

# Сервер "Sendmail"

November 27, 2016

## Передача сообщений

Электронные сообщения создаются при помощи программ почтового интерфейса - например, программы mail. Эти программы называют почтовыми агентами пользователя (MUA). Когда посылается сообщение, интерфейсная программа обычно передает его другой программе для дальнейшей пересылки. Такая программа называется почтовым транспортным агентом (MTA). MTA не используется для написания писем. Ее задача - отправить локальную почту MTA в другую систему.

Локальная пересылка почты не ограничивается простым присоединением входящего сообщения к почтовому ящику получателя. Обычно локальные MTA поддерживают работу с псевдонимами (aliasing). Кроме того, сообщение, которое по каким-то причинам не может быть доставлено, должно возвращаться отправителю с добавленным сообщением об ошибке.

При удаленной пересылке почты используемая транспортная программа обычно определяется природой канала связи. При использовании каналов TCP/IP обычно применяется протокол SMTP. Выступая в роли протокола "сервер-сервер", SMTP требует дополнительного протокола, типа POP3 или IMAP, для локального сбора и обработки сообщений и их доставки конкретным пользователям. Протокол SMTP проектировался с расчетом на то, чтобы почта доставлялась прямо на компьютер получателя, а процесс пересылки согласовывался с демоном SMTP, работающим на удаленном конце. Протокол SMTP наделяется дополнительными возможностями благодаря протоколу ESMTP (Extended Simple Mail Transport Protocol). К таким возможностям относятся, в частности, 8-битовое кодирование MIME без применения типа base64 и возможность получения сервером сведений о размере сообщения (при использовании SMTP единственным способом отказа от приема слишком больших сообщений было получение их целиком и последующее уничтожение, что, естественно, создавало дополнительную нагрузку на сеть).

В обязанности MTA также входит и маршрутизация почты (так, письмо, отправляемое пользователю той же локальной системы, передается непосредственно локальному MDA - Mail Delivery Agent).

В задачи MDA входит обработка приходящих сообщений. Так sendmail, получив сообщение, вызывает MDA для его передачи из очереди sendmail в очередь MUA. Чаще всего эту роль выполняют /bin/mail и procmail.

## Схема работы почтового сервера

### Sendmail 8.12+ E-mail Flow, Configuration Files, Queue Directories, and Logging.

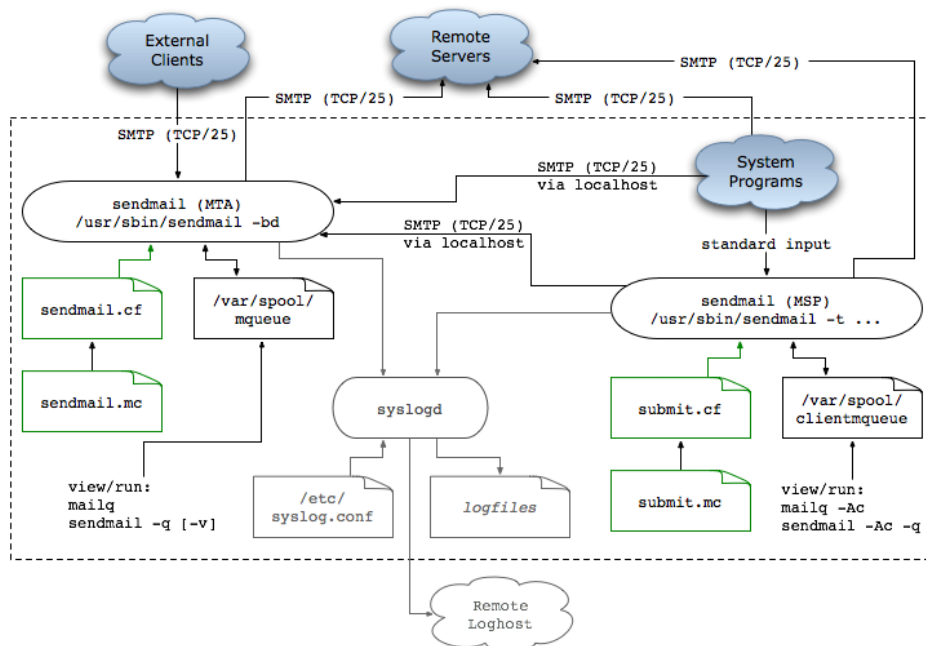


Рис. 1

## Маршрутизация

Процедура направления сообщения на узел получателя называется маршрутизацией (routing). Кроме определения маршрута от отправителя к получателю, маршрутизация подразумевает также проверку на ошибки и оптимизацию скорости и затрат.

