

Sommaire :

Sommaire :	1
Introduction.....	1
1 – Installation du serveur ProFTPD :	2
2 – Mise en place du SSL :	4
3 – Configuration du FTPS :	5

Introduction

Objectif : L'objectif de ce TP est de créer sa propre autorité de certification afin de créer des certificats pour sécuriser les communications entre les services et les clients.

Pré-requis : Il faut des connaissances en sécurité TLS/SSL et en service FTP.

Norme : Toutes les commandes issues d'une machine avec un système d'exploitation Debian ou Windows sont écrites ***en gras et en italique***.

1 – Installation du serveur ProFTPd :

apt install proftpd

```
root@sebftp:~# apt-get install proftpd
```

Paramétrer le serveur en mode standalone. (Indépendamment)



Attention, tous les utilisateurs se connectant sur le serveur Proftp doivent exister réellement sur le système (avec un UID).

Il faut créer la section anonymous pour que les clients puissent se connecter sans authentification, en fait au nom de l'utilisateur ftp, dont le répertoire personnel est /home/ftp, et qui n'a pas de shell, comme le confirme l'examen de /etc/passwd.

```
root@sebftp:~# nano /etc/proftpd/proftpd.conf
```

```
GNU nano 2.2.6 Fichier : proftpd.conf
<Anonymous ~ftp>
User ftp
Group nogroup
# # We want clients to be able to login with "anonymous" as well as "ftp"
UserAlias anonymous ftp
# # Cosmetic changes, all files belongs to ftp user
DirFakeUser on ftp
DirFakeGroup on ftp

RequireValidShell off

# # Limit the maximum number of anonymous logins
MaxClients 10

# # We want 'welcome.msg' displayed at login, and '.message' displayed
# # in each newly chdir'd directory.
DisplayLogin welcome.msg
DisplayChdir .message

# # Limit WRITE everywhere in the anonymous chroot
<Directory *>
  <Limit WRITE>
    DenyAll
  </Limit>
</Directory>

# # Uncomment this if you're brave.
# # <Directory incoming>
# # # Umask 022 is a good standard umask to prevent new files and dirs
# # # (second parm) from being group and world writable.
# # Umask 022 022
# # # <Limit READ WRITE>
# # # DenyAll
# # # </Limit>
# # # <Limit STOR>
# # # AllowAll
# # # </Limit>
# # </Directory>
</Anonymous>

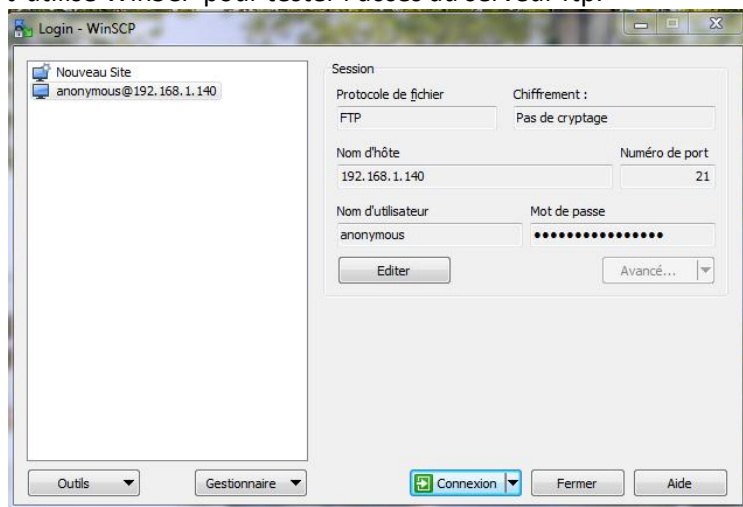
# Include other custom configuration files
Include /etc/proftpd/conf.d/
```

