Seguridad en sistemas de correo electrónico

Master en Seguridad de la Información – 2007

alvaro@hostalia.com

Contenido

Introducción

Protocolos de correo electrónico
- Intercambio de mensajes: SMTP
- Recogida: POP3/IMAP4

MTAs
- Sendmail
- Postfix
- Exim
- Qmail
- MS Exchange

SPAM
- ¿Qué es el SPAM?

Contenido

Medidas anti-SPAM
- Restricciones a nivel de MTA
- Realtime Blackhole Lists
- SpamAssassin

Medidas avanzadas anti-SPAM
- SPF, DomainKeys, DKim
- Greylists

Medidas anti-Virus
- Antivirus a nivel de servidor

Pasarelas de correo
- Amavis
- MailScanner

Introducción

1971: A partir del SNDMSG, Ray Tomlison usa ARPANET para enviar el primer e-mail -> *@servidor*

1977: Primer estándar para mensajes ARPANET: RFC 733

1978 : Primer mensaje de "spam"

1982: RFC 822 y RFC 821 -> Simple Mail Transfer Protocol

1989: Primer intercambio comercial

1994: RFC 1725 -> Post Office Protocol

2000: primeros programas anti-spam

2003: Alan Ralsky, "The king of spam"

2005: Técnicas avanzadas de detección de spam

Introducción

Características del correo electrónico:

- No requiere una presencia en ambos extremos (sí teléfono)
- Barato (~gratis), depende de la conexión utilizada
- Fácil de utilizar
- Permite movilidad
- Permite el envío de diferentes archivos adjuntos
- Diferentes usos: personal, profesional, público...etc
- Envío casi instantáneo

Es el servicio más utilizado en Internet.
Actualmente está en "peligro" debido a las amenazas (spam, virus...).
SMTP es un protocolo antiguo y que no está orientado a la seguridad.

Introducción

Arquitectura básica:

- Agente de usuario (MUA)
  - Programas para leer/escribir mensajes
  - Ej: Thunderbird, Outlook...
- Agente de transferencia (MTA)
  - Transmite mensajes entre máquinas
  - Ej: Sendmail, Postfix, MS Exchange...

Estándares involucrados:

- Formato del mensaje: MIME
- Resolución de nombres: DNS (MX o A en su defecto)
- Protocolo de envío de mensajes : SMTP/ESMTP
- Protocolo de recogida de mensajes: POP/IMAP

RFC 822

RFC 822: Formato estándar de mensajes de texto en Internet

Formato del mensaje completo:

- Cabeceras:
  - Formato: *Nombre-cabecera: valor <CR><LF>*
  - Generadas por MUAs o MTAs
  - Orden aleatorio
  - En NVT ASCII

- Cuerpo del mensaje:
  - En NVT ASCII
  - Solo texto (para otros contenidos, ver ext. MIME)
  - Máximo 1000 caracteres/línea

Ejemplo:

RFC 822

Return-Path: <split@splitcc.net>
X-Original-To: alvaro@hostalia.com
Delivered-To: alvaro@hostalia.com
Received: from mail.splitcc.net (169.Red-80-25-85.staticIP.rima-tde.net [80.25.85.169])
by mail.hostalia.com (Postfix) with ESMTP id C868668031B
for <alvaro@hostalia.com>; Sat, 21 Jan 2006 14:16:44 +0100 (CET)
Received: by mail.splitcc.net (Postfix, from userid 1003)
id 2635D1337D; Sat, 21 Jan 2006 14:16:40 +0100 (CET)
Date: Sat, 21 Jan 2006 14:16:38 +0100
From: Alvaro Marin <split@splitcc.net>
To: alvaro@hostalia.com
Subject: Prueba mensaje
Message-ID: <20060121141638.50de4e31@basajaun>

Mensaje de prueba

MIME

MIME: Multi-Purpose Internet Mail Extensions - RFC 2045

Solventa los problemas de RFC 822:

- Solo admite NVT ASCII
- Lenguas latinas (ñ, á...)
- Lenguas no latinas (hebreo, ruso, chino...)
- Imágenes, sonido, vídeo...

Define 5 nuevas cabeceras:

- **MIME-Version**: debe estar presente para que el mensaje sea tratado como MIME. Actualmente 1.0.
- **Content-type**: cómo interpretar un objeto del cuerpo del mensaje (text/plain; charset=us-ascii).
- **Content-Transfer-Encoding**: cómo está codificado el objeto (por defecto 7bits (NVT ASCII)).
- **Content-Description**: descripción del objeto.
- **Content-Id**: valor único identificativo del objeto.

MIME

Tipos predefinidos para Content-type (type/subtype; parameter=value):

- *text/plain* : texto plano
  - text/plain; charset=us-ascii (por defecto)
  - text/plain; charset=iso-8859-X
- *text/html* : texto html
- *multipart*: cuando el mensaje tiene varias partes
- *image*: el cuerpo es una imagen (image/jpeg, image/gif...)
- *video*: el cuerpo es un vídeo (video/mpeg...)

Opciones para Content-Transfer-Encoding:

- *7-bit*: NVT ASCII (línea < 1000)
- *8-bit*: NVT ASCII + otros caractares (línea < 1000)
- *quoted-printable*: textos con pocos caracteres no NVT ASCII (por ejemplo, mensajes en castellano)
- *base64*: codifica datos binarios (aumenta de tamaño)

MIME

Mensaje en castellano:

```
Mime-Version: 1.0
Content-Type: text/plain; charset=ISO-8859-15
Content-Transfer-Encoding: quoted-printable
```

Mensaje multiparte:

```
Mime-Version: 1.0
Content-Type: multipart/mixed;
 boundary=Multipart_Sat__21_Jan_2006_15_38_40_+0100_6v7h2cun_NTQHy9L
--Multipart_Sat__21_Jan_2006_15_38_40_+0100_6v7h2cun_NTQHy9L
Content-Type: text/plain; charset=US-ASCII
Content-Transfer-Encoding: 7bit
Content-Disposition: inline

prueba jpg
--Multipart_Sat__21_Jan_2006_15_38_40_+0100_6v7h2cun_NTQHy9L
Content-Type: image/jpeg; name=prueba.jpg
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=prueba.jpg

/9j/4AAQSkZJRgABAQEASABIAAD/4QAWRXhpZgAATU0AKgAAAA...

--Multipart_Sat__21_Jan_2006_15_38_40_+0100_6v7h2cun_NTQHy9L--
```

RFC 821

RFC 821: SMTP, Simple Mail Transfer Protocol

Protocolo estándar para enviar mensajes:

MUA -> MTA

MTA <->MTA

Data de 1984, antiguo y simple => inseguro

Usa DNS continuamente:

- Resolver el registro MX del registro destinatario
- Resolver el registro A del resultado anterior
- Resoluciones inversas

Usa los puertos TCP:

- 25: SMTP (587 como alternativo)
- 465: SecureSMTP

RFC 821

Algunos comandos (NVT ASCII) del protocolo SMTP:

- **HELO**: "saludo" inicial en el que el cliente indica quién es (su dominio o hostname o IP). Se podría traducir como : "*Hello, I am <domain>*".
- **MAIL FROM**: indica quién es el que envía. Por ejemplo:
  MAIL FROM: alvaro@hostalia.com
- **RCPT TO**: indica la dirección del destinatario. Por ej:
  RCPT TO: alvaro@rigel.deusto.es
- **DATA**: punto de comienzo en el que se empezará a enviar el cuerpo del mensaje. Acabará con una línea con un ".".
- **QUIT**: cierra la conexión

Ejemplo:

RFC 821

$telnet mail.splitcc.net 25
Trying 80.25.85.169...
Connected to 80.25.85.169.
Escape character is '^]'.
220 mail.splitcc.net ESMTP ready
helo mail.hostalia.com
250 mail.splitcc.net
mail from: alvaro@hostalia.com
250 Ok
rcpt to: split@splitcc.net
250 Ok
data
354 End data with <CR><LF>.<CR><LF>
Este es un mensaje de prueba para el Master.
.
250 Ok: queued as CF52B1337C
quit
221 Bye
Connection closed by foreign host.

RFC 821

Algunas respuestas ante comandos SMTP:

220 <domain> Service ready
221 <domain> Service closing transmission channel
250 Requested mail action okay, completed
251 User not local; will forward to <forward-path>
354 Start mail input; end with <CRLF>.<CRLF>
421 <domain> Service not available, closing transmission channel
450 Requested mail action not taken: mailbox unavailable [E.g., mailbox busy]
451 Requested action aborted: local error in processing
452 Requested action not taken: insufficient system storage
500 Syntax error, command unrecognized
501 Syntax error in parameters or arguments
502 Command not implemented
503 Bad sequence of commands
504 Command parameter not implemented
550 Requested action not taken: mailbox unavailable
[E.g., mailbox not found, no access]

2XX/3XX=> *successful* ***4XX***=>*temporary errors* ***5XX***=>*permanent errors*

RFC 821

MAIL FROM: Origen del mensaje.
RCPT: Destinatario del mensaje.
No confundir con cabeceras "From:" y "To:" de la sección DATA.

$telnet mail.splitcc.net 25
Trying 80.25.85.169...
Connected to 80.25.85.169.
Escape character is '^]'.
220 mail.splitcc.net ESMTP ready
helo mail.hostalia.com
250 mail.splitcc.net
mail from: alvaro@hostalia.com **<- ENVELOPE SENDER**
250 Ok
rcpt to: split@splitcc.net **<- ENVELOPE RECIPIENT**
250 Ok
data
354 End data with <CR><LF>.<CR><LF>
Subject: Asunto del mensaje
From: fromenelMUA@dominio.com <- **FROM SECCIÓN DATA**
To: toenelMUA@dominio.com <- **TO SECCIÓN DATA**
Este es un mensaje de prueba para el Master.
.
250 Ok: queued as CF52B1337C
quit
221 Bye
Connection closed by foreign host.

