# Exim + Dovecot (без MySQL – системные пользователи)

1. Устанавливаем **Exim**

```
# cd /usr/ports/mail/exim
# make install clean
```

**Опции** установки выбрал такие (с заделом на будущее)

2. Отредактируем файл **/etc/mail/mailer.conf**, заменив *sendmail* на *exim*.

```
 sendmail /usr/local/sbin/exim
 send-mail /usr/local/sbin/exim
 mailq /usr/local/sbin/exim -bp
 newaliases /usr/local/sbin/exim -bi
 hoststat /usr/local/sbin/exim
 purgestat /usr/local/sbin/exim
```

Обратите внимание, что в двух строках появились ключи.

3. Создаем **рабочие папки для домена** (или доменов – если нужно) и **почтового ящика**.

```
# mkdir -p /var/vmail/
# chown -R mailnull:mail /var/vmail
```

4. Конфигурационный файл принял такой вид

```
 # CONF EXIM + MYSQL + DOVECOT + CLAMAV
 # Авторизация - довекот. квоты, кламав, БД в мускуле и системные - в файле

 # Имя нашей почтовой системы
 primary_hostname = mail.tst-amo.pp.ua

 # хост/БД/пользователь/пароль
```

```
 mysql_servers = localhost/mail/mailreader/

 # Список доменов нашей почтовой системы
 domainlist local_domains = ${lookup mysql{select domain from
domains where  domain='${domain}'}}

 # Логгирование
 log_selector = +all
 log_file_path = /var/log/exim/%D-%slog

 # Список доменов, для которых наша почтовая система является
резервной
 domainlist relay_to_domains = ${lookup mysql{select domain
from domains where domain='${domain}'}}
 hostlist relay_from_hosts = localhost : 127.0.0.1 :
192.168.1.0/24 : 194.44.219.160/28 : 194.44.31.34
 acl_smtp_rcpt = acl_check_rcpt
 acl_smtp_mime = acl_check_mime

 # Прикручиваем антивирус - при условии, что exim собран
 # с его поддержкой. В качестве антивиря юзаем ClamAV,
 # ибо - ПО должно быть свободным! :)
 # Итак, указываем местоположение сокета clamd.
 acl_smtp_data = acl_check_data
 av_scanner = clamd:/var/run/clamav/clamd.sock

 # Адрес куда слать на проверку спама (SpamAssasin), но я
 # это не юзаю. Не так много у меня спама...
 # spamd_address = 127.0.0.1 78

 # SSL
 tls_certificate = /etc/ssl/certs/dovecot.pem
 tls_privatekey = /etc/ssl/private/dovecot.pem

 # Отключаем IPv6
 disable_ipv6

 #порт smtp
 daemon_smtp_ports = 25 : 465
 tls_on_connect_ports = 465
```

```
 # Дописываем домены отправителя и получателя, если они не
указаны
 qualify_domain = tst-amo.pp.ua
 qualify_recipient = tst-amo.pp.ua

 allow_domain_literals = false
 exim_user = mailnull
 exim_group = mail

 never_users = root

 # Проверять прямую и обратную записи узла отправителя по DNS
 host_lookup = *

 # Отключаем проверку пользователей узла отправителя по
протоколу ident
 rfc1413_hosts = *
 rfc1413_query_timeout = 5s

 # Запрещаем использовать знак % для явной маршрутизации почты
 #percent_hack_domains =

 # Настройки обработки ошибок доставки, используются значения
по умолчанию
 ignore_bounce_errors_after = 2h
 timeout_frozen_after = 7d

 return_size_limit = 10K
 split_spool_directory = true
 syslog_timestamp = no

 # Лимит размера сообщения (50 мегабайт default)
 message_size_limit = 1000M

 ################
 ### конфигурация ACL для входящей почты
 begin acl

 # Эти правила срабатывают для каждого получателя
 acl_check_rcpt:
```

```
 # принимать сообщения которые пришли с локалхоста,
 # не по TCP/IP
   accept  hosts = :

 # Запрещаем письма содержащие в локальной части
 # символы @; %; !; /; |. Учтите, если у вас было
 # `percent_hack_domains` то % надо убрать.
 # Проверяются локальные домены
 deny    message       = "incorrect symbol in address"
 domains       = +local_domains
 local_parts   = ^[.] : ^.*[@%!/|]

 # Проверяем недопустимые символы для
 # нелокальных получателей:
 deny    message       = "incorrect symbol in address"
 domains       = !+local_domains
 local_parts   = ^[./|] : ^.*[@%!] : ^.*/\\.\\./

 # Принимаем почту для постмастеров локальных доменов без
 # проверки отправителя (я закомментировал, т.к. это -
 # основной источник спама с мой ящик).

 accept  local_parts   = postmaster
 domains       = +local_domains

 # Запрещаем, если невозможно проверить отправителя
 # (отсутствует в списке локальных пользователей)
 # У себя я это закоментил, по причине, что некоторые
 # железяки (принтеры, & etc) и программы (Касперский, DrWEB)
 # умеют слать почту, в случае проблем но не умеют ставить
 # нужного отправителя. Такие письма эта проверка не пускает.
 #  require verify        = sender

 # Запрещаем тех, кто не обменивается приветственными
 # сообщениями (HELO/EHLO)

 deny    message       = "HELO/EHLO require by SMTP RFC"
