Installation service FTP et Pare Feu sur Linux

Pare Feu : ufw et FTP : vsftpd

Présentation service FTP

Le service FTP va permettre de mettre, en accès réseau, un système de fichier.
Le service FTP utilise le protocole FTP à la couche Application et TCP à la couche Transport, ce protocole est donc fiable sur les transferts des données circulant sur le réseau.
Le protocole FTP utilise le port 21, pour ce connecter au service FTP il faudra donc utiliser le port 21.

Il existe aussi la version sécurisée de FTP ce nommant SFTP. SFTP est basée sous le protocole de communication sécurisé SSH utilisant le port 22.

Pour utiliser le service FTP, il est nécessaire d'avoir un client FTP et un serveur FTP, car ce système est basé sous la forme client-serveur.

Il existe différents clients FTP sous Linux comme FileZilla, CrossFTP, ou directement le service client FTP inclus dans le Terminal.

Pour mettre en place un service FTP, il existe aussi différents serveurs FTP, comme FileZilla Server ou VSFTPD, ici nous mettrons en place le service VSFTPD.

Le service VSFTPD propose plusieurs options, comme, l'autorisation de connexion au personnes anonymes, la connexion aux utilisateur locaux, la possibilité de mettre en place une liste d'utilisateur pouvant se connecter ou non. VSFTPD prend aussi en charge l'intégration SSL/TLS, ce qui signifie que la communication entre le client et le serveur sera entièrement cryptée. Il est aussi possible "d'emprisonner" les utilisateurs dans leur propre répertoire afin de verrouiller l'accès au système de fichier ascendant. D'autres options de

configuration sont possibles comme la limitation de la bande passante ou la prise en charge de IPv6.

Présentation Pare Feu UFW

Lors de la mise en place du service FTP, il est nécessaire d'utiliser un pare-feu pour assurer la protection contre les attaques pouvant venir de l'extérieur. Il faudra aussi ouvrir les ports de la machine afin que les clients puissent s'y connecter. Sans cette action, le pare-feu bloquera toute tentative de connexion par défaut.

Le pare-feu UFW, rassemble différentes options, ici nous n'utilisons que l'ouverture des ports nécessaire au service FTP.

Installation pare feu UFW

Pour installer le système de pare-feu il faudra actualiser la liste des paquets en entrant la commande `apt update`, puis la commande `apt install ufw` pour installer le service de pare-feu, (voir ci-dessous).

```
arnaud@raspberrypi:~ $ sudo apt update
```

```
arnaud@raspberrypi:~ $ sudo apt install ufw
```

Par défaut, nous allons configurer le parefeu comme interdisant toutes les entrées et autorisant toutes les sorties réseaux. Pour ce faire, entrez les commandes `ufw default deny incoming` et `ufw default allow outgoing`, (voir ci-dessous).

```
arnaud@raspberrypi:~ $ ufw default deny incoming && ufw default allow outgoing
```

Pour l'utilisation du service VSFTPD il sera nécessaire d'ouvrir le port 20 et 21, (protocole FTP), le port 22 et 990 (protocole SSH pour la communication chiffrée), et la plage de ports 40000 à 50000 (utilisé pour le FTP passif).
Il faudra donc entrer les commandes `ufw allow 20,21,22,990/tcp` et `ufw allow 40000:50000/tcp`

Enfin pour activer le pare-feu, veuillez entrer la commande `ufw enable`. Pour vérifier son statut et les ports ouverts entrez la commande `ufw status`, (voir ci-dessous).

```
arnaud@raspberrypi:~ $ sudo ufw enable && sudo ufw status
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
Status: active
```

```
arnaud@raspberrypi:~ $ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
20/tcp                     ALLOW       Anywhere
21/tcp                     ALLOW       Anywhere
20/tcp (v6)                ALLOW       Anywhere (v6)
21/tcp (v6)                ALLOW       Anywhere (v6)
```

Installation service VSFTPD

Le service VSFTPD, Very Secure FTP Daemon, permet la mise en place du service FTP, il joue le rôle de serveur. Ce programme est un programme qui sera exécuté en arrière plan d'où le nom “daemon”.

