

## MISE EN PLACE D'UN SERVICE FTPS SOUS IIS

À une époque, l'une des solutions de transfert de fichiers les plus utilisées dans divers systèmes d'exploitation était le protocole FTP (File Transfer Protocol), mis en place depuis 1971 et dont le fonctionnement est basé sur le modèle de logiciel client/serveur à travers lequel il nous donne la possibilité de transférer tout type de fichier entre ordinateurs basés sur un réseau utilisant le protocole TCP/IP.

L'utilisation du protocole FTP est simple, il suffit qu'un utilisateur accède à un programme client FTP depuis un ordinateur pour se connecter à un autre ordinateur sur lequel un serveur FTP est configuré. Après cela, lorsque la connexion est établie, le client doit s'authentifier avec un nom d'utilisateur et un mot de passe définis. Une fois le client authentifié, le processus de partage de fichiers peut être démarré.

### Avantages FTP

- ✓ Possibilité de gérer les fichiers FTP directement à partir de l'application en mode synchrone ou asynchrone.
- ✓ Prend en charge FTPS - FTP sur TLS 1.2, 1.1, 1.0 et SSL 3.0
- ✓ Compatible avec SSL / TLS
- ✓ Prend en charge les serveurs FTP les plus populaires et les mandataires actuels.
- ✓ Possibilité de reprendre (redémarrer) les téléchargements FTP et les téléchargements sans perdre de temps.
- ✓ Possibilité de synchroniser l'arborescence du répertoire local avec l'arborescence du répertoire distant dans n'importe quel sens.
- ✓ Prend en charge les noms de fichiers internationaux dans toutes les langues principales
- ✓ Prise en charge de l'utilisation de FTP sécurisé (FTPS) via AUTH TLS ou AUTH SSL
- ✓ Supprime le canal de contrôle (CCC) après l'authentification FTPS
- ✓ Possibilité de télécharger des fichiers texte et binaires directement dans la mémoire
- ✓ Possibilité de créer un répertoire distant
- ✓ Possibilité de modifier ou supprimer le nom des fichiers et des répertoires distants.
- ✓ Prise en charge des chargements et téléchargements asynchrones.
- ✓ Prise en charge des transferts binaires et ASCII.
- ✓ Possibilité de télécharger des fichiers de plus de 4 Go.
- ✓ Permet d'utiliser un certificat SSL du client pour les connexions SSL...

Il est possible d'utiliser FTP directement dans Windows 10.

La mise en œuvre sera réalisée ici sur un OS Windows 10 Pro en adressage IP Fixe en 192.168.0.100/24 ou en 172.20.130.130/16.

S'il n'est pas disponible, on peut utiliser des logiciels serveur FTP et client FTP comme :

FileZilla :

FTP Serveur : <https://filezilla-project.org/download.php?type=server>

FTP Client : <https://filezilla-project.org/download.php?type=client>

Cyberduck :

<https://cyberduck.io/>



CoreFTP :

Serveur : <http://www.coreftp.com/server/index.html>

Client : <http://www.coreftp.com/download.html>



Il en existe beaucoup d'autres bien évidemment dont certaines solutions payantes comme :

Cerberus FTP Server :

[https://www.cerberusftp.com/ad/?gclid=CjwKCAiAyPyQBhB6EiwAFUuakgcrplrNQvjnlDiTQPzyralX7qtYJylL8pUWLYShV4MZtiqMJudgNhoCipwQAvD\\_BwE](https://www.cerberusftp.com/ad/?gclid=CjwKCAiAyPyQBhB6EiwAFUuakgcrplrNQvjnlDiTQPzyralX7qtYJylL8pUWLYShV4MZtiqMJudgNhoCipwQAvD_BwE)



CuteFTP :

<https://www.globalscape.com/cuteftp#pick-your-package>



WiseFTP :

<https://www.wise-ftp.de/en/download.html>



## 1) Mise en œuvre

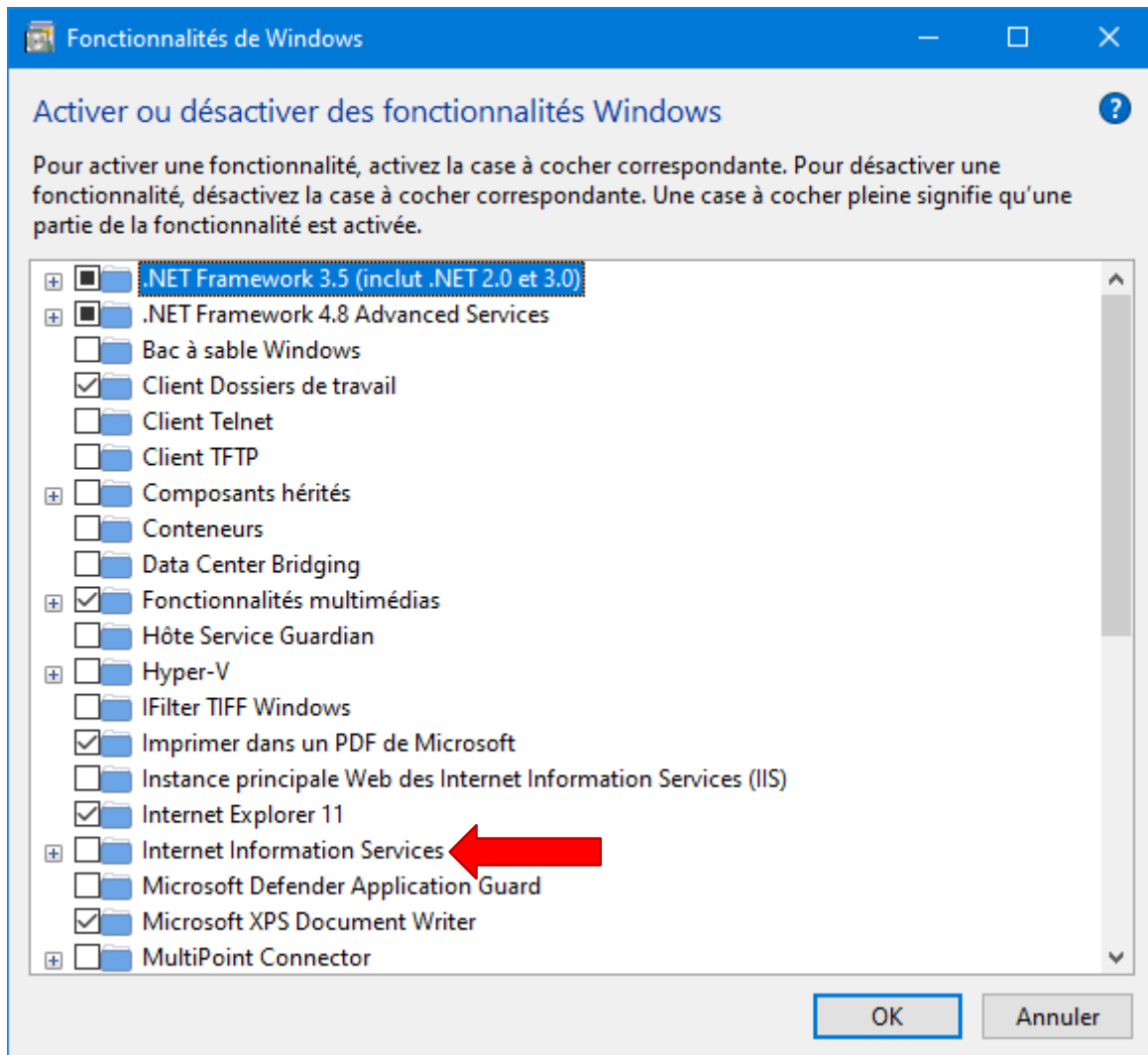
### a. Installation des composants FTP

Sur les OS Windows Pro, on trouve le service Server FTP, c'est une fonctionnalité Windows.

#### Ajout de la fonctionnalité FTP Server

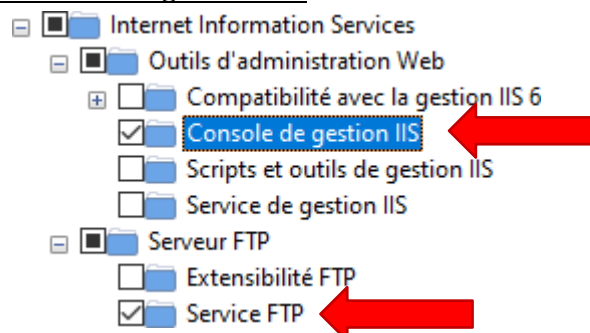
Pour mettre en place un serveur FTP, il faut ajouter les fonctions supplémentaires suivantes :  
Cliquez sur le bouton démarrer de Windows puis saisir optionalfeatures





Internet Information Services (IIS) rassemble un ensemble de composants et de services permettant la prise en charge non seulement des protocoles web standard (HTTP et HTTPS) mais aussi d'autres protocoles comme le FTP, le SMTP (Simple Mail Transfer Protocol)... IIS intègre différents mécanismes d'authentification et peut s'appuyer nativement sur l'annuaire Active Directory ou sur les autorisations NTFS (New Technology File System).

Ajouter le service FTP et la console de gestion IIS :

