

Настройка почтового реля на базе Sendmail

<http://dormestmass.blogspot.com>

Mon, 3 Jan 2008 14:31:37

<http://dormestmass.blogspot.com/2007/07/sendmail.html>

В данном посте я хочу рассказать о настройке почтового сервера для маршрутизации почты (реля).

Причин для создания такого сервера существует несколько. Например, для доставки почты внутрь разветвленной корпоративной сети. Второй пример — некоторые господа админы в качестве основного почтового сервера предпочитают виндовый софт, типа MDAemon, Kerio и иже с ними, но в инет предпочитают выставлять релей, построенный на nix-ax.

Я расскажу о настройке почтового маршрутизатора на базе sendmail. В качестве ОС используется FreeBSD.

Первое, о чем следует позаботиться, это соответствие DNS записей для вашего сервера в прямой и обратной зонах. Для тех, кто не знает что это, поясню на примере. Допустим, имя вашего почтового сервера mail.domain.ua и IP адрес — 195.195.195.195. Так вот, IP адресу 195.195.195.195 должно соответствовать имя mail.domain.com.

```
srn@mail ~>> host mail.yandex.ru
mail.yandex.ru has address 213.180.204.25
srn@mail ~>> host 213.180.204.25
25.204.180.213.in-addr.arpa domain name pointer
mail.yandex.ru.
```

А вот пример несоответствия записей:

```
srn@mail ~>> host domain.ua
domain.ua has address 213.227.xxx.xxx
srn@mail ~>> host 213.227.xxx.xxx
xxx.xxx.227.213.in-addr.arpa domain name pointer a4-
kv.alkar.net.
```

В последнем случае возможны проблемы доставки почты на некоторые домены, администраторы которых пытаются бороться со спамерами, проверяя соотверствия прямой и обратной записей. Впрочем, таких немного.

Вторым шагом будет, как ни странно, выбор hostname для сервера :).

FQDN почтового сервера не должен соответствовать ни одному домену, который мы собираемся релить. К примеру, если мы собираемся маршрутизировать domain.ua, то назвав так-же сервер, мы окажемся в ситуации, когда sendmail всю почту на этот домен будет складывать локально, а не передавать на следующий почтовый сервер. Для sendmail-а FQDN всегда будет локальным доменом.

В принципе, его можно обмануть при помощи конфигурационного параметра, но я не вижу ни одной причины так делать. К тому же, в руководстве по конфигурационному файлу сказано буквально следующее: "This should only be done if your system cannot determine your local domain name, and then it should be set to \$w.Foo.COM, where Foo.COM is your domain name."

Так что, лучшим вариантом будет присвоить серверу hostname, не совпадающее с маршрутизируемыми доменами, к примеру, mail.domain.ua.

В FreeBSD это делается через rc.conf:

```
srn@mail ~>> grep hostname /etc/rc.conf
hostname="mail.domain.ua"
```

Далее. Необходимо убедиться, что sendmail запускается при старте системы. Для этого нужно добавить параметр sendmail_enable в /etc/rc.conf

```
srn@mail ~>> grep sendmail /etc/rc.conf
sendmail_enable="YES"
```

Теперь приступаем к настройке непосредственно sendmail-а.

Конфигурация

естественно будет выполняться при помощи макроцессора m4.

Подробнее

руководство по конфигурации sendmail через m4 находится в

/usr/share/sendmail/cf/README. Сразу отмечу, что для комментирования

строки необходимо поместить служебное слово dnl в её начало.

Здесь и далее предполагается, что рабочим каталогом является

/etc/mail. Итак, заходим в каталог /etc/mail и выполняем команду make.

В результате появится файл `_имя_сервера.мс`, т.е. в нашем случае

`mail.domain.ua.мс`.

Содержимое этого файла – дефолтный конфигурационный файл для FreeBSD.

Его-то мы и будем править.

Основными опциями для наших нужд есть опции **`access_db`** и **`mailertable`**.

Открыв мс-файл редактором, убеждаемся в их наличии:

```
FEATURE(access_db, `hash -o -T /etc/mail/access')  
FEATURE(mailertable, `hash -o /etc/mail/mailertable')
```

В конфигурации по умолчанию `sendmail` настроен на работу по протоколу

IPv6. Если Вы не используете этот протокол, то логично отключить его,

закомментировав строку:

```
DAEMON_OPTIONS(`Name=IPv6, Family=inet6, Modifiers=0')
```

Также, неплохо бы применить некоторые параметры, которые увеличат

защиту нашего `sendmail`-а.

Во-первых, убеждаемся в наличии/незакомментированности строки,

отключающей команды `VERFY` и `EXPN`:

```
define(`confPRIVACY_FLAGS', `authwarnings,noexpn,novrfy')
```

Во-вторых, желательно наложить ограничение на использование системных

ресурсов `sendmail`-ом.