Téléchargement et Installation

Pour installer le service VSFTPD il faut tout d'abord mettre à jour la liste des paquets grâce à la commande `apt update`. Ensuite nous pouvons installer le service grâce à la commande `apt install vsftpd`, (voir ci-dessous).

Certaines distributions Linux requirent l'utilisation de la commande sudo, ce qui permet d'avoir le mode super utilisateur, si vous utilisez une autre distribution Linux il ne sera pas nécessaire de la mettre.

```
arnaud@raspberrypi:~ $ sudo apt install vsftpd
```

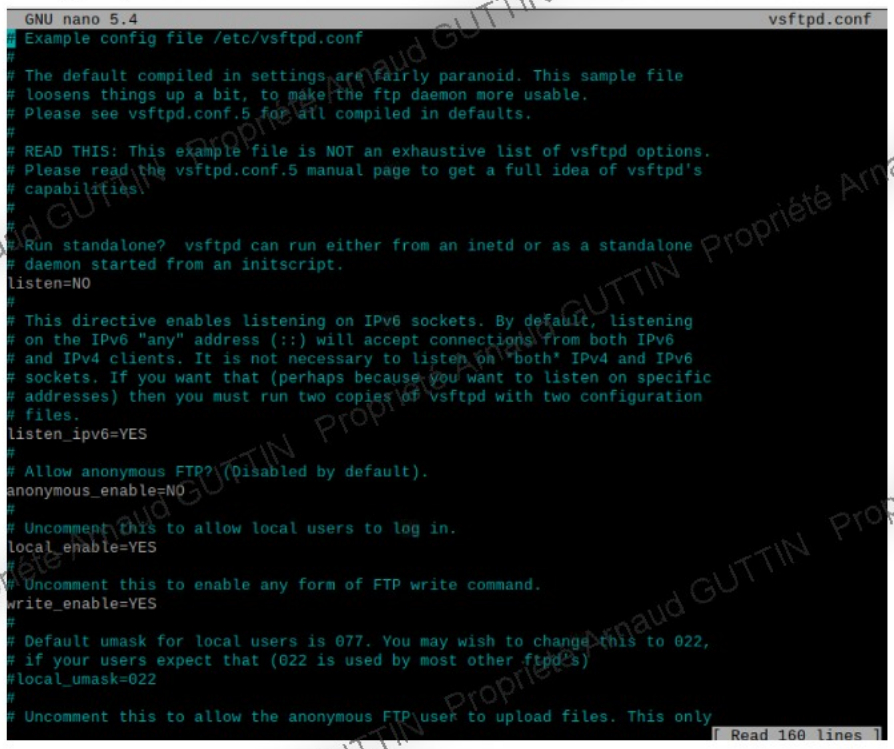
Une fois le service installé vous pouvez vérifier le bon fonctionnement du service en tapant la commande `systemctl status vsftpd`, vous devriez voir le service activé (voir ci dessous).
Si le service n'est pas démarré vous pouvez entrer la commande `systemctl enable vsftpd`.

```
arnaud@raspberrypi:~ $ sudo systemct
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/lib/systemd/sy
     Active: active (running) since
    Process: 2401 ExecStartPre=/bin/
   Main PID: 2402 (vsftpd)
      Tasks: 1 (limit: 779)
        CPU: 26ms
```

Configuration du service VSFTPD

Pour passer à la configuration du service, il faut entrer la commande `nano /etc/vsftpd.conf`, puis éditer le fichier de configuration, (voir ci-dessous).

Lors de votre première modification vous arriverez sur un fichier de configuration pré configuré, nous devrons donc le modifier en fonction de nos conditions d'utilisation.