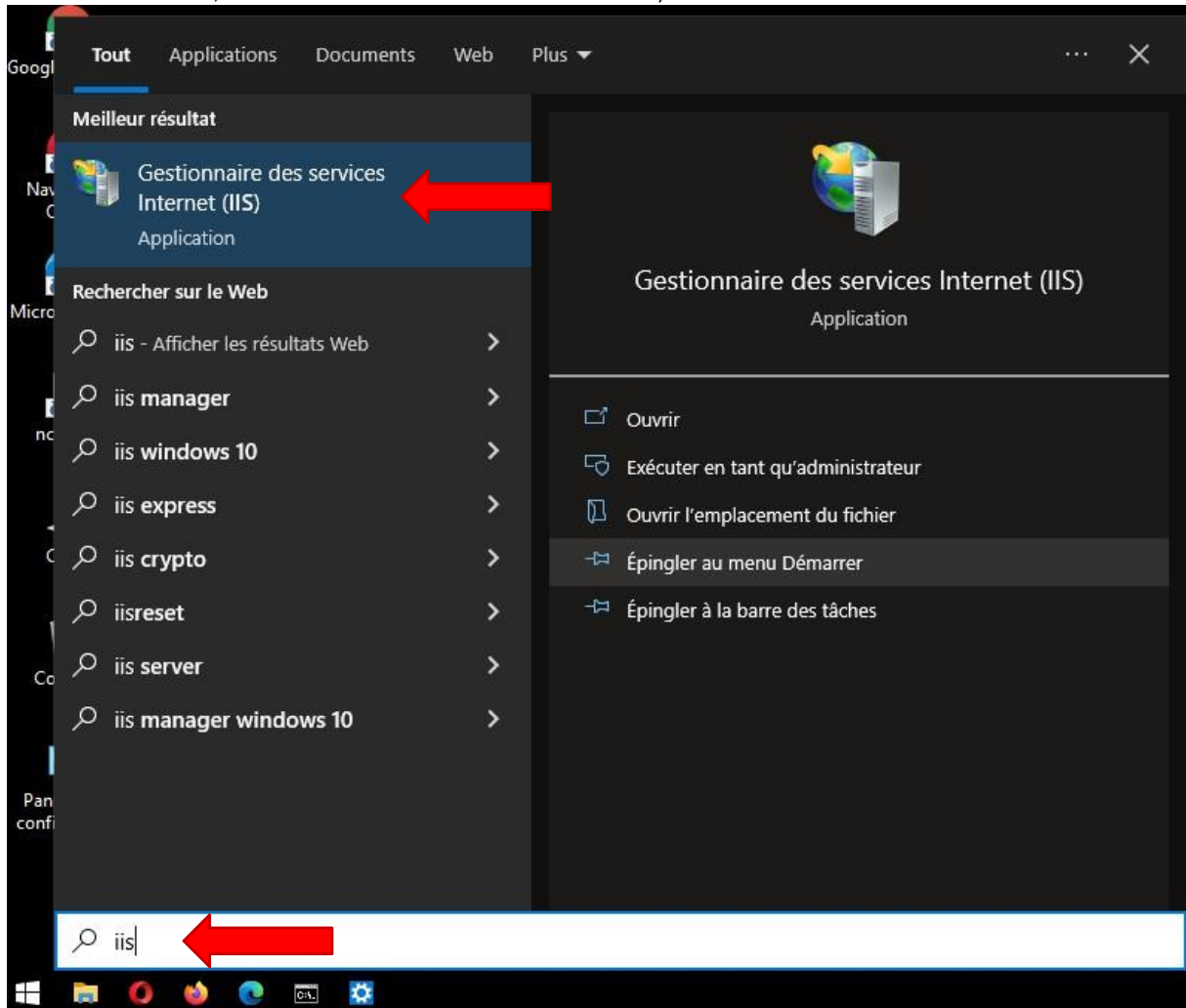


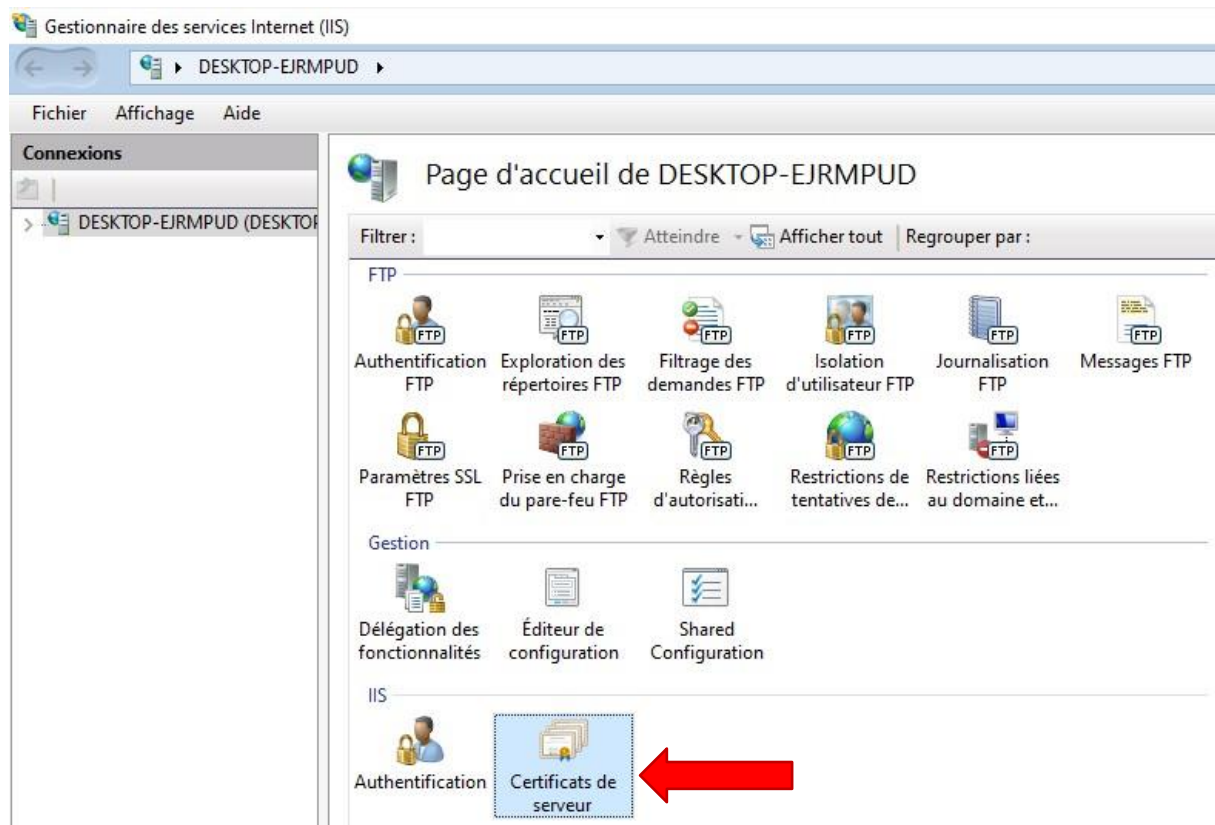
La console de gestion IIS doit être installée sinon vous n'aurez pas d'interface graphique pour gérer votre service FTP Server.



## b. Configuration du Serveur FTP

Ouvrez la console de gestion IIS ou Gestionnaire des services Internet (dans les outils d'administration, Gestionnaire des services Internet) ou saisir directement iis :





### i. Création d'un certificat autosigné

Choisir sur l'écran ci-dessus, Certificats de serveur puis à droite en haut ouvrir la fonctionnalité.  
Cliquer ensuite à droite sur : créer un certificat auto-signé

#### Créer un certificat auto-signé



#### Indiquer un nom convivial

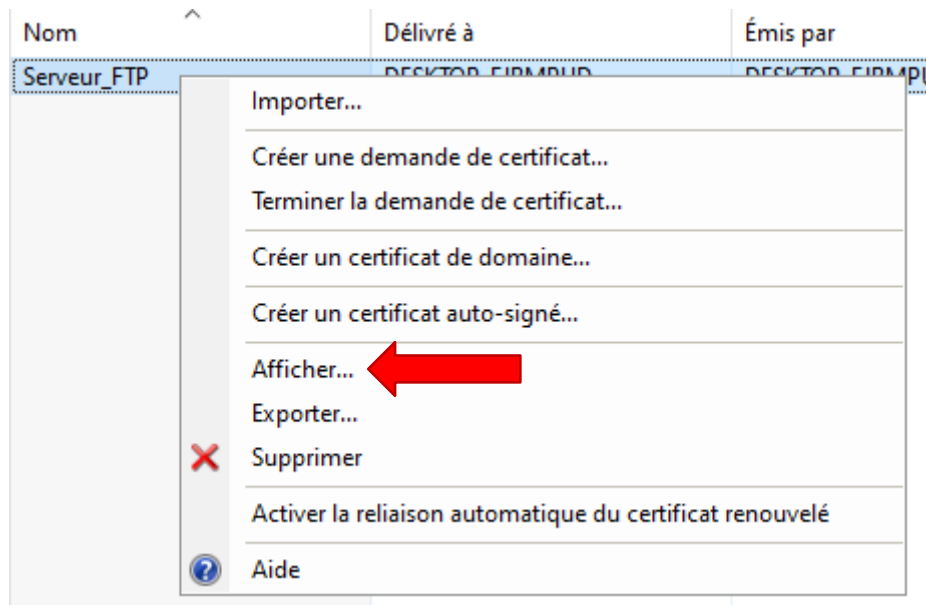
Indiquez un nom de fichier pour la demande de certificat. Ces informations peuvent être envoyées à une autorité de certification en vue de la signature :

Indiquer un nom convivial pour le certificat :

Sélectionnez un magasin de certificats pour le nouveau certificat :

Personnel





Faire ensuite un clic droit sur le certificat et choisir Afficher

Quelles informations pouvez-vous retrouver ?

#### REMARQUE : CERTIFICAT AUTO-SIGNE

Quand un certificat auto-signé est-il approprié ?

En général, un certificat auto-signé peut être une option appropriée lorsqu'il est utilisé pour un site interne (intranet) ou pour tester un site Web avant qu'il ne soit disponible pour le grand public. Cette approche peut permettre aux propriétaires et aux développeurs de sites d'économiser le coût d'achat d'un certificat signé par une autorité de certification tout en offrant certains avantages en matière de sécurité.

Cependant, dès que le site est en ligne, il est fortement recommandé d'utiliser un certificat signé par une autorité de certification d'une tierce partie réputée.

Un certificat auto-signé fournit un certificat permettant d'activer les sessions SSL entre les clients et le serveur, en attendant que le certificat officiellement signé soit renvoyé par l'autorité de certification (CA). Une clé privée et publique est créée au cours de ce processus. La création d'un certificat auto-signé génère un certificat X509 auto-signé dans la base de données de clés identifiée. Un certificat autosigné porte le même nom d'émetteur que son nom de sujet.

Pourquoi et quand exécuter cette tâche ?

Utilisez cette procédure si vous êtes votre propre autorité de certification pour un réseau Web privé. De nombreuses organisations sont tentées d'utiliser des certificats SSL auto-signés plutôt que des certificats émis et vérifiés par une Autorité de Certification, et ce essentiellement pour des raisons financières. A l'inverse des certificats émis par une AC, les certificats auto-signés sont gratuits. Même si les certificats SSL auto-signés chiffrent tout aussi bien les connexions de clients et les identifiants d'autres comptes personnels, ils déclenchent des alertes de sécurité sur la plupart des serveurs web car ils n'ont pas été vérifiés par une Autorité de Certification de confiance. La plupart du temps, ces alertes conseillent aux visiteurs de quitter la page pour des raisons de sécurité.

Quel risque lorsqu'un certificat auto-signé est utilisé sur un site interne

Si les dangers que représente l'utilisation d'un certificat auto-signé sur un site public paraissent évidents, il est important de comprendre qu'ils existent également pour les sites privés.



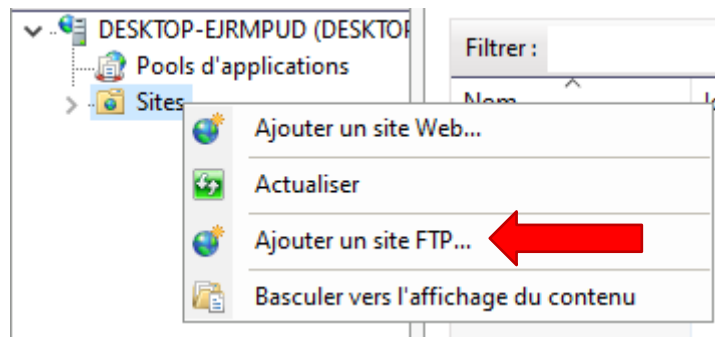
L'utilisation d'un certificat auto-signé sur des sites utilisés en interne, tels qu'un portail pour les employés, déclenche également des messages d'alerte dans les navigateurs. De nombreuses organisations conseillent à leurs employés de simplement ignorer ces messages de sécurité car elles savent que leurs sites sont sans danger. Cependant, un tel comportement peut pousser certaines personnes à également ignorer ces messages lorsqu'elles visitent des sites publics, ce qui les rend vulnérables au malware et aux autres menaces.

Evitez ce risque !

L'utilisation de certificats SSL émis par une Autorité de Certification de confiance élimine les messages de sécurité alarmants dans les navigateurs, ce qui permet de protéger la réputation de votre marque et de conserver la confiance de vos clients. Cela encourage également vos employés à plus de prudence lorsqu'ils naviguent sur Internet.

## ii. Création d'un nouveau site de type FTP

Faire ensuite un clic droit sur Sites puis choisir Ajouter un site FTP :



Définissez le chemin vers le répertoire FTP puis indiquez l'adresse IP locale du serveur FTP ainsi que le port :



Ajouter un site FTP



Informations sur le site

Nom du site FTP :

FTP\_SITE\_STPBB



Répertoire de contenu

Chemin d'accès physique :

C:\inetpub\ftproot




Précédent

Suivant





Ajouter un site FTP ? X

 **Liaison et paramètres SSL**

**Liaison**

Adresse IP : 192.168.0.100 Port : 21

☐ Activer les noms des hôtes virtuels :  
Hôte virtuel (exemple : ftp.contoso.com) :

☒ Démarrer automatiquement le site FTP

**SSL**

☐ Pas de SSL  
☐ Autoriser SSL  
☒ Exiger SSL

Certificat SSL : Serveur\_FTP Sélectionner... Afficher...