В интернете выполнение процедуры маршрутизации зависит от конфигурации узла назначения. По умолчанию сначала определяется узел, на который должно быть доставлено сообщение, после чего сообщение передается на узел назначения напрямую. В большинстве сетей с подключением к Интернету вся входящая почта обычно направляется на специализированный, наиболее доступный почтовый сервер, способный поддерживать большую нагрузку. Этот почтовый сервер осуществляет дальнейшую пересылку почты на локальные сетевые узлы. Чтобы объявить о предоставлении такого рода услуг, сетевой узел должен обладать соответствующей ему записью MX в базе данных DNS. Запись MX означает Mail Exchanger (сервер обмена почтовыми сообщениями) и указывает на то, что данный сетевой узел выполняет функции почтового сервера домена.

Каждая запись MX содержит параметр приоритета. Это положительное целое число. Если почтовое сообщение, адресованное некоторому сетевому узлу может быть доставлено к месту назначения при помощи одного из

нескольких почтовых серверов, почтовый транспортный агент будет пытаться переслать сообщение на сервер MX, у которого этот параметр имеет наименьшее значение, и только в случае неудачи сообщение будет передано на сервер с более высоким значением параметра приоритета. Если локальный узел сам является почтовым сервером для получателя сообщения, он не имеет права пересылать почтовое сообщение на серверы MX с большим значением приоритета, чем его собственный. Таким образом удается избежать передачи почтовых сообщений по замкнутому кругу. Если для домена не осталось ни одной подходящей записи MX или такой записи вообще не существует, транспортный агент проверяет, не связан ли с узлом IP-адрес и пытается доставить почту прямо на узел.

Допустим, в организации VasiyaPupkin, вся почта обрабатывается компьютером mail. В базу данных DNS включаются записи MX следующего вида:

```
boss.vasiyapupkin.org. IN MX 5 mail.vasiyapupkin.org.
```

Это означает, что компьютер mail.vasiyapupkin.org является почтовым сервером для домена boss.vasiyapupkin.org со степенью приоритета 5. Узел, собирающийся передать сообщение для joe@boss.vasiyapupkin.org, сначала обратится к DNS и обнаружит запись MX со ссылкой на mail. Если в базе данных DNS не будет записей MX, относящихся к этому же домену и с приоритетом ниже 5, сообщение будет передано mail, который в дальнейшем перешлет его на boss.

Это только приблизительное описание принципа работы MX, более подробная информация о маршрутизации почты изложена в RFC-821, RFC-974, RFC-1123.

## Настройка

Sendmail использует следующие файлы настройки:

`/etc/mail/access` - файл базы данных доступа sendmail

`/etc/mail/aliases` - синонимы почтовых ящиков

`/etc/mail/local-host-names` - список хостов, для которых sendmail принимает почту

`/etc/mail/mailertable` - таблица доставки почтовой программы

`/etc/mail/sendmail.cf` - основной файл настройки sendmail

`/etc/mail/submit.cf`

`/etc/mail/virtusertable` - таблица виртуальных пользователей и доменов

### `/etc/mail/access`

База данных доступа определяет список хостов или IP адресов, имеющих доступ к локальному почтовому серверу, а также тип предоставляемого доступа. Хосты могут быть перечислены как OK, REJECT, RELAY, DISCARD или просто переданы процедуре обработки ошибок sendmail с заданным сообщением об ошибке. Хостам, перечисленным с параметром по умолчанию OK, разрешено отправлять почты на этот хост, если адрес назначения почты принадлежит локальной машине. Все почтовые соединения от хостов, перечисленных с параметром REJECT, отбрасываются. Параметр DISCARD применяется в случае, если необходимо отклонить почту без уведомления.