                           condition               =   ${if
eq{$sender_helo_name}{}{yes}{no}}
 # Принимаем сообщения от тех, кто аутентифицировался:
 # Вообще, большинство конфигов в рунете - это один и тот же
```

```
 # конфиг написанный Ginger, в котором этот пункт расположен
 # внизу. Но при таком расположении рубятся клиенты с adsl,
 # ppp, и прочие зарезанные на последующих проверках. Но это
 # же неправильно! Этом мои пользователи из дома! Потому
 # я это правило расположил до проверок.

 accept  authenticated = *
 # Рубаем нах, тех, кто подставляет свой IP в HELO
 deny    message       = "Your IP in HELO - access denied!"
           hosts           =  * : !+relay_from_hosts :
!81-196.lissyara.su
         condition     = ${if eq{$sender_helo_name}\
                           {$sender_host_address}{true}{false}}

  # Рубаем тех, кто в HELO пихает мой IP (2500 мудаков за
месяц!)
 deny    condition     = ${if eq{$sender_helo_name}\
                           {$interface_address}{yes}{no}}
         hosts         = !127.0.0.1 : !localhost : *
          message        = "main IP in your HELO! Access
denied!"

 # Рубаем тех, кто в HELO пихает только цифры
 # (не бывает хостов ТОЛЬКО из цифр)
 deny    condition     = ${if match{$sender_helo_name}\
                           {\N^\d+$\N}{yes}{no}}
         hosts         = !127.0.0.1 : !localhost : *
         message       = "can not be only number in HELO!"

 # Рубаем хосты типа *adsl*; *dialup*; *pool*;....
 # Нормальные люди с таких не пишут. Если будут
 # проблемы - уберёте проблемный пункт (у меня клиенты
 # имеют запись типа asdl-1233.zone.su - я ADSL убрал...)
 deny    message       = "your hostname is bad (adsl, poll,
ppp & etc)."
         condition     = ${if match{$sender_host_name} \
                           {adsl|dialup|pool|peer|dhcp} \
                           {yes}{no}}
 # Задержка. (это такой метод борьбы со спамом,
 # основанный на принципе его рассылки) На этом рубается
 # почти весь спам. Единственно - метод неприменим на
```

```
 # реально загруженных MTA - т.к. в результате ему
 # приходится держать много открытых соединений.
 # но на офисе в сотню-две человек - шикарный метод.
 #
 # более сложный вариант, смотрите в статье по exim и
 # курьер имап. Т.к. там метод боле умный (просто правил
 # больше :), то можно и на более загруженные сервера ставить)

warn
 # Ставим дефолтовую задержку в 30 секунд
   set acl_m0 = 30s
 warn
 # ставим задержку в 0 секунд своим хостам и
 # дружественным сетям (соседняя контора :))
 hosts = +relay_from_hosts:192.168.1.0/24:194.44.219.160/28
   set acl_m0 = 0s
 warn
 # пишем в логи задержку (если оно вам надо)
   logwrite = Delay $acl_m0 for $sender_host_name \
                            [$sender_host_address]  with
HELO=$sender_helo_name.  Mail  \
              from $sender_address to $local_part@$domain.
      delay = $acl_m0

 # Проверка получателя в локальных доменах.
 # Если не проходит, то проверяется следующий ACL,
 # и если непрошёл и там - deny
 accept  domains       = +local_domains
         endpass
          message       = "In my mailserver not stored this
user"
         verify        = recipient

 # Проверяем получателя в релейных доменах
 # Опять-таки если не проходит -> следующий ACL,
 # и если непрошёл и там - deny
 accept  domains       = +relay_to_domains
         endpass
          message       = "main server not know how relay to
this address"
         verify        = recipient
```

```
 # Рубаем тех, кто в блэк-листах. Серваки перебираются
 # сверху вниз, если не хост не найден на первом, то
 # запрашивается второй, и т.д. Если не найден ни в одном
 # из списка - то почта пропускается.
 deny    message       = you are in blacklist: $dnslist_domain
--> $dnslist_text
         dnslists      = opm.blitzed.org : \
                         cbl.abuseat.org : \
             #           bl.csma.biz : \
                         dynablock.njabl.org

 # Разрешаем почту от доменов в списке relay_from_hosts
 accept  hosts         = +relay_from_hosts

 # Если неподошло ни одно правило - чувак явно ищет
 # открытый релей. Пшёл прочь. :)
 deny    message       = "relay not permitted"

 ###############
 # Проверка вложений
 acl_check_mime:
 deny message = Данной сообщение содержит опасное вложение
   condition = ${if match{$mime_filename}{\N(?i)\.zip$\N}}
   decode = default
     condition = ${if match{${run{/usr/bin/unzip -l
$mime_decoded_filename}}}{\N(?i)\.(exe|com|vbs|bat|pif|scr|hta
|js|cmd|chm|cpl|jsp|reg|vbe|lnk|dll|sys)\n\N}}