Précédent Suivant Terminer Annuler



Ajouter un site FTP



## Informations sur les autorisations et l'authentification

**Authentification**

☐ Anonyme

☒ De base ←

**Autorisation**

Autoriser l'accès à :

Tous les utilisateurs ←

**Autorisations**

☒ Lecture ←

☒ Écriture ←

Précédent Suivant Terminer

**Sites**

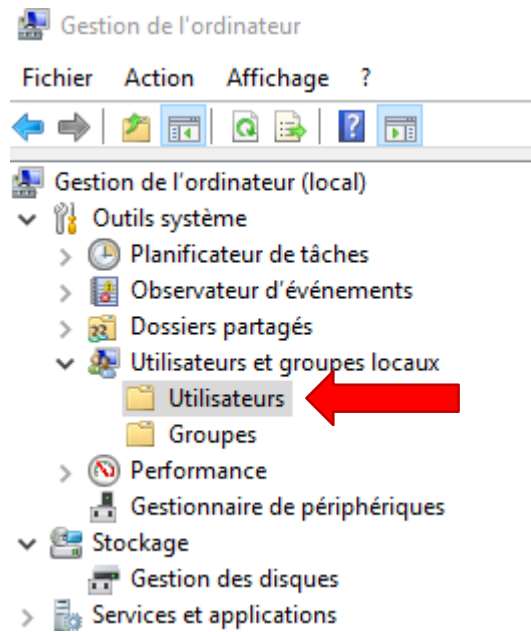
Filtrer : Atteindre Afficher tout Regrouper par : Aucun regroupement

Nom	Identificate...	État	Liaison	Chemin d'accès
Default Web Site	1	Arrêté (Aucun)		%SystemDrive%\inetpub\wwwr
FTP_SITE_STPBB	2	Démarré (ftp)	192.168.0.100:21: (ftp)	C:\inetpub\ftproot ←

## iii. Création d'un utilisateur

Saisir compmgmt.msc





Nouvel utilisateur ? X

Nom d'utilisateur :

Nom complet :

Description :

---

Mot de passe :

Confirmer le mot de passe :

☐ L'utilisateur doit changer le mot de passe à la prochaine ouverture de session

☐ L'utilisateur ne peut pas changer de mot de passe

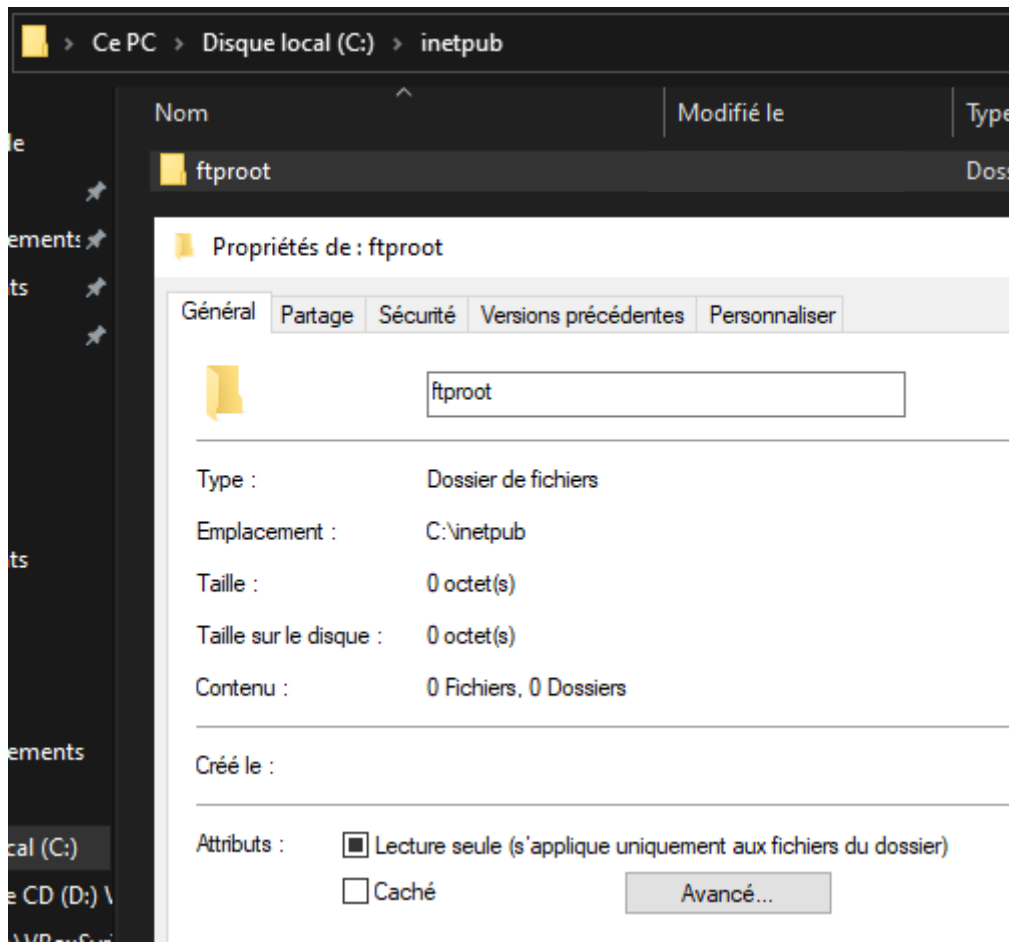
☒ Le mot de passe n'expire jamais

☐ Le compte est désactivé

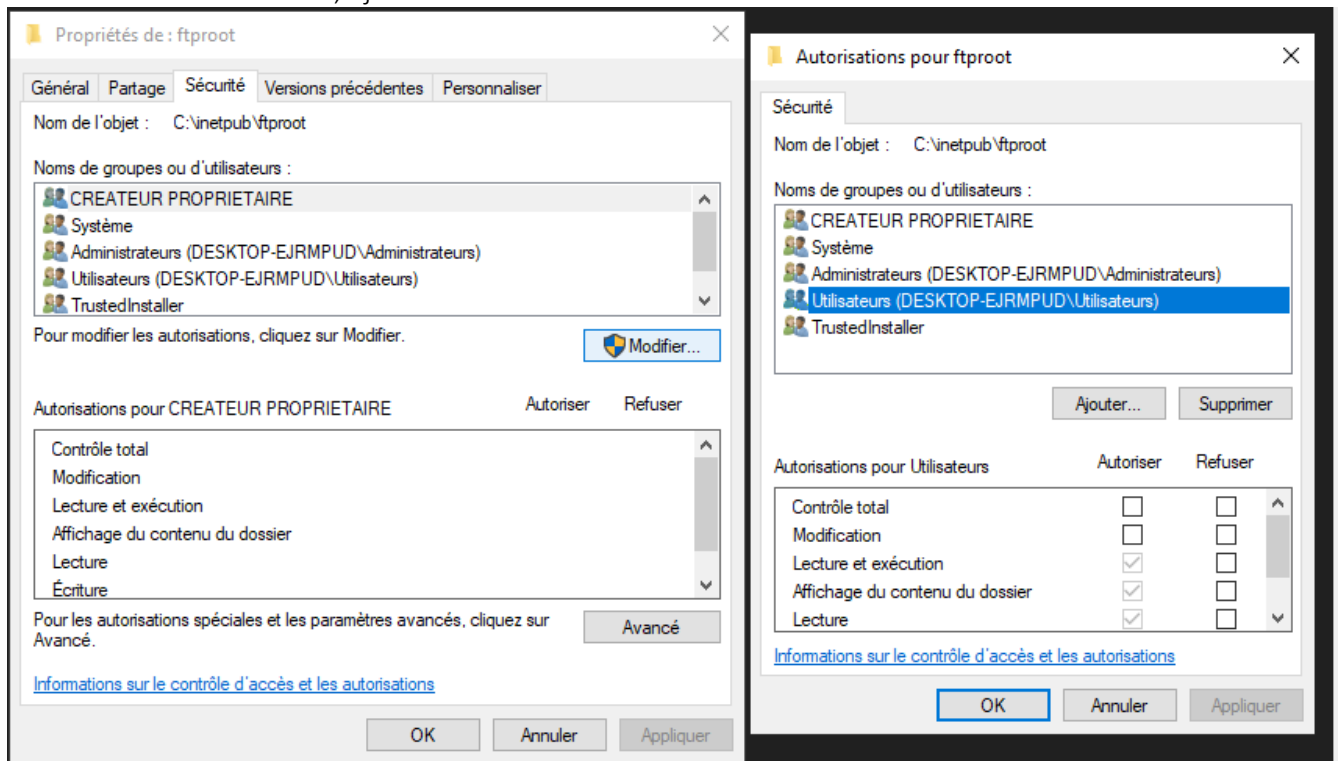
Aide Créer Fermer

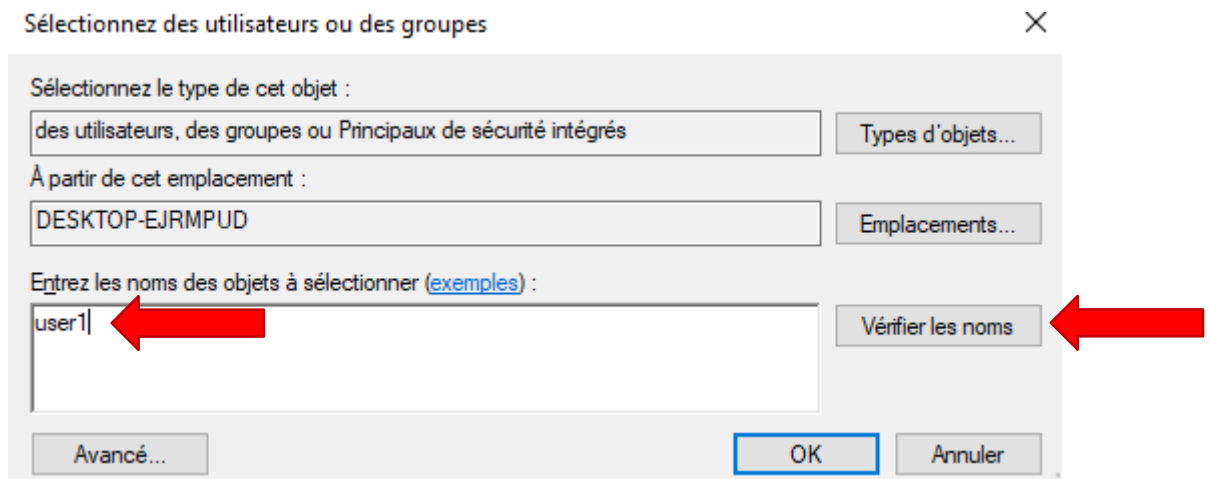
Se rendre dans c:\inetpub puis modifier les propriétés du dossier ftproot :





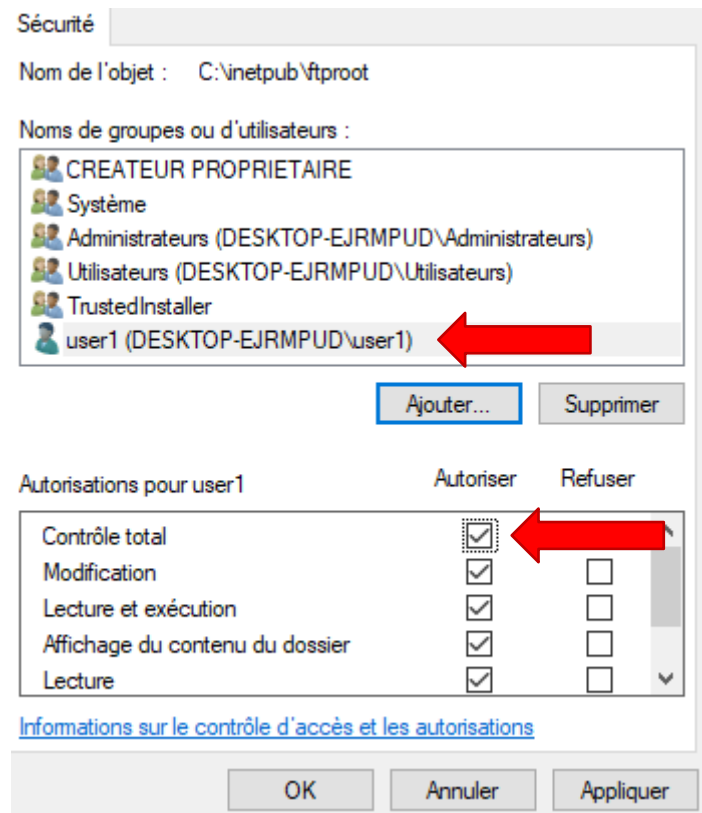
Dans Sécurité Utilisateurs, ajouter user1 :





Choisir Vérifier les noms puis ok :

