SPF:

Luchando contra el SPAM

Toni de la Fuente Diaz [blyx.com]

12 Septiembre'04

Congreso NoConName

Palma de Mallorca

SPF: Luchando contra el SPAM

Toni dlF. Diaz [blyx.com] – Septiembre 2004

Contenido:

- Introducción
- Funcionamiento del correo electrónico
- Falsificación de correo electrónico
- SPF (Sender Policy Framework):
  - Concepto y características
  - Anatomía
  - Sintaxis
  - Ejemplos y análisis
  - Integración con MTAs
  - Caso práctico (qmail)
  - Demostración

¿Preguntas?
:P


BOING!
SPAM!
DO YOU NEED a BIGGER PENIS?
...ACTUALLY I JUST WANT TO READ MY E-MAIL.

SPF: Luchando contra el SPAM

Toni dlF. Diaz [blyx.com] – Septiembre 2004

Introducción:

- **¿Que es SPAM?**
  - Spam es correo no deseado y no solicitado.
  - Más del 80% de los correos electrónicos recibidos por cualquier ISP al día son spam.
- **¿Por qué los Spammers hacen SPAM?**
  - Por dinero.
  - Ahorro en anunciar ciertos productos.
  - Gusanos con propio motor SMTP
  - ...
- **Coste del SPAM:**
  - Pérdida de productividad (4.4s/mensaje) y de recursos del servidor (ancho de banda y almacenamiento).

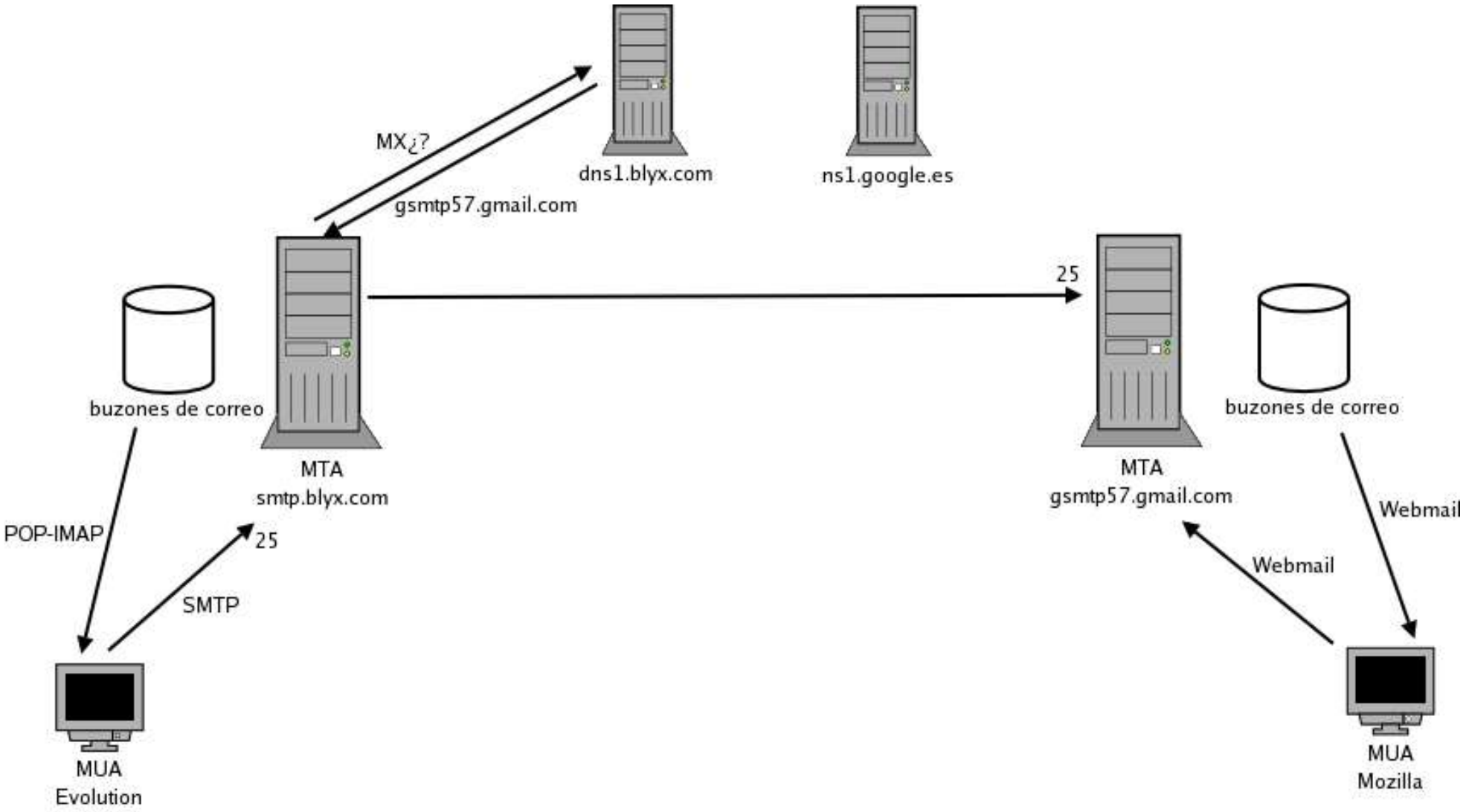
Métodos utilizados para acabar con el SPAM:

- SpamAssassin
- BlackLists basadas en DNS
- WhiteLists
- Filtros “Ballesianos”: Teorema de Bayes
- Filtros en los clientes
- Control de ancho de banda
- Uso intensivo del cortafuegos (trafico saliente puerto 25/TCP).

