

Análisis de Mecanismos AntiSPAM sobre IPv6

LACNIC XIII, Curaçao, Mayo de 2010

¹Universidad Tecnológica Nacional, Facultad Regional Bahía Blanca

²CONICET, CCT Bahía Blanca

Santiago Aggio

Contenido I

1 Introducción

- Acerca de SPAM
- SPAM sobre IPv6
- Migración del Servidor de Email
- MTA's con soporte IPv6
- SMTP en ambientes dual-stack IPv4/IPv6
- RIPE Labs

Contenido II

2 Mecanismos AntiSPAM

- Descripción de Mecanismos AntiSPAM
- RBL
- SPF
- Greylisting
- Resolución del nombre/IP del cliente
- Sender Address Verification SAV
- Recipient Address Verification RAV
- Reglas Empíricas

Contenido III

- 3 Experiencias
 - Conectividad IPv6
 - Registros DNS
 - Registros MX
 - SPF
 - Greylist
- 4 Conclusiones
- 5 Trabajo a Futuro
- 6 FIN

Acerca de SPAM

- De cada 4 mensajes recibidos por lo menos 3 son SPAM
- Implementar políticas AntiSPAM generan un alto costo de infraestructura de red y de recursos humanos en un ISP
- Las políticas antispam no satisfacen lo requerimientos a nivel de **capa 8 !!!**
- El usuario se queja porque recibe SPAM.
¿No están haciendo nada?
- El usuario se queja porque recibe sólo 5 mensajes por día.
Antes recibía más de 20 !!!!. ¿Están filtrando demasiado?
- El usuario no habilita su firewall, no actualiza su antivirus y no advierte las actualizaciones de seguridad de su SO

SPAM sobre IPv6

¿Los mecanismos AntiSPAM que se utilizan en IPv4 funcionan igual bajo IPv6?

MTA's con soporte IPv6

Las últimas versiones de los MTA's de código abierto más utilizados soportan IPv6

- Sendmail
- Postfix
- Exim
- Qmail

SMTP en ambientes dual-stack IPv4/IPv6

- RFC 3974 (Enero 2005)
- Un mensaje puede atravesar varios relays antes de llegar a destino.
- La entrega de mensajes es más complejo que otros servicios de internet que utilizan una comunicación directa IP
- Se requiere de configuración en los registros MX del DNS para una correcta operación IPv4/IPv6 dual-stack
- Se plantea un algoritmo de 9 pasos para el emisor SMTP en ambientes dual-stack
- Para un MX, los registros AAAA podrían tomar preferencia por sobre los A

RIPE Labs

- Es el primer RIR que se involucra en el tema (30/03/2010)
- <http://labs.ripe.net/content/spam-over-ipv6>
- Mediciones de tráfico SPAM sobre IPv6
- Las mediciones excluyen los mensajes rechazados por blacklist y greylist

RIPE Labs

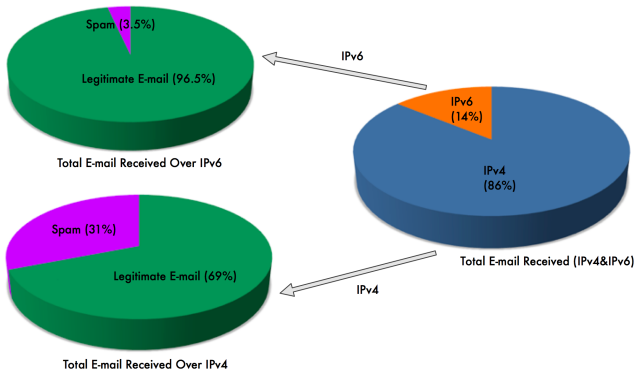


Figura: Número de mensajes SPAM recibidos en una semana.

Descripción de Mecanismos AntiSPAM

- Real-Time Blackhole List (RBL) / DNS BlackList
- Sender Policy Framework (SPF)
- Resolución del nombre/IP del cliente
- Greylisting
- Sender Address Verification (SAV)
- Recipient Address Verification (RAV)
- Clasificación usando Reglas Empíricas

RBL

- Esta basado en la reputación de la dirección IP del emisor
- Se configura en el MTA
- Es el primer mecanismo en actuar al abrirse la conexión
- Requiere de una consulta por DNS a la respectiva Zona para verificar que la IP no se encuentra bloqueada
- Se pueden consultar múltiples RBL de forma secuencial
- Tiene una eficacia del 50 % al 60 %
- Permite ahorrar recursos
- Requiere la intervención del administrador para remover la dirección IP bloqueada