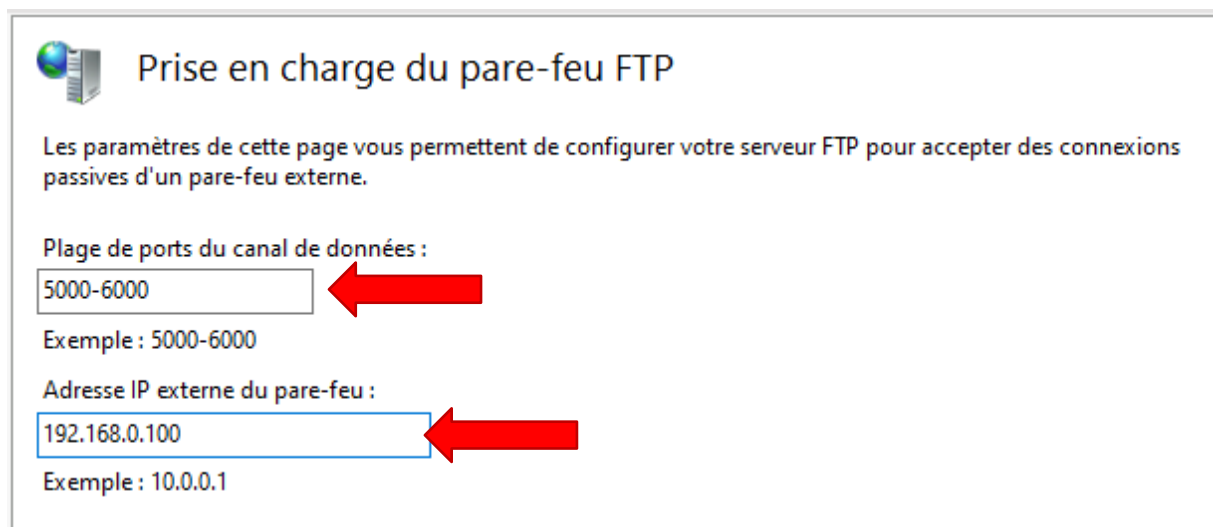
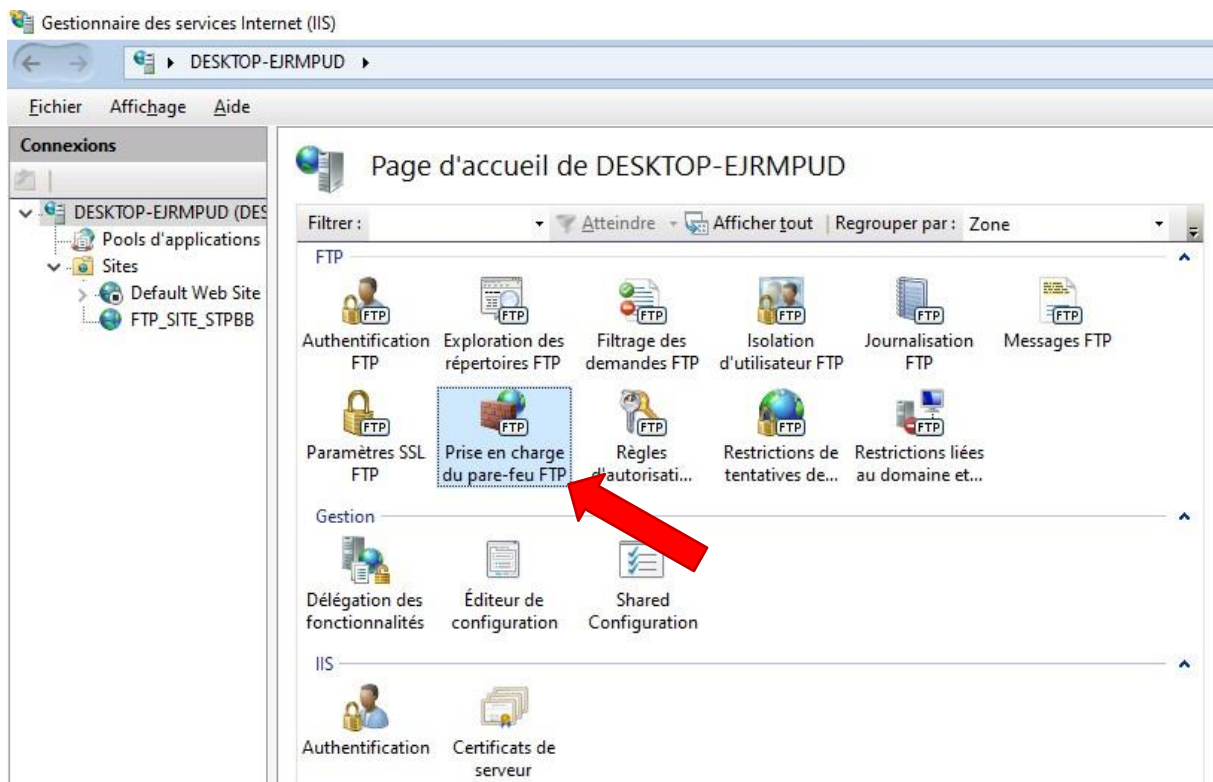
On mettra un contrôle total :



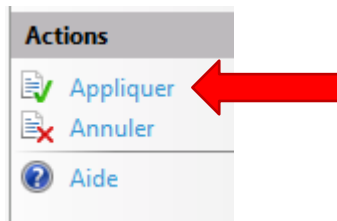
#### iv. Paramétrer la connexion passive reçue depuis le firewall si besoin

Dans la console IIS, on va paramétrer le Firewall :





Choisir à droite Actions, Appliquer puis ok :



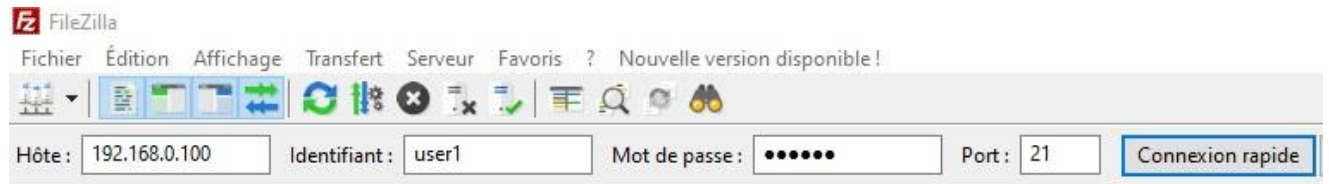
A ce niveau, le serveur FTP est fonctionnel mais pas obligatoirement accessible depuis l'extérieur ! Car, par défaut, le pare-feu intégré de Windows bloquera les connexions FTP lorsqu'elles seront considérées comme une menace pour la sécurité et lorsqu'elles tenteront de se connecter, une erreur d'accès sera générée.



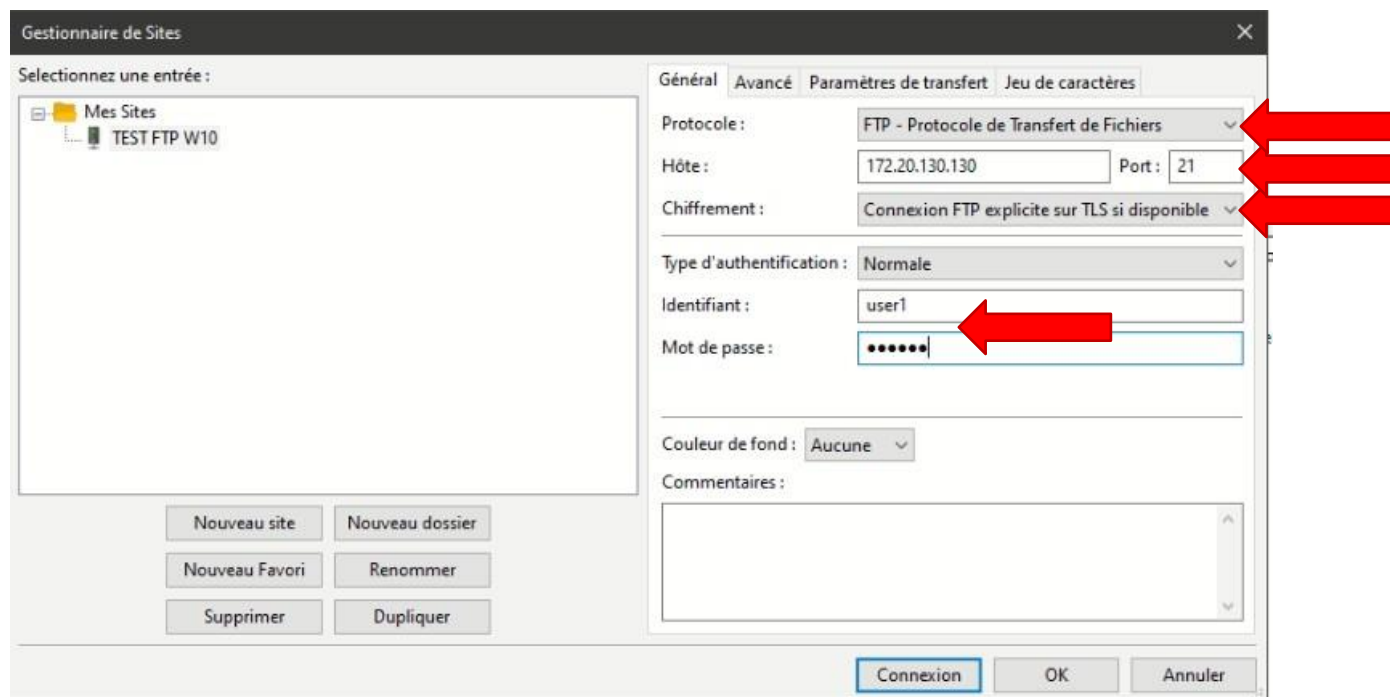
## v. Test de la connexion

Depuis un client FTP comme FileZilla ou Winscp :

Avec FileZilla :

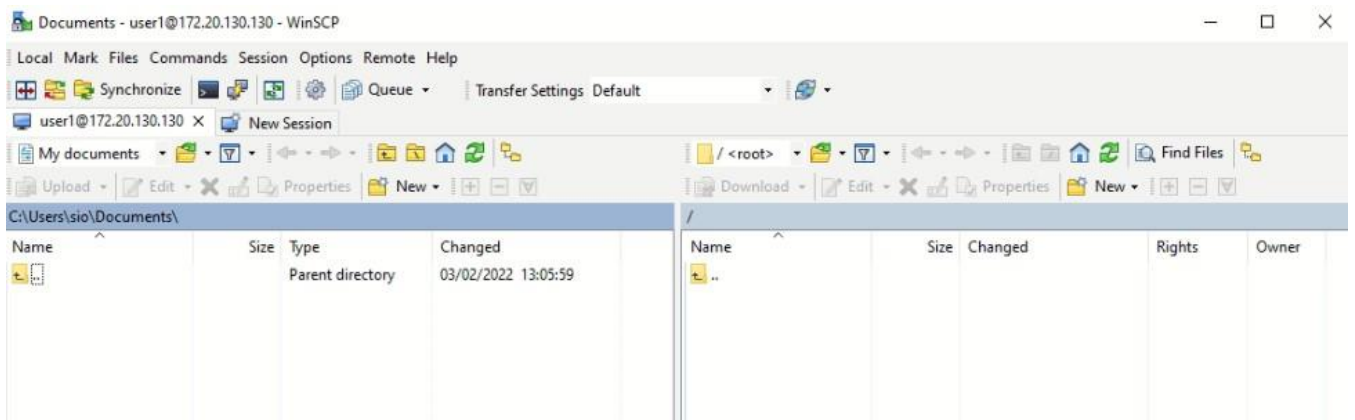
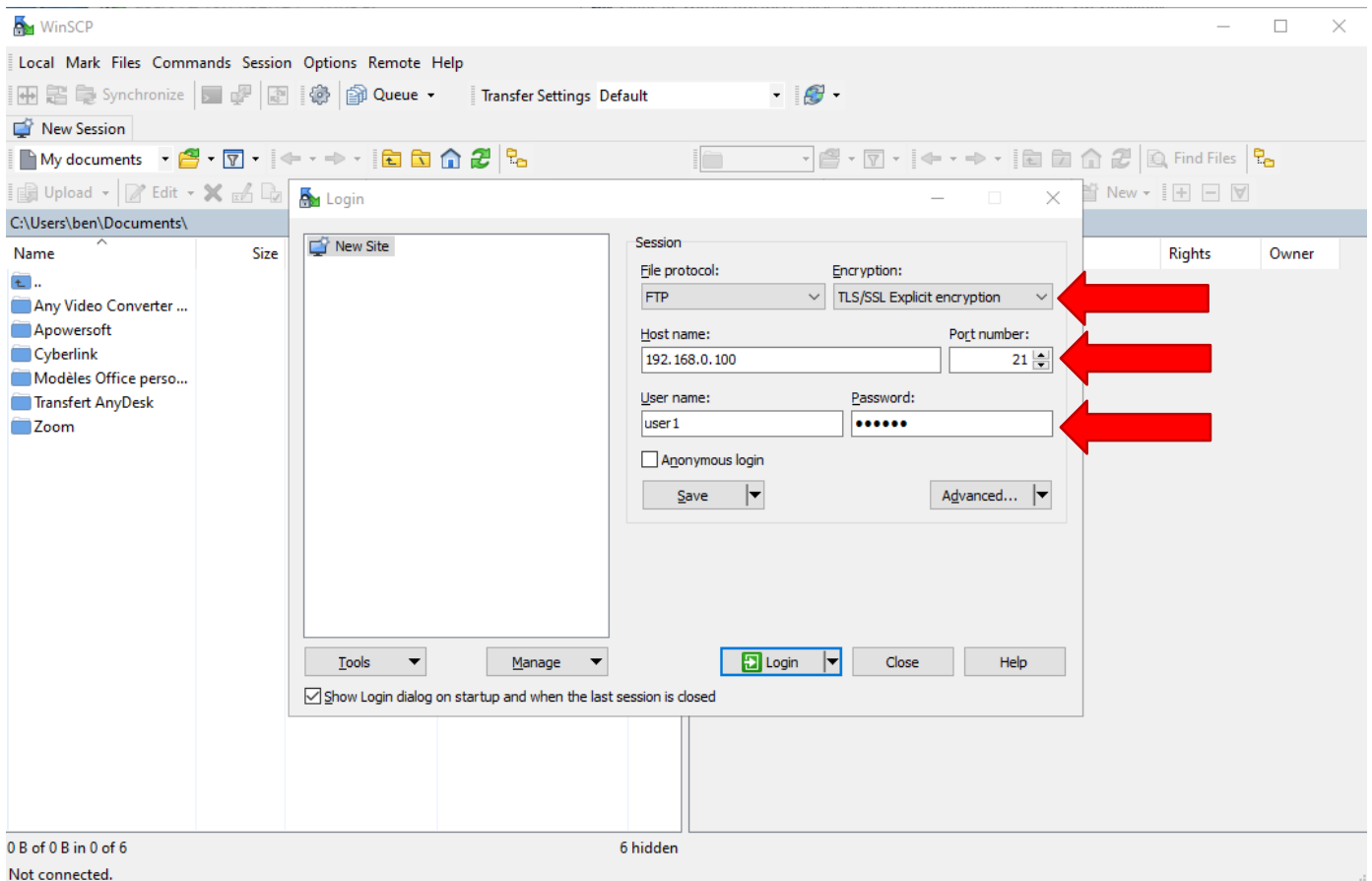


