

SERVEUR FTP(S)

VsFTPD (Very Secure FTP Daemon) est un **serveur FTP** conçu avec la problématique d'une sécurité maximale.

La configuration par défaut de VsFTPD est très restrictive :

1. Seul le compte *Anonyme* est autorisé à se connecter au serveur
2. Les utilisateurs ne peuvent pas accéder à leurs répertoires

Nous allons modifier cela pour que deux utilisateurs, **user1** et **user2**, puissent accéder à leur répertoire personnel via le protocole FTP.

INSTALLATION ET CONFIGURATION DE VSFTPD

Après l'éventuelle mise à jour habituelle, installons le paquet :

```
apt update && apt -y upgrade  
apt -y install vsftpd
```

Modifions ensuite le fichier vsftpd.conf :

```
nano -l /etc/vsftpd.conf  
  
# ligne 14 : changer pour écouter IPv4  
listen=YES
```

```
# ligne 22 : retirer IPv6 (facultatif)
listen_ipv6=NO

# ligne 31 : dé-commenter pour autoriser l'écriture
write_enable=YES

# lignes 99 et 100 : dé-commenter pour autoriser les transferts en mode ascii
ascii_upload_enable=YES
ascii_download_enable=YES

# ligne 122 : dé-commenter pour activer chroot sur les comptes locaux
# (effet : restreint les utilisateurs locaux : leur répertoire racine sera leur répertoire personnel)
chroot_local_user=YES

# ligne 123 : dé-commenter pour activer la liste chroot (--> comptes concernés par chroot)
chroot_list_enable=YES

# ligne 125 : dé-commenter pour définir le chemin vers la liste chroot
chroot_list_file=/etc/vsftpd.chroot_list

# ligne 131 : dé-commenter pour autoriser le listage récursif
ls_recurse_enable=YES
```

À la fin du fichier, ajouter :

```
# désactiver le filtre seccomp
seccomp_sandbox=NO

# à décommenter si l'on souhaite changer le port d'écoute FTP par défaut (21) :
# listen_port=2121
```

CREER LES UTILISATEURS QUI POURRONT SE CONNECTER AU SERVEUR FTP

UTILISATEURS LINUX

Les utilisateurs qui pourront se connecter au serveur seront en fait des utilisateurs Linux « normaux », créés de façon classique. Exemple :

```
adduser user1
adduser user2
```

DROITS SUR LE CONTENU DU SERVEUR

Notons au passage que les droits d'accès aux dossiers seront à contrôler/affiner. En effet, par défaut, à la création d'un utilisateur Linux, les droits sur ses dossiers personnels sont `rw-r-xr-x` (755) et ceux des fichiers sont `rw-r--r--` (644). Autrement dit, si le groupe propriétaire et les « autres » ne peuvent les modifier, ils peuvent les lire, ce qui peut être contraire aux attentes.

Exemple de commandes pour modifier les droits sur tous les dossiers et fichiers du répertoire personnel de l'utilisateur `user1` :

```
find /home/user1 -type d -exec chmod 750 {} \;
find /home/user1 -type f -exec chmod 640 {} \;
```

CONFIGURATION DU SERVEUR FTP POUR QUE LE DOSSIER PERSONNEL DES UTILISATEURS AUTORISES SOIT AUSSI LEUR REPERTOIRE RACINE FTP

Donnons à vsftpd la liste des utilisateurs autorisés en saisissant leur identifiant dans `/etc/vsftpd.chroot_list` :

```
nano /etc/vsftpd.chroot_list

# Utilisateurs autorisés à se connecter via vsftpd
user1
user2
```

