FTP

File Transfert Protocol

FTP

- Le **File Transfer Protocol** (protocole de transfert de fichiers), ou **FTP**, est un protocole de communication destiné à l'échange informatique de fichiers sur un réseau TCP/IP.
- Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, d'administrer un site web, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur.
- La variante de FTP protégée par SSL s'appelle FTPS.

FTP (Client/serveur)

- FTP obéit à un modèle **client/serveur**, c'est-à-dire qu'une des deux parties, le ***client***, envoie des requêtes auxquelles réagit l'autre, appelé ***serveur***.
- En pratique, le serveur est un ordinateur sur lequel fonctionne un logiciel lui-même appelé ***serveur FTP***, qui rend publique une arborescence de fichiers similaire à un ***système de fichiers Unix***

FTP (Client)

- Pour accéder à un serveur FTP, on utilise un logiciel client FTP (possédant une interface graphique ou en ligne de commande)
  - **Client en ligne de commande**
    - ftp,Wget, Curl
  - **Client avec interface graphique**
    - CuteFTP, FileZilla et FTP Expert (windows)
    - Gftp, IE, Navigateur (souvent avec extension)
    - FireFTP extension pour Firefox

FTP (Protocole)

- Le protocole utilise deux types de connexions **TCP** :
  - Une connexion de ***contrôle*** initialisée par le client, vers le serveur (port **21** en général), pour transmettre les commandes de fichiers (transfert, suppression de fichiers, renommage, liste des fichiers…).
  - Une connexion de ***données*** initialisée par le client ou le serveur pour transférer les données requises (contenu des fichiers, liste de fichiers).

FTP (Protocole)

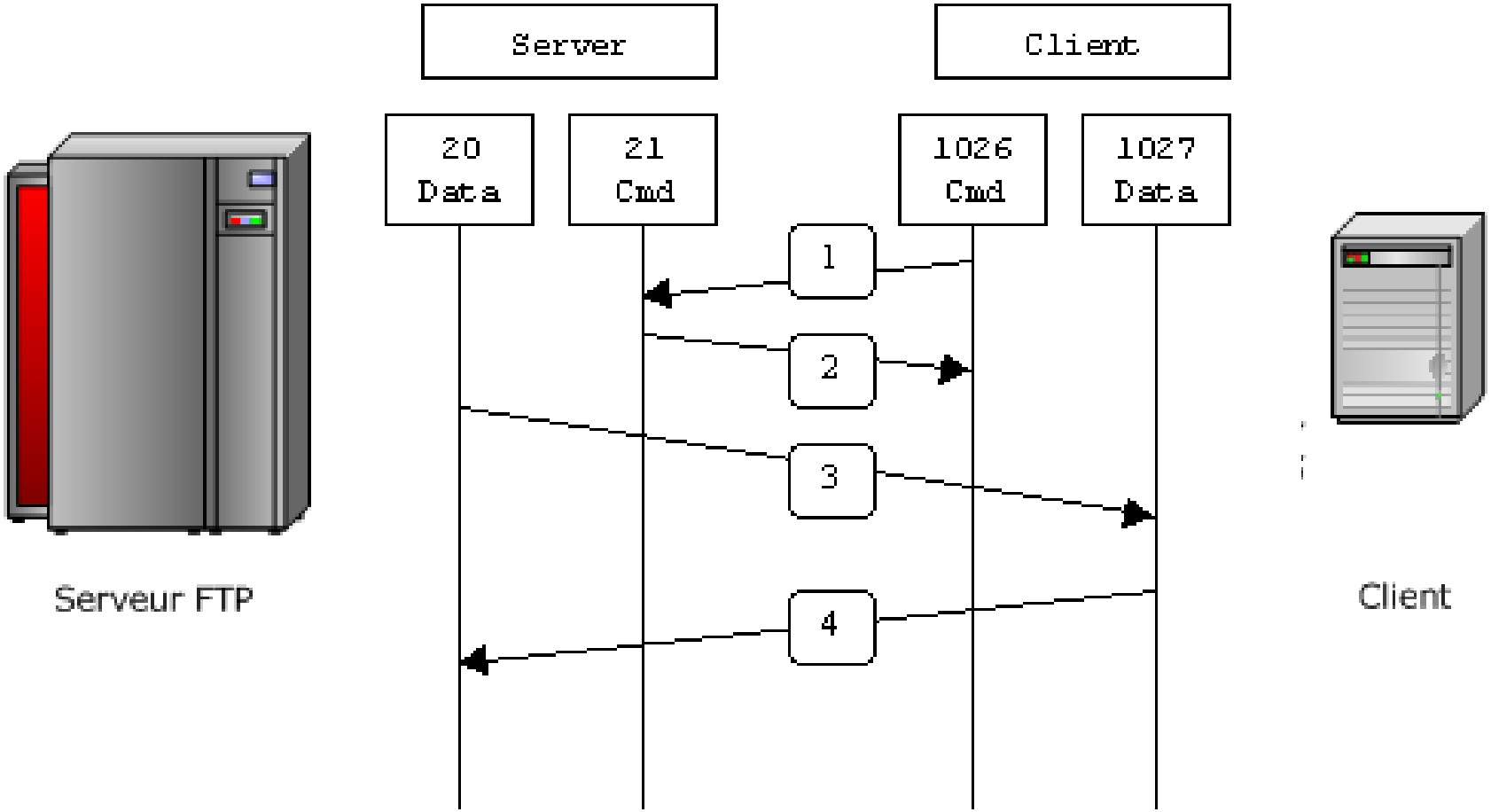
- Le protocole, qui appartient à la couche session du modèle OSI utilise une connexion TCP.
- Il peut s'utiliser de deux façons différentes :
  - **Mode actif**
  - **Mode passif**

