Listas de excepción en RedIRIS (WLES)

Fecha: Mayo 2006-05-23
Estado: borrador.

Introducción

Desde hace tiempo está muy extendido el uso de listas negras (blacklisting - DNSbl) como mecanismo de bloqueo en tiempo real de las transacciones SMTP en los servidores de correo. Este sistema incluso está siendo incorporado en muchos productos comerciales AntiSpam. Las listas negras son muy útiles para frenar el spam en los servidores, por el contrario ocasiona ciertos problemas a las instituciones (falsos positivos). Una forma de reducir estos problemas, manteniendo las listas negras es el uso de Listas blancas o listas de exclusión (whitelisting - DNSwl). Estas listas blancas permitirán aceptar el tráfico de determinadas instituciones independientemente de que estén incluidas en las listas negras, es decir, la transacción SMTP y el correo se acepta independientemente de si el servidor está en un lista negra.

El uso de listas negras ha crecido exponencialmente a raíz de que la mayor parte del spam procede de PC personales infectados (*zombies*) con virus, troyanos o gusanos. Siendo más económico bloquear las transacciones SMTP de *zombies* que analizar los contenidos. Pero a veces es posible que algún dominio bien gestionado sea incluido automáticamente en alguna DNSbl que estemos utilizando por los descuidos de algunos de sus usuarios provocando que *correo bueno* no llegue a sus destinatarios. Las políticas de permanencia en las Listas Negras es dependiente de sus gestores y salir de algunas de ellas puede ser un proceso complejo.

La dinámica de una lista blanca se compone de tres partes:

- Base de datos de servidores (IP) cuyo tráfico de correo será siempre aceptado
- Comité para evaluar altas/bajas y políticas
- Filtros en los servidores para chequear esta base de datos al aceptar el tráfico entrante.

- **Objetivos**

Crear una lista blanca a nivel español (WLES) para evitar el bloqueo de transacciones SMTP y/o correo de servidores de proveedores españoles.

- **Beneficios**

Hay operadores de correo que son gestionados correctamente y su inclusión automática en una Lista negra es una medida que ocasiona problemas al intercambio habitual de tráfico de correo entre instituciones, universidades y proveedores; es aquí donde entrarían los beneficios de las Listas Blancas. Una lista blanca con dominios bien supervisados permitirá reducir muchos problemas así como mejorar la calidad del tráfico SMTP.

- **Implementación**

El mecanismo más sencillo para acceder a la base de datos es vía DNS, cualquier servidor de correo podrá consultar vía DNS la base de datos para chequear si la IP de esta incluida o no recibiendo la respuesta adecuada. La mayor parte de los paquetes de los servidores (postfix, sendmail, qmail, exim etc) o módulos intermedios (spamassassin, amavis, mailscanner etc) permiten hacer chequeos DNS de Listas Blancas, aunque es un tema que habrá que especificar con mas detalle para ayudar los servidores que deseen implementarlo.

Para la construcción de la base de datos será necesario disponer de infraestructura y software DNS. Se creará una zona "wles.rediris.es" para almacenar la base datos. Actualmente hay una zona en pruebas en "testwl.ip6.com.es"

***Debe quedar claro que es la política del Servidor SMTP entrante la que decidirá que acciones tomar con los resultados obtenidos al chequear la whitelisting WL-ES*. No es responsabilidad de la Whitelisting WLES la adopción de dichas acciones.**

- **Formato del registro**

El formato de estos registros deberá ser homogéneo con el que se plantee en otros foros internacionales sobre todos europeos.

Para definir una entrada en la WLES serán necesarios dos registros

- RR A 127.0.0.2
- RR TXT informativo incluyendo el ASN y/o nombre del ISP al que pertenecen, por ejemplo el valor del campo *description* del bloque de dirección al que pertenece.

Ejemplos

- 130.206.1.3 responsable del correo @rediris.es. La entrada en la WLES sería:

3.1.206.130 IN A 127.0.0.2
3.1.206.130 TXT “ASN 766. RedIRIS”

- 213.4.149.64 responsable del correo @telefonica.net. La entrada en la WLES sería:

  64.149.4.213 IN A 127.0.0.2
  64.149.4.213 TXT “AS6813. Telefonica Data Espana”

- **Categorías de Whitelisting**

Se podrán crear las categorías que se consideren oportunas en una definición más específica de la iniciativa, así por ejemplo se podrán definir categorías de relays de Instituciones académicas (RedIRIS), otras de la Administración, otras de operadores etc. Estas categorías podrían ser accesibles definiendo varias zonas. Pero en una primera fase definiremos una única zona para WLES donde se incluyan las IPs de relay confiables.

- **Criterios de altas y bajas**

Una primera aproximación de los criterios de los relays que se incluyan en la WLES serían:

  - Deberán tener una política activa para prevenir y evitar la difusión de virus, spam etc.
  - Deberán disponer de un servicio de gestión de abuse (abuse@) el cual tendrá potestad para **detener** la difusión de spam/virus de sus clientes
  - Las cabeceras “Received:” de sus servidores sean de confianza
  - Deberán pertenecer a un ISP incluido al Foro ABUSES (http://www.rediris.es/abuses)

Las incorporaciones serán recogidas por un formulario Web, inicialmente serán propuestas al Foro ABUSES, evaluadas por un comité y anunciadas a través de dicho Foro.

Deberá de definirse una política pública y consensuada de la Whitelisting **WLES** que defina claramente los criterios de alta y baja de la misma. La relación de IP de la base de datos deberá ser pública en una página Web para que cualquiera pueda comprobar si su relay o el de otros están incorporados.

- **¿Quién podrá utilizar WLES?**

El acceso a la Zona WLES será pública y cualquier relay que confíe en él podrá utilizarla.