RFC 821

Ejemplo: envío un mensaje con mi MUA poniendo:

To: alvaro@rigel.deusto.es, split@splitcc.net

El MUA conectará con el MTA y enviará los siguientes comandos:

RCPT TO: alvaro@rigel.deusto.es
RCPT TO: split@splitcc.net

El MTA preguntará por el MX de rigel.deusto.es y se conectará a él; en el momento de introducir el RCPT pondrá:

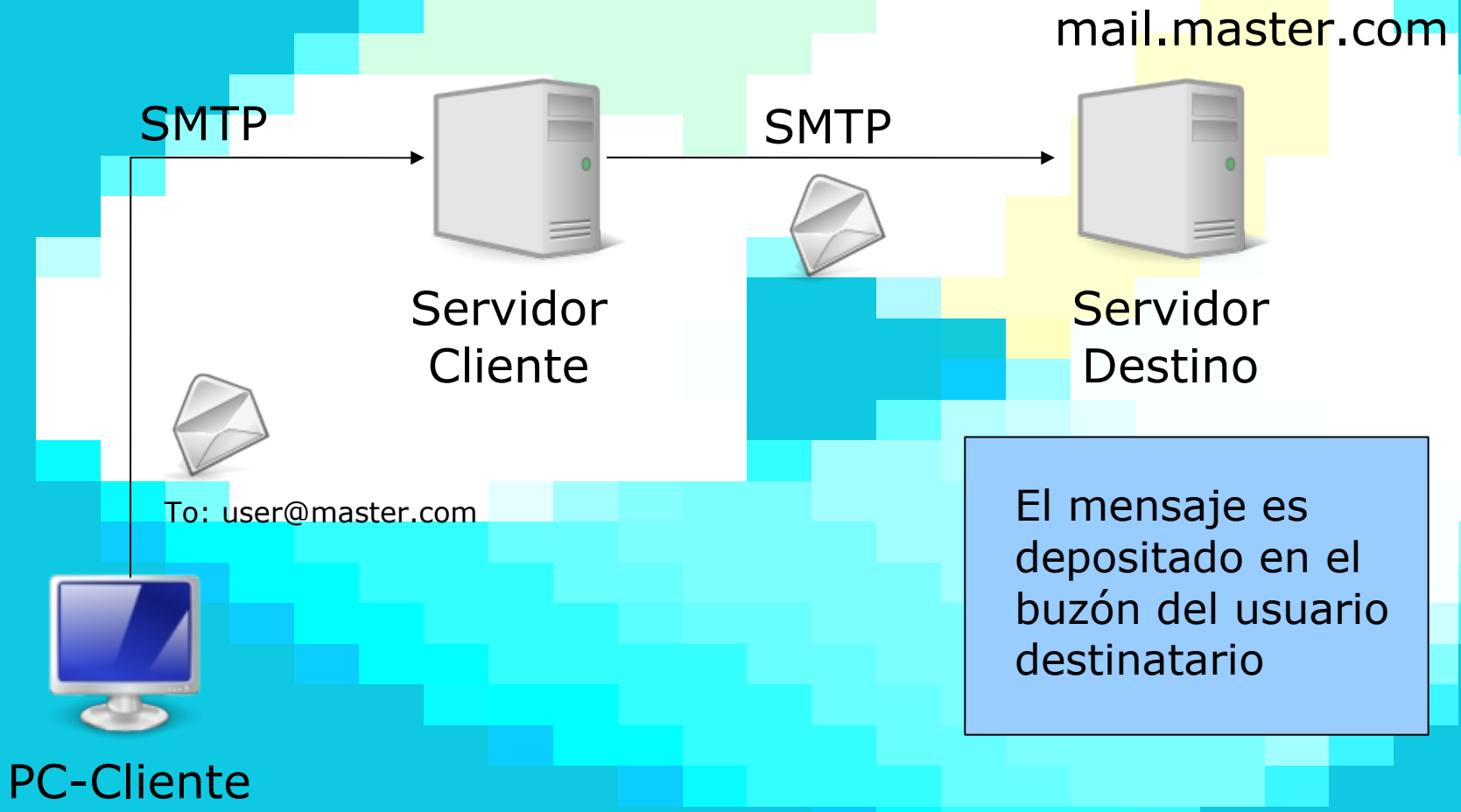
RCPT TO: alvaro@rigel.deusto.es

Seguidamente preguntará por el MX de splitcc.net, se conectará a él y pondrá:

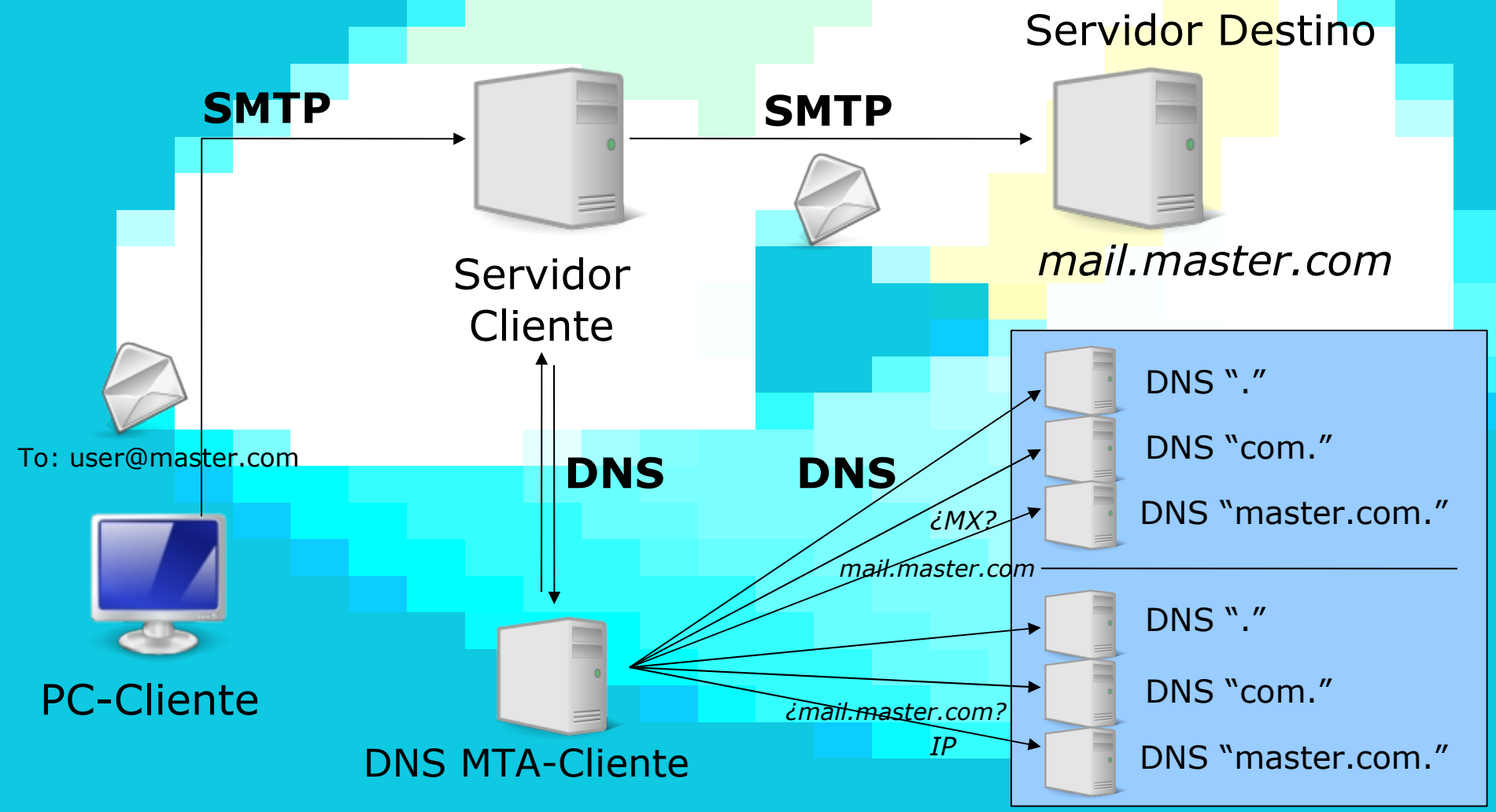
RCPT TO: split@splitcc.net

Ambos desinatarios tendrán como cabecera "To:" la original que puso el MUA, pero la cabecera RCPT TO será diferente (Delivered-To).

Protocolo SMTP



Protocolo SMTP+ DNS



Protocolo ESM TP

Protocolo **ESMTP**, RFC 1869

Extensión del protocolo SMTP anterior (autenticación, cifrado...)
Compatibilidad "hacia atrás".
El cliente que desee utilizarlo, deberá presentarse con "EHLO" en vez del "HELO" habitual.
El servidor responde con los comandos ESMTP que soporta:

$ telnet mail.deusto.es 25
Trying 130.206.100.17...
Connected to mail.deusto.es.
Escape character is '^]'.
220 gr-1.deusto.es ESMTP
EHLO mail.splitcc.net
250-gr-1.deusto.es
250-PIPELINING
250-SIZE 6242880
250-ETRN
250-STARTTLS
250-AUTH LOGIN PLAIN
250 8BITMIME

Cabeceras SMTP

Las más importantes y que más información pueden dar:

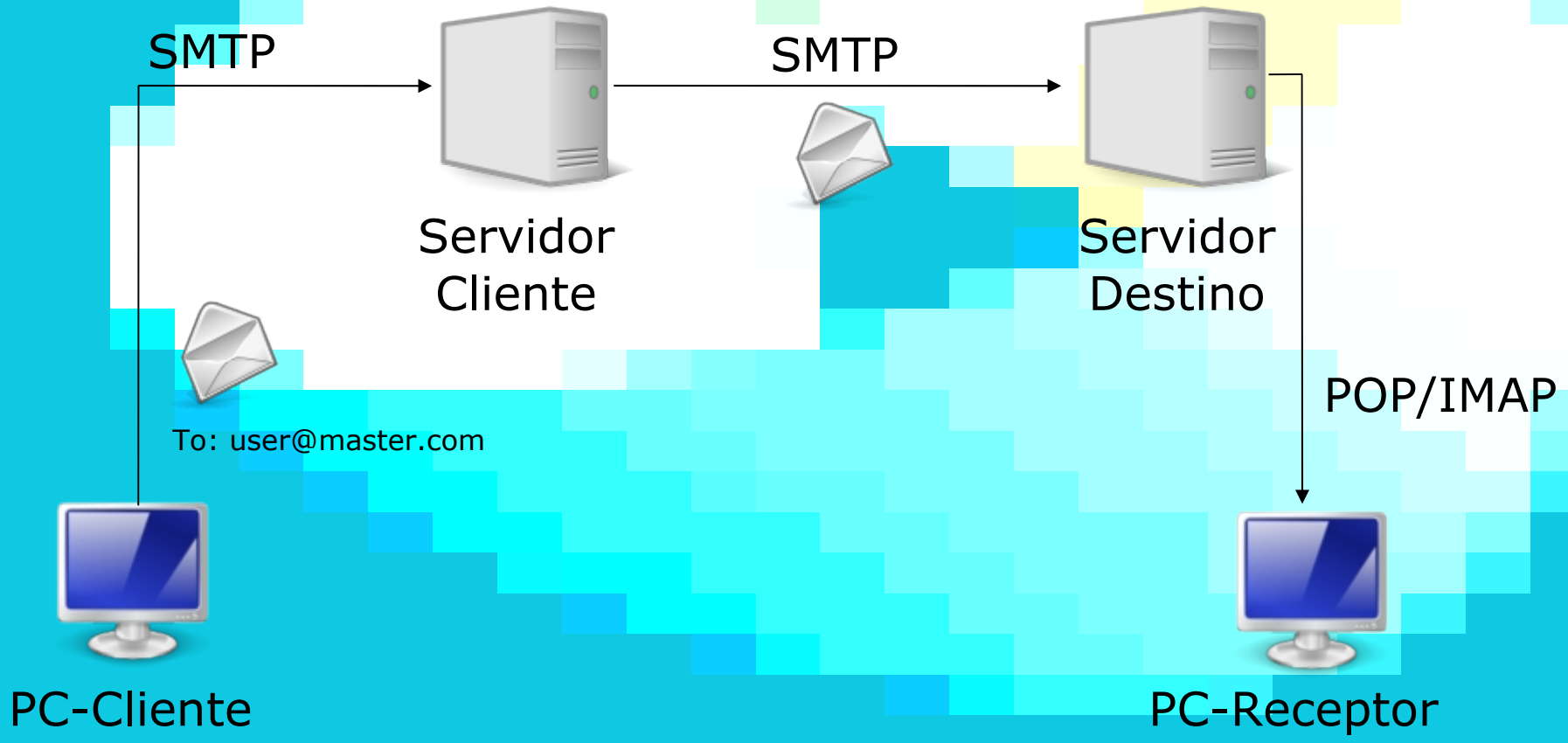
- Cabecera *Received* : es añadida por cada MTA por el que el mensaje pasa. Nos permite saber la ruta de un mensaje, tiempo que ha sido retenido en cada MTA...
- Cabecera *Return-Path*: la genera el MDA final indicando cuál es el emisor real del mensaje, a partir del MAIL FROM. Es usada cuando hay que generar un bounce.
- Cabecera *Reply-To*: la dirección a la que responder o enviar las respuestas. Es añadido por el emisor. Muy común en listas de correo, en las que quien escribe es distinto a quien hay que responder (la lista).
- Cabecera *Delivered-To* : dirección a la que realmente es entregado el mensaje (sin alias).