Vous pouvez également passer par le gestionnaire de Sites de Filezilla et définir un site (dans le cas suivant le serveur FTP est à l'adresse IP 172.20.130.130 :



Avec WinSCP :





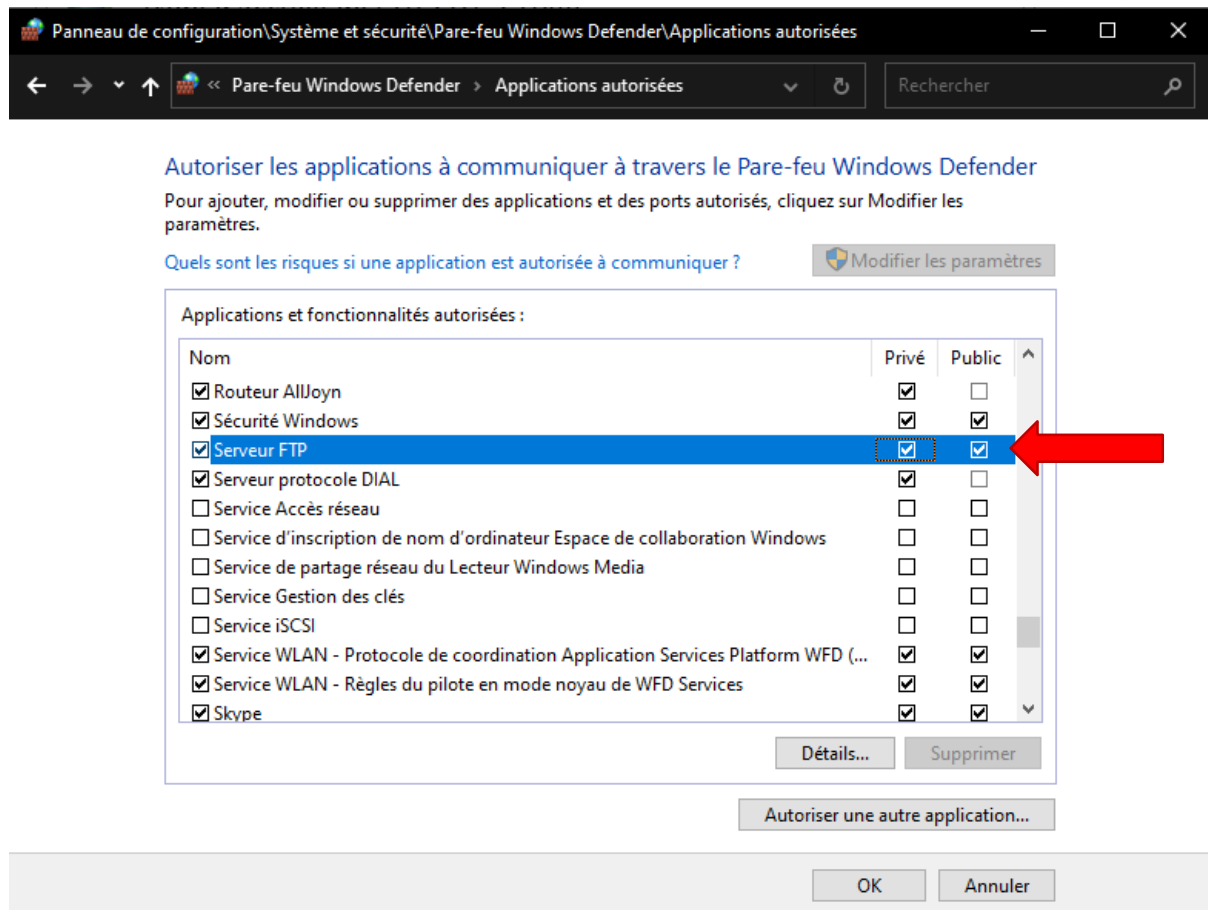
## vi. Configurer les règles de pare-feu dans Windows

Si le pare-feu de Windows est actif, il faut autoriser le FTP au niveau réseau.

Accédez à l'utilitaire « Windows Security », puis à la section « Protection de pare-feu et réseau » :







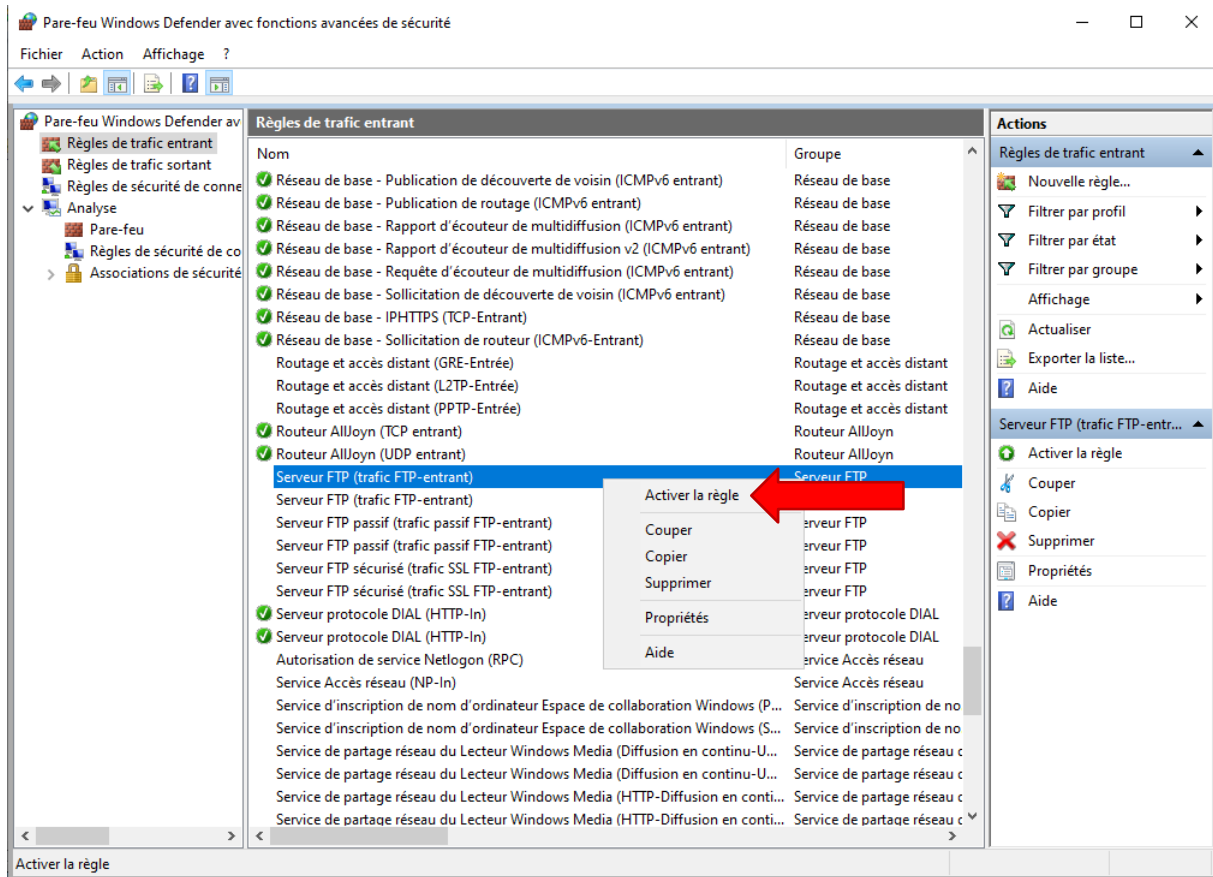
Ouvrez une invite de commande et tapez : netstat -aon | more

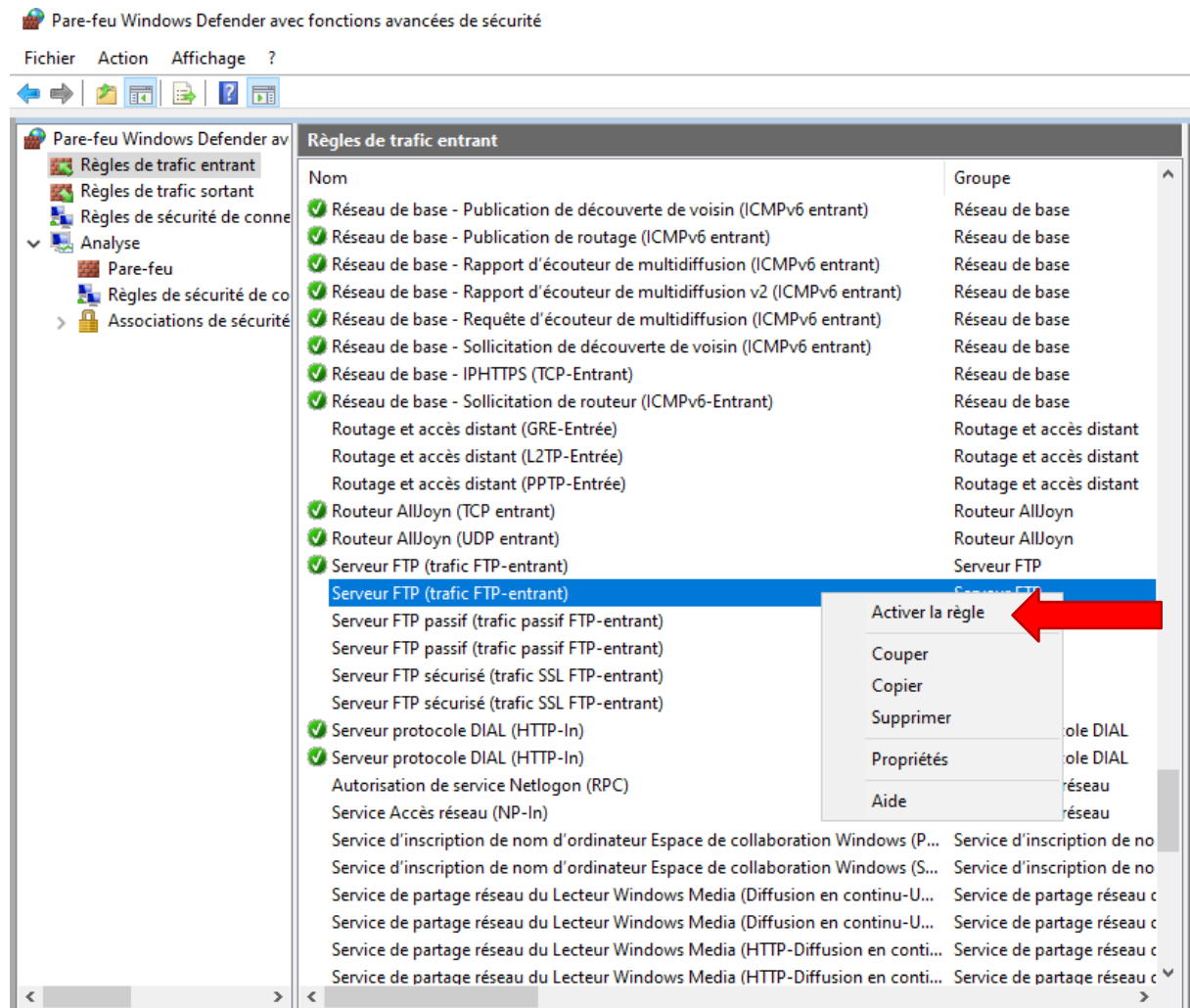

Vous pourrez ainsi voir les connexions en écoute pour le service FTP.