SPF: Luchando contra el SPAM

Toni dlF. Diaz [blyx.com] – Septiembre 2004

¿Cómo funciona el correo electrónico?



Estructura de un mensaje de correo electronico:

Envelope:

mail from: correo@origen.com (Return-Path)
rcpt to: destinatario@destino.com (Delivered-To)

Header:

From: correo@origen.com
Subject: Asunto
To: destinatario@destino.com
Date:
Reply-To:
Message-ID:
ETC...

Una sesión especial:

```
$ telnet smtp.dominio.com 25
Trying 211.35.214.2...
Connected to smtp.dominio.com.
Escape character is '^]'.
220 smtp.dominio.com ESMTP
mail from: pepe@lospepes.com
250 ok
rcpt to: toni@dominio.com
250 ok
data
354 go ahead
From: yomismo@oleoleyole.es
Subject: ayyyy lereee lereee
To: toniblyx@loqueyoquiera.com

Adioooooooosss!!!


.
250 ok 1088708435 qp 3884
quit
221 smtp.dominio.com
Connection closed by foreign host.
```

Resultado, fuente del mensaje recibido:

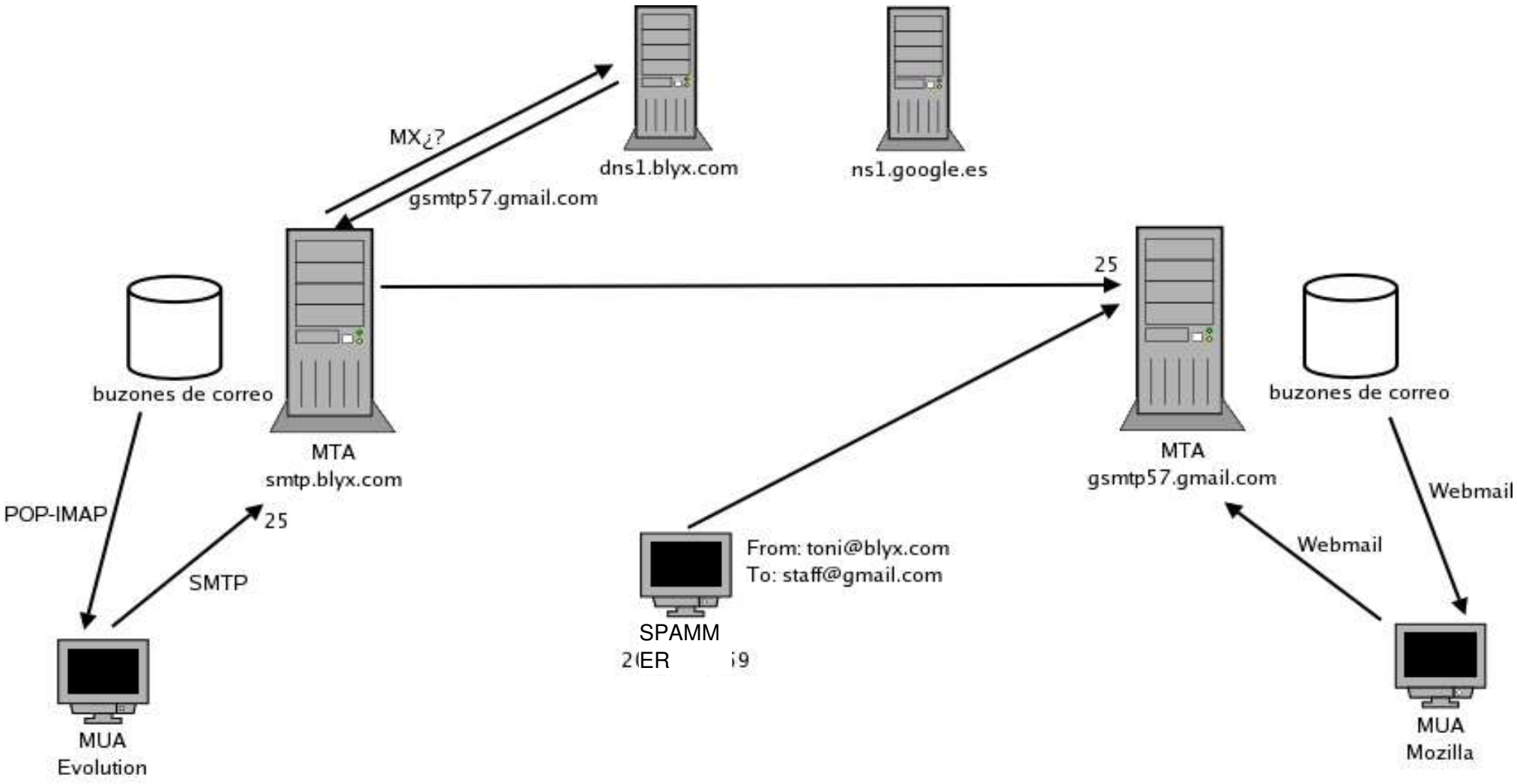
```
Return-Path: <pepe@lospepes.com>
Delivered-To: toni@dominio.com

Received: (qmail 3884 invoked from network); 1 Jul 2004
18:59:20 -0000
Received: from unknown (231.254.21.33) by 0 with SMTP; 1 Jul
2004 18:59:20 -0000
From: yomismo@oleoleyole.es
Subject: ayyyy lereee lereee
To: toniblyx@loqueyoquiera.com
X-Evolution-Source: pop://toni%40diminio.com@pop3.dominio.com
Date: Thu, 01 Jul 2004 20:57:36 +0200
Message-Id: <1088708256.2240.177.camel@flame>
Mime-Version: 1.0
Adioooooooosss!!!
```

