OpenDKIM + Postfix

1. Установка OpenDKIM

Для начала, устанавливаем пакет OpenDKIM. Он выполняет операции шифрования заголовков для DKIM, а также содержит набор для формирования ключей.

Для его установки вводим следующее.

```
cd /usr/ports/mail/opendkim
make config-recursive
make install clean
```

2. Создание сертификата для домена

Для этого можно воспользоваться бесплатным онлайн инструментом на сайте dkimcore.org. Однако, в данном примере, мы воспользуемся opendkim-genkey и сформируем его самостоятельно.

И так, создаем каталог для размещения ключей:

```
mkdir /etc/opendkim
```

И генерируем их следующей командой:

```
opendkim-genkey -D /etc/opendkim/ --domain site.ru --selector relay
```

* *где* ***site.ru*** *— домен, с которого будет отправляться почта:* ***relay*** *— имя селектора (селектор — это строковый идентификатор, он может быть любым).*

В папке /etc/opendkim/ должно появиться два файла с расширениями *.private* и *.txt*. Первый — закрытый ключ (храним его у себя на сервере), второй — готовая txt-запись для DNS.

Задаем группу владельца opendkim для созданных ключей:

```
chown opendlim:opendkim /etc/opendkim/*
```

Если система выдаст ошибку, что группы opendkim не существует (chown: opendkim: illegal group name), необходимо сначала создать учетную запись.

```
pw useradd opendkim -m -s /usr/sbin/nologin -w no
```

3. Настройка DNS

Смотрим содержимое файла txt:

```
cat /etc/opendkim/relay.txt
```

И используя данное содержимое, в панели управления нашим DNS создаем TXT-запись следующего формата:

```
relay._domainkey IN TXT "v=DKIM1; k=rsa; p=MIGfMA0GCSqG...rhyaj8OcbwIDAQAB"
```

* *где **relay** – название нашего селектора **MIGfMA0GCSqG…rhyaj8OcbwIDAQAB** – сокращенная запись открытого ключа (она длиннее).*

BIND не понимает строки длинней 255 символов и поэтому, если вы пропишите публичный ключ в виде *одной длинной строки*, BIND при перезагрузке выдаст ошибку:

```
/var/log/messages
zone 2keep.net/IN: loading from master file masters/2keep.net failed: syntax error
zone 2keep.net/IN: not loaded due to errors.
other/2keep.net/IN: syntax error
```

Прописывать ключ нужно следующим образом:

```
relay._domainkey.site.ru. IN TXT ( "k=rsa\; "
                                   "p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs2WdcyOKgKVU2C/7CV77"
                                   "4mu/b+XVaVixtuASB0wAOjaPnEcFzwI84hu6wmy8cpPJlVImnf1gD/y/pA08+viV"
```

```
                                        "PPP/6bHfEiJjxOSjDnhF2V1+G
lOrl6IYxNxOxXPLw88QpDPak+ZO0yLU58UxJP1K"
                                        "cPdCuftEMFHWd5vuiHquBNYtk
W6MxaGcoX4hK8eE9CdrKDH7EtuLkkJ4uj0Mw4R7"
                                        "kd6FexfyppDXFGGu8oDN+7IUf
CqnKDkUxqb5Dh4rDD24Tn6KdDY5eFgjw7OIUr8H"
                                        "Jbr9KNSE6lF3M5JLx9VX/ny3e
c9ODLm0FGpDQbXcRM+CTmX6H2jGkwJ4VcpqDwVZ"
                                        "RwIDAQAB" )
```

**Если у вас несколько доменов с которых вы отправляете почту, то создайте и для них пару ключей и сделайте аналогичные настройки.*

Дополнительные необязательные записи

```
_domainkey IN TXT "o=~; r=postmaster@site.ru"
```

* *где **o=~** означает, что не все сообщения подписываются для домена (**o=-** – говорит, что все письма используют DKIM).*

```
_adsp._domainkey IN TXT "dkim=all"
```

ADSP это опциональное расширение DKIM, которое позволяет сообщать почтовым серверам-получателям, что делать с письмом пришедшим с якобы нашего домена, но не имеющее подписи.

