POSTFIX - MORE ANTI-SPAM AND ANTI-VIRUSES

I figured I would go a little further with setting up postfix to stop spam and viruses, as it is something that all our email users will appreciate. For this setup I will be using only open-source software (only the best), specifically *spamassassin* and *clam*, with *amavis* to glue it all together. So this paper will be more of a how to get all this up and running.

What we need to start?
As mentioned, you will need a linux server running postfix 2.2 or higher (use *postconf mail_version* to see your version. If you need to upgrade go to http://www.postfix.org/), and also the software mentioned below..

- Amavisd-new (http://www.ijs.si/software/amavisd/)
- Clamav (http://www.clamav.net)
- Perl (I was using version 5.6 or higher)

ClamAV
For those of you who do not know, ClamAV is an open source anti-virus program which can run on multiple platforms but which was built for linux. Ands it's free! Once you have downloaded the software you will need to extract it, and then (you may need to update curl)...

- `useradd clamav`
- `<ClamAV folder>/configure`
- `<ClamAV folder>/make`
- `<ClamAV folder>/make install`

By default, the installation process installs to */usr/local/*. We need to edit the two configuration files found in */usr/local/etc/* as follows..

- `comment out the "Example" option in clamd.conf`
- `enable the AllowSupplementaryGroups in clamd.conf`
- `change user to run as to amavis in both clamd.conf and freshclam.conf`
- `make sure freshclam and clamd have log files in /var/log/ and that they are writable by amavis`
- `edit freshclam.conf to comment out the "Example" option`
- `edit the freshclam.conf and clamd.conf to enable logging to syslog and set user to amavis`
- `Set the socket option in clamd.conf to /var/run/clamav`

Next we need to setup a init startup script for clam. You can use the below example...

```
#!/bin/bash
#
# clamav:    This script controls the clamd
#
# chkconfig: 2345 79 31
# description: clamav
# processname: clamav
# pidfile: /var/run/clam.pid
# Source function library.
. /etc/rc.d/init.d/functions
prog="/usr/local/sbin/clamd"
prog_base="ClamD"
prog_config_file="/usr/local/etc/clamd.conf"
## Check that networking is up.
RETVAL=0

# See how we were called.
case "$1" in
  start)
    echo -n "Starting $prog_base:"
    $prog -c $prog_config_file  >> /var/log/clamd.log &
    RETVAL=$?
    [ $RETVAL -eq 0 ] && touch /var/lock/subsys/${prog_base}
    success
    echo
    ;;
  stop)
    echo -n "Shutting down $prog_base:"
    #Force the kill...
    kill `ps -A | grep clamd | cut -c1-6` &> /dev/null
    RETVAL=$?
    #Sleep for a second or two.
    /bin/sleep 3s
    #Kill the stale socket.
    rm -f /tmp/clamd > /dev/null
    if [ $RETVAL -eq 0 ] ; then
        success
            #echo "${prog_base} stopped"
            rm -f /var/lock/subsys/${prog_base}
        echo
    else
        echo
    fi
    ;;
  status)
    status ${prog_base}
    RETVAL=$?
    ;;
  restart)
    $0 stop
    $0 start
    RETVAL=$?
    ;;
  reload)
    #action $"Reloading ${prog_base}:" ${prog} -c ${prog_config_file} reload
    $0 restart
    RETVAL=$?
    ;;
  *)
    echo "Usage: $0 {start|stop|status|restart|reload}"
    exit 1
esac
exit $RETVAL
```

And the final two steps..

- `setup a cron job for freshclam to enable updates`
- `chkconfig --add clamav`

Amavisd-New

Amavis functions as the conduit which postfix uses to gain access to the spamassasin and clamav functionality. But it is definitely not limited to just those programs, browse through the configuration file and you'll see just how much it can do. Once you have extracted amavis, there is none of the customary make commands, but you do have to satisfy some perl dependencies..

```
perl -MCPAN -e shell
    install Archive::Tar
    install Archive::Zip
    install Compress::Zlib
    install Convert::TNEF
    install Convert::UUlib
    install MIME::Base64
    install MIME::Parser
    install Mail::Internet
    install Net::Server
    install Net::SMTP
    install Digest::MD5
    install IO::Stringy
    install Time::HiRes
    install Unix::Syslog
    install BerkeleyDB
    install Mail::ClamAV
    Install Digest::MD5
    install IO::Wrap
    install IO::Stringy
    install Unix::Syslog
    install Mail::Field
    install Mail::Address
    install Mail::Header
    install Mail::Internet
    install MIME::Words
    install MIME::Head
    install MIME::Body
    install MIME::Entity
    install MIME::Parser
    install MIME::Decoder
    install MIME::Decoder::Base64
    install MIME::Decoder::Binary
    install MIME::Decoder::QuotedPrint
    install MIME::Decoder::NBit
    install MIME::Decoder::UU
    install MIME::Decoder::Gzip64
    install Net::Server
    install Net::Server::PreForkSimple
```

After all of that there are still a couple of steps...

