Implementing a
SPAM and virus scanning mail server
using
RedHat Linux 8.0

Ralf Spenneberg[*]

April 25, 2003

[*] ralf@spenneberg.net

This document was typeset using LaTeX 2_ε.

Contents

1 History

$Revision: 1.7 $ $Date: 2003/04/25 08:40:03 $

2 Installation of RedHat 8.0

2.1 Overview

THIS Document describes the installation and configuration of a e-mail server based on RedHat 8.0. The resulting e-mail server will scan the incoming and outgoing e-mails for SPAM and viruses.

The used products are:

- RedHat 8.0
- Postfix
- Spamassassin
- Amavis
- Sophos Antivirus

2.2 Installing RedHat 8.0

TO install RedHat 8.0 follow the guidelines in the RedHat installation manual. If you did not buy the RedHat box, do not worry. The installation manual is available for free as HTML or PDF on the RedHat webpage.

Since we want to install an e-mail server the partition theme should reflect this:

- / 500 Mb
- /usr 2000 Mb
- /tmp 500 Mb
- /home 2000 Mb
- swap 500 Mb
- /var rest

Make sure you install the postfix package.

2.3 Testing Postfix

Starting with Version 7.3 RedHat packages two mail transport agents (MTA): sendmail (default) and postfix. To choose which MTA to use (only one can bind to port 25!) RedHat adopted the alternatives system originally developed by Debian. The `sendmail` command in `/usr/sbin` is a symbolic link to `/etc/alternatives/mta` which again is a symbolic link to either

- `/usr/sbin/sendmail.sendmail` or
- `/usr/sbin/sendmail.postfix`.

The configuration therefore takes place in the `/etc` directory. These links are managed with the command `alternatives`.

```
#alternatives --display mta
mta - status is auto.
 link currently points to /usr/sbin/sendmail.sendmail
/usr/sbin/sendmail.sendmail - priority 90
 slave mta-mailq: /usr/bin/mailq.sendmail
 slave mta-newaliases: /usr/bin/newaliases.sendmail
 slave mta-rmail: /usr/bin/rmail.sendmail
 slave mta-mailqman: /usr/share/man/man1/mailq.sendmail.1.gz
 slave mta-newaliasesman: /usr/share/man/man1/newaliases.sendmail.1.gz
 slave mta-aliasesman: /usr/share/man/man5/aliases.sendmail.5.gz
/usr/sbin/sendmail.postifx - priority 30
 slave mta-mailq: /usr/bin/mailq.postfix
 slave mta-newaliases: /usr/bin/newaliases.postfix
 slave mta-rmail: /usr/bin/rmail.postfix
 slave mta-mailqman: /usr/share/man/man1/mailq.postfix.1.gz
 slave mta-newaliasesman: /usr/share/man/man1/newaliases.postfix.1.gz
 slave mta-aliasesman: /usr/share/man/man5/aliases.postfix.5.gz
Current ‘best’ version is /usr/sbin/sendmail.sendmail.
```

To switch the used mail transport agent to postfix use the following command:

```
# alternatives --config mta

There are 2 programs which provide ‘mta’.

  Selection    Command
-----------------------------------------------
*+ 1           /usr/sbin/sendmail.sendmail
   2           /usr/sbin/sendmail.postfix

Enter to keep the default[*], or type selection number: 2
```

This command also configures the SysV-initscripts to start postfix by default when booting.

Test this setup by rebooting. Make sure, that the postfix mailserver is started automatically during the boot:

```
# service postfix status
master (pid 10624) is running...
```

Test the availability of the postfix daemon by telnetting to port 25:

```
# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is ’^]’.
220 station.example.com ESMTP Postfix
quit
221 Bye
Connection closed by foreign host.
```

2.4 Configuring postfix

POSTFIX can be configured in two ways as MTA. Postfix can scan all messages as a standalone mailserver or as a relaying mailserver which passes all messages on to the real mailserver.

