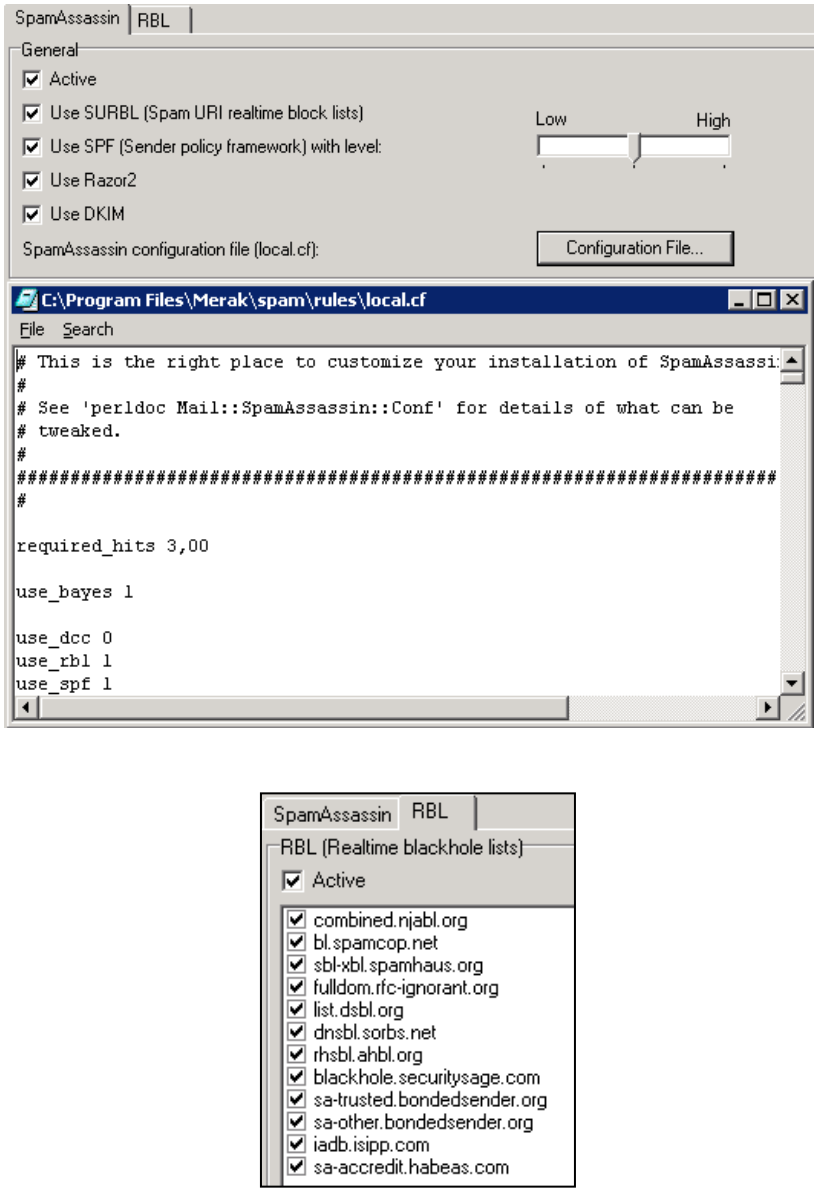


Figura 21: Configuración SpamAssasin en servidor de correo

Además de poseer un filtro bayesiano, y almacenar mensajes en cuarentena.

[18] Spam Assassin, tipo de *greylisting* basado en sus bases de datos internas cuando sospecha que alguna fuente de correo (servidor) está enviando mensajes de correo electrónico de tipo spam.

3.2. Análisis de información

3.2.1. Descripción de funcionamiento

Ecuaonline posee un solo servidor DNS que posee la siguiente configuración en sus interfaces:

eth0:100

addr:200.110.232.2 Bcast:200.110.232.15 Mask:255.255.255.240.

eth0:101

addr:200.110.232.3 Bcast:200.110.232.15 Mask:255.255.255.240.

Además en la interfaz que posee se encuentra la configuración para clientes de la red vieja con IP pública que proveía Andinanet S.A.

eth0

addr:201.219.12.1 Bcast:201.219.12.15 Mask:255.255.255.240

La información de las zonas se almacena mediante el siguiente estándar para el serial yyyy/mm/dd/id es decir año, mes, día, y el número de modificación que se ha realizado como ID.

En lo que se refiere al servidor de correo, este funciona como Open Relay permitiendo retransmisión desde cualquier punto tanto interno como externo a la red de Ecuaonline, no hay ningún tipo de restricción para los clientes y el uso del protocolo SMTP a través del puerto 25 esto quiere decir que desde cualquier punto

de la red de Ecuaonline se puede hacer uso de dicho puerto y enviar correo sin restricción.

No se analiza mayormente los correos salientes es decir desde la red interna de Ecuaonline usando el servidor de correo del ISP se envía cualquier tipo de correo, existe control para el correo entrante mediante el uso de SpamAssassin en un nivel medio y no se verifica la existencia del registro SPF, es decir utiliza la tecnología para determinar si un mensaje como procedentes de un dominio y originarios de otro es válido. Esto se basa en los registros DNS de su publicación, que no siempre es el caso, y un "softfail" puede ocurrir, por lo que la tecnología cree que el envío de host no es válido, pero no puede estar seguro.

Baja - Añade 0,1 a la puntuación de spam

Media - Añade 0,5 a la puntuación de spam

Alto - Añade 5,0 a la puntuación de spam - muy estrictos.

Y la puntuación que un correo necesita para ser considerado como Spam es de 3,00

Los dominios dentro del servidor de correo están configurados de la siguiente manera para todos los dominios que se encuentran registrados dentro del servidor:

A continuación se detalla la configuración del dominio

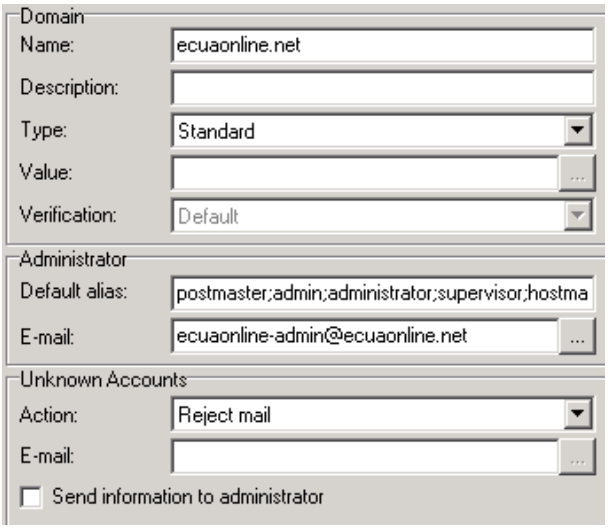


Figura 22: Configuración de un dominio en servidor de correo

Se tiene los campos con el nombre del dominio, seguido por una descripción, se posee también los tipos de dominio que pueden ser los siguientes:

- Campo Dominio
  - Dominio tipo estándar, el más común y como están configurados la mayoría de dominios dentro del servidor cada usuario tiene separado sus mailboxes.
  - Dominios tipo alias, esta opción permite hacer dominio hacia un dominio que debe estar como estándar, no necesita tener cuentas.
  - Dominios tipo backup domain, hace un forward a un servidor distinto, y el mx esta definido en los dos servidores pero en el servidor de backup domain tiene menor prioridad. Además se guarda una copia en el servidor.
  - Dominio tipo distribuid domain, sirve para poner múltiples servidores de correo en diferentes locaciones. Se configura dentro del dominio varios

registros mx de cada uno de los servidores, en los servidores el dominio debe ser configurado como distribuid domain, y el correo llega a la dirección de correo del servidor donde se encuentre creada la cuenta.

- Descripción, una breve descripción del dominio como la empresao razón social del cliente.
- Campo Administrador, especifica la ficha Administrador del dominio así como su Alias y cuentas de correo electrónico para el administrador del dominio:

  Alias, términos con los que se refiere al administrador del dominio

  Email, es la cuenta de correo del administrador de dicho dominio, cuando rebote un correo o sea necesario contactar al administrador llegará a esta cuenta de correo o de ella la información correspondiente, tiene relación con los campos del unknown users.

Además está configurado como dominio principal o primario ecuaonline.net dentro del servidor de correo, los usuarios pueden acceder desde mail.ecuaonline.net, indistintamente de cuál sea su dominio.

Las cuentas de correo tienen la siguiente estructura y están configuradas de la siguiente manera:

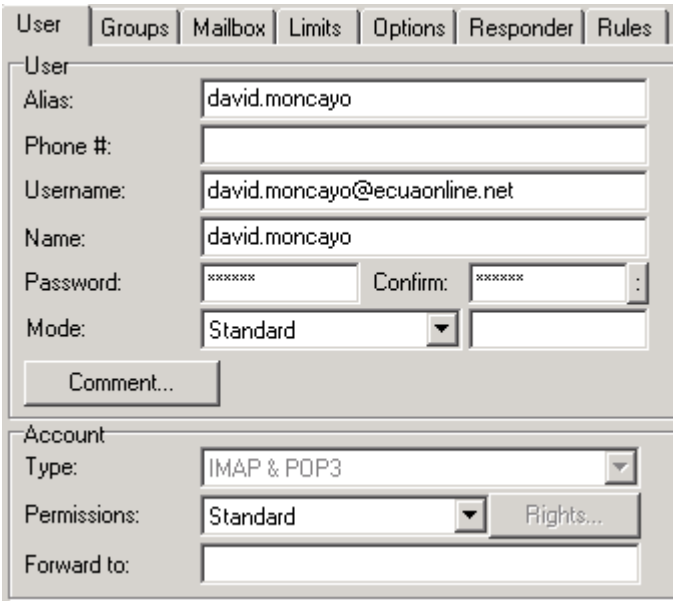


Figura 23: Configuración de cuentas de correo

Hay datos informativos del usuario, así como su alias que refleja el nombre que se va a desplegar cuando se cree la cuenta dentro del dominio.

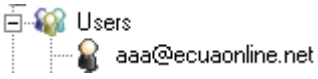


Figura 24: Vista de cuenta una vez que fue creada dentro del dominio al que corresponde

Los usuarios por estándar dentro del servidor se los ha configurado con el nombre de la cuenta seguido del dominio, es decir igual a la cuenta de correo. El campo del nombre posee una breve descripción del nombre y la empresa a la que pertenece o cliente en algunos casos.

Tipo, se refiere al tipo de mailbox que usa para la descargar los correos sea IMAP o POP3, y puede soportar los dos a la vez.

En lo que se refiere a permisos:

Standard, tiene acceso a todos los servicios, pero no puede realizar cambios en las cuentas de los usuarios. Puede cambiar contraseñas a través de webmail.

Domain Administrator, este usuario tiene acceso a los servicios, y además de ello puede modificar vía web los demás usuarios, pero solo de ese dominio.

Administrator, este usuario tiene acceso a los servicios y administrar tanto dominios como cuentas de todos los dominios registrados en el servidor.

En lo que se refiere a la configuración del mailbox, se puede especificar que se haga un forward a una cuenta de correo de esta manera los correos llegan a la cuenta original se almacenan en el mailbox de la misma y se reenvían a la otra cuenta.

Existe la posibilidad de usar un remote address (dirección remota) esto permite que los correos vayan directamente a la dirección de correo remota sin almacenarse en el mailbox de la cuenta de origen.

3.2.1. Análisis de problemas encontrados

- Open Relay, el servidor de correo permite la retransmisión desde cualquier punto, por lo que cualquier persona puede enviar correo a través del servidor, debido a esto la dirección IP del servidor ha sido enlistada en reiteradas

ocasiones a través de las listas negras ya que se envía correo basura a través del servidor.

- No existe las respectivas seguridades dentro del servidor de correo en cuanto a su configuración misma que debe ser reestructurada para la solución definitiva del inconveniente. Además el servidor tiene una dirección estática que no varía por lo que al estar como Open Relay en el momento que se empieza a generar SPAM queda fácilmente enlistado.

- Autenticación de autor de correo, no se garantiza dentro del proveedor que el correo entrante como saliente sea enviado desde los servidores de correo o direcciones IP autorizadas para hacerlo, esto se logra con el uso de SPF para evitar la suplantación de identidad, mediante un convenio entre remitentes a través de los registros dentro del servidor DNS, por lo que se debe buscar que esto se haga para el correo entrante mediante un software anti- spam, y proceder al cambio dentro de los registros del DNS a través del uso de SPF.

- Autenticación requerida para el envió de correo, garantizar que para el envío de correo sea necesario el uso de una contraseña logrando que el servidor de correo solo sea usado por quienes poseen cuenta de correo dentro del mismo.

- Bloqueo de puerto 25 en firewalls y routers, se debe hacer un filtrado de las direcciones IP dentro del proveedor para que de esta manera solo desde ellas se pueda enviar correo a través del puerto 25 de esta manera el proveedor puede bloquear el tráfico SMTP, evitando que las direcciones públicas sean enlistadas, este es un gran problema ya que al no estar bloqueado dicho puerto clientes como los café net que se han incrementado en gran escala dentro de la compañía generan tráfico de correo no deseado dentro del proveedor, y representan un gran problema.

3.2.2. Medición de desempeño

El desempeño en el último período del año ha ocasionado varios problemas dentro de la empresa ya que los correos no llegan a sus destinatarios debido a que Ecuaonline y su red ha sido marcada en varios servidores, como se ve en la parte inferior se muestra el nivel de generación de SPAM hacia Hotmail, por lo que en los meses de febrero y abril del año 2008 se presentaron varios bloqueos en listas negras como se muestra en la figura de la parte inferior.

A continuación se muestra parte de dicha lista:

Activity period [?]	RCPT commands [?]	DATA commands [?]	Message recipients [?]	Filter result [?]	Complaint rate [?]	Trap message period [?]	Trap hits [?]	Sample HELO [?]	Sample MAIL FROM [?]
Total: 77 days	**588,284**	**121,513**	**396,320**	**36 red days**	**0.2%**		**1,027**	**1 distinct values**	**65 distinct values**
4/10/2008 9:00 AM - 4/11/2008 7:00 AM	885	409	684		0.1%		0	mail.ecuaonline.net	cartera.cayambe@ferrostal.com.ec
4/9/2008 9:00 AM - 4/10/2008 8:00 AM	657	342	624		< 0.1%		0	mail.ecuaonline.net	amaldonado@pambaflor.com.ec
4/8/2008 11:00 AM - 4/9/2008 7:00 AM	627	344	605		0.3%		0	mail.ecuaonline.net	florpaxifinca@access.net.ec
4/7/2008 9:00 AM - 4/8/2008 6:00 AM	660	391	642		0.5%		0	mail.ecuaonline.net	mcano@secure.ecuaonline.net
4/5/2008 9:00 AM - 4/6/2008 6:00 AM	151	106	146		0.7%		0	mail.ecuaonline.net	airport@ticargo.com
4/4/2008 8:00 AM - 4/5/2008 7:00 AM	30349	4417	18952		< 0.1%	4/4/2008 1:33 PM - 4/4/2008 5:59 PM	75	mail.ecuaonline.net	systems@ticargo.com
4/3/2008 8:00 AM - 4/4/2008 8:00 AM	478	322	460		0.9%		0	mail.ecuaonline.net	munipm@cyb.ecuaonline.net
4/2/2008 11:00 AM - 4/3/2008 4:00 AM	1646	923	1407		0.2%		0	mail.ecuaonline.net	florpaxifinca@access.net.ec
4/1/2008 1:00 PM - 4/2/2008 6:00 AM	472	290	451		< 0.1%		0	mail.ecuaonline.net	gespinosam@pilvicsa.com
3/31/2008 8:00 AM - 4/1/2008 5:00 AM	701	386	679		0.6%		0	mail.ecuaonline.net	gespinosam@pilvicsa.com
3/29/2008 10:00 AM - 3/30/2008 8:00 AM	118	85	115		< 0.1%		0		

Figura 25: Smart Network Data Service[19]

Como se puede ver en muchas ocasiones son cuentas de correo de proveedores externos a la empresa, es decir usan el SMTP de la compañía para el envío de correo haciendo que la IP pública del servidor de correo y las IP públicas asignadas a clientes caigan dentro de listas negras. Esto ocasiono que no se pueda enviar desde la red de Ecuaonline correo hacia el dominio de Hotmail.

Es decir los usuarios de la red usan el servidor del proveedor para enviar correo desde cualquier locación, y este al permitir la retransmisión abierta no autentica a las cuentas para lo que es el envío

Tabla 2: IP públicas listadas en el mes de Abril de 2008

Smart Network	# VECES

[19] Tomado de http://postmaster.live.com/snds

Data Service	(periodo Abril 2008)
200.110.235.28	5
200.110.233.30	3
200.110.238.12	2
200.110.232.162	2
200.110.232.107	1
200.110.237.167	6
200.110.239.18	1
200.110.233.43	4
200.110.233.30	5
200.110.235.47	1
200.110.238.13	1
200.110.238.109	1

Dichas IP públicas fueron reportadas como generadoras de SPAM durante el mes de abril, y corresponden en gran cantidad a IP públicas son las que están asignadas a café net principalmente localizados en las ciudades de Otavalo e Ibarra. Con respecto al mismo período de tiempo mediante el uso de la herramienta Smart Network Data Service de Windows Live se determino las IP públicas por las cuales Hotmail no permitía el envío hacia su dominio como se ve en el cuadro anterior.

Las IP que se despliegan a continuación son las que aparecieron en los servidores de SPAMCOP en el mes de abril.

Tabla 3: IP públicas listadas en el mes de Abril de 2008 en SPAMCOP

IP REPORTADAS	# VECES
200.110.235.28	1
200.110.233.30	1

200.110.235.33	3
200.110.233.43	2

Como se puede ver en el mes de febrero de 2008 se producía mayor cantidad de correo basura como se ve en la tabla inferior lo cual se redujo con el control en cuanto a servicios dentro del controlador de ancho de banda de la empresa pero no se redujo en su totalidad y se seguían presentando problemas de generación de SPAM desde la red de Ecuaonline.

Tabla 4: IP públicas listadas durante el mes de Febrero

Estas son las IP que tuvieron problemas durante febrero 2008	
200.110.237.76	200.110.232.106
200.110.235.12	200.110.232.254
200.110.235.40	200.110.234.71
200.110.235.28	200.110.232.4
200.110.236.195	200.110.238.110
200.110.235.42	200.110.235.22
200.110.238.205	200.110.232.162
200.110.239.2	200.110.235.9

Como se puede apreciar durante los meses de febrero, marzo y abril de 2008 existió gran incidencia en generación de Spam desde la red de Ecuaonline, por lo que se hacia imposible enviar correo.

A continuación se muestra uno de los reportes SPAMCOP durante el mes de abril de 2008.

