



FTP sécurisé

Le protocole FTP (File Transfer Protocol) est un protocole de transfert de fichier défini par la RFC 959. Ce type de serveur est très utile voire même indispensable pour qui possède une connexion, grâce à lui vous pourrez par exemple mettre vos pages HTML à jour (si vous avez un serveur Apache) ou tout simplement échanger des fichiers. Le serveur ftp que nous allons utiliser est vsftpd.

Sommaire

I.Fonctionnement.....	1
II.Configuration.....	2
a)Messages.....	2
b)Mode PORT.....	3
c)Lancement.....	3
d)Utilisateurs autorisés.....	3
e)« Mettre les utilisateurs en prison ».....	3
1Dans leur répertoire personnel.....	3
2Dans un répertoire différent pour chaque utilisateur.....	4
f)Le compte anonyme.....	4
1Son dossier de connexion, ses droits.....	5
2Sa bande passante.....	5
g)Mode Passif.....	5
III.Mise en place du pare-feu pour le serveur FTP.....	5
a)Connexions.....	5
b)Réponses aux connexions.....	5
c)Mode Actif/PORT.....	6
d)Mode Passif.....	6
Bibliographie.....	6

I. Fonctionnement

Le protocole FTP a besoin de deux canaux pour fonctionner :

- le canal de contrôle qui sert à envoyer les commandes comme le listing de dossier, le changement de dossier
- le canal de données qui sert à envoyer les données au client (y compris les listings de dossier).

Le protocole FTP fonctionne suivant deux modes :

- le mode passif : le client se connecte sur le port 21 du serveur pour le contrôle et sur un port > 1024 (que le serveur choisit) pour le transfert des données. Ce mode passe en général assez bien par les passerelles NAT car il ne nécessite pas



- le mode actif : le client se connecte depuis un port N sur le port 21 du serveur pour le contrôle et le serveur se connecte depuis son port 20 sur le port N+1 du client pour envoyer les données. Ce mode ne peut pas passer par un NAT car il nécessite une connexion entrante vers la machine client.



II. Configuration

Pour installer vsftpd :

```
[root]# yum install vsftpd
```

Le répertoire où se trouve les fichiers de configuration pour vsftpd est `/etc/vsftpd`.

a) Messages

Pour activer un message (fichier `.message` si présent) dans chaque dossier et le message de bienvenu de connexion, dans le fichier `/etc/vsftpd.conf` :

```
#active l'affichage des fichiers .message à l'arrivée dans un
répertoire
```

```
dirmessage_enable=YES
```

```
#message de bienvenu
```

```
ftpd_banner=Bienvenue sur notre FTP service. #message de bienvenue
```

b) Mode PORT

Pour autoriser le mode PORT, il faut mettre dans le fichier `/etc/vsftpd.conf` :

```
#mode PORT sur le port 20
```

```
connect_from_port_20=YES
```

c) Lancement

Pour lancer le service `[root]# service vsftpd start`

d) Utilisateurs autorisés

Pour mettre la liste des personnes autorisés à se connecter en ftp dans le fichier `/etc/vsftpd/vsftpd.user_list` (les autres ne pourront pas), dans le fichier `/etc/vsftpd.conf` :

```
#liste d'utilisateurs activée
```

```
userlist_enable=YES
```

```
#les utilisateurs dans la liste sont autorisés (NO), les autres non
```

```
userlist_deny=NO
```

```
#le fichier contenant la liste des utilisateurs
```

```
userlist_file=/etc/vsftpd/vsftpd.user_list
```

La liste se trouve dans le fichier `/etc/vsftpd/vsftpd.user_list` :

```
anonymous
```

```
ftp
```

```
utilisateur1
```

```
utilisateur2
```

```
...
```

```
utilisateurN
```

e) « Mettre les utilisateurs en prison »