Для хостов, перечисленных с параметром RELAY, разрешена передача через этот сервер почты с любым адресом назначения.

Пример:

```
cyberspammer.com 550 We do not accept mail from spammers
FREE.STEALTH.MAILER@ 550 We do not accept mail from spammers
another.source.of.spam REJECT
okay.cyberspammer.com OK
128.32 RELAY
```

В этом примере приведены пять записей. К отправителям, чей адрес соответствует записи в левой части таблицы, применяется правило записанное в правой части таблицы. В первых двух примерах код ошибки будет передан процедуре обработки ошибок sendmail. В этом случае на удаленном хосте будет получено соответствующее сообщение. В следующем примере почта отбрасывается почта от определенного хоста, another.source.of.spam. В четвертом примере разрешается прием почты от хоста okay.cyberspammer.com, имя которого более точно совпадает с этой записью, чем с cyberspammer.com в примере выше. При более точном совпадении правила перезаписываются. В последнем примере разрешается пересылка почты от хостов с IP адресами, начинающимися с 128.32. Эти хосты смогут отправлять почту через этот почтовый сервер для других почтовых серверов.

### **/etc/mail/aliases**

База данных синонимов содержит список виртуальных почтовых ящиков, принадлежащих другим пользователям, файлам, программам, или другим синонимам.

Пример:

```
root: localuser
ftp: joe,eric,paul
bit.bucket: /dev/null
```

Формат файла прост; имя почтового ящика слева от двоеточия сопоставляется назначению(ям) справа. В первом примере производится сопоставление почтового ящика root почтовому ящику localuser, для которого затем опять будет произведен поиск в базе данных синонимов. Если совпадений не обнаружится, сообщение будет доставлено локальному пользователю localuser. В следующем примере приведен список рассылки. Почта на адрес ftp рассылается на три локальных почтовых ящика: joe, eric и paul. Обратите внимание, что удаленный почтовый ящик может быть задан в виде <user@example.org>. В следующем примере показана запись почты в файл, в данном случае /dev/null.

### **/etc/mail/local-host-names**

В этом файле находится список имен хостов, принимаемых программой sendmail в качестве локальных. Поместите в этот файл любые домены или хосты, для которых sendmail должен принимать почту. Например, если этот почтовый сервер должен принимать почту для домена example.com и

хоста mail.example.com, его файл local-host-names может выглядеть примерно так:

```
example.org
mail.example.org
```

### **`/etc/mail/sendmail.cf`**

Основной файл настройки sendmail, sendmail.cf управляет общим поведением sendmail, включая все, от перезаписи почтовых адресов до отправки удаленным серверам сообщений об отказе от пересылки почты. Основной файл настройки sendmail может быть собран из макроса m4, определяющего возможности и поведение sendmail.

Макропроцессор m4 генерирует файл sendmail.df, когда обрабатывает макрофайл конфигурации, созданный локальным администратором системы. Обычно он называется sendmail.mc.

Процесс конфигурации, в основном, вопрос создания подходящего файла sendmail.mc, который включает макрокоманды, описывающие желательную конфигурацию. Макрокоманды представляют собой выражения, которые макропроцессор m4 понимает и разворачивает в синтаксис файла sendmail.cf. Макровыражения составлены из макроимени (текст в заглавных буквах в начале), которое может быть уподоблено функции в языках программирования, и некоторых параметров (текст внутри скобок), которые используются в расширении. Параметры могут быть переданы буквально в генерируемый файл sendmail.cf или использоваться, чтобы управлять путем, которым происходит обработка данной макрокоманды в подготовленном файле sendmail.mc.

Подробнее этот процесс описан в файле `/usr/share/sendmail/cf/README`.