¿Quien recibe el correo? toni@dominio.com Aunque aparecerá en el cliente toniblyx@loqueyoquiera.com procedente de yomismo@oleoleyole.es

SPF: Luchando contra el SPAM

Toni dlF. Diaz [blyx.com] – Septiembre 2004

Falsear direcciones de correo es fácil:



SPF = Sender Policy Framework

- SPF (antes llamado **Sender Permitted From**) permite a los servidores de correo identificar y bloquear envíos falsificados haciendo una simple consulta al DNS sobre el registro TXT del dominio origen.
- Gran parte de las empresas y asociaciones ya publican sus registros SPF como Google, AOL, gnu.org, oreilly.com, wanadoo.es, etc.
- Cómo se si mi proveedor publica SPF?
  `host -t txt ya.com`

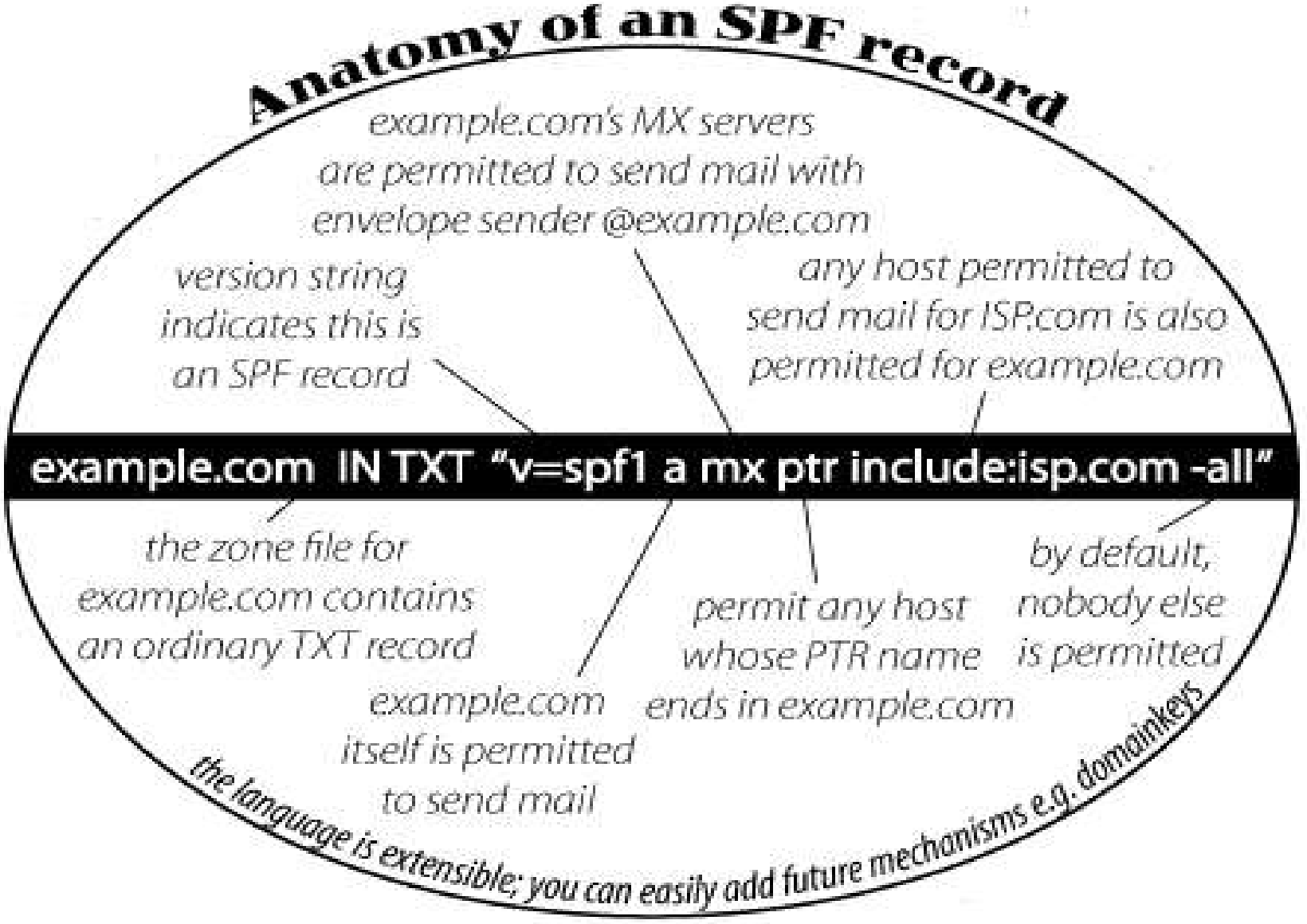
Basado en:
RMX: Reverse Mail eXchanger
DMP: Designated Mailers Protocol