`dn1` Максимальное количество `sendmail`-процессов,

`dn1` которые могут быть запущены одновременно

```
define(`confMAX_DAEMON_CHILDREN', `10')
```

`dn1` Максимальное количество входящих соединений за секунду

```
define(`confCONNECTION_RATE_THROTTLE', `10')
```

`dn1` Максимальный размер почтового сообщения в байтах

```
define(`confMAX_MESSAGE_SIZE', `5242880')
```

`dn1` Максимальное количество получателей в одном сообщении

```
define(`confMAX_RCPTS_PER_MESSAGE', `50')
```

К выбору ограничений следует относиться разумно, ибо слишком заниженные значения приведут к нарушению нормальной работы. В третьих, некоторые особо параноидальные админы меняют SMTP-баннер, чтобы злые дядьки не смогли по его содержимому узнать версию почтовика. Если Вы относите себя к этой когорте, то баннер меняется следующим образом

```
define(`confSMTP_LOGIN_MSG', `MegaMailer 3.8.11 for CP/M ')
```

Идем дальше. По умолчанию sendmail пытается выполнить запрос ident к клиенту. Это совершенно бесполезная фишка, которая, к тому же, может привести к задержкам в доставке почты. Если у клиента блокируется трафик на 113 TCP порт, то это приведет к 5-секундной задержке, поскольку sendmail будет ожидать такое время ответ от клиента. Отключаем выполнение ident-запросов следующим параметром:

```
define(`confTO_IDENT', `0')
```

Если есть желание использовать черные списки для борьбы со спамерами, то эта возможность включается таким образом:

```
FEATURE(dnsbl,`blackholes.mail-abuse.org',` Mail from  
${client_addr} rejected; see  
http://mail-abuse.org/cgi-bin/lookup?\${client\_addr}')
```

```
FEATURE(dnsbl,`relays.mail-abuse.org',` Mail from  
${client_addr} rejected; see  
http://work-rss.mail-abuse.org/cgi-bin/nph-rss?\${client\_addr}')
```

```
FEATURE(dnsbl,`dialups.mail-abuse.org',` Mail from dial-up  
rejected; see http://mail-abuse.org/dul/enduser.htm')
```

После сохранения нашего mc-файла необходимо сгенерировать из него sendmail.cf. Для этого нужно выполнить команды make и make

install:

```
mail# make
/usr/bin/m4 -D_CF_DIR_=/usr/share/sendmail/cf/
/usr/share/sendmail/cf/m4/cf.m4 mail.domain.ua.mc >
mail.domain.ua.cf
mail# make install
install -m 444 mail.domain.ua.cf /etc/mail/sendmail.cf
install -m 444 mail.domain.ua.submit.cf /etc/mail/submit.cf
```

Следующим шагом будет настройка списка доступа и таблицы маршрутизации

почты. В каталоге /etc/mail есть файлы примеров access.sample и mailertable.sample соответственно. Можно скопировать их, а можно и создать пустые файлы access и mailertable.

```
mail# touch access mailertable
```

В файле access прописываем почтовые домены, которые будет релить сервер. К примеру это domain.ua и domain.ru:

```
mail# cat access
domain.ua          RELAY
domain.ru          RELAY
192.168.0.         RELAY
```

В последней строке указана наша локальная подсеть, ведь мы собираемся

не только принимать почту, но и отправлять ;).

В файле mailertable указываем какие домены куда перенаправлять:

```
mail# cat mailertable
domain.ua          smtp:[windoze.mail.server]
domain.ru          smtp:[192.168.0.14]
```

Если в качестве домена указать точку (.), то по этому маршруту будет

отправляться вся почта, для которой не было найдено маршрута.

Файлы access и mailertable в чистом виде не используются, их нужно

скомпилировать в db-файлы.

```
mail# make
/usr/sbin/makemap hash mailertable.db < mailertable
chmod 0640 mailertable.db
/usr/sbin/makemap hash access.db < access
chmod 0640 access.db
```

На этом процесс конфигурирования закончен. Для того, чтобы наша конфигурация вступила в силу выполняем команду make restart

```
mail# make restart
Restarting: sendmail sendmail-clientmqueue.
```

Примечание. Перезапускать sendmail нужно только после внесения изменений в конфигурационный файл (sendmail.cf). При изменении access и mailertable перезапуск не нужен.

После перезапуска проверяем работу нашего почтового сервера.