Cabeceras completas

Return-Path: *<alvaro@hostalia.com>*
Delivered-To: 1almarin@rigel.deusto.es
Received: from mail.hostalia.com (ws.hostalia.com [82.194.64.2])
by gr-1.deusto.es (Postfix) with ESMTP id 1CD1724B56D
for <alvaro@rigel.deusto.es>; Sat, 20 Jan 2007 11:31:47 +0100 (CET)
Received: from basajaun (169.Red-80-25-85.staticIP.rima-tde.net [80.25.85.169])
(using TLSv1 with cipher DHE-RSA-AES256-SHA (256/256 bits))
(No client certificate requested)
by mail.hostalia.com (Postfix) with ESMTP id 3CDA06807DF
for <alvaro@rigel.deusto.es>; Sat, 20 Jan 2007 11:31:51 +0100 (CET)
Date: Sat, 20 Jan 2007 11:31:44 +0100
From: Alvaro Marin <alvaro@hostalia.com>
To: alvaro@rigel.deusto.es
Subject: Prueba
X-Mailer: Sylpheed-Claws 1.0.5 (GTK+ 1.2.10; i486-pc-linux-gnu)
Mime-Version: 1.0
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: quoted-printable
X-Virus-Scanned: by amavis at mail.deusto.es

Protocolos de recogida

Protocolos de recepción de correo almacenado en el servidor.



Protocolo POP 3

Protocolo **POP3**, RFC 1939.
Accede al buzón del usuario y se descarga los mensajes.
Usa TCP:110 y TCP:995 para POP3S.
Protocolo simple: 13 comandos con respuestas +OK o -ERR.

$telnet servidor 110
...
+OK Hello there.
user alvaro <- ***usuario***
+OK Password required.
*Pass *********** <- ***contraseña***
+OK logged in.
list <- ***listar mensajes del buzón***
+OK POP3 clients that break here, they violate STD53.
1 1406
2 1594
.
top 1 10 <- **10 primeras líneas del mensaje 1**
retr 1 <- **ver todo el mensaje 1**
dele 1 <- **borrar el mensaje 1**
quit <- **efectuar cambios y salir**

Protocolo IMAP 4

Protocolo **IMAP4**, RFC 3501.
Más sofisticado y con más opciones que POP3.
Se accede directamente al buzón del servidor donde el usuario puede crear/borrar directorios, mover mensajes...etc.
Usa puertos TCP:143 y TCP:993 para IMAP4S.

```
$ telnet 192.168.1.10 143
Trying 192.168.1.10...
Connected to 192.168.1.10.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT
  THREAD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNION] Courier-IMAP ready. Copyright 1998-2004
  Double Precision, Inc.  See COPYING for distribution information.
1 CAPABILITY
* CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT
  THREAD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNION
1 OK CAPABILITY completed
2 LOGIN split password
2 OK LOGIN Ok.
NAMESPACE
NAMESPACE NO Error in IMAP command received by server.
3 NAMESPACE
* NAMESPACE (("INBOX." ".")) NIL (("#shared." ".")("shared." "."))
3 OK NAMESPACE completed.
```

Message Submission

Message Submission Agent, protocolo especificado en RFC 2476, del año 1998.

Proceso de aceptación de mensajes desde el MUA.

Escucha en el puerto TCP:587 a la espera de la recepción de mensajes. Sustituye al puerto 25 a la hora de envíos desde MUAs.

Ventajas:

- Solo permitir envíos autenticados
- Permite separar políticas 25 *Vs* 587
- Alternativa ante filtros (por ej, Telefónica)
- Protección del MTA ante virus de clientes

MTAs

Existen muchos programas que implementan las funciones que debe realizar un MTA.

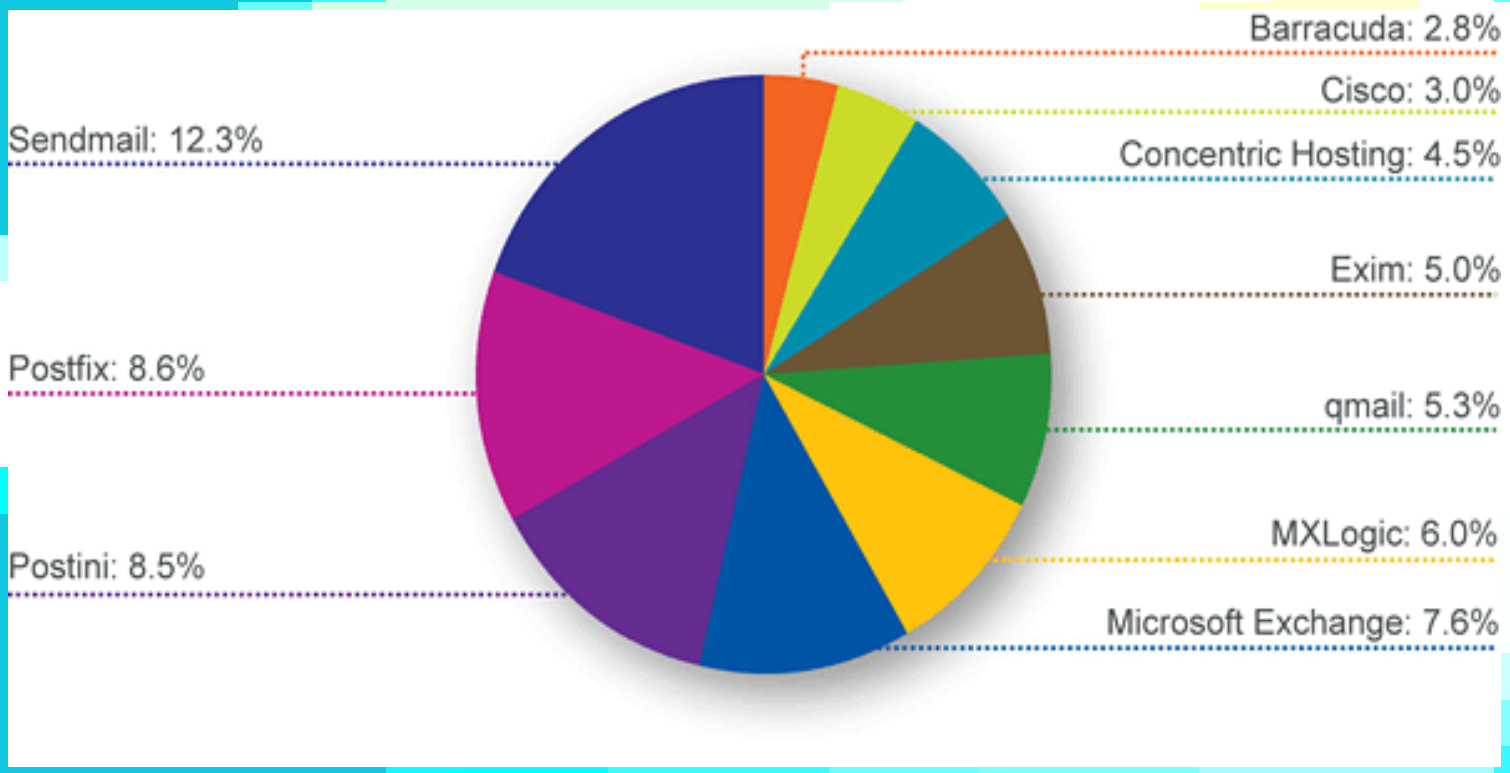
Las características que más se suelen valorar son:

- Capacidad de tratar correo concurrentemente
- Velocidad de entrega local/remota
- Extensibilidad y funciones implementadas
- Estabilidad
- Tratamiento de la cola

Entre los más conocidos se encuentran:

- Sendmail
- Postfix
- Exim
- Qmail
- MS Exchange

MTA s



http://www.oreillynet.com/pub/a/sysadmin/2007/01/05/fingerprinting-mail-servers.html

MTAs - Sendmail

Sendmail es uno de los MTAs más viejos que existen. Implementado para los UNIX existentes en su época.

Al ser el más antiguo, dispone también de una larga lista de vulnerabilidades que le han dado una fama de "inseguro", aunque no sea así.

Muy configurable pero a la vez, muy complejo de configurar.

Versión actual: 8.14.1

Creador: Eric Allman

Página: www.sendmail.org

MTAs - Postfix

Postfix aparece como alternativa a Sendmail, dando una mayor facilidad de instalación/configuración.
Dispone de los comandos que disponía Sendmail.
Muy extensible y adaptable (LDAP,MySQL,SASL,TLS...)
Desarrollo muy activo. Arquitectura modular.
Centrado en la rapidez y la seguridad.

Versión actual: 2.4

Creador: Wietse Venema

Página: www.postfix.org

MTAs – Exim

Exim es un MTA creado en la Universidad de Cambridge. No tiene tanta fama como los anteriores, pero también es ampliamente usado.

Dispone de bastantes ventajas sobre otros MTAs:

- Capaz de hacer llamadas a Perl
- Herramientas y comandos muy potentes:
  - *exim -Mrm ID*
  - *exim -M ID*
  - *exim -Mvh ID*
  - *exim -Mvb ID*
  - *exiqgrep patrón*
  - *exigrep patrón*

Su última versión es la 4.66 (www.exim.org).

MTAs – Qmail y Exchange

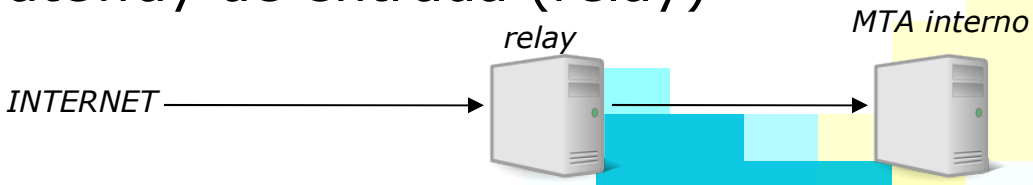
Qmail es un MTA creado por D.J. Bernstein (djbdns).
Su licencia no permite la distribución de binarios, por lo que hay que compilar siempre su código fuente.
Nuevas funcionalidades => parchear código y compilar.
Destaca por su óptima gestión de colas.
Difícil de configurar, en varios archivos.
Su última versión es la 1.0.5 (www.qmail.org)

MS Exchange es un MTA que incorpora otras funcionalidades como buzones compartidos, agendas, libretas de direcciones...
Configuración limitada en comprobaciones SMTP/DNS.
Integración completa con el Directorio Activo.
Webmail integrado muy potente, OWA.