### **`/etc/mail/sendmail.mc`**

Несколько элементов в файле sendmail.mc требуются всегда. Другие могут игнорироваться, если Вы можете избежать неприятностей со значениями по умолчанию. Общая последовательность определений в файле sendmail.mc такая:

```
VERSIONID
OSTYPE
DOMAIN
FEATURE
Local macro definitions
MAILER
LOCAL_* rulesets
```

### **Комментарии (Comments)**

Строки в sendmail.mc, которые начинаются с #, не обрабатываются m4 и будут по умолчанию выводиться непосредственно в файл sendmail.cf.

Допустимы комментарии в sendmail.mc, которые не попадут в файл sendmail.cf: можно использовать лексемы m4 divert и dnl. Команда divert(-1) прекратит весь вывод, divert(0) восстановит его к значению по умолчанию. Любой вывод, сгенерированный строками между ними будет отброшен.

Чтобы достичь того же самого результата для одной строки, можно использовать команду `dnl`, которая означает, буквально, "удаление всех символов следующей строки и перевод на новую строку".

Это стандартные свойства `m4`, и Вы можете получить больше информации относительно их из `man`-страницы.

## VERSIONID и OSTYPE

```
VERSIONID('@(#)sendmail.mc 8.9 (Linux) 01/10/98')
```

Макрокоманда `VERSIONID` факультативная, но полезно записать версию конфигурации `sendmail` в файл `sendmail.cf`. В любом случае убедитесь в наличии:

```
OSTYPE('linux')
```

Это, вероятно, наиболее важное определение. Макрокоманда `OSTYPE` заставляет включить файл определений, которые являются хорошими значениями по умолчанию для Вашей операционной системы. Большинство определений в файле `OSTYPE` устанавливают имена различных файлов конфигурации, имена разных служебных каталогов и имя почтовой программы. Стандартный комплект исходных кодов `sendmail` включает такой файл для Linux. Многие дистрибутивы Linux, особенно Debian, имеют собственный файл определения, который является полностью совместимым с Linux-FHS. При наличии такого файла следует использовать именно его, а не поставляемую в комплекте с `sendmail` версию.

Определение `OSTYPE` должно располагаться поближе к началу файла `sendmail.mc`, так как много других определений зависят от него.

## DOMAIN

Макрокоманда `DOMAIN` полезна, когда имеется желание конфигурировать большое количество машин одним способом.

Стандартная установка имеет каталог шаблонов макрокоманд `m4`, используемых, чтобы управлять процессом конфигурации. Этот каталог обычно называется `/usr/share/sendmail/cf`. Здесь можно найти подкаталог, названный `domain`, содержащий проблемно-зависимые шаблоны конфигурации. Для использования определения `DOMAIN`, надо создать свой файл, содержащий стандартные определения для соответствующего домена, и вписать его в каталог `domain`.

Пакет исходных кодов `sendmail` приходит с рядом типовых файлов макрокоманд `domain`, которые можно использовать как примеры при построении своего.

Если был сохранён собственный файл макрокоманды `domain` как `/usr/share/sendmail/cf/domain/vbrew.m4`, надо включить в файл `sendmail.mc` определение:

```
DOMAIN('vbrew')
```

## FEATURE

Макрокоманда `FEATURE` позволяет включить предопределенные свойства `sendmail` в конфигурацию. Эти свойства `sendmail` делают конфигурации очень простыми в использовании. Для этого надо включить в файл `sendmail.mc` строку наподобие:

```
FEATURE(name)
```

где name задает имя свойства. Некоторые свойства берут один факультативный параметр. Если надо использовать нечто отличное от значения по умолчанию, то запись должна в виде следующей:

```
FEATURE(name, param)
```

где param задает параметр.

### **Локальные макроопределения**

Стандартные макрофайлы конфигурации sendmail обеспечивают большое количество обработчиков прерываний и переменных, с помощью которых можно настроить конфигурацию. Они названы локальными макроопределениями (local macro definitions) . Многие из них перечислены в файле CF в пакете с исходными кодами sendmail.

Локальные макроопределения обычно вызываются, по имени с указанием изменяемого параметра.

### **Определение протокола транспортировки почты**

Если имеется желание использовать sendmail для передачи нелокальной почты, то надо сообщить какой транспорт использовать. Макрокоманда MAILER делает это очень простым. Текущая версия sendmail поддерживает ряд протоколов транспорта почты. Некоторые из них экспериментальны, другие, вероятно, очень редко используются.