Убеждаемся, что сервер слушает 25 порт:

```
mail# netstat -an | grep LISTEN
rawbeer# netstat -an | grep LISTEN
tcp4          0          0  *.587
*.587         LISTEN
tcp4          0          0  *.25
*.25         LISTEN
tcp4          0          0  *.21
*.21         LISTEN
tcp4          0          0  *.22
*.22         LISTEN
tcp4          0          0  *.80
*.80         LISTEN
```

Пытаемся отправить тестовое письмо на наш домен:

```
srn@mail ~>> telnet mail.domain.ua 25
Trying xxx.xxx.xxx.xxx...
Connected to mail.domain.ua.
Escape character is '^]'.
220 mail.domain.ua ESMTP Sendmail 8.14.1/8.14.1; Tue, 17 Jul
```

```
2007 11:00:42 +0300 (EEST)
ehlo xxx
250- mail.domain.ua Hello xxx.domain.ua [yyy.yyy.yyy.yyy],
pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-8BITMIME
250-SIZE 5242880
250-DSN
250-ETRN
250-DELIVERBY
250 HELP
mail from: somebody@domain.com
250 2.1.0 somebody@domain.com... Sender ok
rcpt to: somebody@domain.ua
250 2.1.5 rshramko@domain.ua... Recipient ok
data
354 Enter mail, end with "." on a line by itself
Subject: test
test
.
250 2.0.0 l6H80gGb031272 Message accepted for delivery
quit
221 2.0.0 mail.domain.ua closing connection
Connection closed by foreign host.
```

Убеждаемся что письмо ушло в соответствии с таблицей маршрутизации:

```
mail# less /var/log/maillog
Jul 17 11:01:29 rawbeer sm-mta[[ :]] l6H80gGb031272: from=,
size=20,
class=0, nrcpts=1,
msgid=<200707170801.l6H80gGb031272@mail.domain.ua.>,
proto=ESMTP,
daemon=Daemon0, relay=mail.domain.ua [xxx.xxx.xxx.xxx]
Jul 17 11:01:29 rawbeer sm-mta[[ :]] l6H80gGb031272: to=,
delay=00:00:10,
xdelay=00:00:00, mailer=smtp, pri=30020,
relay=windoze.mail.server. [192.168.0.1], dsn=2.0.0,
stat=Sent (Message received: JLBD0800.50I)
```

По желанию, можно подключится к sendmail-у с какого-нибудь

внешнего

адреса и попытается отправить письмо на какой-нить левый домен.

Естественно, наша попытка должна быть отфутболена.

На этом базовая настройка релея закончилась.

Остался последний штрих. Если на сервере используется пакетный фильтр

и в нем по умолчанию неразрешенные пакеты сбрасываются (DROP), то у

других сендмейлов могут быть проблемы с ident-запросами к нашему

серверу. Не будем им усложнять жизнь и настроим пакетный фильтр так,

чтобы запросы на 113 TCP порт не сбрасывались, а отклонялись.

Для `pf`, который я использую на сервере, это будет следующее правило:

```
block return in quick proto tcp from any to any port 113
```

Для `iptables` в Linux-ах нужно будет сделать что-то вроде этого:

```
iptables -A INPUT -p tcp --dport 113 -j REJECT --reject-with  
tcp-reset
```

Ну и осталось приправить по желанию антиспамом и антивирусом, но

данные вопросы пусть останутся за рамками этого поста.

Обсуждение [RSS]

1.1. Andrey Y. Ostanovsky, 23:14, 10/01/2008

> Сразу отмечу, что для комментирования

> строки необходимо поместить служебное

> слово `dnl` в её начало.

Слово "`dnl`", т.е. с пробелом после букв `dnl`.

1.2. Allan, 15:41, 22/04/2008

Вопрос такой а если я `relay_domains` пропишу все необходимые домены по которым хочу получать почту например (`domain1.ua`, `domain2.ua`, `domain3.ua`), а в `mailertable` укажу "." вместо всех доменов и направлять почту на `192.168.x.1`, то приходить будут только письма с указ. доменами или все?

1.3. Евгений, 12:21, 29/12/2008

День добрый.

а как быть, если мне как раз то и надо, что бы пользователи удаленного офиса могли пользоваться моей внутренней почтой?
то есть:

1. у удаленного офиса есть статический ИП от провайдера

2. Почту они получить могут... а вот отправить – нет.

даже при помощи указания их текущего ИП с access типа
xxx.xxx.xxx.xxx RELAY

оно все равно не ходит...

есть какой то вариант решения?

1.5. VL., 14:23, 29/03/2010

Идеальное пошаговое руководство. Спасибо!

1.6. Konstantin, 15:34, 09/02/2012

в моем случае потребовалось внести изменения в файл
virtusertable. А именно:

```
makemap hash virtusertable.db<virtusertable
@domain.ua          windoze.mail.server
@domain.ru          192.168.0.14
```

Добавить FEATURE с virtusertable.db