RBL

- SpamHaus (libre, con límite en el número de consultas, comercial)
- SpamCop (libre)
- SORBS (libre, con costo para ser removido de la BL)
- uceprotect.net
- NJABL: Not Just Another Bogus List, AHBL: Abusive Hosts Blocking List, VIRBL: Virus Blackhole List
- Comerciales: IronPort, Barracuda, etc
- Proyectos discontinuados: Distributed Sender Blackhole List (DSBL), SPEWS

RBL

- Múltiples zonas disponibles para consulta
- Cada zona referencia diferentes fuentes de SPAM
- No existe un único criterio en los códigos retornados del rango 127/8

Códigos de respuestas de RBL (Fuente: SORBS)

- 127.0.0.2 - Open HTTP Proxy Server ([http.dnsbl.sorbs.net](http://dnsbl.sorbs.net))
- 127.0.0.3 - Open SOCKS Proxy Server (socks.dnsbl.sorbs.net)
- 127.0.0.4 - Open Proxy Server not listed in the SOCKS or HTTP lists. (misc.dnsbl.sorbs.net)
- 127.0.0.5 - Open SMTP relay server (smtp.dnsbl.sorbs.net)
- 127.0.0.6 - Hosts sending spam/UCE/UBE to SORBS, netblocks of spam supporting service providers (list.spam.dnsbl.sorbs.net)
- 127.0.0.7 - Web servers email vulnerabilities (e.g. FormMail scripts) (web.dnsbl.sorbs.net)
- 127.0.0.8 - Hosts demanding not to be tested by SORBS (block.dnsbl.sorbs.net)
- 127.0.0.9 - Networks hijacked from original owners (zombie.dnsbl.sorbs.net)
- 127.0.0.10 - Dynamic IP Address ranges (dul.dnsbl.sorbs.net)
- 127.0.0.11 - Domain names with bad A or MX RRs (badconf.rhsbl.sorbs.net)
- 127.0.0.12 - Domain names with no email originating (nomail.rhsbl.sorbs.net)

RBL sobre IPv6 en Postfix

Algunas limitaciones de Postfix para hacer uso de IPv6 y de RBL
(ver http://www.postfix.org/IPV6_README.html)

- The order of IPv6/IPv4 outgoing connection attempts is not yet configurable. Currently, IPv6 is tried before IPv4
- Postfix currently does not support DNSBL (real-time blackhole list) lookups for IPv6 client IP addresses; currently there are no blacklists that cover the IPv6 address space

Virbl: RBL con soporte IPv6

- Virbl <http://virbl.bit.nl> es un proyecto que nació en la reunión RIPE-48 (Mayo 2004)
- Obtienen informes de servidores de email que envían virus
- Incluye la dirección IP reportada desde donde se enviaron virus en una lista negra.
- Es el primer servicio que soporta consultas IPv6 (desde 15-01-2010)
- **List an entire /64 when we see five IPv6 hosts in the same /64**
- La lista negra es accesible para los formatos bind, rblndsd y texto

RFC 5782

- RFC 5782 DNS Blacklist and Whitelist (Feb 2010)
- Anti-Spam Research Group (ASRG) IRTF
- Define la estructura para las DNSBLs y las DNSWLs

RFC 5782

- IPv4 DNSxLs

```
99.2.0.192.bad.example.com      A      127.0.0.2
```

```
99.2.0.192.bad.example.com      TXT
```

```
"Dynamic address, see http://bad.example.com?192.0.2.99"
```

- IPv6 DNSxLs

Para representar la dirección 2001:db8:1:2:3:4:567:89ab en la DNSxL ugly.example.com

```
b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.8.b.d.0.1.0.0.2.
```

```
ugly.example.com. A 127.0.0.2
```

```
TXT "Spam received."
```

Sender Policy Framework

- Definido en el RFC 4408 (Abril 2006)
- sitio web <http://www.openspf.org>
- Algunos Mail Server lo soportan en forma nativa
- Librerías y Extensiones disponibles
- Soporta IPv6
- Similar a Sender ID que implementa Microsoft

```
domain IN TXT "v=spf a mx ip6:2001:1318:1009:400::8 -all"
```

