

# Filtrando virus y spam con Postfix

Fernando J. Pereda Garcimartín

ferdy@ferdyx.org

## 1. Filtrando virus y spam con Postfix

Bueno, realmente no solo con postfix si no apoyándonos en una gran herramienta, amavisd-new.

Inspirado (y basado) en el artículo de Ricardo Galli (<http://mnm.uib.es/~gallir/>) en BULMA (<http://www.bulma.net>) sobre montar Exim4 con antivirus (clamav) y spamassassin integrado (<http://bulma.net/body.phtml?nIdNoticia=1973>). Me dispuse a investigar cómo sería el tema en postfix y aunque al principio dio un poco de guerra, ahí va la solución:

Se supone que tenemos instalados los paquetes postfix, postfix-tls, amavisd-new, spamassassin y los paquetes de clamav (clamav-daemon clamav libclamav1 y clamav-freshclam).

Lo bueno de amavisd-new es que tiene interfaces a clamav y a spamassassin, con lo que 'mataremos dos pájaros de un tiro' es decir, haremos los dos filtrados en un solo paso. Configurar amavisd-new es muy sencillo, editamos /etc/amavis/amavisd.conf y como opciones tenemos que remarcar las siguientes:

```
$mydomain = 'ferdyx.org';
$forward_method = 'smtp:127.0.0.1:10025';
$notify_method = $forward_method;
$final_spam_destiny = D_PASS;
$sa_tag_level_deflt = 4.0;
$sa_tag2_level_deflt = 5.0;
$sa_kill_level_deflt = $sa_tag2_level_deflt;
```

La opción que merece más atención es \$forward\_method, que será la vía que utilizará amavisd-new para reinyectar el mensaje de correo en postfix; en este caso le hemos dicho que lo haga usando un smtp en localhost por el puerto 10025. Las otras lo que hacen es fijar algunas opciones sobre el SpamAssassin. Una que es importante es \$final\_spam\_destiny. Aquí he puesto D\_PASS ya que a mi me gusta filtrar los emails con maildrop. Además de que si lo dejáramos por defecto (D\_REJECT) estaríamos perdiendo los posibles falsos positivos.

Puedes necesitar hacer un par de cambios más en el amavisd.conf. Busca la siguiente porción de código:

```
### http://clamav.elektrapro.com/
[ 'Clam Antivirus-clamd',
  \&ask_daemon, [ "CONTSCAN {} \n", '/var/run/clamdctl',
  qr/\bOK$/, qr/\bFOUND$/,
  qr/^\.*?: (?!Infected Archive)(.*) FOUND$/ ],
```

Y cambiamos la ruta al socket de /var/run/clamdctl a /var/run/clamav/clamdctl para que se corresponda con la opción LocalSocket del fichero /etc/clamav/clamav.conf.

Ahora veremos la configuración de postfix, la idea es hacer que en los puertos por defecto (25 y 465) postfix pase todos los emails por amavisd-new. Y luego crear un proceso SMTP que solo correrá en la interfaz loopback (127.0.0.1) en el puerto 10025 y que pasará los correos a los usuarios sin pasarlo por amavisd-new. Esto es necesario para evitar que los correos entren en un bucle sin fin.

En /etc/postfix/main.cf añadiremos:

```
content_filter=smtp-amavis:[localhost]:10024
```

Y en /etc/postfix/master.cf:

```
smtp-amavis unix - - y - 2 smtp
-o smtp_data_done_timeout=1200
-o disable_dns_lookups=yes
127.0.0.1:10025 inet n - y - - smtpd
-o content_filter=
-o local_recipient_maps=
-o relay_recipient_maps=
-o smtpd_restriction_classes=
-o smtpd_client_restrictions=
-o smtpd_helo_restrictions=
-o smtpd_sender_restrictions=
-o smtpd_recipient_restrictions=permit_mynetworks,reject
-o mynetworks=127.0.0.0/8
-o strict_rfc821_envelopes=yes
```

La primera línea crea el filtro para amavis y la segunda crea el servidor local por el que permitirá cualquier correo sin intentar filtrarlo.

Para que amavisd-new haga uso de SpamAssassin debemos cerciorarnos de que *no* existe esta línea en el fichero de configuración de amavisd-new. Si la tenemos, es el momento de comentarla.

```
@bypass_spam_checks_acl = qw( . );
```

Ahora podemos iniciar postfix, amavisd-new, clamd, clamav-freshclan y spamassassin y comprobar si todo funciona. Sin embargo no vamos a terminar aquí, ya que hemos instalado (o deberíamos) postfix-tls nos aprovecharemos de la encriptación SSL.

Volveremos a habrir /etc/postfix/main.cf y añadiremos al final:

```
## TLS/SSL
smtp_use_tls = yes
smtpd_use_tls = yes
smtp_tls_note_starttls = yes
smtpd_tls_note_starttls = yes
smtpd_tls_key_file = /etc/postfix/ssl/smtpd-key.pem
smtpd_tls_cert_file = /etc/postfix/ssl/smtpd.pem
smtpd_tls_loglevel = 1
```

Ahora generamos el certificado y la clave, podemos hacerlo con el siguiente comando:

```
openssl req -config /etc/ssl/openssl.cnf -new -x509 -nodes -out /etc/postfix/smtpd.pem \
-keyout /etc/postfix/smtpd-key.pem -days 999999
```

Respondemos a las preguntas. Después en master.cf debemos descomentar las líneas que contienen los servicios tlsmgr y smtps ( o ssmtp, depende del sistema ). Después de esto, reiniciamos postfix

Para acabar os pondré las líneas del sources.list que he usado yo para woody:

```
deb http://www.backports.org/debian stable spamassassin postfix clamav
deb-src http://www.backports.org/debian stable spamassassin postfix clamav
deb http://people.debian.org/~aurel32/BACKPORTS stable main
deb-src http://people.debian.org/~aurel32/BACKPORTS stable main
```

De todas formas, tanto backports.org (<http://www.backports.org>) como apt-get.org (<http://www.apt-get.org>) podrán daros buenas 'líneas del sources.list'.