          log_message    =    forbidden    attachment:
filename=$mime_filename,   content-type=$mime_content_type,
recipients=$recipients

 deny message = Данной сообщение содержит опасное вложение
   condition = ${if match{$mime_filename}{\N(?i)\.rar$\N}}
   decode = default
     condition = ${if match{${run{/usr/bin/unrar l
$mime_decoded_filename}}}{\N(?i)\.(exe|com|vbs|bat|pif|scr|hta
|js|cmd|chm|cpl|jsp|reg|vbe|lnk|dll|sys)\n\N}}
          log_message    =    forbidden    attachment:
filename=$mime_filename,   content-type=$mime_content_type,
recipients=$recipients
 accept
```

```
###############
# Тут идут ACL проверяющие содержимое (тело) письма.
# Без них будут пропускаться все сообщения.

acl_check_data:

# Заблокированные аккаунты
    deny senders  = /usr/local/etc/exim/deny_senders
         message  = "DENY!!!"

# Проверка на вирусы
    deny message = VIRUS found ($malware_name)
    malware = *
    accept

###############
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

dnslookup:
  driver = dnslookup
  domains = ! +local_domains
  transport = remote_smtp
  ignore_target_hosts = 0.0.0.0 : 127.0.0.0/8
  no_more

system_aliases:
  driver = redirect
  allow_fail
  allow_defer
 #  data = ${lookup mysql{select alias from aliases where
email='${quote_mysql:$local_part}'               and
domain='${quote_mysql:$domain}'}}
   data = ${lookup mysql{select alias from aliases where
```

```
email='${quote_mysql:$local_part}' }}
   user = mailnull
   group = mail
   file_transport = address_file
   pipe_transport = address_pipe

 system_aliases2:
   driver = redirect
   allow_fail
   allow_defer
   data = ${lookup{$local_part}lsearch{/etc/aliases}}
   user = mailnull
   group = mail
   file_transport = address_file
   pipe_transport = address_pipe

 userforward:
   driver = redirect
   check_local_user
   no_verify
   no_expn
   check_ancestor
   file_transport = address_file
   pipe_transport = address_pipe
   reply_transport = address_reply
 #  data = ${lookup mysql{select alias from aliases where
email='${quote_mysql:$local_part}'                and
domain='${quote_mysql:$domain}'}}
    data = ${lookup mysql{select alias from aliases where
email='${quote_mysql:$local_part}' }}

 userforward2:
   driver = redirect
   check_local_user
   file = $home/.forward
   no_verify
   no_expn
   check_ancestor
   file_transport = address_file
   pipe_transport = address_pipe
   reply_transport = address_reply
```

```
   condition = ${if exists{$home/.forward} {yes} {no} }

 localuser:
   driver = accept
    domains = ${lookup mysql{select domain from domains where
domain='${domain}'}}
   local_parts = ${lookup mysql{select email from users where
email='${local_part}'}}
   transport = local_delivery
   cannot_route_message = Unknown user

 localuser2:
   driver = accept
   check_local_user
   transport = local_delivery
   transport_current_directory = /
   cannot_route_message = Unknown user

 ####################
 begin transports

 remote_smtp:
   driver = smtp

 local_delivery:
   driver = appendfile
   maildir_format
   maildir_tag = ,S=$message_size
 #  directory = /home/mail/$domain/$local_part
   directory = /var/vmail/$local_part/Maildir
   create_directory
   delivery_date_add
   envelope_to_add
   return_path_add
   group = mail
   mode = 0660
   no_mode_fail_narrower

 address_pipe:
   driver = pipe
   return_output
```

```
address_file:
  driver = appendfile
  delivery_date_add
  envelope_to_add
  return_path_add

address_reply:
  driver = autoreply

begin retry
*                      *           F,2h,15m; G,16h,1h,1.5;
F,4d,6h

begin rewrite

###############
begin authenticators

# Для системных пользователей через EXIM
#LOGIN:
#    driver = plaintext
#    public_name = LOGIN
#    server_prompts = "Username:: : Password::"
#    server_condition = "${if pam {$auth1:$auth2}{yes}{no}}"
#    server_set_id = $auth1

#PLAIN:
#    driver = plaintext
#    public_name = PLAIN
#    server_condition = "${if pam {$auth2:$auth3}{yes}{no}}"
#    server_set_id = $auth2


# Аутентификация через dovecot
dovecot_login:
driver = dovecot
public_name = LOGIN
server_socket = /var/run/dovecot/auth-client
server_set_id = $auth1

dovecot_plain:
```

```
 driver = dovecot
 public_name = PLAIN
 server_socket = /var/run/dovecot/auth-client
 server_set_id = $auth1

 dovecot_cram_md5:
 driver = dovecot
 public_name = CRAM-MD5
 server_socket = /var/run/dovecot/auth-client
 server_set_id = $auth1

 ########################
```

