Настраиваем smart relay на базе postfix

Введение

Сколько раз я слышал фразу - «Я отправил почту в своем php проекте, но письмо в итоге не получил. Почему?!». Особенно это касается случаев, когда адрес получателя обслуживается gmail, у которого довольно таки строгие критерии фильтрации почты. И почта, отправленная от apache@localhost.localdomain в 95% случаев будет заблокирована, в лучшем случае попадет в папку SPAM. В принципе, тоже касается и других крупных почтовых провайдеров в той или инной степени. А все связанно с сленью php программистов, да и не только php, которые отправляют почту посредством функции mail(), передавая, как правило, 3 параметра - тему, получателя и само тело письма.

Ну что же, наша задача помочь разработчикам и облегчить им жизнь. А именно, мы настроем отправку почты от заданного имени с авторизацией через соответствующий релей.

Подготовка

Я специально создал 4 тестовых ящика на крупных почтовых сервисах:

- relay.test.2015@gmail.com
- relay.test_2015@yahoo.com
- relay.test.2015@outlook.com
- relay.test.2015@mail.ru

Для отправки будем использовать следующие параметры релеев

```
GMAIL
mail from: relay.test.2015@gmail.com
server address: smtp.googlemail.com
port: 25
```

```
YAHOO
mail from: relay.test_2015@yahoo.com
server address: smtp.mail.yahoo.com
port: 465
```

```
OUTLOOK
email: relay.test.2015@outlook.com
server address: smtp-mail.outlook.com
port: 587
```

```
MAIL.RU
mail from: relay.test.2015@mail.ru
server address: smtp.mail.ru
port: 2525
```

Настройка

Ниже привожу минимально необходимые изменения файла main.cf. Итак, по нашей задумке, вся почта, отправляемая от имени relay.test.2015@gmail.com будет уходить через соответствующий релей - smtp.googlemail.com с аутентификацией. Аналогично и для других сервисов. Т.е. все, что остается сделать разработчику указать соответсвующий адрес в поле mail from, всю остальную работу за него выполнит postfix.

```
smtpd_recipient_restrictions =
    permit_mynetworks,
    reject_unauth_destination,
    permit_sasl_authenticated

smtp_tls_protocols = !SSLv2, !SSLv3
smtp_tls_security_level = secure
smtp_tls_mandatory_protocols = !SSLv2, !SSLv3
smtp_tls_mandatory_ciphers = high
smtp_tls_secure_cert_match = nexthop

smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_security_options = noanonymous
smtp_sasl_tls_security_options = noanonymous
smtp_sasl_type = cyrus
smtp_tls_CAfile = /etc/ssl/certs/ca-bundle.crt
smtp_use_tls = yes

sender_dependent_relayhost_maps = hash:/etc/postfix/sender_relay_maps

smtp_tls_loglevel = 1
smtpd_tls_loglevel = 1
```

В файле /etc/postfix/sasl_passwd мы указываем на каком релеи под кем мы будет проходить аутентификацию, а в файле /etc/postfix/sender_relay_maps мы указываем через какой релей отправлять почту от определенного отправителя. Остальные параметры по сути больше относятся к общим настрйокам и настройкам безопасности. Привел их для полноты картины.

```
# cat sasl_passwd
[smtp.googlemail.com]:25 relay.test.2015@gmail.com:7654321
[smtp.mail.yahoo.com]:465 relay.test_2015@yahoo.com:7654321
[smtp-mail.outlook.com]:587 relay.test.2015@outlook.com:7654321
[smtp.mail.ru]:2525 relay.test.2015@mail.ru:7654321
```

```
# cat sender_relay_maps
relay.test.2015@gmail.com [smtp.googlemail.com]:25
relay.test_2015@yahoo.com [smtp.mail.yahoo.com]:465
relay.test.2015@outlook.com [smtp-mail.outlook.com]:587
```

```
relay.test.2015@mail.ru [smtp.mail.ru]:2525
```

