IntegratedInPostfixWithAmavis

SpamAssassin Integration with Postfix, using Amavis

This is just a summary of the following websites. Go there for more detailed information.

http://flakshack.com/anti-spam/wiki/index.php (Detailed instructions for OpenBSD, RedHat, and Debian)

http://www.freespamfilter.org/

http://www.ijs.si/software/amavisd/README.postfix.html

http://www.ijs.si/software/amavisd/#faq-spam

http://www.ijs.si/software/amavisd/amavisd-new-docs.html

http://www200.pair.com/mecham/spam/

This document describes the configuration for sitewide use of SpamAssassin with Amavis and Razor. The distribution used is SuSE Linux 9.0. If you use something else, some options may be different. For example Amavis may run as user amavis, not vscan and the path to the Amavis spool directory may be /var/amavis not /var/spool/amavis

Postfix Configuration

This section describes how to configure Postfix to use amavisd-new as an after-queue content filter (see the FILTER_README file that comes with your version of Postfix).

First, a few services must be defined in master.cf. The first service will setup an extra SMTP listener on a different port (10025 in this example). It will be used for the reinjection of mail back into Postfix. By unsetting the content_filter parameter, content filtering will be disabled for incoming mail on this port. This avoids loops.

```
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_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
```

The second service added is not strictly necessary, but is a good idea to have. It defines a service to use when sending the mail into amavisd-new. The "2" in the seventh column is the maximum number of processes of this type. Do not set this number too high, and make sure it is equal to the maximum number of amavisd-new processes (set in amavis.conf).

```
smtp-amavis       unix       -       -       y       -       2       smtp
        -o smtp_data_done_timeout=1200
        -o disable_dns_lookups=yes
```

Finally, we must configure Postfix to actually use our content filter. This is done with the content_filter parameter which we add to main.cf. We configure Postfix to use our newly defined smtp-amavis service and to connect to a certain host and certain port. Obviously, the port set here must be the port amavisd-new is listening to.

```
content_filter = smtp-amavis:[127.0.0.1]:10026
```

In this case, amavisd-new is running on the same host as Postfix, but it can be any host. With brackets surrounding the hostname, MX lookups of the hostname are suppressed. They are also necessary when specifying bare IP addresses instead of hostnames. MX records in DNS can be used to create simple load-balancing and fallback configurations.

This simple setup will cause address rewriting both before and after the content filter. For most configurations this is not only unnecessary, but will cause duplicate mail to be delivered in configurations with virtual aliases of the form a -> a,b. Virtual rewriting must be turned off either before or after the content filter. How this is done is, again, documented in Postfix's FILTER_README file doc.

Amavis configuration

Amavis is just used for spam detection, not virus protection. See the options below.

/etc/amavisd.conf

Change the following options:

- $mydomain = 'example.com'
  Change 'example.com' to 'domain1.com'

- @bypass_virus_checks_acl . . . .
  Change to @bypass_virus_checks_acl = qw(.);

We only want spam protection and no virus scanning, so this will disable virus scanning for all domains.

- $mailfrom_notify_spamadmin . . .
  Change
  "spam.police@$mydomain"; to "postmaster@domain1.com";

- #$spam_quarantine_to = 'spam-quarantine';

and insert a # symbol at the beginning of that line On the very next line, you'll see:

#$spam_quarantine_to = "spam-quarantine@$mydomain";

Here, remove the leading # symbol. (And make sure you have a mailbox for this address on a destination server -
This is where you will review quarantined emails, and will forward on any "false positives" to the proper recipients.)
Alternative: Instead of delivering the spam to a mailbox on the internal server, drop it into a folder right on the spamfilter. To do that, comment out the "spam_quarantine_to" line above that references the email address, and instead select and indicate a folder name for the value "spam_quarantine_to". (Read the comments in this area of amavisd.conf for more info.)

Go to the chapter # SpamAssassin settings When you run SpamAssassin with Amavis, you have to do most of the configuration in amavisd.conf.

See http://www.ijs.si/software/amavisd/#faq-spam for details.

- $sa_local_tests_only = 0;
  If you want to use Razor, this has to be set to 0.