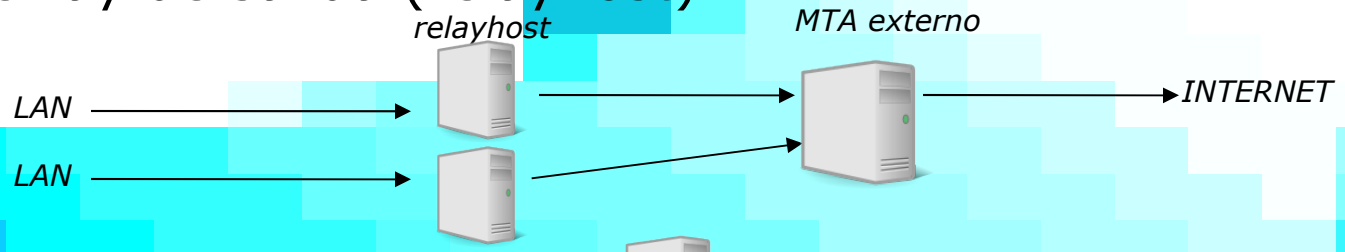
MTAs

Configuraciones típicas:

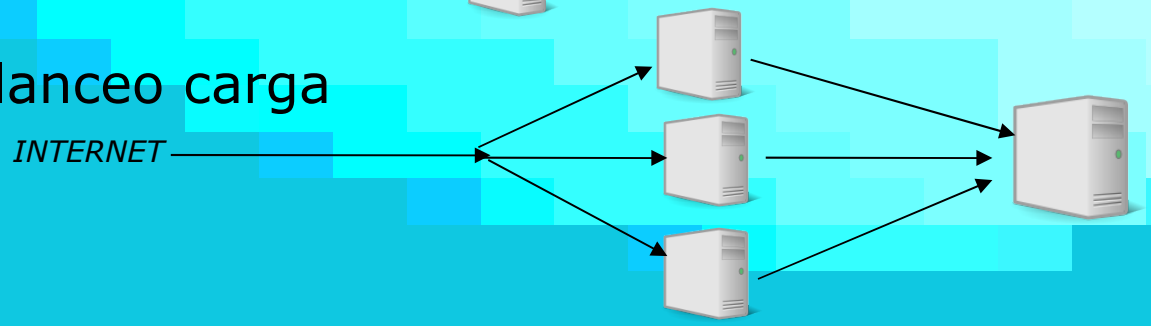
- Gateway de entrada (relay)



- Gateway de salida (relayhost)



- Balanceo carga



SPAM

Mensajes de correo comerciales no solicitados.

El origen de éstos suelen ser servidores de correo mal configurados, gusanos, CGIs no protegidos...etc.

Supone una gran amenaza para la continuidad y eficacia del correo electrónico ya que puede llegar a colapsar los MTAs. Se invierte mucho dinero en intentar frenarlo.

Las últimas cifras hablan que el 80% de los e-mails son spam.

SPAM

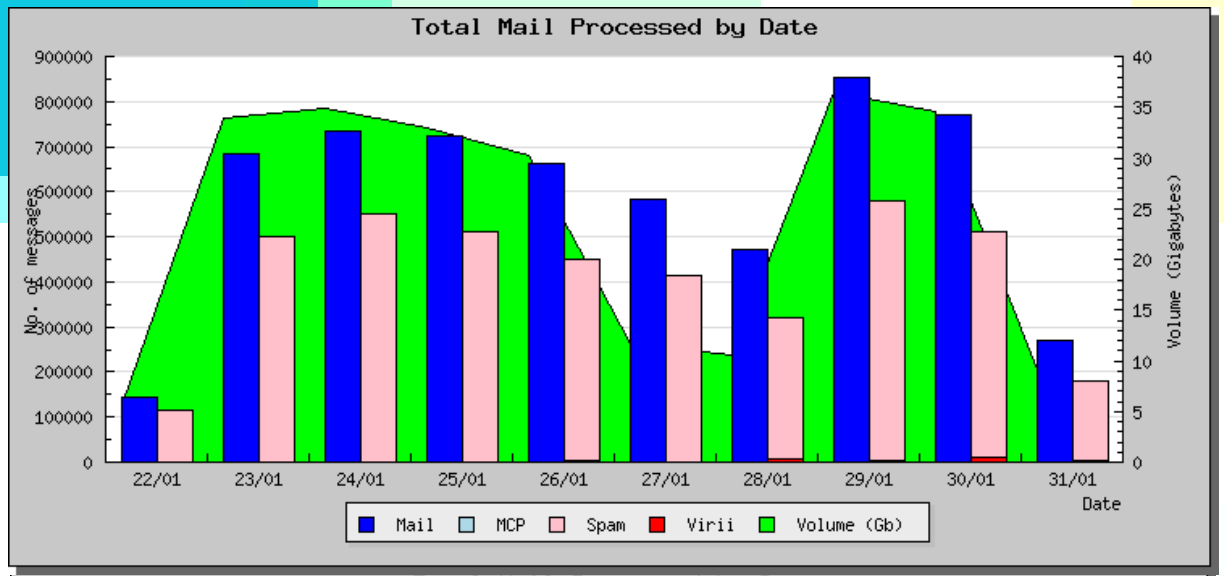
¿Porqué se envía spam? => se vende a través de él y es un buen negocio para el emisor (muy barato).

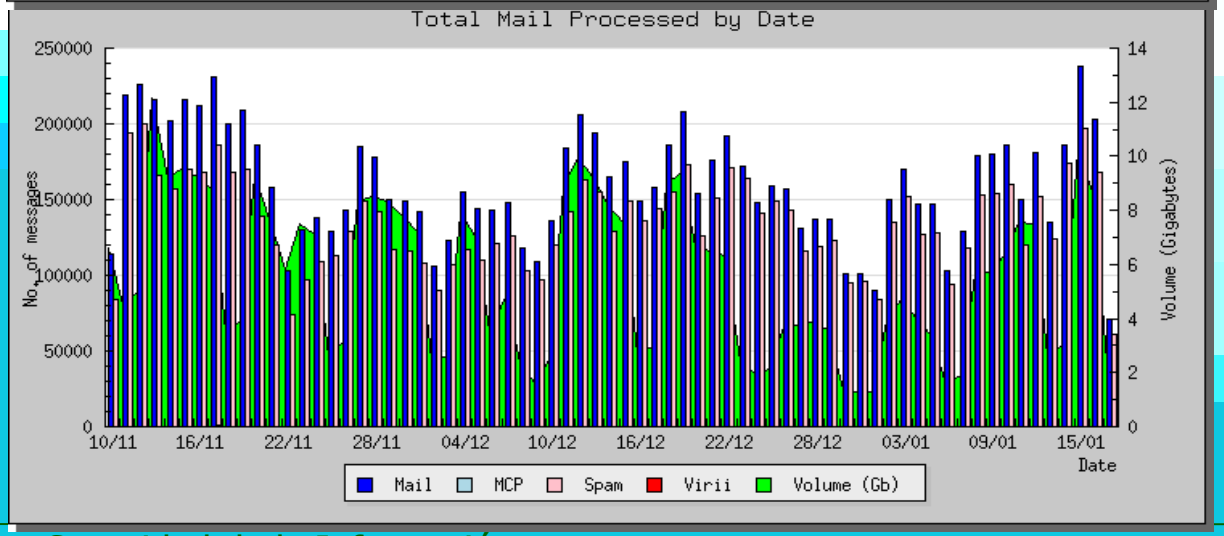
Cómo se envía el spam:

- Falsificando los From de los correos
- Recogiendo los destinatarios de webs, news...etc.
- Usando servidores mal configurados
- Usando ordenadores "*zombies*" =>filtrado puerto SMTP
- Por medio de ataques a CGIs, PHPs, ASPs...
- Inyección de código en formularios web
- ...

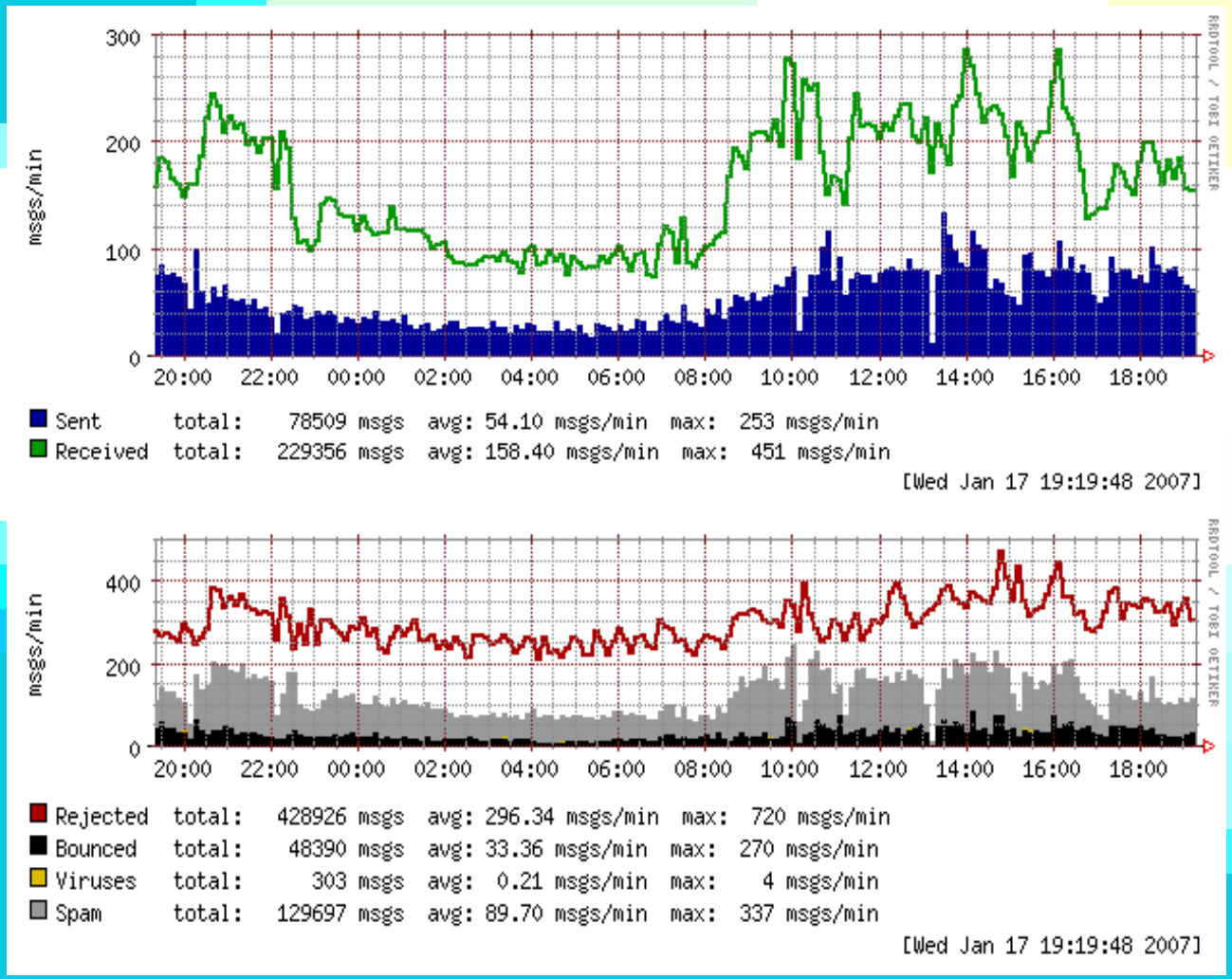
El SPAM en estadísticas:

SPAM

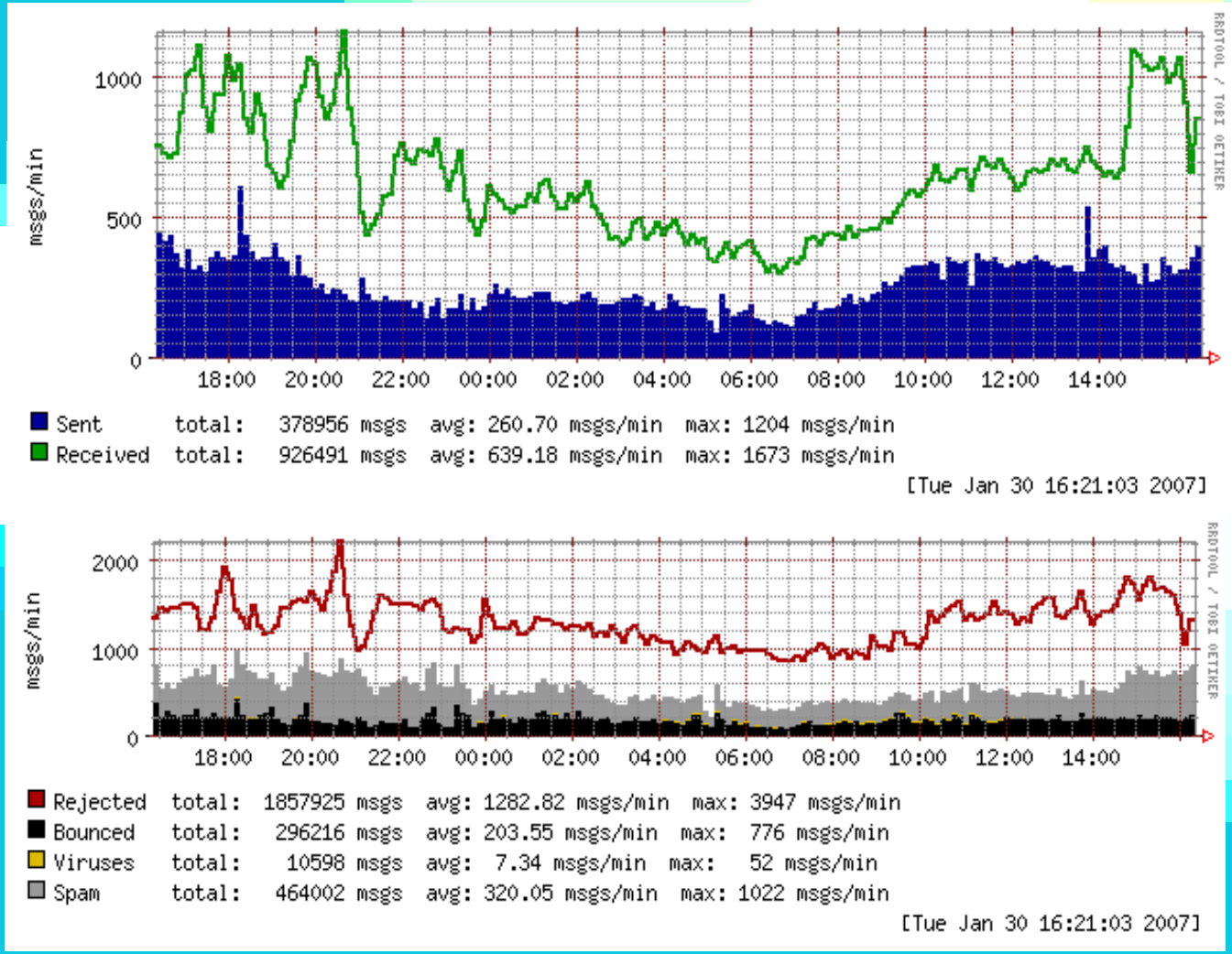

Total Mail Processed by Date
No. of messages
Volume (Gigabytes)
900000
800000
700000
600000
500000
400000
300000
200000
100000
0
40
35
30
25
20
15
10
5
0
22/01
23/01
24/01
25/01
26/01
27/01
28/01
29/01
30/01
31/01
Date
Mail
MCP
Spam
Virii
Volume (Gb)


Total Mail Processed by Date
No. of messages
Volume (Gigabytes)
250000
200000
150000
100000
50000
0
14
12
10
8
6
4
2
0
10/11
16/11
22/11
28/11
04/12
10/12
16/12
22/12
28/12
03/01
09/01
15/01
Date
Mail
MCP
Spam
Virii
Volume (Gb)

SPAM


msgs/min
300
200
100
0
20:00
22:00
00:00
02:00
04:00
06:00
08:00
10:00
12:00
14:00
16:00
18:00
Sent total: 78509 msgs avg: 54.10 msgs/min max: 253 msgs/min
Received total: 229356 msgs avg: 158.40 msgs/min max: 451 msgs/min
[Wed Jan 17 19:19:48 2007]
msgs/min
400
200
0
Rejected total: 428926 msgs avg: 296.34 msgs/min max: 720 msgs/min
Bounced total: 48390 msgs avg: 33.36 msgs/min max: 270 msgs/min
Viruses total: 303 msgs avg: 0.21 msgs/min max: 4 msgs/min
Spam total: 129697 msgs avg: 89.70 msgs/min max: 337 msgs/min
[Wed Jan 17 19:19:48 2007]

SPAM


msgs/min
1000
500
0
18:00 20:00 22:00 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00
RRDTOOL / TOBI OETIKER
Sent total: 378956 msgs avg: 260.70 msgs/min max: 1204 msgs/min
Received total: 926491 msgs avg: 639.18 msgs/min max: 1673 msgs/min
[Tue Jan 30 16:21:03 2007]
msgs/min
2000
1000
0
18:00 20:00 22:00 00:00 02:00 04:00 06:00 08:00 10:00 12:00 14:00
RRDTOOL / TOBI OETIKER
Rejected total: 1857925 msgs avg: 1282.82 msgs/min max: 3947 msgs/min
Bounced total: 296216 msgs avg: 203.55 msgs/min max: 776 msgs/min
Viruses total: 10598 msgs avg: 7.34 msgs/min max: 52 msgs/min
Spam total: 464002 msgs avg: 320.05 msgs/min max: 1022 msgs/min
[Tue Jan 30 16:21:03 2007]

SPAM

NOQUEUE+Procesados: 3272057

Clean mail:	19772 - 0.60%
Marked(delivered) mail:	198084 - 6.05%
Spam(deleted) mail:	543078 - 16.60%
NOQUEUE RBL-SpamCop:	1659614 - 50.72%
NOQUEUE RBL-SpamHaus:	408694 - 12.49%
NOQUEUE RBL-Dsbl:	54037 - 1.65%
NOQUEUE RBL-DnsSrv:	112575 - 3.44%
NOQUEUE HostRejected:	143114 - 4.37%
NOQUEUE DomainNotFound:	127120 - 3.89%
NOQUEUE FQDN:	2543 - 0.08%
NOQUEUE RcptRejected:	126 - 0.00%
NOQUEUE MalformedDNS:	33 - 0.00%
NOQUEUE RelayDenied:	3267 - 0.10%

SPAM

Países generadores de SPAM (Informe Comisión Europea, 30/11/2006):

1º Estados Unidos de América, con un 21,6%
2º China (incluido Hong Kong), con un 13,4%
3º Francia, con un 6,3%
3º Corea del Sur, también con un 6,3%
5º España, con un 5,8%
6º Polonia, con un 4,8%
7º Brasil, con un 4,7%
8º Italia, con un 4,3%
9º Alemania, con un3,0%
10º Taiwán, con un 2,0%
11º Israel, con un 1,8%
12º Japón, con un 1,7%
Otros, 24,3%

Spammers : *http://www.spamhaus.org/statistics/spammers.lasso*

Anti-SPAM

Existen actualmente numerosas medidas anti-spam, tanto comerciales como gratuitas.
La mejor será aquella que de menos falsos positivos (mensajes legítimos marcados como SPAM) y detecte más mensajes SPAM.
La más conocida puede que sea SpamAssasin.

Diferentes técnicas: a nivel de MTA, listas negras, software analizador...etc.

Debe tenerse en consideración que perder mensajes legítimos por el uso de un filtro da al traste el uso del correo electrónico.
Posible solución: MARCAR(por ejemplo, mediante cabeceras) y que el cliente decida qué hacer.

Anti-SPAM

Restricciones a nivel de MTA.

Se pueden poner una serie de reglas o restricciones a nivel del propio MTA (en el momento de recibier el mail, antes de procesarlo). Éstas se suelen hacer:

- *client*: denegar la conexión a la IP en concreto, chequear si tiene registro PTR...
- *helo*: chequear el dominio pasado al comando HELO, si cumple el RFC...
- *mail from*: chequear que la dirección es correcta, el dominio resuelve a un registro A...
- *rcpt to*: sintaxis correcta, usuario válido...

Anti-SPAM

Listas negras (RBL - Realtime Blackhole List o DNSBL)

Listas públicas en Internet en las que se añaden IPs de spammers conocidos.

El MTA se configura para que las consulte:

- Se coge la IP del cliente (Ej: 85.216.102.58)
- Se le añade el dominio de la lista que deseamos consultar, por ej: *58.102.216.85.bl.spamcop.net*.
- Hacemos una consulta DNS preguntando por el reg. A:

```
$dig 58.102.216.85.bl.spamcop.net +short
127.0.0.2
```

- Además, podemos preguntar por el registro TXT:

```
$dig TXT 58.102.216.85.bl.spamcop.net +short
"Blocked - see http://www.spamcop.net/bl.shtml?85.216.102.58"
```

- Rechazo del email(nivel RCPT) para generar un *bounce.*

Anti-SPAM

Listas negras (RBL - Realtime Blackhole List o DNSBL)

Las más conocidas son:

- SpamCop: *www.spamcop.net*
- SpamHaus: *www.spamhaus.org*, se divide en:
  - SBL: IPs verificadas de spammers
  - XBL: máquinas con gusanos, exploits...etc
  - PBL: rangos de IPs residenciales, dinámicas...
  - ZEN: las tres anteriores en una
- DSBL
- ORDB (cerrada)
- SORBS (pago para dar de baja)

Ver: www.rbls.org

Anti-SPAM

Además de los métodos comentados anteriormente, que consumen pocos recursos, existen programas específicos para el análisis de los mensajes.

