Postfix SSL HOWTO

Postfix SSL HOWTO

Justin Davies

v1.0, December 2002

This is an introduction to the use of TLS/SSL with the Postfix MTA. Using TLS can provide the user with a means to encrypt the mail connection, to encrypt plaintext authentication. Using TLS, you can also authenticate a user based on a private key to allow mail relaying.

1. Introduction

2. Postfix as a TLS Server

- 2.1 Configuration paramaters
- 2.2 Testing TLS

3. Postfix as a TLS client

- 3.1 Configuring the client
- 3.2 Generating the fingerprint

4. Setting up the server to relay based on fingerprints

- 4.1 Server relay configuration

5. Finishing Up

6. Links

Next Previous Contents Next Previous Contents

1. Introduction

Postfix and SSL Postfix is one of the most popular e−mail servers after Sendmail. It benefits from most of Sendmail's features, but is a lot easier to install and maintain. Where Sendmail uses m4 files for configuration, Postfix uses the familiar *key=value* configuration files. SSL provides a way to encrypt a connection based on certificates. For more information on SSL and certificates, make sure you read Introduction to SSL on the site. Postfix and SSL can provide a way to allow relaying from dynamic IP addresses (road warriors). It bases its decision on whether to allow the client to relay if the certificate offered by the client is registered in a Postfix hash table. It also encrypts the channel between the client and the server, providing that little bit of extra security.

Next Previous Contents Next Previous Contents

2. Postfix as a TLS Server

Postfix on SuSE comes built with support for SSL/TLS, so all that is needed is configuration of the server to allow SSL connections. The first thing you need to do is create the server certificate as detailed in the Introduction to SSL. You need to copy the server key and the server certificate to the /etc/postfix directory. It is very important that you change the permissions on the server private key:

```
chown root.root server.key
chmod 400 server.key
```

2.1 Configuration paramaters

Edit the /etc/postfix/main.cf

Add the following lines to the end of the document...

```
# Other configurable parameters.
smtpd_tls_key_file = /etc/postfix/zen.key
smtpd_tls_cert_file = /etc/postfix/zen.pem
smtpd_tls_CAfile = /etc/postfix/CAcert.pem
smtpd_use_tls = yes
```

smtpd_tls_key_file is the location of the server private key.
smtpd_tls_cert_file is the location of the server certificate.
smtpd_tls_CAfile is the location of the Certificate Authority certificate (needed to verify the certificates).
smtpd_use_tls TLS is not active by default. You need to specifically tell the Postfix server that it should support TLS.

2.2 Testing TLS

Once the server configuration is complete, restart Postfix and check that TLS has been activated:

```
justin@zen:~> telnet mail.suse.co.uk 25
Trying 10.32.0.1...
Connected to mail.suse.co.uk.Escape character is ^]

220 mail.suse.co.uk
ESMTP Postfix
EHLO zen.suse.co.uk
250-mail.suse.co.uk
250-PIPELINING
250-SIZE 10240000250-ETRN
250-STARTTLS
250 8BITMIME
STARTTLS
220 Ready to start TLS
```

The server response of **"220 Ready to start TLS"** after issuing the **STARTTLS** signifies that the server is willing to communicate over TLS.

At this point, look at */var/log/mail* to see if there are any errors.
TLS will warn you if a certificate can not be loaded, or if TLS cannot be started for some reason.

3. Postfix as a TLS client

Postfix can act as a client to a master mail server. This is where SSL/TLS becomes really useful...

In a large domain, many mail servers may be used for each department. Linking these servers up can be accomplished by giving the Postfix system a default host to relay mail to. You can then force the Postfix client to authenticate against the master server using a client certificate.
Using certificates to authenticate to an SMTP server allows you to setup a secure mail relaying system for clients. This becomes very beneficial when you are dealing with "road warriors", as relaying based on an IP address is not possible due to the fact that the IP address of the client machine changes every time the user dials into their ISP.
Using a client certificate will allow you to authenticate against the mail server to allow realying. And benificial side effect of this is that all communication to the mail server is encrypted for the duration of the session.