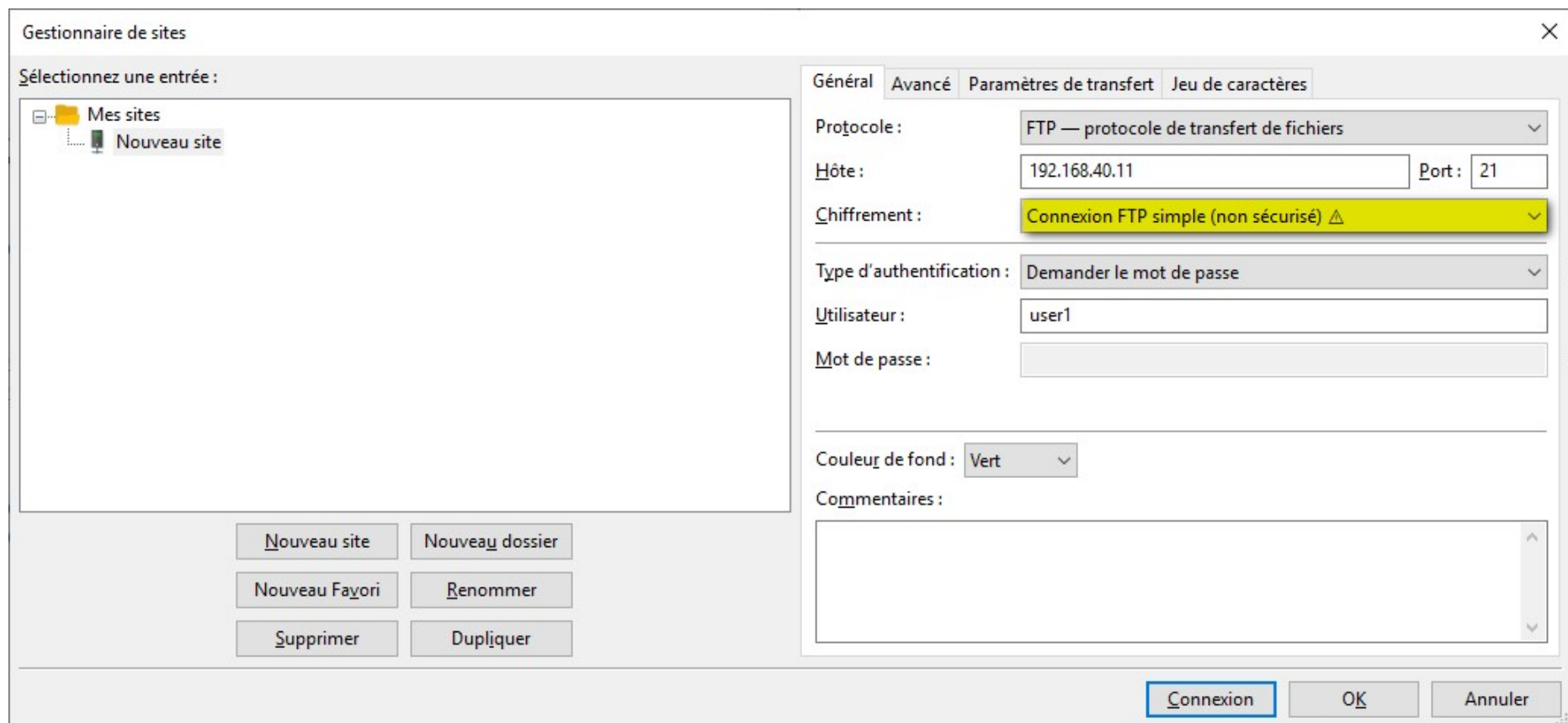
Redémarrer le service :

```
systemctl restart vsftpd
```

