Postgrey + Postfix

Обновляем порты:

```
# portsnap fetch update
```

Устанавливаем и добавляем в автозагрузку:

```
# portmaster mail/postgrey
# echo 'postgrey_enable="YES"' >> /etc/rc.conf
```

Стартуем и проверям:

```
# service postgrey start
# service postgrey status
```

Редактируем конфигурационный файл Postfix, вставляя в секции smtpd_recipient_restrictions после параметра reject_unauth_destination:

```
# ee /usr/local/etc/postfix/main.cf
.....
smtpd_recipient_restrictions =
    check_client_access hash:/usr/local/etc/postfix/blacklist-IP
   permit_mynetworks
   permit_sasl_authenticated
   check_recipient_access hash:/usr/local/etc/postfix/recipient-list
   reject_non_fqdn_recipient
   reject_unauth_destination
   check_policy_service inet:127.0.0.1:10023
   reject_unknown_recipient_domain
   reject_unverified_recipient
   permit
.....
```

- **/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** – e-mail пользователей, для которых **Greylist** будет отключен.

Перезапускаем Postfix:

```
# service postfix restart
```

Отправляем себе письмо и смотрим в логах примерно такой вывод:

```
...: Recipient address rejected: Greylisted, see http://postgrey.schweikert.ch/help/tst-amo.net.ua.html (in reply to RCPT TO command))
```

Whitelisting

In postgrey its possible to whitelist senders as well as recipients. All that needs doing in order to whitelist a host is to add its fully qualified domain name or its ip address to the /etc/postfix/postgrey_whitelist_clients.local file. eg:

```
192.168.1.10
mydesktop.office.mydomain.com
```

Now all email recieved from either 192.168.1.10 or mydesktop.office.mydomain.com will not be greylisted, it will be accepted immediately (as long as its valid, and passes all postfix rules). On the other hand if you want to whitelist a recipient you can add their username part of the email address to the /etc/postfix/postgrey_whitelist_recipients file. eg:

```
postmaster@
abuse@
theboss@
```

Now all emails being received for any of these email address’ wont be greylisted, and all email will be accepted right away. Note that postgrey already comes with whitelist setup for postmaster and abuse.

Reporting

Postgrey includes a reporting tool call postgreyreport. Its installed by default when you install the postgrey rpm. Postgreyreport will parse a maillog (read from STDIN), compare it with the postgrey db and output details on all ‘fatal’ greylist entries. A host is considered to be ‘fatally’ greylisted when it does not retry within 300 seconds from its first attempt at email delivery for a specific destination. Postgreyreport uses the complete triple as a candidate. You can tune this delay of 300 seconds using the command line option –delay, however 300 is a good benchmark. Most mail servers will retry within 300 seconds.

Basic usage :

```
cat /var/log/maillog | postgreyreport --delay=300
```

Depending on how busy your server is, the report can get quite large. To get only the top 20 sources getting greylisted out – you can use something like this :

```
cat /var/log/maillog | postgreyreport | awk '{print $1}' | sort | uniq -c | sort -nr | head -n20
```

To get a list of the top 20 email address that the greylisted sources are sending email to :

```
cat /var/log/maillog | postgreyreport | awk '{print $4}'  | sort  | uniq -c | sort -nr | head -n20
```

To get a list of all options that postgreyreport supports and their functions:

```
postgreyreport -h
```

http://muff.kiev.ua/content/postgrey-serye-spiski-dlya-postfix
https://wiki.centos.org/HowTos/postgrey