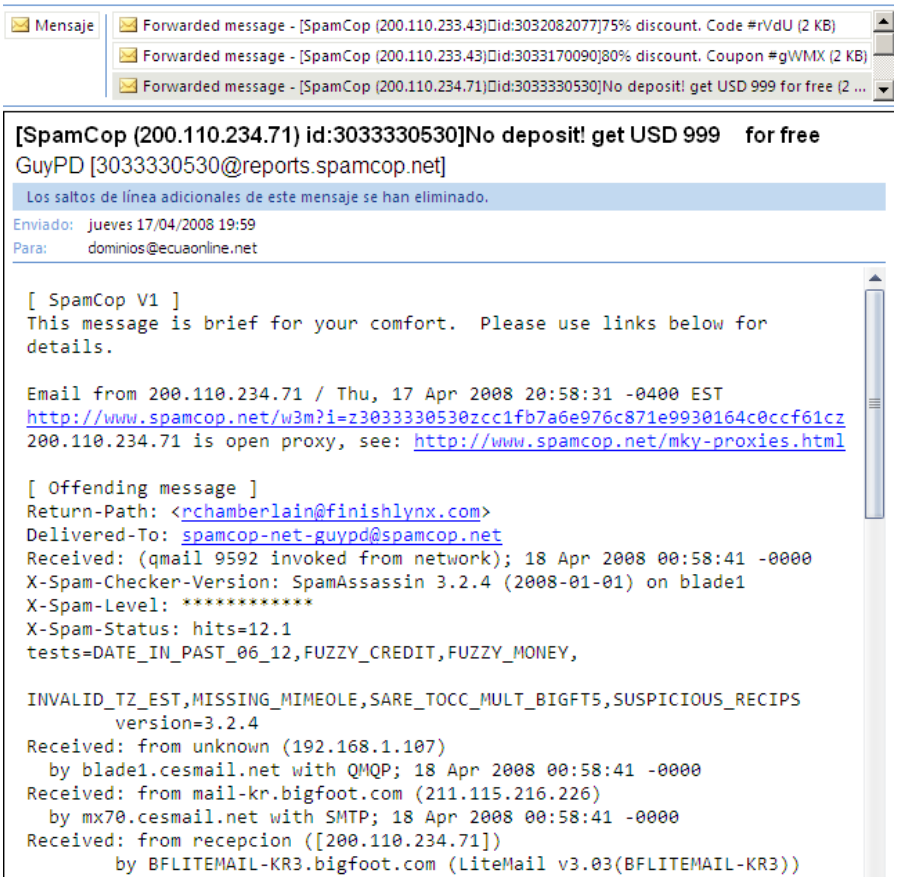


Figura 26: Información correo generado por parte de SPAMCOP

Hace referencia a que un proxy puede ser utilizado por un spammer para enviar anónimamente correo Spam, el correo que se generaba tenía la siguiente información en el cuerpo del mensaje

```
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
       Are you bored and want some excitëment?
   Las Vegas Has Just Showed Up In Yoour Neigbourhood!
  In fact, you wont evenn have to leavee your çomputer!
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-


 Onlinee Casino Advantages:
-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
```

* Plày in your pyjamas
* Plây for fun optionn (without gambling möney)
* Free money to play with!
* Confidential and safê
* No travel headaches
* No hotel bill suprises
* Täke your time playingg!
* Play with ýour crëditcard
* Get advice as you pláy!
* AAlmost 98% payout!

CAPÍTULO IV

DISEÑO E IMPLEMENTACIÓN DE SOLUCIÓN ANTI SPAM

4. Diseño de solución Anti Spam

4.1. Proyección a futuro

El crecimiento sin ningún tipo de control ni restricciones en la red de Ecuaonline ha hecho que se produzcan problemas con los clientes en lo que se refiere al envío y recepción de correo, se ha incrementado el número de clientes y cada vez más existen algunos que no ocupan el servicio SMTP, pero sin embargo por virus presentes en sus máquinas que empiezan actuar como zombies se produce tráfico SMTP que con el transcurso del tiempo hace que las IP públicas del proveedor estén marcadas dentro de listas negras.

Con un mayor control se logra que no se consuman recursos innecesarios dentro de la red del proveedor y que los correos lleguen a sus destinatarios y el cliente no consuma gran ancho de banda en recibir correos basura que hacen que en ocasiones se sature su enlace perdiendo tiempo no solo para recibir correo sino además al momento de leer los mismos debido a la cantidad de correo electrónico que llega al buzón de entrada.

Se debe definir el número de dominios y cuentas de correo que existe dentro de cada uno de los dominios para tener una proyección de crecimiento de usuarios

de correo para determinar el hardware y software a emplearse asi como el tipo de licencias.

Tabla 5: Proyección de crecimiento por dominios y cuentas de correo activas

Proyección de Crecimiento			
Servidor	**# Clientes Actuales**	**# Clientes proyectados**	**Crecimiento**
Correo Ecuaonline			
Dominios	57	67	10
Cuentas de Correo	660	900	240
Externos Administrados por proveedor			
Dominios	5	10	5
Cuentas de Correo	85	185	100

Todas estas cuentas de correo y dominios van a estar configuradas dentro del firewall anti – spam del proveedor.

4.2. Análisis de requerimientos

La configuración actual presenta inconvenientes ya que no existe un control efectivo del correo no deseado, el problema que se ha vuelto recurrente se debe a que varias IP públicas están siendo marcadas dentro de listas negras, y se consume gran ancho de banda con la generación tanto interna como externa de correo basura.

Se necesita un mayor control especialmente para los clientes que están dentro de la red del proveedor, además de que el servidor de correo actualmente

permite retransmisión directa, por lo que los requerimientos principales son el control a los usuarios del servicio SMTP para evitar la generación de correo basura, así como el control a través de un firewall anti – spam para el filtrado de correo electrónico.

Equipos Firewall Anti Spam

A continuación se detalla los posibles equipos a ocuparse para la solución que mas se ajuste a la empresa de acuerdo al número de dominios y cuentas de correo.

Firewall Barracuda

Presenta una solución integrada entre hardware y software para proteger a los servidores de correo, es compatible con todo tipo de servidor de correo, dependiendo del modelo de servidor puede soportar hasta treinta mil usarios activos de correo.

Presenta las siguientes especificaciones técnicas que están distribuidas dentro de las 12 capas para el análisis que el firewall posee y son las siguientes:

Protección

- Filtrado de Spam y virus
- Previene spoofing y phishing
- Protección por Denial of Service
- Filtrado de correo saliente

Filtro SPAM

- Análisis de IP
- Análisis Fingerprints
- Análisis de Imágenes
- Reglas basadas en algoritmos basadas en puntajes
- Algoritmos bayesianos

Autenticación de remitente

- SPF

Filtro de virus

- Protección real anti virus

Los usuarios finales pueden ver los correos que han sido puesto en cuarentena y tienen la posibilidad de darles un puntaje y permitir los que sean necesarios.

Debido al número de usuarios de correo y número de dominios el proveedor se necesita el modelo de Barracuda cuatrocientos ya que acepta un número de mil a cinco mil usuarios de correo activos y hasta quinientos dominios; o como mínimo el modelo trescientos, de acuerdo a las características del cuadro que se muestra a continuación.

Tabla 6: Barracuda Anti Spam, cuadro comparativo por modelo de Firewall Anti-spam

Modelo / Comparación	Modelo 100	Modelo 200	Modelo 300	Modelo 400	Modelo 600	Modelo 800	Modelo 900
Capacidad							
Usuarios activos e mail	1 -50	50- 500	300- 1000	1000-5000	3000-10000	8000-22000	15000-30000
Dominios	10	50	250	500	5000	5000	5000
Log almacenado de mensajes	512 MB	1 GB	2 GB	10 GB	20 GB	40 GB	60 GB
Mensajes en Cuarentena			10 GB	50 GB	100 GB	200 GB	250 GB
Características							
Compatible con servidores de correo	si	si	si	si	si	si	si
MS Exchange / LDAP	no	no	si	si	si	si	si

El costo del producto modelo cuatrocientos en el país es de alrededor de 9.000 a 10.000 dólares que es alto dentro de los cambios que se deben hacer.

Firewall Spam Titan

Esta solución de software presenta una solución para eliminar el correo no deseado a través de las siguientes características dentro de las 7 capas que este maneja.

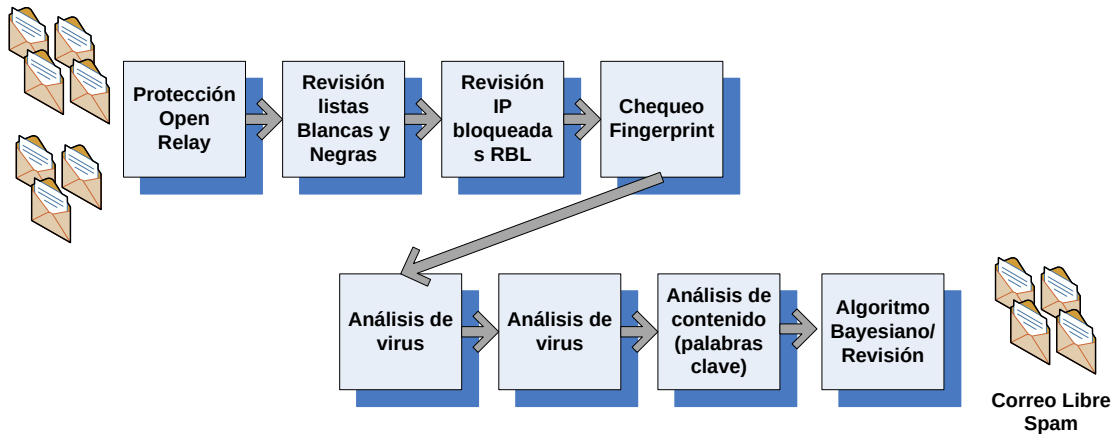


Figura 27: Capas de análisis control Anti Spam (Spam Titan)

Protección doble antivirus, utiliza dos antivirus para el control de virus en correo entrante y saliente a través de Kaspersky anti virus y Clam AV, mismas que se actualizan periódicamente.

Análisis multicapa para control de Spam, incluye mediante el uso de capas las siguientes características de seguridad el uso de SPF dentro del software del la verificación de la existencia del remitente, uso de algoritmo bayesianos, análisis tanto del asunto como del cuerpo del mensaje de correo a través de puntajes para determinar si se trata de un correo SPAM.

Filtro de contenido de correo, se incluye un análisis de los documentos adjuntos, para que no se reciba cierto tipo de archivos.

Listas Blancas y negras que pueden ser vistas por cada una de los usuarios una vez que se encuentre activado el reporte del dominio y de las cuentas de los usuarios. Además los usuarios pueden acceder a ver los correos que han sido considerados como SPAM o que tiene contenido tal como virus o extensiones no permitidas, dentro de la carpeta cuarentena.

Reportes, se encuentra reportes de diagnóstico así como reportes del funcionamiento referentes a donde se está generando correo no deseado tanto interna como externamente. Así como la detección de virus y correos electrónicos en determinado periodo de tiempo. El costo de licencia es de alrededor de dos mil dólares.

Pineapp

Incorpora el control de tráfico no deseado incluyendo control de virus, spam y phishing, independientemente del contenido, analizando las IP y las cabeceras de los mensajes de correo electrónico, liberando ancho de banda y recursos para que se pueda analizar el contenido de los restantes mensajes de correo electrónico.

Sistema de detección de zombis, protege a través del bloqueo de tráfico de correo saliente de ordenadores infectados mediante protección en niveles de IP y según la cabecera de cada correo, protegiendo la reputación de la organización, dominio.

Motores anti virus, posee cinco motores anti virus a traves de Mail- Secure y F- Secure.

Control de contenido inapropiado, implica una búsqueda en la base de datos de Watch Foundation, control de contenido en internet de esta maneras pude bloquear contenido tal como pornografía.

Servidor de correo opcional, tiene un módulo de correo opcional donde se puede crear y administrar cuentas de correo.

Comparación de series	1000	2000	3000	5000
Licencia (usuarios de correo)	Hasta 50	Hasta 500	Hasta 1500	Hasta 10000
Control del cumplimiento de las directivas	Global	Directiva de tres niveles	Directiva de tres niveles	Directiva de tres niveles
Balanceo de carga interno *		✓	✓	✓
Protocolos examinados	SMTP, POP3			
Protocolos de servicios de correo	ESMTP/S con soporte para autenticación LDAP, POP3/S, IMAP4/S, acceso Web**			
Protocolos de entrega de correo	SMTP/S, POP3 Modo "pull" y local**			
Motores antivirus	5 motores que incluyen: F-Secure®, Zero-Hour™ y un motor heurístico de PineApp			
Motores antispam	11 capas, que incluyen: RPD™ (detección de patrones recurrentes), RBL, ZDS™ (sistema de detección de zombis), bayesianos y reglas			
Interfaces de red	1XGbE***	4x10/100Mbps	4XGbE	4XGbE
Tamaño de almacenamiento	80 GB	80 GB SATA	80 GB SATA	2X73/146GB SAS (RAID1)
Dimensiones (ancho x profundidad x altura)	31x35,8x8,75 cm (12,2x14,1x3,4 pulg.)****	42,9x36x4,4 cm (16,9x14,2x1,7 pulg.)	42,9x38,2x4,4 cm (16,9x15x1,7 pulg.)	43,2x61x4,4 cm (17x24x1,7 pulg.)
Garantía	1 año de garantía limitada			
Certificaciones	FCC, CE, UL, CUL, CB, RoHS	FCC, CE, LUV, RoHS	FCC, CE, LUV, RoHS	CE, CB, FCC, LUV, UL, RoHS

Figura 28: Cuadro comparativo por modelo Pineapp Anti Spam[20]

En el caso del proveedor de requiere del modelo dos mil o tres mil por el número de usuarios de correo debido a la licencia, este firewall anti spam presenta

[20] Tomado de http://www.pineapp.com/products.php?ms2000

algunos beneficios que no muestran los dos anteriores pero su costo es superior se lo encuentra a este equipo israelí por aproximadamente quince mil dólares.

4.3. Infraestructura para equipamiento necesario

4.3.1. Selección de Hardware y Software a emplearse

En la salida a internet existe un Router de borde Cisco 7200, en donde se configurará la lista de acceso para los clientes que tienen o no restricción en lo que al uso del protocolo SMTP se refiere, el equipo ya se encuentra funcionando actualmente.

Para lo que es el Core existe un switch Catalyst 3750, este equipo de capa 3 nos permitirá concentrar las características de enrutamiento, es un punto central de la red en lo que se refiere a la conexión con los clientes.

Servidores DNS, se utilizará dos equipos Cisco Content Engine, que utilizaran el sistema operativo GNU Linux con la distribución 8.04.1, serán configurados el uno como primario y el otro como secundario garantizando de esta forma que en el caso de que se presente alguna falla con el DNS primario de la empresa se pueda seguir trabajando a través del servidor secundario.

Servidor de correo, se seguirá usando el mismo software Merak, pero será instalado en un servidor HP Proliant DL 380 G5, donde además será instalado el

software anti spam aprovechando de esta manera al máximo los recursos de dicho equipo.

Para ello se instalara VM Ware dentro del servidor. Se modificará varios parámetros dentro de la configuración inicial.

Se utilizará el firewall SPAM Titan debido al costo de la licencia y además debido a que la aplicación permite ser instalada dentro de una máquina virtual en el servidor, con una base Linux robusta incluyendo scripts para la instalación funcionando en las siguientes versiones de VM Ware:

VMware Workstation

VMware Server

VMware Player

Esta aplicación permite hacer un control tanto del tráfico de correo entrante como saliente, genera reportes y permite que haya administradores de cada uno de los dominios, asi como administrador de toda la aplicación

Por lo que en total se requerirá una inversión de seis mil seiscientos dólares, entre licencias y el servidor que se va a utilizar para la implementación.

A continuación se detallan los equipos que va a ser utilizados, y que deben ser comprados para la implementación de la solución:

Tabla 7: Equipos y propósito dentro del cuarto de servidores

Equipo	Cantidad	Propósito	Costo (dólares)
HP Proliant DL 380 G5	1	Servidor de correo en el que estarán los dominios y las cuentas de cada una de ellos así como el software anti virus, y filtros bayesianos. Servidor Web server	$ 3071 incluido impuestos
Aplicación Spam Titan	1	Firewall anti spam, filtro de correo no deseado. Número de usuarios activos 750	$ 2000 dólares (licencia por un año de uso)
VM Ware Server	1	Se pondrá las máquinas virtuales de los respectivos servidores	$ 1500 dólares

4.4. Diseño de la solución

Los siguientes números de VLAN están asignados con su respectiva IP para equipos administrativos.

Tabla 8: Identificación de VLAN para servidores

Metro Ethernet Proveedor			
Vlan Id	**Descripción**	**Subred**	**Subred Clientes**

		Administración	
Oficinas Ecuaonline			
400	Switches Backbone	10.250.0.0/25	NA
401	Servidores	10.250.1.0/24	200.110.232.0/27

4.4.1. Diagrama lógico de solución dentro del proveedor

El diagrama que se detalla a continuación describe la topología lógica de la conexión de los servidores que intervienen en el intercambio de correo dentro del proveedor, así como la forma en la que se realiza el control de correo no deseado y uso del protocolo SMTP por parte de los usuarios.

Se muestra la forma como se encuentra la conexión de los servidores así como la salida desde el proveedor hacia internet, y el tipo de conexión que los mismos tienen hacia los servidores tanto dentro como fuera de la red del proveedor, mostrando el funcionamiento de la implementación que se realizó para servidores de correo de clientes que ocupan el servidor anti- spam, como para los que no lo ocupan.

Detalla también el tipo de conexión dentro del proveedor y como se va a realizar el filtrado de tráfico SMTP, y el tipo de solución dentro de los diferentes escenarios con respecto a servidores de correo y usuarios

Se muestra el diagrama con la topología lógica de conexión

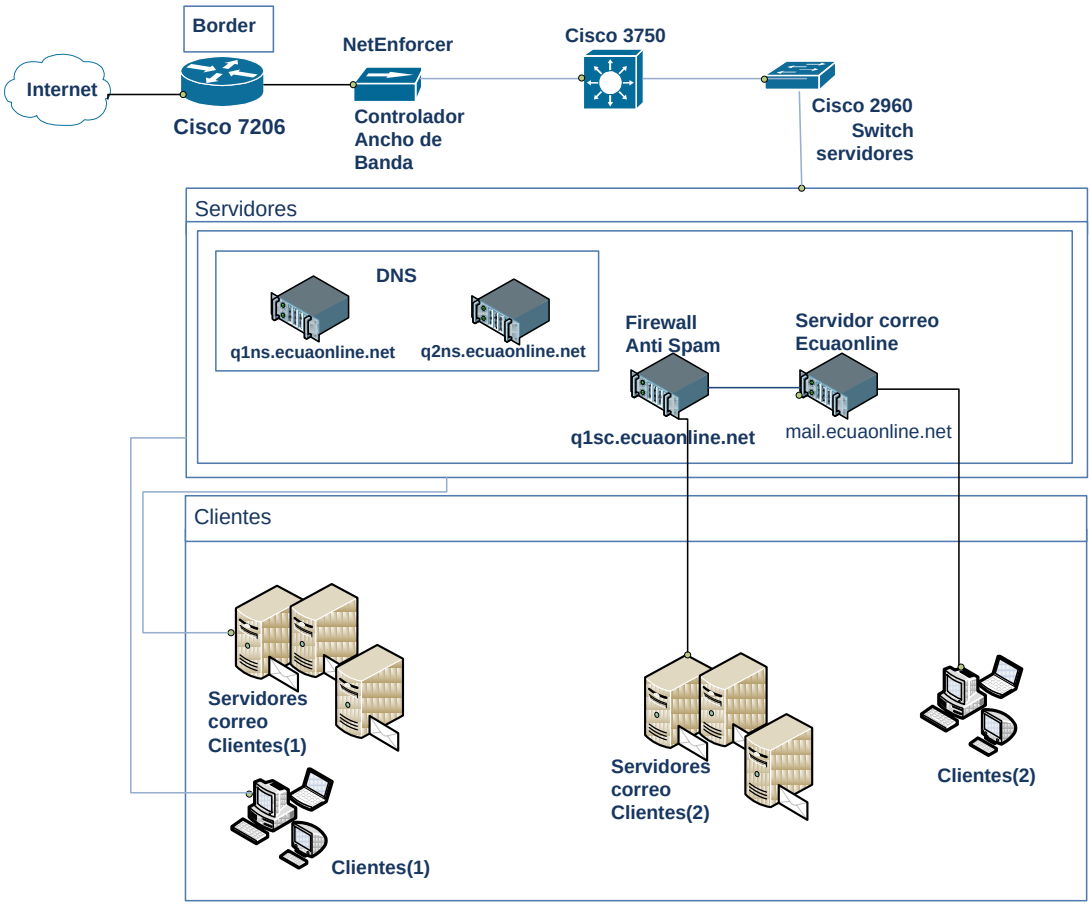


Figura 29: Diagrama Lógico funcionamiento de entrega y recepción de correo electrónico

Servidores de correo clientes (1), son los clientes que poseen su propio servidor de correo dentro de la red de Ecuaonline y el control de Spam lo realizan directamente mediante su servidor, se les permite el uso del puerto 25 y el servicio SMTP a través de listas de acceso que están configuradas en el Router de borde del proveedor.

Servidores de correo clientes (2), son los clientes que tienen su propio servidor de correo, pero que se realiza retransmisión de su servidor de correo hacia

el firewall anti – spam del proveedor para que de esta manera el servidor q1sc.ecuaonline.net sea el encargado del intercambio de correo.