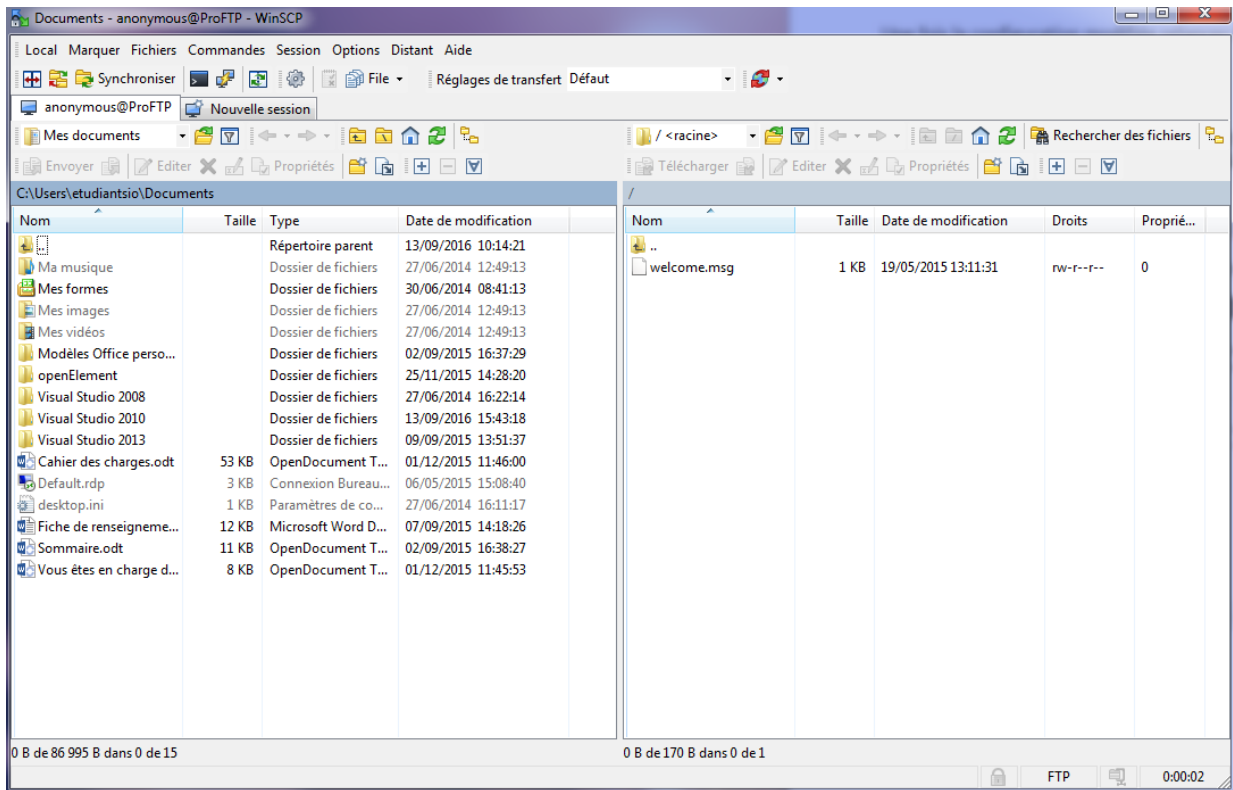
Une fois la configuration modifiée relancez le serveur.

reboot

Le fichier de configuration est [/etc/proftpd/proftp.conf](#).

J'utilise WinSCP pour tester l'accès au serveur ftp.





On remarque que l'on accède à notre serveur.

2 – Mise en place du SSL :

Voir procédure.

3 – Configuration du FTPS :

<http://www.pierre-galvez.fr/Installer-un-serveur-FTP-%28ProFTPd%29-securise-sur-Debian/>

https://doc.ubuntu-fr.org/proftpd_et_tls_ssl

Nous allons nous connecter en FTPS explicite.

