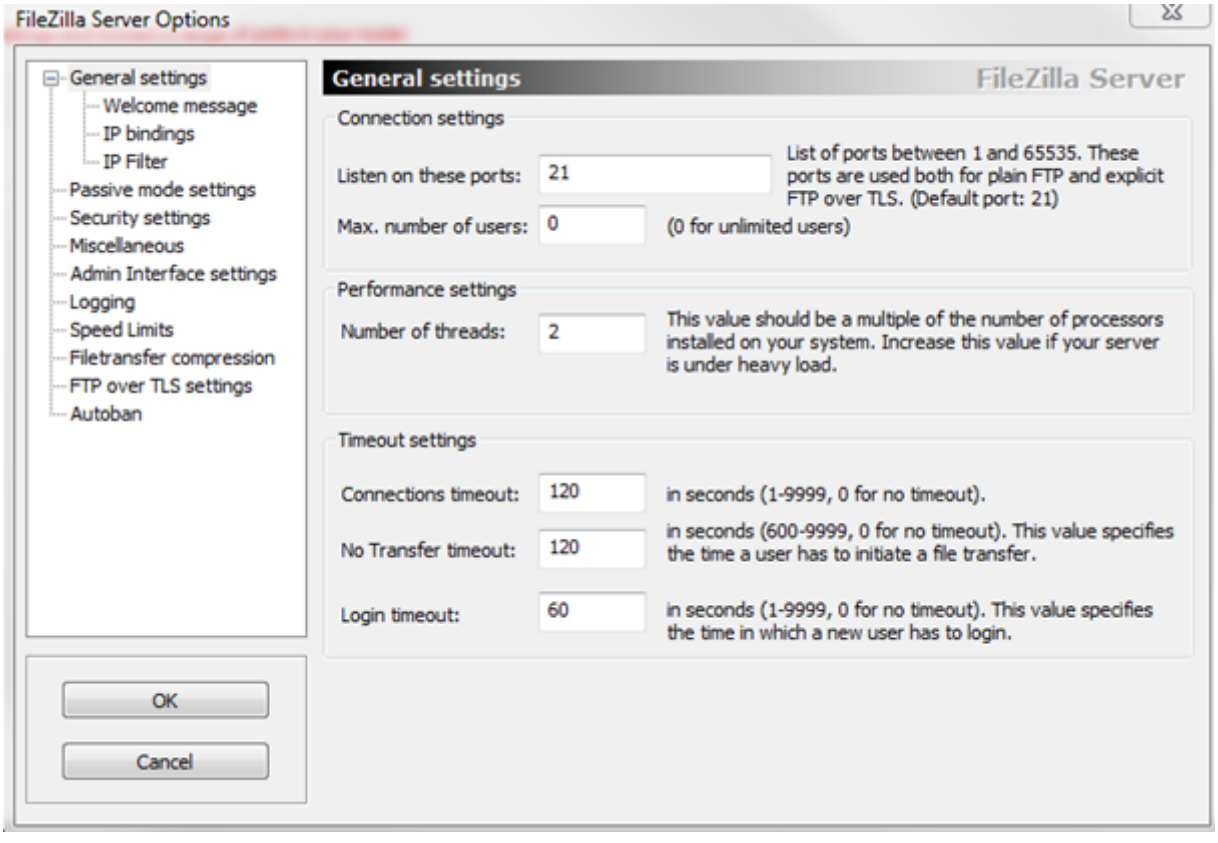
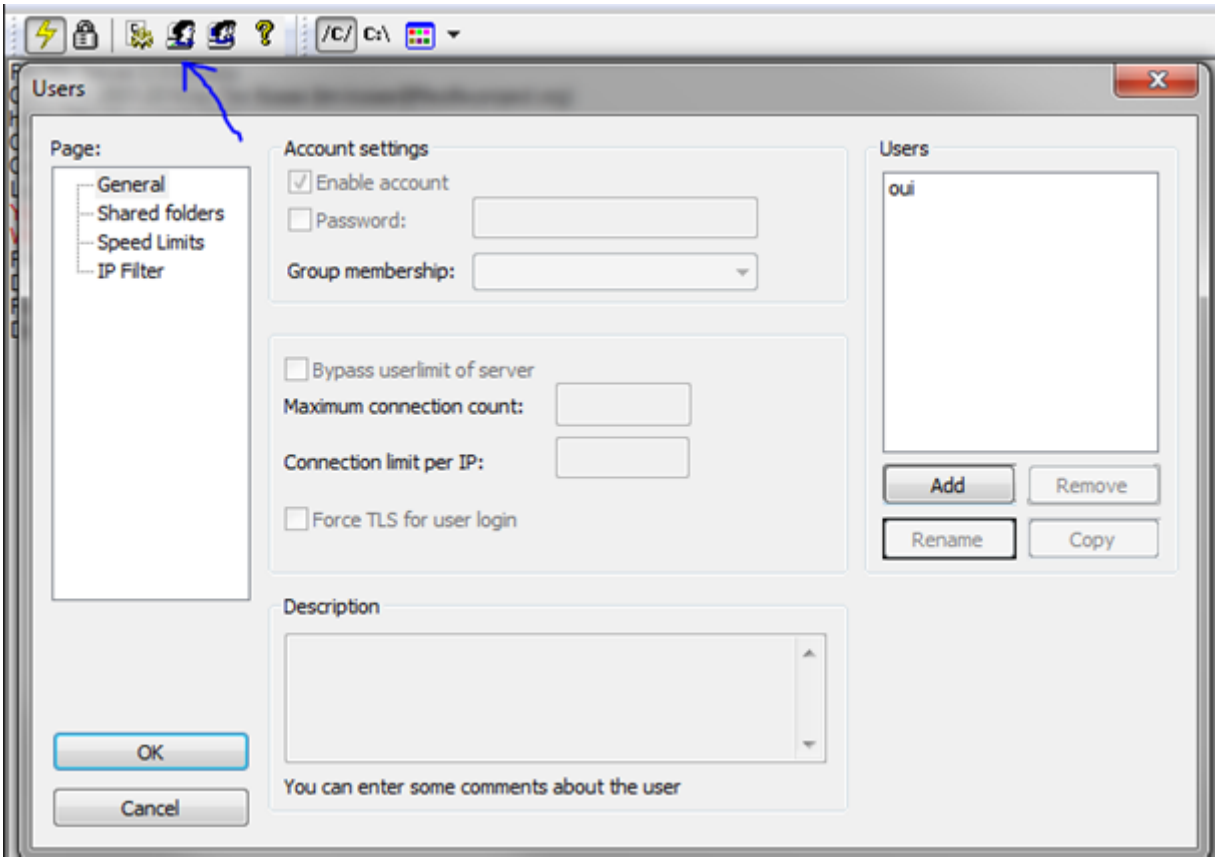
Serveur FTP

