

Setting Up SpamAssassin and ClamAV with Sendmail on FreeBSD

This document covers setting up a mail server on FreeBSD 5.4 RELEASE using Sendmail 8.13.3, SpamAssassin 3.1.0 and ClamAV 0.87. **Combining these altogether results in a mail server with strong protection against spam and virus-infected mails.**

Below are the procedures to setup the MTA (Mailer Transfer Agent) Sendmail. Configuration for other MTAs will be different so please be aware of this.

NB: All the following operations are performed as the root user.

Install FreeBSD

Fetch and burn the FreeBSD ISO images available at: (just disc1 should be sufficient)

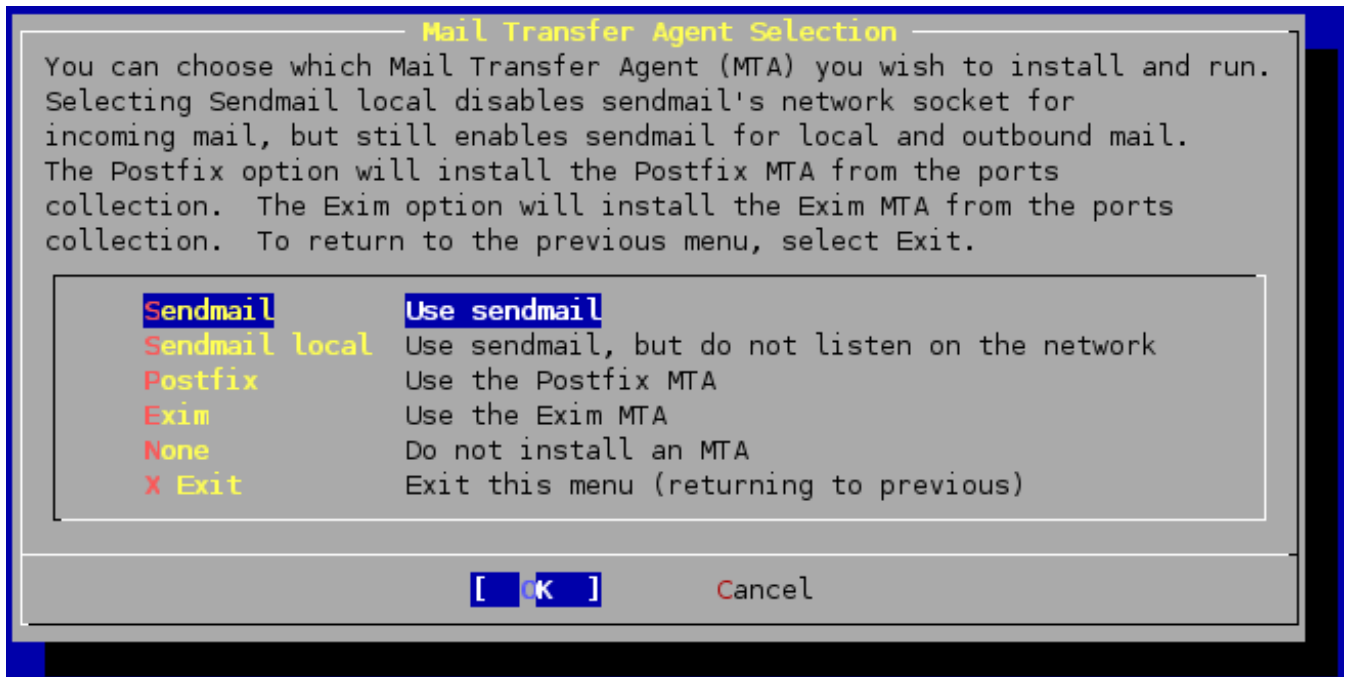
<ftp://ftp.jp.freebsd.org/pub/FreeBSD/ISO-IMAGES-i386/5.4/>

Don't install the ports collection from the CD as it's an old version. Download the latest from:

<ftp://ftp.jp.freebsd.org/pub/FreeBSD/ports/ports/ports.tar.gz>

and untar it in /usr after the OS has installed such that /usr/ports/* will be created.