Configuration pour connexion avec un utilisateur local

Nous allons modifier le fichier de configuration pour que le service FTP prenne en charge l'accès aux utilisateurs possédant un compte utilisateur local.

Si vous souhaitez créer un utilisateur local il faudra entrer la commande `adduser "nom-user"`, puis répondre aux différentes questions posées, (voir ci-dessous).

```
arnaud@arnaud:~ $ sudo adduser ftpuser
Adding user `ftpuser' ...
Adding new group `ftpuser' (1001) ...
Adding new user `ftpuser' (1001) with group `ftpuser' ...
Creating home directory `/home/ftpuser' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for ftpuser
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
```

Par défaut, le système Linux aura créé un répertoire utilisateur dans /home.
La configuration ci-dessous sera nécessaire à tous les utilisateurs locaux voulant avoir un accès FTP en lecture seul avec un répertoire en écriture.

Nous avons créé un répertoire “ftp” grâce à la commande `mkdir /home/ftpuser/ftp`. L’utilisateur sera redirigé lors de la connexion sur ce répertoire.
Nous allons modifier le propriétaire du répertoire ftp, par nobody:nogroup, cela permet d’apporter les privilèges minimum afin d’avoir une meilleur sécurité, (voir ci-dessous).

```
arnaud@arnaud:/etc $ sudo chown nobody:nogroup /home/ftpuser/ftp
```

Il sera aussi nécessaire de supprimer les autorisation d'écriture grâce à la commande `chmod a-w /home/ftpuser/ftp`.

Vous pouvez vérifier les autorisations en utilisant la commande `ls -la /home/ftpuser/ftp`

Il faut ensuite créer un répertoire autorisant l'écriture et la modification permettant à l'utilisateur de déposer ou supprimer des fichiers. On utilisera la commande `mkdir /home/ftpuser/ftp/files`. Enfin on attribuera la propriété à l'utilisateur concerné grâce à la commande `chown ftpuser:ftpuser /home/ftpuser/ftp/files`, (voir ci-dessous).

```
arnaud@arnaud:/etc $ sudo mkdir /home/ftpuser/ftp/files && sudo chown ftpuser:ftpuser /home/ftpuser/ftp/files
```

Il faut maintenant passer à la configuration du fichier vsftpd.conf grace a la commande `nano /etc/vsftpd.conf`

Veillez à vérifier que le fichier de configuration contient les deux lignes ci-dessous, cela permet d'interdire les connexions anonymes et d’autoriser les connexions locales.

```
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
```

Pour autoriser les utilisateurs à écrire et modifier dans leur répertoire, il faut ordonner au service FTP que l’utilisateur a le droit de faire des requêtes de modification du répertoire, pour ce faire, il faut décommenter la ligne ci-dessous.

```
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
```

Pour une meilleure sécurité, il est nécessaire d'interdire aux utilisateurs l'accès au système de fichiers en dehors de leur arborescence, il seront donc “emprisonnés” dans leur répertoire. Il faudra décommenter la ligne ci-dessous.

```
# You may restrict local users to their home directories.  See the FAQ for
# the possible risks in this before using chroot_local_user or
# chroot_list_enable below.
chroot_local_user=YES
```

Si vous souhaitez une meilleure convivialité ou transmettre un message lors de l'ouverture d'une session FTP, vous avez la possibilité d'ajouter une bannière, il faudra décommenter la ligne ci-dessous et indiquer le message que vous souhaitez.

```
# You may fully customise the login banner string:
ftpd_banner=Bienvenue sur le serveur FTP de Arnaud.
```

Veuillez ajouter les deux lignes suivantes, cela permet de définir les ports à utiliser pour le mode FTP passif. Attention, si vous utilisez une plage de ports différents il faudra effectuer les modifications sur le pare-feu.

```
# Customization
pasv_min_port=40000
pasv_max_port=50000
```

Enfin ajoutez les deux lignes suivantes, cela va indiquer au serveur dans quel répertoire seront redirigés les utilisateurs lors de l'ouverture d'une session FTP.