- Serveur FTP non sécurisé
- Serveur FTP sécurisé

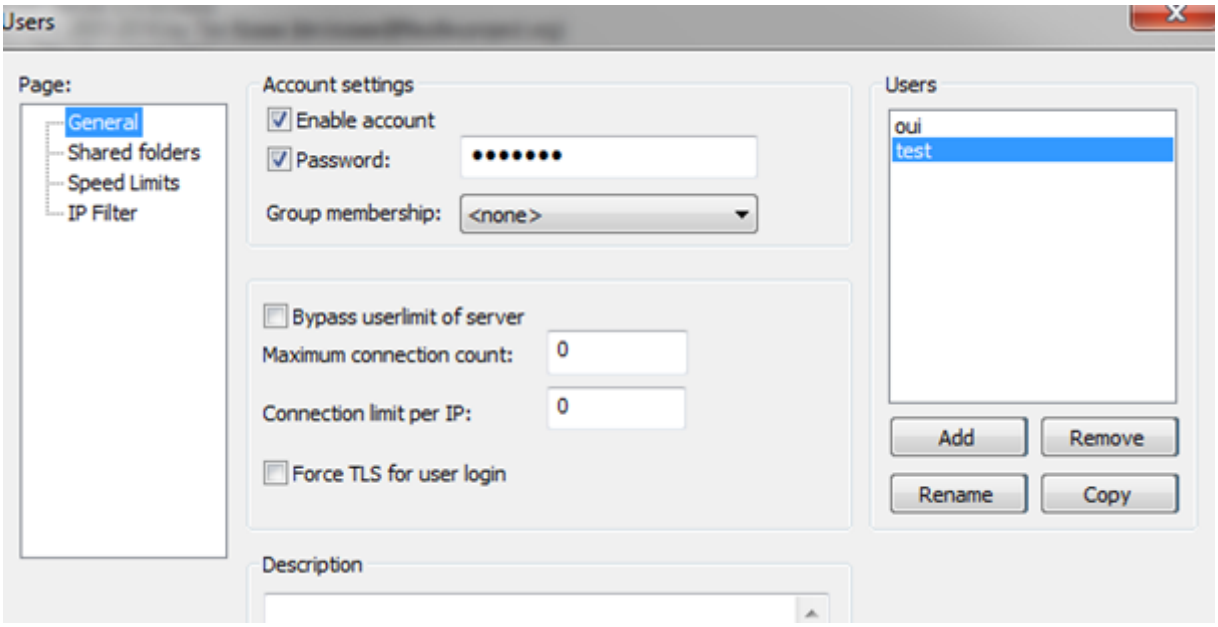
Serveur FTP non sécurisé



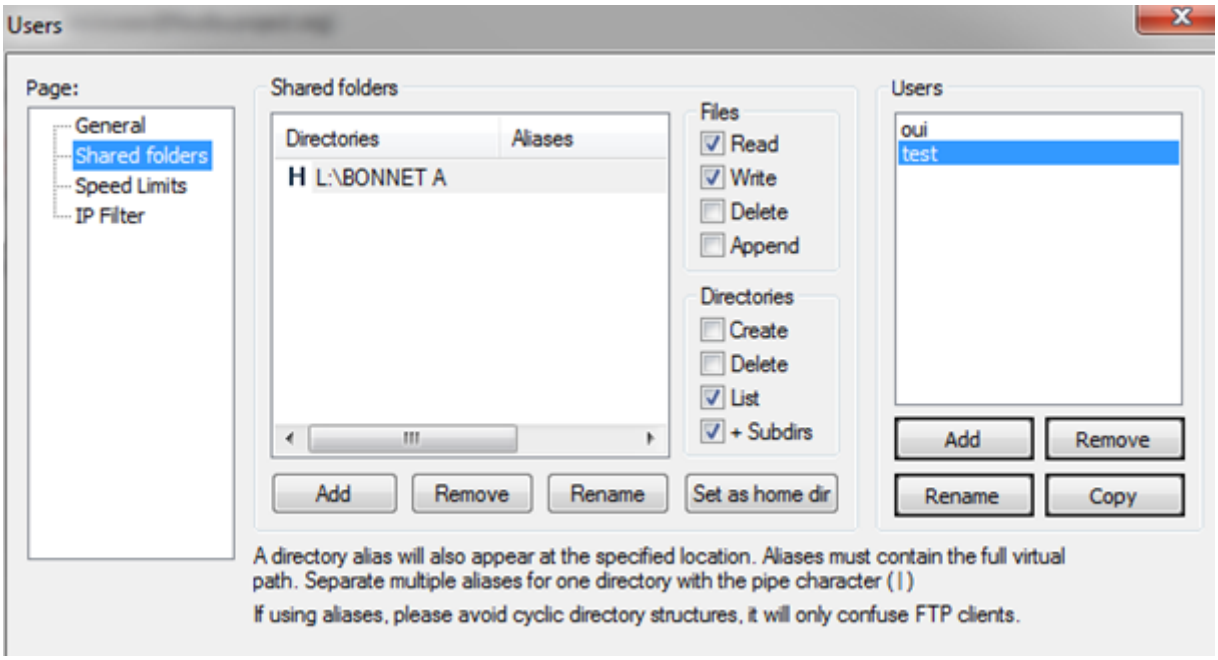
Ici on peut voir les paramètres du serveur FileZilla. Le port est par défaut à 21 et le nombre d’utilisateurs à 0 (ce qui correspond à illimité).



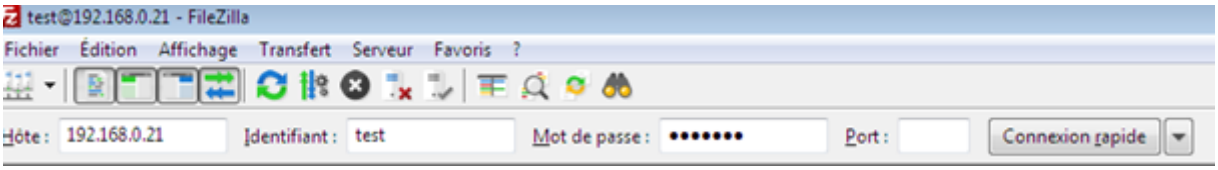
En cliquant sur cette icône, on a accès à la liste des utilisateurs. Nous allons