FTP (Protocole)

- **Mode actif**
- c'est le client FTP qui détermine le port de connexion à utiliser pour permettre le transfert des données. Ainsi, pour que l'échange des données puisse se faire, le serveur FTP va initier la connexion de son port de données (port 20) vers le port spécifié par le client. C'est le numéro de port précédent le port. e contrôle. Donc pour un serveur qui écoute sur le port 10021, ce sera par défaut 10020.

FTP (Protocole)

Diagramme FTP actif

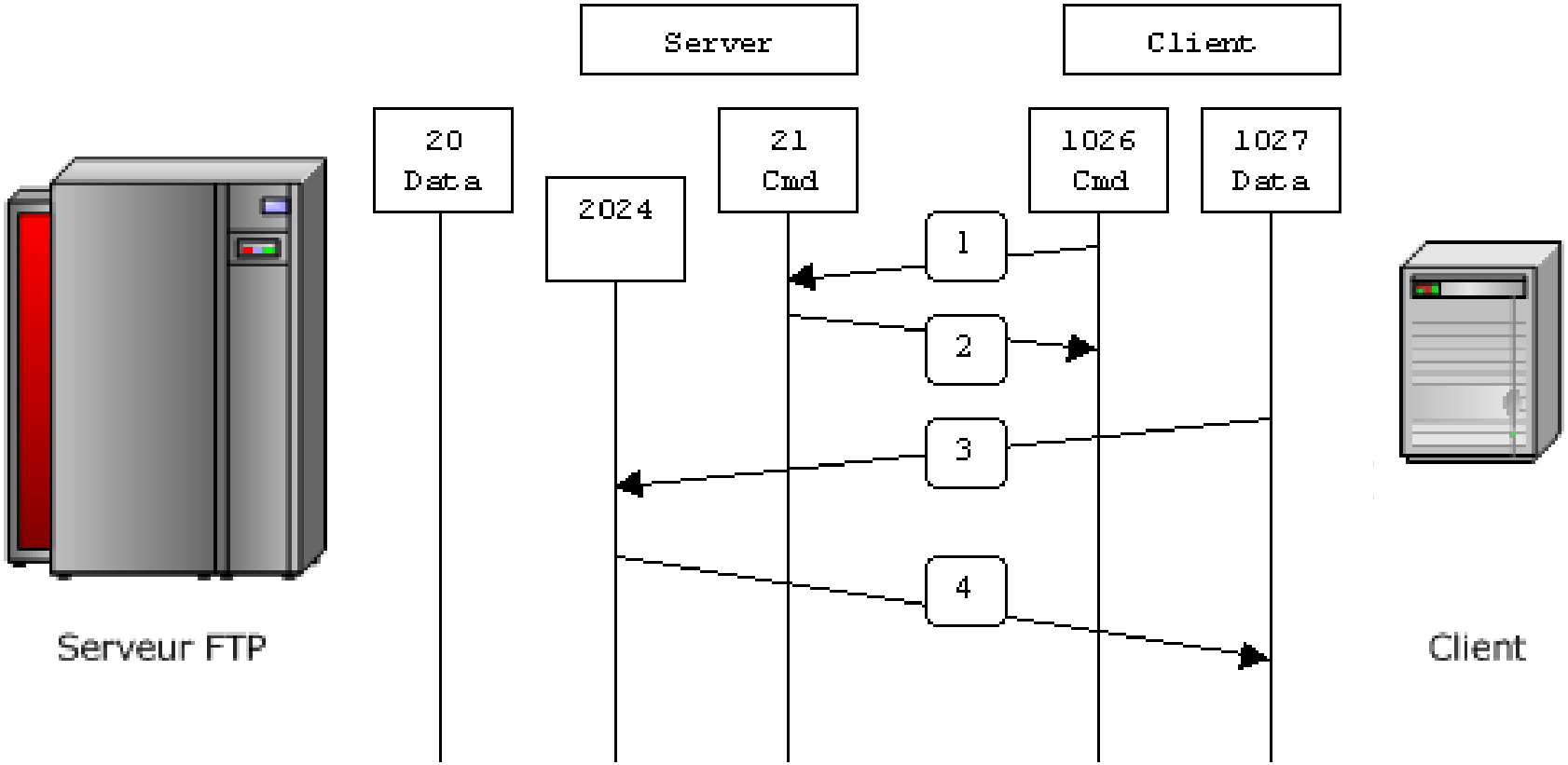


FTP (Protocole)

- **Mode passif**
- le serveur FTP détermine lui même le port de connexion à utiliser pour permettre le transfert des données (data connexion) et le communique au client. Dans le cas de l'existence d'un pare-feu devant le serveur FTP celui-ci devra être configuré pour autoriser la connexion de données. L'avantage de ce mode, est que le serveur FTP n'initie aucune connexion. Dans le cas des clients FTP sur un réseau local, ce mode est beaucoup plus sécurisé que le FTP en mode actif, car le pare-feu ne devra laisser passer que les flux sortant vers internet pour permettre aux clients d'échanger des données avec le serveur. C'est pour cette raison que ce mode est qualifié de *firewall-friendly*

FTP (Protocole)

Diagramme FTP passif



FTP (Serveur)

- VsFTPd est un serveur FTP conçu avec la problématique d'une sécurité maximale.
- Contrairement aux autres serveurs FTP (ProFTPd, PureFTPd, etc.), aucune faille de sécurité n'a jamais été décelée dans VsFTPd.
- Ce serveur est notamment utilisé à grande échelle par des entreprises

FTP (Serveur VsFTPd)

- La configuration *par défaut* de VsFTPd est très restrictive :
  - Seul le compte anonyme est autorisé à se connecter au serveur