Clientes (1), son los clientes cuyo servidor de correo esta fuera de la red del proveedor, se les permite el uso del puerto 25 y el servicio SMTP a través de listas de acceso que están configuradas en el Router Border del proveedor. Solo para casos específicos de determinados clientes se permite esta opción, ya que de lo contrario se generaría correo no deseado desde la red del proveedor.

Clientes (2), son los clientes que ocupan el servidor de correo de Ecuaonline, la gran mayoría tienen alojado su dominio en el servidor de correo del proveedor y algunos otros ocupan el dominio ecuaonline.net para el envío de correo a través del servidor, por lo que para los clientes que solo lo usan para el envío y no tienen el dominio dentro del proveedor se debe crear una cuenta para que puedan autenticar el envío de no ser posible deben estar dentro de la lista de acceso, la IP pública del servidor SMTP del cliente. Véase el caso anterior, clientes (1).

Los clientes que tienen su dominio dentro del servidor de correo de Ecuaonline y tienen el servicio de Internet con otro proveedor al momento de enviar correo deberán hacerlo usando el puerto 465 para evitar falsificación de identidad y que se permita la conexión SMTP hacia el servidor de correo, ya que muchos proveedores tienen bloqueado el puerto 25 o el servicio SMTP, además debe estar puesto nombre de usuario y contraseña para el envío, en caso de usar el servidor SMTP.

4.5. Diseño del Plan de Implementación

Para el diseño de solución se configurará un dominio de prueba dentro del servidor DNS, y servidor Anti Spam para verificar el funcionamiento correcto y posteriormente se procederá a implementar con los dominios restantes dentro de la configuración de los servidores DNS y el firewall para correo no deseado.

Se revisará la forma de conexión de los equipos dentro del cuarto de servidores así como la restructuración del uso del protocolo SMTP para envío de correo desde la red del proveedor.

Se solucionará la configuración de la retransmisión abierta dentro del servidor de correo de la compañía, para cambiar configuración en los programas que utilizan los clientes para que de esta manera autentiquen con el usuario y contraseña el envío de correo.

Por otra parte existen usuarios que ocupan el SMTP para envío de correo y que no tienen cuentas de correo con el proveedor para que puedan enviar con el SMTP de su proveedor o en su defecto a través del proveedor del servicio de internet, en este caso Ecuaonline.

4.6. Implementación de Diseño

4.6.1. Diagrama de solución

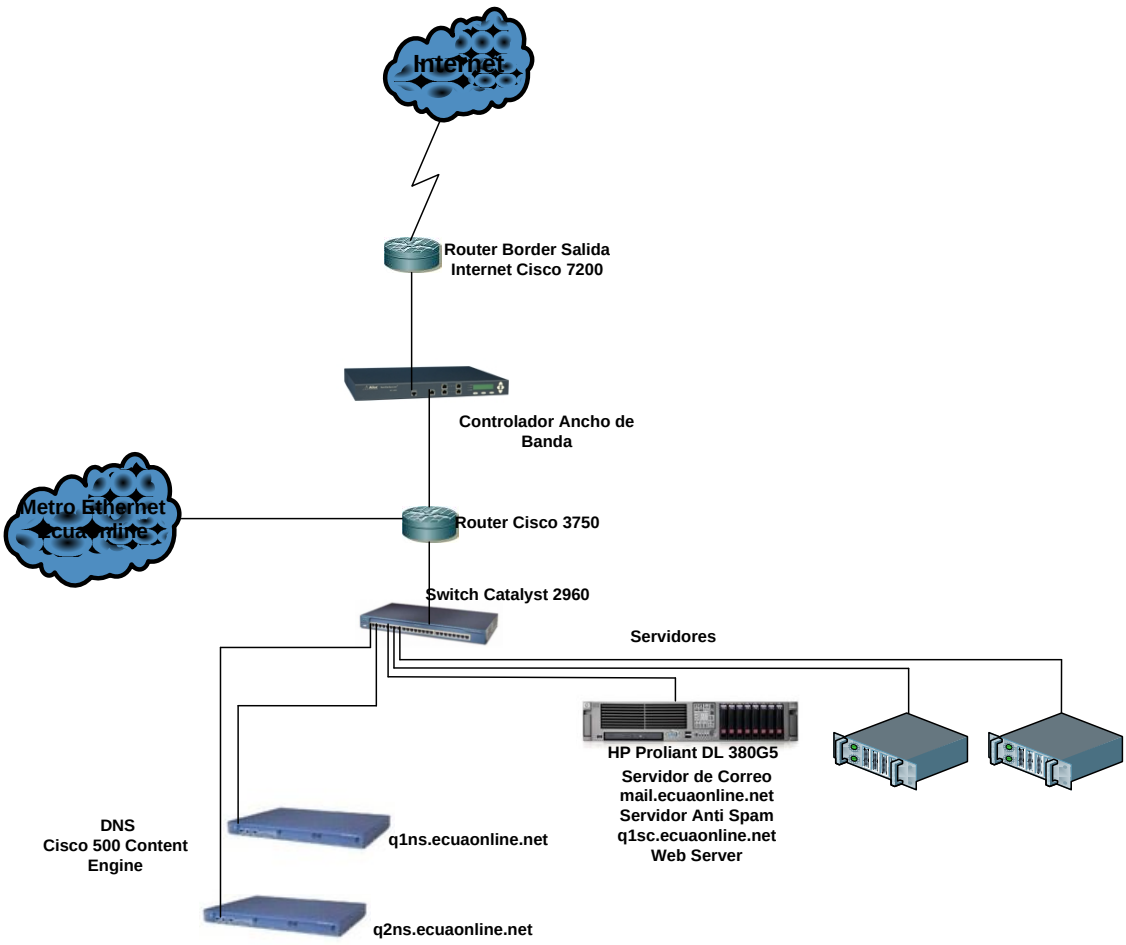


Figura 30: Diagrama conexión actual de servidores y equipos involucrados en envío y recepción de correo

4.6.2. Configuración de equipos

4.6.2.1. Servidores DNS

Se configuro dos servidores con GNU Linux distribución Ubuntu 8.04.1, dentro de dos equipos Cisco 500 Content Engine, uno de los equipos se encuentra configurado como servidor DNS primario q1ns.ecuaonline.net y el otro como servidor DNS secundario q2ns.ecuaonline.net, ya que antes solo se contaba con un servidor y al presentarse algún problema con el equipo los clientes perdían el servicio no solo

de correo sino de internet, por otra parte hay cambios en la configuración de las zonas mismos que se los detalla más adelante y tienen que ver con una reestructuración dentro de la configuración de los servidores DNS.

Los valores estándar para las zonas se encuentran configurados de la siguiente forma para el servidor primario, nombre del servidor DNS es q1ns.ecuaonline.net. El valor estándar de las zonas se mantiene por año, mes, día y ID de modificación yyyy/mm/dd/id.

```
//        Ecuaonline Name Server Configuration
//
// Master Name Server
//
// DNS Server Name:            q1ns.ecuaonline.net
// Hostname:                   ankaa.ecuaonline.net
// Assigned IP Address:        200.110.232.2
//
// Maintained By:
//      - Jorge Suarez
//      - David Moncayo
//      - Alejandro Ulloa
//
// Standard Zone Values
//     200xxxxx01   ; Serial yyyy/mm/dd/id
//          10800   ; Refresh (3 hours)
//           3600   ; Retry (1 hours)
//         604800   ; Expire (7 days)
//          43200 ) ; Negative Cache TTL (12 hours)
```

Se comenta también las fechas cuando se realizaron las modificaciones en lo que agregar y remover las zonas se refiere esto quiere decir se puede ver cuando se agrego o cuando se quito algún dominio dentro de los servidores DNS esta información debe ser modificada dentro de los dos servidores DNS, los dominios removidos se los deshabilita y no son eliminados del servidor DNS como política.

La zona base es la siguiente y esta configurada como primario dentro de este servidor y se crea una copia de dicha zona hacia el servidor secundario con IP pública 200.110.232.3 que es q2ns.ecuaonline.net y es el servidor configurado como esclavo es decir es el servidor secundario de la empresa.

```
zone "ecuaonline.net" IN {
        type master;
        file "zones/ecuaonline.net";
        allow-update { none; };
        allow-query { any; };
        allow-transfer { 200.110.232.3; };
};
```

Como se puede apreciar se hace una transferencia desde este servidor hacia 200.110.232.3 que es el servidor secundario.

En lo que a zonas delanteras de operaciones de búsqueda se mantiene de manera similar a la configuración que se menciono en el capítulo anterior respecto a zonas de operaciones de búsqueda, con la única diferencia que se hace una trasferencia de la misma al servidor 200.110.232.3.

```
zone "adrialpetro.com" IN {
        type master;
        file "zones/adrialpetro.com";
        allow-update { none; };
        allow-query { any; };
        allow-transfer { 200.110.232.3; };
};
```

Las zonas reversas de operaciones de búsqueda se mantienen con la configuración que se especifico en el capitulo anterior, y debe ser guardaba la configuración dentro del servidor primario de la empresa, y realizarse una transferencia de la configuración hacia el servidor secundario.

Al igual que la configuración de las zonas delanteras de operaciones de búsqueda solo se realiza los cambios de la información de los registros en el servidor primario, ya que automáticamente dicha información pasa hacia el servidor secundario, por lo que los archivos solo deben ser creados o modificados en el servidor primario.

```
zone "235.110.200.in-addr.arpa" IN {
        type master;
        file "zones/235.110.200.db";
        allow-update { none; };
        allow-query { any; };
        allow-transfer { 200.110.232.3; };
```

Por otra parte el archivo con información de la zona tiene la siguiente configuración.

```
$TTL    43200
@       IN      SOA     q1ns.ecuaonline.net. dominios.ecuaonline.net.  (
                                2008120802  ; Serial
                                10800       ; Refresh
                                3600        ; Retry
                                604800      ; Expire
                                43200 )     ; Minimum
; Name Servers Records.

        IN      NS      q1ns.ecuaonline.net.
        IN      NS      q2ns.ecuaonline.net.

; Mail exchange (MX records).

        MX      2       q1sc.ecuaonline.net.

; Address (A) records.
mail            IN      A       200.110.232.4
www             IN      A       190.95.133.226
```

Como se ve en la parte informativa del registro SOA un cambio importante es que se envié cualquier reporte hacia dominios@ecuaonline.net, ya que las personas pueden salir de la empresa y la cuenta de correo de dicho administrador sería eliminada, de esta manera información de problemas como lo que se presentan cuando alguna IP de la red de la empresa esta en lista negra llegan hacia la cuenta de correo dominios@ecuaonline.net.

Además quien realiza el intercambio de correo es q1sc.ecuaonline.net, que es el servidor anti – spam, y en la identificación de la máquina en el registro A esta

configurado para que se identifique al servidor de correo de la empresa que tiene la IP pública 200.110.232.4, esto se encuentra configurado de esta manera para que el servidor de filtrado de correo sea el anti- spam, luego se realice la retransmisión de correo hacia el servidor de correo del proveedor o en su defecto en el caso de los clientes que tienen su propio servidor de correo pero el filtro de correo lo realiza el proveedor se realiza la retransmisión del correo del servidor anti spam hacia los servidores de correo de dichos clientes.

A continuación se detalla la configuración para el caso en el que el proveedor realiza el filtrado de correo, para un cliente dentro de la red del proveedor que posee su propio servidor de correo.

```
$TTL    43200
@       IN      SOA     q1ns.ecuaonline.net. dominios.ecuaonline.net.  (
                                2008100904  ; Serial
                                10800       ; Refresh
                                3600        ; Retry
                                604800      ; Expire
                                43200 )     ; Minimum
; Name Servers Records.

        IN      NS      q1ns.ecuaonline.net.
        IN      NS      q2ns.ecuaonline.net.

; Mail exchange (MX records).
        MX      5       q1sc.ecuaonline.net.

; Address (A) records.
```

```
mail            IN      A       200.110.232.140
www             IN      A       200.110.232.140
```

Como se puede ver el cliente tiene su propio servidor de correo con una IP pública del proveedor, pero el control de SPAM lo realiza Ecuaonline, quien también se encarga del intercambio de correo para que llegue al servidor de correo del cliente, ya que el MX es q1sc.ecuaonline.net.

Paro los casos en los que no interfiere el servidor anti – spam la configuración de las zonas se mantiene, es decir no sufrió ningún cambio.

La configuración de las zonas dentro del servidor secundario tiene la siguiente estructura:

```
zone "adrialpetro.com" IN {
        type slave;
        file "zones/adrialpetro.com";
//        allow-update { none; };
        allow-query { any; };
        masters { 200.110.232.2; };
};
```

Se especifica el tipo de servidor como esclavo, las zonas son creadas dentro de los dos servidores se permite que se haga consultas hacia el servidor, además se especifica cuál es el servidor DNS primario y no se permite actualizaciones de los archivos de operaciones delanteras de búsqueda ni de zonas reversa de operaciones de búsqueda ya que ello solo se configura en el servidor primario.

Configuración de registro SPF, se define uno o más mecanismos para describir los hosts designados para realizar el envió de correo de un determinado dominio. Los mecanismos pueden tener las siguientes características.

“+” Pass “-” Fail “~” Softfail “?” Neutral

Pass, el registro SPF esta diseñado de manera que sea permitido para enviar (accept).

Fail, el registro SPF se encuentra diseñado de manera para que no sea permitido para el envió (reject).

SoftFail, esta diseñado para que sea permitido el envió, pero con una transición (accept but mark).

Neutral, se especifica que nada se puede decir acerca de la validación (accept).

None, que no se encuentra el registro SPF, o que este no produce ningún resultado (accept).

Ejemplos de algunos mecanismos utilizados para el registro SPF:

"v=spf1 mx -all"

Permite a los dominios de los registros MX para la retransmisión de correo, prohibiendo a todos los demás.

"v=spf1 -all"

El dominio no puede enviar correo de ninguna forma, si se especifica la siguiente configuración, a diferencia del anterior.

"v=spf1 +all"

Cuando se cree que no es necesario el uso del registro o no lo considera importante.

En la parte inferior se encuentra la configuración del dominio ecuaonline.net:

```
$TTL    43200
@       IN      SOA     q1ns.ecuaonline.net. dominos.ecuaonline.net.  (
                                2008100706  ; Serial
                                10800       ; Refresh
                                3600        ; Retry
                                604800      ; Expire
                                43200 )     ; Minimum
; Name Servers Records.

        IN      NS      q1ns.ecuaonline.net.
        IN      NS      q2ns.ecuaonline.net.

; Mail exchange (MX records).

                MX      10      q1sc.ecuaonline.net.
                MX      20      q1ms.ecuaonline.net.
                MX      30      q2ms.ecuaonline.net.
; Address (A) records.
; Mail Servers
mail            IN      A       200.110.232.4
```

```
cyb             IN      A       200.110.232.11
uio             IN      A       200.110.232.11
; NS Servers
q1ns            IN      A       200.110.232.2
q2ns            IN      A       200.110.232.3
; Network Devices
pop             IN      A       200.110.232.8
smtp            IN      A       200.110.232.4
; Servers And Services
www             IN      A       200.110.232.10
www2            IN      A       200.110.232.10
secure          IN      A       200.110.232.253
hot106          IN      A       200.110.232.6
stcs.3m         IN      A       200.110.232.5
speed           IN      A       200.110.232.7
; Server Hostnames
q1ms            IN      A       200.110.232.4
q2ms            IN      A       200.110.232.7
q1sc            IN      A       200.110.232.11
q1nms           IN      A       200.110.232.7
redes01         IN      A       200.110.232.250
ftp.ecuaonline.net. IN  CNAME   www.ecuaonline.net.
ecuaonline.net. IN TXT "v=spf1 mx ~all"
q1ms.ecuaonline.net. IN TXT "v=spf1 a -all"
q2ms.ecuaonline.net. IN TXT "v=spf1 a -all"
q1sc.ecuaonline.net. IN TXT "v=spf1 a -all"
```

Las consultas SPF que no coincidan con el mecanismo devolverán SoftFail, los mensajes que sean enviados desde cualquier servidor serán aceptados, pero serán sometidos a un escrutinio.

```
ecuaonline.net. IN TXT "v=spf1 mx ~all"
```

Se permite la retransmisión de correo electrónico desde los siguientes servidores q1ms.ecuaonline.net que es el servidor de correo de Ecuaonline, q2ms.ecuaonline.net que es la dirección del servidor de back up de correo de Ecuaonline y por último se encuentra el servidor anti– spam que dentro de los registros MX es el que tiene la prioridad para el envío de correo en primera instancia. Los servidores que están detrás de esos nombres se les permiten enviar mensajes de ecuaonline.net.

```
q1ms.ecuaonline.net. IN TXT "v=spf1 a -all"
q2ms.ecuaonline.net. IN TXT "v=spf1 a -all"
q1sc.ecuaonline.net. IN TXT "v=spf1 a -all"
```

Las revisiones de estos registros las realizan los software de los servidores de correo o de los firewall anti – spam de esta manera se tiene una puntuación por no hacer uso de dichos registros.

4.6.2.2. Servidor de Correo

Por decisión de la empresa se hizo una inversión para que los servidores ya no sean clones y además sean servidores que se los pongan dentro de un rack por lo que se configuro un nuevo servidor de correo, mismo que se lo subió dentro del

servidor que tiene instalado VM Ware Server (máquina virtual), y donde se encuentran además del servidor de correo a través de maquinas virtuales instalados el servidor WEB de la empresa, el servidor anti - spam y el servidor para monitoreo de la red y soporte al cliente. Se ocupo el mismo sistema operativo es decir Windows 2003 server pero de 64 bits con Service Pack 2.

Uno de los principales inconvenientes con respecto a la configuración del servidor de correo es que este permitía la retransmisión abierta desde cualquier punto, es decir funciona como Open Relay, por lo que la primera medida fue cambiar dicho parámetro dentro de la configuración del servidor.

Al elegir dicha opción los clientes deben tener autenticación dentro del servidor del servidor de correo saliente a través en el nombre de usuario y contraseña, que es como se utilizo en la configuración dentro del servidor; ya que también se puede elegir la selección de POP antes de SMTP con lo que también se verifique haya autenticación, a menos que sean de confianza el host o los hosts dentro del servidor como se muestra en la siguiente figura.

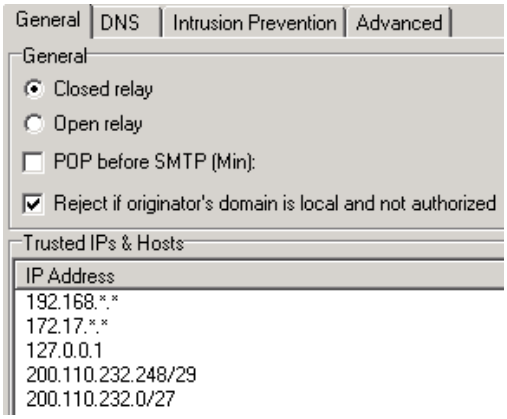


Figura 31: Configuración seguridad del servidor de correo (closed relay)

Todos estos rangos IP podrán enviar correo sin requerir autenticación, todas los demás tienen que usar autenticación.

Parte importante de la configuración es la retransmisión hacia el servidor anti–spam mismo que se encargará del envío y recepción del correo a través de la retransmisión que se hace hacia q1sc.ecuaonline.net que es el servidor anti- spam.

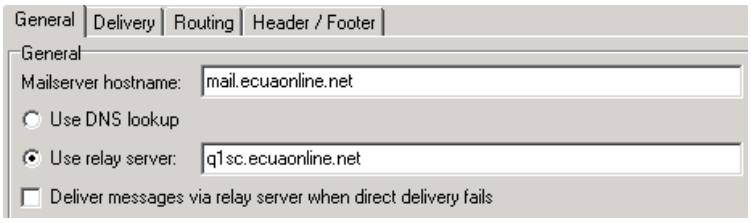


Figura 32: Configuración de retransmisión hacia servidor Anti Spam

Un parámetro importante es la configuración del puerto 465 como puerto SSL, protocolo de conexión de capa segura proporciona autenticación y privacidad de la

información en los extremos de internet mediante el uso de criptografía, evitando así la falsificación de identidad.