en créer un en cliquant sur Add sur le côté droit. On définit un nom d’utilisateur et un mot de passe.



Une fois le nom de l'utilisateur et mot de passe définis, on clique sur « Shares folders ». Ce sont les dossiers partagées entre le serveur et l'utilisateur concerné.

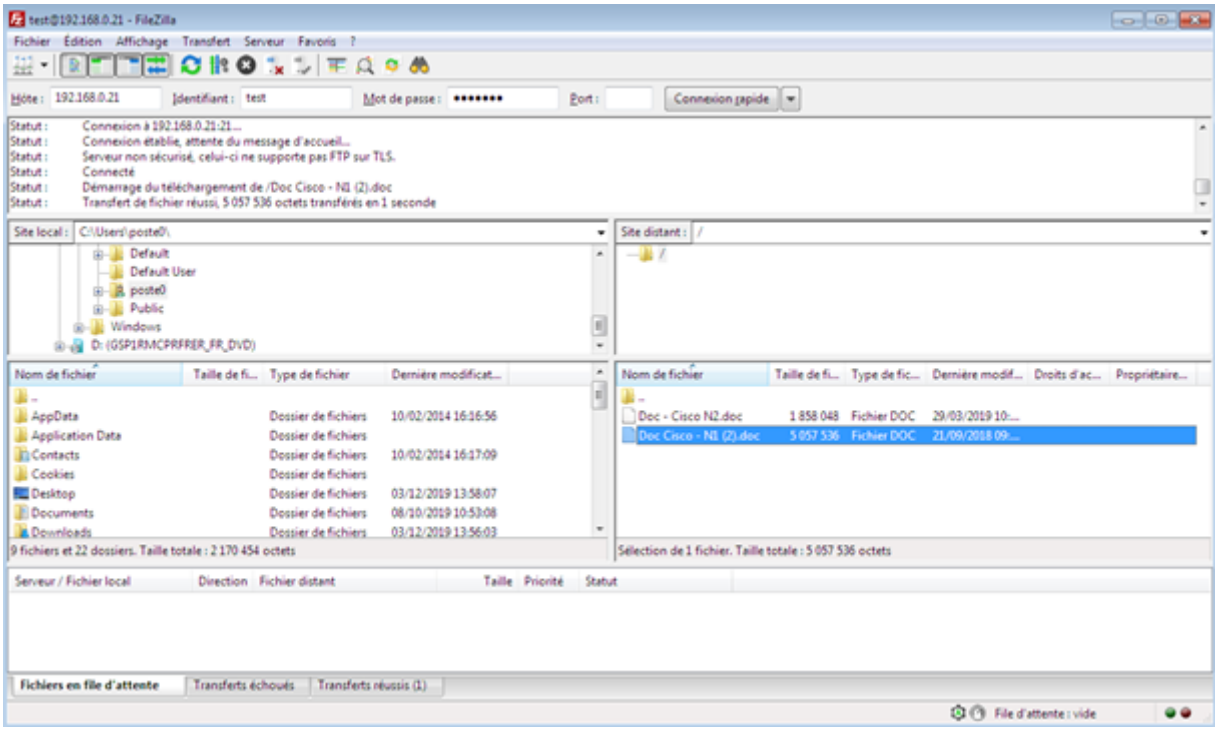


On choisit ensuite en cochant ou non les cases les permissions : lecture, écriture, suppression... Tout est prêt.