  - En **lecture seule**
  - Les utilisateurs ne peuvent accéder à leur compte

FTP (Installation Serveur VsFTPd)

- yum install vsftpd (yum install vsftpd)
- find /etc -name "vsftpd.conf "

- **Configuration via le fichier : vsftpd.conf**

FTP (Configuration via le fichier : vsftpd.conf)

Options	Description	Commentaire
listen	Permet de définir si le démon est en standalone (YES) ou dirigé par (x)inetd (NO)	Partisan du (x)inetd, Partisan du standalone.. chacun son choix. Personnellement, je préfère le standalone...
anonymous_enable	Permet d'accepter les connexions anonymes	Tout dépend du but de votre serveur. Par défaut, je conseillerai de rejeter les connexions anonymes. Mais si votre serveur est au sein d'un réseau et que tout le monde doit y accéder, alors mettez YES, sinon NO

FTP (Configuration via le fichier : vsftpd.conf)

Options	Description	Commentaire
local_enable	Oblige les personnes à s'identifier avec un compte utilisateur	Dans tous les cas, je dis YES. Si une personne a un compte, le serveur ftp est présent pour elle. Sauf si vous voulez pas les laisser exporter ou importer des fichiers
write_enable	Permission d'écriture	Comme les deux précédents, tout dépend de vos besoins et de la fonction de votre service ftp

FTP (Configuration via le fichier : vsftpd.conf)

Options	Description	Commentaire
write_enable	Permission d'écriture	Comme les deux précédents, tout dépend de vos besoins et de la fonction de votre service ftp
xferlog_file	Ecriture d'un log des fichiers	Obligatoire selon moi pour tout administrateur digne de ce nom. Il faut savoir ce qu'il se passe surtout sur ces protocoles qui permettent les entrées/sorties de données.