Se suelen basar en reglas (+ IA en algunos casos).

Posibles problemas:

- Consumen muchos recursos (CPU+RAM) en el análisis de los mensajes (cabeceras+cuerpo).
- Pueden dar falsos positivos.
- Debe de configurarse y estar atentos a ver cómo evoluciona la detección.
- Si las reglas quedan obsoletas => no se detecta nada.

SpamAssa ssin

Uno de los programas más conocidos (v3.1.7)
Escrito en PERL (ahora bajo el proyecto Apache).
Utiliza una serie de reglas estáticas y puede usar redes bayesianas para el aprendizaje de nuevo conocimiento.

Analiza el mensaje sumándole puntos por coincidir una de sus reglas o "conocimiento aprendido", por ejemplo:

Content analysis details: (9.1 points, 4.0 required)

pts	rule name	description
0.5	FROM_ENDS_IN_NUMS	From: ends in numbers
1.7	MSGID_FROM_MTA_ID	Message-Id for external message added locally
2.3	DATE_IN_FUTURE_12_24	Date: is 12 to 24 hours after Received: date
0.1	NORMAL_HTTP_TO_IP	URI: Uses a dotted-decimal IP address in URL
0.5	WEIRD_PORT	URI: Uses non-standard port number for HTTP
0.0	HTML_60_70	BODY: Message is 60% to 70% HTML
1.5	HTML_IMAGE_ONLY_12	BODY: HTML: images with 800-1200 bytes of words
0.0	HTML_MESSAGE	BODY: HTML included in message
1.0	HTML_FONT_LOW_CONTRAST	BODY: HTML font color similar to background
1.2	MIME_HTML_ONLY	BODY: Message only has text/html MIME parts
0.4	FROM_HAS_ULINE_NUMS	From: contains an underline and numbers/letters

SpamAssassin

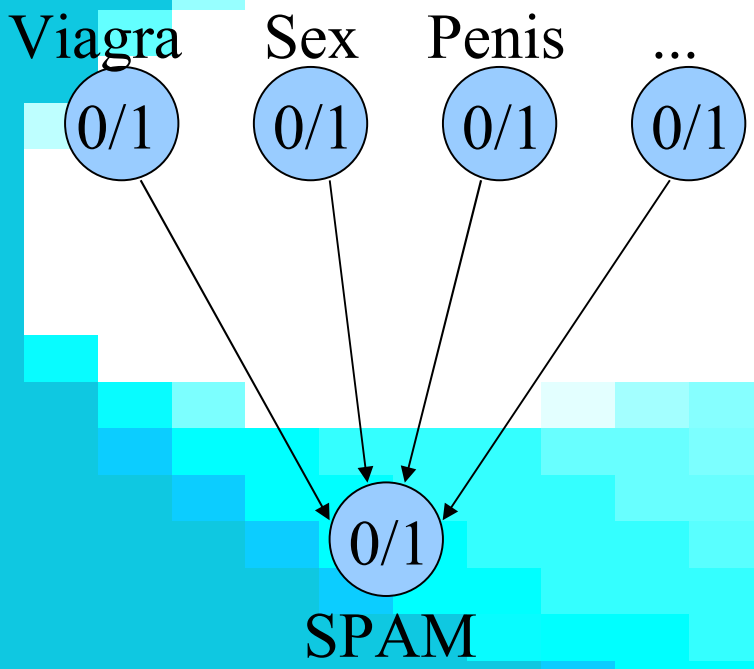
SpamAssassin solamente se encarga de marcar los e-mails. Añadiendo "*reports*" como el anterior o añadiendo ciertas cabeceras:

```
X-Spam-Flag: YES
X-Spam-Checker-Version: SpamAssassin 3.0.3 (2005-04-27) on TARTALO
X-Spam-Level: *********
X-Spam-Status: Yes, score=9.1 required=4.0 tests=DATE_IN_FUTURE_12_24,
        FROM_ENDS_IN_NUMS,FROM_HAS_ULINE_NUMS,HTML_60_70,
        HTML_FONT_LOW_CONTRAST,HTML_IMAGE_ONLY_12,HTML_MESSAGE,MIME_HTML_ONLY,
        MSGID_FROM_MTA_ID,NORMAL_HTTP_TO_IP,WEIRD_PORT autolearn=no
        version=3.0.3
```

Deberá ser por tanto el MTA u otro software quien se encargue de borrarlos en base al número de puntos sacados, si es lo que pretendemos.

SpamAssa ssin

Redes Bayesianas de SpamAssassin => APRENDIZAJE



Prob(SPAM=1|V=1,S=0,P=1)=0

sa-learn mail SPAM=1

Prob(SPAM=1|V=1,S=0,P=1)=1

SpamAssassin

Plugins interesantes de SpamAssassin:

- *BayesStore* : diferentes formas de guardar las bases de datos bayesianas (MySQL, pgsql, db...)
- *RelayCheck* : comprueba de qué países son los servidores por los que ha pasado el email.
- *URIDNSBL*: listas negras para los dominios de las URLs que aparezcan en el email.
- *FuzzyOCR* : "lector" de imágenes contra emails con solo .gifs adjuntos.
- *DCC, Razor, Pyzor*...etc

DCC, Pyzor, R azor

DCC, Pyzor y Razor son 3 herramientas colaborativas de identificación de mensajes de SPAM.

Su funcionamiento se basa en HASHes MD5 de cada mensaje que son comprobados con una base de datos pública de HASHes ya conocidos como SPAM.

Se integran con SpamAssassin, de tal forma que cuando un mensaje es encontrado en la BD, se le asigna una serie de puntos.

Disponen de herramientas para reportar mensajes.

Falsificación del remitente

Aparte de los programas del estilo de SpamAssassin (Dspam, bogofilter...etc), existen nuevos sistemas de detección de SPAM en base a la falsificación del FROM desde el cuál llega un determinado e-mail.

Los más conocidos son SPF y DomainKeys y ambos usan el sistema DNS para tal cometido.

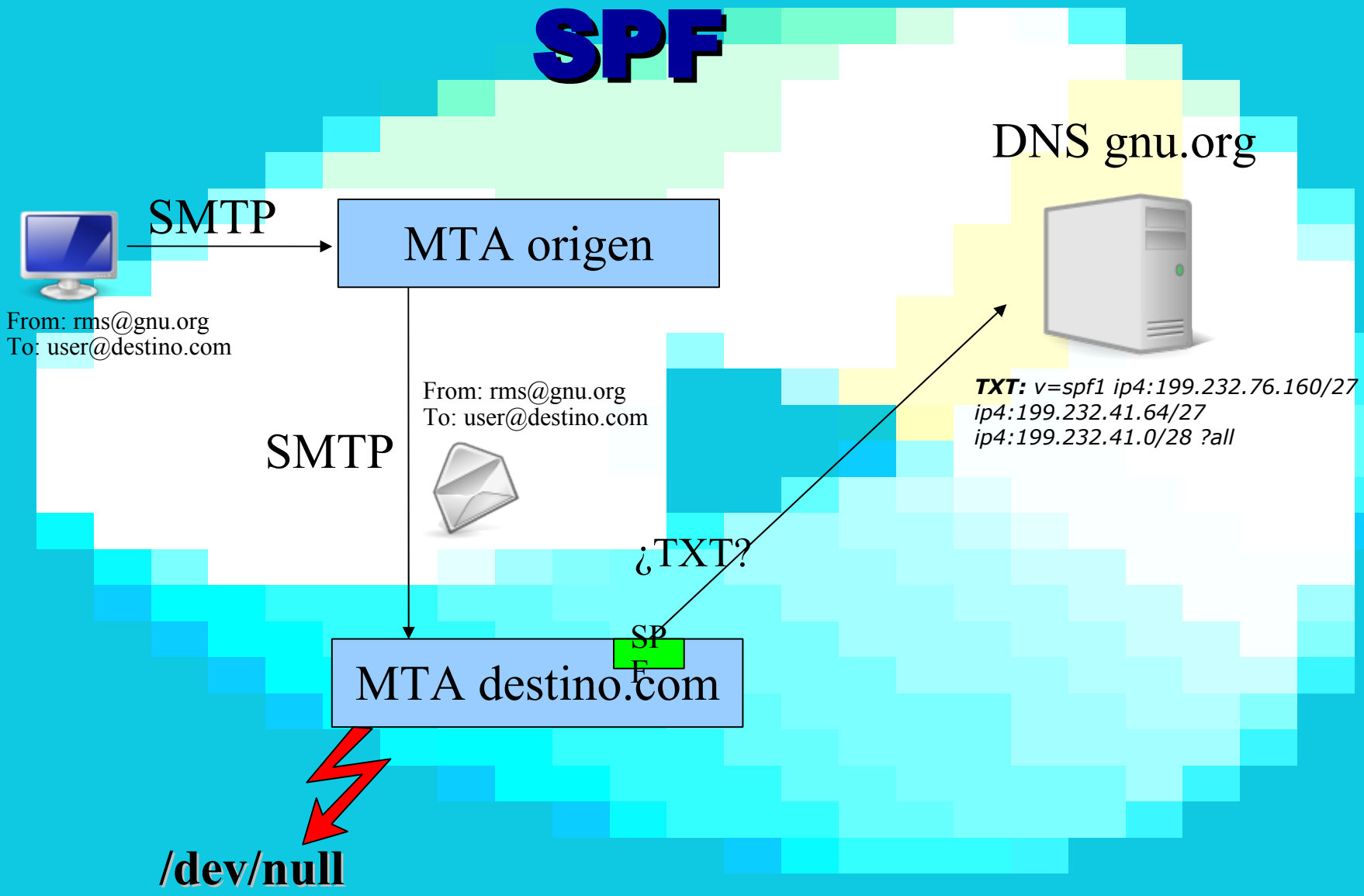
SPF

SPF – Sender Policy Framework.
Registro TXT del dominio + agente SPF en el MTA destino.
Permite la detección de falsificación de direcciones del <MAIL FROM>.

