Amavisd-new

Устанавливаем (добавить поддержку MySQL)

```
cd /usr/ports/security/amavisd-new
make config
make install clean
```

```
cd /usr/local/etc
cp amavisd.conf amavisd.conf_orig
```

Редактируем ее amavisd.conf

```
$mydomain = 'example.com';
$MYHOME = '/var/amavis';
```

Остальное оставил по дефолту.

Для Clamav убираем комменты у абзацев

```
@av_scanners = (
 ['ClamAV-clamd',
        \&ask_daemon,         ["CONTSCAN        {}\n",
"/var/run/clamav/clamd.sock"],
 qr/\bOK$/m, qr/\bFOUND$/m,
 qr/^.*?: (?!Infected Archive)(.*) FOUND$/m ],
 );

@av_scanners_backup = (
 ### http://www.clamav.net/ - backs up clamd or Mail::ClamAV
 ['ClamAV-clamscan', 'clamscan',
 "--stdout --no-summary -r --tempdir=$TEMPBASE {}",
  [0], qr/:.*\sFOUND$/m, qr/^.*?: (?!Infected Archive)(.*)
FOUND$/m ],
 );
```

Добавляем в группу clamav пользователя vscan и наоборот

```
pw groupmod clamav -m vscan
pw groupmod vscan -m clamav
```

Делаем запись

```
echo 'amavisd_enable="YES"' >> /etc/rc.conf
```

и запускаем

```
service amavisd start
```

Можно вывести лог amavis-a в отдельный файл

```
ee /etc/syslog.conf
local6.* /var/log/amavisd-new.log
```

```
ee /usr/local/etc/amavisd.conf
$syslog_facility = 'local6';   # Syslog facility as a string
```

Перезапускаем и проверяем, если есть ошибки вида

```
Sep 25 11:50:22 tmail amavis[56730]: (!!)TROUBLE in child_init_hook:
BDB can't connect db env. at /var/amavis/db: BDB0087 DB_RUNRECOVERY: Fatal error,
run database recovery, No such file or directory. at (eval 93) line 338.
```

то меняем в amavisd.conf

```
$enable_db = 0;              # enable use of BerkeleyDB/libdb (SNMP and nanny)
```

Для связи Clamav-Spamassassin-Postfix-Amavis добавляем после определения алиасов

```
ee /usr/local/etc/postfix/main.cf
```

```
# Amavisd-new
content_filter = smtp-amavis:[127.0.0.1]:10024
receive_override_options = no_address_mappings
```

и в файле master.cf дописываем вверху строку с контент фильтром

```
smtp inet n - n - - smtpd
 -o content_filter=smtp-amavis:[127.0.0.1]:10024
```

и в самый низ (после транспорта Довекота)

```
#with virus-scanner amavis
smtp-amavis unix - - - - 2 smtp
 -o smtp_data_done_timeout=1200
 -o smtp_send_xforward_command=yes
 -o disable_dns_lookups=yes
 -o max_use=20

127.0.0.1:10025 inet 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_reci
pient_checks
```

Если в процессе отладки возникнет необходимость полностью *отключить* функции защиты от СПАМа, добавьте строку

```
@bypass_spam_checks_maps = (1);
```

для *полного отключения защиты от вирусов* предназначена строка

```
@bypass_virus_checks_maps = (1);
```

Параметры

$sa_tag_level_deflt - (оценка, при которой к заголовкам добавляются соответствующие X-Spam-тэги),
$sa_tag2_level_deflt - (оценка, при которой сообщения

помечаются как СПАМ), $sa_kill_level_deflt - (оценка, при которой с сообщениями выполняется предопределенные действия, в нашем случае уничтожение)

имеют достаточно гуманные значения, которые вполне меня устраивают. Чем сильнее Вы уменьшите эти числа, тем лучше будет фиксироваться СПАМ, но одновременно возрастет вероятность потери валидных сообщений. Лучше всего определить эти значения экспериментальным путем.