Транспорт local включен по умолчанию. Если Вы включаете оба транспорта, smtp и uucp, Вы должны всегда убедиться, что определили smtp первым.

Обычно используемые транспорты, доступные в макрокоманде MAILER, описаны в следующем списке:

**local**

Этот транспорт включает локальный агент поставки, используемый, чтобы послать почту в почтовый ящик пользователя на этой машине, и агент prog используемый, чтобы послать сообщения локальным программам. Этот транспорт включен по умолчанию.

**smtp**

Этот транспорт осуществляет Simple Mail Transport Protocol (SMTP), который является наиболее общим средством транспортировки почты в Internet. Кроме этого транспорта четыре агента будут сконфигурированы: smtp (нормальный SMTP), esmtp (расширенный SMTP), smtp8 (8-битный двоичный SMTP) и relay (специально разработан для шлюзования писем между разными хостами).

**uucp**

Транспорт uucp обеспечивает поддержку двух агентов: uucp-old, который является традиционным UUCP, и uucp-new, который позволяет указывать много получателей, которые будут обработаны в одной передаче сразу.

**usenet**

Этот агент позволяет посылать сообщения почты непосредственно в сети Usenet. Любое локальное сообщение, направленное к адресу news.group.usenet, будет подано в сеть новостей для группы новостей news.group.

**fax**

При имеющемся установленном программном обеспечении NylaFAX, этот агент позволит направлять письма так, что можно будет создать шлюз email-fax.

Имеются и другие агенты, например, pop, prosmail.

## **/etc/mail/virtusertable**

Файл virtusertable сопоставляет виртуальные почтовые домены и почтовые ящики реальным почтовым ящикам. Эти почтовые ящики могут быть локальными, удаленными, синонимами, определенными в /etc/mail/aliases, или файлами.

Пример:

```
root@example.org root
postmaster@example.org postmaster@noc.example.net
@example.com joe
```

В примере выше наблюдается сопоставление адресов для домена example.org. Почта обрабатывается по первому совпадению с записью в этом файле. Первая запись сопоставляет адрес <root@example.org> локальному почтовому ящику root. Вторая запись сопоставляет <postmaster@example.org> локальному почтовому ящику postmaster на хосте noc.example.net. Наконец, до этого момента адрес в домене example.org не совпал ни с одним из предыдущих, будет применено последнее сопоставление, в котором соответствует всякое другое почтовое сообщение, отправленное на любой адрес в example.com. Это сообщение будет доставлено в локальный почтовый ящик joe.

## **/etc/mail/authinfo**

Формат файла следующий:

```
AuthInfo:other.dom "U:user" "I:user" "P:secret" "R:other.dom"
"M:DIGEST-MD5"
AuthInfo:more.dom "U:user" "P=c2VjcmV0"
AuthInfo:relay.dnsexit.com "U:USERNAME" "P:PASSWORD" "M:PLAIN"
```

где:

```
U user (authorization) id
I authentication id
P password
R realm
M list of mechanisms delimited by spaces
```