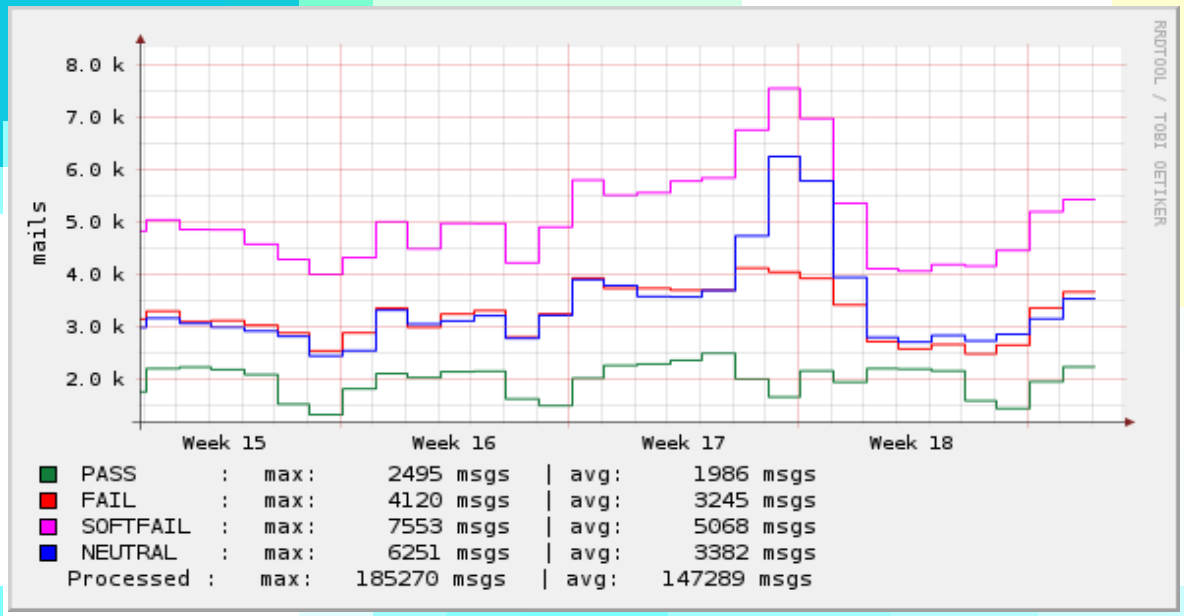
En el registro TXT del DNS del dominio se publican las direcciones IP de los MTAs que están permitidos enviar correo con dirección origen una de dicho dominio (@dominio).
El MTA receptor, consultará el registro para ver si la IP origen está en las IPs permitidas.

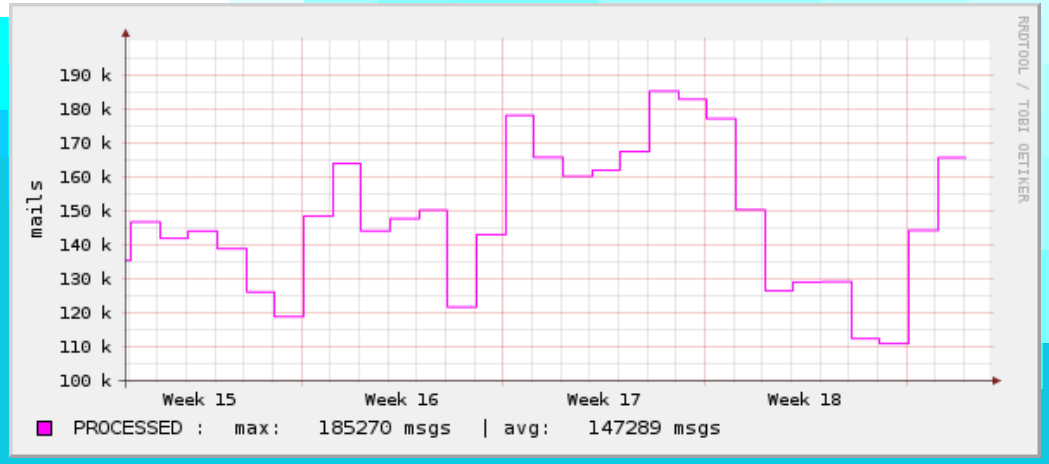
Por ejemplo:
$ dig txt +short gnu.org
"v=spf1 ip4:199.232.76.160/27 ip4:199.232.41.64/27 ip4:199.232.41.0/28 ?all"

SPF


DNS gnu.org
SMTP
MTA origen
From: rms@gnu.org
To: user@destino.com
From: rms@gnu.org
To: user@destino.com
SMTP
TXT: v=spf1 ip4:199.232.76.160/27
ip4:199.232.41.64/27
ip4:199.232.41.0/28 ?all
¿TXT?
SP
F
MTA destino.com
/dev/null

SPF


8.0 k
7.0 k
6.0 k
5.0 k
4.0 k
3.0 k
2.0 k
mails
Week 15
Week 16
Week 17
Week 18
RRDTOOL / TOBI OETIKER
PASS : max: 2495 msgs | avg: 1986 msgs
FAIL : max: 4120 msgs | avg: 3245 msgs
SOFTFAIL : max: 7553 msgs | avg: 5068 msgs
NEUTRAL : max: 6251 msgs | avg: 3382 msgs
Processed : max: 185270 msgs | avg: 147289 msgs


190 k
180 k
170 k
160 k
150 k
140 k
130 k
120 k
110 k
100 k
mails
Week 15
Week 16
Week 17
Week 18
RRDTOOL / TOBI OETIKER
PROCESSED : max: 185270 msgs | avg: 147289 msgs

DomainKeys

DomainKeys es una idea desarrollada por Yahoo para detectar las falsificaciones de From.

Usa claves públicas/privadas para certificar el origen de un e-mail a través de DNS.

Un servidor, crea dos claves, la pública la publica en un registro TXT de su DNS y la privada la usa para firmar los mensajes añadiendo el resultado en una cabecera.

El servidor destino, consultará la clave pública y chequeará que se corresponde con la clave que ha firmado el mensaje.

DomainKeys

El propio Yahoo y Google ya lo usan:

$host -t TXT beta._domainkey.gmail.com
beta._domainkey.gmail.com text "t=y\; k=rsa\;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC69TURXN3oNfz+G/m3g5rt4P6
nsKmVgU1D6cw2X6BnxKJNlQKm10f8tMx6P6bN7juTR1BeD8ubaGqtzm2rWK4LiMJqho
QcwQziGbK1zp/MkdXZEWMCflLY6oUITrivK7JNOLXtZbdxJG2y/RAHGswKKyVhSP9niRsZ
F/IBr5p8uQIDAQAB"

Como desventajas, este método sobrecarga bastante el trabajo del MTA así como las peticiones DNS que se realizan.

A partir de DomainKeys y a un acuerdo con Cisco, nace DKIM (DomainKeys Identified Mail), que parece va a sustituir al primero.

GreyLists

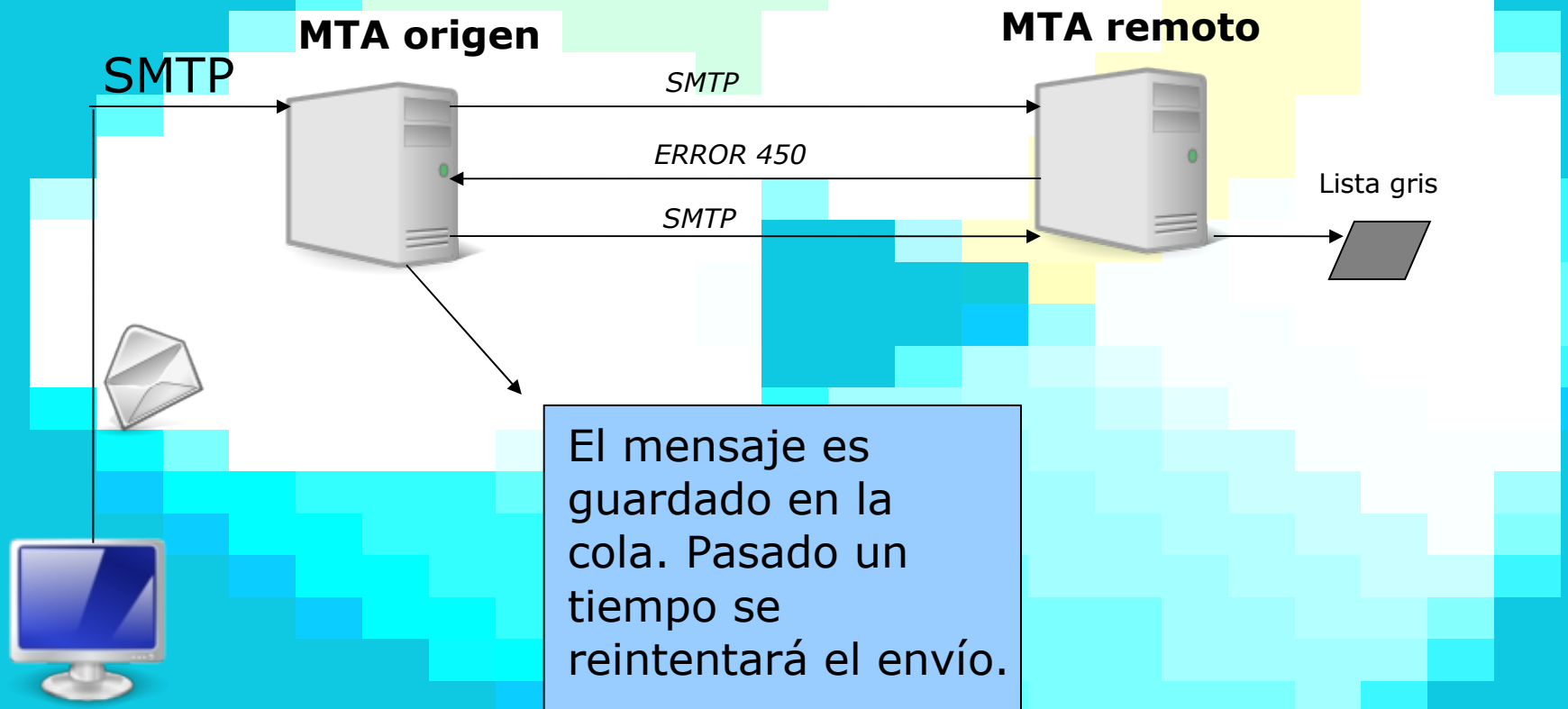
La "técnica" de **GreyListing** consiste en una mezcla entre listas negras y listas blancas.

La primera vez que se recibe un email, el MTA devuelve un error temporal 4XX, de tal forma, que si el MTA origen sigue el RFC, deberá de volver a intentar la entrega del mensaje pasados X minutos. Cuando se reintenta el envío, se deja pasar y la IP se mete en una lista blanca.

Página: *http://projects.puremagic.com/greylisting/*

Necesidad de instalar un agente en el MTA que se encargue de gestionar los errores.

GreyLists


MTA origen
MTA remoto
SMTP
SMTP
ERROR 450
SMTP
Lista gris
El mensaje es guardado en la cola. Pasado un tiempo se reintentará el envío.

GreyLists

El MTA origen recibiría un mensaje como:

*450 <******@origen.com>: Recipient address rejected: Greylisted for 5 minutes*

Pasado el tiempo de reintento del MTA origen, se reenviará el mensaje, y si han pasado 5 minutos (en este caso) será finalmente entregado.

Muchos spammers no usan un MTA para enviar mensajes, sino un agente SMTP que entrega directamente el mensaje al MTA destino, por lo que con esto evitaríamos muchos mensajes.

Problemas: retraso en entregas, servidores mal configurados...

Anti-VIRUS

Otra de las amenazas del correo electrónico son los virus, gusanos...etc que se transmiten vía e-mail.

Mucho consumo de recursos al analizar adjuntos grandes.

Prevenir que ciertos correos pasen al antivirus, bloqueando extensiones peligrosas (.exe, .scr, .pif, .com...) y evitando que el antivirus se ejecute para ellos.

Uno de los más usados es ClamAV (www.clamav.net).

Pasarelas de correo

Para la mejor integración del propio MTA con los antivirus, sistemas antispam y otra serie de filtros o analizadores, existen las pasarelas de correo.

Su tarea es recibir o coger el correo del MTA y gestionar todas las llamadas a los antivirus y antispam.

La pasarela puede ser capaz de eliminar correos directamente (por ejemplo, los que tengan un virus, tengan muchos puntos de spam...).

