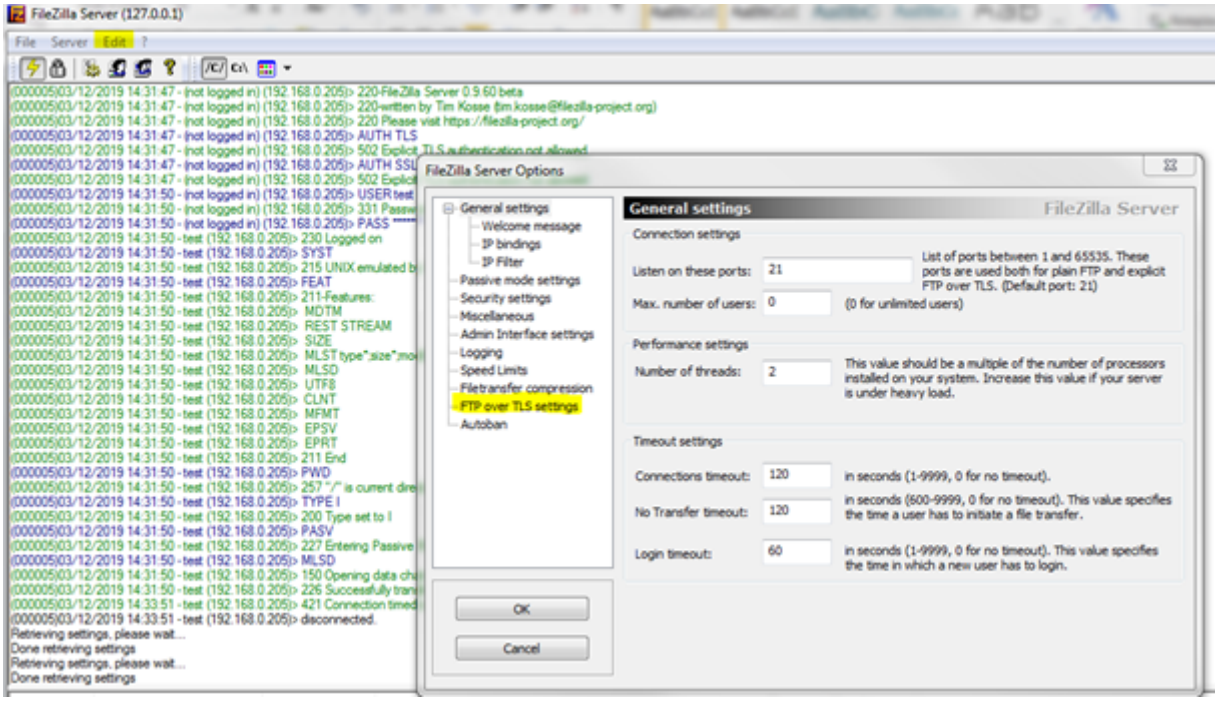
Serveur FTP sécurisé

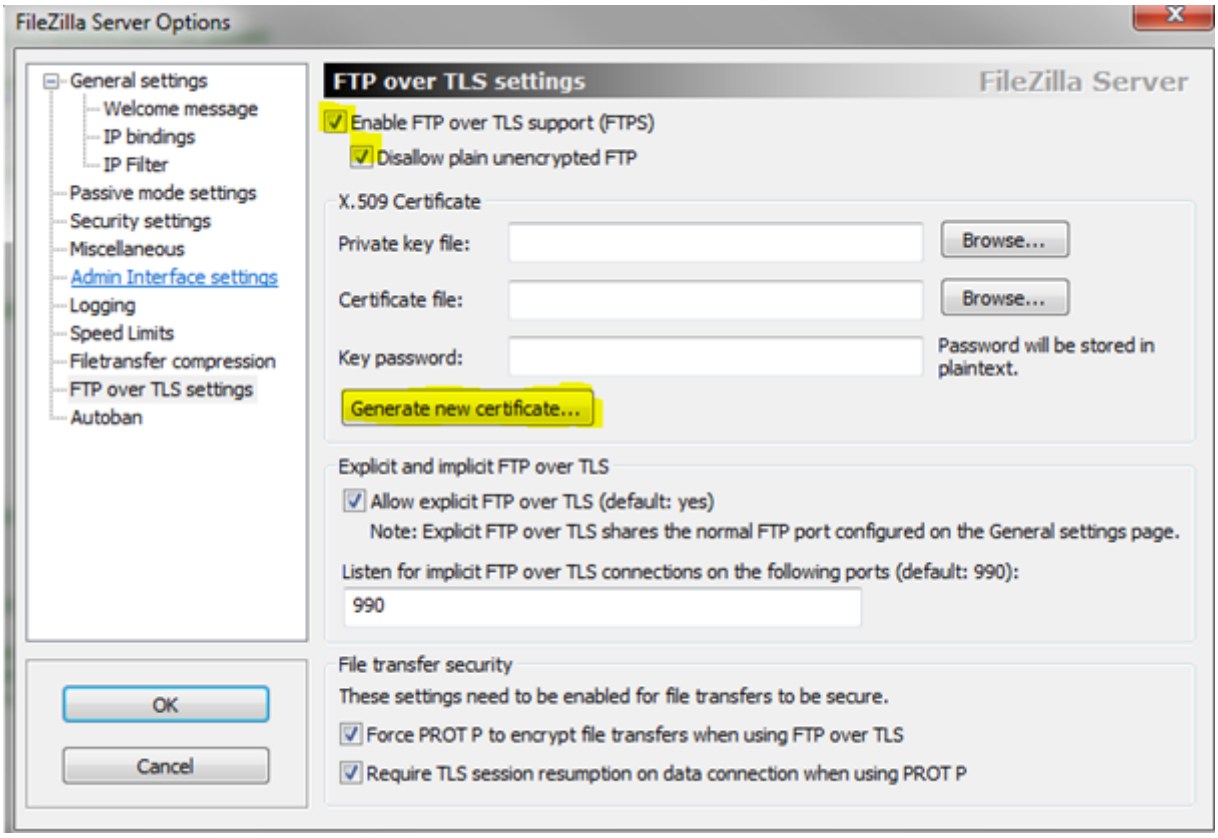
Il est important de sécuriser le serveur FTP, en utilisant le SFTP ou le FTPS.

Le FTPS est le protocole FTP avec