SpamAssassin и настройка Exim

SpamAssassin можно установить двумя способами:

1. perl -MCPAN -e shell;
2. /usp/ports/mail/spamassassin.

Я ставил из портов. SpamAssassin – это перловый модуль, и для его установки требуется куча зависимостей из тех же перловых модулей. Устанавливаем их:

```
cd /usr/ports/security/p5-Digest-MD5
make install clean
cd /usr/ports/www/p5-HTML-Parser
make install clean
cd /usr/ports/dns/p5-Net-DNS
make install clean
cd /usr/ports/japanese/p5-Mail-SpamAssassin
make install clean
```

Во время установки будет огромная куча вопросов, связанных с функциональностью тех или иных модулей.

После установки настраиваем SpamAssassin.

```
cat /usr/local/etc/mail/spamassassin/local.cf
trusted_networks 192.168.1/24
required_score 5.0

report_safe 0
rewrite_header subject [SPAM]
use_bayes 1
#bayes_path /usr/local/etc/mail/spamassassin/bayes/
bayes_file_mode 0666
bayes_min_spam_num 1
bayes_min_ham_num 1
bayes_learn_to_journal 1
skip_rbl_checks 0
bayes_auto_learn 0

#ok_languages ru en
```

```
ok_locales ru_en

score BAYES_00 0.0001 0.0001 -6.0 -6.0
score BAYES_05 0.0001 0.0001 -3.0 -3.0
score BAYES_20 0.0001 0.0001 -1.0 -1.0
score BAYES_50 0.0001 0.0001 1.6 1.6
score BAYES_60 0.0001 0.0001 2.0 2.0
score BAYES_80 0.0001 0.0001 4.0 4.0
score BAYES_95 0.0001 0.0001 6.5 6.5
score BAYES_99 0.0001 0.0001 10.0 10.0
score RDNS_NONE 0.0001 0.0001 3.0 3.0

score SUBJ_FULL_OF_8BITS 0.00
score HTML_COMMENT_8BITS 0.01
score HEADER_8BITS 0.00
score TO_NO_USER 0.01
score FORGED_MUA_OUTLOOK 0.5
score X_AUTH_WARNING 0.01
score SUBJ_HAS_UNIQ_ID 9.99
score HTTP_USERNAME_USED 9.99
score FORGED_YAHOO_RCVD 9.99
score FORGED_JUNO_RCVD 16
score UNWANTED_LANGUAGE_BODY 1.02
score MLM 5.55
score RCVD_NUMERIC_HELO 4.95
```

Теперь добавляем в конфиг exim’а до acl’ов строчку

```
spamd_address = 127.0.0.1 783
```

и в ACL’ах в правило *acl_check_data*, где *spam* – это *user* под которым стартует *exim*

```
acl_check_data:

#deny  message = Virus found ($malware_name)
        #malware = *

  warn  message = X-Spam-Score: $spam_score ($spam_bar)
        hosts   = !+relay_from_hosts
        spam    = mailnull:true
```

```
  warn  message = X-Spam-Report: $spam_report
        hosts   = !+relay_from_hosts
        spam    = mailnull:true

  warn  message = Subject: [SPAM] $h_Subject:
        hosts   = !+relay_from_hosts
        spam    = mailnull

  deny  message = This message scored $spam_score spam points.
        spam    = mailnull:true
        # Отбрасывает спамовые письма с указанием ошибки
        hosts   = +relay_from_hosts
        condition = ${if >{$spam_score_int}{120}{1}{0}}

  accept
```

Запускаем spamd и рестартим exim

```
echo 'spamd_enable="YES"' >> /etc/rc.conf
/usr/local/etc/rc.d/sa-spamd start
/usr/local/etc/rc.d/exim restart
```

У меня spamd стартовал с *ошибкой* о невозможности создать *user_prefs*. Решил созданием директории по предложенному пути

```
mkdir /var/spool/.spammassassin/
chown -R spamd /var/spool/.spammassassin/
```

Наша связка начинает сразу работать с заранее предустановленными параметрами. Но что бы увеличить вероятность правильного срабатывания для отсеевания спама необходимо систему обучить – скормить ей более 200 писем с примерами “белых писем” **(ham)** и более 200 спамовых писем **(spam)**.