Sur la machine cliente, on entre dans « Hôte » l'adresse IP du serveur FTP, dans « Identifiant » le nom d'utilisateur, « Mot de passe » le mot de passe lié à l'utilisateur et le port (par défaut 21). On clique sur connexion rapide.

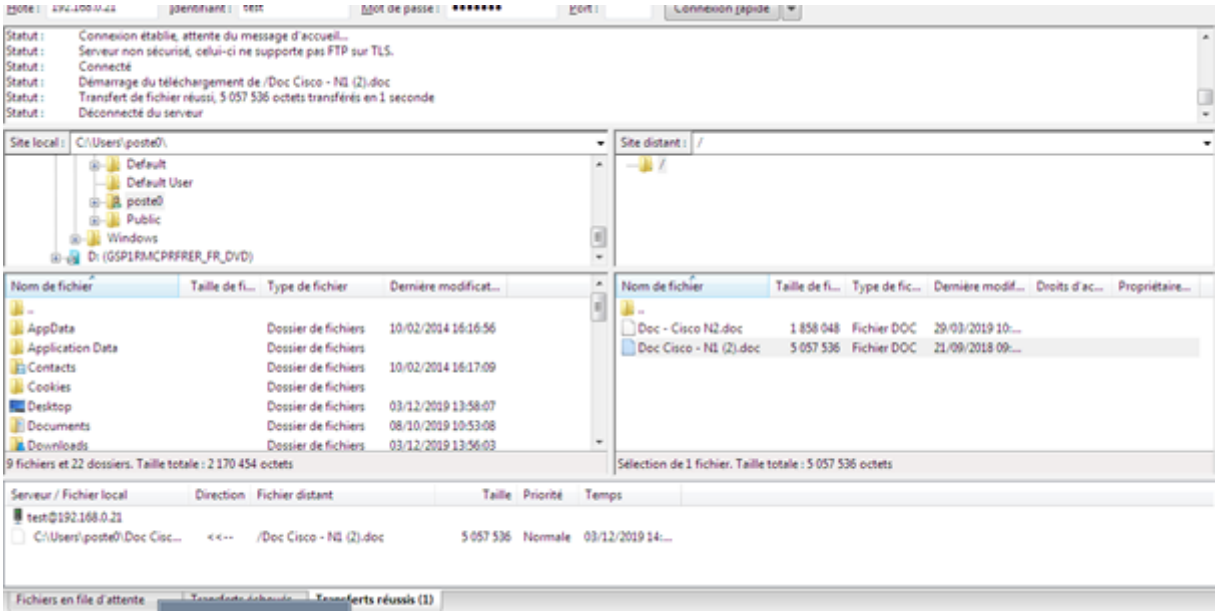
Un message s'affiche disant que la connexion n'est pas sécurisé. En effet, les logins ne sont pas protégés.



On a ensuite un dialogue nous confirmant la connexion.

Juste en dessous à gauche, on a site local : il s'agit de la destination de téléchargement des fichiers. A droite, le site distant correspondant au chemin des fichiers du serveur. Dans le serveur, dans cette exemple, nous avons deux fichiers.

On effectue un clic droit sur « Doc – Cisco N2.doc » par exemple, et télécharger. On a un message en bas à droite de l'écran nous confirmant la réussite du téléchargement.



Dans l'onglet « Transferts réussis » en bas de l'écran, on a une ligne par fichier, avec la destination de téléchargement, le fichier distant, la taille, la priorité et le temps.

