Implementing a
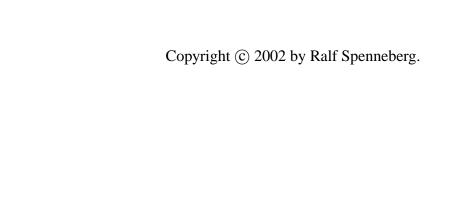# SPAM and virus scanning mail server using
RedHat Linux 8.0
and amavisd-new

Ralf Spenneberg*

May 21, 2003

* ralf@spenneberg.net

This document was typeset using LaTeX 2_ε.

Contents

1 History

$Revision: 1.3 $ $Date: 2003/04/13 11:32:43 $

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

S TARTING with Version 7.3 RedHat packages two mail trans-
port 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` direc-
tory. 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]
```

You will have to call the command postmap /etc/postfix/transport to activate the map.

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
```

Spamassassin will be directly called by Amavisd-new. No filter script is needed to call spamassassin. The spamassassin daemon does not have to be started at boot time.

4   Amavisd-new - 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. Amavisd-new is a full rewrite of the original Amavis. It has been daemonized and a spamassassin interface has been added.

4.1   Installation

The installation of Amavisd-new is quite simple if you use RPM packages. Unfortunately Amavisd-new 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 Amavisd-new may be downloaded at http://www.spenneberg.org/Firewall/Amavisd-new. All packages in that directory are needed for the installation of Amavisd-new 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. Amavisd-new 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

After installing the Amavisd-new package, check that you have a user amavis and the email-aliases ̈virusalert ̈and ̈postfix ̈on your system.

4.2   Configuration

Now Postfix needs to be configured to call amavisd-new. Edit the file `/etc/postfix/master.cf` and add the following lines:

```
127.0.0.1:10025 inet n - y - - smtpd
    -o content_filter=
    -o local_recipient_maps=
    -o smtpd_helo_restrictions=
    -o smtpd_client_restrictions=
    -o smtpd_sender_restrictions=
    -o smtpd_recipient_restrictions=permit_mynetworks, \
reject_unauth_destination
    -o mynetworks=127.0.0.0/8

smtp-amavis unix - - y - 2 smtp
    -o smtp_data_done_timeout=1200
    -o disable_dns_lookups=yes
```

The first lines define an additional smtp-listener on port 10025. This smtpd is used by amavisd-new to reinject the scanned messages into postfix.

Then add the following line to the file `/etc/postfix/main.cf`:

```
content_filter = smtp-amavis:[127.0.0.1]:10024
```

This instructs postfix to send all emails for content filtering to amavis on localhost port 10024. This port is opened by amavis by default.

Then configure Amavis to use the virus scanner. In the case of a command line virus scanner like Sophos you usually do not have to do anything. Amavisd-new finds these virusscanners by itself. If

you use a daemonized version like OpenAntiVirus or Sophie, you will have to modify the configurationfile `/etc/amavisd.conf`.

This configuration file also gives the flexibility to turn spamassassin on or off (on by default) and to define white and blacklists for virusscanning.

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.

sectionLinks

- 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