FTP (Configuration via le fichier : vsftpd.conf)

Options	Description	Commentaire
ftpd_banner	Banniere d'affichage a la connexion FTP	Etrangement, je trouve très importante cette bannière qui peut sembler superflue. Pourquoi? Parce que vous pouvez l'utiliser pour communiquer : Dire sur quel serveur l'utilisateur se connecte (pratique quand on doit se connecter à divers serveurs), donner des informations sur les mises à jour, les maintenances ...etc. Indispensable si vous voulez envoyer des informations.
chroot_local_user	Permet de chrooter la connexion de l'utilisateur	Quand l'utilisateur se connecte en ftp, il arrive dans son répertoire home(défini dans /etc/passwd). Cette option active vous permet de l'obliger à rester dans ce répertoire (ou tout du moins de ne pas redescendre dans l'arborescence). Il reste dans son répertoire home. Très intéressant, si vous ne voulez pas qu'il se balade partout et télécharge des fichiers systèmes.

FTP (Configuration via le fichier : vsftpd.conf)

Options	Description	Commentaire
userlist_file	***Fichier des users***	***userlist_file=/etc/vsftpd/user_list # Si vous n'avez pas encore créé ce fichier, exécutez ces commandes : mkdir /etc/vsftpd puis # J'ajoute tous les utilisateurs du système dans ce fichier (grâce à cette commande : # less /etc/vcat /etc/passwd |cut -d: -f1 > /etc/vsftpd/user_list) et je commente les users AUTORISES***
userlist_enable	***=YES***	Quand l'utilisateur se connecte en ftp, il arrive dans son répertoire home(défini dans /etc/passwd). Cette option active vous permet de l'obliger à rester dans ce répertoire (ou tout du moins de ne pas redescendre dans l'arborescence). Il reste dans son répertoire home. Très intéressant, si vous ne voulez pas qu'il se balade partout et télécharge des fichiers systèmes.

Cas concret de configuration

pasv_enable=YES : On active le mode passif (pour autoriser les connexions extérieures), voir schéma ci-dessus.
pasv_promiscuous=NO : Par sécurité, vérifie que la machine qui a demandé la connexion au serveur (flèche rouge) est bien la même que celle qui demande à recevoir les données (flèche verte).
pasv_min_port=40000, **pasv_max_port=40100** : Les plages de ports utilisables par le client (à remplacer sur le schéma TCP/1024-65534 (en bleu) par TCP/40000-401000 pour correspondre avec mon exemple). Vous pouvez modifier ces valeurs.
pasv_address=X.X.X.X : Là vous avez deux solutions, soit vous renseignez votre adresse IP (adresse IP publique), soit vous mettez le nom de domaine par lequel ce serveur FTP sera accessible.
pasv_addr_resolve=YES : Cette ligne est utile uniquement si vous avez mis un nom de domain ci-dessus

Cas concret de configuration

Si vous désirez faire un serveur pour que quelques amis viennent télécharger les vidéos de vacances, avec ces règles

- Utilisateurs déclarés
- Rien à protéger
- Ecriture interdite

```
listen=YES
anonymous_enable=NO
local_enable=YES
write_enable=NO
xferlog_file=YES
ftpd_banner=/etc/ma_banniere
chroot_local_user=NO
```

Cas concret de configuration

Vous êtes en entreprise :

- Chaque utilisateur doit se déclarer
- Compartimenter les utilisateurs pour éviter les allers-retours dans le système

listen=YES
anonymous_enable=NO
local_enable=YES
write_enable=YES
xferlog_file=YES
ftpd_banner=‘”Bienvenue au serveur de ….’
chroot_local_user=YES
//renforcer les règles de sécurité

Cas concret de configuration

Un autre cas pour terminer avec l'anonymous
Les règles sont les suivantes :

- Pas besoin de s'identifier
- Compartimenter les anonymes
- Pas de compartiment pour les utilisateurs identifiés.

```
listen=YES
anonymous_enable=NO
local_enable=YES
write_enable=NO
xferlog_file=YES
ftpd_banner=/etc/ma_banniere
chroot_local_user=YES
chroot_list_enable=YES
chroot_list_file=/etc/vsftpd.chroot_list
```

- **Dans le fichier vsftpd.chroot_list, vous devez mettre : "anonymous" afin de spécifier que les personnes connectées en anonyme seront chrootées.**
- **Si vous mettez chroot_local_user à YES, le fichier vsftpd.chroot_list contiendra la liste des personnes NON compartimentées!**

C'est fini ! Votre serveur ftp est installé.
Les options vues sont simples et efficaces.

Merci ☺