После внесения любых изменений в файлы sasl_passwd/sender_relay_maps не забываем обновить соответствующие hash файлы

```
# postmap sasl_passwd sender_relay_maps
# service postfix restart
```

Тестирование

Для тестирование smtp есть очень удобная утилита swaks. Именно с помощью нее мы и будем производить наши тесты

```
# echo "Hello world" | swaks -s 127.0.0.1 --from relay.test.2015@gmail.com -
-to relay.test.2015@mail.ru  --h-Subject "GMail relay test" --body -
=== Trying 127.0.0.1:25...
=== Connected to 127.0.0.1.
<-  220 mail.example.net ESMTP
 -> EHLO mail.example.net
<-  250-mail.example.net
<-  250-PIPELINING
<-  250-SIZE 10240000
<-  250-VRFY
<-  250-ETRN
<-  250-AUTH PLAIN LOGIN
<-  250-ENHANCEDSTATUSCODES
<-  250-8BITMIME
<-  250 DSN
 -> MAIL FROM:<relay.test.2015@gmail.com>
<-  250 2.1.0 Ok
 -> RCPT TO:<relay.test.2015@mail.ru>
<-  250 2.1.5 Ok
 -> DATA
<-  354 End data with <CR><LF>.<CR><LF>
 -> Date: Sun, 22 Mar 2015 15:32:31 -0400
 -> To: relay.test.2015@mail.ru
 -> From: relay.test.2015@gmail.com
 -> Subject: GMail relay test
 -> X-Mailer: swaks v20130209.0 jetmore.org/john/code/swaks/
 ->
 -> Hello world
 ->
 ->
 -> .
<-  250 2.0.0 Ok: queued as 42BB512324B
 -> QUIT
<-  221 2.0.0 Bye
=== Connection closed with remote host.
```

Смотрим maillog

```
Mar 22 15:32:31 web-srv01 postfix/smtpd[13837]: connect from
localhost[127.0.0.1]
Mar 22 15:32:31 web-srv01 postfix/smtpd[13837]: 42BB512324B:
client=localhost[127.0.0.1]
Mar 22 15:32:31 web-srv01 postfix/cleanup[13839]: 42BB512324B: message-
id=<20150322193231.42BB512324B@mail.example.net>
Mar 22 15:32:31 web-srv01 postfix/qmgr[13834]: 42BB512324B:
from=<relay.test.2015@gmail.com>, size=427, nrcpt=1 (queue active)
Mar 22 15:32:31 web-srv01 postfix/smtpd[13837]: disconnect from
localhost[127.0.0.1]
Mar 22 15:32:31 web-srv01 postfix/smtp[13840]: setting up TLS connection to
smtp.googlemail.com[74.125.136.16]:25
Mar 22 15:32:31 web-srv01 postfix/smtp[13840]: Verified TLS connection
established to smtp.googlemail.com[74.125.136.16]:25: TLSv1.2 with cipher
ECDHE-RSA-AES128-GCM-SHA256 (128/128 bits)
Mar 22 15:32:32 web-srv01 postfix/smtp[13840]: 42BB512324B:
to=<relay.test.2015@mail.ru>, relay=smtp.googlemail.com[74.125.136.16]:25,
delay=1.6, delays=0.01/0/0.65/0.96, dsn=2.0.0, status=sent (250 2.0.0 OK
1427052699 nh17sm7809110wic.5 - gsmtp)
Mar 22 15:32:32 web-srv01 postfix/qmgr[13834]: 42BB512324B: removed
```

Как видно, все работает так, как мы и хотели. Письмо было отправлено через smtp.googlemail.com.