Обучение может производится автоматически, с помощью **bayes_auto_learn** – когда очки письма (без учета очков за AWL, BAYES_XX, BLACKLIST и WHITELIST) выходят за пределы между **auto_learn_threshold_nonspam** и **auto_learn_threshold_spam**. Это можно узнать если в заголовке письма в поле **X-Spam-Status:** присутствует запись **autolearn=spam** или **autolearn=ham**.

И обучение может производиться вручную (или при помощи скрипта) командой **sa-lean**. Для этого нужно скормить каталог писем со спамом **spam** и каталог благонадежных писем **ham**. Письма нужно иметь в не модифицированном виде (без forward`а и прочих почтовых пересылок перенаправлений). Для удобства завёл специальные папочки в которые складывал примеры писем. После накопления необходимого количества писем, экспортировал их на сервер и скормил обучалке:

```
#   /usr/local/bin/sa-learn   --ham   /var/vmail/tst-amo.pp.ua/svm/Maildir/cur
#   /usr/local/bin/sa-learn   --spam   /var/vmail/tst-amo.pp.ua/svm/Maildir/.imp_spam/cur
```

Проверка конфигурации – полный вывод

```
#spamassassin --lint -D
```

Проверка конфигурации – вывод только проблемных мест

```
#spamassassin --lint
```

Если в процессе выводит что то типа

```
 warn: bayes: bayes db version 0 is not able to be used, aborting!
                                                                  at /usr/local/lib/perl5/site_perl/Mail/SpamAssassin/BayesStore/DBM.pm line 208.
```

то выполните команду

```
sa-learn --sync
```

Тест на спам

Отправляем на тестируемые сервер письмо с таким текстом:

```
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
```

Должно получить как минимум 1000 очков и получить гордый титул SPAM.

Пропишем *транспорт* и *роутер* для спама

```
ee /usr/local/etc/exim/configure
```

```
###############
begin routers

check_malware:
 driver = redirect
 condition = ${if def:h_X-Quarantine-Me-Malware: {1}{0}}
 headers_remove = Subject
 headers_add = Subject: [CLAMAV: $acl_m2] $h_Subject
 data = postmaster@tst-amo.pp.ua
 file_transport = address_file

# SpamAssassin
spamcheck_router:
 driver = accept
 condition = "${if and { \
 {!def:h_X-Spam-Flag:} \
 {!eq {$received_protocol}{spam-scanned}} \
 {!eq {$received_protocol}{local}} \
 {!eq {$sender_host_address}{127.0.0.1}} \
 {<{$message_size}{50k}} \
 } {1}{0}}"
 retry_use_local_part
 transport = spamcheck
 no_verify
```

```
##################
begin transports

remote_smtp:
 driver = smtp

# SpamAssassin
spamcheck:
 driver = pipe
 batch_max = 100
 command = /usr/local/sbin/exim -oMr spam-scanned -bS
 current_directory = "/tmp"
 home_directory = "/tmp"
```

```
 group = mail
 user = mailnull
 log_output
 message_prefix =
 message_suffix =
 return_fail_output
 no_return_path_add
 transport_filter = /usr/local/bin/spamc -u mailnull
 use_bsmtp
```

Так как на сервере работает *dovecot* с *sieve*, то работа по сортировке спама ляжет на него.

Сам скрипт для укладывания спама в папку *Junk*

```
require ["regex", "fileinto", "imap4flags"];
# Catch mail tagged as Spam, except Spam retrained and delivered to the mailbox
 if exists "X-Spam-Status"
 {
# Mark as read
 setflag "\\Seen";
# Move into the Junk folder
 fileinto "Junk";
# Stop processing here
 stop;
}
```

Выполнить команду для компиляции sieve скрипта

```
sievec /usr/local/etc/dovecot/sieve/
```