Uso de listas blancas y SPF en qmail

Autor: Roberto Navarro Reyes (TusProfesionales, SL.)

Uso de listas blancas *ESWL/MTAWL*

Para activar el uso de listas blancas en qmail, y en particular las listas ESWL y MTAWL bastará con editar el fichero `/var/qmail/supervise/qmail-smtpd/run` incluyendo antes de la entrada "`qmail-smtpd`" la ruta al binario `rblsmtpd`, las listas negras que queramos consultar con el flag `-r` junto con las listas blancas que queramos consultar con el flag `-a`. Por ejemplo (en el que consultamos la lista negra sbl-xbl de spamhaus y las dos listas blancas de la iniciativa de RedIris):

```
#!/bin/sh
QMAILDUID=`id -u vpopmail`
NOFILESGID=`id -g vpopmail`
MAXSMTPD=`cat /var/qmail/control/concurrencyincoming`
LOCAL=`head -1 /var/qmail/control/me`

if [ -z "$QMAILDUID" -o -z "$NOFILESGID" -o -z "$MAXSMTPD" -o -z
"$LOCAL" ]; then
echo QMAILDUID, NOFILESGID, MAXSMTPD, or LOCAL is unset in
echo /var/qmail/supervise/qmail-smtpd/run
exit 1
fi
if [ ! -f /var/qmail/control/rcpthosts ]; then
echo "No /var/qmail/control/rcpthosts!"
echo "Refusing to start SMTP listener because it'll create an open
relay"
exit 1
fi
exec /usr/local/bin/softlimit -m 40000000 \
/usr/local/bin/tcpserver -v -R -t 0 -l "$LOCAL" -x /etc/tcp.smtp.cdb -
c "$MAXSMTPD" \
-u "$QMAILDUID" -g "$NOFILESGID" 0 smtp \
/usr/local/bin/rblsmtpd  -r sbl-xbl.spamhaus.org \
-a eswlrev.dnsbl.rediris.es -a eswlrev.dnsbl.rediris.es \
/var/qmail/bin/qmail-smtpd mail.midominio.com \
/home/vpopmail/bin/vchkpw /usr/bin/true 2>&1
```

Configuración de qmail para que realice comprobaciones SPF en tiempo SMTP

Personalmente, recomiendo utilizar el *Combined Patch Set* de John M. Simpson que además del uso de SPF añade gran cantidad de características interesantes a qmail:

- limitar el número de destinatarios
- rechazar mensajes en los el dominio del destinatario no exista
- cambia el comportamiento de qmail con respecto al manejo de la quota de los buzones, de un "soft" error a un "hard" error
- nos permite invocar terceros programas como milters que gestionen la cola de correo
- no anunciar la posibilidad del comando AUTH si la conexión no es segura. En el caso de que el cliente de correo no soportase TLS sí que le permitiría usar autenticación.

- incrementar el buffer de memoria de qmail para almacenar direcciones IP
- rechazar en tiempo SMTP los mensajes dirigidos a destinatarios inexistentes
- soportar DomainKeys (inestable debido a un fallo en software de terceros)
- y por supuesto, soportar SPF

Actualmente, la versión estable de este parche es la 6c5, y se puede descargar y consultar su documentación en la siguiente url:

http://qmail.jms1.net/patches/combined-6c5.shtml

Tras aplicar el parche a nuestro qmail, e instalarlo, podemos activarlo de dos modos:

- definiendo la variable de entorno `SPFBEHAVIOR` (preferiblemente en `/var/qmail/supervise/qmail-smtpd/run`)
- creando el fichero `/var/qmail/control/spfbehavior`

En cualquiera de las dos opciones, en función del valor el comportamiento variará:

- **0**: No realiza comprobaciones SPF
- **1**: Sólo añade las cabeceras SPF al mensaje, pero nunca lo bloquea
- **2**: Devolverá "*temporary errors*" cuando por problemas DNS no pueda realizar la comprobación SPF
- **3**: rechazará los mensajes cuando SPF devuelva *fail*
- **4**: rechazará los mensajes cuando SPF devuelva *softfail*
- **5**: rechazará los mensajes cuando SPF devuelva *neutral*
- **6**: rechazará los mensajes cuando SPF NO devuelva *pass*

Personalmente, no recomiendo a nadie un valor por encima de 3.

Además, a través de los siguientes ficheros que deberemos crear en `/var/qmail/control` podemos gestionar aspectos adicionales del comportamiento de qmail respecto a SPF:

`spfrules`: Nos permite definir reglas que son ejecutadas antes de que las reglas reales de un dominio puedan fallar (*fail, softfail, neutral*). Además, son ejecutadas para aquellos dominios que no dispongan de registros SPF

`spfguess`: Nos permite definir reglas a ejecutar para aquellos dominios que no dispongan de registros SPF

`spfepx`: Nos permite redefinir el mensaje que devolverá nuestro MTA cuando rechace en tiempo SMTP un mensaje por SPF. Nos permite usar macros.