5. Отключаем sendmail и включаем exim:

```
# ee /etc/rc.conf
sendmail_enable="NONE"
sendmail_submit_enable="NO"
exim_enable="YES"
```

11. Отправим тестовое письмо.

```
# mail -s ‘First letter for sentec mail server’ info@sentec.ru
 This is test message!
 .
 EOT
#
```

Посмотрим, что в лог-файле:

```
# tail /var/log/exim/mainlog
```

Вот примерная картинка, которую мы увидим в случае успеха:

```
2010-10-26 21:34:24 1PAnPk-0005al-AG <= root@mail.sentec.ru
U=root P=local S=323
2010-10-26 21:34:24 1PAnPk-0005al-AG => info <info@sentec.ru>
R=localuser
T=local_delivery  2010-10-26  21:34:24  1PAnPk-0005al-AG
Completed
```

12. Теперь надо сделать так, чтобы мы смогли *получать почту* с нашего сервера.

Для этого ставим проверенный и надежный POP/IMAP-сервер **Dovecot** (голубятня :)).

```
# cd /usr/ports/mail/dovecot
# make install clean
```

13. Создадим….

14. Создадим **SSL-сертификаты** (если нужен шифрованный трафик, если нет – пропускаем). Информация об издателе будет взята из файла *dovecot-openssl.cnf*.

```
# mkdir -p /etc/ssl/certs
# mkdir -p /etc/ssl/private
# /usr/local/share/examples/dovecot/mkcert.sh
# ls -l /etc/ssl/certs && ls -l /etc/ssl/private
```

15. Запускаем dovecot.

```
# /usr/local/etc/rc.d/dovecot start
```

16. Настраиваем почтового клиента на получение-отправку почты с помощью разрешенных протоколов (SMTP/POP3/IMAP). Не забудьте, что в */etc/rc.firewall* должны быть разрешены соответствующие порты: *25, 110, 143, 993*.
На этом – все.