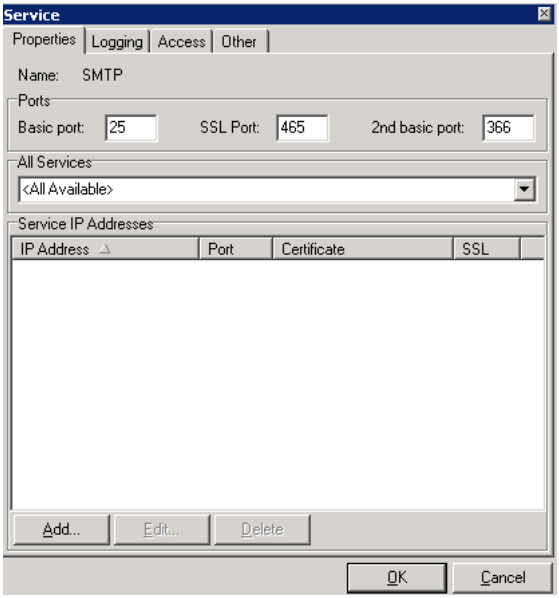


Figura 33: Configuración puertos SMTP

Se cambio también los parámetros en la configuración del anti – spam del servidor de correo se desactivo todo lo que es anti– spam en el servidor, ya que se usa ya los filtros del q1sc.ecuaonline.net.

Lo que se mantiene en la configuración es la prevención de intrusos, para que el número de conexiones desde una IP no sea mayor a 100 durante un minuto, que se verifique el tamaño de los correos y que no sobrepasen los 30 MB, no se bloquea por el score que posean en SPAM la configuración dentro del servidor es la siguiente.

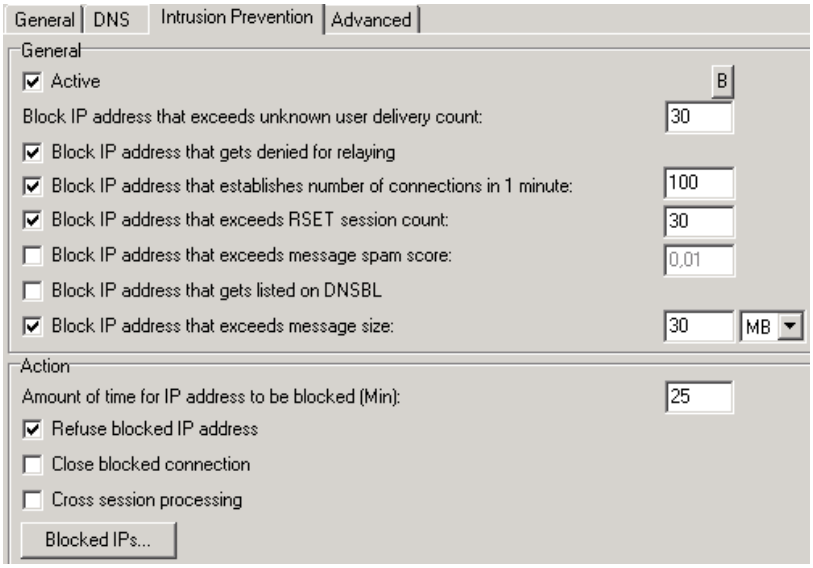


Figura 34: Configuración seguridad servidor de correo prevención de intrusos

Como se puede ver en la parte superior los clientes que caigan dentro de algunas restricciones serán bloqueados por el lapso de 25 minutos, durante este tiempo no le permitirá enviar correos a los usuarios que salgan a través de esa dirección pública.

4.6.2.3. Firewall Anti– Spam

Se instalo el software SPAM TITAN con el número de licencia STP-0750-669267con un número de usuarios de 750, perteneciente a la empresa Ecuaonline.

El acceso hacia el servidor selo hace via web a través de http://q1sc.ecuaonline.net conectándose como administrador.

El servidor anti- spam tiene el siguiente nombre q1sc.ecuaonline.net, con la redes de confianza 200.110.232.0/26 que corresponde a la subred en la que encuentran los servidores del proveedor.

Además se encuentran creados todos los dominios de los clientes que se encuentran dentro del servidor de correo de Ecuaonline, así como los clientes que tienen su propio servidor de correo pero desean que se realice el filtrado de SPAM por parte del proveedor y están dentro de la red de Ecuaonline. Esto se hace a través de lo que se conoce dentro del servidor como incoming mails donde se especifican los dominios y hacia que servidor se va a hacer la retransmisión de los mensajes de correo, se especifica el puerto de destino y el servidor de destino de correo que es mail.ecuaonline.net, con esto se garantiza que haya retransmisión hacia el servidor de correo del proveedor, para cada uno de los dominios. Por otra parte también existe algunos otros servidores de correo de clientes que se encuentran dentro de la red de la empresa y que el control de Spam lo realiza Ecuaonline, en este caso el servidor de destino es el servidor de correo del cliente al cual se va a realizar la retrasmisión.

Como se ve a continuación

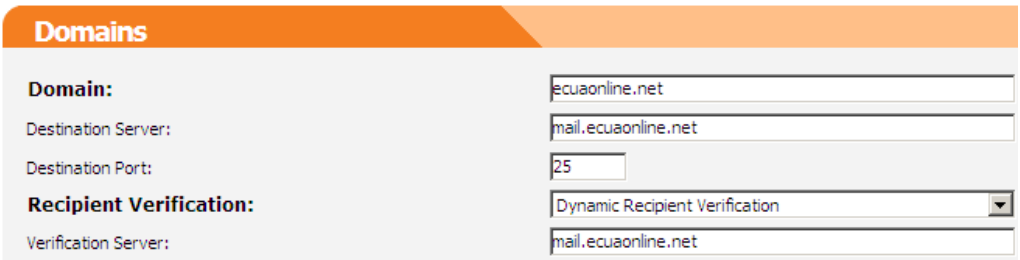


Figura 35: Configuración de retransmisión hacia servidor de correo

Existe dos tipos de configuración dentro del servidor anti – spam utilizadas cuando el servidor de correo lo manejan los clientes, pero el filtrado de correo lo realiza el proveedor y son los siguientes:

a) Cuando el servidor de correo lo administra el cliente y el proveedor se encarga solo del filtrado de correo, se debe en primera instancia cambiar los registros de la zona delantera de búsqueda para que el intercambio de correo lo realice el proveedor a través del servidor anti spam, y se realice la retransmisión hacia el servidor de correo del cliente.

```
$TTL    43200
@       IN      SOA     q1ns.ecuaonline.net. dominios.ecuaonline.net.  (
                        2008092603  ; Serial
                        10800       ; Refresh
                        3600        ; Retry
                        604800      ; Expire
                        43200 )     ; Minimum
; Name Servers Records.

        IN      NS      q1ns.ecuaonline.net.
        IN      NS      q2ns.ecuaonline.net.

; Mail exchange (MX records).

        MX      5       q1sc.ecuaonline.net.

; Address (A) records.

www     IN      A       200.110.232.10
ftp     IN      A       200.110.232.10
mail    IN      A       200.110.233.56
```

Dentro del servidor anti – spam cambia el servidor de destino, la configuración es la siguiente:

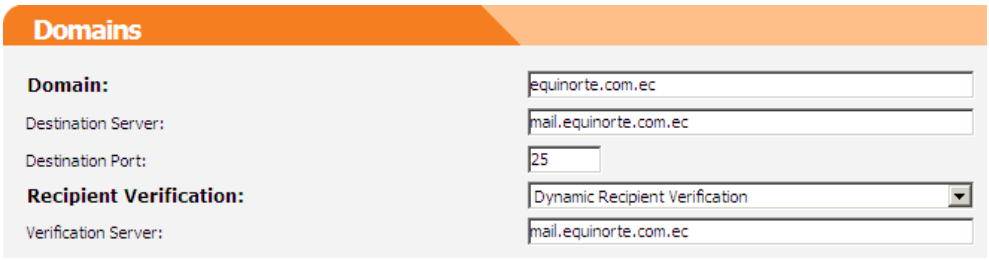


Figura 36: Configuración de retransmisión a servidor de correo del cliente

b) Existe un caso particular de un cliente en especifico en el que el correo llega hacia el servidor de correo de Ecuaonline, y de ahí es retransmitido hacia el servidor del cliente tanto en Quito como en Guayaquil.

Para ello se configuro dentro de la zona delantera de búsqueda de la siguiente manera los registros:

```
$TTL    43200
@       IN      SOA     q1ns.ecuaonline.net. dominios.ecuaonline.net.  (
                        2008102001  ; Serial
                        10800       ; Refresh
                        3600        ; Retry
                        604800      ; Expire
                        43200 )     ; Minimum
; Name Servers Records.

        IN      NS      q1ns.ecuaonline.net.
        IN      NS      q2ns.ecuaonline.net.

; Mail exchange (MX records).

        MX      10      q1sc.ecuaonline.net.

; Address (A) records.

uio     IN      A       200.110.233.57
gye     IN      A       200.110.237.35
```

Con lo que el intercambio de correo se realiza a través del servidor anti- spam del proveedor, luego se realiza una retransmisión hacia el servidor de correo y de ahí a través del manejo del mailbox en el servidor de correo del proveedor, los mensajes son enviados tanto al servidor de correo de Quito o Guayaquil del cliente.

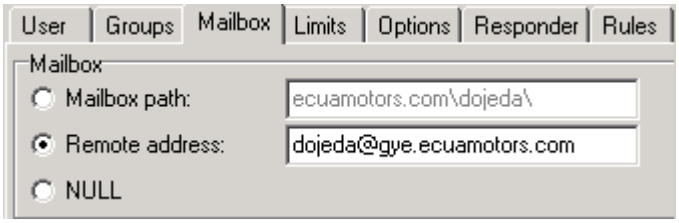


Figura 37: Configuración de buzón de correo para re envío de correo a servidor de correo de cliente

En el servidor anti– spam la configuración es la misma que para cualquier cliente que el proveedor administra el correo, dentro de dicho servidor. Por lo tanto las cuentas están creadas dentro de los dos servidores de correo tanto el del cliente así como el de la empresa.

De la siguiente forma:

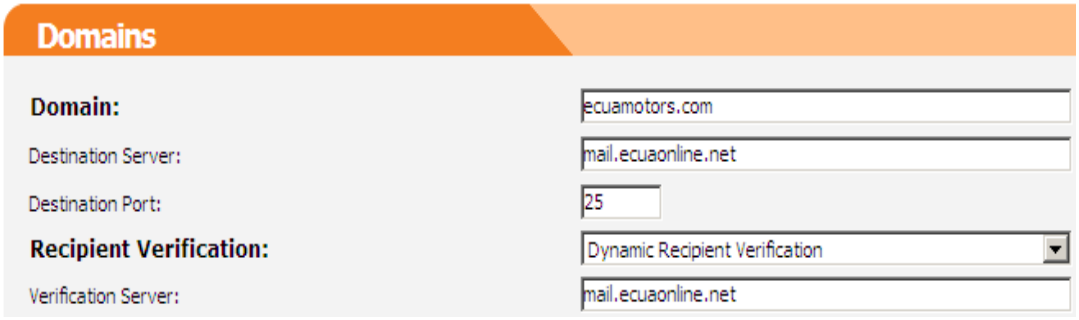


Figura 38: Configuración de retransmisión a servidor de correo del proveedor

Se configuro la opción verificación de cuentas que existen dentro de cada dominio garantizando que se haga una revisión para prevenir lo que se conoce como Dictionary Attack con lo que se bloquea toda dirección que no pertenezca a dicho dominio y dicho correo es eliminado o marcado como spam, la opción con la que está configurado es como Dynamic Recipient Verification, y es soportada por la mayoría de servidores de correo.

Para el filtrado se encuentra habilitado las opciones de filtrado por registro SPF y a través de la revisión de listas RBLs zen.spamhous.org. También cuando no existe un registro MX o registro A los correos son rechazados.

En lo que se refiere a anti virus se encuentra instalada la versión Kaspersky Anti-Virus server 5.5.10, misma que se actualiza automáticamente dentro del servidor. El reporte de virus llega a la dirección de correo electrónico ecuaonline-admin@ecuaonline.net.

Lo que tiene que ver con las opciones restantes, como son el filtrado de contenido esta habilitado lo que es filtrado de Spam añadiendo a las cabeceras del

mensaje el score que tiene el correo mientras se efectuó el análisis del mismo. Dentro del filtro de contenido se encuentra bloqueadas las siguientes extensiones de archivos

1	exe	Delete
2	vbs	Delete
3	pif	Delete
4	scr	Delete
5	bat	Delete
6	cmd	Delete
7	com	Delete
8	dll	Delete

Figura 39: Extensiones no permitidas para envío y recepción de correo dentro de servidor Anti- Spam

Pruebas de red, utiliza para la detección de SPAM y filtrado de las redes a través de Razor y Pyzor versión 2 mismos que utilizan procesos estadísticos. Razor sólo incluye mensajes calificados como spam, mientras que Pyzor incluyen todos los mensajes que han sido procesados como SPAM, llevando la cuenta de cuantas veces lo han sido para de esta manera determinar el tipo de correo electrónico.

- Razor: requiere acceso de salida al puerto TCP 2703 y el puerto TCP 7.
- Pyzor: requiere acceso de salida en los puertos TCP y UDP 24441.

Se encuentra activada la base de datos bayesiana que se basa en lo que se conoce como fichas; palabras o frases que se encuentran comúnmente en correos no permitidos. Por ejemplo, si la base de datos bayesiana se ha enterado de 100 mensajes con alguna frase en común considerada como correo no deseado, el

código bayesiano determina que es bastante seguro que el correo que contiene esta frase es Spam y, como tal, plantea la puntuación de Spam de ese mensaje.

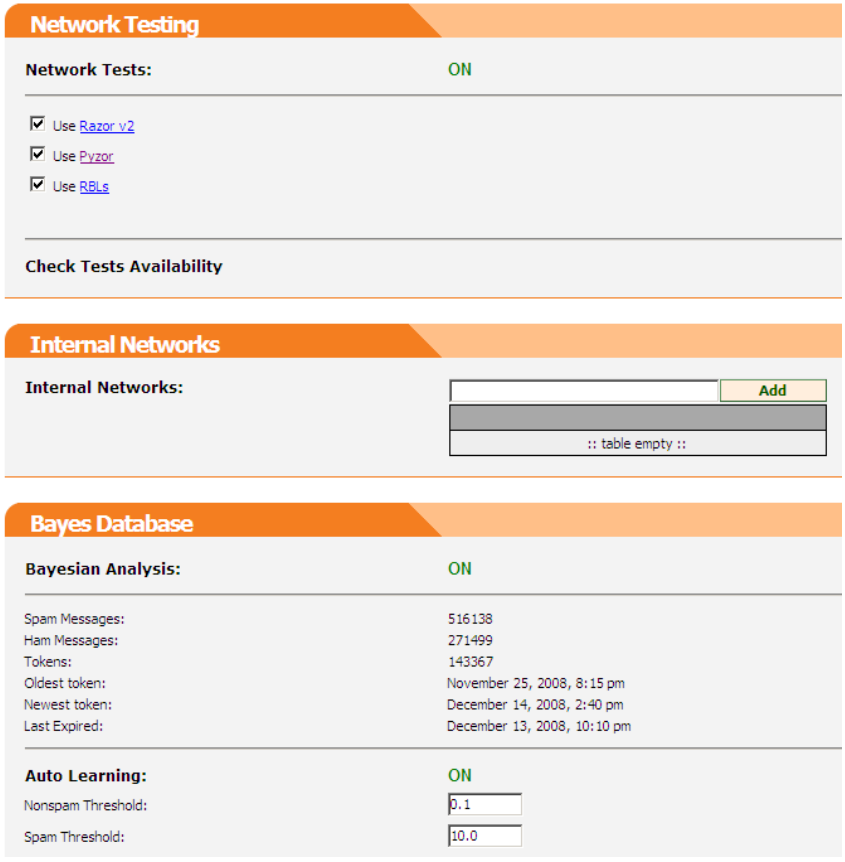


Figura 40: Pruebas de red, algoritmos bayesianos utilizados para detección de SPAM

En lo que se refiere a la base de datos bayesiana indica el número de mensajes de correo que se han aprendido como spam. En lo que se conoce como mensajes Ham indica el número de mensajes que se han aprendido como no spam. Fichas se indica el número total de fichas aprendido.

Si se encuentra habilitada la opción de auto aprendizaje quiere decir que esta habilitado Spamassassin, con lo que se recibe una puntuación para los correos electrónicos dentro del clasificador del filtro bayesiano.

SpamAssassin requiere por lo menos 3 puntos para la cabecera, y 3 puntos en el cuerpo del mensaje para auto-aprender y determinar a un correo como spam. Por lo tanto, el valor mínimo de trabajo para esta opción es de 6.

Esta activada la opción de reconocimiento óptico OCR, para poder escañera imágenes dentro del correo electrónico para de esta manera definir si la figura que está dentro del correo debe poseer una puntuación de spam.

Análisis de bootnet, revisa en primera instancia desde donde que máquina se están originando los correos y revisa si es que esta IP pública tiene un registro de zona reversa o algún registro para intercambio de correo MX.

Identificación de pasivos OS es un plugin que permite al anti- spam identificar el sistema operativo de la conexión SMTP cliente con una exactitud razonable. La mayoría de Spam se origina en los sistemas de escritorio de Windows.

Procesos SMTP, se trata de ver el número de procesos SMTP se están originado en un determinado momento en forma paralela y dentro del servidor se permite hasta 4 procesos.

Los mecanismos bayesianos son soportados en varios idiomas tal como se muestra en la figura.

Todas las opciones anteriormente mencionadas como se puede ver en la imagen que se encuentra a continuación están activadas dentro del servidor.

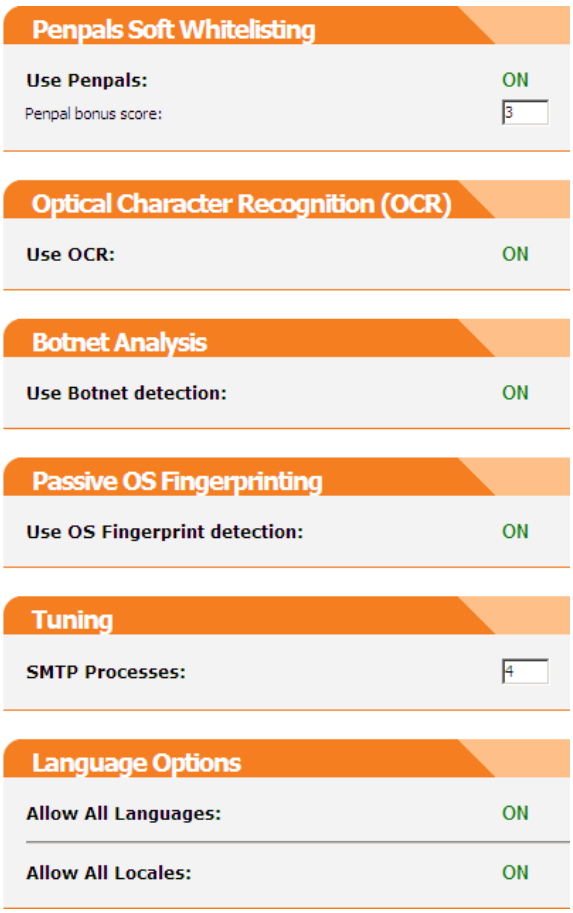


Figura 41: Filtros Anti Spam

Todo correo cuyo score después del test que se mencione sobrepase la calificación de 5 será considerado como Spam, así como los correos que contengan virus o un archivo adjunto con alguna extensión no permitida, serán enviados a cuarentena.

Los reportes de los correos que han sido considerados como Spam o que se encuentran dentro de cuarentena llegaran los días viernes, para ello se debe

configurar para que lleguen dichos reportes a cada uno de los dominios a los que se realiza la retransmisión de correo, con lo que la persona puede marcar como seguro o hacer que este se descargue a su bandeja de correo entrante correos que pudieran ser considerados como correo no deseado.