Cette règle précédente n'autorise en principe que les accès au serveur FTP en local et est insuffisante pour des accès de l'extérieur. Il vous faudra souvent ouvrir le port 21 (par défaut) en TCP sur le firewall frontal (et tous les firewalls traversés en fait par le flux FTP) ainsi que « NATTER » le port FTP vers le serveur FTP.

Dans mes tests, il a fallu que j'autorise également dans les fonctions avancées du pare-feu les règles de trafic entrant concernant serveur FTP :



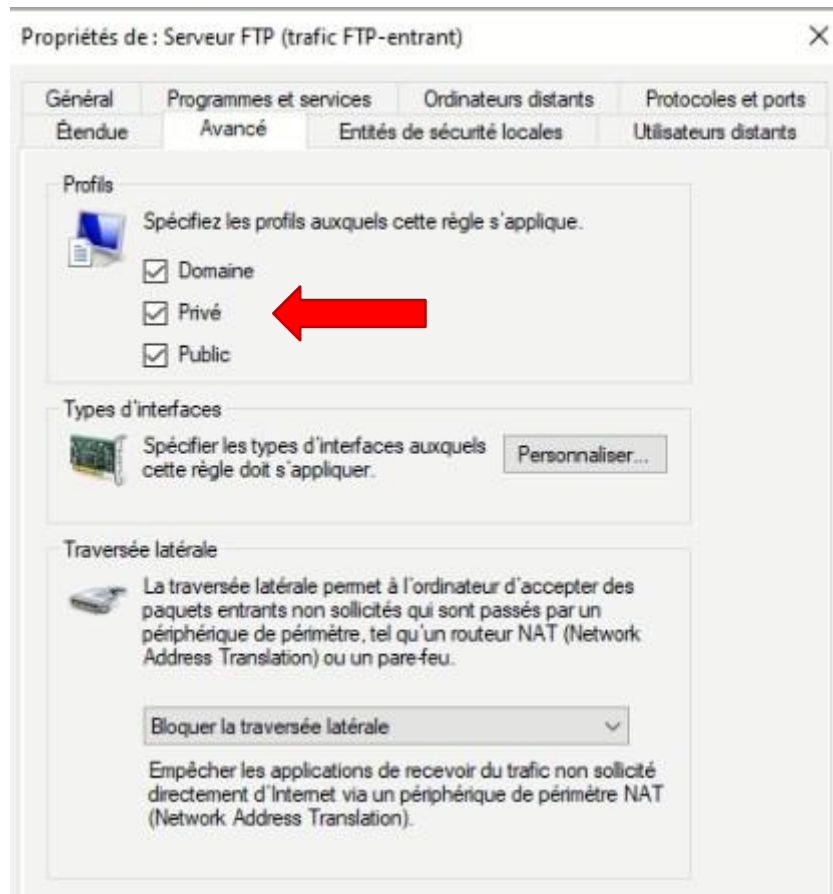


✓ Serveur FTP (trafic FTP-entrant)	Serveur FTP	Tout	Oui
✓ Serveur FTP (trafic FTP-entrant)	Serveur FTP	Tout	Oui
✓ Serveur FTP passif (trafic passif FTP-entra...	Serveur FTP	Tout	Oui
✓ Serveur FTP passif (trafic passif FTP-entra...	Serveur FTP	Tout	Oui
✓ Serveur FTP sécurisé (trafic SSL FTP-entra...	Serveur FTP	Privé, ...	Oui

Parfois, il faut également se rendre dans les propriétés et valider les profils :

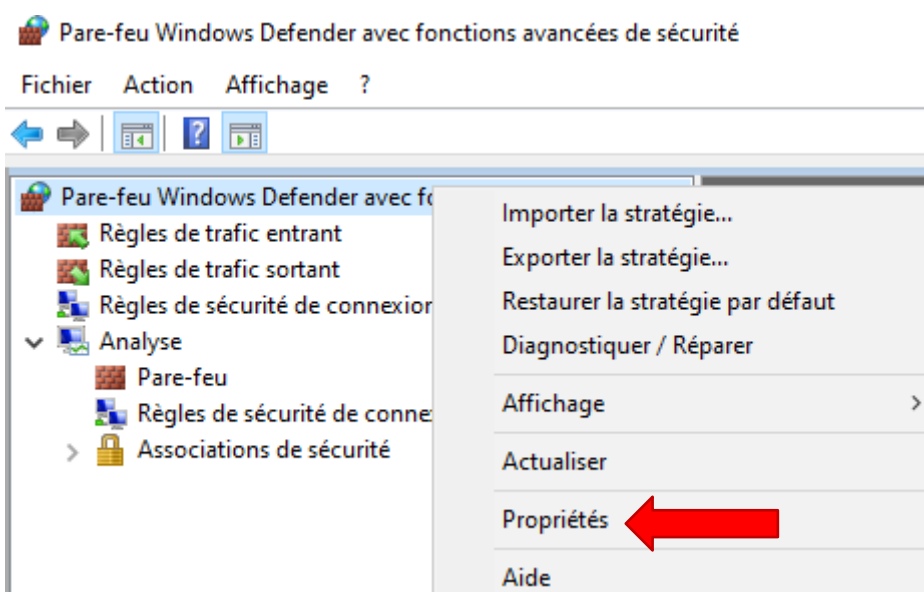




Lors de mes différentes mise en œuvre, il a parfois été laborieux de « trouver » les bons paramétrages pour que le pare-feu autorise le service FTP !

Pour gagner du temps, vous pouvez activer les « logs » du pare-feu et vous pourrez alors vous assurer que c'est bien lui qui bloque et non pas un autre souci.

Rendez-vous dans les propriétés du pare-feu avancé :



Propriétés de : Pare-feu Windows Defender avec fonctions avancées... X

Profil de domaine Profil privé Profil public Paramètres IPsec

Spécifiez le comportement lorsqu'un ordinateur est connecté à un emplacement réseau privé.

**État**

État du pare-feu : **Activé (recommandé)**

Connexions entrantes : **Bloquer (par défaut)**

Connexions sortantes : **Autoriser (par défaut)**

Connexions réseau protégées : **Personnaliser...**

**Paramètres**

☒ Spécifier les paramètres définissant le comportement du Pare-feu Windows Defender. **Personnaliser...**

**Enregistrement**

☒ Spécifiez les paramètres de journalisation pour le dépannage. **Personnaliser...**

**OK Annuler Appliquer**

Personnaliser les paramètres de journalisation pour le Profil privé X

Nom : **.\system32\LogFiles\Firewall\pfirewall.log** **Parcourir...**

Taille maximale (Ko) : **4 096**

Enregistrer les paquets ignorés : **Oui**

Consigner les connexions réussies : **Oui**

Remarque : si vous configurez le nom du fichier journal sur un objet de stratégie de groupe, assurez-vous que le compte du service de Pare-feu Windows Defender possède les autorisations d'écriture dans le dossier contenant le fichier journal.

Le chemin d'accès par défaut du fichier journal est %systemroot%\system32\logfiles\firewall\pfirewall.log.

**OK Annuler**

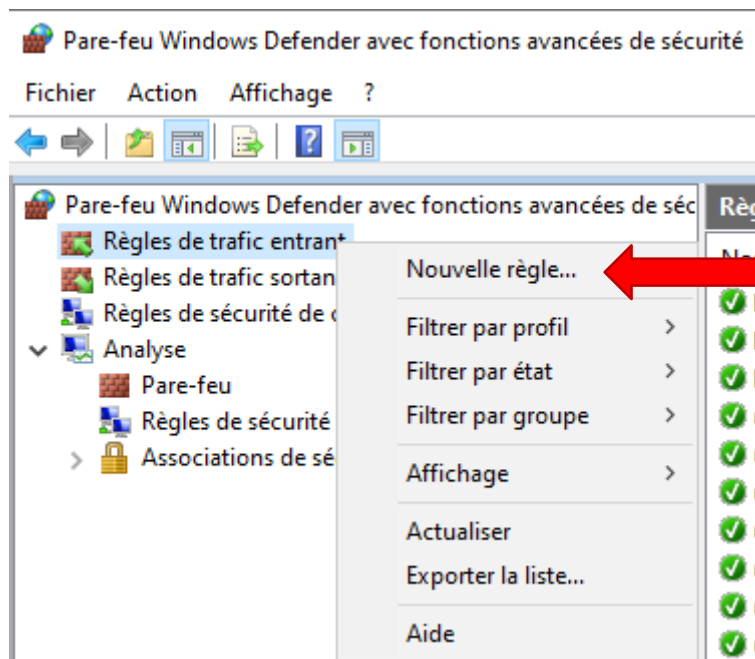
Voici l'exemple de « log » obtenu à la lecture du fichier pfirewall.log :

```
2022-03-01 15:01:03 DROP TCP 192.168.0.250 192.168.0.100 53671 21 52 S 18690475 0 64240 - - - RECEIVE
2022-03-01 15:01:07 DROP TCP 192.168.0.250 192.168.0.100 53670 21 52 S 3093917835 0 64240 - - - RECEIVE
2022-03-01 15:01:08 DROP UDP 192.168.0.250 192.168.0.100 61085 1000 346 - - - RECEIVE
```

Le poste en 192.168.0.250 n'arrive pas à ouvrir une session FTP sur le serveur 192.168.0.100 car le pare-feu Windows « drop » les paquets !



On va ouvrir les ports 20 et 21 en TCP pour le service FTP :



Assistant Nouvelle règle de trafic entrant

### Type de règle

Sélectionnez le type de règle de pare-feu à créer.

Étapes :

- Type de règle
- Protocole et ports
- Action
- Profil
- Nom

Quel type de règle voulez-vous créer ?

- ☐ **Programme**  
Règle qui contrôle les connexions d'un programme.
- ☒ **Port**  
Règle qui contrôle les connexions d'un port TCP ou UDP.
- ☐ **Prédéfinie :**  
@FirewallAPI.dll,-80200  
Règle qui contrôle les connexions liées à l'utilisation de Windows.
- ☐ **Personnalisée**  
Règle personnalisée.



## Assistant Nouvelle règle de trafic entrant

### Protocole et ports

Spécifiez les protocoles et les ports auxquels s'applique cette règle.

**Étapes :**

- Type de règle
- Protocole et ports
- Action
- Profil
- Nom

Cette règle s'applique-t-elle à TCP ou UDP ?

☒ **TCP** 

☐ **UDP**

Cette règle s'applique-t-elle à tous les ports locaux ou à des ports locaux spécifiques ?

☐ **Tous les ports locaux**

☒ **Ports locaux spécifiques :**  

Exemple : 80, 443, 5000-5010

## Assistant Nouvelle règle de trafic entrant



### Action

Spécifiez une action à entreprendre lorsqu'une connexion répond aux conditions spécifiées dans la règle.

**Étapes :**

- Type de règle
- Protocole et ports
- Action
- Profil
- Nom

Quelle action entreprendre lorsqu'une connexion répond aux conditions spécifiées ?

☒ **Autoriser la connexion** 

Cela comprend les connexions qui sont protégées par le protocole IPsec, ainsi que celles qui ne le sont pas.