3.1 Configuring the client

As is familiar to most thing in Postfix, the server uses a hash table for lookups of the client authentication data. Using The way the Postfix implementation of TLS works with regards to relaying is based on a finger−print of the client certificate. This allows the server to use a lookup map to see if a fingerprint of the client certificate offered is in the map. If it is, the client is allowed to relay mail. If the fin−gerprint is not found, the client is given the usual **"Relay access denied"** message from the server. The location of the fingerprint hash table file is */etc/postfix/relay_clients*. The format of the file is:

```
fingerprint value
```

The "value" key above is anything you want. Postfix needs to have a hash pair to be able to convert the hash to a map. It is best to use the hostname of the client machine, to be able to distinguish the owner of the certificate fingerprint.

3.2 Generating the fingerprint

To generate the fingerprint of the certificate, run the following command:

```
openssl x509 −fingerprint −in ./certificate.pem
```

This will produce the MD5 fingerprint of the key. Copy the fingerprint to the file */etc/postfix/relay_clients* (create it if it doesn't exist). You should have something like this:

```
95:B4:G5:87:D7:34:CA:C4:27:B0:F3:8F:66:8A:77:8D zen.suse.co.uk
```

Once this has been done, convert the file to a map:

```
postmap /etc/postfix/relay_clientcerts
```

The owner of the certificate that corresponds to the above fingerprint will be able to relay through the server.

4. Setting up the server to relay based on fingerprints

When relaying, Postfix runs through a set of rules to determine if the client machine is allowed to relay mail through the server. We need to tell Postfix that all users specified in the relay_clientcerts file are allowed to relay mail. To do this we add permit_tls_clientcerts to the **smtpd_recipient_restrictions** statement in *main.cf*. There is another relay option that can be used to allow relaying if the client certificate can be verified (can be trusted via a CA). For a small installation, it is better to use the **permit_tls_clientcerts** statement as it allows individual control over users.

4.1 Server relay configuration

The server is now setup to allow relaying via certificate authentication. We still need to setup the client configuration to talk to the server, and authenticate using its client certificate. The client setup is relatively painless. You only need to add a few lines to the *main.cf* file, and setup relaying to the server. Edit the *main.cf* file on the client machine, adding the following lines:

```
smtp_tls_key_file = /etc/postfix/zen.key
smtp_tls_cert_file = /etc/postfix/zen.pem
smtp_tls_CAfile = /etc/postfix/CAcert.pem
smtp_use_tls = yes
```

As you can see, it is very similar to the server configuration, apart from the fact that it refers to "smtp", not "smtpd". The values mean exactly the same thing as the server configuration. For relaying, you have two options. You can specify a default route for all mail via the **relayhost** parameter in *main.cf*, or you can setup the transport map to route your mail based on client rules. I cannot tell you the best way to go on this one. Only that if you are only going to be using one mail hub, specify it in *main.cf* via the relayhost parameter. If you use multiple hubs (many large organisations do), use the transport map.

For more information about the transport map, see the *transport(5)* man page. In our case, we will choose the **relayhost** mechanism to relay all mail through a server:

```
relayhost = [mail.organisation.co.uk]
```

Next Previous Contents Next Previous Contents

5. Finishing Up

To complete the setup, save *main.cf* and restart the Postfix server. Send a test mail and view the log file */var/log/mail*. You should see the mail relay through your mail hub. Check the log file on the mail hub to see if the mail was successfully sent. If not, check the system log file */var/log/messages*. Postfix will log SSL transactions in the system log. If a mail cannot be sent, it can be diagnosed via the system log file. For more information about Postfix, take a look at the man pages. The Postfix man pages are some of the best I have seen. They are clear and concise, making a sys admin's job a lot easier.

Next Previous Contents Next Previous Contents

6. Links

- Postfix Home
- Postfix/TLS Home
- Home of the Postfix/TLS HOWTOS

Next Previous Contents