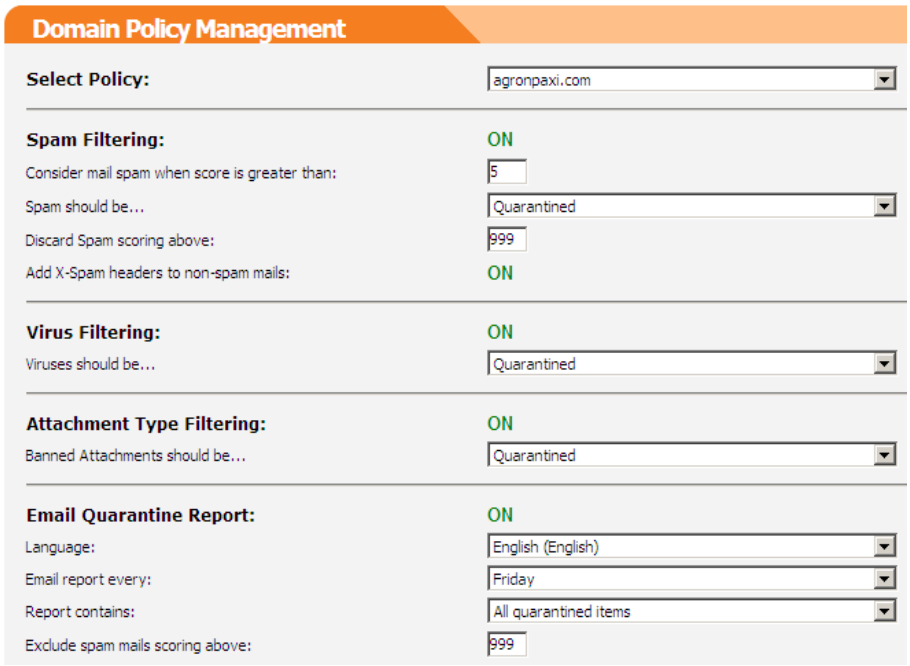


Figura 42: Manejo de reportes y filtros anti spam

El reporte que llega a cada usuario puede ser modificando para que le llegue en un lapso menor de tiempo, asi como puede marcar a ciertos remitentes como seguros. El usuario puede marcar la frecuencia con la que desea recibir el reporte, de manera diaria, semanal, mensual o si no desea recibir dicho reporte.

Dentro del reporte se puede ver en el caso de los mensajes en cuarentena el score por el cual fueron marcados como SPAM, asi como el asunto y las acciones que se pueden tomar con respecto a ese correo como es hacer que llegue a la bandeja de entrada, poner en lista blanca al remitente del correo o borrarlo, los

mensajes que quedan en cuarentena por un lapso mayor a 21 días son eliminados automáticamente del servidor.

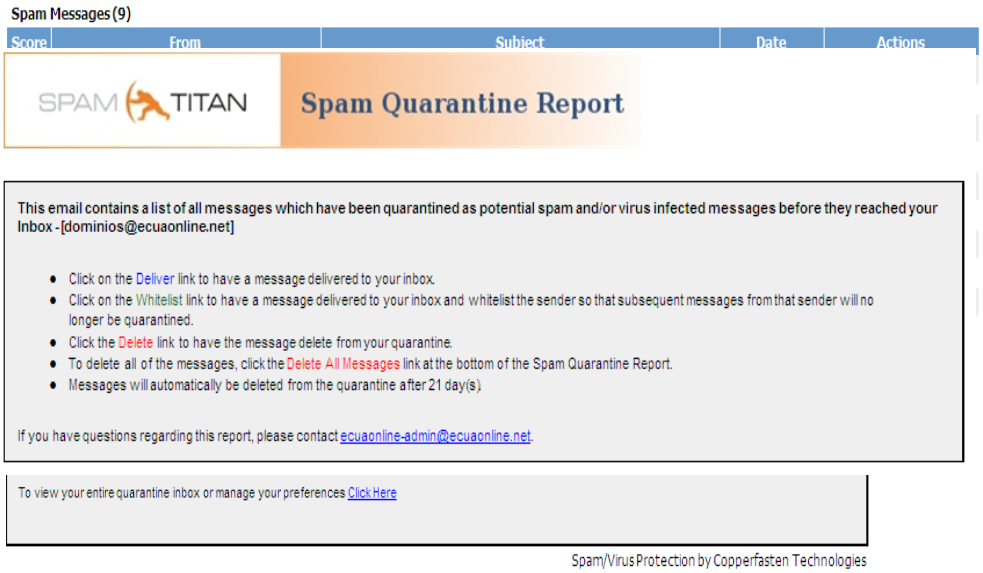
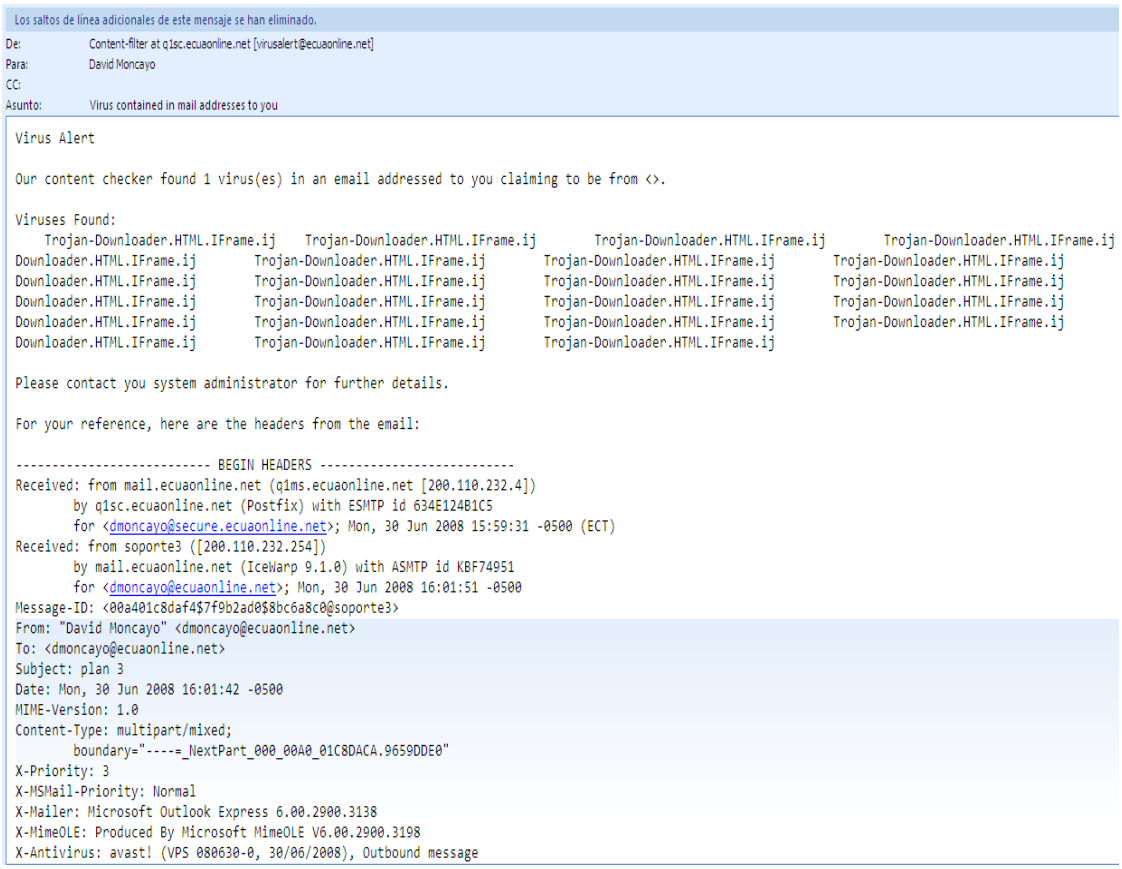


Figura 43: Reporte a Usuarios de cuarentena Anti- Spam

Por otra parte cuando se presenta un problema con algún correo enviado desde algún dominio que pasa por el filtro de contenidos llega un mensaje similar al buzón de correo de quien emitió el correo, especificando el archivo que contiene el virus, de manera similar se presenta un correo cuando se envía un correo con un archivo con una extensión no permitida o se esta generando correo spam desde alguna cuenta de correo en específico.



Los saltos de línea adicionales de este mensaje se han eliminado.

De: Content-filter at q1sc.ecuaonline.net [virusalert@ecuaonline.net]
Para: David Moncayo
CC:
Asunto: Virus contained in mail addresses to you

Virus Alert

Our content checker found 1 virus(es) in an email addressed to you claiming to be from <>.

Viruses Found:
Trojan-Downloader.HTML.IFrame.ij Trojan-Downloader.HTML.IFrame.ij Trojan-Downloader.HTML.IFrame.ij Trojan-Downloader.HTML.IFrame.ij
Downloader.HTML.IFrame.ij Trojan-Downloader.HTML.IFrame.ij Trojan-Downloader.HTML.IFrame.ij Trojan-Downloader.HTML.IFrame.ij
Downloader.HTML.IFrame.ij Trojan-Downloader.HTML.IFrame.ij Trojan-Downloader.HTML.IFrame.ij Trojan-Downloader.HTML.IFrame.ij
Downloader.HTML.IFrame.ij Trojan-Downloader.HTML.IFrame.ij Trojan-Downloader.HTML.IFrame.ij Trojan-Downloader.HTML.IFrame.ij
Downloader.HTML.IFrame.ij Trojan-Downloader.HTML.IFrame.ij Trojan-Downloader.HTML.IFrame.ij

Please contact you system administrator for further details.

For your reference, here are the headers from the email:

---------- BEGIN HEADERS ----------
Received: from mail.ecuaonline.net (q1ms.ecuaonline.net [200.110.232.4])
by q1sc.ecuaonline.net (Postfix) with ESMTP id 634E124B1C5
for <dmoncayo@secure.ecuaonline.net>; Mon, 30 Jun 2008 15:59:31 -0500 (ECT)
Received: from soporte3 ([200.110.232.254])
by mail.ecuaonline.net (IceWarp 9.1.0) with ASMTP id KBF74951
for <dmoncayo@ecuaonline.net>; Mon, 30 Jun 2008 16:01:51 -0500
Message-ID: <00a401c8daf4$7f9b2ad0$8bc6a8c0@soporte3>
From: "David Moncayo" <dmoncayo@ecuaonline.net>
To: <dmoncayo@ecuaonline.net>
Subject: plan 3
Date: Mon, 30 Jun 2008 16:01:42 -0500
MIME-Version: 1.0
Content-Type: multipart/mixed;
boundary="----=_NextPart_000_00A0_01C8DACA.9659DDE0"
X-Priority: 3
X-MSMail-Priority: Normal
X-Mailer: Microsoft Outlook Express 6.00.2900.3138
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.3198
X-Antivirus: avast! (VPS 080630-0, 30/06/2008), Outbound message

Figura 44: Correo de alerta por detección de Virus

El correo que se muestra en la parte superior, llego desde la dirección de correo virusalert@ecuaonline.net, como se muestra se puede apreciar dentro de las cabeceras la dirección de correo de origen asi como la dirección IP pública desde donde fue originado. De esta manera se puede solucionar el problema con un usuario en específico.

En el caso a anterior se trataba de un virus troyano, que se había enviado desde una cuenta de correo del dominio ecuaonline.net.

Se muestra la notificación cuando un correo ha sido tratado de enviar hacia una dirección de correo que se encuentra dentro del servidor, es decir que es de algún dominio del proveedor.

Virus Alert

Our content checker found %#V virus(es) in an email addressed to

you claiming to be from %s.

Viruses Found:

%V

Please contact you system administrator for further details.

For your reference, here are the headers from the email:

---------- BEGIN HEADERS ----------

[%H|\n]

---------- END HEADERS ----------

Dichas notificaciones de correo electrónico son enviadas en respuesta a virus, Spam, prohibición de un determinado archivo adjunto. Para lo cual se generan tres tipos de correo electrónico. En el **Anexo C** del presente documento se puede observar la estructura que tienen las notificaciones restantes.

Al administrador se le envía todas las notificaciones, al remitente a través de la no entrega del correo y enviándole un correo de notificación o por último a los destinatarios del correo por medio de advertencias acerca del correo que puede contener un virus o un archivo adjunto prohibido.

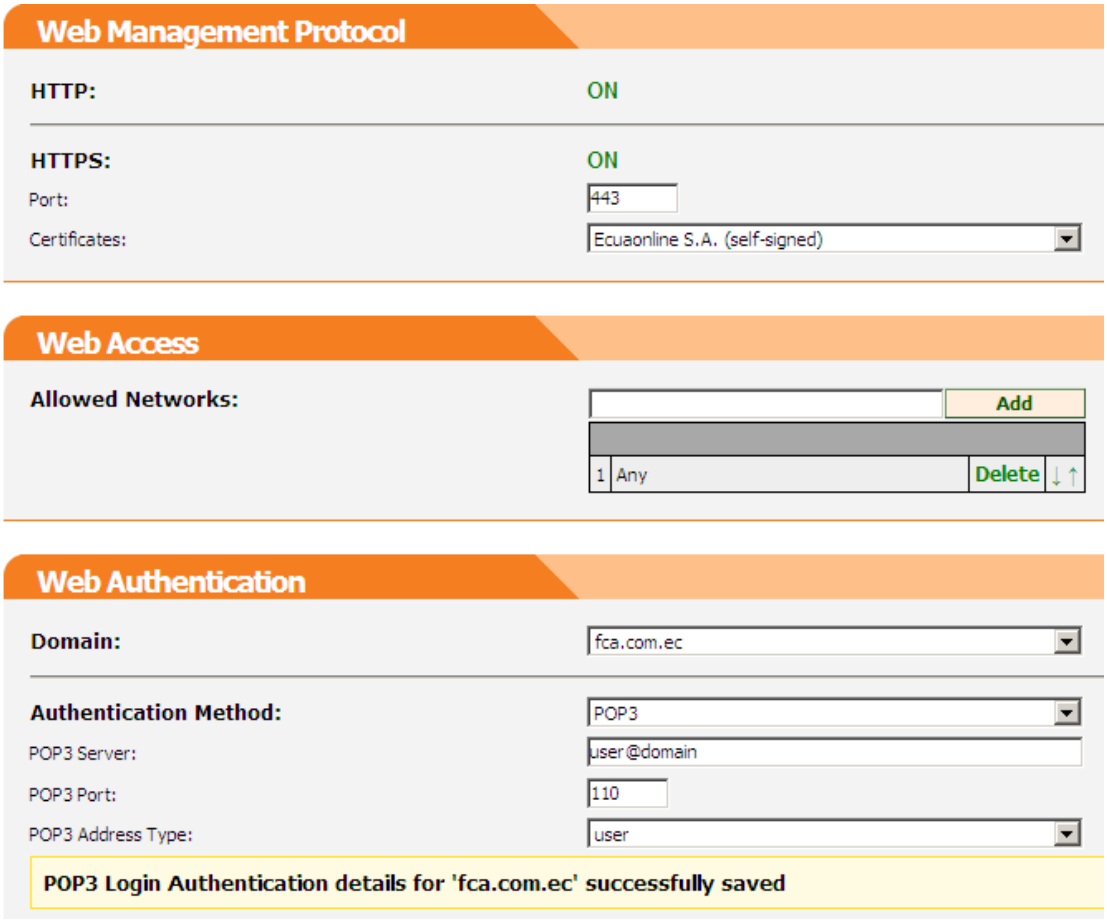


Figura 45: Modo de autenticación por protocolo POP y en base a usuarios

Para la conexión de los clientes hacia el servidor se realiza a través del nombre de usuario y contraseña, igual que la que se tiene para el POP3, en el caso de los clientes configurados dentro del servidor de correo de Ecuaonline por lo que cuando el cliente trate de conectarse en el usuario debe poner usuario@dominio y su contraseña correspondiente, allí se le desplegará por lapso de tiempo que elija los correos marcados como spam, virus, etc y se puede elegir para la búsqueda una dirección de correo en especifico. Además el administrador puede ver tantos los destinatarios de correo como los remitentes del correo.

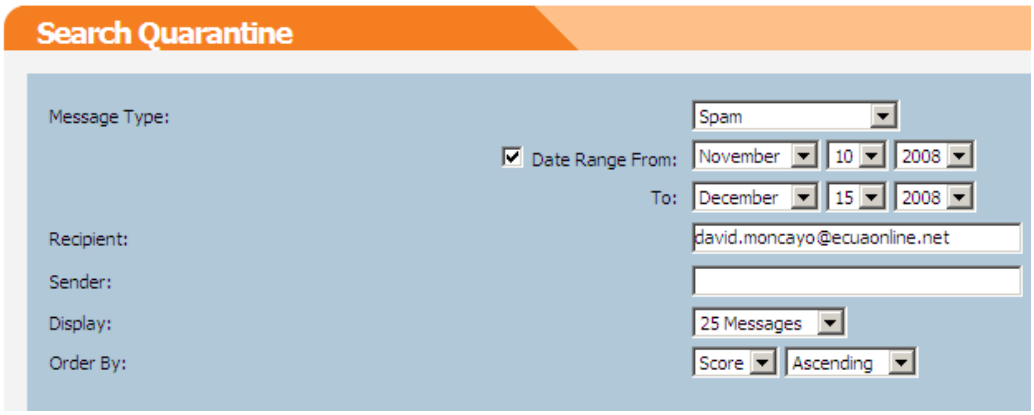


Figura 46: Reporte de correos que se encuentran en cuarentena por fecha

Existen otras opciones con reportes de correos que han sido filtrados por el servidor y los correos que no han llegado hacia distintas cuentas por algunas circunstancias.

4.6.2.4. Router Border Cisco 7200

Para solucionar el problema con el uso del puerto 25 a través del protocolo SMTP se permite el uso solo a determinadas IP públicas dentro de la red de Ecuaonline para que hagan uso de dicho puerto, así como para que se puedan enviar correo hacia determinados servidores de clientes, que se encuentran fuera de la red del proveedor, mediante el uso de ACL[21], misma configuración que se encuentra en la router que permite la salida hacia el internet de los clientes.

```
int f0/1
no ip access-group OUTPUT_FILTER in
no ip access-list extended OUTPUT_FILTER
ip access-list extended OUTPUT_FILTER

!internos
```

[21] ACL, Access Control List, tiene que ver con la seguridad informática y se refiere a una lista de reglas que detallan puertos de servicio o nombres de dominio que tienen permiso para usar un servicio.

permit tcp host 200.110.232.4 any eq smtp
permit tcp host 200.110.232.11 any eq smtp
permit tcp host 200.110.232.74 any eq smtp
permit tcp host 200.110.232.130 any eq smtp
permit tcp host 200.110.232.251 any eq smtp
permit tcp host 200.110.232.90 any eq smtp
permit tcp host 200.110.232.162 any eq smtp
permit tcp 200.110.232.168 0.0.0.7 any eq smtp
permit tcp host 200.110.232.194 any eq smtp
permit tcp host 200.110.233.3 any eq smtp
permit tcp host 200.110.233.5 any eq smtp
permit tcp host 200.110.237.35 any eq smtp
permit tcp host 200.110.233.51 any eq smtp
permit tcp host 200.110.233.56 any eq smtp
permit tcp host 200.110.233.57 any eq smtp
permit tcp host 200.110.233.76 any eq smtp
permit tcp host 200.110.233.84 any eq smtp
permit tcp host 200.110.233.136 any eq smtp
permit tcp host 200.110.233.228 any eq smtp
permit tcp host 200.110.233.229 any eq smtp
permit tcp host 200.110.233.230 any eq smtp
permit tcp host 200.110.233.231 any eq smtp
permit tcp host 200.110.233.232 any eq smtp
permit tcp host 200.110.233.233 any eq smtp
permit tcp host 200.110.233.234 any eq smtp
permit tcp host 200.110.233.235 any eq smtp
permit tcp host 200.110.233.236 any eq smtp
permit tcp host 200.110.233.237 any eq smtp
permit tcp host 200.110.233.238 any eq smtp
permit tcp host 200.110.233.242 any eq smtp
permit tcp host 200.110.233.243 any eq smtp
permit tcp host 200.110.233.246 any eq smtp
permit tcp host 200.110.234.80 any eq smtp
permit tcp host 200.110.237.6 any eq smtp
permit tcp host 200.110.237.133 any eq smtp
permit tcp host 200.110.237.220 any eq smtp
permit tcp host 200.110.239.94 any eq smtp
permit tcp host 200.110.239.98 any eq smtp

!externo

permit tcp any host 64.46.64.7 eq smtp
permit tcp any host 64.147.180.30 eq smtp
permit tcp any host 66.40.66.242 eq smtp
permit tcp any host 66.197.149.48 eq smtp
permit tcp any host 69.16.208.58 eq smtp
permit tcp any host 69.80.208.30 eq smtp
permit tcp any host 72.29.85.55 eq smtp
permit tcp any host 72.52.167.89 eq smtp
permit tcp any host 72.52.184.71 eq smtp
permit tcp any host 75.125.231.146 eq smtp
permit tcp any host 75.126.12.34 eq smtp
permit tcp any host 165.252.36.195 eq smtp
permit tcp any host 168.144.68.77 eq smtp
permit tcp any host 190.11.28.110 eq smtp
permit tcp any host 190.154.229.2 eq smtp
permit tcp any host 195.13.63.21 eq smtp
permit tcp any host 200.63.212.101 eq smtp
permit tcp any host 200.63.212.103 eq smtp
permit tcp any host 200.63.217.202 eq smtp
permit tcp any host 200.93.216.2 eq smtp
permit tcp any host 200.225.83.22 eq smtp
permit tcp any host 205.178.146.50 eq smtp
permit tcp any host 207.97.245.100 eq smtp
permit tcp any host 208.75.84.26 eq smtp
permit tcp any host 208.76.82.4 eq smtp
permit tcp any host 208.116.51.202 eq smtp
permit tcp any host 209.85.51.247 eq smtp
permit tcp any host 216.93.182.208 eq smtp
permit tcp any host 216.237.126.162 eq smtp
permit tcp any host 217.23.143.4 eq smtp

```
deny   tcp any any eq smtp
permit ip any any
exit
int f0/1
ip access-group OUTPUT_FILTER in
```

En el Access List se puede ver que existe una lista de direcciones IP pertenecientes a la compañía desde donde se puede enviar correo a través del puerto 25 sin ningún tipo de restricción permitiendo así el tráfico SMTP ya que varios de estas IP son pertenecientes a los servidores de correo de los clientes quienes manejan directamente la seguridad y control de Spam dentro de su red, y teniendo total y absoluta responsabilidad sobre la generación y recepción de correo SPAM, sin embargo siempre se verifica que ninguna de las direcciones anteriormente mencionadas se encuentren dentro de listas negras ya que cualquier correo se verifica dentro de dominios@ecuaonline.net, que es en donde se almacena la información acerca de la red de Ecuaonline tal como dominios que están por caducar, IP públicas marcadas dentro de listas negras, entre otras cosas.