☐ **Autoriser la connexion si elle est sécurisée**

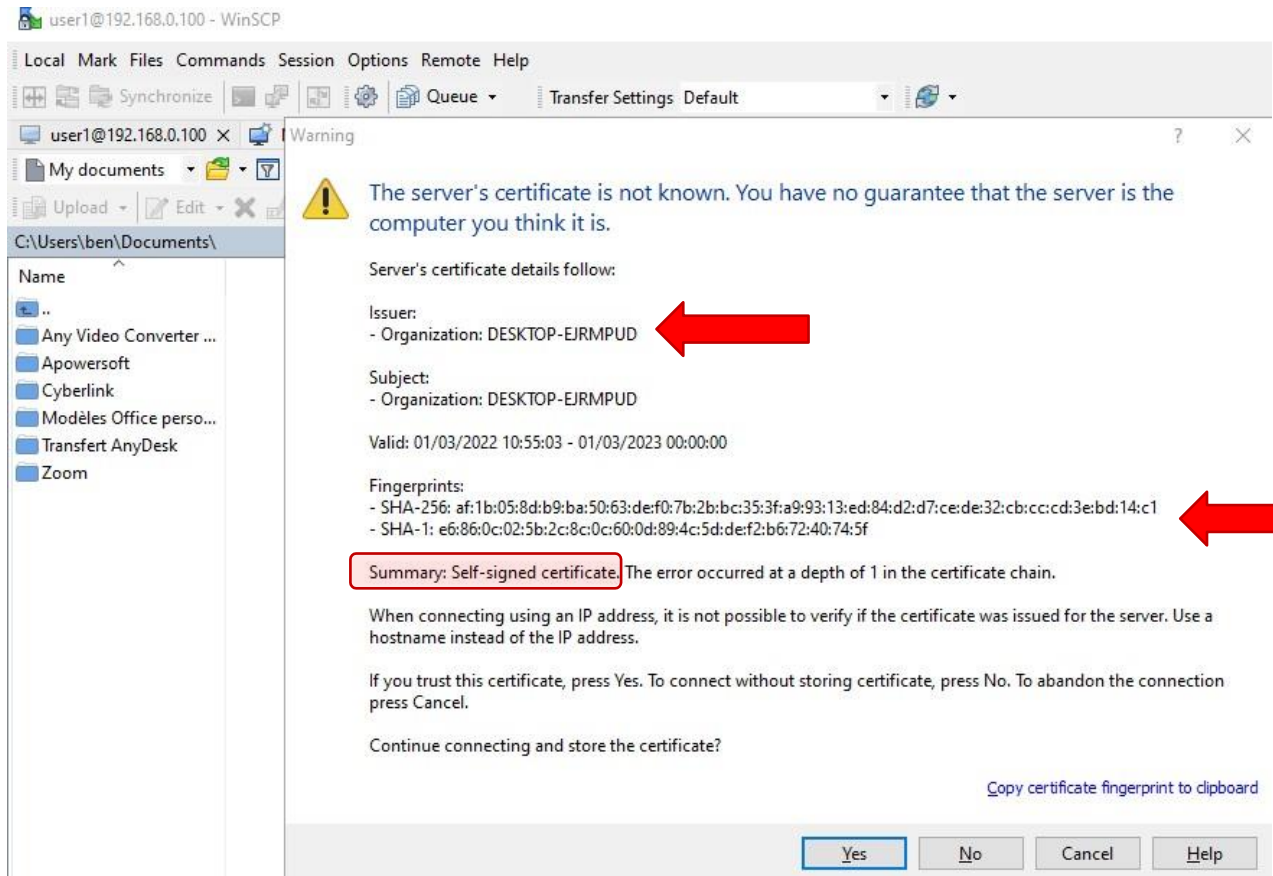
Cela comprend uniquement les connexions authentifiées à l'aide du protocole IPsec. Les connexions sont sécurisées à l'aide des paramètres spécifiés dans les propriétés et règles IPsec du nœud Règle de sécurité de connexion.

☐ **Bloquer la connexion**

Les accès sont maintenant autorisés et la présentation du certificat lors de la connexion FTP apparaît :



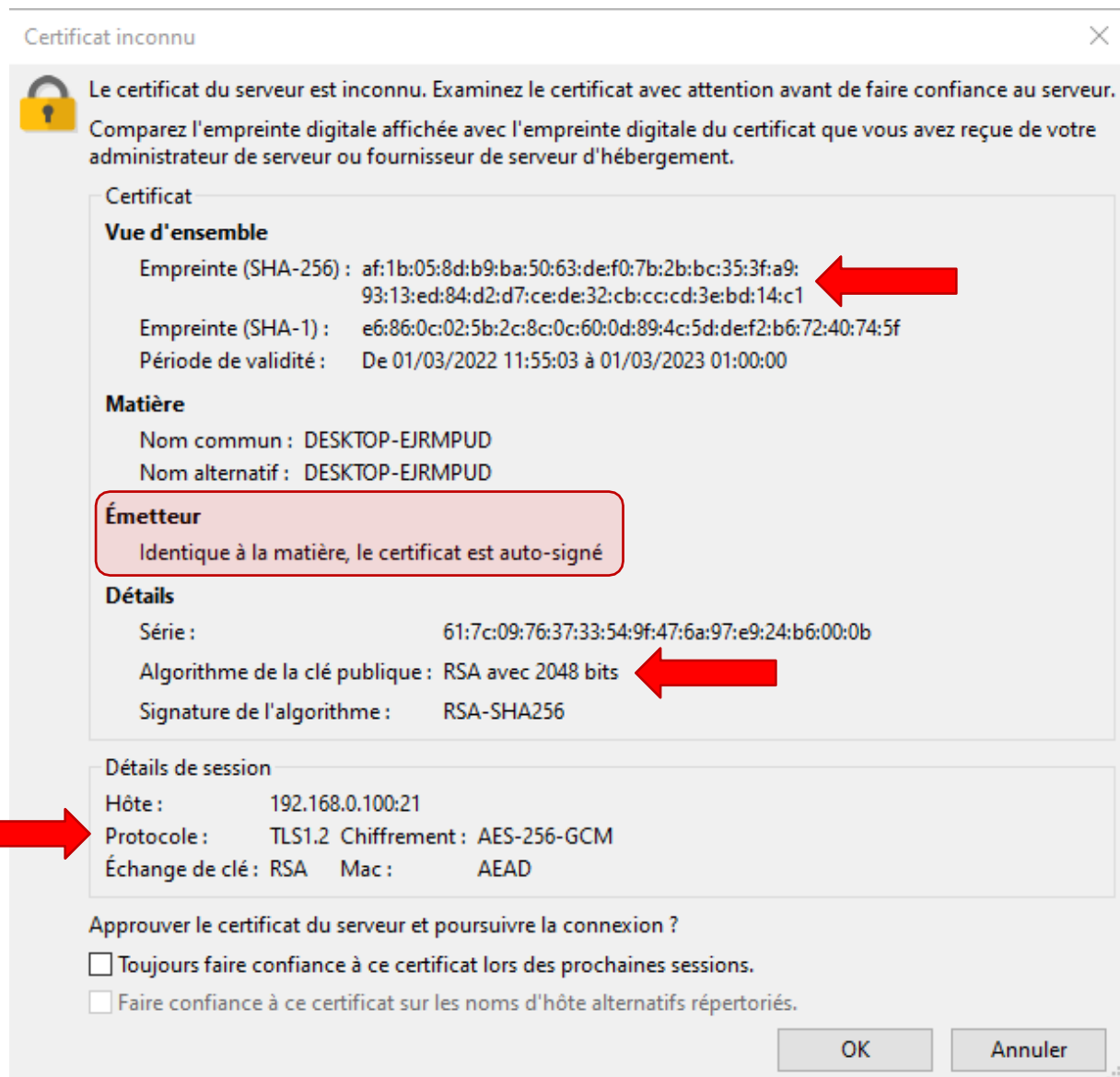




Ci-après l'affichage avec FileZilla :







Voici l'exemple de « log » obtenu à la lecture du fichier pfirewall.log :

```
2022-03-01 15:18:48 ALLOW TCP 192.168.0.250 192.168.0.100 53982 21 0 - 0 0 0 - - - RECEIVE
```

La connexion est autorisée.

*Vous pouvez désactiver les logs si vous n'en n'avez plus besoin ! sinon, faites attention à ce que le fichier de logs ne grossisse pas trop et ne sature pas le disque dur du serveur !*

## vii. Bug du service FTP

On retrouve parfois sur Internet des utilisateurs qui ont fait remonter des « bugs » sur certaines versions de Windows Server ou Windows 10 Pro. A priori, le service FTP même bien configuré, ne fonctionne pas correctement. Lors de l'utilisation en passif, le listing du répertoire distant ne monte pas.

Voici une solution :



```

C:\Windows\System32\LogFiles\Firewall> sc sidtype ftpsvc unrestricted
[SC] ChangeServiceConfig2 réussite(s)

C:\Windows\System32\LogFiles\Firewall>net stop ftpsvc
Le service Service FTP Microsoft s'arrête.
Le service Service FTP Microsoft a été arrêté.

C:\Windows\System32\LogFiles\Firewall>net start ftpsvc
Le service Service FTP Microsoft démarre.
Le service Service FTP Microsoft a démarré.

C:\Windows\System32\LogFiles\Firewall>sc sidtype
DESCRIPTION :
    Modifie le paramètre de type de SID (Security
    Identifier) d'un service.

    Si ce paramètre est « unrestricted », le Gestionnaire de
    contrôle des services (SCM) ajoute le SID de ce service au jeton de
    processus du service au démarrage suivant du processus du service
    provoqué par le démarrage du premier service du processus.

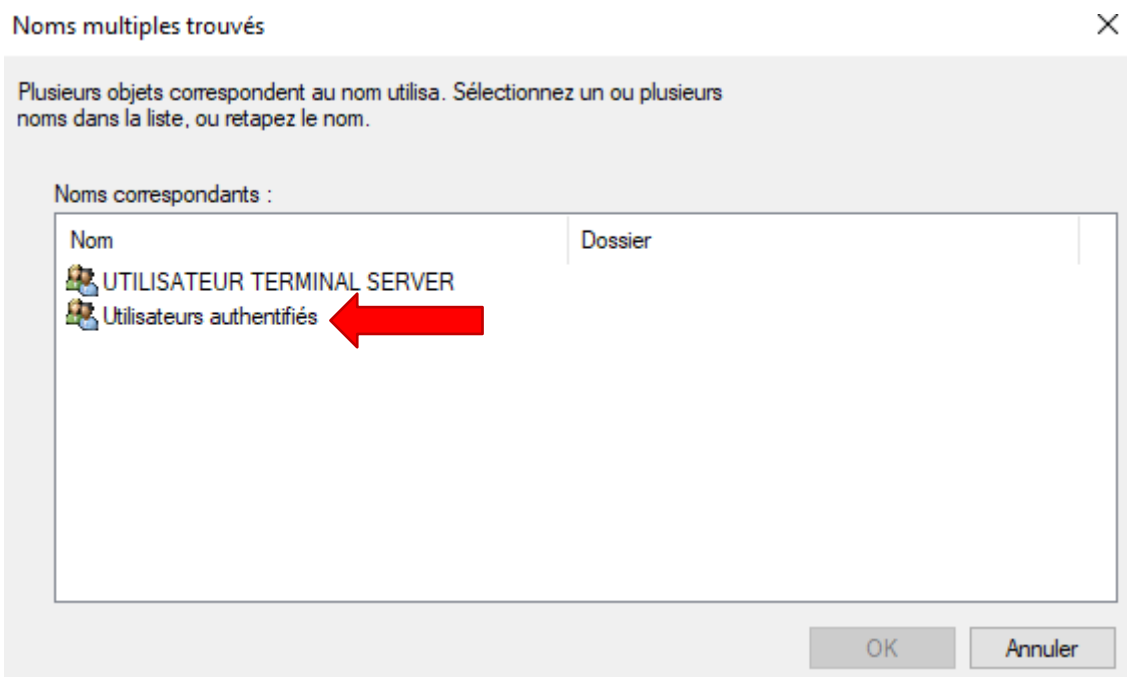
```

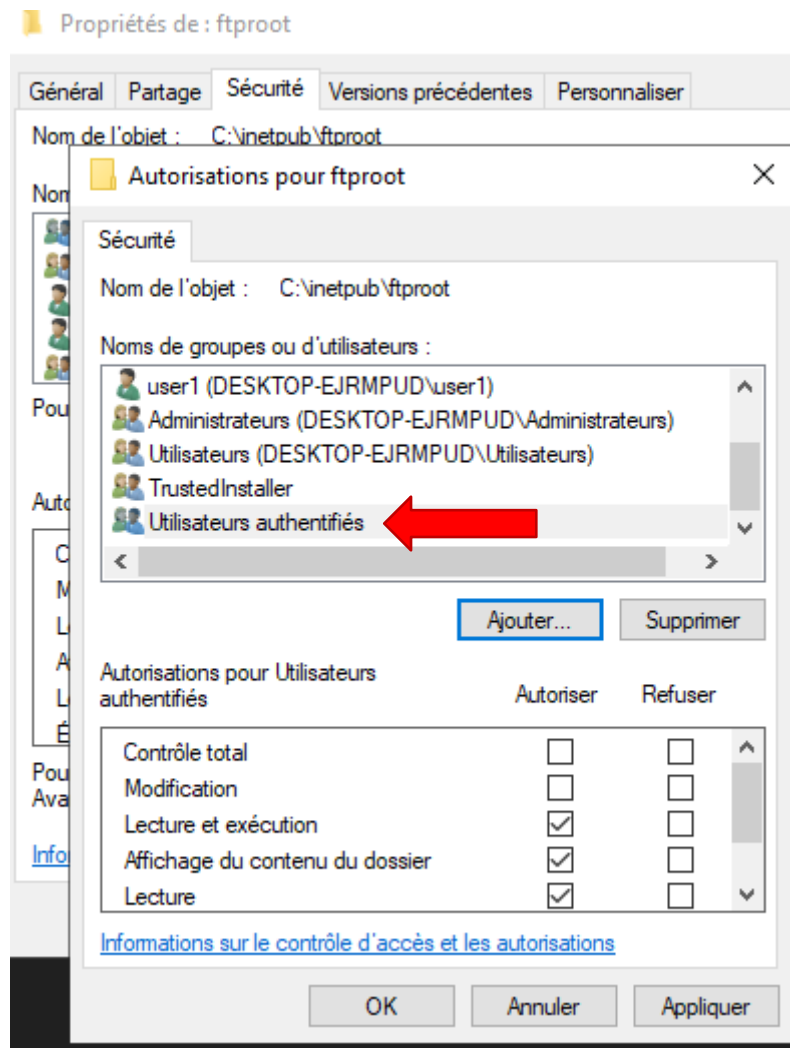
*On modifie le type de SID à « unrestricted » puis on arrête et redémarre le service FTP.*

## i. Problème de droits

On retrouve également sur Internet des utilisateurs qui ont fait remonter des problèmes de droits. Parfois les accès en lecture/écriture au FTP sont interdits.