After installation is done, run the sysinstall command and goto Configure (Do post-install configuration of FreeBSD) -> Networking (Configure additional network services) -> Mail (This machine wants to run a Mail Transfer Agent) and select Sendmail (Use sendmail). See the following picture:



The line `sendmail_enable="YES"` will be automatically added to `/etc/rc.conf` so Sendmail will

be run at boottime. If the line doesn't get added just add it yourself using your favourite editor.

Now would be a good time for you to update your system to the latest release of FreeBSD. Instructions for these procedures are out of the scope of this document but check [here](#) for info on how to do so. Use cvsup.

Get The Latest Perl 5.8

The default version of Perl in FreeBSD 5.4 is 5.8.6 but version 5.8.7 was the latest at the time of writing this article and I often found that having only 5.8.6 installed prevented various ports from installing properly so we'll upgrade Perl:

```
cd /usr/ports/lang/perl5.8
make deinstall
make install
```

It's necessary to upgrade Perl before going ahead and doing the SpamAssassin and ClamAV installs as the locations of libraries and such change.

Install SpamAssassin

Compile and install SpamAssassin:

```
cd /usr/ports/mail/p5-Mail-SpamAssassin
make install
```

The following dialogue will appear (this will not appear again after the first installation):



DOMAINKEYS and RAZOR are worthwhile having so leave them selected. I chose [SPF_QUERY](#)

because it's becoming more and more popular. I'm not sure exactly what TOOLS and RELAY_COUNTRY are but I included them anyway

At this point there should be the following startup script:

```
# ls -l /usr/local/etc/rc.d
total 2
-r-xr-xr-x 1 root wheel 696 Sep  2 18:01 sa-spamd.sh
```

Install spamassassin-milter

spamassassin-milter is the software that bridges SpamAssassin and Sendmail.

```
cd /usr/ports/mail/spamass-milter
make install
```

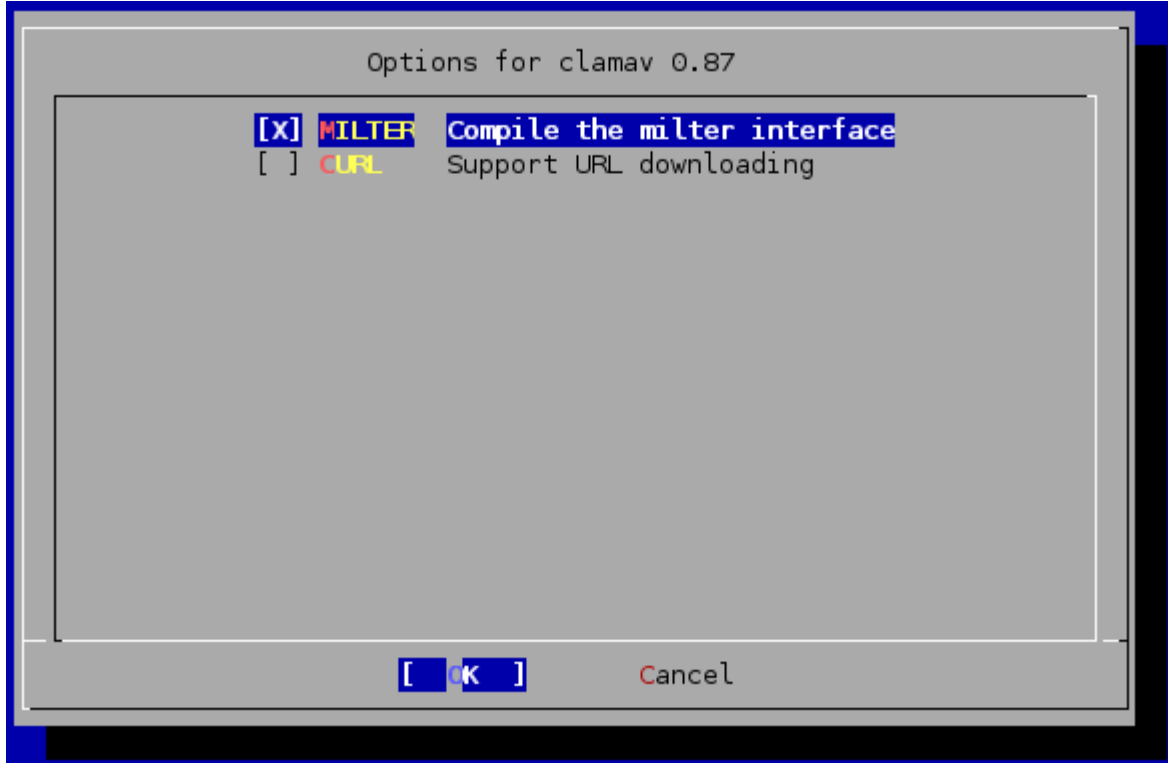
Now there should be the following two startup scripts:

```
# ls -l /usr/local/etc/rc.d
total 4
-r-xr-xr-x 1 root wheel 696 Sep  2 18:01 sa-spamd.sh
-r-xr-xr-x 1 root wheel 1013 Sep  2 18:04 spamass-milter.sh
```