une couche SSL, exigeant un certificat.

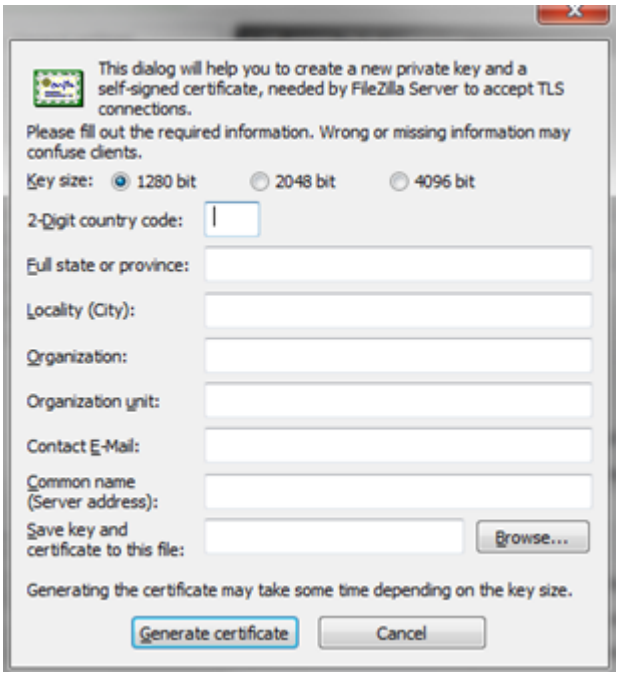
Le SFTP est le transfert de fichiers via SSH (port 22). On pourrait parler de transfert FTP encapsulé dans un tunnel SSH sécurisé.