- $sa_tag_level_deflt = -999;
  The number of hits needed to update the mail headers.
  With a value of -999 all headers will be updatedt with X_Spam_Flag, X_Spam_Level and X_Spam_Status

- $sa_tag2_level_deflt = 5.0;
  The number of hits required to set X_Spam_Flag to Yes.

- $sa_spam_subject_tag = '***SPAM*** ';
  Remove the # if you want ***SPAM*** to be added to the subject of spam mails.

- SpamAssassin configuration*

Go to /etc/mail/spamassassin and edit local.cf. My file looks like this.

Be sure to doublecheck this options with amavisd.conf. If one of these options is in amavisd.conf, the one in local.cf will not be used.

```
# Add your own customisations to this file.  See 'man Mail::SpamAssassin::Conf'
# for details of what can be tweaked.
#
# How many hits before a message is considered spam.

required_hits          5.0

# Whether to change the subject of suspected spam

rewrite_subject        0

# Text to prepend to subject if rewrite_subject is used

subject_tag            *****SPAM*****

# Encapsulate spam in an attachment

report_safe            1

# Use terse version of the spam report

use_terse_report       0

# Enable the Bayes system

use_bayes              1

# Enable Bayes auto-learning

auto_learn             1

# Enable or disable network checks

skip_rbl_checks        0
use_razor2             1
use_dcc                0
use_pyzor              0

# Mail using languages used in these country codes will not be marked
# as being possibly spam in a foreign language.

ok_languages           all

# Mail using locales used in these country codes will not be marked
# as being possibly spam in a foreign language.

ok_locales             all
```

Amavis expects to see spamassassin's user_prefs file in /var/spool/amavis/.spamassassin but that directory and that file do not exist. Spamassassin's Bayes data is also stored there.

```
cp -r /root/.spamassassin /var/spool/amavis
```

This will create it (and copy user_prefs to that directory at the same time).

```
chown -R vscan:vscan /var/spool/amavis/.spamassassin
```

Give amavis ownership

If you run spamassassin --lint -D from a command line you will notice that
spamassassin looks for config files in /root/.spamassassin and razor files in /root/.razor
This is misleading and confusing because
that is not where it looks when it runs under amavis.
You can create symbolic links to help make the command line debug look cleaner.
Also, it will not find any Bayes files in /root/.spamassassin so the
symbolic links will help there too.

```
cd /root/.spamassassin

rm user_prefs
```

```
ln -s /var/spool/amavis/.spamassassin/user_prefs user_prefs

ln -s /var/spool/amavis/.spamassassin/bayes_seen bayes_seen

ln -s /var/spool/amavis/.spamassassin/bayes_toks bayes_toks
```

- Razor configuration*

Open port 2703 in your firewall.

`razor-client`
This creates sym-links

`razor-admin -d -create`
Creates files in /root/.razor and shows debugging info.

`razor-admin -register`
Creates a random user name and password.
Necessary for data access to Razor2 servers.

`razor-admin -discover`
Refreshes the list of razor servers

Razor has to be patched to run under SpamAssassin.
Browse to http://www.ijs.si/software/amavisd/Razor2.patch-quinlan
use Save Page As and save in:
/usr/lib/perl5/vendor_perl/5.8.1/i586-linux-thread-multi/Razor2

```
cd /usr/lib/perl5/vendor_perl/5.8.1/i586-linux-thread-multi/Razor2

patch -p0 < Razor2.patch-quinlan

vi /root/.razor/razor-agent.conf
```
and insert
razorhome = /var/spool/amavis/.razor

Change the debuglevel from 3 to 0 or the log file will eventually
consume all disk space.
Save the file. We are going to copy Razor to it's new home in a moment.
Seems Amavis is not happy unless Razor is in that directory and it owns it.

`cp -r /root/.razor /var/spool/amavis`
This copies the stuff we need to where we need it.

`razor-admin -d -create -home=/var/spool/amavis/.razor`
This tries to force Razor to live there.

`chown -R vscan:vscan /var/spool/amavis/.razor`
Now amavis owns it.

`vi /var/spool/amavis/.spamassassin/user_prefs`
and insert

`razor_config /var/spool/amavis/.razor/razor-agent.conf`
This forces SpamAssassin to find the file here.