Greylisting

- Base de datos dinámica
- Cada entrada es una tripleta: IPv4 o IPv6/From/Rcpt-To
- Agrega un retardo al recibir un mensaje si la entrada no existe
- Error temporal 4xx
- Un envío posterior al tiempo de retardo es aceptado
- Registro permanece en una DB por 72 Hs
- postgrey soporta IPv6

Resolución del nombre/IP del cliente

- Evita recibir mensajes provenientes de maquinas que no tienen un registro en el DNS del respectivo dominio pa
- En IPv4 no están correctamente delegados las direcciones IPv4 respecto a los dominios que sirven, en especial los registros MX y el A asociado
- Las más usadas: Unknown Client Hostname / Unknown Reverse Client Hostname
- Muchos mensajes no llegan y es preferible (más fácil) usar excepciones o desactivarla
- En IPv6 también necesitamos consistencia entre las zonas directas e inversas, y las que asignemos y deleguemos a los clientes.

Sender Address Verification SAV

- Se verifica que la dirección del remitente (From:) sea válida antes de aceptar el mensaje
- Se realiza una conexión hacia el
- Algunos MTA implementan una cache para disminuir el número de consultas
- Alto número de consultas puede considerarse SPAM y ser incluido en listas negras
- Genera errores cuando el mensaje es generado por un Mailhub o un Smart Mailer.
- Su funcionamiento es similar para IPv4 e IPv6, siendo IPv6 la primer opción de consulta

Recipient Address Verification RAV

- Se verifica que la dirección del destinatario (Rcpt-To:) sea válida antes de aceptar el mensaje
- Los usuarios pueden ser locales o virtuales, almacenados en archivos o backends (DB, LDAP)
- Se requiere de una consulta que valide la existencia del usuario
- Los MX secundarios requieren tener acceso a la validación y así evitar saturar sus colas de mensajes con destinatarios no válidos (no alcanza solo con el dominio)
- Su funcionamiento es similar para IPv4 e IPv6, solo es necesario su configuración en el DNS con las respectivas preferencias

Reglas Empíricas

- Se aplican sobre el mensaje aceptado y encolado
- Se evalúa cada campo del header y el cuerpo del mensaje
- Se aplican a mensajes de tamaño reducido (200KBytes)
- Se definen umbrales de SPAM y de descarte
- El puntaje obtenido clasifica finalmente al mensaje
- Se advierte al usuario que el mensaje es SPAM indicándolo en el asunto (Subject:)
- Se utilizan reglas genéricas y propias
- Cada regla tiene un puntaje.

SpamAssassin

- Es uno de los paquetes más utilizados para clasificar SPAM
- La versión 3.3.0 presenta varias mejoras respecto al uso de IPv6
- some of the IPv6 functionality in SpamAssassin requires that a perl module `IO::Socket::INET6` is available (like accessing a DNS resolver over `inet6`, talking to a `dccifd` host over `inet6` socket, SPAMC protocol)
- Algunas reglas utilizan plugin's que requieren consultas externas: Razor, Pyzor, Dcc
- Contiene reglas que usan RBL y asignan un puntaje al score final

Conectividad IPv6

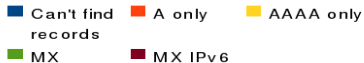
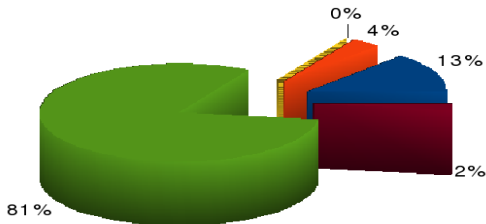
- IPv6 nativo por Innova-Red - RedClara
- IPv6: 2001:1318:1009::/48
- 540 entradas en la tabla BGP (es poco!!!!)
- ::/0 via IPv6 router de borde iBGP
- No peering IPv6 con otros ISP

```
smtp warning: connect to mx.ejemplo.com [2001:YYYY:ZZZZ:WWW::2]:  
No route to host (port 25)
```