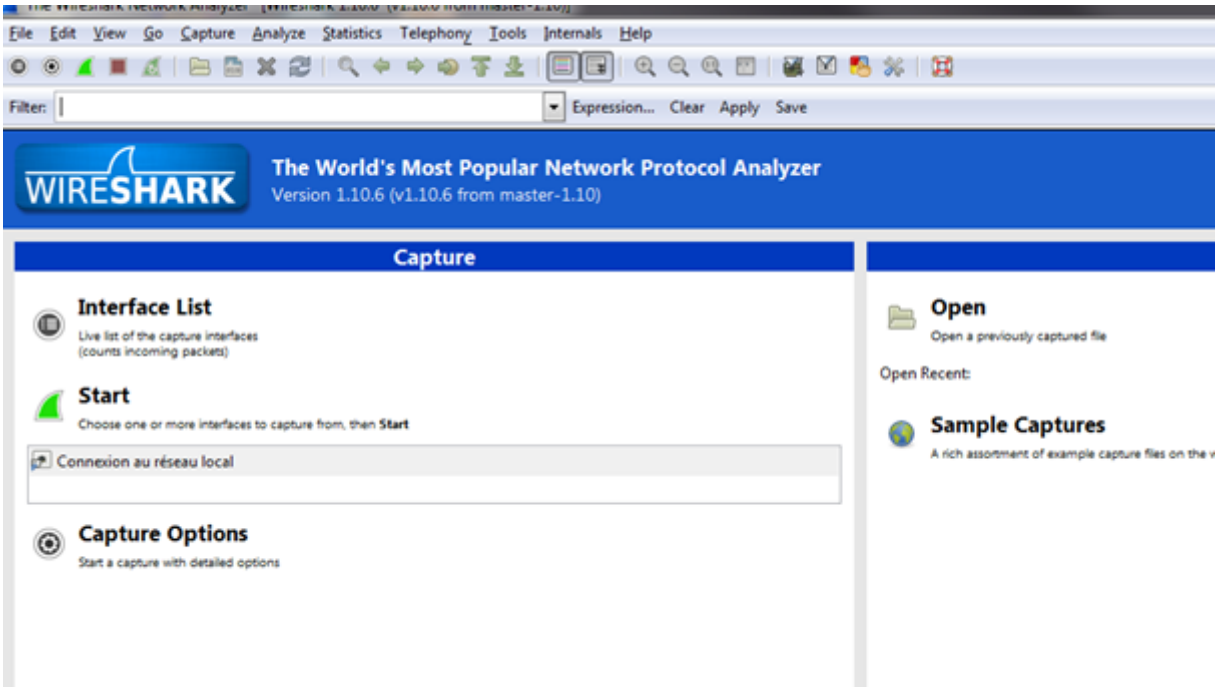
Du côté serveur, nous avons des lignes confirmant le téléchargement :

```
(000004)03/12/2019 14:19:10 - test (192.168.0.205)> RETR Doc Cisco - N1 (2).doc
(000004)03/12/2019 14:19:10 - test (192.168.0.205)> 150 Opening data channel for file download from server of "/Doc Cisco - N1 (2).doc"
(000004)03/12/2019 14:19:10 - test (192.168.0.205)> 226 Successfully transferred "/Doc Cisco - N1 (2).doc"
```

De même pour les connexions/déconnexions au serveur :

```
(000004)03/12/2019 14:19:10 - (not logged in) (192.168.0.205)> USER test
(000004)03/12/2019 14:19:10 - (not logged in) (192.168.0.205)> 331 Password required for test
(000004)03/12/2019 14:19:10 - (not logged in) (192.168.0.205)> PASS ********
(000004)03/12/2019 14:19:10 - test (192.168.0.205)> 230 Logged on
```

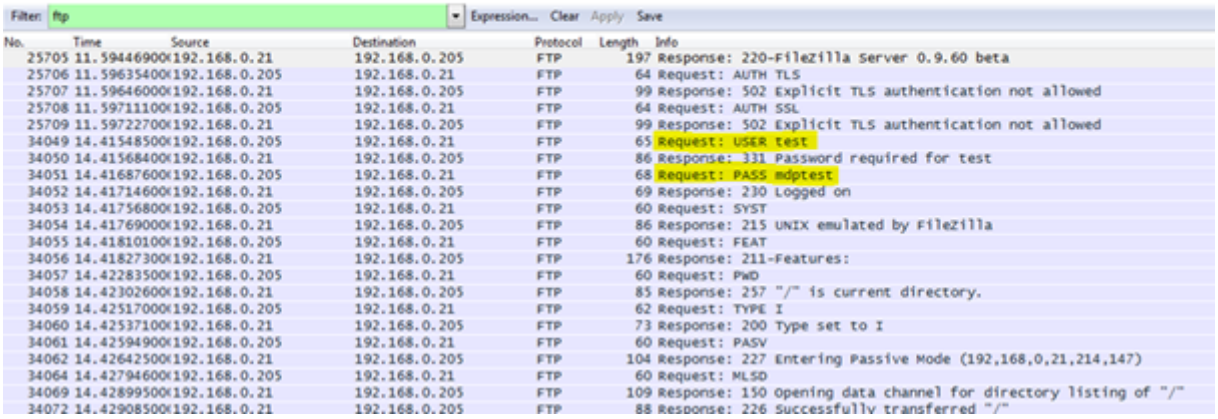
Afin de prouver la non sécurisation du FTP, nous pouvons utiliser Wireshark. Celui –ci va analyser et lister les trames du réseau.



Une fois le programme lancé, on va écrire « ftp »dans « Filter » afin de filtrer les trames. On aura donc les trames liés au protocole ftp d'affichées.

Une fois écrit, nous allons cliquer sur « Start ». On se connecte alors sur la machine physique au serveur. On peut ensuite arrêter la capture des trames.

On obtient le résultat suivant :



On peut y retrouver l'identifiant et le mot de passe de connexion. A la ligne 6, on a « USER test » ce qui correspond à « Identifiant : test ». L'identifiant de connexion est « test ».

Deux lignes en dessous, on a « PASS mdp test » ce qui correspond à « mot de passe : mdptest ». Le mot de passe est donc « mdptest ».