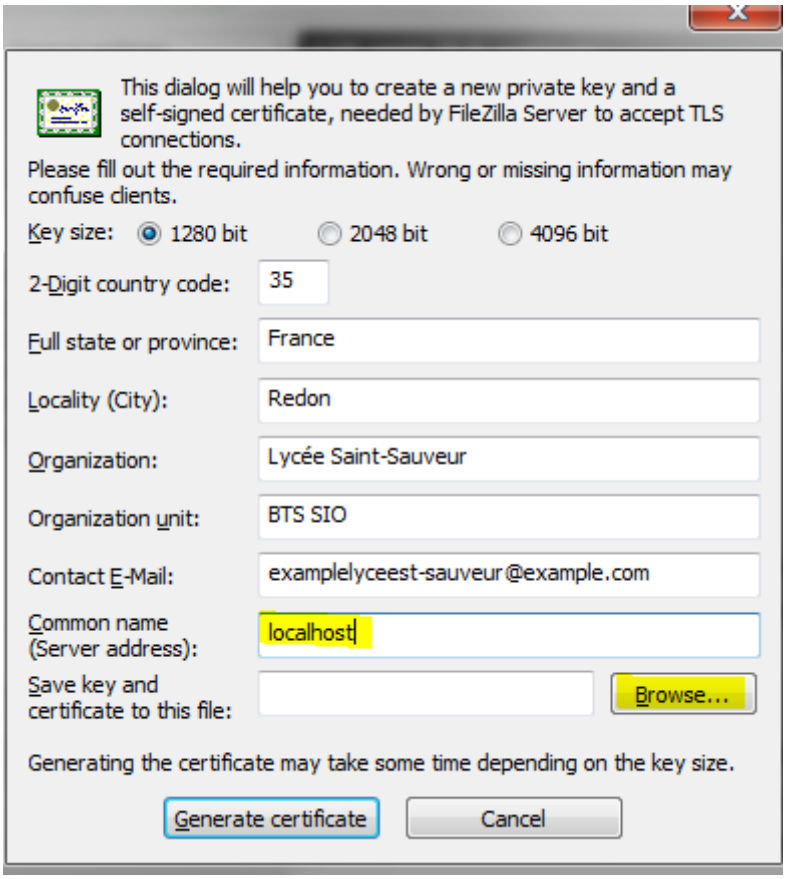
Au niveau du FileZilla Serveur, cliquez sur « Edit » et « Settings », puis l’onglet « FTP over TLS settings ».



On coche les deux premières cases afin de sécuriser le FTP, puis on clique sur « Generate new certificate… » afin de générer un certificat SSL et d’accepter les connexions TLS.