Install ClamAV

ClamAV is free anti-virus software which can scan mails for virii.

```
cd /usr/ports/mail/p5-Mail-ClamAV
make install
```



After a while the above dialog screen will appear. Check MILTER.

A permission error saying clamd.log cannot be read/write accessed when executing clamav-milter can be solved by creating an empty file in advance:

```
touch /var/log/clamav/clamd.log
chown clamav /var/log/clamav/clamd.log
```

Now you should have all the following startup scripts:

```
# ls -l /usr/local/etc/rc.d
total 10
-r-xr-xr-x 1 root wheel 687 Sep 2 18:17 clamav-clamd.sh
-r-xr-xr-x 1 root wheel 722 Sep 2 18:17 clamav-freshclam.sh
-r-xr-xr-x 1 root wheel 1066 Sep 2 18:17 clamav-milter.sh
-r-xr-xr-x 1 root wheel 696 Sep 2 18:01 sa-spamd.sh
-r-xr-xr-x 1 root wheel 1013 Sep 2 18:04 spamass-milter.sh
```

Configure Sendmail

Sendmail is software for handling mail delivery (MTA). When installing FreeBSD the other two MTAs you can choose from are PostFix and Exim but I chose Sendmail as that's the one I'm most familiar with. The following procedures can only be used for Sendmail.

In order to use SpamAssassin and ClamAV with Sendmail there are various mechanisms which need to be defined in sendmail.cf (the configuration file). Also, definitions must be added to use RBLs (Real-time Black Lists - lists of hostnames, domains, mail addresses etc. found to be used by spammers that can be used to reject spam from these spammers).

Usually you do not directly modify sendmail.cf but rather modify the macro file (m4's .mc file format) which when parsed by m4 will generate sendmail.cf.

When you configure Sendmail on FreeBSD as described below, a macro file with its name as the server's hostname will be automatically created. Do the following:

```
cd /etc/mail
make
```

then, for example, if your machine is called mail.example.mu then a file called mail.example.mu will be created in that directory. From here on I will use mail.example.mu to refer to the sendmail.mc macro file as we add various configurations below, eventually leading up to the creation of the final Sendmail configuration file, sendmail.cf.

Once mail.example.mu has been created it'll not be overwritten if you run make again so when you want to add/modify some configuration, edit the file directly.

0) Basic configuration

First we define what kind of e-mail address formats your mail server will receive.

The e-mail address formats mail.example.mu will receive are:

```
test@example.mu
test@mail.example.mu
```

We create a file called `/etc/mail/local-host-names` and add the following:

```
example.mu
mail.example.mu
```

`mail.example.mu` is optional because it has the same domain as the first entry (`example.mu`). Please make sure that there are no inconsistencies between this file and the DNS MX settings for `example.jp`. Regardless of which e-mail address format is used, all mail will be delivered to `mail.example.mu`.