Características para la implementación de SPF

- Implica a los protocolos **DNS** (sólo TXT) y **SMTP** (necesita modificación).
- La adopción de SPF puede ser asimétrica, no es necesario que otros utilicen SPF.
- Uso de SMTP Autenticado muy recomendable. Usuarios viajeros con MTA propios, etc.
- Hay otras iniciativas como M$ Caller-ID o M$ SenderID. SPF es compatible.
- Web del proyecto: http://spf.pobox.com/

RFCs:
http://spf.pobox.com/spf-draft-200406.txt
http://spf.pobox.com/draft-ietf-marid-protocol-00.txt

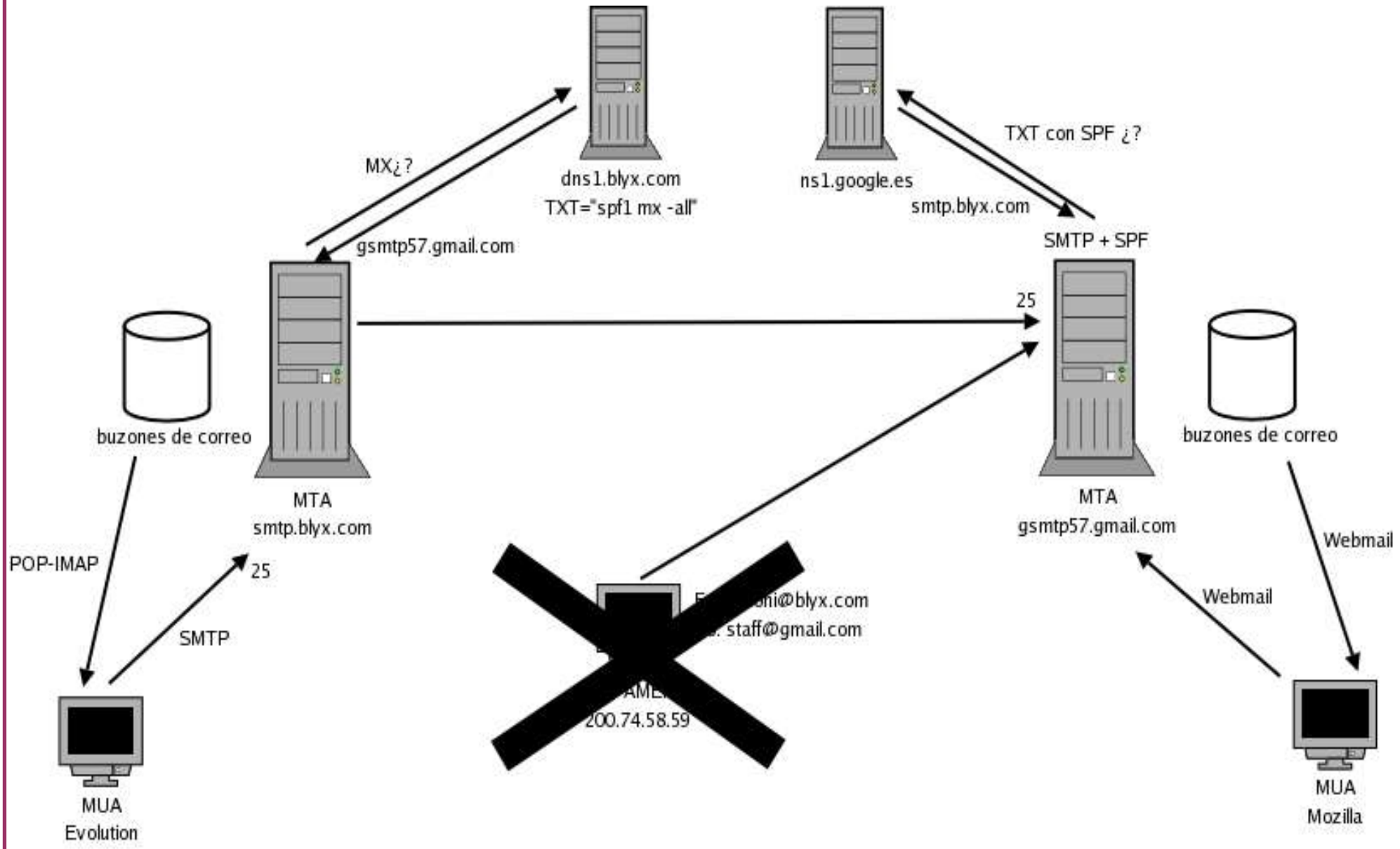
Anatomía de un registro SPF:



SPF: Luchando contra el SPAM

Toni dlF. Diaz [blyx.com] – Septiembre 2004

Con SPF:



Sintaxis http://spf.pobox.com/mechanisms.html

Ejemplo:

Sólo los MX de blyx.com pueden enviar correos de @blyx.com:

En BIND:

```
blyx.com. IN TXT "v=spf1 mx -all"
```

En tinydns/djbdns:

```
'blyx.com:v=spf1 mx -all:600
```

NOTA: `all` es equivalente a `+all`

Existen asistentes para configuración de la zona TXT para SPF:
http://spf.pobox.com/wizard.html
http://old.spf.infinitepenguins.net/create.php

SPF: Luchando contra el SPAM

Toni dlF. Diaz [blyx.com] – Septiembre 2004

Prefijos:

- fail
~ softfail
+ pass
? neutral

Operadores (mechanism):

v = versión de SPF, actualmente es spf1
a = registros A en DNS
mx = registros MX en DNS
ptr = registros PTR (resolución inversa) en DNS
ip4/ip6 = declaración de ip o rangos Ipv4 o Ipv6
all = redes e IP restantes
include = comprueba registro SPF de otro dominio y pasa al siguiente operador
exist = si existen registros SPF de otro dominio

Modificadores:

exp = (explanation) respuesta en caso de rechazo (pj. explicar como utilizar smtp-auth)
redirect = consulta el registro SPF de otro dominio

Otros ejemplos:

Si blyx.com sólo fuera un dominio de web y no envía correo:

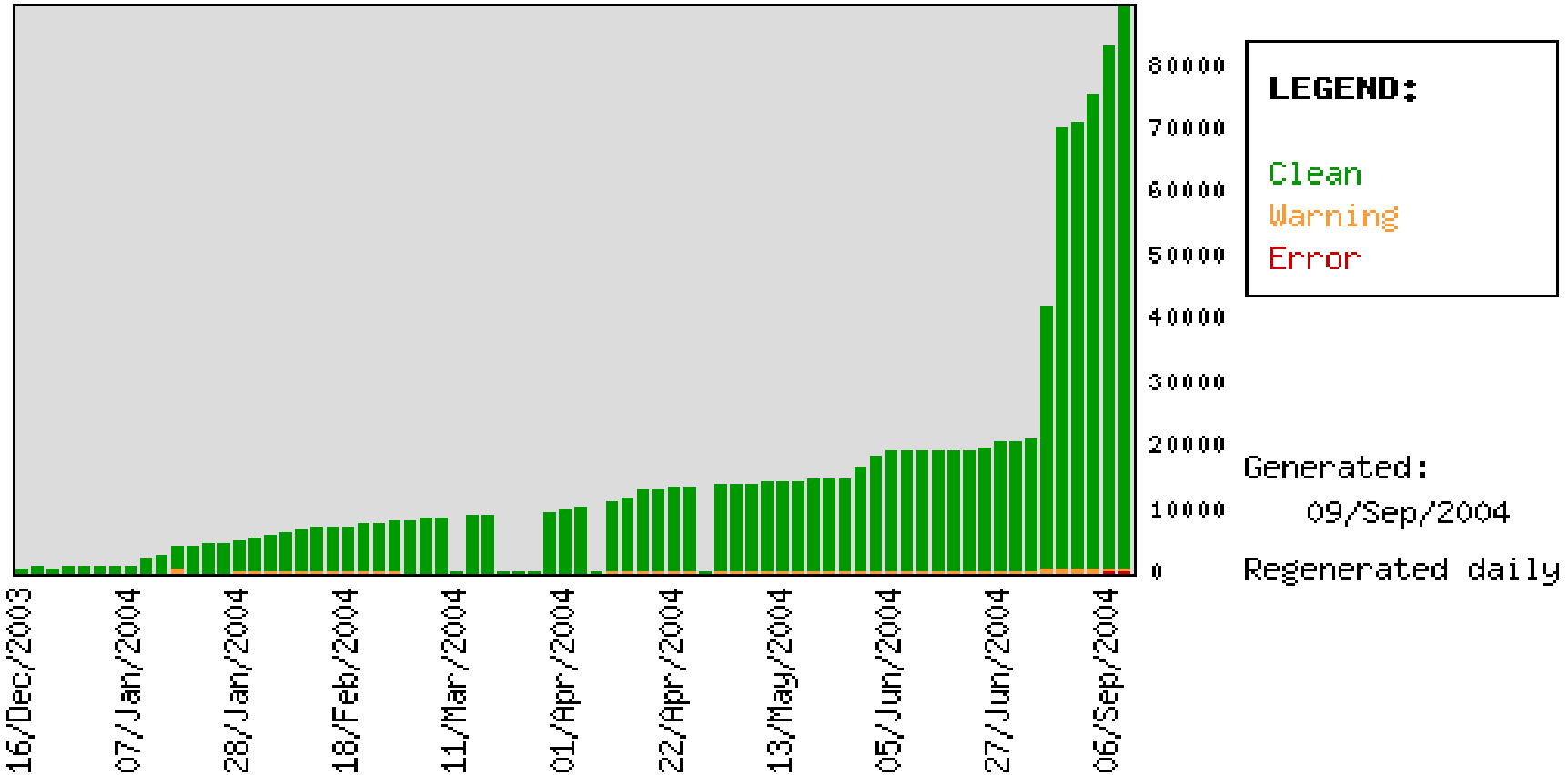
```
blyx.com. TXT "v=spf1 -all"
```

Informe de los fails por IP (no aparece en spf v2):

```
“v=spf1 mx report=toni@blyx.com -all"
```

Registro SPF y comprobación:

http://spf.infinitepenguins.net/register.php
http://spf.infinitepenguins.net/earlyadopters.php



Comprobación con libspf: (www.libspf.org)

Prueba satisfactoria:

```
# spfquery -i 212.163.0.2 -s toni@blyx.com -h blyx.com
pass
policy result: (pass) from rule (ip4:212.163.0.0/26)
(null)
```

Prueba fallida:

```
# spfquery -i 212.163.0.134 -s toni@blyx.com -h blyx.com
fail
policy result: (fail) from rule (-all)
See
http://spf.pobox.com/why.html?sender=toni@blyx.com&ip=212.163
.0.134&receiver=spfquery
```