Los más conocidos:

- Amavis
- MailScanner

Amavisd-new

Amavisd-new es una pasarela creada a partir del antiguo Amavis.
Página: *http://www.ijs.si/software/amavisd/*

Escrito en PERL.
Interfaz entre el MTA y los antivirus, sistemas antispam...

Funciona de tal forma, que el MTA entrega al correo al puerto TCP:10024 donde escucha amavisd-new. Cuando éste termina de hacerle los chequeos y pasarlo por los analizadores, se devuelve al puerto TCP:10025 del MTA.

Debemos de tener por tanto, dos demonios smptd corriendo, uno para aceptar la conexiones externas SMTP y otro para las conexiones de Amavisd-new.

MailScanner

MailScanner es un programa escrito en Perl por Julian Field.
Página: *www.mailscanner.info*

Se trata de un demonio que va analizando los mensajes que coge de la cola de entrada del MTA. Una vez analizados, los deposita en la cola de salida del MTA.

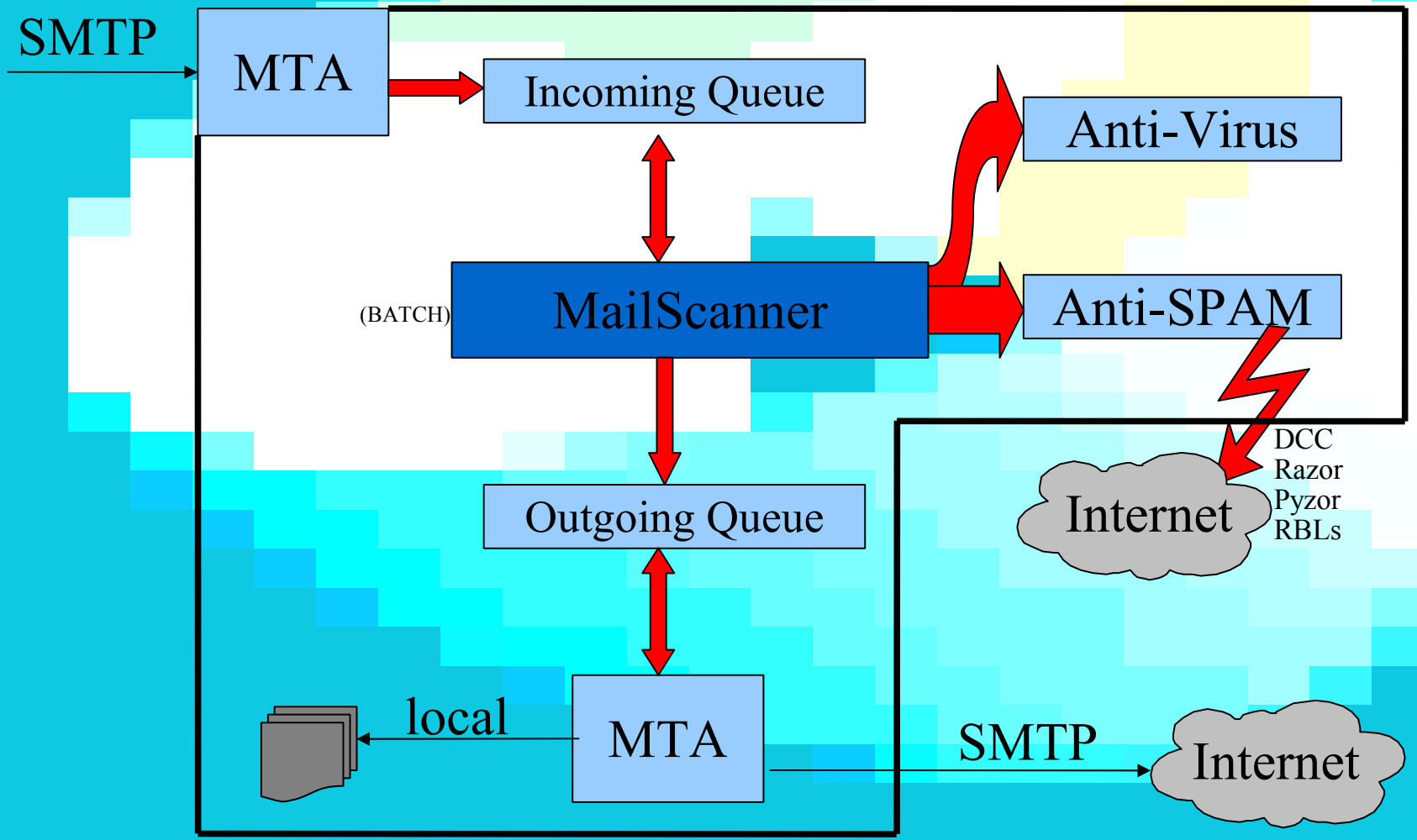
MailScanner comprobará el mensaje con reglas de filtrado de extensiones de archivos, listas negras, analizadores antispam, antivirus...etc

MailScanner

Las características que tiene MailScanner son:

- Interfaz con SpamAssassin (y otros)
- Interfaz con antivirus
- Poner en cuarentena virus, spam etc...
- Diferentes acciones dependiendo de los puntos del SA
- Chequea extensiones de archivos en busca de dobles extensiones, ext. peligrosas (exe,scr,pif...)...
- Anti-phishing
- Chequea mails con ataques HTML, Scripts...
- Reportes a destinatarios, emisores, admins...
- Añadido de cabeceras personalizadas
- Listas negras/blancas por usuario, dominio...
- Caché del resultado del SpamAssassin
- Casi toda directiva puede ser un archivo
- ...

MailScanner



MailWatch

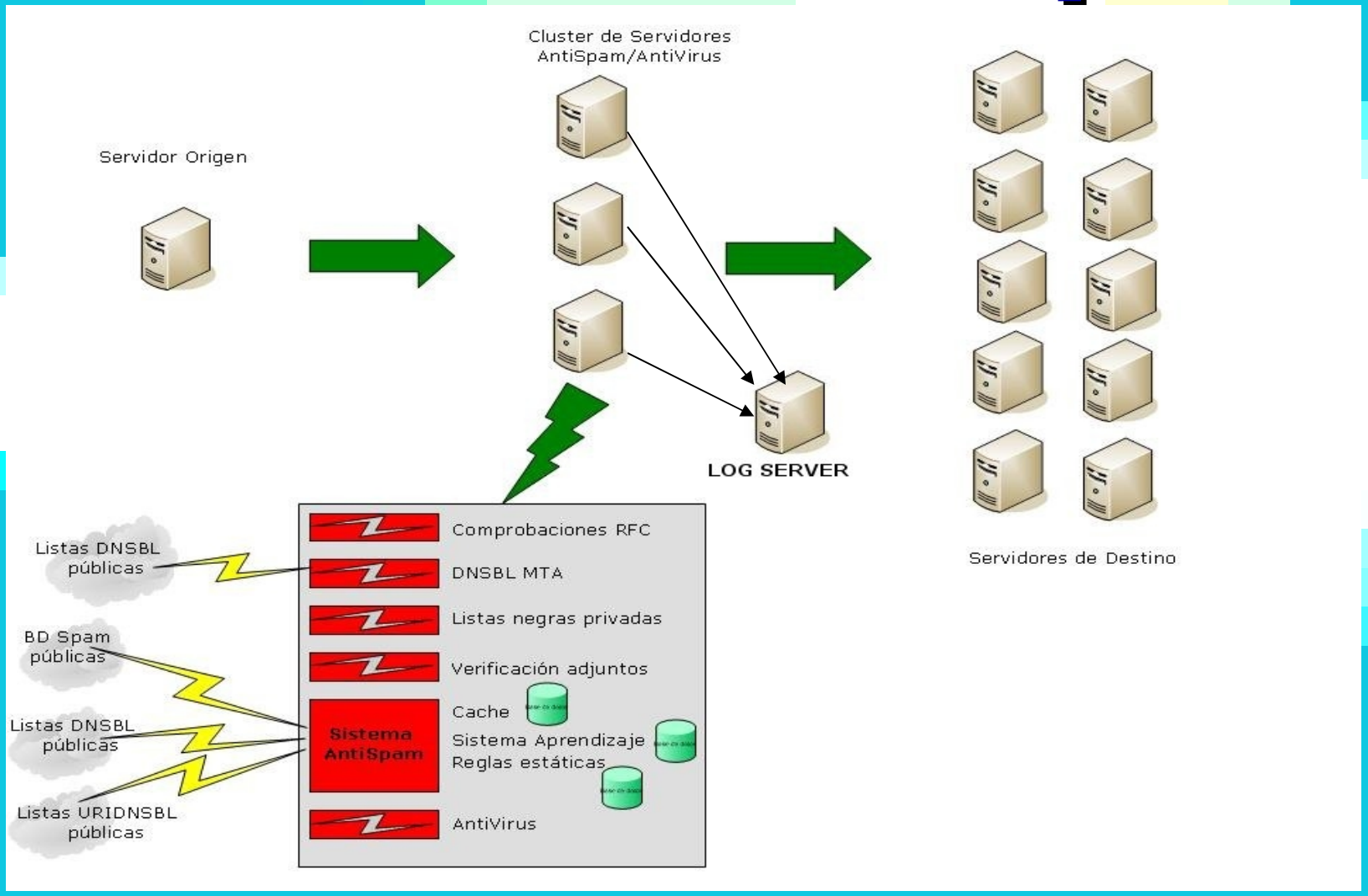
MailWatch es una interfaz web que permite, entre otras cosas:

- Liberar de cuarentena mensajes
- Estadísticas de virus, relays, spam...etc
- Listas blancas/negras en MySQL
- Acceso por usuario/admin de dominio/admin total
- Configuraciones distribuidas vía PHP-XMLRPC

Se configura indicando en la configuración de MailScanner, que por cada mail que procese haga una INSERT en una base de datos. Posteriormente, mediante PHP, con MailWatch se acceden a todos esos emails.

Sitio web: *http://mailwatch.sf.net*

Solución completa



Recomendaciones

Recomendaciones de postmaster a postmaster ;-)

- Configurar correctamente el registro A del hostname
- Configurar correctamente el registro PTR
- Configurar correctamente el registro A del PTR
- Configurar correctamente los MX (=registro A)
- Autenticar toda clase de envío a través del servidor
- Leer abuse@ y postmaster@ para posibles notificaciones
- Revisar *logs* cada cierto tiempo
- Monitorizar el estado de la cola
- Controlar los *mailings* de los usuarios
- ...

Futuro

¿Hacia dónde avanza el correo electrónico y la lucha contra el spam?

- Más inversión en hardware para el análisis de correo
- Acuerdos mínimos entre operadores e ISPs
- Evitar la salida del spam desde el punto más cercano al punto de emisión (ISPs de conectividad)
- Solo aceptar correo de MTAs que cumplan RFCs
- Integración de las últimas tecnologías

Enlaces de interés

http://www.rediris.es/mail/aupREDIRIS.es.html
http://www.rediris.es/abuses/
www.rbls.org
www.spamhaus.org
www.spamcop.net
postmaster.msn.com
abuse.hostalia.com

Álvaro Marín Illera
alvaro@hostalia.com