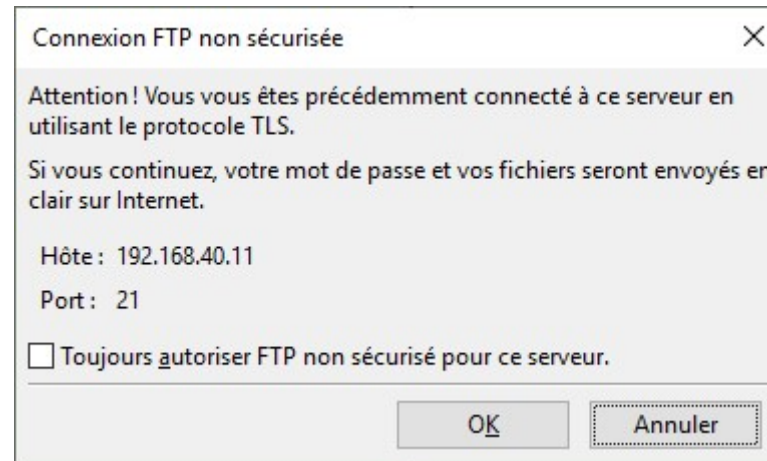
CONNEXION SANS CHIFFREMENT

Normalement, le service est maintenant opérationnel.

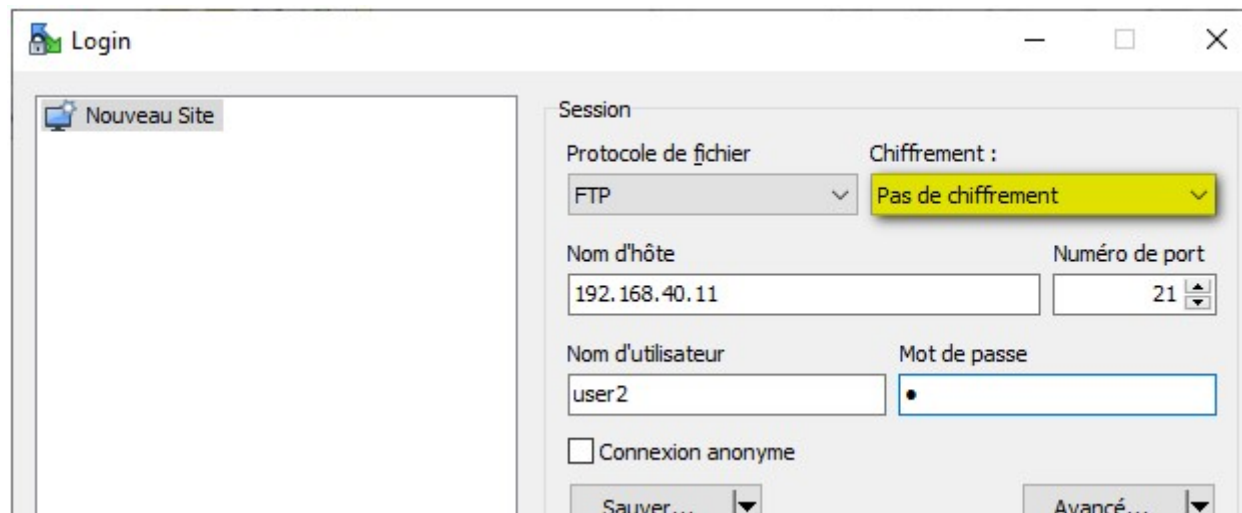
- Via FileZilla, il sera accessible en passant par le Gestionnaire de sites pour ajouter un nouveau site et en sélectionnant le mode simple :



À ce stade de la configuration, un avertissement est susceptible d'apparaître, rappelant que la connexion n'est pas sécurisée.



- Sur WinSCP, il suffira de préciser « Pas de chiffrement » :



CONFIGURER VSFTPD POUR UTILISER SSL/TLS

Afin d'ajouter une couche de sécurité, nous allons créer un certificat pour authentifier notre serveur. Ce certificat sera auto-signé (*comprendre : un certificat signé en local et non par une autorité publiquement reconnue – ce certificat pourra donc être considéré comme fiable en interne, mais moins en externe*).