SPF: Luchando contra el SPAM

Toni dlF. Diaz [blyx.com] – Septiembre 2004

Comprobación:

captura-ethereal-query-response-spf.dump - Ethereal

File Edit View Go Capture Analyze Statistics Help

Filter: Expression... Limpiar Aplicar

No.	Time	Source	Destination	Protocol	Info
15	49.22719	212.163.145.141	212.163.0.2	DNS	Standard query A ftp.dulug.duke.edu
16	49.43779	212.163.0.2	212.163.145.141	DNS	Standard query response CNAME mirror.dulug.duke.edu A 15
17	58.52948	212.163.145.141	212.163.0.2	DNS	Standard query AAAA ftp.dulug.duke.edu
18	58.69173	212.163.0.2	212.163.145.141	DNS	Standard query response CNAME mirror.dulug.duke.edu
19	58.69206	212.163.145.141	212.163.0.2	DNS	Standard query A ftp.dulug.duke.edu
20	58.75611	212.163.0.2	212.163.145.141	DNS	Standard query response CNAME mirror.dulug.duke.edu A 15
21	69.23333	212.163.145.141	212.163.0.13	DNS	Standard query CNAME blyx.com
22	69.50102	212.163.0.13	212.163.145.141	DNS	Standard query response
23	69.50132	212.163.145.141	212.163.0.13	DNS	Standard query CNAME blyx.com.blyx.com
24	69.71061	212.163.0.13	212.163.145.141	DNS	Standard query response, No such name
25	69.71088	212.163.145.141	212.163.0.13	DNS	Standard query TXT blyx.com
26	69.86057	212.163.0.13	212.163.145.141	DNS	Standard query response TXT
27	72.78089	212.163.145.141	212.163.0.2	DNS	Standard query AAAA ftp.dulug.duke.edu
28	72.94391	212.163.0.2	212.163.145.141	DNS	Standard query response CNAME mirror.dulug.duke.edu
29	72.97846	212.163.145.141	212.163.0.2	DNS	Standard query A ftp.dulug.duke.edu
30	73.16348	212.163.0.2	212.163.145.141	DNS	Standard query response CNAME mirror.dulug.duke.edu A 15

```
▷ Flags: 0x8580 (Standard query response, No error)
  Questions: 1
  Answer RRs: 1
  Authority RRs: 1
  Additional RRs: 1
▷ Queries
▽ Answers
  ▽ blyx.com: type TXT, class inet
      Name: blyx.com
      Type: Text strings
      Class: inet
      Time to live: 1 day
      Data length: 31
      Text: v=spf1 ip4:212.163.0.0/26 -all
```

```
0040  00 10 00 01 c0 0c 00 10  00 01 00 01 51 80 00 1f   ........ ....Q...
0050  1e 76 3d 73 70 66 31 20  69 70 34 3a 32 31 32 2e   .v=spf1  ip4:212.
0060  31 36 33 2e 30 2e 30 2f  32 36 20 2d 61 6c 6c c0   163.0.0/ 26 -all.
0070  0c 00 02 00 01 00 01 51  80 00 07 04 64 6e 73 31   .......Q ....dns1
0080  c0 0c c0 51 00 01 00 01  00 01 51 80 00 04 d4 a3   ...Q.... ..Q.....
```

P: 30 D: 30 M: 0

Análisis de algunos registros SPF:

AOL:

```
aol.com text
"v=spf1 ip4:152.163.225.0/24 ip4:205.188.139.0/24
ip4:205.188.144.0/24 ip4:205.188.156.0/23
ip4:205.188.159.0/24 ip4:64.12.136.0/23
ip4:64.12.138.0/24 ptr:mx.aol.com ?all"
```

Implementación interesante de SPF:

WANADOO:

```
wanadoo.es text
"v=spf1 +a:allow.spf.wanadoo.es ?all"
```

Ejecuta:

```
# nslookup allow.spf.wanadoo.es
```

Interesante ¿verdad?

Desventajas:

- Problemas con los reenvios de correo:

Solución: Protocolo SRS (Sender Rewriting Scheme) marcas de camino, MTA original: seguimiento de correo. http://www.libsrs2.org

- Usuarios móviles con MTA propios:

Solución: SMTP-AUTH

¿Qué hago en mi servidor SMTP?

Paquetes y parches disponibles para MTAs en:
http://spf.pobox.com/downloads.html

Mail::SPF::Query – Módulo de Perl que permite la implementación con Sendmail, paquetes RedHat, Fedora y Debian.

Postfix - http://spf.pobox.com/postfix-policyd.txt + Mail::SPF::Query

Sendmail-milter - http://spf.pobox.com/sendmail-milter-spf-1.41.pl

qmail - http://www.saout.de/misc/spf/

Exim - http://spf.pobox.com/exim4.spf.acl-2.09.txt

Courier - http://search.cpan.org/search?query=Courier::Filter::Module::SPF

http://www.libspf2.org/ - Librerias en C para Sendmail y Qmail

http://www.wayforward.net/spf/ - Librerias en Python

https://sourceforge.net/projects/spfjava/ - Librerias en Java

Caso práctico: ímplementación con qmail

1- Publicar los registros SPF en el dns:

Añadir en la zona /var/named/blyx.com.db:

```
blyx.com. IN TXT "v=spf1 mx -all"
```

2- Parchear, compilar, instalar:

Parche simple:

http://www.saout.de/misc/spf/qmail-spf-rc2.patch

Parche con soporte ldap, smtp-auth, tls:

http://www.saout.de/misc/spf/other/

3- Configurar qmail (/var/qmail/control):