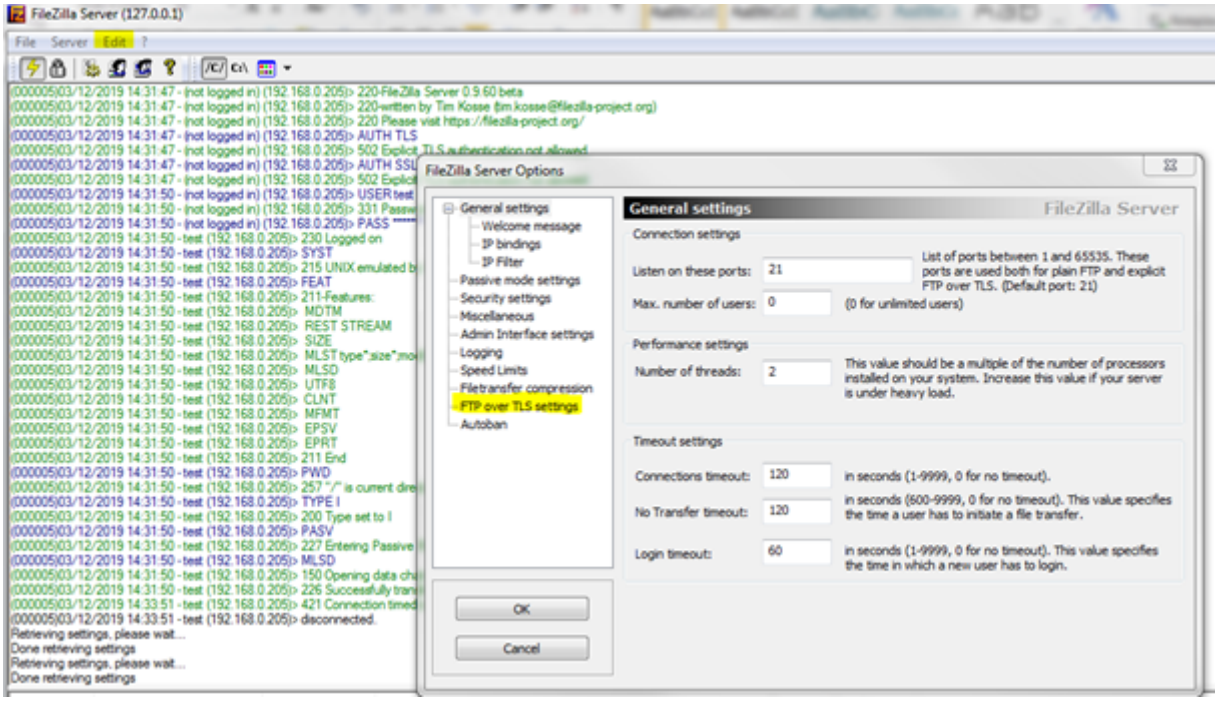
Afin de sécuriser un serveur FTP, on doit utiliser un autre port que 21 et un certificat SSL en utilisant un protocole sécurisé.

Serveur FTP sécurisé

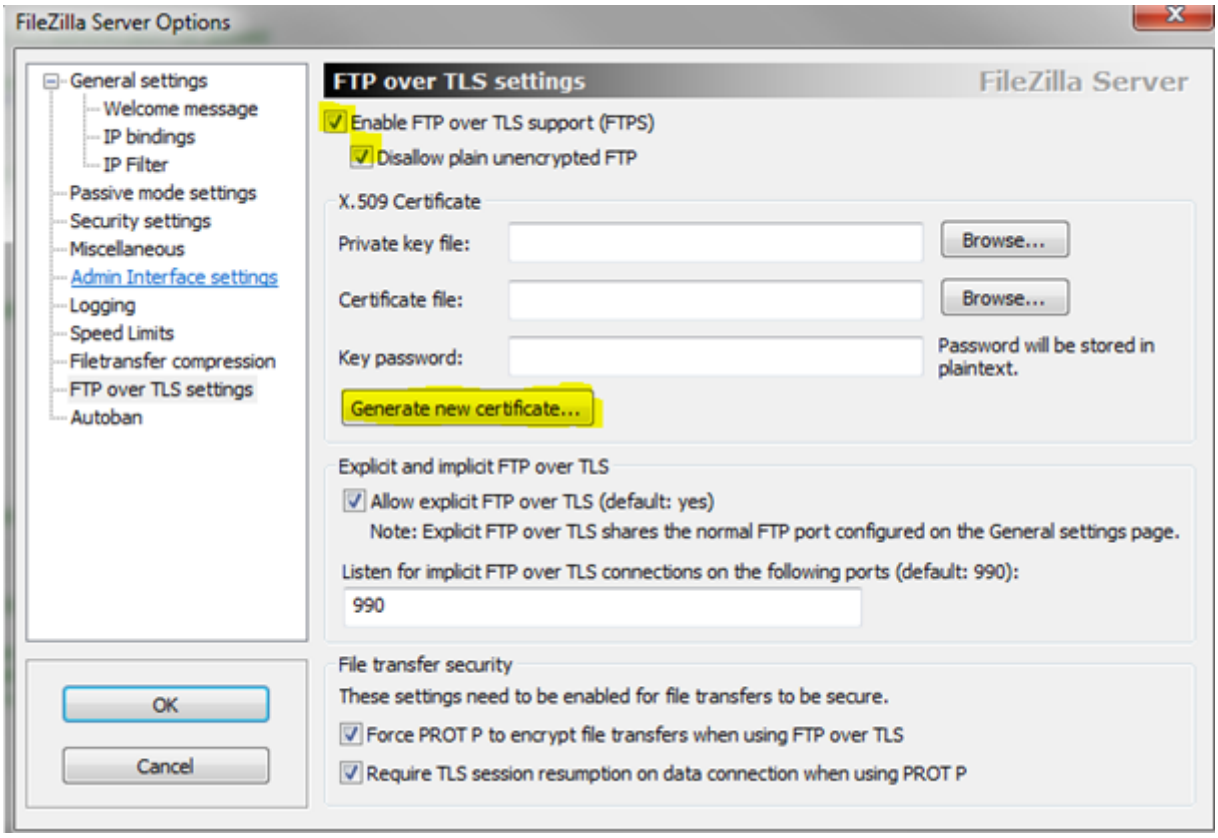
Il est important de sécuriser le serveur FTP, en utilisant le SFTP ou le FTPS.

