

Secure_Outgoing_SMTP_via_Postfix,_Courier,_TLS_and_SASL

• OK. First off: apt-get

```
apt-get install postfix-tls libsasl2 sasl2-bin libsasl2-modules
```

Main Website used for Config: http://www.falkotimme.com/howtos/perfect_setup_debian_sarge/index.php

Secondard Website - however uses a different Auth file:

<http://www.tribulaciones.org/docs/postfix-sasl-tls-howto.html>

More Good Info & a SIMPLE WAY TO OVERCOME CHROOT -> http://wiki.ev-15.com/debian:mail_system

• Configing:

```
/etc/postfix/main.cf
```

```
/etc/postfix/sasl/smtpd.conf
```

```
/etc/postfix/ssl/* - tls certs
```

1.

```
# SASL Support
```

```
smtpd_sasl_local_domain =
```

```
smtpd_sasl_auth_enable = yes
```

```
smtpd_sasl_security_options = noanonymous
```

```
broken_sasl_auth_clients = yes
```

```
smtpd_recipient_restrictions = permit_sasl_authenticated,permit_mynetworks,reject_unauth_destination
```

2.

```
# SASL Auth
```

```
vi /etc/postfix/sasl/smtpd.conf
```

```
pwcheck_method: saslauthd
```

```
mech_list: plain login
```

3.

```
# TLS Certs
```

```
mkdir /etc/postfix/ssl
```

```
cd /etc/postfix/ssl/
```

```
openssl genrsa -des3 -rand /etc/hosts -out smtpd.key 1024
```

```
chmod 600 smtpd.key
```

```
openssl req -new -key smtpd.key -out smtpd.csr
```

```
openssl x509 -req -days 3650 -in smtpd.csr -signkey smtpd.key -out smtpd.crt
```

```
openssl rsa -in smtpd.key -out smtpd.key.unencrypted
```

```
mv -f smtpd.key.unencrypted smtpd.key
```

```
openssl req -new -x509 -extensions v3_ca -keyout cakey.pem -out cacert.pem -days 3650
```

```
# TLS Config in /etc/postfix/main.cf
```

```
# Moving onto TLS on its own.
```

```
smtpd_tls_auth_only = yes
```

```
smtp_use_tls = yes
```

```
smtpd_use_tls = yes
```

```
smtp_tls_note_starttls_offer = yes
```

```
smtpd_tls_key_file = /etc/postfix/ssl/smtpd.key
```

```
smtpd_tls_cert_file = /etc/postfix/ssl/smtpd.crt
```

```
smtpd_tls_CAfile = /etc/postfix/ssl/cacert.pem
```

```
smtpd_tls_loglevel = 1
```

```
smtpd_tls_received_header = yes
```

```
smtpd_tls_session_cache_timeout = 3600s
```

```
tls_random_source = dev:/dev/urandom
```

- **Restart Postfix**

Now continuing onto Auth

Because postfix runs chrooted - need to move the /var/run dir

```
mkdir -p /var/spool/postfix/var/run/saslauthd
rm -fr /var/run/saslauthd
```

Edit /etc/default/saslauthd

Remove # in front of START=yes

Add the line PARAMS="-m /var/spool/postfix/var/run/saslauthd"

Edit /etc/init.d/saslauthd

```
Add a # to dir=`dpkg-statoverride --list $PWDIR`
Add in dir="... below the PIDFILE entry
#dir=`dpkg-statoverride --list $PWDIR`
Change PWDIR and PIDFILE to the following:
PWDIR="/var/spool/postfix/var/run/${NAME}"
PIDFILE="${PWDIR}/saslauthd.pid"
dir="root sasl 755 ${PWDIR}"
```

- **Save & Close**
- **restart saslauthd**
- **/etc/init.d/saslauthd start**
- **MAKE SURE TO ADJUST FIREWALL - OPEN UP PORT 111 Locally**

Debugging and testing

```
user@otherserver:~$ telnet mail.burkesys.com 25
Trying 78.47.9.122...
Connected to mail.burkesys.com.
Escape character is '^]'.
220 mail.burkesys.com ESMTP Postfix (Debian/GNU)
ehlo localhost
250-mail.burkesys.com
250-PIPELINING
250-SIZE 20000000
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
```

After connecting via telnet, type "ehlo localhost" and watch for the "STARTTLS" line. This *should* show up.

Of course o2 have started filtering external traffic over port 25, and filtering out the starttls which makes life difficult for thunderbird. See: <http://markmail.org/message/v5uofqpx5l5pu4rm> Just as well I have port 587 open for use with a nice iptable rule:

```
iptables -t nat -A PREROUTING -p tcp --dport 587 -j DNAT --to ip.address:25
iptables -t nat -L
iptables -t nat -D PREROUTING 1
```