## **Примеры настройки**

### **Минимальная конфигурация**

```
dnl# This is the default sendmail .mc file for Slackware.
To generate
dnl# the sendmail.cf file from this (perhaps after making
some changes),
```



```

dnl# use the m4 files in /usr/share/sendmail/cf like this:
dnl#
dnl# cp sendmail-slackware.mc /usr/share/sendmail/cf/config.mc
dnl# cd /usr/share/sendmail/cf
dnl# sh Build config.cf
dnl#
dnl# You may then install the resulting .cf file:
dnl# cp config.cf /etc/mail/sendmail.cf
dnl#
include('./m4/cf.m4')
VERSIONID('default setup for Slackware Linux')dnl
OSTYPE('linux')dnl
dnl# These settings help protect against people verifying
email addresses
dnl# at your site in order to send you email that you probably
don't want:
define('confPRIVACY_FLAGS', 'authwarnings,novrfy,noexpn,restrictqrun')dnl
dnl# Uncomment the line below to send outgoing mail through
an external server:
dnl define('SMART_HOST','mailserver.example.com')
dnl# No timeout for ident:
define('confTO_IDENT', '0')dnl
dnl# Enable the line below to use smrsh to restrict what
sendmail can run:
dnl FEATURE('smrsh','/usr/sbin/smrsh')dnl
dnl# See the README in /usr/share/sendmail/cf for a ton
of information on
dnl# how these options work:
FEATURE('use_cw_file')dnl
FEATURE('use_ct_file')dnl
FEATURE('mailertable','hash -o /etc/mail/mailertable.db')dnl

FEATURE('virtusertable','hash -o /etc/mail/virtusertable.db')dnl
FEATURE('access_db', 'hash -T<TMPF> /etc/mail/access')dnl
FEATURE('blacklist_recipients')dnl
FEATURE('local_procmail','','procmail -t -Y -a $h -d $u')dnl
FEATURE('always_add_domain')dnl
FEATURE('redirect')dnl
FEATURE('relay_hosts_only')dnl
dnl# Turn this feature on if you don't always have DNS,
or enjoy junk mail:
dnl FEATURE('accept_unresolvable_domains')dnl
EXPOSED_USER('root')dnl
dnl# Also accept mail for localhost.localdomain:
LOCAL_DOMAIN('localhost.localdomain')dnl
MAILER(local)dnl
MAILER(smtp)dnl
MAILER(procmail)dnl
dnl DAEMON_OPTIONS('Port=10025, Name=MTA')dnl

```

Если необходимо вместо local-мэйлера использовать доставщик почты от IMAP-сервера dovecot, то настройка будет выглядеть так:

```
LOCAL_DOMAIN('localhost.localdomain')dnl
MAILER(dovecot)dnl
MAILER(smtp)dnl
MAILER(procmail)dnl
```

При использовании шифрования надо в конфигурационный файл добавить пути к сертификатам и ключу:

```
OSTYPE('linux')dnl
dnl#
dnl# You will need to create the certificates below with
OpenSSL first:
define('confCACERT_PATH', '/etc/mail/certs/')
define('confCACERT', '/etc/mail/certs/CA.cert.pem')
define('confSERVER_CERT', '/etc/mail/certs/smtp.cert.pem')
define('confSERVER_KEY', '/etc/mail/certs/smtp.key.pem')
define('confCLIENT_CERT', '/etc/mail/certs/smtp.cert.pem')
define('confCLIENT_KEY', '/etc/mail/certs/smtp.key.pem')
define('confCRL', 'CERT_DIR/revocation.list')
define('confDONT_BLAZE_SENDMAIL', 'GroupReadableKey-
File')dnl
dnl# Use DH parameters with 2048 bit key
dnl# openssl dhparam -out dh_params.pem 2048
define('confDH_PARAMETERS', '/etc/mail/certs/dh_params.pem')

dnl
dnl# These settings help protect against people verifying
email addresses
DAEMON_OPTIONS('Port=smtp, Name=MTA')dnl
DAEMON_OPTIONS('Port=smtps, Name=MSA-SSL, M=E')dnl
dnl
dnl# Do not allow the weak SSLv2:
dnl O CipherList=ALL:!ADH:!NULL:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:
-Low:+SSLv3:+TLSv1:-SSLv2:+EXP:+eNULL
dnl 1.) Adds the provisions for the 2048 bit Diffie-Hellman file.
dnl 2.) Enforces a pretty solid cipher list and disables weak
ciphers.
dnl 3.) Disables SSLv2 and SSLv3 for server connections
dnl 4.) Disables SSLv2 and SSLv3 for client connections
dnl O CipherList=EDH+CAMELLIA:EDH+aRSA:EECDH+aRSA+AESGCM:
EECDH+aRSA+SHA384:EECDH+aRSA+SHA256:EECDH:
+CAMELLIA256:+AES256:+CAMELLIA128:+AES128:+SSLv3:
!aNULL:!eNULL:!LOW:!3DES:!MD5:!EXP:!PSK:!DSS:!RC4:!SEED
:!ECDH:CAMELLIA256-SHA:AES256-SHA:CAMELLIA128-SHA:
AES128-SHA
O CipherList=HIGH:!ADH
O ServerSSLOptions=+SSL_OP_NO_SSLv2
+SSL_OP_NO_SSLv3 +SSL_OP_CIPHER_SERVER_PREFERENCE
```

```
0 ClientSSLOptions=+SSL_OP_NO_SSLv2 +SSL_OP_NO_SSLv3 dnl
```

```
MAILER(dovecot)dnl
```

