Postfix + STARTTLS

1. Генерируем сертификаты

Добавляем секции отвечающие за TLS

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

```
# TLS
 smtpd_use_tls = yes
 smtpd_tls_security_level = may
 smtpd_tls_auth_only = yes
 smtpd_tls_key_file = /usr/local/etc/postfix/device.key
 smtpd_tls_cert_file = /usr/local/etc/postfix/device.crt
 smtpd_tls_CAfile = /usr/local/etc/postfix/rootCA.pem
 smtpd_tls_loglevel = 1
 smtpd_tls_received_header = yes
 smtpd_tls_session_cache_timeout = 3600s
 tls_random_source = dev:/dev/urandom

# Аутентификация SMTP
 smtpd_sasl_auth_enable = yes
 smtpd_sasl_exceptions_networks = $mynetworks
 smtpd_sasl_security_options = noanonymous
 broken_sasl_auth_clients = yes
 smtpd_sasl_type = dovecot
 smtpd_sasl_path = private/auth
```

Далее, основываясь на рекомендациях mozilla, делаем так – в секции TLS дописываем
main.cf:

```
smtp_tls_mandatory_ciphers = high
smtp_tls_mandatory_protocols=!SSLv2,!SSLv3

tls_high_cipherlist = ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-
```

```
AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-
SHA:ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-
RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:DHE-RSA-AES128-
SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-
AES256-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-
SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK

smtpd_tls_mandatory_ciphers = high
smtpd_tls_mandatory_protocols=!SSLv2,!SSLv3
```

так мы еще оставляем самые *надежные*, на сегодня, алгоритмы.

Далее, раскоментируем в /usr/local/etc/postfix/master.cf секцию с *sabmission*

```
## Open 587 port for STARTTLS
submission inet n - n - - smtpd
  -o syslog_name=postfix/submission
  -o smtpd_tls_security_level=encrypt
  -o smtpd_sasl_auth_enable=yes
  # -o smtpd_tls_auth_only=yes
  -o smtpd_reject_unlisted_recipient=no
  # -o smtpd_client_restrictions=$mua_client_restrictions
  # -o smtpd_helo_restrictions=$mua_helo_restrictions
  # -o smtpd_sender_restrictions=$mua_sender_restrictions
  # -o smtpd_recipient_restrictions=
  -o smtpd_relay_restrictions=permit_sasl_authenticated,reject
  -o milter_macro_daemon_name=ORIGINATING

## Open 465 port for SSL/TLS
smtps inet n - n - - smtpd
  -o syslog_name=postfix/smtps
  -o smtpd_tls_wrappermode=yes
  -o smtpd_sasl_auth_enable=yes
```

Для Dovecot дописываем в *dovecot.conf*

```
# SSL (если нет то ="NO")
disable_plaintext_auth = yes
ssl = yes
ssl_cert = </usr/local/etc/postfix/device.crt
ssl_key = </usr/local/etc/postfix/device.key
## Disable SSLV3 - Poodle
```

```
ssl_protocols = !SSLv2 !SSLv3
##
```

В итоге при просмотре исходника письма в GMAIL заголовок такой:

```
Received: from smtp.279.ru (smtp.279.ru. [77.220.185.16])
by mx.google.com with ESMTP id
o79si14839747lfi.52.2016.02.15.04.15.43
for <deryabinsergey@gmail.com>;
Mon, 15 Feb 2016 04:15:43 -0800 (PST)
```

становится вот таким:

```
Received: from smtp.279.ru (smtp.279.ru. [77.220.185.16])
by mx.google.com with ESMTPS id
d124si14810044lfg.170.2016.02.15.04.20.45
for <deryabinsergey@gmail.com>
(version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256
bits=128/128);
Mon, 15 Feb 2016 04:20:45 -0800 (PST)
```

И появляется замочек в секции безопасность