Il faut créer un nouveau certificat autosigné avec la commande :

openssl req -x509 -nodes -days 365 -newkey rsa:1024 -out proftpd-rsa.pem -keyout proftpd-key.pem

```
sebastien@debianseb:~/tpssl$ tree
.
├── cacert.pem
├── certs
│   ├── newreq.pem
│   ├── proftpd-rsa.pem
│   └── webcert.pem
├── crl
├── index.txt
├── index.txt.attr
├── index.txt.old
├── newcerts
│   └── 01.pem
├── openssl.cnf
├── private
│   ├── cakey.pem
│   ├── proftpd-key.pem
│   └── webkey.pem
├── rootca.tar.gz
├── serial
└── serial.old
```

Puis, inclure le fichier de configuration `tls.conf` dans `/etc/proftpd/proftpd.conf` :

```
# Includes DSO modules
Include /etc/proftpd/modules.conf
Include /etc/proftpd/tls.conf_
```

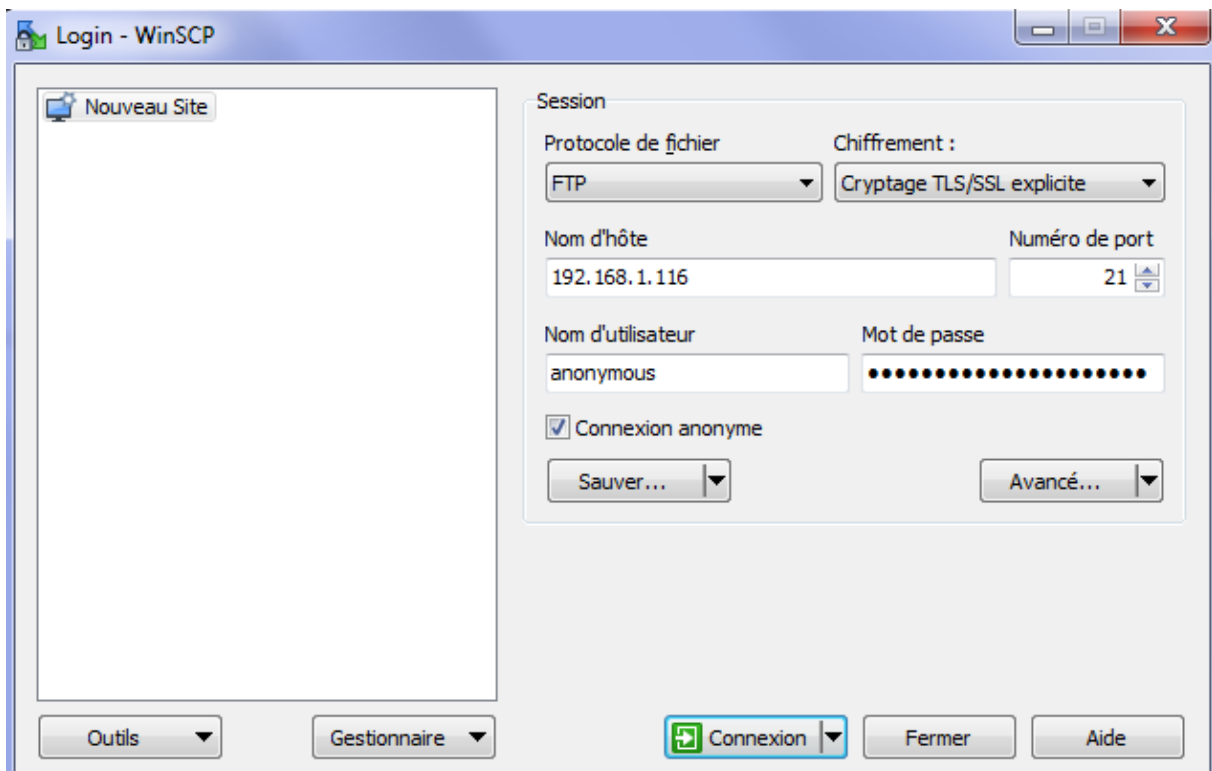
Il faut ensuite modifier le fichier `/etc/proftpd/tls.conf` :

```
<IfModule mod_tls.c>
TLSEngine                on
TLSLog                   /var/log/proftpd/tls.log
TLSProtocol               SSLv23
TLRSACertificateFile     /home/sebastien/tpssl/certs/proftpd-rs$
TLRSACertificateKeyFile  /home/sebastien/tpssl/private/proftpd-$
TLSVerifyClient          off
#
# Are clients required to use FTP over TLS when talking to this server?
#
TLSRequired               on
```