2.4.1 Standalone mailserver

A standalone mailserver receives and sends emails on its own. It takes care for all emails of the domain it is responsible of. The configuration of postfix for such a setup is quite simple. The needed configuration file `/etc/postfix/main.cf` follows:

```
# Queue directory and chroot
queue_directory = /var/spool/postfix

# Location of the post* commands
command_directory = /usr/sbin

# Location of the postfix daemon commands
daemon_directory = /usr/libexec/postfix

# Privileges
mail_owner = postfix

# Name of the mailserver
myhostname=host.example.com

# Domain to serve
mydomain=example.com

# Domain to masquerade as
myorigin=$mydomain

# ip addresses to listen on
inet_interfaces = all

# Names to receive email for
mydestination=$mydomain, $myhostname, localhost

# ip addresses to relay emails for
mynetworks=192.168.0.0/24, 127.0.0.0/8

# if a relayhost is used for the connection to the internet
# relayhost=[$mail.myprovider]

# Aliases database
alias_database = hash:/etc/postfix/aliases

# if dns resolution is not permanently available
# disable_dns_lookups=yes
```

The configuration file `/etc/postfix/master.cf` usually does not need any tweaking.

```
# ====================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (50)
# ====================================================================
smtp      inet  n       -       y       -       -       smtpd
#smtps     inet  n       -       y       -       -       smtpd \
-o smtpd_tls_wrappermode=yes -o smtpd_sasl_auth_enable=yes
#submission inet n       -       y       -       -       smtpd \
-o smtpd_enforce_tls=yes -o smtpd_sasl_auth_enable=yes
#628      inet  n       -       n       -       -       qmqpd
pickup    fifo  n       -       y       60      1       pickup
cleanup   unix  n       -       y       -       0       cleanup
#qmgr     fifo  n       -       y       300     1       qmgr
qmgr      fifo  n       -       y       300     1       nqmgr
rewrite   unix  -       -       y       -       -       trivial-rewrite
bounce    unix  -       -       y       -       0       bounce
defer     unix  -       -       y       -       0       bounce
flush     unix  n       -       y       1000?   0       flush
smtp      unix  -       -       y       -       -       smtp
showq     unix  n       -       y       -       -       showq
error     unix  -       -       y       -       -       error
local     unix  -       n       n       -       -       local
virtual   unix  -       n       n       -       -       virtual
lmtp      unix  -       -       n       -       -       lmtp
```

Postfix cannot deliver emails to root using the setup of the RedHat 8.0 Linux distribution. Therefore you must define an alias in the file `/etc/postfix/aliases`

2.4.2 Relaying mailserver

If postfix will be used as a mail relay the setup needs a special configuration file. Postfix will serve as a relay between the internet and the real internal email server.

The file `/etc/postfix/main.cf`:

```
# Queue directory and chroot
queue_directory = /var/spool/postfix

# Location of the post* commands
command_directory = /usr/sbin

# Location of the postfix daemon commands
daemon_directory = /usr/libexec/postfix

# Privileges
mail_owner = postfix

# Name of the mailserver
myhostname = host.example.com

# Domain to serve
mydomain = example.com

# Domain to masquerade as
myorigin = $mydomain

# Internal Mailserver (IP address)
internal_mail = x.x.x.x

# ip addresses to listen on
inet_interfaces = $myhostname

# Names to receive email for
mydestination = $mydomain

# ip addresses to relay emails for
mynetworks = $internal_mail, 127.0.0.0/8

# how to deliver the emails
transport_maps = hash:/etc/postfix/transport

# how to restrict the delivery of the email
smtpd_recipient_restrictions = permit_mynetworks, \
reject_unauth_destinations

# if a relayhost is used for the connection to the internet
# relayhost=[$mail.myprovider]

# Aliases database
alias_database = hash:/etc/postfix/aliases

# if dns resolution is not permanently available
# disable_dns_lookups=yes
```

An email relay does not need any local delivery service. It can be disabled in the configuration file /etc/postfix/master.cf.

```
# ====================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (50)
# ====================================================================
smtp      inet  n       -       y       -       -       smtpd
#smtps     inet  n       -       y       -       -       smtpd \
-o smtpd_tls_wrappermode=yes -o smtpd_sasl_auth_enable=yes
#submission inet n       -       y       -       -       smtpd \
-o smtpd_enforce_tls=yes -o smtpd_sasl_auth_enable=yes
#628      inet  n       -       n       -       -       qmqpd
pickup    fifo  n       -       y       60      1       pickup
cleanup   unix  n       -       y       -       0       cleanup
#qmgr     fifo  n       -       y       300     1       qmgr
qmgr      fifo  n       -       y       300     1       nqmgr
rewrite   unix  -       -       y       -       -       trivial-rewrite
bounce    unix  -       -       y       -       0       bounce
defer     unix  -       -       y       -       0       bounce
flush     unix  n       -       y       1000?   0       flush
smtp      unix  -       -       y       -       -       smtp
showq     unix  n       -       y       -       -       showq
error     unix  -       -       y       -       -       error
#local     unix  -       n       n       -       -       local
virtual   unix  -       n       n       -       -       virtual
lmtp      unix  -       -       n       -       -       lmtp
```