En la parte inferior y después del campo que se encuentra comentado como externos, se encuentran los servidores SMTP de clientes que tienen sus correos afuera de la red de Ecuaonline, lo que quiere decir que se permite que haya tráfico SMTP que tenga como destino las IP mencionadas logrando que todo ese tráfico vaya hacia dichos servidores de correo, esta lista igual debe ser controlada ya que el permitir que demasiados clientes no tengan restricción en el tráfico SMTP hace que el control sea más complicado y haya más posibilidades de que se genere SPAM.

Para solucionar lo que tiene que ver con la llegada de correo SPAM hacia la red del proveedor, solo puede llegar tráfico SMTP a las siguientes direcciones, las

direcciones denegadas pertenecen a servidores de correo de clientes que el control del correo no deseado se realiza dentro del servidor anti- spam de la compañía y los servidores restantes de clientes que están dentro de la red del proveedor no se realiza ningún tipo de control.

```
ip access-list extended INPUT_FILTER
    deny   tcp any host 200.110.232.4 eq smtp log
    deny   tcp any host 200.110.233.56 eq smtp
    deny   tcp any host 200.110.233.140 eq smtp
    deny   tcp any host 200.110.232.242 eq smtp
```

4.7. Configuración de cuentas de correo en programas clientes de correo

Existe tres casos en lo que a configuración de las cuentas de correo se refiere, el primer caso es que el cliente tenga el servicio de internet con Ecuaonline y el servicio de correo también con el mismo proveedor en este caso lo que se debe hacer es configurar como servidor de correo entrante mail.ecuaonline.net y servidor de correo saliente mail.ecuaonline.net, como el servidor de correo saliente requiere autenticación se debe marcar la opción de mi servidor requiere autenticación o ocupar la misma configuración de nombre de usuario y contraseña que se tiene para el correo entrante como se muestra a continuación:

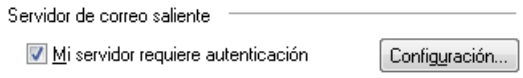


Figura 47: Autenticación de servidor de correo saliente

En el caso de Outlook Express en servidores de correo se debe ver que se encuentre habilitada la opción para que el servidor de correo electrónico saliente requiera autenticación y que se utilice la misma configuración en lo que se refiere a nombre de usuario y contraseña que la del correo entrante tal como se muestra en la figura siguiente:

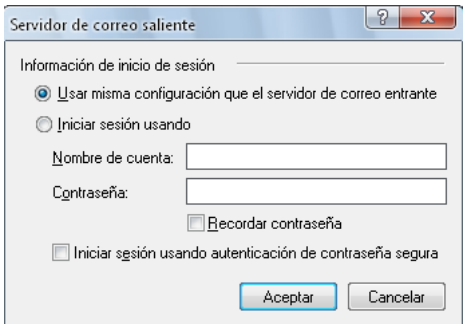


Figura 48: Autenticación de servidor correo saliente usando misma configuración de servidor de correo entrante

El segundo caso es cuando el cliente tiene el servicio de correo electrónico con Ecuaonline, pero el servicio de internet lo tiene con otro proveedor por lo que en la mayoría de casos otros proveedores tiene cerrado el puerto 25 para el tráfico SMTP, por lo que se usa el puerto 465 por medio de una conexión segura SSL para que de esta manera se pueda enviar correo desde cualquier lugar con cualquier otro proveedor, igualmente se debe configurar la autenticación para el correo saliente, esto debe ser configurado en opciones avanzadas del programa cliente de correo del usuario, de la manera siguiente:

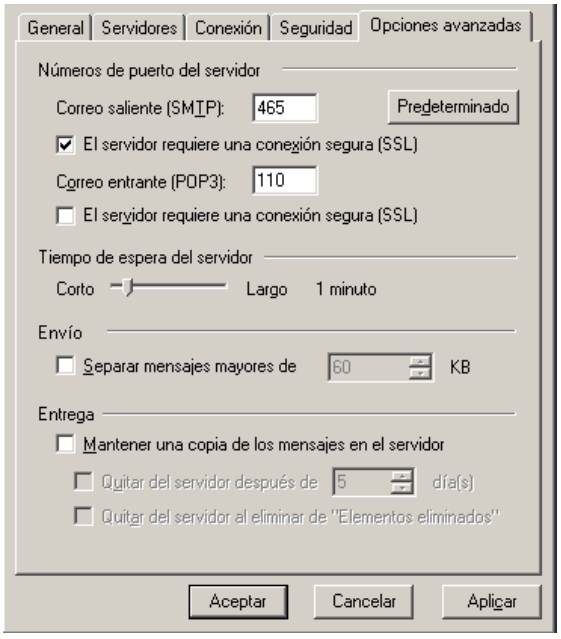


Figura 49: Opciones avanzadas configuración de puertos para servidor de correo entrante y saliente

Como se puede ver en la imagen anterior se habilita la opción para que el servidor requiera una conexión segura SSL y posteriormente se cambia el puerto al 465, posterior a esto cuando se proceda a enviar y recibir correo se debe aceptar el certificado del servidor de correo.

Por último existe la posibilidad de que el cliente no tenga el servicio de correo con el proveedor y desee salir por el servidor SMTP de Ecuaonline, es decir que no esté dentro del access list que se encuentra en el router de la salida a internet de la compañía. Para ello se realizo la siguiente configuración:

Se debe configurar en el servidor de correo entrante ya sea POP3 o IMAP con la información proporcionada por el proveedor de correo así como su nombre de usuario y contraseña, en tanto que para el correo saliente se debe configurar para

que se envié el correo a través del servidor de correo de Ecuaonline, es decir con el SMTP mail.ecuaonline.net

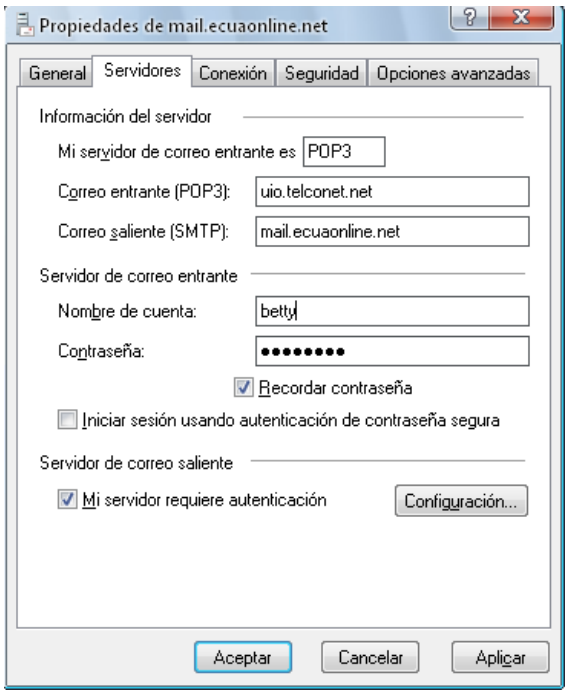


Figura 46: Configuración cuenta de correo cuando el cliente tiene solo servicio de internet con el proveedor

Al igual que en los casos anteriores se requiere autenticación para el correo saliente, pero con la diferencia en que la configuración debe estar marcada para que se inicie sesión usando una configuración de cuenta distinta a la que se tiene para el correo entrante.

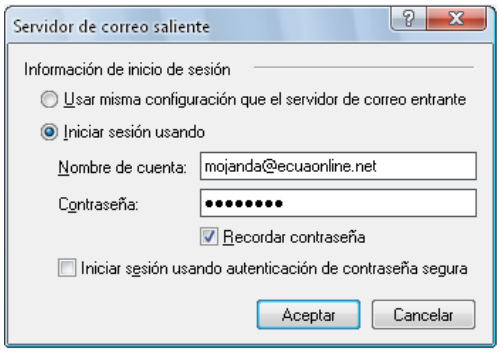


Figura 50: Configuración usuario y contraseña para

Esto se puede ocupar para todas las cuentas de correo que se tenga en donde el cliente es decir para que se envíe el correo por nuestro servidor utilizando una sola cuenta pero tomando en cuenta que en la pestaña de la información general tal como se muestra en la imagen a continuación debe estar marcada la opción de dirección de respuesta o correo electrónico de respuesta para que de esta manera las personas que reciben correo de estos usuarios respondan a las direcciones de correo original, que son las correspondientes a la de los proveedores externos a Ecuaonline.

Esto se debe a que todas las cuentas para usar el servidor SMTP, deben ser autenticadas, en el caso de usar el SMTP de la empresa

Como se muestra en la parte inferior:

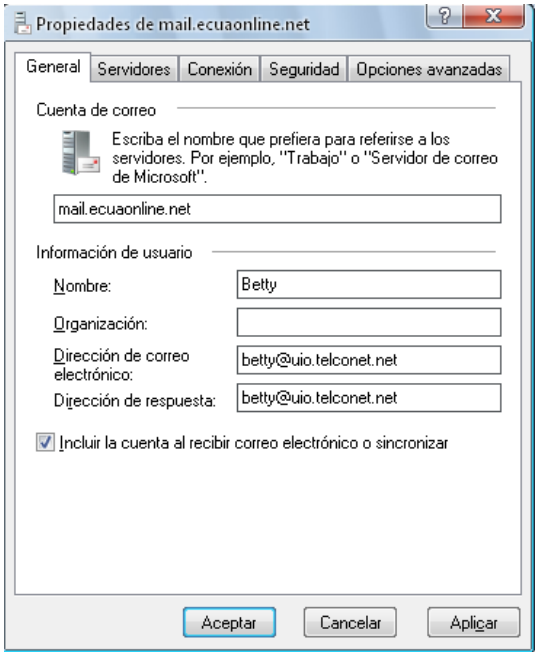


Figura51: Configuración dirección correo de respuesta

4.8. Verificación de configuraciones y correcciones

Es importante revisar que cuando se incluye un nuevo dominio dentro del servidor anti- spam se pueda sincronizar para que este encuentre todas las cuentas existentes del servidor de correo ya sea del proveedor o del cliente en específico si esto no ocurre se debe a problemas con la configuración del servidor de correo por lo que en algunos casos en especial, cuando se trata de servidores que son administrados por el cliente se debe incluir las cuentas manualmente.

Esto se debe a problemas de configuración en el servidor del cliente, por otra parte se debe verificar la existencia de las cuentas. Y que se estén generando reportes para todos los dominios una vez que estos hayan sido creados dentro del servidor anti spam.

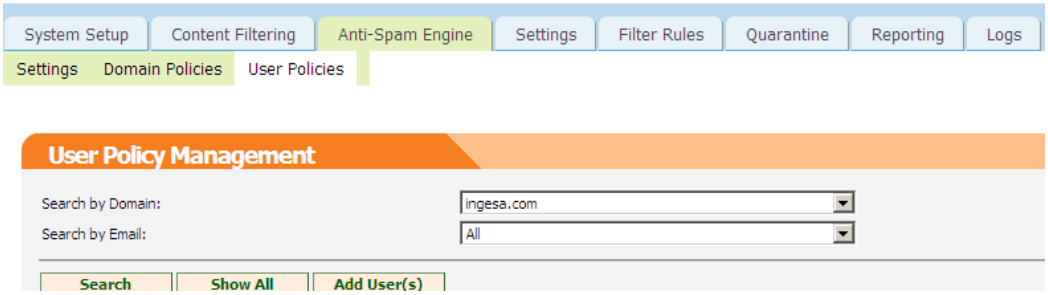


Figura 52: Configuración para un nuevo usuario dentro de un dominio existe para control y reportes anti spam

Como se puede ver uno puede ingresar las cuentas a las que se enviará el reporte, además se puede remover cuentas que no existan, corriendo un wizard para eliminar dichas cuentas de correo.

4.9. Análisis de Resultados

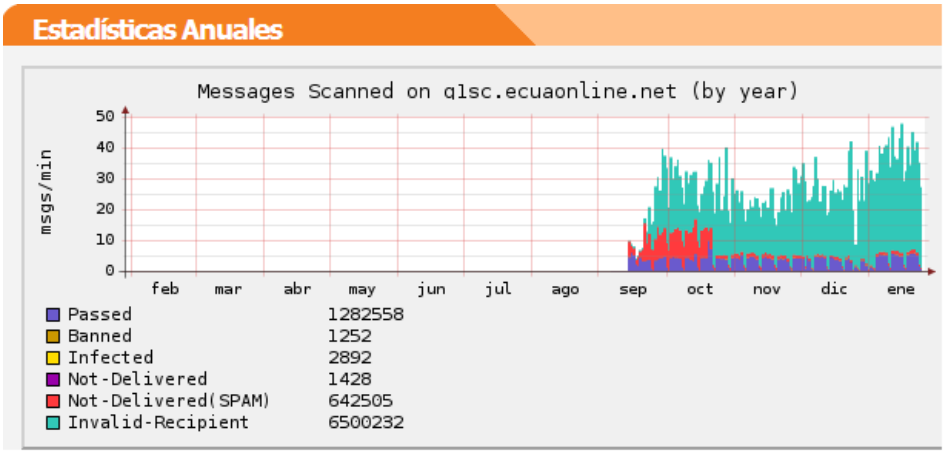
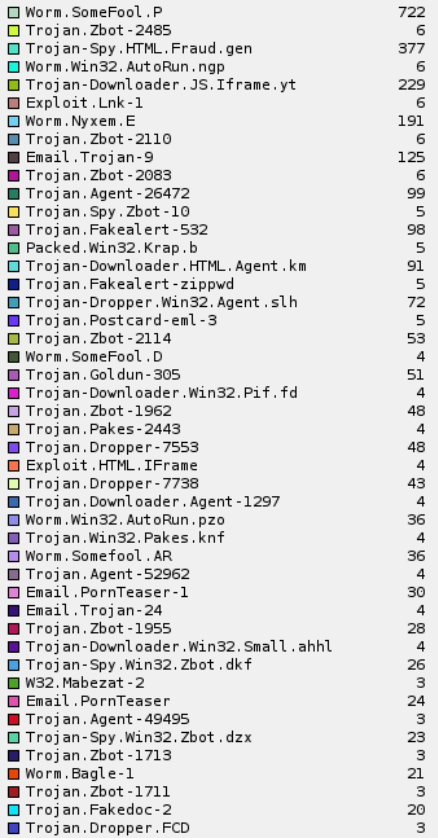


Figura 53: Estadística Anual funcionamiento Anti Spam

Como se puede ver en los datos estadísticos que se muestran en la parte superior desde que se instalo el software ANTI SPAM varios correos fueron bloqueados alrededor de 15 correos por minuto, y se puede ver que este tipo de

correo hacia los dominios que se encuentran configurados dentro del servidor ha disminuido, estos datos estadísticos muestran el número de correos electrónicos procesados, marcados por su contenido como Spam o por su contenido de virus, así como los correos que no presentaron ningún tipo de problema.

Por otra parte a continuación se muestra los principales tipo de virus encontrados en los mensajes de correo durante dicho periodo.



Worm.SomeFool.P	722
Trojan.Zbot-2485	6
Trojan-Spy.HTML.Fraud.gen	377
Worm.Win32.AutoRun.ngp	6
Trojan-Downloader.JS.Iframe.yt	229
Exploit.Lnk-1	6
Worm.Nyxem.E	191
Trojan.Zbot-2110	6
Email.Trojan-9	125
Trojan.Zbot-2083	6
Trojan.Agent-26472	99
Trojan.Spy.Zbot-10	5
Trojan.Fakealert-532	98
Packed.Win32.Krap.b	5
Trojan-Downloader.HTML.Agent.km	91
Trojan.Fakealert-zippwd	5
Trojan-Dropper.Win32.Agent.slh	72
Trojan.Postcard-eml-3	5
Trojan.Zbot-2114	53
Worm.SomeFool.D	4
Trojan.Goldun-305	51
Trojan-Downloader.Win32.Pif.fd	4
Trojan.Zbot-1962	48
Trojan.Pakes-2443	4
Trojan.Dropper-7553	48
Exploit.HTML.IFrame	4
Trojan.Dropper-7738	43
Trojan.Downloader.Agent-1297	4
Worm.Win32.AutoRun.pzo	36
Trojan.Win32.Pakes.knf	4
Worm.Somefool.AR	36
Trojan.Agent-52962	4
Email.PornTeaser-1	30
Email.Trojan-24	4
Trojan.Zbot-1955	28
Trojan-Downloader.Win32.Small.ahhl	4
Trojan-Spy.Win32.Zbot.dkf	26
W32.Mabezat-2	3
Email.PornTeaser	24
Trojan.Agent-49495	3
Trojan-Spy.Win32.Zbot.dzx	23
Trojan.Zbot-1713	3
Worm.Bagle-1	21
Trojan.Zbot-1711	3
Trojan.Fakedoc-2	20
Trojan.Dropper.FCD	3

Figura 54: Detección de virus dentro del Firewall Anti Spam

A continuación se presenta una muestra del tráfico de correo en la semana del 20 de Enero de 2009 hasta el día 26 de Enero de 2009, en donde se puede apreciar que el mayor tipo de correos bloqueados es el que se produce desde destinatarios inválidos lo que se conoce como envío de correo no deseado de

diccionario como se puede ver esta es la mayor causa de correo no deseado en la muestra que se tomo como mínimo en el día 26 de Enero de 2009 existen veinte y tres mil quinientos cuarenta y uno correos con destinatarios inválidos.

Tabla 9: Muestra de tráfico de correo Firewall Anti Spam

Semana del 20 de Enero a 26 de Enero de 2009								
Fecha	Total	Spam	Limpios	Destinatarios inválidos	Virus	Envíos Denegados	Corresponden a RBL	Rechazados por HELO
2009-01-26	38628	568	4828	23541	22	84	9259	0
2009-01-25	48115	611	876	38336	0	89	7891	0
2009-01-24	60343	735	1764	44703	0	241	12034	0
2009-01-23	76043	1276	7256	48552	2	309	17892	0
2009-01-22	67677	1535	8076	42713	33	197	14475	0
2009-01-21	70599	1774	8110	43626	3	233	16292	0
2009-01-20	74847	1652	7915	45038	33	183	19587	0

De la información de la tabla anterior se obtiene la siguiente figura.