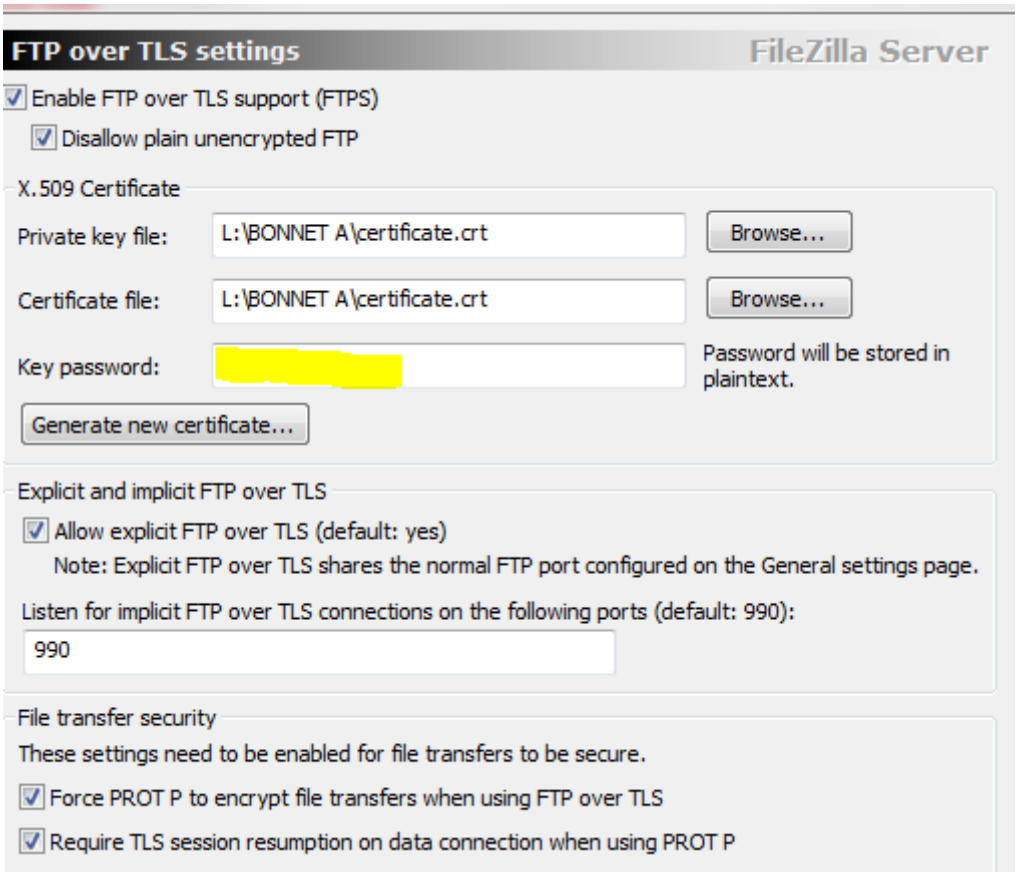


On rentre ensuite les données, par exemple :



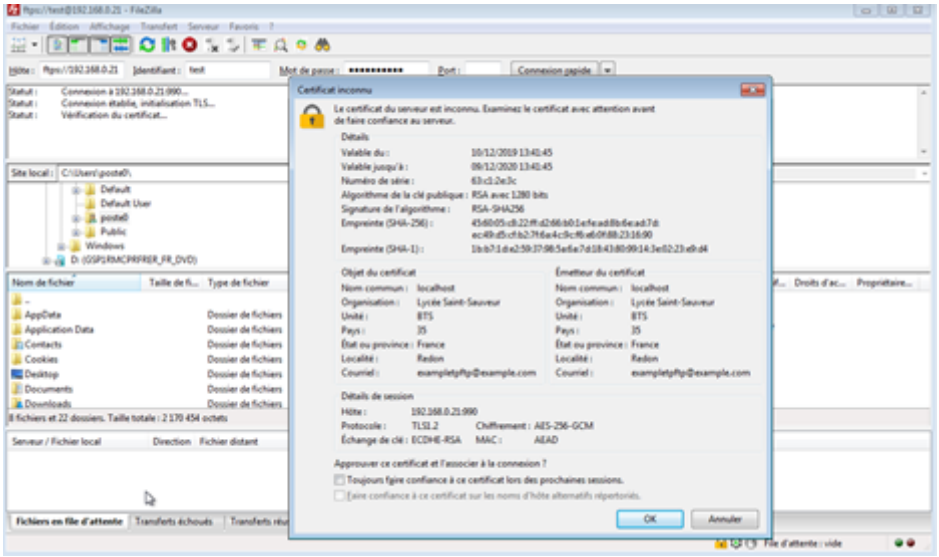
On rentre l’adresse du serveur dans « Common name », ici « localhost » ou l'adresse IP du serveur FTP.