Для возможности аутентификации используется sasl-настройка:

```
dnl
dnl define('confDEF_AUTH_INFO','/etc/mail/default-auth-info')
FEATURE('authinfo','hash /etc/mail/authinfo.db')dnl
dnl
dnl# Allow SASL authentication/relaying:
define('confAUTH_OPTIONS','A p y')dnl
define('confAUTH_MECHANISMS','DIGEST-MD5 CRAM-MD5 LOGIN
PLAIN')dnl
TRUST_AUTH_MECH('DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
dnl
```

Использование anti-spam фильтров в sendmail:

```
dnl DNSBL
FEATURE('dnsbl','b.barracudacentral.org','554 Rejected
"
${client_addr} " found in:
http://www.barracudacentral.org/lookups/ip-reputation"')dnl
FEATURE('dnsbl','dnsbl.sorbs.net','554 Rejected "
${client_addr} " found in dnsbl.sorbs.net"')dnl
FEATURE('dnsbl','bl.spamcop.net','Spam blocked see:
http://spamcop.net/bl.shtml?${client_addr}','t')dnl
dnl
MAILER(procmail)dnl
dnl DAEMON_OPTIONS('Port=10025, Name=MTA')dnl
dnl
dnl # enable spam assassin
INPUT_MAIL_FILTER('spamassassin',
'S=local:/var/run/spamass/spamass.sock,
F=, T=C:15m;S:4m;R:4m;E:10m')
define('confMILTER_MACROS_CONNECT','t, b, j, _, {daemon_name},
{if_name}, {if_addr}')dnl
define('confMILTER_MACROS_HELO','s, {tls_version}, {cipher},
{cipher_bits}, {cert_subject}, {cert_issuer}')dnl
define('confMILTER_MACROS_ENVFROM','{auth_authen}, {auth_type}')dnl
define('confMILTER_MACROS_ENVRCPT','r, v, Z')dnl
dnl
dnl DKIM
INPUT_MAIL_FILTER('/usr/sbin/opensslkim',
'S=inet:8891@localhost')
dnl INPUT_MAIL_FILTER('/usr/sbin/dkim-filter',
'S=local:/var/run/dkim-filter/dkim-filter.sock') dnl
dnl MILTER-GREYLIST
dnl
INPUT_MAIL_FILTER('greylist',
```

```
'S=local:/var/milter-greylis/milter-greylis.sock, F=,
T=S:1m;R:1m')dnl
define('confMILTER_MACROS_CONNECT', 'j, {if_addr}')dnl
define('confMILTER_MACROS_HELO', '{verify}, {cert_subject}')dnl
define('confMILTER_MACROS_ENVFROM', 'i, {auth_authen}')dnl
define('confMILTER_MACROS_ENVRCPT', '{greylis}')dnl
dnl
```

Анти-вирус clamav:

```
MAILER(procmail)dnl
define('confLOG_LEVEL', '20')dnl
dnl
dnl clamav-milter
INPUT_MAIL_FILTER('clmilter', 'S=local:/var/run/clamav/clmilter.sock,
F=, T=S:4m;R:4m')dnl
define('confINPUT_MAIL_FILTERS', 'clmilter')
dnl
dnl Add anti-spam filter
define('confMILTER_MACROS_CONNECT', '{client_addr}, {client_name}')dnl
INPUT_MAIL_FILTER('SMC-milter',
'S=local:/var/run/smc-milter.sock, F=T, T=C:30m;S:10m;R:10m;E:30m')dnl
dnl
```