This is more a less a DRAFT (Version 0.1) and should not be use on a productive system!
The HowTo is not ready but i will make it public so that other user can go on with it. Feel free to change it

For any question use the Forum or PM me (BeNe)

Needed Packages

aptitude install libaprutil1-dbd-mysql razor libnet-dns-perl libmailtools-perl spamc spamassassin libmail-dkim-perl dkim-filter clamsmtp libtie-cache-perl libdbd-mysql-perl pyzor

Spamassassin

User spamd

```
groupadd -g 5001 spamd
useradd -u 5001 -g spamd -s /sbin/nologin -d /var/lib/spamassassin spamd
mkdir /var/lib/spamassassin
chown spamd:spamd /var/lib/spamassassin
```

/etc/default/spamassassin

Change the file like this:

```
ENABLED=1
SAHOME="/var/lib/spamassassin/"
OPTIONS="-d -q --create-prefs --max-children 5 --username spamd --helper-
home-dir ${SAHOME} -s ${SAHOME}spamd.log"
PIDFILE="${SAHOME}spamd.pid"
```

/etc/spamassassin/local.cf

Change the file like this:

```
rewrite_header Subject [***** SPAM _SCORE_ *****]
required_score 2.0
#to be able to use _SCORE_ we need report_safe set to 0
#If this option is set to 0, incoming spam is only modified by adding some
"X-Spam-" headers and no changes will be made to the body.
report_safe 0
```

```
# Enable the Bayes system
use_bayes 1
use_bayes_rules 1

# Enable Bayes auto-learning
bayes_auto_learn 1

# Enable or disable network checks
skip_rbl_checks 0
use_razor2 0
#use_dcc 0
use_pyzor 0
```

we set spamassassin's spamd default settings to rewrite email subject to [* SPAM _SCORE_ *], where _SCORE_ is the score attributed to the email by spamassassin after running different tests, only if the actual score is greater or equal to 2.0. So email with a score lower than 2 won't be modified.

To be able to use the _SCORE_ in the rewrite_header directive, we need to set report_safe to 0.

In the next section, we tell spamassassin to use bayes classifier and to improve itself by auto-learning from the messages it will analyse.

In the last section, we disable collaborative network such as pyzor, razor2 and dcc. Those collaborative network keep an up-to-date catalogue of know mail checksum to be recognized as spam. Those might be interresting to use, but I'm not going to use them here as I found it took long enough to spamassassin to deal with spams only using it rules.

```
/etc/init.d/spamassassin start
```

/etc/postfix/master.cf

Change /etc/postfix/master.cf

```
# Uncomment the second line below when unsing AMaViS
smtp      inet  n       -       -       -       -       smtpd
#  -o receive_override_options=no_address_mappings
```

to

```
# Uncomment the second line below when unsing AMaViS
smtp      inet  n       -       -       -       -       smtpd
 -o content_filter=spamassassin
#  -o receive_override_options=no_address_mappings
```

Add on the end of the file:

```
spamassassin unix -     n       n       -       -       pipe
```

```
  flags=Rq user=vmail argv=/usr/bin/spamc -u ${user}@${domain} -e
/usr/sbin/sendmail -oi -f ${sender} ${recipient}
```

/etc/postfix/main.cf

Add to main.cf

```
spamassassin_destination_recipient_limit = 1
```

Spamassassin / SQL

Create MySQL User

```
mysql -h localhost -u root -p
use mysql;
insert into user (Host, User, Password)
values('localhost','spamassassin',password("YoUrPaSSworD"));
insert into db (Host, Db, User, Select_priv, Insert_priv, Update_priv,
Delete_priv)
values('localhost','spamassassin','spamassassin','Y','Y','Y','Y');
create database spamassassin;
flush privileges;
quit;
```

Import SQL-Files

```
/usr/share/doc/spamassassin/sql# mysql -u spamassassin -p YoUrPaSSworD <
awl_mysql.sql
/usr/share/doc/spamassassin/sql# mysql -u spamassassin -p YoUrPaSSworD <
userpref_mysql.sql
/usr/share/doc/spamassassin/sql# mysql -u spamassassin -p YoUrPaSSworD <
bayes_mysql.sql
```