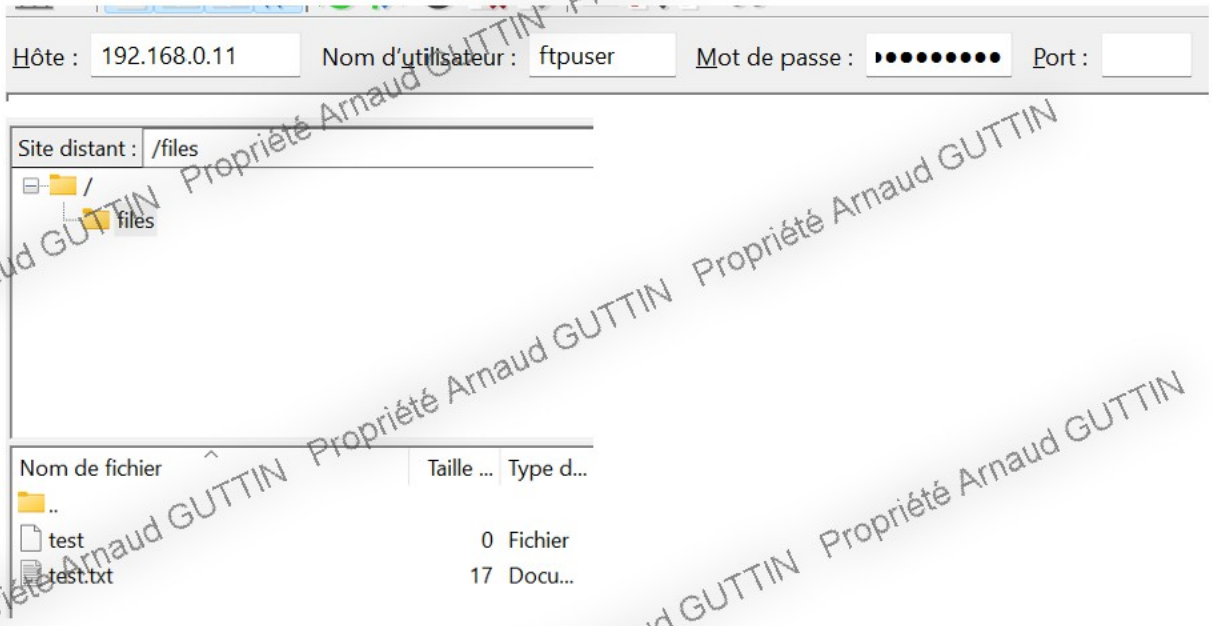
```
user_sub_token=$USER
local_root=/home/$USER/ftp
```

Une fois les modifications terminées, il faudra enregistrer le fichier vsftpd.conf en faisant les touches Ctrl + X puis le bouton Y. Enfin il faudra redémarrer le service pour qu'il prenne en compte les modifications apportés grâce à la commande, `systemctl restart vsftpd`.

Vous pouvez ensuite vérifier que la configuration est bonne grâce à la commande systemctl status vsftpd. En cas d'erreur de rédaction sur le fichier vsftpd.conf il sera indiqué le message ci-dessous.

```
arnaud@arnaud:~ $ sudo systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/lib/systemd/system/vsftpd.service
     Active: failed (Result: exit-code) since Wed 2023-
    Process: 1539 ExecStartPre=/bin/mkdir -p /var/run/v
    Process: 1540 ExecStart=/usr/sbin/vsftpd /etc/vsftp
   Main PID: 1540 (code=exited, status=2)
        CPU: 29ms
```

Une fois la bonne configuration réalisée, vous pouvez essayer de vous connecter grâce à un client FTP.