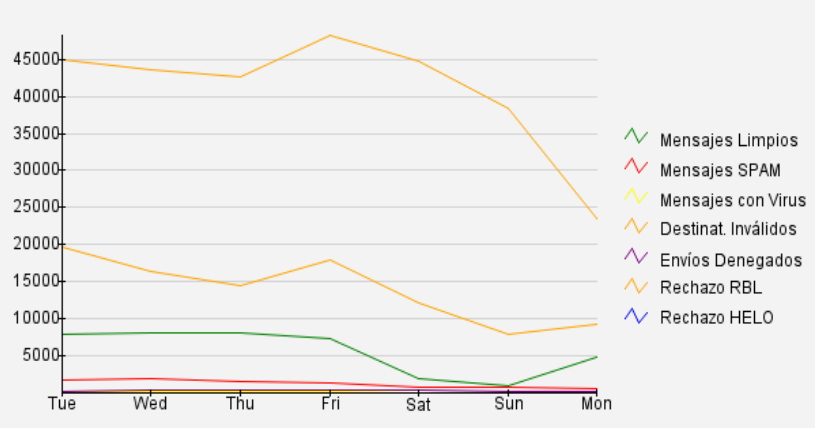


Figura 55: Muestra de tráfico de correo Firewall Anti Spam

Otra información importante que se puede obtener es la que presenta las transacciones que se están realizando al momento, dependiendo la transacción y usuario que escojamos.

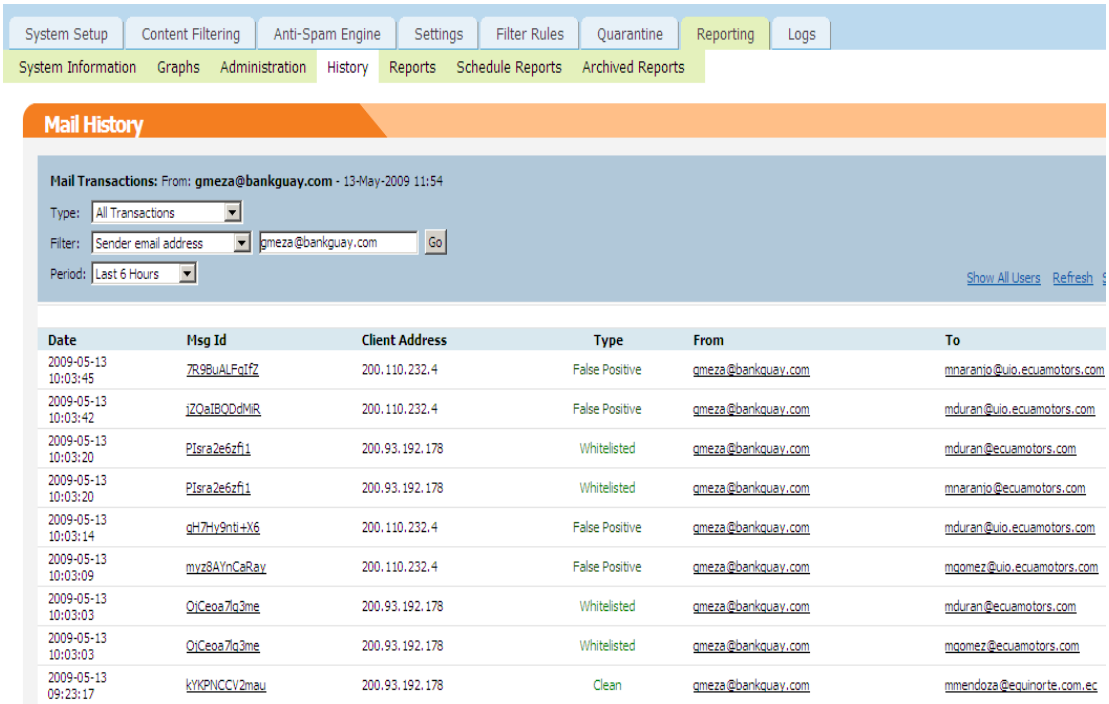


Figura 56: Historial de transacción de correo

A continuación se detalla el tráfico de correo que ha pasado por el servidor:

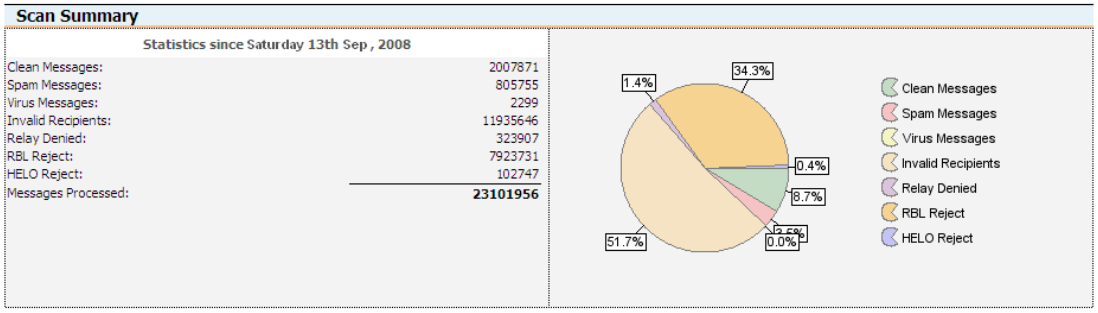


Figura 57: Estadística de correo procesado por el servidor

También se pudo observar en una muestra tomada el día 19 de Mayo de 2009, las direcciones IP públicas desde donde se generaba mayor cantidad de SPAM, así como el tipo de virus que mayormente se ha transmitido por este medio y desde que dirección se retransmitió.

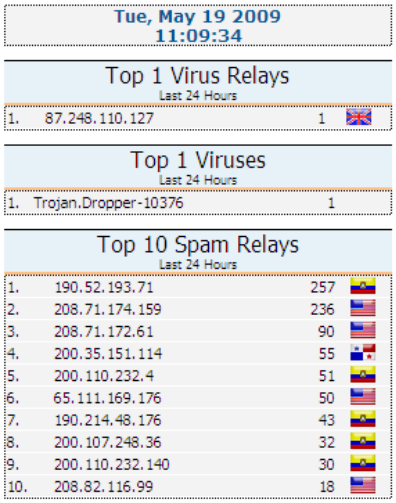


Figura 58: Sitios desde donde se ha retransmitido correo SPAM, correo con Virus

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- La implementación de una solución ANTI SPAM, permite a los proveedores de servicio de internet y correo optimizar recursos ya que el correo electrónico no deseado consume gran ancho de banda, además de ocasionar pérdida de tiempo al cliente ya que recibe correos que no le son de utilidad.
- El uso de controles para el tráfico y uso de SMTP dentro de la red del proveedor ayuda a que el correo solo pueda ser enviado desde equipos que estén autorizados a hacerlo evitando así problemas de enlistamiento de las IP públicas que el proveedor brinda a los clientes.
- Mayor control sobre el tráfico SMTP, debido a que se utilizan mecanismos a través del firewall ANTI SPAM para el filtrado correo no deseado y virus que van por este medio.
- Mejor rendimiento del servidor de correo ya que el filtrado del correo se lo realiza por medio del servidor ANTI SPAM y luego se realiza la retransmisión hacia el servidor de correo de la empresa.
- Se han bloqueado mas de seis millones de correos electrónicos que tienen destinatarios no válidos que generan tráfico hacia el servidor de correo de la empresa con lo que este tiene mejor rendimiento.

- Al no permitir retransmisión abierta (open relay) desde el servidor de correo, se garantiza que se autentiquen las cuentas para el envió de correo reduciendo en gran cantidad el correo no deseado que se genera desde la red del proveedor

5.2. Recomendaciones

- Buscar soluciones Anti Spam para las empresas que se ajuste a las necesidades de las mismas, que cumpla con los requerimientos y los precios no sean altos.
- Fomentar el uso de firewall anti spam, control de uso de servicio SMTP para envío de correo y el filtrado de tráfico.
- Configurar los servidores de correo para que no permita retransmisión abierta, y determinar hacia que servidores o que equipos de ser necesario dentro de la red debe ser permitida la retransmisión.
- Innovar varias alternativas que se podrán vender como un servicio agregado de la empresa a clientes, para administrar de esta forma sus dominios y cuentas de correo de los mismos.
- Verificar de manera continua dentro de sitios como www.dnsstuff.com que las IP públicas no estén siendo marcadas en lista negra para prevenir futuros inconvenientes y dar solución oportuna a los problemas de envío de correo electrónico

LISTADO DE REFERENCIAS BIBLIOGRÁFICAS

- Cricket Liu & Paul Albitz , DNS and Bind, quinta edición , O'Reilly , 2006
- Matthias Kalle Dalheimer & Matt Welsh , Running Linux , quinta edición , O'Reilly ,2005
- Philip Hazel , The exim SMTP Mail Server , cuarta edición , UIT Cambridge, 2003
- Ramadas Shanmugam, R. Padmini, & S. Nivedita , Special edition using TCP/IP , segunda edición , 2002.

LINKCOGRAFÍA

- DNS
  http://www.programacionweb.net/articulos/articulo/?num=415
- RFC 1034
  http://www.rfc-es.org/rfc/rfc1034-es.txt
- DIG
  http://www.ignside.net/man/redes/dig.php
- FQDN
  http://es.wikipedia.org/wiki/FQDN
- Archivos de zonas (DNS)
  http://hp.fciencias.unam.mx/~amem/dns/dns-3.html
- Merak (Servidor de correo)

http://www.icewarp.com

- Anti Spam (Spam Titan for VM Ware)

  http://www.spamtitan.com/anti-spam/vmware/technical-specifications

  http://download.spamtitan.com/manuals/spamtitan_admin.pdf

- SMTP

  http://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

  http://tools.ietf.org/html/rfc821

  http://www.eventhelix.com/RealtimeMantra/Networking/SMTP_Sequence_Diagram.pdf

- SMTP- AUTH

  http://tools.ietf.org/html/rfc4954

- SPF

  http://en.wikipedia.org/wiki/Sender_Policy_Framework

  http://www.openspf.org/

  http://www.openspf.org/blobs/sender-authentication-whitepaper.pdf

- SPAM

  http://es.wikipedia.org/wiki/Correo_no_deseado

- Autenticación correo electrónico

  http://209.85.171.104/translate_c?hl=es&sl=en&tl=es&u=http://ece.arizona.edu/~edatools/home/email/Email_Authentication.htm&usg=ALkJrhjX2Y5uTZiR_nATLlyPEn9nsHLSjQ

- Técnicas ANTI SPAM

http://209.85.171.104/translate_c?hl=es&sl=en&tl=es&u=http://en.wikipedia.org/wiki/Anti-spam_techniques_(e-mail)&usg=ALkJrhi1Y6mda0v0XIVcn84DuN1yh8Fmow

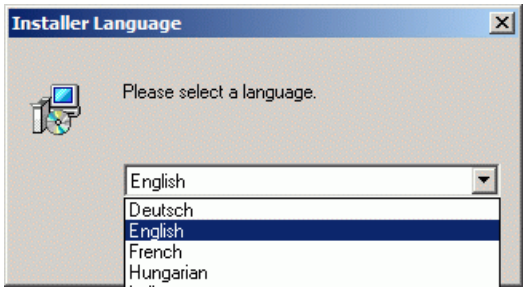
- MTA

  http://en.wikipedia.org/wiki/Mail_transfer_agent

ANEXO A

Instalación de servidor de correo mediante la herramienta Icewarp Merak Mail Server

A continuación se muestra la forma en la que se instala el software de la aplicación Icewarp Merak Mail Server, se debe seleccionar el idioma en el que se va a instalar la aplicación.



Selección de Idioma

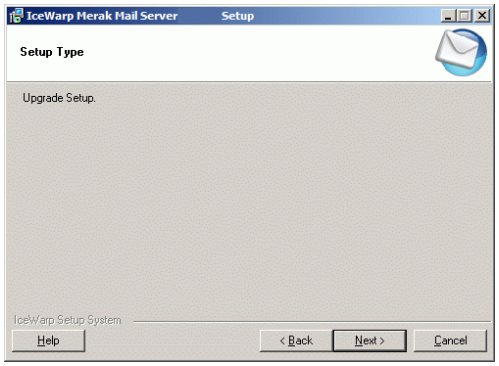
Después de escoger el idioma se consulta si se desea proceder con la instalación, donde se confirma si se desea proceder o no con la instalación.

Luego de aceptar en si se desea o no continuar con la instalación después de seleccionar el idioma, se procede a través de un wizard a instalar el programa que en primera instancia muestra el acuerdo para el uso de la licencia del progama y se acepta el acuerdo de licencia de uso del programa.

Como se muestra a continuación:

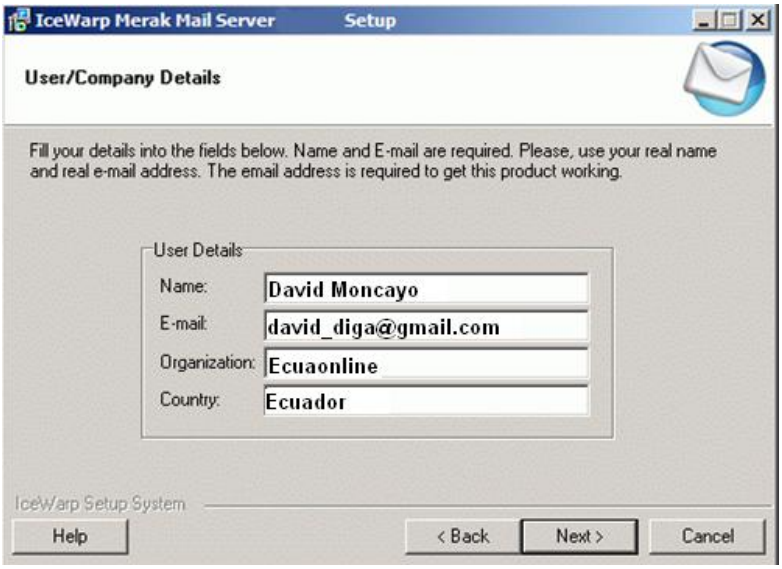
Acuerdo de licencia de software

Luego se selecciona el tipo de instalación que se va a realizar, en este caso se selecciono la de actualización, de no ser este el caso se selecciona una nueva instalación



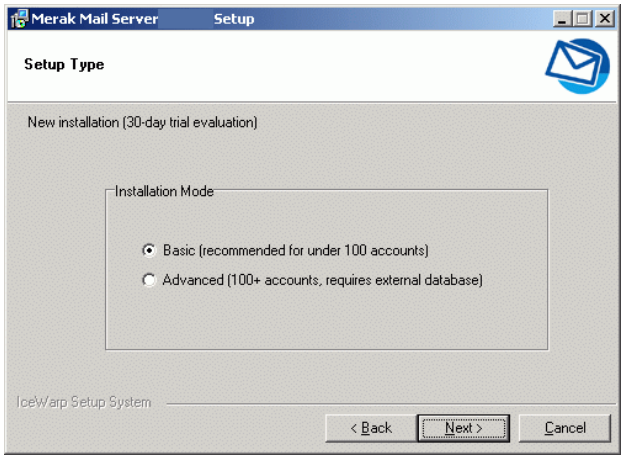
Pantalla Upgrade Setup

Se procede con los datos personales con una cuenta de correo existente para proceder a realizar la instalación del software.



Pantalla Datos informativos empresa/ usuario

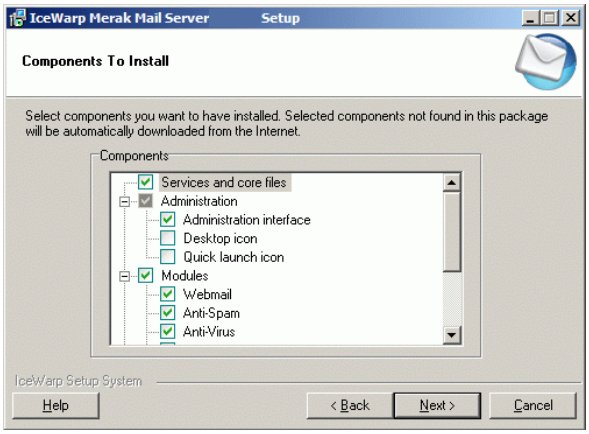
En la siguiente pantalla se selecciona el tipo de servidor de base de datos IceWarp uso.



Selección tipo de servidor de base de datos

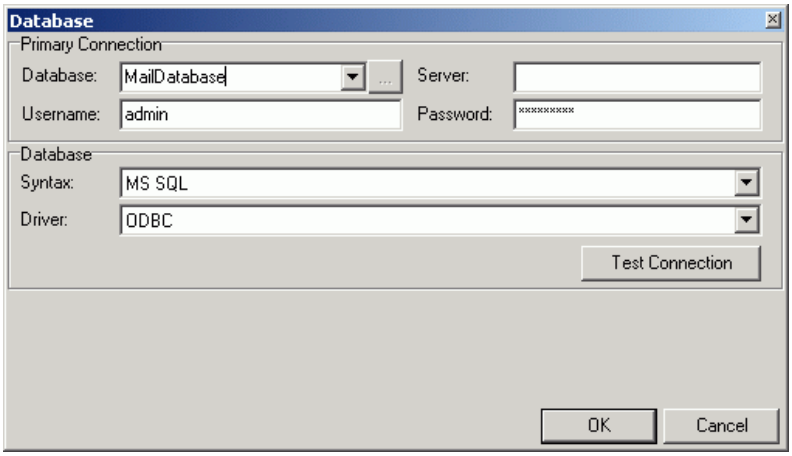
Instalación básica crear y utilizar una base de datos de MS Access, sin más información de usted mismo.

Si no necesita una base de datos externa, simplemente se selecciona la opción básica y haga clic en Siguiente y continúe con la Selección de componentes.



Pantalla de componentes instalados

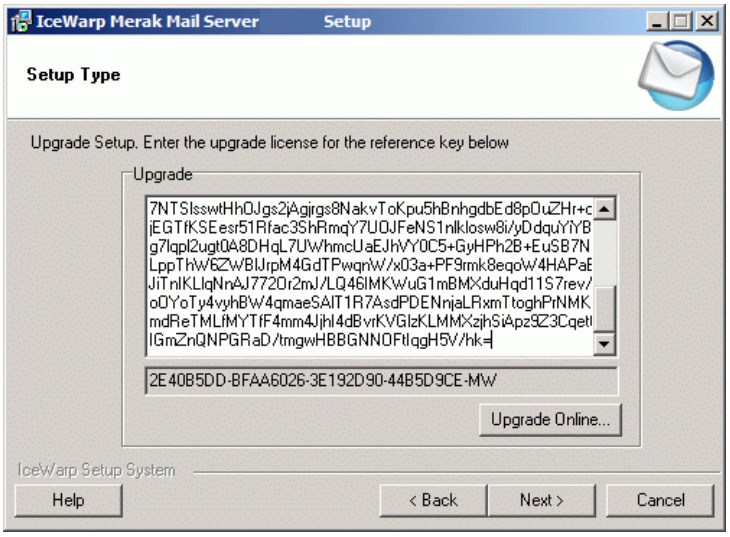
Si se escogiera la opción de instalación avanzada pedirá la información necesaria para acceder al sistema de base de datos externa.



Pantalla de selección de base de datos

Seleccione la opción avanzada y haga clic en Siguiente.

El cuadro de diálogo pedirá abrir la base de datos donde se ingresa las credenciales para acceder a la base de datos.