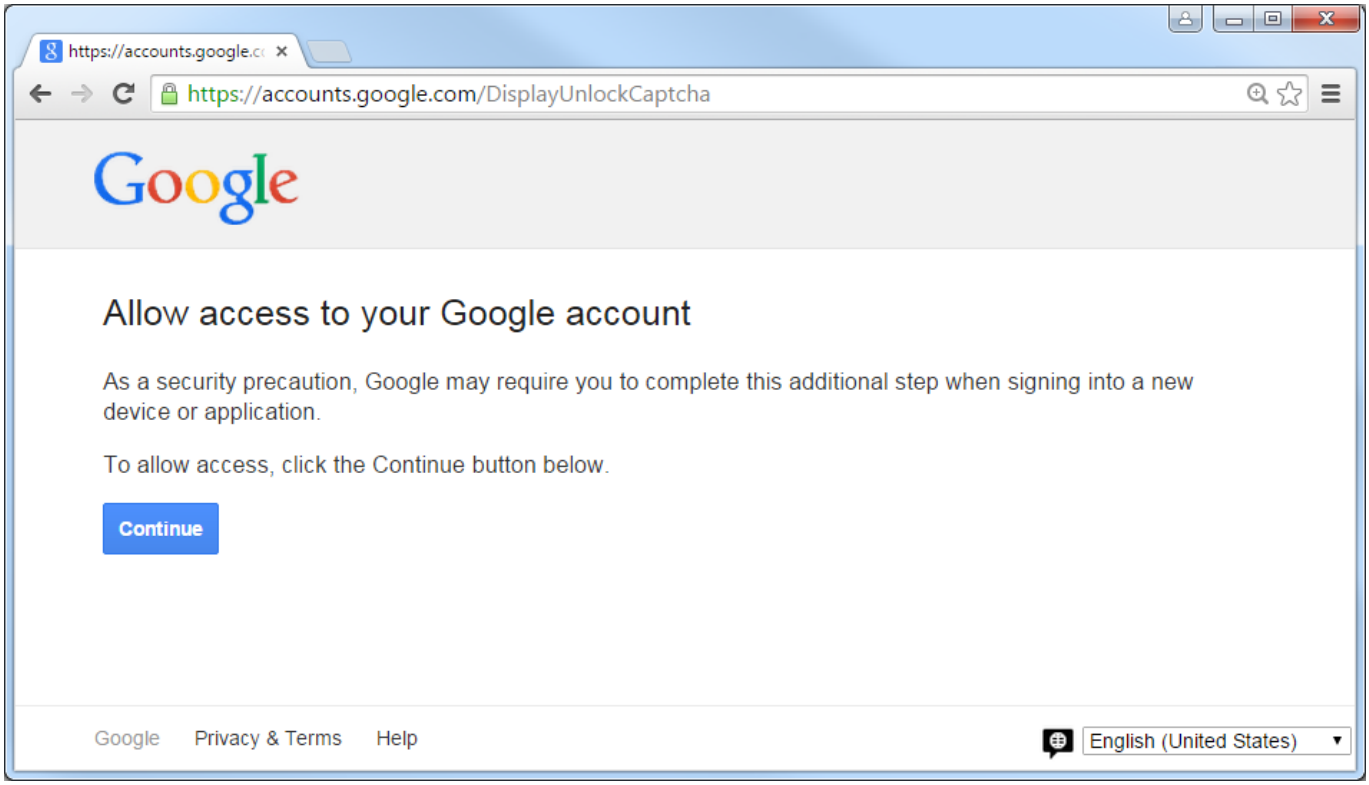
Иногда при попытке отправить через gmail в логах можно встретить запись вида

```
Mar 21 09:05:56 web-srv01 postfix/smtp[13621]: 6BFC712322F:
to=<relay.test.2015@mail.ru>,
relay=smtp.googlemail.com[74.125.136.16]:25, delay=0.74,
delays=0.02/0.05/0.67/0, dsn=4.7.14,
status=deferred (SASL authentication failed; server
smtp.googlemail.com[74.125.136.16] said: 534-5.7.14
<https://accounts.google.com/ContinueSignIn?sarp=1&scc=1&plt=AKgnsbvF2?534-5
.7.14 NpTuN0HNSVo0YmFefbM4hb_L3-
SKFJHL46LDaVqFQRf3ZyREUFunFIeKYO0rMdb5AIYijb?534-5.7.14
ZsDZ3xUgsrVfI1fH3XCRHhmTuw9nd651QmAmPJyiREf4z0AeHVf-
k8cmfi9XeJttBKvdo3?534-5.7.14
TRyMpDA_M3APtZxkYdSTMYLJdY8_WWf4QErEarlckquMjh4ENrW-
Sho3Nm8kZcMY3jKop6?534-5.7.14
GhWRpUg> Please log in via your web browser and then try again.?534-5.7.14
Learn more at?534 5.7.14
https://support.google.com/mail/bin/answer.py?answer=78754 g8sm2272355wiy.19
- gsmtp)
```