Une solution consisterait à ajouter dans les droits, le groupe des utilisateurs authentifiés !





### c. Analyse du trafic réseau avec Wireshark

Il est toujours intéressant de regarder le trafic réseau lors d'une connexion FTP pour voir que la communication est correctement chiffrée :

No.	Time	Source	Destination	Protocol	Length	Info
160	12.298865	172.20.34.23	172.20.130.130	TCP	60	50929 → 21 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
161	12.299150	172.20.130.130	172.20.34.23	FTP	81	Response: 220 Microsoft FTP Service
162	12.299367	172.20.34.23	172.20.130.130	FTP	64	Request: AUTH TLS
163	12.299423	172.20.130.130	172.20.34.23	FTP	103	Response: 234 AUTH command ok. Expecting TLS Negoti
164	12.302243	172.20.34.23	172.20.130.130	TLSv1.2	427	Client Hello
166	12.303289	172.20.130.130	172.20.34.23	TLSv1.2	928	Server Hello, Certificate Server Hello Done
167	12.303792	172.20.34.23	172.20.130.130	TLSv1.2	321	Client Key Exchange
168	12.303792	172.20.34.23	172.20.130.130	TLSv1.2	60	Change Cipher Spec
169	12.303792	172.20.34.23	172.20.130.130	TLSv1.2	99	Encrypted Handshake Message
170	12.303817	172.20.130.130	172.20.34.23	TCP	54	21 → 50929 [ACK] Seq=951 Ack=702 Win=2101504 Len=0
171	12.304968	172.20.130.130	172.20.34.23	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
172	12.307256	172.20.34.23	172.20.130.130	TLSv1.2	95	Application Data
173	12.307342	172.20.130.130	172.20.34.23	TLSv1.2	106	Application Data
174	12.307571	172.20.34.23	172.20.130.130	TLSv1.2	96	Application Data
175	12.307842	172.20.130.130	172.20.34.23	TLSv1.2	104	Application Data



## 2) Travail à faire

### Monter un site FTP avec isolation des utilisateurs

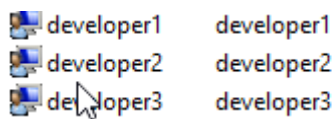
Afin de fournir un espace de stockage Internet à vos utilisateurs, ou encore à des clients pour lesquels vous hébergez des sites Web, vous aurez sûrement besoin de leur fournir un accès FTP.

De façon à restreindre leur champ d'action et à vous assurer qu'ils ne verront pas les répertoires des autres personnes, vous allez devoir configurer l'isolation des utilisateurs.






- Configuration de l'isolation des utilisateurs :

1. Ajout de 3 utilisateurs nommés « developer » :



2. Ajout des 3 dossiers pour chaque utilisateur :

 developer1	14/03/2022 11:37	Dossier de fichiers
 developer2	14/03/2022 11:39	Dossier de fichiers
 developer3	14/03/2022 11:08	Dossier de fichiers

3. Création d'un site FTP avec le gestionnaire des services internet (IIS) :

« Ajouter un site FTP »

4. Nécessité d'un nom de site ainsi que son chemin d'accès :



Nom du site FTP :

Répertoire de contenu

Chemin d'accès physique :

 ...

5. Insertion de l'adresse IP avec le port « 21 », possibilité de choisir un SSL et précision d'un certificat

Liaison

Adresse IP :  Port :

☐ Activer les noms des hôtes virtuels :

Hôte virtuel (exemple : ftp.contoso.com) :

☒ Démarrer automatiquement le site FTP

SSL

☐ Pas de SSL

☐ Autoriser SSL

☒ Exiger SSL

Certificat SSL :

Sélectionner... Afficher...

Sit Web world

Avant Terminer Annuler



6. Préciser l'authentification et l'autorisation des utilisateurs, sélectionner « Terminer »

**Authentification**  
☐ Anonyme  
☒ De base

**Autorisation**  
 Autoriser l'accès à :  

Non sélectionné

  
**Autorisations**  
☐ Lecture  
☐ Écriture


Précédent

Suivant


Terminer

Annuler


7. Partage des dossiers pour chaque utilisateur :



developer1 (CLIENT\_DHCP\developer1)



developer2 (CLIENT\_DHCP\developer2)



developer3 (CLIENT\_DHCP\developer3)

8. Donner un accès total :

Contrôle total	✓
Modification	✓
Lecture et exécution	✓
Affichage du contenu du dossier	✓
Lecture	✓
Écriture	✓



9. Ajout d'une règle d'autorisation pour les 3 utilisateurs dans les règles d'autorisations FTP :

Ajouter une règle d'autorisation Autoriser ? X

Autoriser l'accès à ce contenu à :

☐ Tous les utilisateurs

☐ Tous les utilisateurs anonymes

☐ Rôles ou groupes d'utilisateurs définis :

Exemple : Administrateurs, Invités

☒ Utilisateurs définis :

Exemple : Utilisateur1, Utilisateur2

Autorisations




☒ Lecture

☒ Écriture

OK Annuler

10. Les utilisateurs ont accès au dossier des autres sans restriction.

11. Modification des autorisations sur le dossier, accepter « Affichage du contenu du dossier » sur chaque utilisateur :

 developer1 (CLIENT\_DHCP\developer1)  
 developer2 (CLIENT\_DHCP\developer2)  
 developer3 (CLIENT\_DHCP\developer3)

Pour modifier les autorisations, cliquez sur Modifier.

Modifier...

Autorisations pour developer2		Autoriser	Refuser
Contrôle total			
Modification			
Lecture et exécution			
Affichage du contenu du dossier		✓	
Lecture			
Écriture			



12. Donner les droits à chaque utilisateur sur leur propre dossier :

developer1 (CLIENT\_DHCP\developer1)  
 developer2 (CLIENT\_DHCP\developer2)  
 developer3 (CLIENT\_DHCP\developer3)

Pour modifier les autorisations, cliquez sur Modifier.

Modifier...

Autorisations pour developer1	Autoriser	Refuser
Contrôle total	✓	
Modification	✓	
Lecture et exécution	✓	
Affichage du contenu du dossier	✓	
Lecture	✓	
Écriture	✓	

13. Ajouter un répertoire virtuel :

- Préciser l'alias
- Préciser le chemin d'accès

Ajouter un répertoire virtuel ? X

Nom du site : sitweb  
Chemin d'accès : /

Alias :  
  
 Exemple : images

Chemin d'accès physique :  
 ...

Authentification directe

Se connecter en tant que... Tester les paramètres...

OK Annuler





14. Cocher « répertoire des noms d'utilisateurs (désactiver les répertoires virtuels globaux) », appliquer :



## Isolation d'utilisateur FTP

L'isolation d'utilisateur FTP empêche les utilisateurs d'accéder au répertoire FTP de base d'un autre utilisateur sur ce site FTP.

Ne pas isoler les utilisateurs. Les utilisateurs démarrent dans :

- ☐ Répertoire racine FTP
- ☐ Répertoire des noms d'utilisateurs

Isoler les utilisateurs. Limiter les utilisateurs au répertoire suivant :

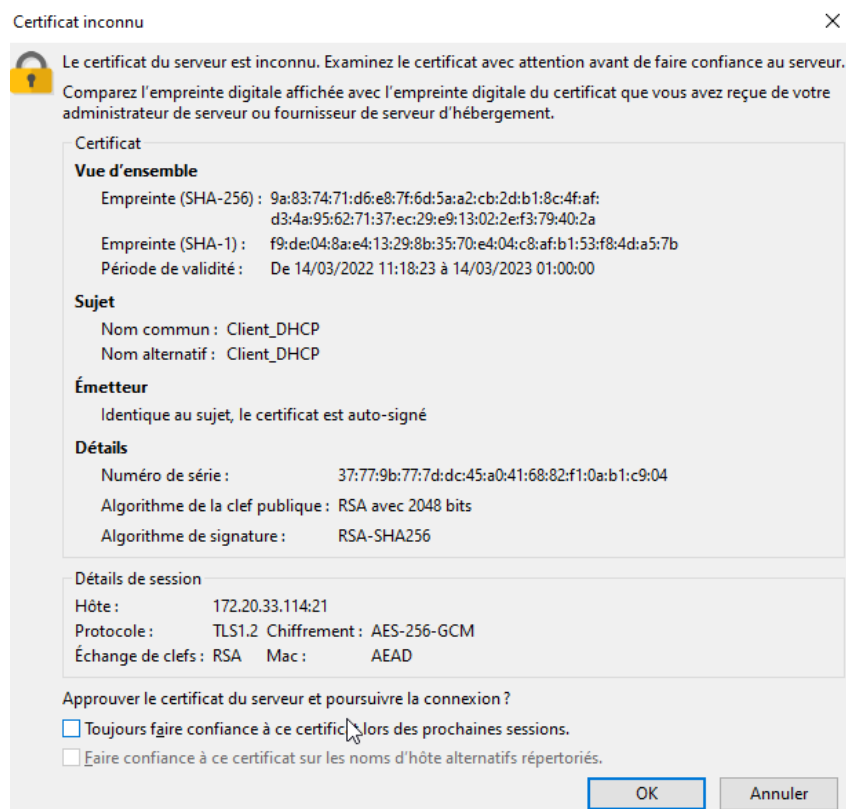
- ☒ Répertoire des noms d'utilisateurs (désactiver les répertoires virtuels globaux)
- ☐ Répertoire physique des noms d'utilisateurs (activer les répertoires virtuels globaux)
- ☐ Répertoire de base FTP configuré dans Active Directory



- ☐ Personnalisé

15. Les utilisateurs sont donc maintenant isolés, ils peuvent accéder uniquement à leur dossier.

16. Accepter le certificat :



17. L'utilisateur à maintenant accès uniquement à son dossier, il ne peut pas accéder à la racine :

Hôte : 172.20.33.114 Nom d'utilisateur : developer1 Mot de passe : \*\*\*\* Port : Connexion rapide

Statut : Connexion établie, attente du message d'accueil...  
 Statut : Initialisation de TLS...  
 Statut : Connexion TLS établie.  
 Statut : Connecté  
 Statut : Démarrage du téléchargement de /testfail.txt  
 Statut : Transfert de fichier réussi, 186 octets transférés en 1 seconde

Site local : C:\Users\flpetit\ Site distant : /

Nom de fichier	Taille de fi...	Type de fichier	Dernière modif...
cache		Dossier de fichiers	15/09/2021 09:04:03
dotnet		Dossier de fichiers	10/09/2021 09:04:21
VirtualBox		Dossier de fichiers	15/03/2022 10:21:16
vscode		Dossier de fichiers	10/09/2021 10:05:26
3D Objects		Dossier de fichiers	10/09/2021 08:59:09
AppData		Dossier de fichiers	10/09/2021 08:59:08
Application Data		Dossier de fichiers	07/03/2022 11:58:18
Cisco Packet Tracer 8.0.1		Dossier de fichiers	30/11/2021 11:52:40
Contacts		Dossier de fichiers	10/09/2021 08:59:10
Cookies		Dossier de fichiers	13/09/2021 08:18:41
Desktop		Dossier de fichiers	09/03/2022 08:14:35
Documents		Dossier de fichiers	07/03/2022 12:00:16
Downloads		Dossier de fichiers	14/03/2022 11:49:32
Favorites		Dossier de fichiers	10/09/2021 08:59:10
IntelGraphicsProfiles		Dossier de fichiers	14/03/2022 10:18:56
Links		Dossier de fichiers	10/09/2021 08:59:10
Local Settings		Dossier de fichiers	10/03/2022 10:57:39

13 fichiers et 32 dossiers. Taille totale : 9 008 554 octets

Nom de fichier	Taille de fi...	Type de fic...	Dernière modif...	Droits d'ac...	Propriétaire...
testfail.txt	186	Document ...	14/03/2022 11:...		

Sélection de 1 fichier. Taille totale : 186 octets

