Filtering Mail With FreeBSD, Sendmail, And Milters

Warren Block, May 2005

Milters are plug-in email filters that make it easy to add filtering features to mail transfer agents that support the libmilter feature. We will use two milters along with sendmail to filter spam and viruses from email.

Caution: Milters and other email filters may discard wanted as well as unwanted email. If the risk of losing wanted email is unacceptable, please do not use these filtering methods.

Filtering email for spam and viruses can be very controversial, and the implications should be carefully researched and considered before implementation.

Using `milter-greylist`

Greylisting is a method of filtering email that can be summed up by the phrase “if it's important, they'll call back.” A greylisting filter temporarily refuses the first email from an unknown IP address. Legitimate email will be resent automatically, but spammers can't afford to wait for retries.

`Milter-greylist` (http://hcpnet.free.fr/milter-greylist) implements the greylisting technique described in more detail at http://projects.puremagic.com/greylisting.

Install `milter-greylist` from ports:

```
      # cd /usr/ports/mail/milter-greylist
      # make install clean
```

Configure `/usr/local/etc/mail/greylist.conf` by adding the netblocks of computers inside the LAN. For example, adding `addr 10.0.0.0./24` will allow email from computers at those addresses to pass through the greylist milter without being delayed. It's also possible to add domains or individual email addresses here.

To enable `milter-greylist`, add `miltergreylist_enable="YES"` to the `/etc/rc.conf` file. `milter-greylist` will be started at system boot, or you can run it manually (as root) with:

```
      # /usr/local/etc/rc.d/milter-greylist.sh start
```

Configure sendmail to use the milter by editing `/etc/mail/hostname.mc`:

```
      INPUT_MAIL_FILTER(`greylist', `S=local:/var/milter-greylist/milter-greylist.sock')
      define(`confMILTER_MACROS_CONNECT', `j, {if_addr}')
      define(`confMILTER_MACROS_ENVFROM', `i, {auth_authen}')
      define(`confINPUT_MAIL_FILTERS', `greylist')dnl
```

Rebuild the sendmail configuration and restart sendmail:

```
      # cd /etc/mail
      # make all install restart
```

At this point, incoming email will be processed by `milter-greylist`, and this will stop a great deal of spam. However, some virus-generated spam is sent through an ISP's email system, retrying and eventually passing through `milter-greylist`. In the next section we'll add virus filtering for incoming and outgoing email.

Adding `clamav-milter`

Many computer viruses propagate by sending copies of themselves attached to email. Rejecting virus messages protects users of both local and remote systems. To reject messages containing viruses, we'll add `clamav-milter`. Install `clamav-milter` (it is part of the `security/clamav` port):

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

Configure `/usr/local/etc/clamav.conf` by making sure these lines are uncommented:

```
    LogFile /var/log/clamav/clamd.log
    LogSyslog
    PidFile /var/run/clamav/clamd.pid
    DatabaseDirectory /usr/local/share/clamav
    LocalSocket /var/run/clamav/clamd
    FixStaleSocket
    StreamSaveToDisk
    ScanMail
```

Check `/usr/local/etc/freshclam.conf` and make any needed changes.

Enable and configure clamav-milter options in the /etc/rc.conf file:

```
  clamav_clamd_enable="YES"
  clamav_freshclam_enable="YES"
  clamav_milter_enable="YES"
  clamav_milter_flags="--quiet --local --outgoing --max-children=50 --dont-log-clean --noxheader --outgoing"
  freshclam_enable="YES"
```

`clamd` is the daemon that actually checks for viruses and is called by `clamav-milter`. freshclam is a daemon that will check for new virus definitions. See http://www.clamav.net for more information.

Note: Carefully examine the man page for `clamav-milter(8)` before using these options. As shown, they will cause email with attached viruses to be rejected. Viruses typically forge the `From` address, so bouncing virus email to those addresses often results in bombarding innocent users. Rejecting, or refusing these emails before receipt, causes no collateral damage.

`clamd`, `clamav-milter`, and `freshclam` will be started at system boot, or you can run them manually (as root) with:

```
    # /usr/local/etc/rc.d/clamav-freshclam.sh start
    # /usr/local/etc/rc.d/clamav-clamd.sh start
    # /usr/local/etc/rc.d/clamav-milter.sh start
```

Configure sendmail to use `clamav-milter` in addition to `milter-greylist`:

```
INPUT_MAIL_FILTER(`clamav', `S=local:/var/run/clamav/clmilter.sock, F=, T=S:4m;R:4m')dnl
```

Replace the `confINPUT_MAIL_FILTERS` line with:

```
define(`confINPUT_MAIL_FILTERS', `greylist,clamav')dnl
```

Rebuild the sendmail configuration and restart sendmail:

```
    # cd /etc/mail
    # make all install restart
```

Note: Having `greylist-milter` test email first saves bandwidth, since`clamav-milter` may have to receive the entire DATA portion of a message before detecting a virus. A greylisted message can be rejected after only the sending IP address has been determined.

With the combination of `milter-greylist` and `clamav-milter`, your email system will be protected from most forms of spam. If spam is still getting through, other methods of mail rejection can be added, including sendmail's `access.db` and DNS blocking lists. See `http://sendmail.org/m4/anti_spam.html`for more information.