Для избежания подобных проблем достаточно перейти по ссылке - https://www.google.com/settings/security/lesssecureapps и разрешить доступ с т.н. небезопасных приложений.

Если и вышеописанный пункт не помог, то возможно поможет следующая ссылка. Она на

время (около 10 минут) дает возможность зарегистрировать новое приложение



Аналогично производим тестирование и остальных сервисов.

Проверяем outlook.com

```
# echo "Hello world" | swaks -s 127.0.0.1 --from relay.test.2015@outlook.com
--to relay.test.2015@gmail.com --h-Subject "Outlook relay test" --body -
```

```
Mar 23 10:18:41 web-srv01 postfix/smtpd[23427]: connect from
localhost[127.0.0.1]
Mar 23 10:18:41 web-srv01 postfix/smtpd[23427]: 47B00123269:
client=localhost[127.0.0.1]
Mar 23 10:18:41 web-srv01 postfix/cleanup[23429]: 47B00123269: message-
id=<20150323141841.47B00123269@mail.example.net>
Mar 23 10:18:41 web-srv01 postfix/qmgr[21841]: 47B00123269:
from=<relay.test.2015@outlook.com>, size=455, nrcpt=1 (queue active)
Mar 23 10:18:41 web-srv01 postfix/smtpd[23427]: disconnect from
localhost[127.0.0.1]
Mar 23 10:18:41 web-srv01 postfix/smtp[23430]: setting up TLS connection to
smtp-mail.outlook.com[65.55.176.126]:587
Mar 23 10:18:42 web-srv01 postfix/smtp[23430]: Verified TLS connection
established to smtp-mail.outlook.com[65.55.176.126]:587: TLSv1.2 with cipher
ECDHE-RSA-AES256-SHA384 (256/256 bits)
Mar 23 10:18:45 web-srv01 postfix/smtp[23430]: 47B00123269:
to=<relay.test.2015@gmail.com>, relay=smtp-
mail.outlook.com[65.55.176.126]:587, delay=4, delays=0.02/0.04/1.9/2.1,
dsn=2.6.0, status=sent (250 2.6.0
<20150323141841.47B00123269@mail.example.net> Queued mail for delivery)
Mar 23 10:18:45 web-srv01 postfix/qmgr[21841]: 47B00123269: removed
```

Проверяем mail.ru

```
# echo "Hello world" | swaks -s 127.0.0.1 --from relay.test.2015@mail.ru --
to relay.test.2015@outlook.com --h-Subject "Mail.ru relay test" --body -
```

```
Mar 23 10:23:41 web-srv01 postfix/smtpd[23495]: connect from
localhost[127.0.0.1]
Mar 23 10:23:41 web-srv01 postfix/smtpd[23495]: BD48D123269:
client=localhost[127.0.0.1]
Mar 23 10:23:41 web-srv01 postfix/cleanup[23515]: BD48D123269: message-
id=<20150323142341.BD48D123269@mail.example.net>
Mar 23 10:23:41 web-srv01 postfix/qmgr[21841]: BD48D123269:
from=<relay.test.2015@mail.ru>, size=455, nrcpt=1 (queue active)
Mar 23 10:23:41 web-srv01 postfix/smtpd[23495]: disconnect from
localhost[127.0.0.1]
Mar 23 10:23:41 web-srv01 postfix/smtp[23494]: setting up TLS connection to
smtp.mail.ru[94.100.180.160]:2525
Mar 23 10:23:42 web-srv01 postfix/smtp[23494]: Verified TLS connection
established to smtp.mail.ru[94.100.180.160]:2525: TLSv1 with cipher DHE-RSA-
AES256-SHA (256/256 bits)
Mar 23 10:23:42 web-srv01 postfix/smtp[23494]: BD48D123269:
to=<relay.test.2015@outlook.com>, relay=smtp.mail.ru[94.100.180.160]:2525,
delay=0.63, delays=0.02/0/0.46/0.15, dsn=2.0.0, status=sent (250 OK
id=1Ya3Fg-0007N1-At)
Mar 23 10:23:42 web-srv01 postfix/qmgr[21841]: BD48D123269: removed
```