1 Dans leur répertoire personnel

Pour que tous les utilisateurs autorisés à se connecter en ftp soient chrooté dans leur répertoire personnel (home directory), c'est à dire qu'ils voient ce dossier comme la racine, donc qu'il ne puissent pas en sortir, dans le fichier `/etc/vsftpd.conf` :

```
#chroot des users locaux dans leur dossier
chroot_local_user=YES

#si chroot_local_user=YES alors
# tous les utilisateurs seront chrootés
# dans leur home directory
# SAUF ceux de la liste vsftpd.chroot_list
#sinon si chroot_local_user=NO alors
# aucun utilisateur ne sera chrooté
# dans leur home directory
# SAUF ceux de la liste vsftpd.chroot_list

#le fichier de la liste des utilisateurs
chroot_list_file=/etc/vsftpd/vsftpd.chroot_list

#activer le fichier
chroot_list_enable=YES
```

2 Dans un répertoire différent pour chaque utilisateur

Soit un compte titi ayant pour répertoire de connexion `/home/titi`. Pour que lui uniquement soit chrooté dans le répertoire `/home`, dans le fichier `/etc/vsftpd.conf` :

```
#chroot des users locaux dans leur dossier
chroot_local_user=YES

#activer le ./ dans le fichier passwd
passwd_chroot_enable=YES

#l'emplacement de ./ dans le répertoire home d'un utilisateur
#indique dans quel dossier il sera chrooté.
#S'il n'y a pas de ./, il sera chrooté dans son home.
```

Dans le fichier `/etc/vsftpd/vsftpd.chroot_list` :

```
toto #si chroot_local_user=YES alors toto ne sera pas chrooté
```

Dans le fichier `/etc/passwd` remplacer `/home/titi` par `/home/./titi` pour indiquer à `vsftpd` que le chroot se fait dans `/home`

Cela signifie que l'utilisateur sera chrooté dans le dossier précédent le ./

f) Le compte anonyme

Le compte anonyme peut s'appeler ftp, anonymous et prendre comme mot de passe ftp, anonymous où l'email de l'utilisateur qui se connecte.

1 Son dossier de connexion, ses droits

Pour configurer un accès ftp anonyme sur le serveur ftp uniquement en lecture dans le répertoire /home/ftp, dans le fichier /etc/vsftpd.conf :

```
#anonyme activé
anonymous_enable=YES

#dans le dossier /home/ftp
anon_root=/home/ftp

#en lecture seule
anon_upload_enable=NO
```

2 Sa bande passante

Pour limiter la bande passante pour l'accès anonyme à 1M/s, dans le fichier /etc/vsftpd.conf :

```
anon_max_rate=1048576 #maxi 1Mo/s (traduit en octet)
```

g) Mode Passif

On peut limiter la plage des ports utilisés pour le mode passif. Par exemple, pour que les ports utilisés en passive soient situés entre 60000 et 65000, dans le fichier /etc/vsftpd.conf :

```
pasv_min_port=60000 #entre 60000
pasv_max_port=65000 #et 65000
```

III. Mise en place du pare-feu pour le serveur FTP

a) Connexions

Il est nécessaire d'autoriser les connexions entrantes sur le port 21 :

```
[root@server ~]# iptables -A INPUT -m state --state NEW -p tcp --
dport 21 -j ACCEPT
```

b) Réponses aux connexions

Il est nécessaire d'autoriser le trafic sortant du port 21 :

```
[root@server ~]# iptables -A OUTPUT -m state --state  
RELATED,ESTABLISHED -p tcp -s sport 21 -j ACCEPT
```

c) Mode Actif/PORT

Il est nécessaire d'autoriser les connexions sortantes du port 20 et le trafic entrant sur le port 20 :

```
# mode PORT de ftp  
iptables -A OUTPUT -m state --state NEW -p tcp --sport 20 -j  
ACCEPT
```

d) Mode Passif

Il est nécessaire d'autoriser les connexions entrantes sur la plage de port définie pour le mode passif :

```
# mode PASSIF (entre le port 60000 et 65000) de ftp  
iptables -A INPUT -p tcp --dport 60000:65000 -j ACCEPT
```

En théorie, l'utilisation du module `state` et de l'état `RELATED` permet d'autoriser les connexions passives en rapport avec les connexions sur le port 21, mais je n'ai pas réussi à le faire réellement fonctionner. Cela devrait fonctionner (*à la fois pour le mode passif côté serveur et pour le mode port côté client*) :

```
iptables -A INPUT -p tcp -m state --state RELATED -j ACCEPT
```

Bibliographie

Page de man de vsftpd

[vsftpd - Secure, fast FTP server for UNIX-like systems](#)