This configuration needs one further file /etc/postfix/transport. This file defines the method to deliver the emails to the internal mailserver. This file has the following contents:

```
example.com    smtp:[ip_internal_mail]
```

3 SpamAssassin

3.1 Installation

THe installation of spamassassin is quite straightforward since it is included in the RedHat 8.0 Linux distribution. Depending on your installation the following packets need to be installed:

1. perl-Digest-SHA1-2.01-6.i386.rpm
2. perl-Digest-HMAC-1.01-8.noarch.rpm
3. perl-Net-DNS-0.26-2.noarch.rpm
4. spamassassin-2.31-16.i386.rpm

If you subscribed to the RedHat Network, you can use the up2date command for the installation:

```
# up2date spamassassin
```

This command will resolve all dependencies and install all needed packages.

If you did not subscribe, you will need to install the packages manually using the rpm command:

```
# rpm -i perl-Digest-SHA1-2.01-6.i386.rpm
# rpm -i perl-Digest-HMAC-1.01-8.noarch.rpm
# rpm -i perl-Net-DNS-0.26-2.noarch.rpm
# rpm -i spamassassin-2.31-16.i386.rpm
```

3.2 Configuration

SPAMASSASSIN comes preconfigured out of the box when installed. The configuration files are located in `/etc/mail/spamassassin`. For the reduction of false positives the file `/etc/mail/spammassassin/local.cf` should list known allowed email addresses:

```
whitelist_from ralf@spenneberg.com
whitelist_from  ralf@spenneberg.net
```

Now postfix must be configured to use spamassassin. For this the simple content filter example from the postfix `FILTER.README` is used. Postfix calls an external script and pipes the email to this script. This script will scan the email and reinject the email using sendmail.postfix.

For performance reasons spamassassin is run in deamon mode. The RedHat 8.0 spamassassin package includes a start script which can be called using:

```
# service spamassassin start
```

To ensure a startup at boottime enter the following command:

```
# chkconfig spamassassin on
```

The script `spamfilter.sh` to call the spamassassin client consists of a few lines of code:

```
#!/bin/sh
#
INSPECT_DIR=/var/spool/filter
SENDMAIL="/usr/sbin/sendmail -i"
SPAMASSASSIN=/usr/bin/spamc

# Exit codes from <sysexits.h>
EX_TEMPFAIL=75
EX_UNAVAILABLE=69

cd $INSPECT_DIR || { echo $INSPECT_DIR does not exist; \
exit $EX_TEMPFAIL; }

# Clean up when done or when aborting.
trap "rm -f in.$$; rm -f out.$$" 0 1 2 3 15

# SpamAssassin uses a safe failover mode. If you do not want
# Emails to be delivered when Spamassassin doesn’t run remove
# the comments

cat | $SPAMASSASSIN -f > out.$$ #|| \
#   { echo Message content rejected; exit $EX_UNAVAILABLE; }

$SENDMAIL "$@" < out.$$

exit $?
```

Now create a user and group `spamfilter` to use when calling this script:

```
# useradd -d /dev/null -s /bin/false spamfilter
```

The temporary directory `/var/spool/filter` must be created:

```
# mkdir /var/spool/filter
# chgrp spamfilter /var/spool/filter
# chmod 770 /var/spool/filter
```

Now the configuration file `/etc/postfix/master.cf` needs to be modified, so that postfix calls spamassassin. Two lines are needed defining the filterscript and calling the filter for all incoming email using smtp.

```
filter    unix  -   n   n   -   -   pipe
    user=spamfilter argv=/usr/local/bin/spamfilter.sh
    -f ${sender} -- ${recipient}
smtp   inet  n   -   n   -   -   smtpd
    -o content_filter=filter:
```

It is very important, that wrapped lines are indented on the second line.

Restart postfix and test your setup. Every email should pass twice through postfix now. Once before scanned and once after the scanning.

To test the setup send an email with the following body:

```
subject to credit approval
be amazed
ma femme Jody
Free Membership
Credit Card Offers
Compare Rates
```

This should trigger the Spam detection machinery.

Now all emails are scanned for spam. Incoming and outgoing emails. When outgoing emails should not be scanned add your email addresses to a `whitelist_from`.