Next, create `/etc/mail/relay-domains` and add the following to define who is allowed to send mail from this server:

```
example.mu
192.168.0
```

The second line allows any machines on the local `192.168.0.0/24` network (assuming the mail server has global and local network interfaces) to relay e-mail through this server. Change this value according to your local network.

With the above configuration basic mail delivery can now be performed.

1) Add SpamAssassin and ClamAV settings

```
cd /etc/mail
vi mail.example.mu
```

and add the following:

```
INPUT_MAIL_FILTER(`spamassassin', `S=local:/var/run/spamass-milter.sock, F=,
T=C:15m;S:4m;R:4m;E:10m')dnl
INPUT_MAIL_FILTER(`clmilter', `S=local:/var/run/clamav/clmilter.sock, F=,
T=S:4m;R:4m')dnl
define(`confINPUT_MAIL_FILTERS', `clmilter,spamassassin')dnl
```

2) Settings related to reverse DNS lookups

Here we configure Sendmail to reject mail sent from hosts with no reverse DNS lookup. By doing this we're able to avoid most spam from Chinese and Korean servers which don't have reverse DNS lookup entries.

A side effect of this setting though is that mail from legit hosts maybe rejected due to bad server configuration. There are some people who are against setting their SMTP to use this mechanism. Do some research on Google yourself first before deciding if you want to set this on your mail server.

Add [these settings](#) to `mail.example.mu` if you want to ONLY reject hosts with no reverse DNS lookup.

OR if you want to reject both the above and hosts whose reverse DNS lookup and normal DNS

lookup do not match then add [these settings](#).

The tab characters must be preserved so be careful when copy/pasting.

If you want to be able to receive mail from hosts which do not have a reverse DNS lookup entry then you must not use these settings. Likewise, if you're likely to receive lots of legit mail from China and/or Korea (which have many such mail servers) you should avoid using these settings.

3) Setting up Sendmail RBLs

If an incoming mail is marked as spam by SpamAssassin the mail will still be delivered (and left for something else to filter it) but if you enable the RBL features in Sendmail, as we do below, then mail from a host that is rejected because of some RBL policy will not be delivered. Please keep this in mind when deciding whether to use the following.

There are various RBLs out there, we chose to use the following 4. Add this to mail.example.mu:

```
FEATURE(dnsbl,`bl.spamcop.net')dnl
FEATURE(dnsbl,`sbl-xbl.spamhaus.org')dnl
FEATURE(dnsbl,`list.dsbl.org')dnl
FEATURE(dnsbl,`all.rbl.jp')dnl
```

Make sure the above lines come before MAILER(smtp) and MAILER(local) lines in mail.example.mu.

There are many stories in Japanese mailing lists that too many legit addresses get registered in spamcop.net so if you are thinking on the safe side it would be okay to leave this line out.

The following 3 RBLs have not so good reputations , we don't recommend to use them.

```
BLARS
JAMM
SORBS
```

Sendmail's requests to the RBLs are done in the order listed in the configuration file. Even if all RBLs had exactly the same data, a culprit host would be rejected by the first RBL and the rejection would stop there. So only the rejection from the first RBL would be recorded in the Sendmail log file.

Just because you have a high number of RBLs configured it does not mean your server will be effective in avoiding spam. Unnecessary amounts of traffic and server load will be generated if you have too many RBLs defined so please choose an amount suitable for your mail server's purpose and intended use. Once all your configuration is done, run your server for a while, look at the mail log and see if there are one or more configured RBLs which don't appear much (or at all). This would indicate that they're not doing much in the way of contributing to rejecting hosts, most probably because they've got data in their databases similar (or the same) as one of the RBLs you've configured higher up in the list which do the rejecting first. Determine which one(s) are so and delete them.