- **spfbehavior:** valor ideal 3

*mas info:

```
# man 8 qmail-smtpd
```

spfbehavior: Comportamiento de nuestro MTA

Configura el comportamiento del MTA según las respuestas SPF obtenidas. El valor por defecto es 0 (off). Los valores son de 0 a 6:

0: Never do SPF lookups, don't create Received-SPF headers
1: Only create Received-SPF headers, never block
2: Use temporary errors when you have DNS lookup problems
3: Reject mails when SPF resolves to fail (deny)
4: Reject mails when SPF resolves to softfail
5: Reject mails when SPF resolves to neutral
6: Reject mails when SPF does not resolve to pass

Demostración:

En DNS: blyx.com text = "v=spf1 mx -all"

En MTA: /var/qmail/control/spfbehavior = 6

```
$ telnet smtp.blyx.com 25
Trying 213.14.251.3...
Connected to 213.14.251.3.
Escape character is '^]'.
220 smtp.blyx.com ESMTP
mail from: atacante@aol.com
250 ok
rcpt to: toni@blyx.com
550 See http://spf.pobox.com/why.html?sender=atacante%
40aol.com&ip=216.89.87.65&receiver=213.14.251.3 (#5.7.1)
quit
221 smtp.blyx.com
Connection closed by foreign host.
```

Captura del tráfico con tcpdump:

```
22:37:57.291209 smtp.blyx.com.32771 > chico.rediris.es.domain:  36152+ [1au] TXT? aol.com.
(36) (DF)
22:37:57.708396 chico.rediris.es.domain > smtp.blyx.com.32771:  36152* 1/4/5 TXT[|domain]
(DF)
```

Análisis de cabeceras:

Caso neutral ?all

```
Return-Path: <asdfdsf@aol.com>
Delivered-To: toni@blyx.com
Received: (qmail 21460 invoked by uid 508); 9 Sep 2004 15:48:51
-0000
Received: from unknown (HELO fcmx1.nostracom.com) (212.163.0.13) by
        pop.nostracom.com with SMTP; 9 Sep 2004 15:48:51 -0000
Received: (qmail 17947 invoked by uid 600); 9 Sep 2004 15:51:56
-0000
Received: from 182.red-80-24-243.pooles.rima-tde.net (80.24.243.182)
by212.163.0.13 with SMTP; 9 Sep 2004 15:51:56 -0000
Received-SPF: neutral (212.163.0.13: 80.24.243.182 is neither
permitted nor denied by SPF record at aol.com)
X-Evolution-Source: pop://toni%40blyx.com@mailbox1.nostracom.com/
From:
Date: Thu, 09 Sep 2004 17:47:46 +0200
Subject: No Subject
Message-Id: <1094744866.2772.496.camel@flame.nostracom.com>
Mime-Version: 1.0
```

Análisis de cabeceras:

Caso pass -all

```
Return-Path: <bo-bz0214fa94ddcqbh1mccmbv7qgpamb@b.info.redhat.com>
Delivered-To: toni@blyx.com
Received: (qmail 18251 invoked by uid 508); 8 Sep 2004 19:59:11 -0000
Received: from unknown (HELO fcmx1.nostracom.com) (212.163.0.13) by
pop.nostracom.com with SMTP; 8 Sep 2004 19:59:11 -0000
Received: (qmail 17466 invoked by uid 600); 8 Sep 2004 20:02:18 -0000
Received: from mta201.info.redhat.com (65.125.54.186) by 212.163.0.13
with SMTP; 8 Sep 2004 20:02:18 -0000
Received-SPF: pass (212.163.0.13: SPF record at b.info.redhat.com
designates 65.125.54.186 as permitted sender)
Date: Wed, 8 Sep 2004 20:04:12 -0000
Message-ID:
<bz0214fa94ddcqbh1mccmbv7qgpamb.187926463.2492@mta201.info.redhat.com>
List-Unsubscribe:
        <mailto:rm-0bz0214fa94ddcqbh1mccmbv7qgpamb@info.redhat.com>
From: "Red Hat" <redhat@info.redhat.com>
To: toni@blyx.com
Subject: Under the Brim | Red Hat | September 2004
```

Análisis de cabeceras:

Caso none sin SPF declarado

```
Return-Path: <fxksjis@iol.ie>
Delivered-To: toni@blyx.com
Received: (qmail 32142 invoked by uid 508); 3 Sep 2004 20:41:21 -00
Received: from unknown (HELO fcmx1.nostracom.com) (212.163.0.13) by
pop.nostracom.com with SMTP; 3 Sep 2004 20:41:21 -0000
Received: (qmail 21366 invoked by uid 600); 3 Sep 2004 20:44:29 000
Received: from 19.red-80-26-109.pooles.rima-tde.net (HELO iol.ie)
(80.26.109.19) by 212.163.0.13 with SMTP; 3 Sep 2004 20:44:29 -0000
Received-SPF: none (212.163.0.13: domain at noconname.org does not
designate permitted sender hosts)
Received: from peron (hugo.iol.ie [192.168.0.2]) by iol.ie(Postfix)
with SMTP id 8521D23 for <toni@blyx.com>; Fri,  3 Sep 2004 22:49:43
+0200 (CEST)
Message-ID: <008d01c491f6$f830b320$0200a8c0@peron>
From: <fxksjis@iol.ie>
To: "Toni dlF. Diaz" <toni@blyx.com>
```

