
System-wide virus and spam scanning

Installing **qmail-scanner**, **Clam Antivirus** and **SpamAssassin** under **FreeBSD**

Paul Hoadley
Eric Parsonage

Copyright © 2002, 2003, 2004 Paul Hoadley and Eric Parsonage

\$Date: 2004/03/17 13:08:06 \$

Revision History

Revision 1.3	2004/03/17	paulh
First version describing installation of applications from the ports system.		
Revision 1.2	2004/01/21	paulh
Original version describing all applications built by hand from source.		

This document describes how to effect system-wide virus and spam scanning of incoming email. The approach is based on the **qmail** mail transport agent, and is not applicable to sites running **sendmail**. This document describes how to install **qmail-scanner**, an enhancement for **qmail** that allows incoming mail to be passed through third-party filters prior to normal local delivery. The two filters described in this document are **Clam AntiVirus**, an open source virus scanning package, and **SpamAssassin**, an open source spam detector.

1. Pre-requisites

The following instructions are intended to be comprehensive, but there are at least these pre-requisites:

- The system should be running **qmail** as its mail transport agent. *The following instructions are targeted specifically at a **qmail** installation and will not work with **sendmail**.* Instructions for installing **qmail** as a replacement for **sendmail** can be found in the document **Installing qmail under FreeBSD**.
- **qmail** must be compiled with the `WITH_QMAILQUEUE_PATCH` option by specifying *at least*:

```
# make WITH_QMAILQUEUE_PATCH=yes
```

at the build stage. If **qmail** was built using the instructions in the [Installing qmail under FreeBSD](#) document, this patch will have been applied.

It is necessary to install **Clam AntiVirus** and **SpamAssassin** *prior* to installing **qmail-scanner**, as the latter tries to automatically detect available third-party scanners at installation time. There are no dependencies between **Clam AntiVirus** and **SpamAssassin** in the following approach—installation of either can be omitted if that functionality is not required.

2. Installing Clam AntiVirus

2.1. Installing Clam AntiVirus from the ports system

Clam AntiVirus can be installed from the ports system:

```
# cd /usr/ports/security/clamav
# make install
```

The port installation process will create a new user, `clamav`, and a new group, `clamav`.

2.2. Testing the installation

You should now read the documentation for **clamscan** (`man clamscan`, or read the [online documentation](#)). You can test the scanner by running:

```
# clamscan --recursive --log=/tmp/clamscan.log /usr/home
```

Obviously this can be run on the base directory of your choice, and the log file location is also arbitrary. Next, use the **freshclam** command to update your databases:

```
# freshclam --verbose
```

2.3. Running freshclam as a daemon

The port installation will place `clamav-freshclam.sh` in `/usr/local/etc/rc.d/`, so that **freshclam** can be run as a daemon from startup. Add the following line to `/etc/rc.conf` to enable **freshclam** as a daemon:

```
clamav_freshclam_enable="YES"
```

The **freshclam** manual page details the options available. The default options supplied by the startup script should be sufficient, but additional ones can be supplied by specifying them with the keyword `clamav_freshclam_flags`.

2.4. Running clamscan on a regular basis

If you have a filesystem directory tree that you think would benefit from regular virus scanning (anything accessible from any **Microsoft Windows** machines on your LAN would probably be candidates), you can set up a **cron** job to run **clamscan** on a regular basis. Read the **Clam AntiVirus** documentation and decide which options to **clamscan** are appropriate for your site. For example, you may not wish to specify the `--remove` option, and you may wish to `--exclude` any number of files or directories from scanning. As an example, the following entry appended to `/etc/crontab` will scan `/usr` daily at 6.00am:

```
0 6 * * * root /usr/local/bin/clamscan --recursive
--infected
--exclude /usr/local/share/clamav/viruses.db
--exclude /usr/local/share/clamav/viruses.db2
--log=/var/log/clamscan.log
/usr/home
```



Note

The line in `/etc/crontab` is shown broken here to improve readability, but should appear as a single line in the file.

3. Installing SpamAssassin

3.1. Installing SpamAssassin from the ports system

SpamAssassin can be installed easily from the ports system:

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

3.2. Testing the installation

You should now test **SpamAssassin** on the sample files provided. Firstly, test some known spam:

System-wide virus and spam scanning

```
# spamassassin -t < sample-spam.txt > spam.out
```

View the resulting file, `spam.out`. **SpamAssassin** should add the following headers to the message:

```
X-Spam-Status: Yes, hits=14.7 required=5.0
tests=ALL_CAPS_HEADER,CALL_FREE,DATE_IN_PAST_24_48,
DRASTIC_REDUCED,FROM_HAS_MIXED_NUMS,HOME_EMPLOYMENT,
INVALID_DATE,INVALID_MSGID,LINES_OF_YELLING,
MSGID_HAS_NO_AT,NO_REAL_NAME,ONCE_IN_LIFETIME,REMOVE_SUBJ,
SMTPD_IN_RCVD,SPAM_PHRASE_21_34,UNDISC_RECIPS
version=2.43
X-Spam-Flag: YES
X-Spam-Level: *****
X-Spam-Checker-Version: SpamAssassin 2.43 (1.115.2.20-2002-10-15-exp)
```

Additionally, there will be a banner explaining in detail what tests were failed.