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

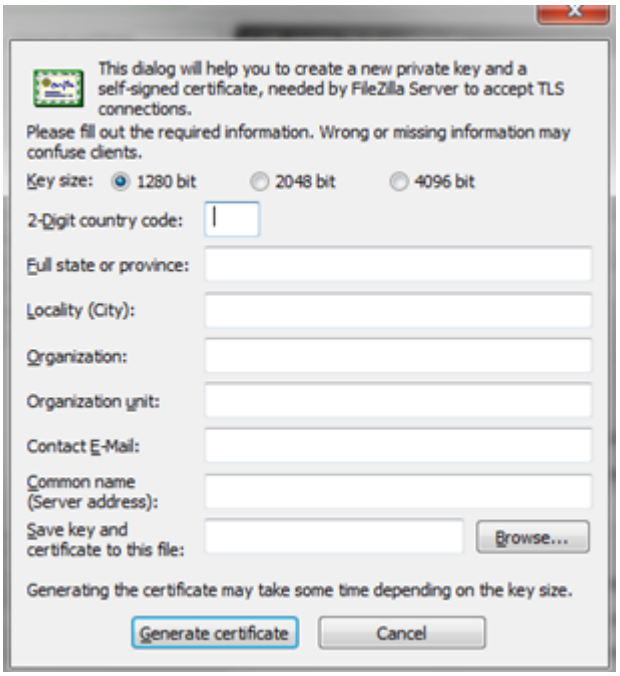
Le SFTP est le transfert de fichiers via SSH (port 22). On pourrait parler de transfert FTP encapsulé dans un tunnel SSH sécurisé.



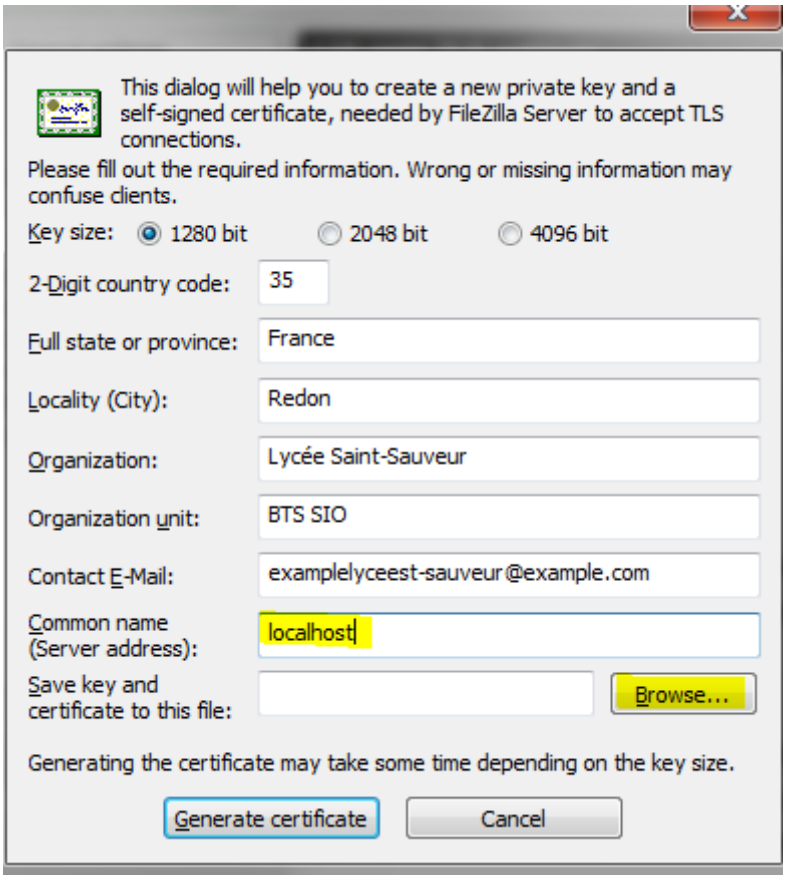
Au niveau du FileZilla Serveur, cliquez sur « Edit » et « Settings », puis l'onglet « FTP over TLS settings ».



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.

