Postgrey - "серые списки" для Postfix

Опубликовано muff в Чт, 2010-07-15 03:27

Postgrey (Postfix Greylisting Policy Server) - решение на Perl реализации технологии **Greylisting** [1] для **MTA Postfix**.

Собственно говоря, Greylisting уже давно использую на корпоративных почтовых серверах. Но там в качестве **MTA** используется **Exim**. Сегодня знакомый пожаловался, что увеличилось количество приходящего спама на почтовые ящики в некоторых доменах. Эти домены я не так давно перенес на отдельный сервер, чтобы отделить грешное от праведного, тоесть клиентские данные от корпоративных.

На этом сервере в качестве **MTA** используется **Postfix**. Ряд дополнительных проверок уже установлен. Теперь дело за малым - включить поддержку Greylisting. Итак, по вышеуказанной ссылке можно узнать, как работает технология "серых списков". Поэтому не будем тратить время на описание технологии, а сразу приступим к настройке. Выполним установку Postgrey из системы портов:

```
# cd /usr/ports/mail/postgrey/ && make install clean && rehash
```

Следующим шагом добавляем поддержку Postgrey при загрузке:

```
# echo '# Postfix Greylisting' >> //etc/rc.conf
 # echo 'postgrey_enable="YES"' >> /etc/rc.conf
```

Запускаем службу:

```
# sh /usr/local/etc/rc.d/postgrey start
Starting postgrey.
```

Далее, следуя инструкциям, приступаем к редактированию конфигурационного файла Postfix - **main.cf**. Необходимо в параметр **smtpd_recipient_restrictions** сразу после **reject_unauth_destination** добавить опцию **check_policy_service inet:127.0.0.1:10023**. Навожу пример моего параметра **smtpd_recipient_restrictions:**

```
smtpd_recipient_restrictions = permit_mynetworks, permit_sasl_authenticated, reje
ct_unknown_client, reject_unknown_hostname, reject_unknown_sender_domain, reject_
unverified_sender, reject_non_fqdn_hostname, reject_non_fqdn_sender, reject_non_f
qdn_recipient, reject_unauth_destination, check_policy_service inet:127.0.0.1:1002
3, reject_unauth_pipelining, reject_unlisted_recipient, reject_invalid_hostname
```

Также следует обратить внимание на следующие файлы:

- **/usr/local/etc/postfix/postgrey_whitelist_clients** - вносим в этот список доверенные домены. Почта с этих доменов будет приниматься, минуя **Greylist**;
- **/usr/local/etc/postfix/postgrey_whitelist_recipients** - вносим в этот список адреса e-mail пользователей, для которых **Greylist** будет отключен.

После внесения необходимых изменений перезапускаем Postfix:

```
# sh /usr/local/etc/rc.d/postfix restart
postfix/postfix-script: stopping the Postfix mail system
postfix/postfix-script: starting the Postfix mail system
```

Для проверки посмотрим логи почтового сервера:

```
# tail -f /var/log/maillog
```

В случае обнаружения примерно такой записи:

```
Jul 15 15:41:32 web0 postfix/smtpd[75888]: NOQUEUE: reject: RCPT from
mail.example.com[xxx.xxx.xxx.xxx: 450 4.2.0 office [at] example [dot] com: Recipient address
rejected: Greylisted, see http://postgrey.schweikert.ch/help/example.com.html; from=admin
[at] example [dot] org to=office [at] example [dot] org proto=ESMTP helo=<mail.example.com>
```

можно считать, что настройка завершена успешно.

Настройки по умолчанию я не изменял, время грейлистинга - 5 минут.

Ознакомиться с доступными опциями можно на странице руководства:

```
# man postgrey
```

Необходимые ключи запуска необходимо добавить в **/usr/local/etc/rc.d/postgrey** и перезапустить **potgrey**.

Сформировать отчет можно, используя утилиту **postgreyreport**, следующей командой :

Источник (получено *2025-07-15 23:32*):
http://muff.kiev.ua/content/postgrey-serye-spiski-dlya-postfix

Ссылки:
[1] http://muff.kiev.ua/content/greylisting-pora-poznakomitsya-s-tekhnologiei-serykh-spiskov