# Política de tráfico SMTP en la Comunidad Académica RedIRIS

Fecha: 07 Mayo 2006
Autor: Jesús Sanz de las Heras (RedIRIS)

## Introducción

El tráfico SMTP gestionado por los servidores de correo es extremadamente alto, un % muy alto del mismo (60-70%)[1] es tráfico no útil, tráfico oscuro. Este tráfico es ocasionado por conexiones procedentes de IPs comprometidas con algún tipo de malware con capacidad de motor SMTP propio, que se emplean para difundir spam, virus, ataques de diccionario (Directory Harvest Attaks) , denegación de Servicio (DoS), mensajes a destinatarios no existentes. La mayor parte de las soluciones de seguridad en el correo electrónico no tienen en cuenta este tráfico indeseado a través del puerto 25 que es aceptado, analizado y rechazado con el consiguiente uso de recursos necesarios.

Cuando una dirección de correo electrónico ha sido capturada e incluida en la base de datos de los spammers/hackers es **completamente imposible** eliminarla de dichos círculos, por lo que direcciones y buzones de carácter académico/científico está literalmente en peligro.

Hasta ahora ha sido mas sencillo definir el **spam detectado** (contenido del mensaje) sin prestar atención al **spam rechazado** (sobre del mensaje) más allá de las clásicas listas negras vía DNS, pero hay mas. La idea es definir los límites entre el **spam rechazado** del **spam detectado** y es acerca del primero adonde se dirige este documento

## Objetivo

El actual problema de seguridad en el correo electrónico es lo suficientemente grave como para tomar medidas comunes y consensuadas por parte de una Comunidad homogénea como es la comunidad académica española (RedIRIS)**.**

En definitiva el objetivo es definir un conjunto de recomendaciones para toda la Comunidad RedIRIS con el objeto de consensuar la gestión del tráfico SMTP entrante. Estas recomendaciones en bloque forman una **Política de tráfico SMTP en la Comunidad Académica RedIRIS** que permitirá:

- Disponer de una política común en RedIRIS
- Ser la base para construir un correo electrónico mas seguro en la comunidad científica
- Estar preparados para los nuevos protocolos que están por llegar (SPF,DKIM,CSV,Sender-ID etc.)
- Las medidas adoptadas puedan tener mas peso en la Red y contribuir en mejorar el correo global.

Las recomendaciones de esta Política están basadas en el respeto a los actuales estándares (RFCs) así como recomendaciones internacionales de Buenas prácticas para operadores de red. Estas recomendaciones son independientes de productos y configuraciones de software y hardware. Esperamos que el despliegue de esta política tenga impacto directo en una reducción de los recursos de los servidores, en los buzones de los usuarios y en la propia satisfacción del servicio.

Las recomendaciones serán complementarias a cualquier configuración de seguridad en las plataformas de correo electrónico en las instituciones RedIRIS

Para unificar esta política se especifican códigos de respuesta del protocolo SMTP especificados en: RFC2821 y RFC1123 y para los códigos de los motivos el RFC1893 y RFC2034, pudiendo **opcionalmente** añadir un url a esta política general

[1] Datos de tráfico oscuro de la Universidad Jaume I http://www.infospam.uji.es/?q=node/11

Esta política esta pensada como **pautas** y **recomendaciones** a seguir por las Servicios de Correo Electrónico de instituciones de la comunidad académica española. Cualquier duda para su implantación puede ser planteada a RedIRIS o a través del Grupo de Coordinación IRIS-MAIL.

## Recomendaciones

Una transacción SMTP según el estándar RFC821 tiene varias etapas: Conexión (CONNECT), Presentación (HELO), Emisor (MAIL FROM), Receptor (RCP TO:) y Contenidos (DATA). Estas recomendaciones van enfocadas a controles en el **Sobre** de las transacciones SMTP no a los **Contenidos**. Los controles SMTP en el Sobre tienen como objetivo verificar la validez de la dirección del servidor de correo remoto que solicita establecer la transacción SMTP.

**Conexión** (CONNECT)

1. Rechazar el establecimiento de conexión SMTP desde **IPs** y **dominios** incluidas en:
   - Listas de bloqueo internacional como Spamhaus

Código: 554. 1 Access blocked using sbl-xbl.spamhaus.org. SMTP. Policy of RedIRIS in http://www.rediris.es

   - Listas de IPs asociadas a conexiones residenciales de tipo ADSL/cable dinámica que no son servidores de correo autorizado

Código: 554. SMTP Policy of RedIRIS doesn't accept traffic generic cable/dsl hostnames. Policy of RedIRIS in http://www.rediris.es

   - Listas de bloqueo locales: IP, dominio inverso

Código: 554. 5.7.1 Relaying denied. IP/domain is banned

2. Rechazar el establecimiento de conexión SMTP desde IPs que no dispongan de resolución inversa.

Código: 554. No reverse DNS configuration for IP. Policy of RedIRIS in http://www.rediris.es

**Presentación** (HELO)

3. Rechazar el establecimiento de conexión SMTP cuyo valor HELO/EHLO sea nulo o sin canonificar tal como se especifica en el apartado 4.1.1.1 de RFC2821

Código: 554. 5.7.1 Helo command rejected: Host not found. Policy of RedIRIS in http://www.rediris.es

**Emisor** (MAIL FROM)

4. Interrumpir la transacciones SMTP cuyo valor MAIL FROM: sea un dominio no existente

Código: 554. Access denied . Domain of sender address does not resolve. Policy of RedIRIS in http://www.rediris.es

5. Interrumpir la transacciones SMTP cuyo valor MAIL FROM: sea un dominio local

Código: 554. Access denied. Domain of sender address its a local domain. Policy of RedIRIS in http://www.rediris.es

6. Chequear la responsabilidad del servidor remoto con SPF, DKIM, SenderID para comprobar que el correo procede del servidor oficial responsable del dominio.

**Receptor** (RCPT TO)

7. Rechazar la conexión si el dominio destinatario no es de nuestra responsabilidad.

Código: 554. Relay access denied

8. Rechazar la conexión si el la dirección destinataria no está permitida

Código: 554. Access denied

**Otros** (flujos)

9. Sistema de control de flujos SMTP que permita controlar un número inusualmente elevado de conexiones SMTP comparando IP,From,To

**Contenidos** (DATA)

10. Analizar el contenido del correo en busca del **spam** y **malware**. Este control es el que se aplica después de haber sido analizada la transacción SMTP (Sobre) y es dependiente de la política de contenidos de cada institución.
11. Definir un tamaños máximo de mensaje superior a 50 M. Esto permitirá el intercambio de ficheros ligeros entre instituciones de la Comunidad RedIRIS.