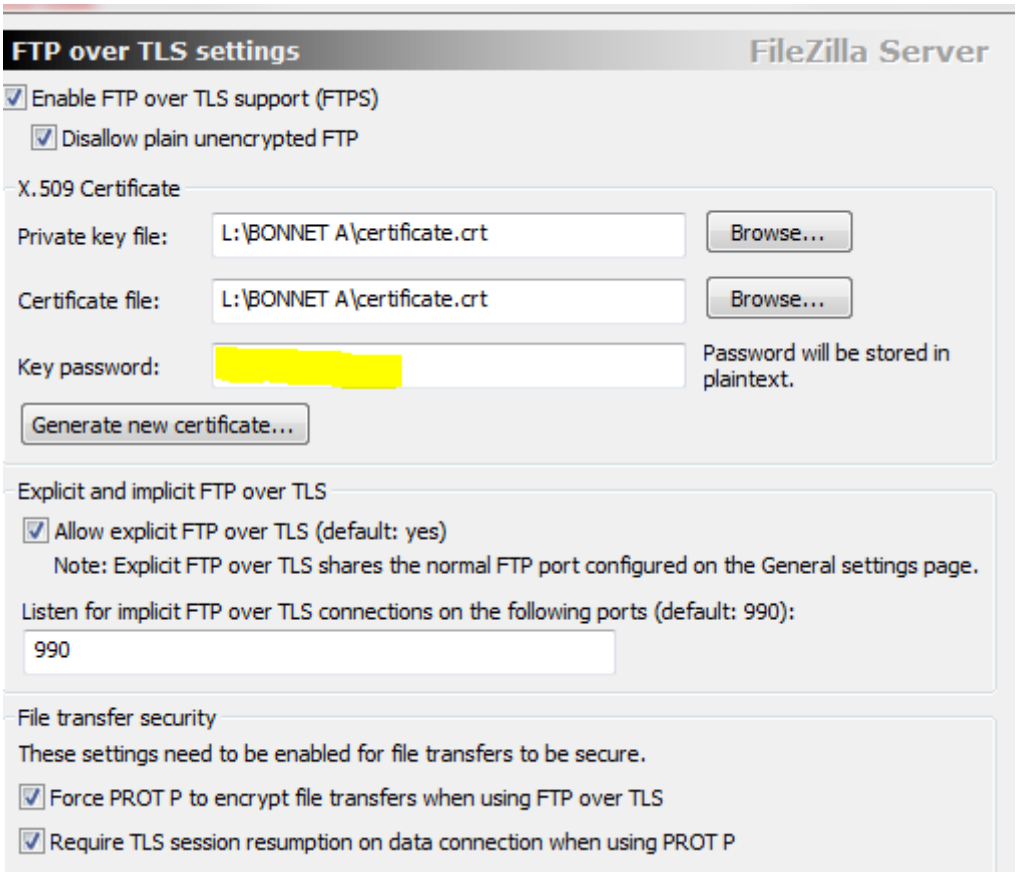


On rentre ensuite les données, par exemple :



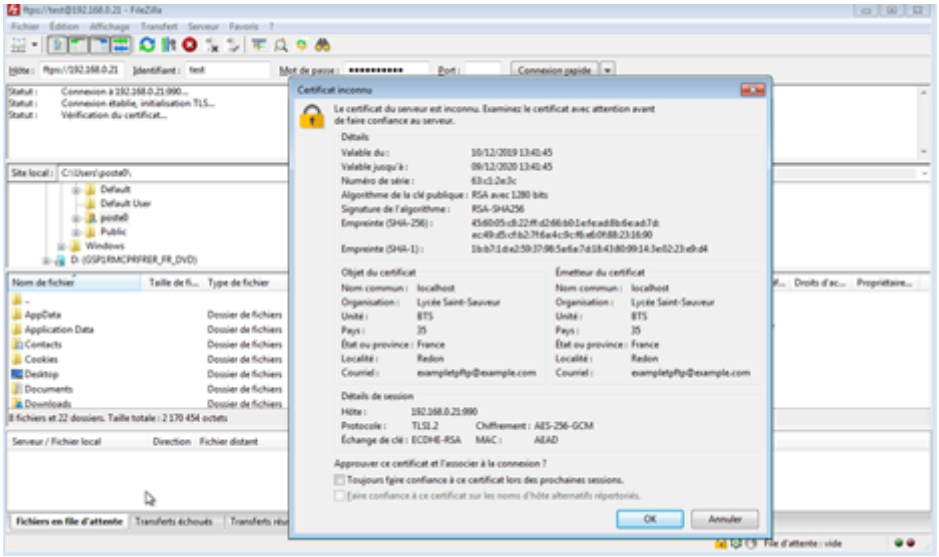
On rentre l’adresse du serveur dans « Common name », ici « localhost » ou l'adresse IP du serveur FTP.

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



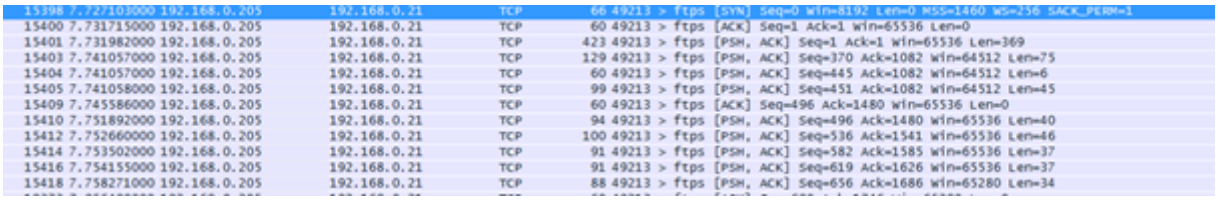
On rentre ensuite un mot de passe puis on clique sur « OK ». Les connexions sont désormais sécurisées et chiffrées.

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.