- as root: useradd -d /var/amavis -m amavis
- as amavis user: mkdir /var/amavis/tmp /var/amavis/var /var/amavis/db
- as root: cp <amavis folder>/amavisd /usr/local/sbin/
- as root: cp <amavis folder>/amavisd.conf /usr/local/etc/
- as root: mkdir /var/virusmails
- as root: chown amavis:amavis /var/virusmails
- as root: chmod 750 /var/virusmails
- as root: ln -s /usr/local/etc/amavisd.conf /etc/amavisd.conf
- as root: chown -R amavis. /var/run/clamav/ (for socket)
- as root: chgrp -R amavis /usr/local/share/clamav
- add clamav user to amavis group
- install amavisd init script (copy amavisd_init.sh to /etc/init.d and make changes needed to startup script)
- as root: chkconfig --add amavisd
- edit file /etc/amavisd.conf to;
    - adjust variables to refelect the created user and directories
    - $final_virus_destiny   = D_DISCARD;
    - $final_banned_destiny   = D_DISCARD;
    - $final_spam_destiny   = D_DISCARD;
    - $final_bad_header_destiny = D_PASS;
    - uncomment clamd virus check section

Spamassassin

This is a brilliant piece of software to do anti-spam. It does blacklist, phrase check, bayesian filters, and much more. To install it we need a couple of perl modules..

```
perl -MCPAN -e shell
    install ExtUtils::MakeMaker
    install File::Spec
    install Pod::Usage
    install HTML::Parser
    install Sys::Syslog
    install DB_File
    install Net::DNS
    install Mail::Audit
    install Digest::SHA1
    install Archive::Tar
    install Archive::Zip
```

```
        install Compress::Zlib
        install Convert::TNEF
        install Convert::UUlib
        install MIME::Base64
        install MIME::Tools
        install Net::Server
        install IO::Stringy
        install Time::HiRes
        install Mail::SPF::Query
        install IP::Country
        install Net::Ident
        install IO::Socket::INET6
        install IO::Socket::SSL
        install DBI
```

Once all of that is done, then you can..

```
        install Mail::SpamAssassin
```

This will install the configuration files to */etc/mail/spamassassin* and the rules to */usr/share/spamassassin*. Now that we have gotten this far, lets finish with the following steps..

- add spam user (we will use this as a spamdrop mailbox for review)
- vi /etc/amavisd.conf
    - comment out @bypass_spam_checks_maps
    - point $spam_quarantine_to = "spam-quarantine\@$mydomain"; to the spam user email address
- vi /etc/mail/spamassassin/local.cf
    - report_safe   1
    - use_terse_report   0
    - use_bayes   1
    - auto_learn   1
    - use_auto_whitelist
    - required_hits 5
    - rewrite_subject 1
    - subject_tag **[SPAM]**

Getting Postfix to use it all
So far, so good. The first thing to do is to test the amavis installation..

- amavisd -u amavis -g amavis -c /etc/amavisd.conf debug
- on a different terminal check that port 10024 is listening
- If all is fine, shutdown this instance, and startup with /etc/init.d/amavisd start

If you pick up any hassles you will need to sort them out before carrying on. But if all is fine, lets setup Postfix..

- edit your /etc/postfix/master.cf so it looks like;
    - smtp inet n - y - - smtpd
      ```
          -o content_filter=smtp-amavis:[127.0.0.1]:10024
      ```
- at the bottom put;

    -
      ```
      smtp-amavis unix - - y - 2 smtp
          -o smtp_data_done_timeout=1200
          -o disable_dns_lookups=yes
      127.0.0.1:10025 inet n    -    y/n    -    -  smtpd
          -o content_filter=
          -o local_recipient_maps=
          -o relay_recipient_maps=
          -o smtpd_restriction_classes=
          -o smtpd_delay_reject=no
          -o smtpd_client_restrictions=permit_mynetworks,reject
          -o smtpd_helo_restrictions=
          -o smtpd_sender_restrictions=
          -o smtpd_recipient_restrictions=permit_mynetworks,reject
          -o mynetworks_style=host
      ```

```
               -o mynetworks=127.0.0.0/8
               -o strict_rfc821_envelopes=yes
               -o smtpd_error_sleep_time=0
               -o smtpd_soft_error_limit=1001
               -o smtpd_hard_error_limit=1000
               -o smtpd_client_connection_count_limit=0
               -o smtpd_client_connection_rate_limit=0
               -o receive_override_options=no_header_body_checks,no_unknown_recipient_checks
```

Lastly, we have the final two steps..

- `postconf -e 'content_filter=smtp-amavis:[127.0.0.1]:10024'`
- `/etc/init.d/postfix reload`

Further Tweaking
A couple of common changes you make want to make include..

- If you want amavis to knock out emails with certain extensions tailor the *$banned_filename_re* to meet your needs.
- Add additional spamassassin rules into */usr/share/spamassassin*. Like the ones from
  - http://wiki.apache.org/spamassassin/CustomRulesets
  - http://www.rulesemporium.com/
  - http://www.exit0.us/index.php

Final Words
There you go. I know it was a bit of work (easy though), but trust me you and your email users will not regret it. Even though this setup uses many of the packages default settings -which do a very good job nonetheless, there is still a truckload of customizing and tweaking you can do to make it function the way you want to. As always, learn and have fun.