Rendons-nous dans le répertoire dédié aux clés SSL :

```
cd /etc/ssl/private
```

Nous allons y générer le fichier **vsftpd.pem**, contenant à la fois le certificat voulu et une clé RSA de 2048 bits, valable 365 jours :

```
openssl req -x509 -nodes -newkey rsa:2048 -keyout vsftpd.pem -out vsftpd.pem -days 365
```

Le système nous demandera de saisir des informations pour compléter le certificat. Exemple :

```
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:Rhone-Alpes
Locality Name (eg, city) []:Grenoble
Organization Name (eg, company) [Internet Widgits Pty Ltd]:AFPA
Organizational Unit Name (eg, section) []:TSSR
Common Name (e.g. server FQDN or YOUR name) []:ftp.tssr.lan
Email Address []:adminftp@gmail.com
```

Restreignons les permissions sur le fichier nouvellement créé au seul utilisateur propriétaire :

```
chmod 600 vsftpd.pem
```

Il faut maintenant modifier le fichier de configuration de vsftpd afin qu'il tienne compte du certificat :

```
nano /etc/vsftpd.conf
```

Nous y ajouterons les lignes suivantes :

```
rsa_cert_file=/etc/ssl/private/vsftpd.pem
rsa_private_key_file=/etc/ssl/private/vsftpd.pem
ssl_enable=YES
```

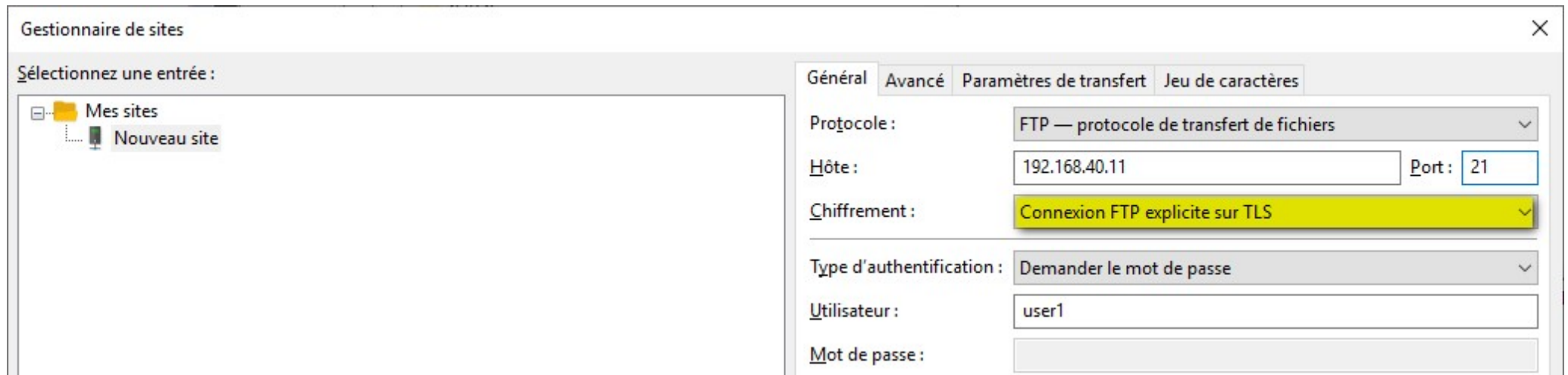
```
ssl_ciphers=HIGH
ssl_tlsv1=YES
ssl_sslv2=NO
ssl_sslv3=NO
force_local_data_ssl=YES
force_local_logins_ssl=YES
```

Reste à redémarrer le service :