Pantalla de credenciales de base de datos

ANEXO B

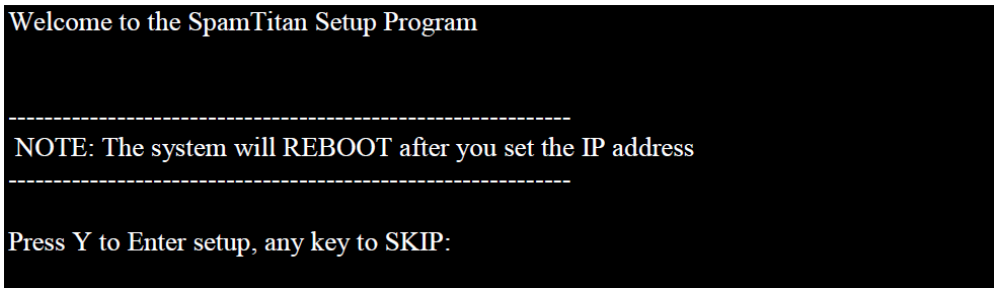
Instalación de servidor anti- spam mediante el uso de la herramienta SPAM Titan

Instalación de la aplicación dentro de VMware Server

Se necesita en primera instancia 512 MB en RAM y 40 GB de espacio en disco

Luego se debe descargar la aplicación desde http://www.spamtitan.com para VMwareServer

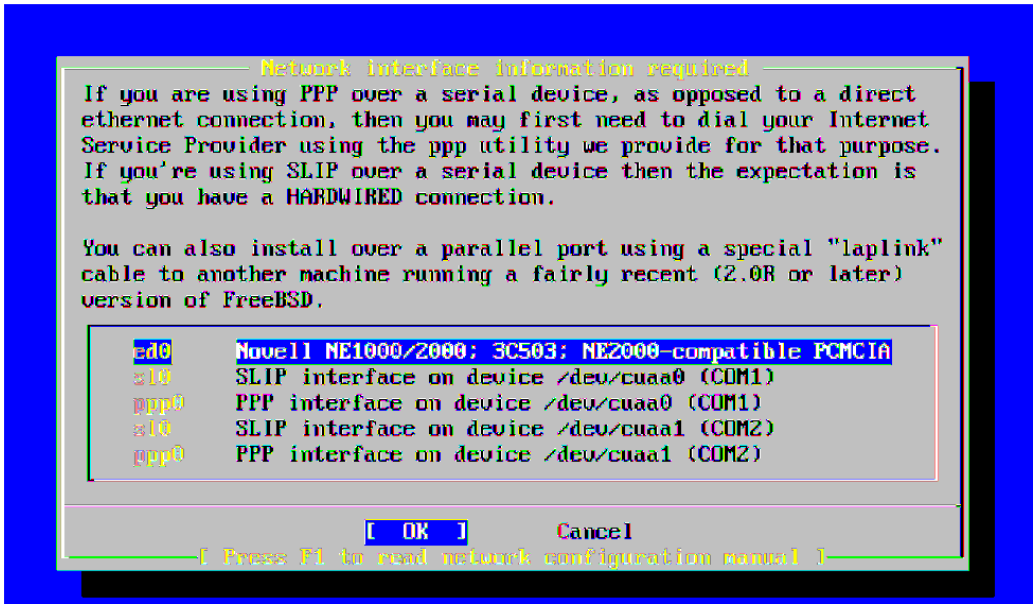
Asegurarse de que el BIOS del servidor está configurado para arrancar desde el CD-ROM seguida de la unidad de disco duro principal.



Pantalla de inicio de instalación

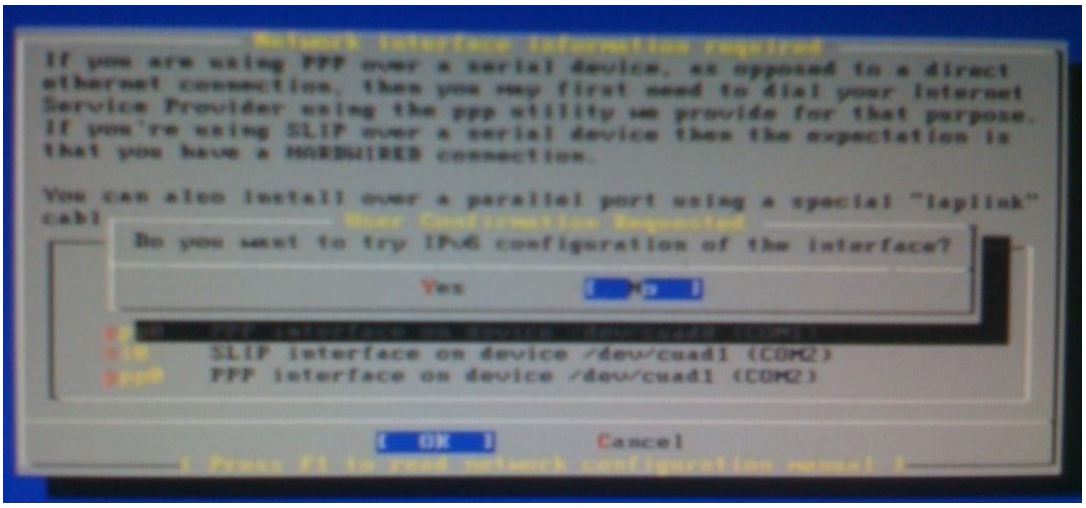
Luego aparecerá una pantalla donde se selecciona el dispositivo de Ethernet del servidor, por lo general se selecciona la primera opción que se muestra a menos que existan múltiples dispositivos de Ethernet, de ser asi se debe seleccionar de la lista el adecuado.

Como se ve en la siguiente figura:



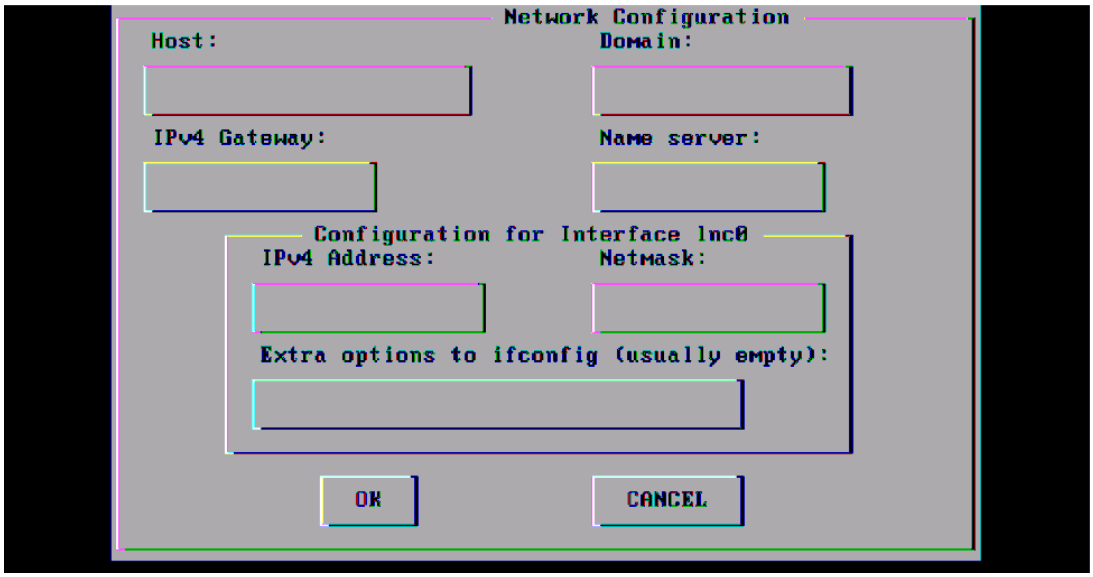
Pantalla para elección de dispositivo de Ethernet

Después de ello se habilita o no IPv6



Pantalla para habilitar IPv6 o IPv4

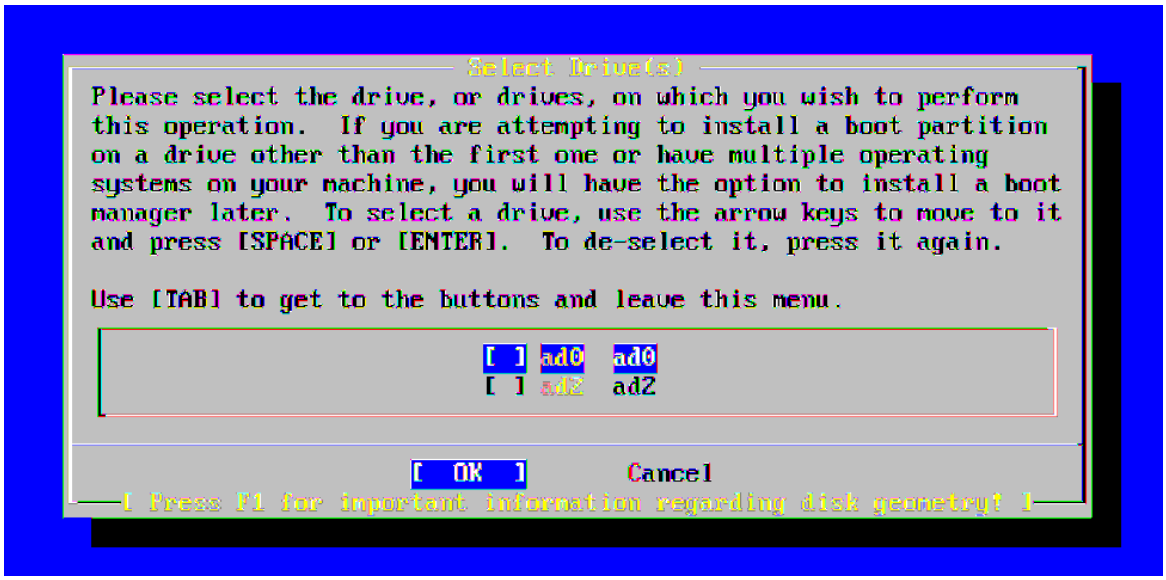
A continuación se debe detallar la configuración de la interfaz, se debe introducir los datos tal como se muestra en la figura siguiente, con el nombre de la máquina FQDN que en este caso q1sc.ecuaonline.net, y después de ello se debe configurar los campos IP con su respectiva mascara



Pantalla configuración IP, nombre host y dominio

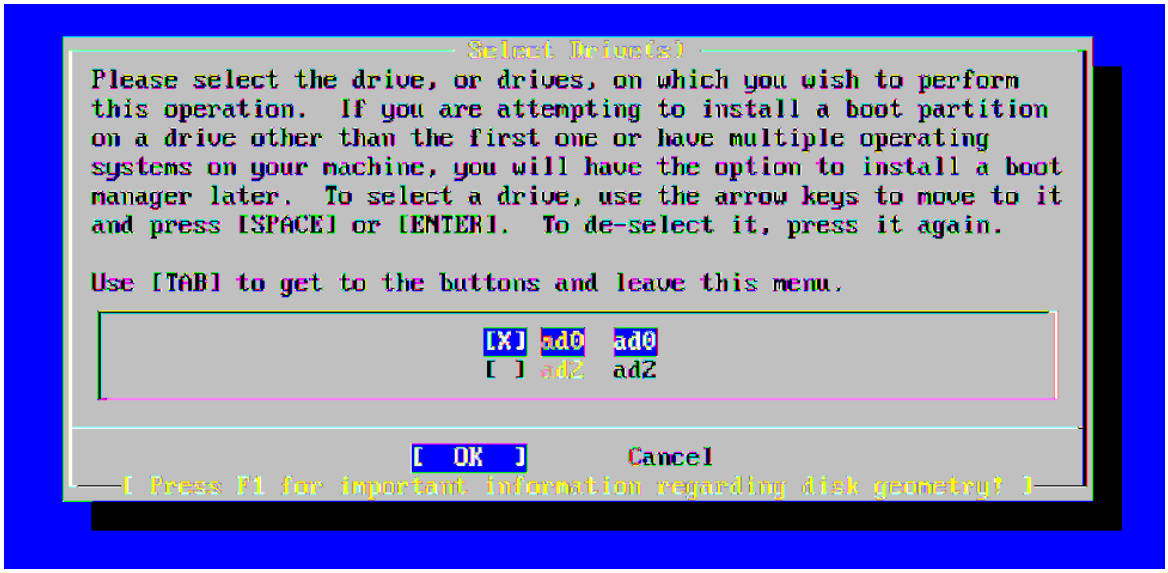
A continuación se pide que se seleccione el disco en el que se desea instalar SpamTitan, si el servidor utiliza una unidad IDE a continuación, los discos se llamarán ad0 para el disco 1 AD1 para el disco 2 etc, en tanto que si se tratá de sistemas SCSI se denominan da0 etc, normalmente se instalará en SpamTitan su primer disco IDE.

Como se ve en la siguiente imagen:



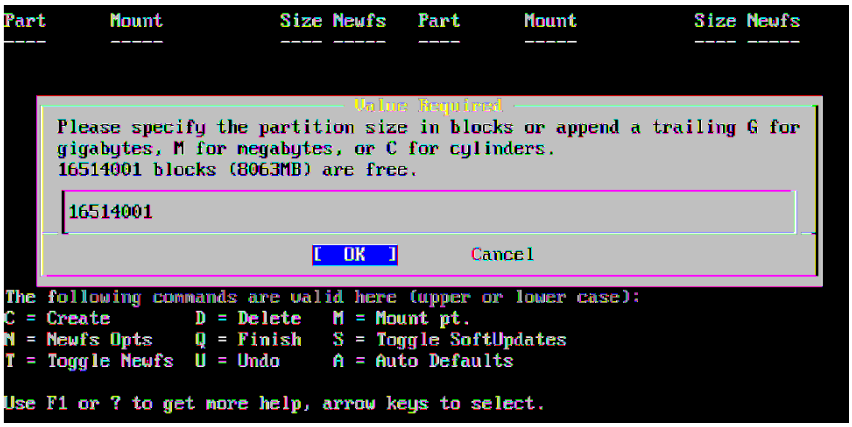
Pantalla de selección de disco a utilizar para instalación

Se verá después una pantalla mostrando si desea ocupar todo el disco duro, después de ello se verá la partición en la que se desea instalar, se debe pulsar una X para seleccionar la partición



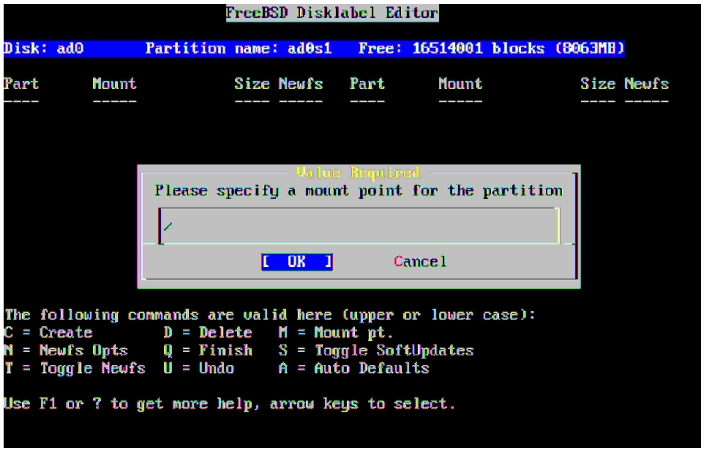
Pantalla de selección de partición de disco

Después de ello se debe elegir el tamaño para la partición



Pantalla Tamaño de partición

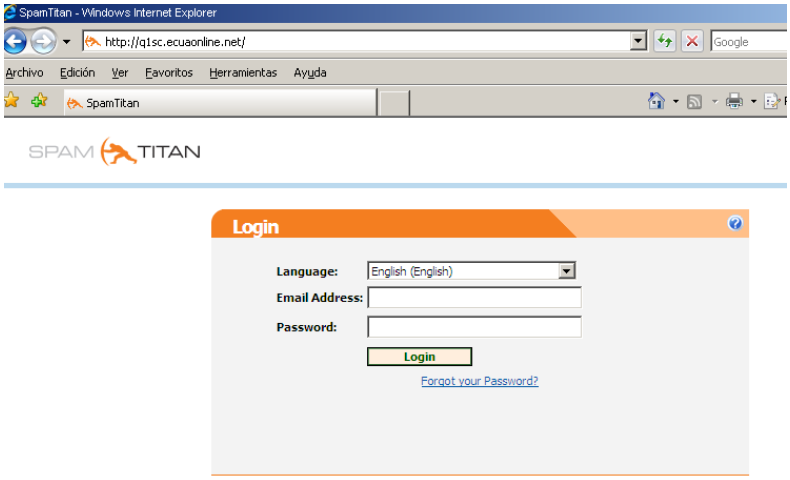
Se le solicitará el tipo de partición, es decir si es sistema de archivos o SWAP. En este caso elegimos sistema de archivos es un método para almacenar y organizar los archivos y los datos que contienen para que sea fácil de encontrar y acceder a ellos, el tamaño total de la partición que se creo en nuestro caso es de 40 GB que se deben repartir para las siguientes paritiviones swap, /user, /temp y /var. Luego se debe seleccionar el punto en que se va a instalar la partición, en este caso en la raíz.



Pantalla selección donde se montara la partición

Lo mismo se debe hacer para las particiones restantes, para finalizar se debe presionar q.

Después de ello se debe configurar SpamTitan appliance



Pantalla inicio configuración aplicación

Para acceder a la cuenta de administrador con el usuario admin y la contraseña hiadmin

ANEXO C

Mensajes de notificación que se presentan a los usuarios por parte del Servidor Anti Spam

Los siguientes mensajes llegan al destinatario o al remitente del correo electrónico dependiendo del problema que se presente.

Plantilla de notificación de Virus al destinatario

Virus Notification

Virus(es) detected:

%V

Scanner detecting a virus: %W

The mail originated from: <%o>

First upstream SMTP client IP address: %a (%g)

According to the 'Received' trace, the message originated

at: %e

---------- BEGIN HEADERS ----------

Return-Path: %s

[%H|\n]

---------- END HEADERS ----------

Plantilla de notificación de Virus al remitente

Our content checker found %#V virus(es) in email presumably from

you (%s) to the following recipient(s):

%R

Please check your system for viruses or ask your system administrator

to do so.

For your reference, here are the headers from your email:

---------- BEGIN HEADERS ----------

Return-Path: %s

[%H|\n]

---------- END HEADERS ----------

Plantilla de notificación al destinatario de rechazo de correo

Banned Attachment Alert

Our content checker found %#F banned names: %F

in an email addressed to you claiming to be from %s.

Please contact your system administrator for further details.

For your reference, here are the headers from the email:

---------- BEGIN HEADERS ----------

[%H|\n]

---------- END HEADERS ----------

Plantilla de notificación al administrador de rechazo de correo

Banned Attachment Notification

Banned name(s) detected:

%F

The mail originated from: <%o>

First upstream SMTP client IP address: %a (%g)

According to the 'Received' trace, the message originated

at: %e

---------- BEGIN HEADERS ----------

Return-Path: %s

[%H|\n]

---------- END HEADERS ----------

Plantilla de notificación al remitente de rechazo de correo

Banned Attachment Alert

Our content checker found %#F banned attachment(s) in email

presumably from you (%s) to the following recipient(s):

%R

The message has been blocked because it contains a component

(as a MIME part or nested within) with declared name or MIME type

or contents type violating our access policy.

To transfer contents that may be considered risky or unwanted

by site policies, or simply too large for mailing, please consider

publishing your content on the web, and only sending an URL of the

document to the recipient.

Plantilla de notificación de Spam al administrador

Unsolicited bulk email identified from (possibly forged) sender:

%o

To: %R

Subject: %j

[? %q |Message not quarantined.|Message quarantined]

SpamAssassin Report:

[%A|\n]

---------- BEGIN HEADERS ----------

Return-Path: %s

[%H|\n]

---------- END HEADERS ----------

Plantilla de notificación de Spam al remitente

Your message to:

%R

was considered unsolicited bulk e-mail (SPAM) by

our mail filters.

Subject: %j

Return-Path: %s

Delivery of the email was stopped!

BIOGRAFÍA DEL AUTOR

DAVID MONCAYO FERNÁNDEZ DE CÓRDOVA

Fecha de nacimiento:	11 de Octubre de 1982
Lugar de nacimiento:	Quito- Pichincha
Nacionalidad:	Ecuatoriana
Dirección Domiciliaria:	Urbanización Club los Chillos, calle #4 casa 7-16
Dirección de correo electrónico:	david_diga@hotmail.com
Referencia:	Colegio Marista
Bachillerato:	Ciencias
Especialización:	Físico- Matemático
Ingreso a la ESPE:	Periodo Septiembre 01- Febrero 02
Egreso de la ESPE:	Periodo Académico Octubre06- Febrero07

HOJA DE LEGALIZACIÓN DE FIRMAS

ELABORADA POR

_____

David Moncayo

COORDINADOR DE LA CARRERA

_____

Ing. Danilo Martínez

Lugar y fecha: _____