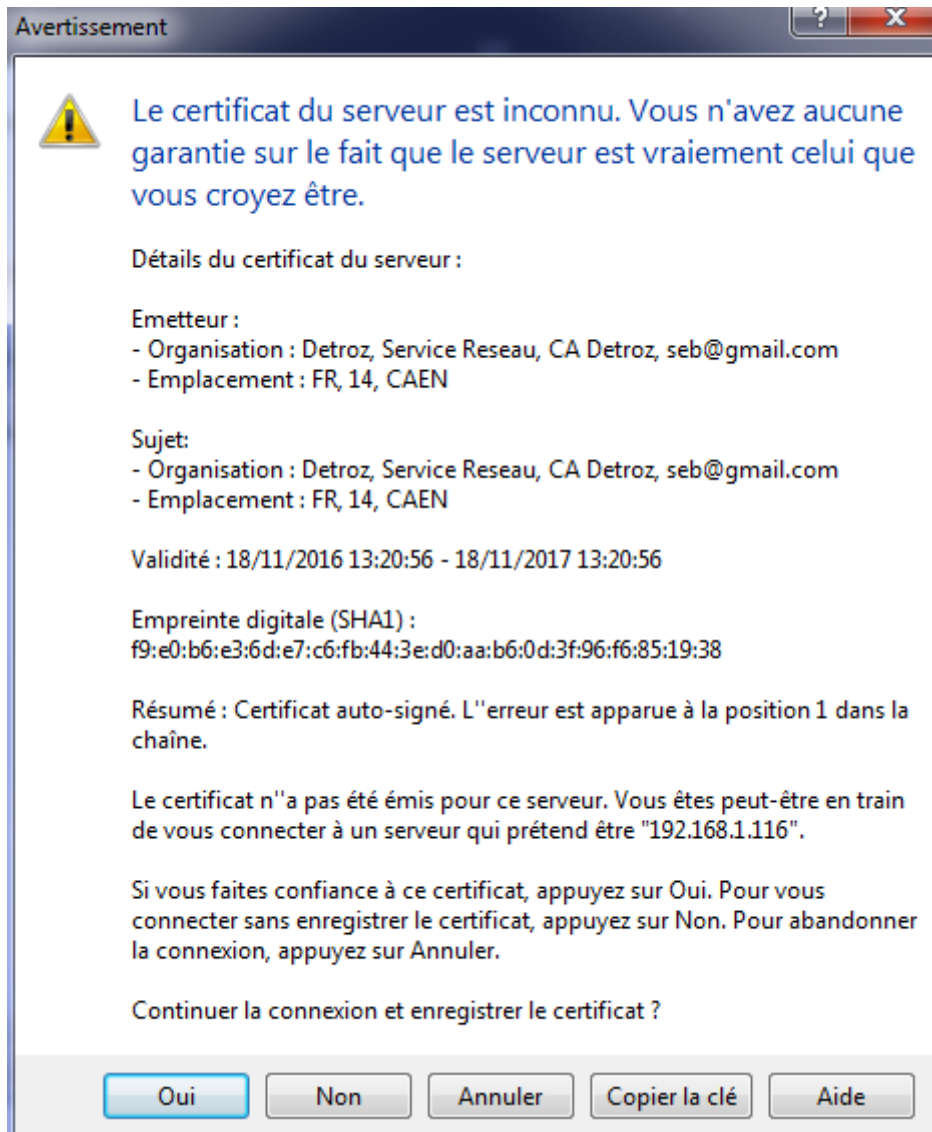
On redémarre le service :

```
root@debianseb:~# service proftpd restart
```

On se connecte ensuite en TLS/SSL explicite :



On accepte le certificat :



Et on est connecté :