Nous pouvons voir que l'utilisateur a bien les accès lecture dans le répertoire ftp, qui pour celui-ci est le répertoire racine, et les droit d'écriture dans le répertoire files.

Configuration connexion anonyme

Le service VSFTPD propose aussi l'accès aux utilisateurs anonymes, c'est à dire qu'il n'est pas nécessaire d'entrer un nom d'utilisateur et un mot de passe pour se connecter au serveur FTP.

Nous allons créer un répertoire où les utilisateurs anonymes seront dirigés lors de l'ouverture d'une session FTP. Pour ce faire, entrez la commande `mkdir /home/nom-repertoire`, (voir ci-dessous).

Nous devons aussi modifier la propriété du répertoire a nobody:nogroup.

```
arnaud@arnaud:/etc $ sudo mkdir /home/anonymous
arnaud@arnaud:/etc $ sudo chown nobody:nogroup /home/anonymous
```

Pour que le serveur accepte les connexions anonymes il est nécessaire d'apporter des modifications au fichier vsftpd.conf, modifier le grâce a la commande nano /etc/vsftpd.conf.

Vous pouvez modifier la ligne ci-dessous et mettre le paramètre "YES" :

```
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=YES
```

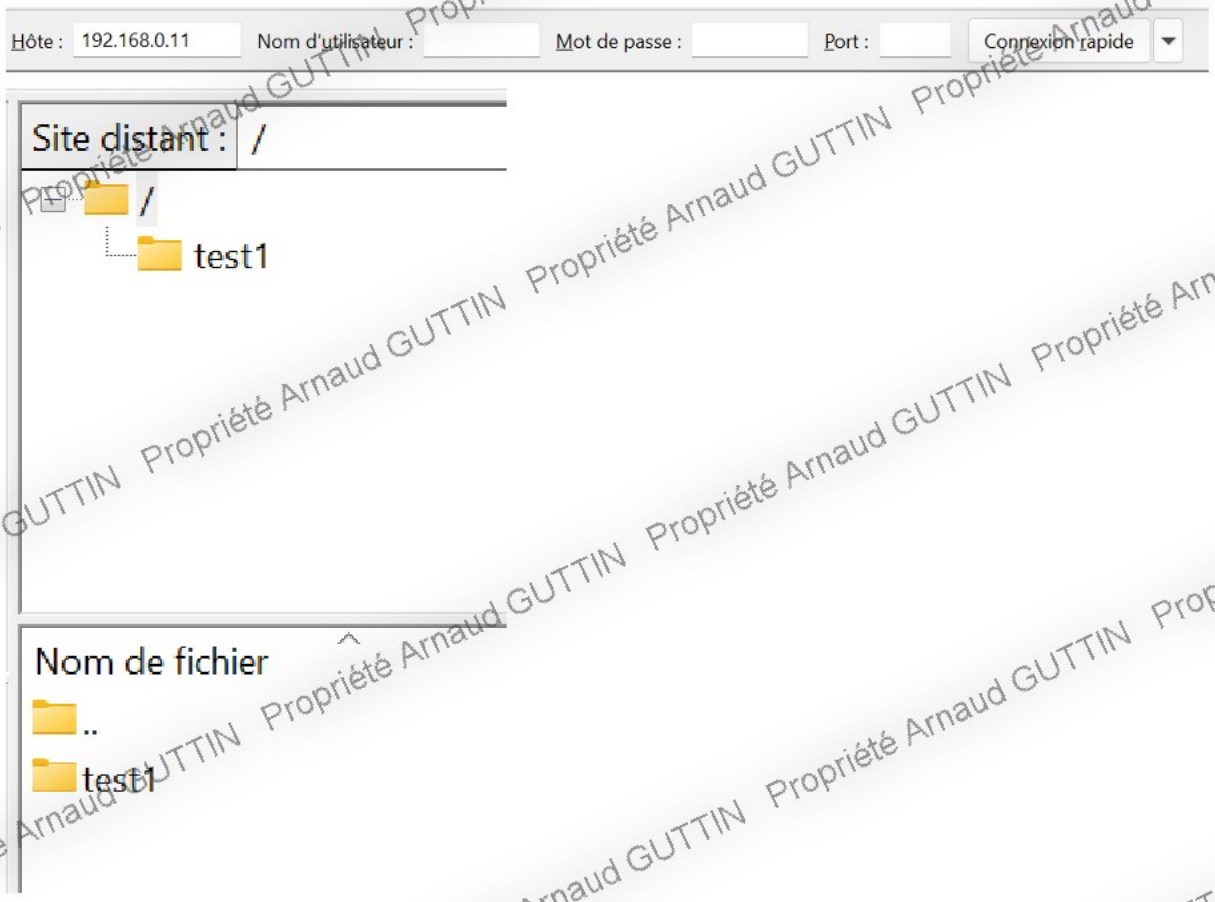
Si vous souhaitez aussi laisser l'accès aux utilisateurs locaux sur leur propre répertoire il faudra laisser la ligne avec YES, si vous mettez la ligne ci-dessous à NO, le serveur FTP, autorisera uniquement les connexions anonymes.

```
# Uncomment this to allow local users to log in.
local_enable=NO
#
```