* ***all** запрещает принимать письма от домена без цифровой подписи. Другие варианты: **discardable** – блокировать сообщения на стороне получателя, **unknown** – по умолчанию (такую запись создавать не обязательно).*

4. Настройка OpenDKIM и Postfix

Открываем конфигурационный файл opendkim.

```
ee /usr/local/etc/mail/opendkim.conf
```

И приводим его к следующему виду:

```
AutoRestart             Yes
AutoRestartRate         10/1h
```

```
Umask                   002
Syslog                  yes
SyslogSuccess           Yes
LogWhy                  Yes
Canonicalization        relaxed/simple
ExternalIgnoreList      refile:/etc/opendkim/TrustedHosts
InternalHosts           refile:/etc/opendkim/TrustedHosts
KeyTable                refile:/etc/opendkim/KeyTable
SigningTable            refile:/etc/opendkim/SigningTable
Mode                    sv
PidFile                 /var/run/opendkim/opendkim.pid
SignatureAlgorithm      rsa-sha256
UserID                  opendkim:opendkim
Socket                  inet:12301@localhost
```

* *все параметры можно оставить, как в данном примере, за исключением* ***Socket*** *– можно указать любой другой порт, вместо* ***12301****.*

Создаем файл доверенных узлов. В него войдут имена хостов, доменов и IP-адресов, которые будут приняты, как доверенные и подписаны.

```
ee /etc/opendkim/TrustedHosts
```

И вносим следующее:

```
127.0.0.1
localhost
*.site.ru
```

* *где* ***site.ru*** *– почтовый домен.*

Создаем таблицу *KeyTable*. В ней хранится список соответствий между селекторами, доменами и файлами с закрытыми ключами. Формат записей:
<селектор>._domainkey.<домен> <домен>:<селектор>:<путь к закрытому ключу>

```
ee /etc/opendkim/KeyTable
```

И в соответствии с форматом приводим его к нужному виду:

```
relay._domainkey.site.ru
site.ru:relay:/etc/opendkim/relay.private
```

И напоследок, создаем *SigningTable*. В данной таблице хранятся соответствия между определенными email-адресами и записями в *KeyTable*.

```
ee /etc/opendkim/SigningTable
```

И приводим к такому виду:

```
*@site.ru relay._domainkey.site.ru
```

Запускаем службу opendkim.

```
service milter-opendkim onestart
```

Добавляем демона в rc.conf:

```
echo 'milteropendkim_enable="YES"' >> /etc/rc.conf
echo 'milteropendkim_uid="opendkim"' >> /etc/rc.conf
```

* *первая команда разрешает запуск демона, вторая – принудительно заставляет его запускаться от пользователя* ***opendkim.***

И запускаем его:

```
service milter-opendkim start
```

Открываем конфигурационный файл Postfix.

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

Добавляем или редактируем:

```
milter_protocol = 2
milter_default_action = accept
smtpd_milters = inet:localhost:12301
```

non_smtpd_milters = inet:localhost:12301

** если **smtpd_milters** и **non_smtpd_milters** присутствуют в конфигурационном файле, то приведенные в данном примере значения нужно дописать к имеющимся. ** **12301** – порт работы opendkim, который был задан в **opendkim.conf**.*

Перезапускаем Postfix:

```
service postfix restart
```

5. Проверка

Отправляем письмо

Отправляем электронное сообщение на различные почтовые системы – mail.ru, gmail.com, yandex.ru.

Способов отправки несколько, например, можно выполнить следующую команду:

```
echo "Test DKIM" | mail -s 'Testing DKIM' -r admin@site.ru test@mail.ru
```

** где **admin@site.ru** – почтовый ящик, от которого отправляется письмо (напомню, в данном примере подпись создается для домена site.ru), **test@mail.ru** – Ваш адрес почты, на который придет письмо.*

Второй способ – настроить почтовый клиент, который будет отправлять почту через настроенный нами сервер.

Проверяем заголовки

Открываем наше письмо и смотрим заголовки (в mail.ru: **Еще – Служебные заголовки**).

Среди них мы должны увидеть следующую строчку:

dkim=pass header.d=site.ru

Проверка домена на базе DKIM настроена успешно.