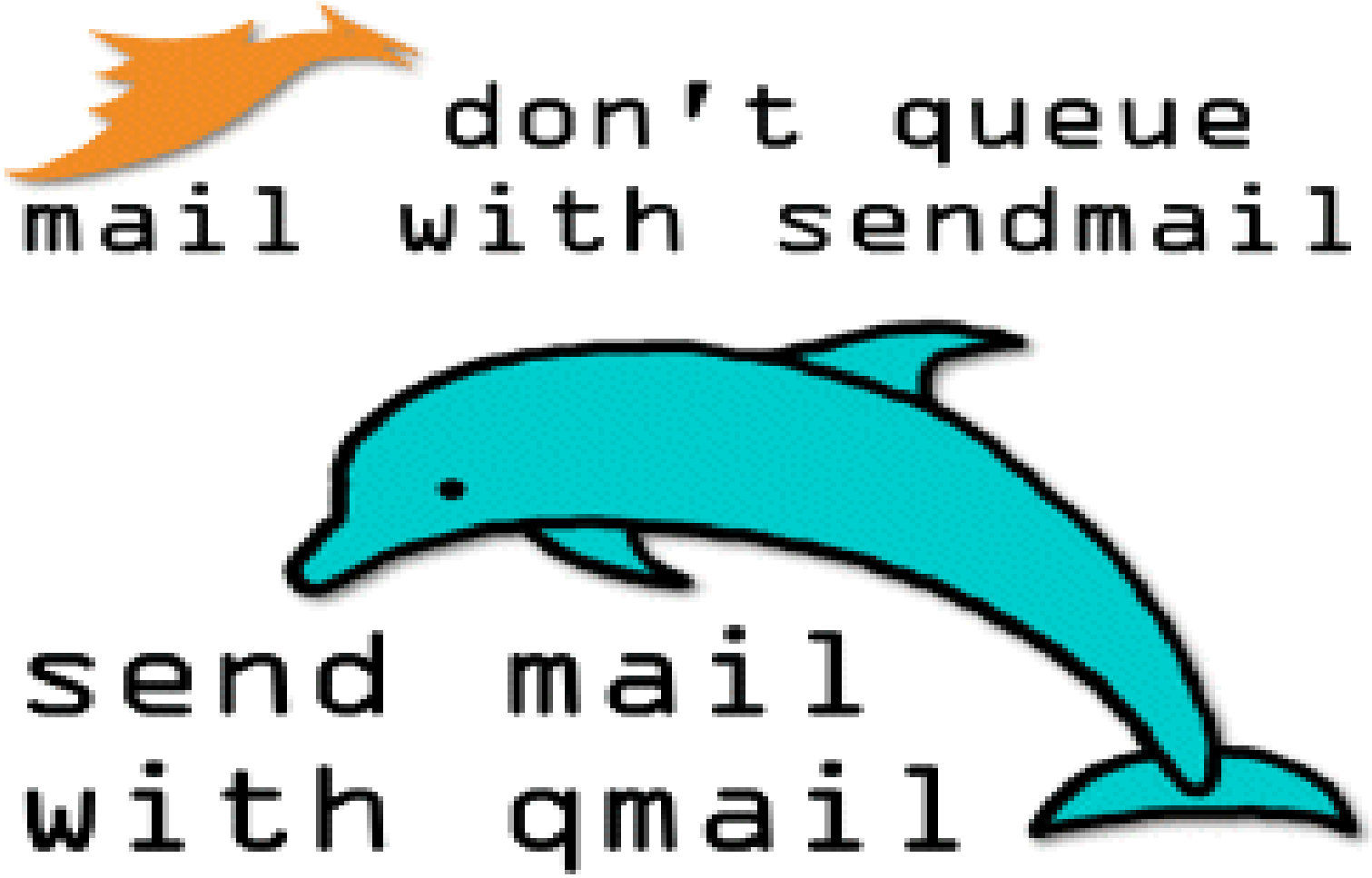
SPF: Luchando contra el SPAM

Toni dlF. Diaz [blyx.com] – Septiembre 2004

Apuntes:

Tipo	Nombre	Función
SOA	Start Of Authority	Define una zona representativa del DNS
Zona		
NS	Name Server	Identifica los servidores de zona, delega subdominios
A	Dirección IPv4	Traducción de nombre a dirección
AAAA	Dirección IPv6 original	Actualmente obsoleto
Básicos		
A6	Dirección IPv6	Traducción de nombre a dirección IPv6
PTR	Puntero	Traducción de dirección a nombre
DNAME	Redirección	Redirección para las resoluciones inversas IPv6
MX	Mail eXchanger	Controla el enrutado del correo
KEY	Clave pública	Clave pública para un nombre de DNS
Seguridad		
NXT	Next	Se usa junto a DNSSEC para las respuestas negativas
SIG	Signature	Zona autenticada/firmada
CNAME	Canonical Name	Nicks o alias para un dominio
LOC	Localización	Localización geográfica y extensión
Opcionales		
RP	Persona responsable	Especifica la persona de contacto de cada host
SRV	Servicios	Proporciona la localización de servicios conocidos
TXT	Texto	Comentarios o información sin cifrar

Securizar el Servidor DNS Bind:
http://www.ziries.com/contenido.php?opcion=articulo-bind



¡¡¡GRACIAS!!!