By Cameron Summers
Published: 2008-12-12 16:21

Postfix SMTP Authentication - On The Secure Port Only

So let's say your users are going away for holidays but need to use your mailserver to relay mail from outside the organisation... Let's set up SMTP authentication for the secure port only and allow access to this from outside your network.

[yourserver = server hostname]
[your-ip = your server's IP address]

```
cd /etc/postfix

vi main.cf
```

Paste under *mynetworks*:

```
####### smtp auth
smtpd_tls_auth_only = no
smtp_use_tls = yes
smtpd_sasl_auth_enable =  yes
smtpd_sasl_type = cyrus
local_recipient_maps =
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
########
```

Then:

```
vi master.cf
```

Paste under *smtp*:

```
smtps inet n - n - - smtpd
    -o smtpd_sasl_auth_enable=yes
    -o smtpd_reject_unlisted_sender=yes
    -o smtpd_recipient_restrictions=permit_sasl_authenticated,reject
    -o broken_sasl_auth_clients=yes
```

Check the smtpd.conf file and amend it:

```
locate smtpd.conf

vi /usr/lib/sasl2/smtpd.conf
```

Delete the contents of the file and paste into it:

```
pwcheck_method: saslauthd
mech_list: plain login
```

To check the SASL available mechanisms run:

```
saslauthd -V
```

Set SASL authentication to start at system boot:

```
chkconfig --levels 235
saslauthd on
```

Set up the encryption keys:

```
mkdir /etc/postfix/ssl

cd 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
```

Set up the client certificate for importing into Internet Explorer (for Outlook) / Thunderbird (this will suppress warnings about using a selfsigned certificate):

```
openssl pkcs12 -export
-in smtpd.crt -inkey smtpd.key -out OutlookSMTP.p12
```

Reload the config:

```
postfix reload
```

Finally insert a relevant iptables rule to access from outside usingyour firewall script:

```
$IPTABLES -A INPUT -i $EXTIF -p tcp -s $UNIVERSE -d $EXTIP --destination-port 465 -j ACCEPT
```

Or if your mail server is behind a firewall (Assuming the LAN addressof your server is 10.10.1.4), add these rules on your firewall:

```
$IPTABLES -A FORWARD -i   $EXTIF -p tcp --dport 465 -d 10.10.1.4 -o $INTIF -j ACCEPT
$IPTABLES -A FORWARD -o   $EXTIF -p tcp --sport 465 -s 10.10.1.4 -i $INTIF -j ACCEPT
$IPTABLES -t nat -A PREROUTING -i $EXTIF -p tcp -d $EXTIP2 --dport 465 -j DNAT --to 10.10.1.4:465
```

Done!

Testing

Check if the port is listening:

```
netstat -ntpl | grep
master
```

```
tcp      0     0     127.0.0.1:10025   0.0.0.0:*       LISTEN   8366/master
  tcp      0     0      0.0.0.0:465       0.0.0.0:*       LISTEN   8366/master
  tcp      0     0      0.0.0.0:25        0.0.0.0:*       LISTEN    8366/master
```

Test if TLS and AUTH is working:

```
telnet localhost 465
```

```
[root@ls1 postfix]#  telnet localhost 465
  Trying 127.0.0.1...
  Connected to  localhost.localdomain (127.0.0.1).
  Escape character is '^]'.
  220 yourserver ESMTP  Postfix
  ehlo me
  250-yourserver
  250-PIPELINING
  250-SIZE 10240000
  250-VRFY
  250-ETRN
  250-STARTTLS
  250-AUTH LOGIN PLAIN
  250-AUTH=LOGIN PLAIN
  250 8BITMIME
  ^]
  telnet> quit
  Connection closed.
  [root@ls1 postfix]#
```

To test further create an account and attain the Base64 Mime password with mmencode or the following perl script:

```
#!/usr/bin/perl
use strict;
use MIME::Base64;
if ( $#ARGV !=1) {
  die "Usage: encode_sasl_plain.pl <username> <password>n";
}
print encode_base64("$ARGV[0]?$ARGV[0]?$ARGV[1]");
exit 0;
```

Generate the Mime password:

```
encode_sasl_plain.pl <username> <password>
```

Y2FtZXJvbnMAY2FtZXJvbnMAdGVzdGluZzA4

```
telnet localhost 465
```

```
Trying 127.0.0.1...
Connected to localhost.localdomain (127.0.0.1).
Escape character is '^]'.
220 yourserver ESMTP Postfix
```

ehlo me
250-yourserver
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS

250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
AUTH PLAIN Y2FtZXJvbnMAY2FtZXJvbnMAdGVzdGluZzA4
235 2.0.0 Authentication successful

**If the authentication is not successful, you may have to change the MECH value in */etc/sysconfig/saslauthd* and */etc/init.d/saslauthd*.

Possible values are listed with the command

```
saslauthd -V
```

and restart saslauthd:

```
/etc/init.d/saslauthd
restart
```

Test the connection from outside:

```
telnet
yourserver
```

465

cameron@cs:~$ telnet yourserver 465
Trying your-ip...
Connected to yourserver.
Escape character is '^]'.
220 yourserver ESMTP Postfix
ehlo me

```
250-yourserver
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH PLAIN LOGIN
250-AUTH=PLAIN LOGIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
AUTH PLAIN  Y2FtZXJvbnMAY2FtZXJvbnMAdGVzdGluZzA4
235 2.0.0 Authentication  successful
```

To test further, set up an account in Evolution / Thunderbird / Outlook and test the SMTP with the username and password you set up earlier.

Remember that because you are using a self signed certifcate, your email client will prompt you each time about an untrusted certificate so you can use the client certificate you created to suppress these warnings.

For Thunderbird, if you are really lazy you can even install **this addon**.