/etc/spamassassin/sql.cf

```
bayes_store_module      Mail::SpamAssassin::BayesStore::MySQL
bayes_sql_dsn           DBI:mysql:spamassassin:localhost:3306
bayes_sql_username      spamassassin
bayes_sql_password      YoUrPaSSworD

auto_whitelist_factory          Mail::SpamAssassin::SQLBasedAddrList
```

```
user_awl_dsn                    DBI:mysql:spamassassin:localhost:3306
user_awl_sql_username           spamassassin
user_awl_sql_password           YoUrPaSSworD

user_scores_dsn                  DBI:mysql:spamassassin:localhost:3306
user_scores_sql_username         spamassassin
user_scores_sql_password         YoUrPaSSworD
user_scores_sql_custom_query     SELECT preference, value FROM _TABLE_ WHERE
username = _USERNAME_ OR username = '$GLOBAL' OR username =
CONCAT('%',_DOMAIN_) ORDER BY username ASC

# Override the username used for storing
# data in the database. This could be used to group users together to
# share bayesian filter data. You can also use this config option to
# trick sa-learn to learn data as a specific user.
#
#bayes_sql_override_username vmail
```

/etc/default/spamassassin

```
# /etc/default/spamassassin
# Duncan Findlay

# WARNING: please read README.spamd before using.
# There may be security risks.

# Change to one to enable spamd
##ENABLED=0

# Options
# See man spamd for possible options. The -d option is automatically added.

# SpamAssassin uses a preforking model, so be careful! You need to
# make sure --max-children is not set to anything higher than 5,
# unless you know what you're doing.

##OPTIONS="--create-prefs --max-children 5 --helper-home-dir"

# Pid file
# Where should spamd write its PID to file? If you use the -u or
# --username option above, this needs to be writable by that user.
# Otherwise, the init script will not be able to shut spamd down.
##PIDFILE="/var/run/spamd.pid"

# Set nice level of spamd
#NICE="--nicelevel 15"
```

```
# Cronjob
# Set to anything but 0 to enable the cron job to automatically update
# spamassassin's rules on a nightly basis
CRON=0

ENABLED=1
SAHOME="/var/lib/spamassassin/"
OPTIONS="-d -q --create-prefs --max-children 5 --username spamd --helper-
home-dir ${SAHOME} -s ${SAHOME}spamd.log"
PIDFILE="${SAHOME}spamd.pid"
```

DEBUG

```
spamd -D -q -x --create-prefs --max-children 5 --username spamd --helper-
home-dir /var/lib/spamassassin/ -s /var/lib/spamassassin/spamd.log --
pidfile=/var/lib/spamassassin/spamd.pid
```

ClamSMTP

/etc/clamsmtp

```
# ------------------------------------------------------------------------
----
#                         SAMPLE CLAMSMTPD CONFIG FILE
# ------------------------------------------------------------------------
----
#
# - Comments are a line that starts with a #
# - All the options are found below with their defaults commented out


# The address to send scanned mail to.
# This option is required unless TransparentProxy is enabled
OutAddress: 10025

# The maximum number of connection allowed at once.
# Be sure that clamd can also handle this many connections
#MaxConnections: 64

# Amount of time (in seconds) to wait on network IO
#TimeOut: 180

# Address to listen on (defaults to all local addresses on port 10025)
Listen: 127.0.0.1:10026
```

```
# The address clamd is listening on
ClamAddress: /var/run/clamav/clamd.ctl

# A header to add to all scanned email
#Header: X-AV-Checked: ClamAV using ClamSMTP

# Directory for temporary files
TempDirectory: /var/spool/clamsmtp

# PidFile: location of PID file
PidFile: /var/run/clamsmtp/clamsmtpd.pid

# Whether or not to bounce email (default is to silently drop)
Bounce: on

# Whether or not to keep virus files
#Quarantine: off

# Enable transparent proxy support
#TransparentProxy: off

# User to run as
User: clamsmtp

# Virus actions: There's an option to run a script every time a
# virus is found. Read the man page for clamsmtpd.conf for details.

VirusAction: /usr/local/bin/clamsmtpvirus.sh
```