4 Amavis - A MAil VIrus Scanner

Amavis is not a virus scanner by itself. Rather it is the glue between the mailserver and a commandline virus scanning tool. Amavis intercepts the e-mail message and rips it apart, storing and unzipping attachments in separate files. These are then scanned by the external (commercial) virus scanner.

4.1 Installation

The installation of Amavis is quite simple if you use RPM packages. Unfortunately Amavis is not part of the Red Hat distribution yet. Therefore the RPM packages are not provided by Red Hat. Furthermore Amavis needs some additional Perl packages and archiving utilities like zoo, arc and rar.

RPM packages for the installation of Amavis may be downloaded at http://www.spenneberg.org/Firewall/Amavis. All packages in that directory are needed for the installation of Amavis on Red Hat 8.0. Additional packages may be needed from the Red Hat installation CDs:

- perl-Archive-Tar
- perl-Compress-Zlib
- perl-TimeDate
- ncompress
- unarj

Install all these packages and a virus scanner of your own choice. Amavis supports the following virusscanners:

- Network Associates Virus Scan
- DrSolomon (obsolete)
- H+BEDV AntiVir/X
- Sophos Sweep
- Lab AntiViral Toolkit Pro (AVP)
- CyberSoft VFind
- Trend Micro FileScanner

- CAI InoculateIT
- F-Secure Inc. (former DataFellows) F-Secure AV
- OpenAntiVirus

When installing the Amavis package, the installer tells you what to do:

```
Congratulations. You successfully installed amavis-perl for
Postfix on this machine.

You still need to configure some parts:
Add the emailusers
\"virusalert\"  and \"postfix\"
to your /etc/postfix/aliases file and redirect the mails to a
user. Configure Postfix to use amavis. The following is quoted
from the amavis Documentation README.postfix:
  Configuring postfix is very simple in this scenario:

  * add

     content_filter = vscan:

     to /etc/postfix/main.cf

  * add

     vscan  unix  -    n    n    -    10   pipe user=spamfilter
       argv=/usr/sbin/amavis \${sender} \${recipient}
     localhost:10025  inet  n   -   n   -    -      smtpd
       -o content_filter=

    to /etc/postfix/master.cf.
```

4.2 Configuration

To fulfil these requirements first create a user `virusalert` and a user `postfix`. The user `postfix` is often already generated by the postfix package.

The rest of the instructions are for an Amavis installation with SpamAssassin. When used without SpamAssassin a different approach (like displayed by the package when installing) needs to be taken.

Edit the file `/etc/postfix/master.cf` and modify the line starting with filter:

```
filter unix - n n - 10 pipe user=spamfilter \
argv=/usr/local/bin/spamfilter.sh ${sender} ${recipien
```

Then add the following line:

```
localhost:10025 inet n - n - - smtpd -o content_filter
```

Then modify the spamfilter.sh script:

```
#!/bin/sh
#
INSPECT_DIR=/var/spool/filter
SENDMAIL="/usr/sbin/sendmail -i"
SPAMASSASSIN=/usr/bin/spamc
AMAVIS=/usr/sbin/amavis

# Exit codes from <sysexits.h>
EX_TEMPFAIL=75
EX_UNAVAILABLE=69

cd $INSPECT_DIR || { echo $INSPECT_DIR does not exist; \
exit $EX_TEMPFAIL; }

# Clean up when done or when aborting.
trap "rm -f in.$$; rm -f out.$$" 0 1 2 3 15

# SpamAssassin uses a safe failover mode. If you do not want
# Emails to be delivered when Spamassassin doesn’t run remove
# the comments

# Filter for Spam
cat | $SPAMASSASSIN -f > out.$$ # || \
#   { echo Message content rejected; exit $EX_UNAVAILABLE; }

Filter for Viruses
$AMAVIS "$@" < out.$$

exit $?
```

Then configure Amavis to use the virus scanner. In case of Sophos edit the Line 58 in the script `/usr/sbin/amavis`:

```
my $SOPHOS = "/usr/bin/sweep"
```

4.3 Testing

Test the virus scanning engine by zipping the test virus `eicar.com`. Generate an email and attach the zipped virus. Amavis should detect the virus and send appropiate emails.

4.4 Congratulations

Your Mailserver now scans for Viruses and filters Spam.

4.5 Links

- Postfix: http://www.postfix.org
- Amavis: http://www.amavis.org
- SpamAssassin: http://www.spamassassin.org
- Ralf Hildebrandts Postfix pages: http://www.stahl.bau.tu-bs.de/˜hildeb/postfix