So far, the updates we've added to mail.example.mu are [here](#). The tab characters must be preserved so make sure your browser doesn't break them if you copy/paste.

MAILER(local) and MAILER(smtp) were already in mail.example.mu before we started changing it. It's important that the RBL definitions (FEATURE(...) etc) come before the MAILER(...) definitions. The order is critical. The stuff below LOCAL_RULESETS are the

definitions to only reject mail from hosts which don't have a reverse DNS lookup and not when the normal and reverse DNS entries do not match.

4) Generating sendmail.cf

After the above configuration steps have been completed:

```
cd /etc/mail
make
```

and a file called mail.example.mu.cf will be made. This will now become our new Sendmail configuration file. Copy the file as follows:

```
cp mail.example.mu.cf sendmail.cf
```

Configure Autoboot

Add the following to /etc/rc.conf:

```
spamass_milter_enable="YES"
spamd_enable="YES"
clamav_clamd_enable="YES"
clamav_milter_enable="YES"
clamav_freshclam_enable="YES"
```

There we have it, Sendmail with SpamAssassin and ClamAV support running on FreeBSD configured to use some RBLs. However, please also install the packages below to make your mail server even more efficient in stamping out spam. Look at Running and Checking below for executing everything.

Other Software to Install

1) procmail

```
cd /usr/ports/mail/procmail
make install
```

Procmail is installed by default on Linux but on FreeBSD you need to install it manually.

Procmail allows you to manipulate mails marked as spam, for example placing them in a different folder, making them unreadable etc. As is out of the scope of this document, please Google to find more info on how to use it.

2) portupgrade

```
cd /usr/ports/sysutils/portupgrade
make install
```

portupgrade will make updating your installed ports to the newest versions easy. So, seeing as we installed SpamAssassin and ClamAV from ports we can use the following commands to

update them to their latest versions.

Remember, you must download and untar the latest version of ports.tar.gz into /usr/ports yourself beforehand.

```
portupgrade -vr p5-Mail-ClamAV
```

```
portupgrade -vr p5-Mail-SpamAssassin
```

```
portupgrade -vr clamav
```

Extra

If you decide to upgrade ClamAV without using portupgrade do it the following way:

```
cd /usr/ports/security/clamav
make WITH_MILTER=yes
make deinstall
make WITH_MILTER=yes install
```

If you've updated SpamAssassin and/or ClamAV and it's not the first time (ie. the programs are already running) then you need to restart them:

```
/usr/local/etc/rc.d/clamav-clamd.sh restart
/usr/local/etc/rc.d/clamav-freshclam.sh restart
/usr/local/etc/rc.d/clamav-milter.sh restart
/usr/local/etc/rc.d/sa-spamd.sh restart
```

Running and Checking

Reboot the server and check by making sure the following processes are running:

```
# ps -axw | grep -e clam -e spam
 480 ?? Is   0:09.97 /usr/local/sbin/clamd
 487 ?? Is   0:00.13 /usr/local/bin/freshclam --daemon
 494 ?? Ss   2:57.21 /usr/local/sbin/clamav-milter --pidfile /var/run/clamav/clamav-
milter.pid --postmaster-only --local --pos
 522 ?? Ss   0:45.65 /usr/local/sbin/spamass-milter -f -p /var/run/spamass-milter.sock
 5314 ?? Is   0:03.04 /usr/local/bin/spamd -c -d -r /var/run/spamd/spamd.pid (perl5.8.7)
28621 ?? I    2:44.87 spamd child (perl5.8.7)
28632 ?? I    2:43.92 spamd child (perl5.8.7)
```

After confirming this, try sending a mail to yourself on the server and look at the header, checking for the word SpamAssassin on the X-Spam-Checker-Version line and ClamAV on the X-Virus-Scanned line.