Example:

```
#Если Спам - переслать в ящик
$sa_spam_subject_tag = '***Spam*** ';
#$spam_quarantine_to = 'spam@uni.ka';
$final_spam_destiny = D_PASS; # D_PASS / D_DISCARD / D_REJECT
$final_virus_destiny = D_DISCARD; # (defaults to D_BOUNCE)
$final_banned_destiny = D_BOUNCE; # (defaults to D_BOUNCE)
$final_bad_header_destiny = D_PASS;
```

В этом примере, при очках более 10 письмо помечается как спам (дописывается в тему ***Spam***) и доставляется пользователю.

Если сделать

$final_spam_destiny = D_DISCARD

то письмо пользователю не доставляется, а сохраняется в директории */var/amavis/* под именем *spam****.gz* (там же хранятся и virus и bounce)

и если

D_REJECT

то письмо отбрасывается.

Если раскоментировать

#$spam_quarantine_to = 'spam@uni.ka';

то письмо перешлется на ящик spam@uni.ka.

Т.е. если нужно, что бы письма, помеченные как спам, пользователю не доставлялись, а пересылались на спам ящик, то:

```
### Если Спам - перслать в ящик
$sa_spam_subject_tag = '***Spam*** ';
$spam_quarantine_to = 'spam@uni.ka';
$final_spam_destiny = D_DISCARD
$final_virus_destiny = D_DISCARD; # (defaults to D_BOUNCE)
$final_banned_destiny = D_BOUNCE; # (defaults to D_BOUNCE)
$final_bad_header_destiny = D_PASS;
```

D_REJECT - отклонять письма с сообщением вида

```
The mail system
<acc@uni.ka>: host 127.0.0.1[127.0.0.1] said: 554 5.7.0
Reject, id=38216-01 -
    spam (in reply to end of DATA command)
```

Команда *amavisd-release* осуществляет доставку попавшего в карантин письма его получателю

```
# cd /var/virusmails
# amavisd-release spam-yVhEw7tY3+tr.gz
250 2.0.0 Ok, id=rel-yVhEw7tY3+tr, from
MTA([127.0.0.1]:10025): 250 2.0.0 Ok: queued as 93F4561C1C
```

Черные и белые списки

1. вариант – мягкий блэклист

в секции добавляем нужный адрес/домен и балы (позитив – черный, негатив – белый), например:

```
    'clusternews@linuxnetworx.com' => -3.0,
   # soft-blacklisting (positive score)
    'sender@example.net' => 3.0,
    'spam@com' => 10.0,
   },
  ], # end of site-wide tables
});
```

2. вариант – черные и белые списки

```
   },
```

```
  ], # end of site-wide tables
});
### BEGIN White and black lists!!!
read_hash(\%whitelist_sender, '/var/amavis/whitelist');
read_hash(\%blacklist_sender, '/var/amavis/blacklist');
#read_hash(\%spam_lovers, '/var/amavis/spam_lovers');
### END
```

```
# cat /var/amavis/blacklist
 126.com
 marketing@sw.solarwinds.com
 info@twitter.com
```

```
# cat /var/amavis/whitelist
 root@domen.com
 mail.domen.com
 domen.com
 root@mail.domen.com
```

Эти варианты можно комбинировать.

3. вариант (еще не пробовал)

1) I created the file /etc/amavisd/whitelist
where I inserted the addresses of the senders that I wanted to whitelist, one per line.
it works also for whole domains (but without the @)

Example:

```
user1@example.com
 user2@example.org
 example.net
 example.eu
```

2) in /etc/amavisd/amavisd.conf I decommented AND modified the following section:

```
# This policy will perform virus checks only.
 read_hash(\%whitelist_sender, '/etc/amavisd/whitelist');
 @whitelist_sender_maps = (\%whitelist_sender);

$interface_policy{'10026'} = 'VIRUSONLY';
```

```
 $policy_bank{'VIRUSONLY'} = { # mail from the pickup daemon
  bypass_spam_checks_maps  =>  ['@whitelist_sender_maps'],  #
don't spam-check this mail
  bypass_banned_checks_maps  =>  ['@whitelist_sender_maps'],  #
don't banned-check this mail
  bypass_header_checks_maps  =>  ['@whitelist_sender_maps'],  #
don't header-check this mail
 };
```