

HOWTO Configure Spam Filtering on SME 7 (SpamAssassin + Clam Antivirus)

Be sure to update to the latest SME 7 (RC2+) or some of this will not work!

This is a quick configuration howto, not an in-depth look at SpamAssassin. Much more can be done beyond this document. See 'More Information' at the end.

SpamAssassin

Server-Manager

Using the Server-Manager Configuration/E-Mail panel, adjust the settings to these reasonable defaults.

Virus scanning	Enabled
Spam filtering	Enabled
Spam sensitivity	Custom
Custom spam tagging level	5
Custom spam rejection level	13
Sort spam into junkmail folder	Enabled
Modify subject of spam messages	Enabled

I would also recommend blocking all executable content. To do so, select (highlight) all of the attachment types other than zip files (the last two).

Click Save.

Enable RBL (Blacklist) Testing

These commands will enable the disabled default blacklists and check that the settings were actually changed.

```
config setprop qpsmtpd DNSBL enabled RHSBL enabled
signal-event email-update
svc -t /service/qpsmtpd
```

then

```
config show qpsmtpd
```

How It Works

With this configuration, the spammiest messages, those marked as 10 or above, will be rejected at the SMTP level. Those spam messages marked between 5 and 10, will be routed to the users' (IMAP) junkmail folder. This is done so the users can check for false-positives...valid messages that were classified as spam by SpamAssassin.

Users may check their junkmail folders for false-positives via webmail, or, if they are using an IMAP mail client, by simply checking the junkmail folder exposed by their mail client.

```
https://servername/webmail
```

Tweaking

The server will automatically delete old spam in the junkmail folders after 90 days. You can control the number of days old spam is kept with the following commands. Where 15 is the number of days you want keep messages, do...

```
db configuration setprop spamassassin MessageRetentionTime 15
signal-event email-update
svc -t /service/qpsmtpd
```

then

```
config show spamassassin
```

If you are afraid of losing misclassified mail, adjust the 'Custom spam rejection level' higher.

If too much spam is making through to your inbox, carefully adjust the 'Custom spam tagging level' down.

If too much spam is building up in your (IMAP) junkmail folder, adjust the 'Custom spam rejection level' down or change the number of days spam is kept in the junkmail folder before being automatically deleted by the server.

Bayesian (Learning) Filter

Bayesian filtering is optional and can be enabled, if you want. Research this subject before doing so.

```
db configuration setprop spamassassin UseBayes 1
signal-event email-update
svc -t /service/qpsmtpd
```

then

```
cat /etc/mail/spamassassin/local.cf
```

For each user that is to participate in training the Bayesian filter, we must enable the bash shell. This has security ramifications, so think about it before enabling Bayesian filtering. As root, enter

```
chsh -s /bin/bash <user>
```

Install the LearnAsSpam.pl perl script and configure a nightly cron job like this:

```
cd /usr/bin
wget
http://distro.ibiblio.org/pub/linux/distributions/smeserver/contribs/bread/mailstats/LearnAsSpam.pl
chmod +x LearnAsSpam.pl
cd /etc/cron.d
wget
http://distro.ibiblio.org/pub/linux/distributions/smeserver/contribs/bread/mailstats/LearnAsSpam.cron
```

Be sure to enter the wget lines as one long line.

Using an IMAP mail client, create a new folder called 'LearnAsSpam'. I created mine at the top level, like 'Inbox'. Webmail will work fine for creating this folder, as well as checking the junkmail (filtered mail or quarantine) folder.

If any spam messages make it past the filter and into your inbox, just move them into the LearnAsSpam folder. A nightly cron job will process them and delete them for you. This is how you train the Bayesian filter.

Bayesian filtering must receive 200 spam messages before it starts to function. You can check this status by logging into the server as one of the regular users configured above (using the console, ssh or PuTTY) and entering this command:

```
sa-learn -D --dump magic
```

Clam Antivirus

Update and check your Clam Antivirus with this command.

```
freshclam -v
```

or

```
freshclam --debug
```

Verify hourly update checking by viewing the freshclam/current log file via the Server-Manager View Log Files panel.

More Information

Here is another great howto (URL is all one line).

```
http://distro.ibiblio.org/pub/linux/distributions/smeserver//contribs/rmitchell/smeserver/how  
to/Spam%20blocking%20HOWTO%20using%20qpsmtpd%20&%20RBL%20for%20sme%20server.htm
```

Informative URLs:

```
http://contribs.org/modules/pbboard/viewtopic.php?t=31278  
http://contribs.org/modules/pbboard/viewtopic.php?t=31279  
http://contribs.org/modules/pbboard/viewtopic.php?t=32158  
http://distro.ibiblio.org/pub/linux/distributions/smeserver/contribs/bread/mailstats/
```

Enter this command at a console.

```
perldoc Mail::SpamAssassin::Conf
```