Post-config Changes

If you make any updates to SpamAssassin's local.cf:

```
/usr/local/etc/rc.d/sa-spamd.sh restart
```

will restart spamd (the SpamAssassin daemon). Then check the following processes are running:

```
# ps -ax | grep spam
 522 ?? Ss   0:46.57 /usr/local/sbin/spamass-milter -f -p /var/run/spamass
46349 ?? Ss   0:02.89 /usr/local/bin/spamd -c -d -r /var/run/spamd/spamd.pi
46356 ?? S    0:00.71 spamd child (perl5.8.7)
46360 ?? S    0:00.01 spamd child (perl5.8.7)
```

The following might or might not be running:

```
46347 ?? S    0:00.03 /usr/local/bin/spamc
```

depending on whether SpamAssassin is processing anything at that time.

If you make any updates to sendmail.cf:

```
cd /etc/mail
make restart
```

will restart Sendmail. Then check the following processes are running:

```
# ps -ax | grep sendmail
16383 ?? Is   0:01.10 sendmail: Queue runner@00:30:00 for /var/spool/client
16385 ?? Ss   1:57.27 sendmail: accepting connections (sendmail)
```

Having a Local Reject List

Using `/etc/mail/access` it is possible for you to have your own reject list. In this file you can specify e-mail address, domain names, hostnames and/or IP addresses.

Edit the file:

```
cd /etc/mail
vi access
```

and create your list based on the following format. The format is simply the address, hostname or IP followed by a TAB or space character and then the word REJECT. You may have as many lines as you like with one address per line but you must not have repeated lines.

```
privatefun@usa.net REJECT
mta163060.savings1friend.com REJECT
69.63.161.83 REJECT
72.26.220 REJECT
exrim.net REJECT
```

- The first line rejects any incoming mail from this address.
- The second line rejects any incoming mail from a server with that hostname and also any mail with that hostname in the From: field.
- The third line rejects any incoming mail from the machine with that IP address.

- The fourth line rejects any incoming mail from any host on the 72.26.220 subnet, ie from any machine with an IP address that is in the range 72.26.220.0-255.
- The fifth line rejects any incoming mail from any machine whose reverse DNS belongs to this domain and also any mail with this domain in the From: field.

In the case of all the lines above, mails will also not be able to be sent to the corresponding hostname/domain/IP/address. Usually if you're rejecting from you won't have the need to send to the same place, but in case you do, to enable only rejection from but allow sending to add "From: " at the beginning of the line, for example:

```
From:exrim.net      REJECT
```

to reject all mails from exrim.net but still allow sending to this domain.

When you've finished making the reject list:

```
cd /etc/mail
make
```

and then the changes will become immediately effective. There is no need to restart Sendmail.

Troubleshooting

- If you have a syntax error in SpamAssassin's local.cf then all configuration after that syntax error will not be read properly. Check the syntax by running:

```
spamassassin --lint
```

to find out where the problem is that needs fixing. There will be no output if there are no errors.

- If a process (or processes) is not running as expected, check /var/log/maillog and /var/log/messages for any relevant messages. There will probably be something in one or both of these log files explaining the problem.

- In the case a process is not running you can try starting it manually by running its bootstrap script in /usr/local/etc/rc.d, for example:

```
/usr/local/etc/rc.d/sa-spamd.sh start
```

will manually start SpamAssassin. Other valid arguments are usually stop and restart. If something's wrong a message will likely be displayed after running the script (if not also in the log files mentioned above).

- If you edit a configuration file on Windows be careful with the carriage return character (CR) as Windows uses CR LF (carriage return line feed) but Unix (FreeBSD et al) only uses LF. When you upload the configuration file from Windows to your FreeBSD server make sure only the LF exists on the end of each line and that there is no CR in sight otherwise you'll get unexpected errors on the FreeBSD box because the configuration file.

Miscellaneous

The FreeBSD OS and ports packages are constantly evolving. If the packages being used are old there is a chance the virus definition data etc will be unusable. Please make sure you keep your server updated with the most recent versions.

There are a ton of possible configurations in Sendmail's local.cf. We've only covered some of them in this document. Check the Spam Rejection Diary Hart Computer often updates with tips and tricks to further beef up SpamAssassin,