А самое интересное я оставил на последок. А именно релей с использованием smtps (465 порт).

```
# echo "Hello world" | swaks -s 127.0.0.1 --from relay.test_2015@yahoo.com -
-to relay.test.2015@mail.ru --h-Subject "Yahoo relay test" --body -
```

При попытке отправить, мы получим сообщение об ошибке, в maillog появятся записи вида

```
Mar 23 10:29:47 web-srv01 postfix/smtpd[23603]: connect from
localhost[127.0.0.1]
Mar 23 10:29:47 web-srv01 postfix/smtpd[23603]: 37E7C123269:
client=localhost[127.0.0.1]
Mar 23 10:29:47 web-srv01 postfix/cleanup[23605]: 37E7C123269: message-
id=<20150323142947.37E7C123269@mail.example.net>
Mar 23 10:29:47 web-srv01 postfix/qmgr[21841]: 37E7C123269:
from=<relay.test_2015@yahoo.com>, size=447, nrcpt=1 (queue active)
Mar 23 10:29:47 web-srv01 postfix/smtpd[23603]: disconnect from
localhost[127.0.0.1]
Mar 23 10:30:47 web-srv01 postfix/smtp[23606]: 37E7C123269:
to=<relay.test.2015@mail.ru>, relay=smtp.mail.yahoo.com[188.125.69.59]:465,
delay=60, delays=0.01/0.03/60/0, dsn=4.4.2, status=deferred (lost connection
with smtp.mail.yahoo.com[188.125.69.59] while receiving the initial server
greeting)
```

После прочтение документации, находим там такую информацию

The Postfix SMTP client does not support the obsolete «wrappermode» protocol, which uses TCP port 465 on the SMTP server!
Начиная с postfix 3.0 появилась поддержка smtps в режиме smtp клиента, для этого достаточно включить smtp_tls_wrappermode

Т.е. когда postfix выступает в роле smtp клиента, как в нашем случае, то он не может поддерживать протокол smtps. В режиме сервера никаких проблем нет. Чтобы обойти данную проблему, нам необходимо поднять тунель с помощью stunnel и отправлять письма на yahoo.com через этот тунель.

Настройки stunnel очень простые

```
# cat /etc/stunnel/yahoo-smtps.conf
[smtp-tls-wrapper]
accept = 127.0.0.1:10465
client = yes
connect = smtp.mail.yahoo.com:465
```

После чего запускаем stunnel и проверяем работу

```
# stunnel /etc/stunnel/yahoo-smtps.conf
# telnet 127.0.0.1 10465
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
220 smtp.mail.yahoo.com ESMTP ready
quit
221 2.0.0 Bye
Connection closed by foreign host.
```

Теперь меняем в sasl_passwd и sender_relay_maps [smtp.mail.yahoo.com]:465 на [127.0.0.1]:10465. Не забываем пересоздать карты и перезапустить postfix.

```
# postmap sasl_passwd sender_relay_maps
# service postfix restart
```