Next, test **SpamAssassin** with a piece of genuine email:

```
# spamassassin -t < sample-nospam.txt > nospam.out
```

This should add only the following headers to the mail, indicating the message is not considered spam:

```
X-Spam-Status: No, hits=0.9 required=5.0
tests=GAPPY_TEXT,LINES_OF_YELLING,PGP_SIGNATURE,
SPAM_PHRASE_02_03,TO_BE_REMOVED_REPLY
version=2.43
X-Spam-Level:
```



Note

SpamAssassin's only action is to mark mail that it considers spam with the `X-Spam-` headers. It does not delete or even remove spam. Another agent is required in the chain to move the spam once detected. Instructions are given [below](#) for a simple per-user **procmail** recipe for moving spam to a separate folder.

3.3. Running SpamAssassin as a daemon: `spamd`

A startup script for **spamd** will have been placed in `/usr/local/etc/rc.d/spamd.sh`. Adding the following line to `/etc/rc.conf` will ensure that **spamd** is run as a daemon at startup:

```
spamd_enable="YES"
```

3.4. Using procmail to filter the spam

As noted above, **SpamAssassin** only tags spam with `X-Spam-` headers. If you don't do anything else, you'll still receive spam in your mailbox—it will just be identified as spam by those headers. One common solution is to use **procmail** as a mail delivery agent and instruct it to place the spam in a Maildir of its own. There is a lot of good documentation on installing and running **procmail**, and a thorough treatment of that complex program is beyond the scope of this document. If you have **procmail** installed at your site already, though, or even if you are prepared to install it from the Ports System *just to redirect SpamAssassin-tagged spam*, the following is a minimal procmail recipe to redirect spam to the Maildir `$HOME/Maildir/.Spam/`:

```
# Divert spam
:0:
* ^X-Spam-Status: Yes
$HOME/Maildir/.Spam/

# Deliver all other mail to inbox
:0:
$HOME/Maildir/
```

This recipe would be placed in each user's `.procmailrc` file. In addition, placing it in the file `/usr/share/skel/dot.procmailrc` will ensure that any newly created users will have a `.procmailrc` file generated in their home directory. Each user will also need to have a `.Spam` Maildir created for them. For example, to create the Maildir for `paulh`, enter:

```
# su paulh
# cd $HOME
# /var/qmail/bin/maildirmake Maildir/.Spam
# exit
```

In order to get **qmail** to call **procmail**, each user's `.qmail` file should contain the following:

```
|IFS=' ' && exec /usr/local/bin/procmail -f- || exit 75
```

Again, to ensure all new users have this `.qmail` created for them, replace the contents of `/usr/share/skel/dot.qmail` with the line above.



Note

Installing and running **procmail** is non-trivial. Read the documentation and the numerous FAQs and How-Tos if you plan to do this.

4. Installing qmail-scanner

4.1. Installing qmail-scanner from the ports system

qmail-scanner can be installed from the ports system:

```
# cd /usr/ports/mail/qmail-scanner
# make install
```

qmail-smtpd needs to be instructed to use the **qmail-scanner-queue.pl** script in `/var/qmail/bin` instead of the standard **qmail-queue** binary. If your site uses **tcpserver** to handle connections to **qmail-smtpd** (as described in [Installing qmail under FreeBSD](#)), `/etc/tcp.smtp` should be updated to set the `QMAILQUEUE` environment variable. The precise contents of this file will vary between sites depending on your LAN configuration. The `/etc/tcp.smtp` file constructed in [Installing qmail under FreeBSD](#) would be modified as follows:

```
192.168.0.:allow,RELAYCLIENT=" ",QMAILQUEUE="/var/qmail/bin/qmail-scanner-queue.pl"
127.:allow,RELAYCLIENT=" ",QMAILQUEUE="/var/qmail/bin/qmail-scanner-queue.pl"
:allow,QMAILQUEUE="/var/qmail/bin/qmail-scanner-queue.pl"
```

Now rebuild the ruleset for **tcpserver**:

```
# /usr/local/bin/tcprules /etc/tcp.smtp.cdb /etc/tcp.smtp.tmp < /etc/tcp.smtp
```

Finally, stop and restart the **qmail** binaries:

```
# /usr/local/etc/rc.d/qmail.sh stop
# /usr/local/etc/rc.d/qmail.sh start
```

4.2. Testing the installation

The **qmail-scanner** distribution provides a script and some test files containing virus signatures to test the virus scanner. Run these through **qmail-scanner** now:

```
# cd /usr/ports/mail/qmail-scanner/work/qmail-scanner-1.20
# ./contrib/test_installation.sh -doit
```

This will send three emails to the address you specified as `--admin` during the **qmail-scanner** installation. The first should arrive unmodified (though it will have an `X-Spam-Status:` header if you have set up **SpamAssassin**), but the second and third should be caught by either the internal (simple) virus scanner of **qmail-scanner** or by **Clam AntiVirus**. Email caught by

qmail-scanner is deposited in `/var/spool/qmailscan/quarantine` in Maildir format.

Contacting the authors

This document was written by **Paul Hoadley** and **Eric Parsonage**. This document describes what we did to get **qmail-scanner** co-operating with **Clam AntiVirus** and **SpamAssassin** on two FreeBSD 4.7 systems. Your mileage may vary. If you notice any errors in this document, or your experience with the software used was vastly different, please **let us know**. In particular, the original version of this document described building the applications from their source distributions, as there were no ports available. The descriptions of installing the applications from the ports system have not been rigourously tested, and bug reports are appreciated.