On clique sur « Browse » et on choisit l’emplacement du certificat puis on clique sur « Generate certificate ».



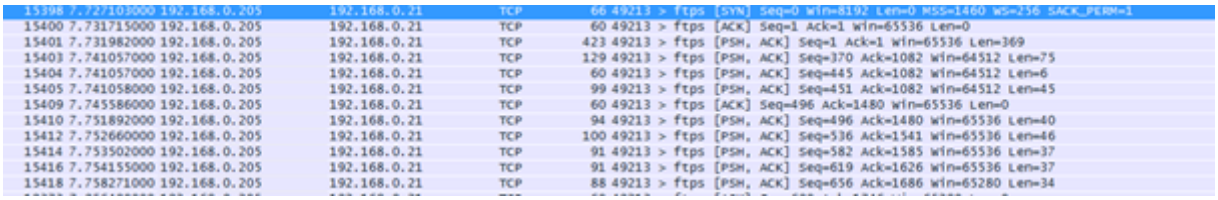
On rentre ensuite un mot de passe puis on clique sur « OK ». Les connexions sont désormais sécurisées et chiffrées.

On peut alors se connecter au serveur via FileZilla Client.



On obtient ce message car le certificat est inconnu des . Pour plus de sécurité, il est nécessaire d’acheter un certificat auprès d’une entreprise reconnue ou de le générer avec Let's Encrypt en utilisant un domaine.

Avec Wireshark lors d'une connexion et transfert de fichiers :



```
15398 7.727103000 192.168.0.205 192.168.0.21 TCP 66 49213 > ftps [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
15400 7.731715000 192.168.0.205 192.168.0.21 TCP 60 49213 > ftps [ACK] Seq=1 Ack=1 Win=65536 Len=0
15401 7.731982000 192.168.0.205 192.168.0.21 TCP 423 49213 > ftps [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=369
15403 7.741057000 192.168.0.205 192.168.0.21 TCP 129 49213 > ftps [PSH, ACK] Seq=370 Ack=1082 Win=64512 Len=75
15404 7.741057000 192.168.0.205 192.168.0.21 TCP 60 49213 > ftps [PSH, ACK] Seq=445 Ack=1082 Win=64512 Len=6
15405 7.741058000 192.168.0.205 192.168.0.21 TCP 99 49213 > ftps [PSH, ACK] Seq=451 Ack=1082 Win=64512 Len=45
15409 7.745586000 192.168.0.205 192.168.0.21 TCP 60 49213 > ftps [ACK] Seq=496 Ack=1480 Win=65536 Len=0
15410 7.751892000 192.168.0.205 192.168.0.21 TCP 94 49213 > ftps [PSH, ACK] Seq=496 Ack=1480 Win=65536 Len=40
15412 7.752660000 192.168.0.205 192.168.0.21 TCP 100 49213 > ftps [PSH, ACK] Seq=536 Ack=1541 Win=65536 Len=46
15414 7.753502000 192.168.0.205 192.168.0.21 TCP 91 49213 > ftps [PSH, ACK] Seq=582 Ack=1585 Win=65536 Len=37
15416 7.754155000 192.168.0.205 192.168.0.21 TCP 91 49213 > ftps [PSH, ACK] Seq=619 Ack=1626 Win=65536 Len=37
15418 7.758271000 192.168.0.205 192.168.0.21 TCP 88 49213 > ftps [PSH, ACK] Seq=656 Ack=1686 Win=65280 Len=34
```

Ici, nous ne voyons plus les identifiants de l’utilisateur.

Pour plus de sécurité, on peut restreindre l'accès au serveur sur une certaine plage d'adresse IP, et changer le port par défaut.

Revision #1
Created 2021-02-14 12:12:27 UTC by Khroners
Updated 2021-02-14 13:23:12 UTC by Khroners