

Creating a SSL/TSL connection for FTP

Contributed by Administrator
Saturday, 18 November 2006
Last Updated Thursday, 25 October 2007

Using Secure FTP is a great way to add security to your site. Regular FTP sends the username and password in plain text.

Using Secure FTP is a great way to add security to your site. Regular FTP sends the username and password in plain text. To Secure your FTP connection there is two choices SSH and SSL. SSH uses a secure shell. The problem with using Secure Shell (SSH) for SFTP is that the user must have a username and password for the Linux server. Of course this would not be a username with root access, but even without root access the username and password in the wrong hands can be very dangerous. It can be very time consuming and confusing for a Linux noobie to allow the ssh username access to FTP only. The answer to this is FTP over SSL or TLS (FTPS). Unfortunately this isn't enabled by default on most servers. You can test your server by selecting FTP over TLS in you FTP Client. When the connection is successful you maybe asked if you would like to connect to the server issuing the certificate. If the connection could not be established some code has to be added in the proftpd.conf file. I did this on my CentOS 4 server running Plesk 8.0.1. Open up a SSH connection to your server using Putty for Windows or open a terminal in Linux/Mac and type the line below replacing the username and ip address with yours:

```
ssh username @ 68.168.155.89
```

-or-

```
ssh -l username 68.168.155.89
```

We need to create a Certificate to use for SSL. First we need a place to store it. I created my own directory.

```
cd /etc/
```

```
mkdir ssl
```

```
cd ssl/
```

```
mkdir certs
```

```
cd certs/
```

Now we will generate a Certificate. I used the default values by just pressing enter when prompted.

```
openssl req -new -x509 -days 365 -nodes -out /etc/ssl/certs/proftpd.cert.pem -keyout /etc/ssl/certs/proftpd.key.pem
```

Generating a 1024 bit RSA private key

```
.....++++++
```

```
.....++++++
```

```
writing new private key to '/etc/ssl/certs/proftpd.key.pem'
```

```
-----
```

You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter '.', the field will be left blank.

```
-----
```

Country Name (2 letter code) [AU]:

State or Province Name (full name) [Some-State]:

Locality Name (eg, city) []:

Organization Name (eg, company) [Internet Widgits Pty Ltd]:

Organizational Unit Name (eg, section) []:

Common Name (eg, YOUR name) []:

Email Address []:

Below is the code we will be entering in the proftpd.conf

```
TLSEngine on
```

```
TLSLog /var/log/tls.log
```

```
TLSProtocol SSLv23
```

```
TLSRequired off
```

```
TLSOptions NoCertRequest  
TLRSACertificateFile /etc/ssl/certs/proftpd.cert.pem
```

```
TLRSACertificateKeyFile /etc/ssl/certs/proftpd.key.pem
```

```
TLSVerifyClient off
```

Next we will back up the proftpd.conf file and open it using a text editor.

```
cd /etc/
```

```
cp proftpd.conf proftpd.conf.bak
```

```
vi proftpd.conf
```

Paste in the code above to make the proftpd.conf file look like the one below.

```
#
```

```
# To have more informations about Proftpd configuration
```

```
# look at : http://www.proftpd.org/
```

```
#
```

```
# This is a basic ProFTPD configuration file (rename it to
```

```
# 'proftpd.conf' for actual use. It establishes a single server
```

```
# and a single anonymous login. It assumes that you have a user/group
```

```
# "nobody" and "ftp" for normal operation and anon.
```

```
ServerName "ProFTPD"
```

```
ServerType inetd
```

```
ServerType inetd
```

```
DefaultServer on
```

```
<Global>
```

```
DefaultRoot ~ psacln
```

```
AllowOverwrite on
```

```
</Global>
```

```
DefaultTransferMode binaryUseFtpUsers on
```

```
# Port 21 is the standard FTP port.
```

```
Port 21
```

```
# Umask 022 is a good standard umask to prevent new dirs and files
```

```
# from being group and world writable.
```

```
Umask 022
```

```
# To prevent DoS attacks, set the maximum number of child processes
```

```
# to 30. If you need to allow more than 30 concurrent connections
```

```
# at once, simply increase this value. Note that this ONLY works
```

```
# in standalone mode, in inetd mode you should use an inetd server
```

```
# that allows you to limit maximum number of processes per service
```

```
# (such as xinetd)
```

```
MaxInstances 30
```

```
#Following part of this config file were generate by PSA automatically
```

```
#Any changes in this part will be overwritten by next manipulation
```

```
#with Anonymous FTP feature in PSA control panel.
```

#Include directive should point to place where FTP Virtual Hosts configurations

#preserved

ScoreboardFile /var/run/proftpd/scoreboard

Primary log file must be outside of system logrotate province

TransferLog /opt/psa/var/log/xferlog

#Change default group for new files and directories in vhosts dir to psacn

<Directory /var/www/vhosts>

 GroupOwner psacn

</Directory>

Enable PAM authentication

AuthPAM on

AuthPAMConfig proftpd

TLS

TLSEngine on

TLSLog /var/log/tls.log

TLSProtocol SSLv23

TLSRequired off

TLSOptions NoCertRequest

TLSRSACertificateFile /etc/ssl/certs/proftpd.cert.pem

TLSRSACertificateKeyFile /etc/ssl/certs/proftpd.key.pem

TLSVerifyClient off

delay on login off

IdentLookups off

UseReverseDNS off

AuthGroupFile /etc/group

Include /etc/proftpd.include

Now restart proftpd or apache and you should be able to connect by setting your FTP client to use TLS. My favorite client for Windows is Filezilla on a Mac I prefer Yummy FTP.

When you are able to connect using TLS I would recommend enforcing the client to use FTPS. This can be done by modifying the proftpd.conf file again.

Change:

TLSRequired off

To This:

TLSRequired on

If you are still having trouble consider some of the sources below:

Proftpd - The Proftpd website.

EV1Servers - A forum from a hosting company.

mod_tls - Just a forum for TLS on the Proftpd website.