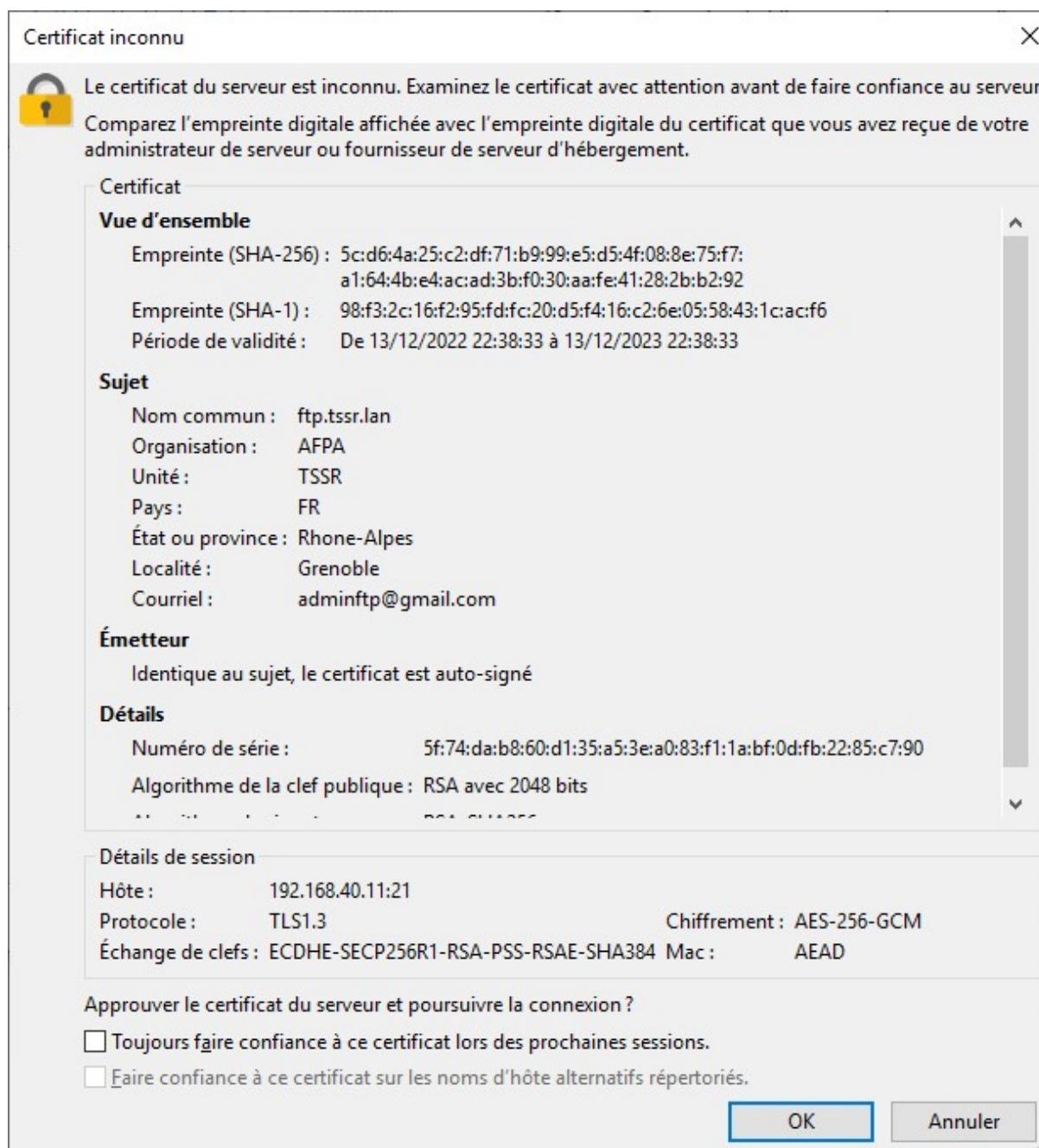
```
systemctl restart vsftpd
```

CONFIGURER UN CLIENT FTP POUR UTILISER LA CONNEXION FTPS

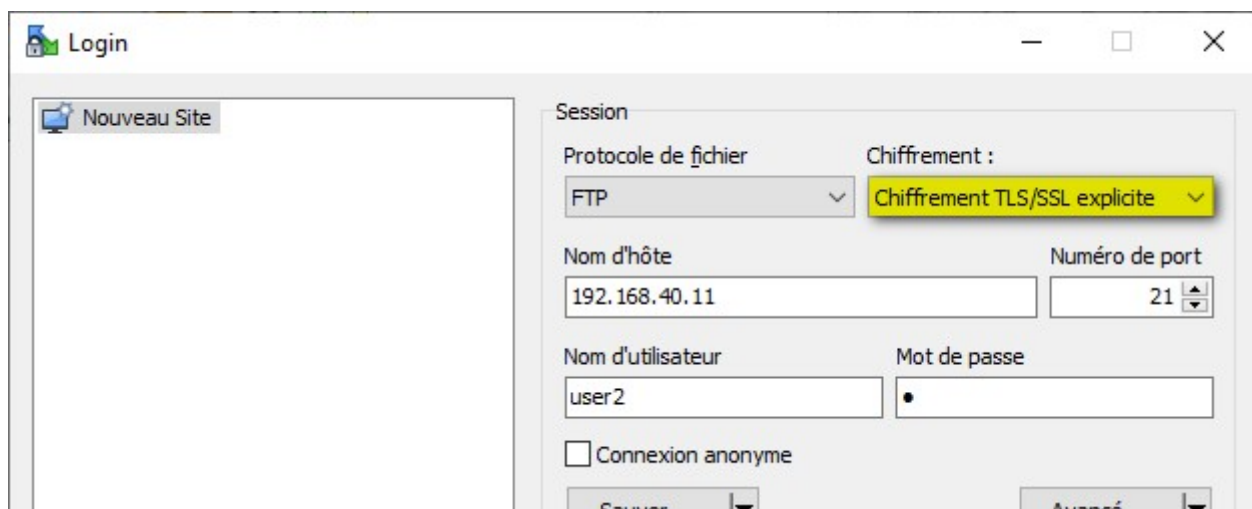
- Avec FileZilla, contrairement à l'étape sans SSL/TLS, nous opterons pour une « Connexion FTP explicite sur TLS » :



Initialement inconnu de notre PC, le certificat est affiché. À nous de l'approuver s'il donne des données cohérentes avec notre infrastructure :