Action Script

```
#!/bin/bash
# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
#   WARNING WARNING WARNING WARNING WARNING WARNING WARNING
#
#  By using variables passed in from clamsmtpd in FILE
#  manipulation commands without escaping their contents
#  you are opening yourself up to REMOTE COMPROMISE. You
#  have been warned. Do NOT do the following unless you
#  want to be screwed big time:main.inc.php
#
#  mv $EMAIL "$SENDER.eml"
#
##  An attacker can use the above command to compromise your
#  computer. The only variable that is guaranteed safe in
#  this regard is $EMAIL.
#
```

```
#  The following script does not escape its variables
#  because it only uses them in safe ways.
#
# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

# A sample script for virus actions. When testing make sure
# everything can run as the clamav (or relevant) user.

FILE="/var/log/clamsmtpd.log"
DIR="/var/spool/clamsmtp"

exec 1>>$FILE
exec 2>>$FILE

# Add some fun log lines to the log FILE

echo "------------------------------------------------------------"
echo Sender  $SENDER
echo Recipients  $RECIPIENTS
echo Virus  $VIRUS
echo "------------------------------------------------------------"

# Move the virus FILE to another DIRectory
# This only works if Quarantine is enabled
#
#if [ -n "$EMAIL" ]; then
#       mv "$EMAIL" "$DIR"
#fi

#
MAILNAME="$(cat /etc/mailname)"
ADMIN="postmaster@server"
DATEI=$(echo "$DIR/$(ls -ltr $DIR )" | awk '{print $8}' | tail -n 1)
ZEILE=$(grep -n -v -e [0-9] -e [a-z] -e [A-Z] $DIR/$DATEI \
|awk -F: '{print $1}' |head -n1)
#
#Text fuer die Email
MAILTEXT="
Dies ist der Postfix Mailserver von $MAILNAME

Es tut mir leid Ihnen mitteilen zu muessen, dass Ihre Nachricht
gesendet von: $SENDER
gesendet an: $RECIPIENTS
nicht zugestellt werden konnte. Es wurde ein Virus gefunden!

*** VIRUS ***: $VIRUS

Detailierte Emailkopfzeile der Nachricht:

$(head -n $ZEILE $DIR/$DATEI)
```

```
postmaster@$MAILNAME

"
#
#Mail verschicken
### Mail an den Absender der Virusmail schicken
echo "$MAILTEXT" | mail -s "Ihre Nachricht an $RECIPIENTS,\
$(date)" $SENDER
### Mail an den eigentlichen Empfänger schicken
echo "$MAILTEXT" | mail -s "Virus Email von $SENDER empfangen,\
$(date)" $RECIPIENTS
### Mail an den Admin senden
echo "$MAILTEXT" | mail -s "Virus Email von $SENDER an $RECIPIENTS
empfangen,\
$(date)" $ADMIN
```

master.cf

```
# AV scan filter (used by content_filter)
scan    unix    -       -       n       -       16      smtp
  -o smtp_send_xforward_command=yes

# For injecting mail back into postfix from the filter
127.0.0.1:10025 inet n - n - 16 smtpd
  -o content_filter=
  -o
receive_override_options=no_unknown_recipient_checks,no_header_body_checks
  -o smtpd_helo_restrictions=
  -o smtpd_client_restrictions=
  -o smtpd_sender_restrictions=
  -o smtpd_recipient_restrictions=permit_mynetworks,reject
  -o mynetworks_style=host
  -o smtpd_authorized_xforward_hosts=127.0.0.0/8
```

main.cf

```
content_filter = scan:127.0.0.1:10026
receive_override_options = no_address_mappings
```

Roundcube

Download Plugin / Install

```
cd /var/www/imscp/gui/public/tools/webmail/plugins
wget http://www.tehinterweb.co.uk/roundcube/plugins/sauserprefs.tar.gz
tar -xvzf sauserprefs.tar.gz
chown -R vu2000:www-data sauserprefs
```

Modify sauserprefs

```
vi
/var/www/imscp/gui/public/tools/webmail/plugins/sauserprefs/config.inc.php
```

Add your MySQL Data to connect to the spamassassin DB

```
// spamassassin database settings
$rcmail_config['sauserprefs_db_dsnw'] =
'mysql://spamassassin:YoUrPaSSworD@localhost/spamassassin';
```

Enable Plugins

```
vi /var/www/imscp/gui/public/tools/webmail/config/main.inc.php
```

Add sauserprefs and managesieve

```
$rcmail_config['plugins'] = array('sauserprefs', 'managesieve');
```

ToDo

Spamassassin CronJob
Mark as Junk2
sa-learn
This and that