Veuillez ajouter les trois lignes ci-dessous, cela permet d'indiquer au service où seront redirigés les utilisateurs lors de l'ouverture de session. De plus cela indique aussi qu'il n'a pas de mot de passe à entrer lors de la connexion.

```
anon_root=/home/anonymous/
no_anon_password=YES
hide_ids=YES
```

Après avoir redémarrer le service VSFTPD grâce à la commande `systemctl restart vsftpd` vous pouvez tester la connexion en tant que utilisateur anonyme.



Configuration du service FTP en SFTP

Maintenant que le service FTP fonctionne, il est préférable d'avoir une connexion sécurisée. Le protocole FTP fait circuler les données en clair sur le réseau, si un attaquant écoute le réseau il pourra récupérer la totalité des fichiers transmis. Pour ce faire, on utilisera la version sécurisée de FTP, SFTP.

Pour le mettre en place nous utiliserons le service OpenSSL.

Afin de générer les certificats pour une durée de 1 an, entrez la commande `openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem`

Ensuite, il faudra répondre aux différentes questions posées.

```
arnaud@arnaud:/etc $ sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/vsftpd.pem -out /etc/ssl/private/vsftpd.pem
Generating a RSA private key
.....+++++
.....+++++
writing new private key to '/etc/ssl/private/vsftpd.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:fr
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
```

Veuillez modifier le fichier de configuration vsftpd.conf (nano /etc/vsftpd.conf) et commenter les deux lignes ci-dessous.

```
#rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
#rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
```

Il faudra les remplacer par les deux lignes:

- rsa_cert_file=/etc/ssl/private/vsftpd.pem
- rsa_private_key_file=/etc/ssl/private/vsftpd.pem

Ces deux lignes permettent d'appeler les clés de chiffrement et le certificat.
Enfin modifier la ligne ssl_enable à "YES" pour forcer l'utilisation du service crypté (SSL), (voir ci-dessous).

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

Vous pouvez aussi ajouter les trois lignes ci-dessous. Cela permettra d'autoriser la connexion sécurisée aux utilisateurs anonymes et de forcer la connexion et le transfert des fichiers de façon sécurisée.

```
allow_anon_ssl=YES
force_local_data_ssl=YES
force_local_logins_ssl=YES
```

Il faudra enfin redémarrer le service VSFTPD, (systemctl restart vsftpd).

Lors de la connexion avec un client FTP, il vous sera demandé d'autoriser la connexion chiffré, et de valider le certificat, une fois validé vous serez connecté au serveur FTP, avec le protocole SFTP, soit en arrière plan le protocole SSH.