Registros DNS

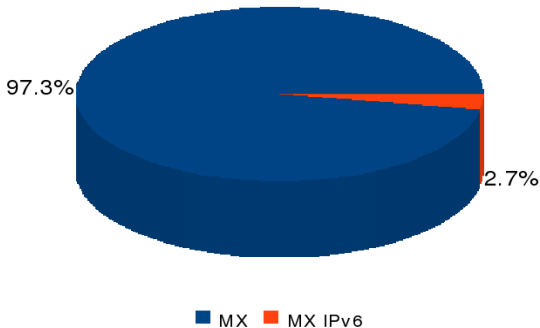
Registros DNS

261.893 Dominios



Registros MX

Registros MX

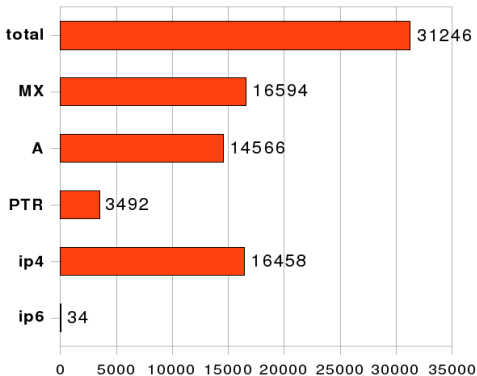


SPF

```
Apr 28 19:15:52 mecha postfix/smtpd[8949]: NOQUEUE: reject: RCPT from  
unknown[2002:xxxx::1234:c487]: 550 5.7.1 <usuario@criba.edu.ar>:  
Recipient address rejected: Message rejected due to: SPF fail - not authorized.  
Please see http://www.openspf.org/Why?s=mfrom;id=profesor@universidad.edu;  
ip=2002:xxxx::1234:c487;r=usuario@criba.edu.ar; from=<profesor@universidad.edu>  
to=<usuario@criba.edu.ar> proto=ESMTP helo=<host.universidad.edu>
```

SPF

Registros SPF



Greylisting

	Tripla	Porcentaje	Clientes	Porcentaje
IPv4	85841	99.95	16207	99.89
IPv6	47	0.05	18	0.11

Cuadro: Greylist IPv4 e IPv6

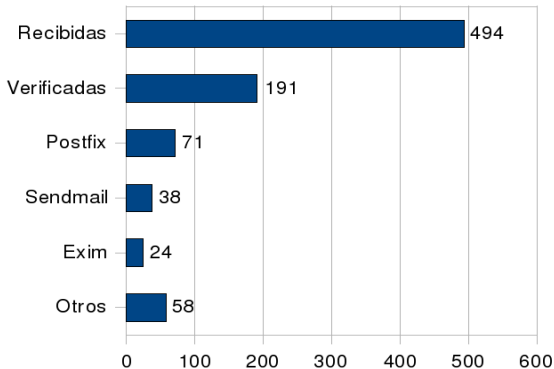
MTA en IPv6

Si la conexión se establece por IPv6, para la IPv6 fuente es aconsejable:

- Definir un registro MX para dominio del remitente
- Definir un registro AAAA
- Resolver en inversa la IPv6 del cliente
- Si tiene definido SPF para su dominio en IPv4, es necesario definirlo para IPv6 (mx, ip6:)
- responder sobre el puerto 25 para consultas SAV (Firewall, MTA)

Conexiones IPv6 port 25

Conexiones IPv6 puerto 25



Conclusiones

- Se cumplió el objetivo de brindar el servicio de email sobre IPv6
- Crece el trafico IPv6, ergo, crece el SPAM
- No todos los mecanismos AntiSPAM están hoy soportados sobre IPv6 respecto a IPv4
- Falta una política para fijar el subnetting (/64?) en una RBL IPv6
- No se llega al puerto 25 de un gran número de MX sobre IPv6 por no ser alcanzables
- Rechazo de mensajes que llegan desde conexiones IPv6 por malas configuraciones de DNS: MX y SPF

Conclusiones

- RBL requiere más disponibilidad de consulta y una implementación completa en los MTA
- Los productos comerciales AntiSPAM tendrán que adoptar IPv6 en sus servicios de reputación
- Los DNS seguirán cumpliendo un rol fundamental para consultas RBL sobre IPv6
- Necesitamos revisar los logs para constatar que los mensajes se envían por una conexión IPv6 o IPv4
- Las declaraciones SPF suelen olvidar las direcciones IPv6

Trabajo a Futuro

- El gran número de direcciones IPv6 y la autoconfiguración definirá el uso de listas blancas además de listas negras.
- Proponer un proyecto para DNS RBL y DNS WL que cubra los bloques IPv6 administrados (LACNIC?)
- Generar un grupo de trabajo para definir el servicio
- Poner a disposición dichas listas con diferentes formatos

¿ Preguntas ?

¿ Preguntas ?

Muchas gracias!!!

slaggio@criba.edu.ar