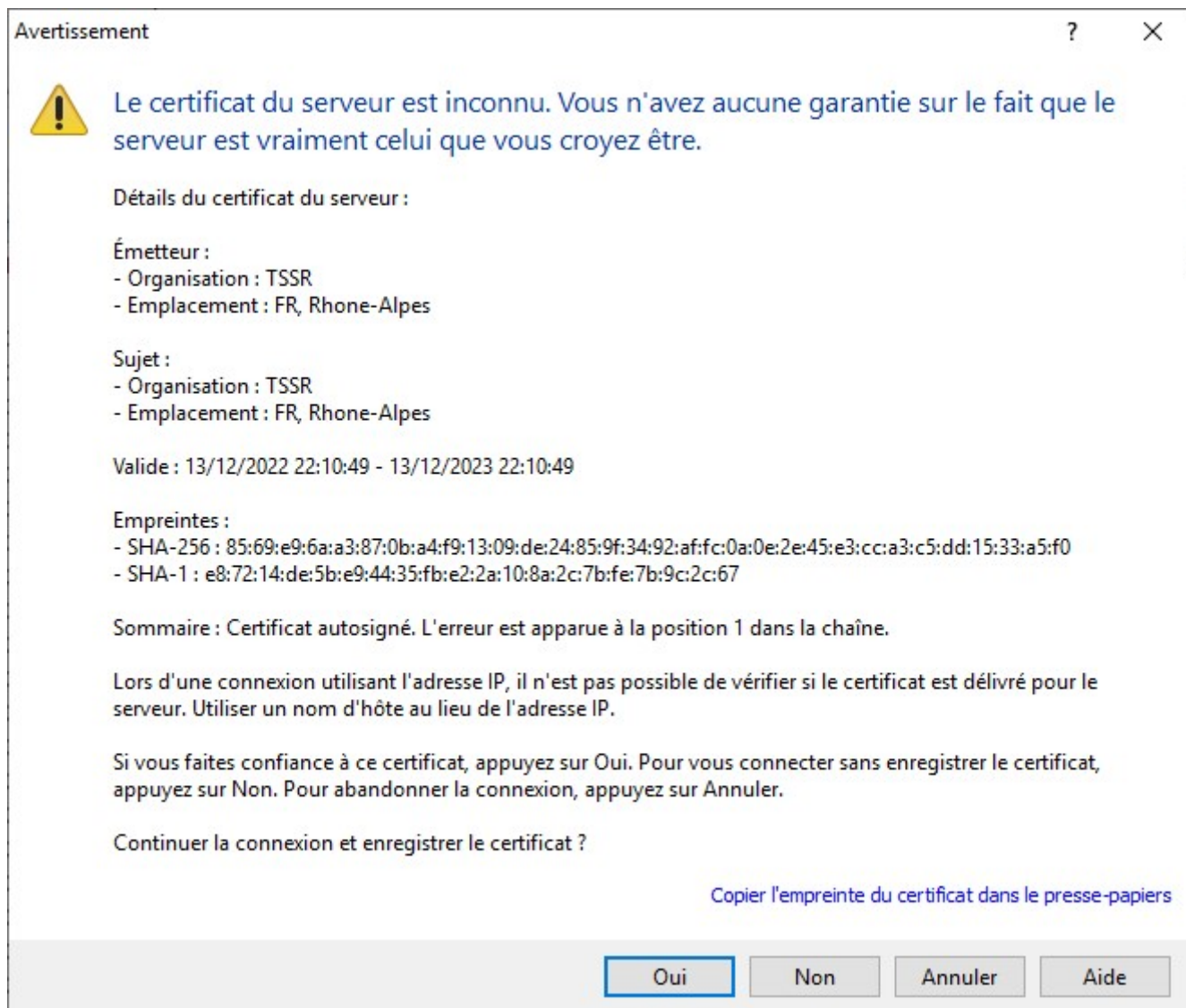


- Sur WinSCP :



The image shows the WinSCP Login dialog box. On the left, there is a 'Nouveau Site' button. The main area is titled 'Session' and contains the following fields and options:

- Protocole de fichier:** A dropdown menu set to 'FTP'.
- Chiffrement:** A dropdown menu set to 'Chiffrement TLS/SSL explicite'.
- Nom d'hôte:** A text field containing '192.168.40.11'.
- Numéro de port:** A spinner box set to '21'.
- Nom d'utilisateur:** A text field containing 'user2'.
- Mot de passe:** A password field with a single dot.
- Connexion anonyme:** An unchecked checkbox.
- At the bottom, there are 'Sauver' and 'Avancé' buttons.



The image shows a Windows 'Avertissement' (Warning) dialog box with a yellow warning icon. The text inside is as follows:

Le certificat du serveur est inconnu. Vous n'avez aucune garantie sur le fait que le serveur est vraiment celui que vous croyez être.

Détails du certificat du serveur :

Émetteur :

- Organisation : TSSR
- Emplacement : FR, Rhone-Alpes

Sujet :

- Organisation : TSSR
- Emplacement : FR, Rhone-Alpes

Valide : 13/12/2022 22:10:49 - 13/12/2023 22:10:49

Empreintes :

- SHA-256 : 85:69:e9:6a:a3:87:0b:a4:f9:13:09:de:24:85:9f:34:92:af:fc:0a:0e:2e:45:e3:cc:a3:c5:dd:15:33:a5:f0
- SHA-1 : e8:72:14:de:5b:e9:44:35:fb:e2:2a:10:8a:2c:7b:fe:7b:9c:2c:67

Sommaire : Certificat autosigné. L'erreur est apparue à la position 1 dans la chaîne.

Lors d'une connexion utilisant l'adresse IP, il n'est pas possible de vérifier si le certificat est délivré pour le serveur. Utiliser un nom d'hôte au lieu de l'adresse IP.

Si vous faites confiance à ce certificat, appuyez sur Oui. Pour vous connecter sans enregistrer le certificat, appuyez sur Non. Pour abandonner la connexion, appuyez sur Annuler.

Continuer la connexion et enregistrer le certificat ?

[Copier l'empreinte du certificat dans le presse-papiers](#)

At the bottom, there are four buttons: 'Oui' (highlighted with a blue border), 'Non', 'Annuler', and 'Aide'.