И снова пробуем отправить почту. И получаем такое сообщение.

```
Mar 23 10:54:18 web-srv01 postfix/qmgr[24105]: BC42912083A:
from=<relay.test_2015@yahoo.com>, size=447, nrcpt=1 (queue active)
Mar 23 10:54:18 web-srv01 postfix/smtpd[24108]: disconnect from
localhost[127.0.0.1]
Mar 23 10:54:19 web-srv01 postfix/smtp[24111]: BC42912083A:
to=<relay.test.2015@mail.ru>, relay=127.0.0.1[127.0.0.1]:10465, delay=0.24,
delays=0.02/0.04/0.18/0, dsn=4.7.4, status=deferred (TLS is required, but
was not offered by host 127.0.0.1[127.0.0.1])
```

А связано оно с тем, что тунель итак уже шифрованный, за нас эту работу делает stunnel, поэтому нам надо указать postfix, что не нужно второй раз шифровать тунель. Для этого

добавим параметр smtp_tls_policy_maps

```
  smtp_tls_policy_maps = hash:/etc/postfix/tls_policy
```

```
# cat /etc/postfix/tls_policy
[127.0.0.1]:10465 none

# postmap /etc/postfix/tls_policy
# service postfix restart
```

Таким образом мы указываем postfix, что не нужно шифровать канал при обращении к 127.0.0.1:10465. И снова пробуем отправить письмо.

```
Mar 23 11:04:36 web-srv01 postfix/smtpd[24377]: BCD9312083A:
client=localhost[127.0.0.1]
Mar 23 11:04:36 web-srv01 postfix/cleanup[24379]: BCD9312083A: message-
id=<20150323150436.BCD9312083A@mail.example.net>
Mar 23 11:04:36 web-srv01 postfix/qmgr[24373]: BCD9312083A:
from=<relay.test_2015@yahoo.com>, size=447, nrcpt=1 (queue active)
Mar 23 11:04:36 web-srv01 postfix/smtpd[24377]: disconnect from
localhost[127.0.0.1]
Mar 23 11:04:38 web-srv01 postfix/smtp[24380]: BCD9312083A:
to=<relay.test.2015@mail.ru>, relay=127.0.0.1[127.0.0.1]:10465, delay=1.7,
delays=0.01/0.05/1.1/0.53, dsn=2.0.0, status=sent (250 OK , completed)
Mar 23 11:04:38 web-srv01 postfix/qmgr[24373]: BCD9312083A: removed
```

На этот раз все работает так, как нам нужно.

Подводные камни

На днях настраивал подобную схему и столкнулся с проблемой отправки письма. При этом в логах были подобные ошибки

```
# cat /var/log/maillog | grep 44D1A54801F9
Sep 16 10:33:12 vhem postfix/smtpd[29298]: 44D1A54801F9:
client=localhost[127.0.0.1]
Sep 16 10:33:12 vhem postfix/cleanup[29301]: 44D1A54801F9: message-
id=<20150916103312.44D1A54801F9@vhem.example.com>
Sep 16 10:33:12 vhem postfix/qmgr[29295]: 44D1A54801F9:
from=<root@example.com>, size=503, nrcpt=1 (queue active)
Sep 16 10:33:12 vhem postfix/smtp[29302]: 44D1A54801F9: to=<user@gmail.com>,
relay=smtp.googlemail.com[173.194.67.16]:587, delay=0.47,
delays=0.28/0.04/0.15/0, dsn=4.7.0, status=deferred (SASL authentication
failed; cannot authenticate to server smtp.googlemail.com[173.194.67.16]: no
mechanism available)
```

При этом из консоли через swaks все отправлялось без проблем. Как в итоге выяснилось, проблема была в том, что в системе не были установлены соответствующие модули для cyrus-sasl, а именно **cyrus-sasl-plain/cyrus-sasl-ldap/cyrus-sasl-md5**. А swaks работал потому, что

для аутентификации использует соответствующий perl модуль perl-Authen-SASL. Так что не забываем установить соответствующие модули.

```
# yum install cyrus-sasl-plain
```

Так как на момент написания статьи gmail поддерживал только следующие методы аутентификации

```
250-AUTH LOGIN PLAIN XOAUTH2 PLAIN-CLIENTTOKEN XOAUTH
```

то модуля cyrus-sasl-plain должно быть достаточно для корректной работы с gmail.