Tutoriel : Installation et Sécurisation d'un Serveur FTP / FTPS

SOMMAIRE :

1. Introduction

Ce tutoriel explique comment installer un serveur FTP basique et comment le convertir en FTPS pour plus de sécurité.

2. Mettre à jour le système

Pour mettre jour la liste des paquets disponibles et installe les dernières versions des paquets déjà installés :

apt update

apt upgrade –y

3. Configurer une adresse IP statique

Ouvre le fichier de configuration des interfaces réseau pour édition :

nano /etc/network/interfaces

3.1 ma configuration :

```
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo eth0

iface lo inet loopback

# The primary network interface
#allow-hotplug eth0
#iface eth0 inet dhcp

iface eth0 inet static
address 192.168.102.11 /24
gateway 192.168.102.1
dns-nameservers 172.30.0.5
```

3.2 Redémarre les services réseau pour appliquer la nouvelle configuration :

systemctl restart networking

4. Installation d'un Serveur FTP

4.1 Installation de vsftpd

Exécutez la commande suivante pour installer vsftpd sur Debian :

apt-get install vsftpd

```
root@srv-FTP:~# apt-get install vsftpd
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les NOUVEAUX paquets suivants seront installés :
  vsftpd
0 mis à jour, 1 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 142 ko dans les archives.
Après cette opération, 351 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://deb.debian.org/debian bookworm/main amd64 vsftpd amd64 3.0.3-13+b2 [142 kB]
142 ko réceptionnés en 0s (4 318 ko/s)
Préconfiguration des paquets...
Sélection du paquet vsftpd précédemment désélectionné.
(Lecture de la base de données... 38148 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../vsftpd_3.0.3-13+b2_amd64.deb ...
Dépaquetage de vsftpd (3.0.3-13+b2) ...
Paramétrage de vsftpd (3.0.3-13+b2) ...
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /lib/systemd/system/vsftpd.service.
Traitement des actions différées (« triggers ») pour man-db (2.11.2-2) ...
```

4.2 Verifier la version de vsftpd :

vsftpd -version

```
root@srv-FTP:~# vsftpd -version
vsftpd: version 3.0.3
```

4.3 Lancer le service FTP :

systemctl start vsftpd

```
root@srv-FTP:~# systemctl start vsftpd
```

4.4 Lancer le service FTP à chaque démarrage du serveur:

systemctl enable vsftpd

```
root@srv-FTP:~# systemctl enable vsftpd
Synchronizing state of vsftpd.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable vsftpd
```

4.5 Vérifie l'état du service FTP :

systemctl status vsftpd

```
root@srv-FTP:~# systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/lib/systemd/system/vsftpd.service; enabled; preset: enabled)
     Active: active (running) since Sat 2025-03-01 16:54:12 CET; 8min ago
   Main PID: 703 (vsftpd)
      Tasks: 1 (limit: 1029)
     Memory: 1.2M
        CPU: 3ms
     CGroup: /system.slice/vsftpd.service
             └─703 /usr/sbin/vsftpd /etc/vsftpd.conf

mars 01 16:54:12 srv-FTP systemd[1]: Starting vsftpd.service - vsftpd FTP server...
mars 01 16:54:12 srv-FTP systemd[1]: Started vsftpd.service - vsftpd FTP server.
```

4.6 Configuration de vsftpd

Ouvrez le fichier de configuration :

nano /etc/vsftpd.conf

```
#Désactiver l'accès anonyme (IMPORTANT pour la sécurité)
anonymous_enable=NO

#Autoriser uniquement les utilisateurs locaux
local_enable=YES
write_enable=YES

#Sécuriser les permissions
chroot_local_user=YES
allow_writeable_chroot=YES

#Activer le mode passif (utile pour les connexions derrière un NAT)
pasv_enable=YES
pasv_min_port=40000
pasv_max_port=50000

#Limiter le nombre de connexions pour éviter la surcharge
max_clients=10
max_per_ip=2
```

Redémarre vsftpd pour appliquer les changements :

systemctl restart vsftpd

4.7 Configuration du Pare-feu (UFW)

Installer UFW:

apt install ufw

```
root@srv-FTP:~# apt install ufw
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  iptables libip6tc2 libnetfilter-conntrack3 libnfnetlink0
Paquets suggérés :
  firewalld rsyslog
Les NOUVEAUX paquets suivants seront installés :
  iptables libip6tc2 libnetfilter-conntrack3 libnfnetlink0 ufw
0 mis à jour, 5 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 435 ko/603 ko dans les archives.
Après cette opération, 3 606 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] o
Réception de :1 http://deb.debian.org/debian bookworm/main amd64 libip6tc2 amd64 1.8.9-2 [19,4 kB]
Réception de :2 http://deb.debian.org/debian bookworm/main amd64 libnfnetlink0 amd64 1.0.2-2 [15,1 kB]
Réception de :3 http://deb.debian.org/debian bookworm/main amd64 libnetfilter-conntrack3 amd64 1.0.9-3 [40,7 kB]
Réception de :4 http://deb.debian.org/debian bookworm/main amd64 iptables amd64 1.8.9-2 [360 kB]
435 ko réceptionnés en 0s (11,6 Mo/s)
Préconfiguration des paquets...
Sélection du paquet libip6tc2:amd64 précédemment désélectionné.
(Lecture de la base de données... 38207 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../libip6tc2_1.8.9-2_amd64.deb ...
Dépaquetage de libip6tc2:amd64 (1.8.9-2) ...
Sélection du paquet libnfnetlink0:amd64 précédemment désélectionné.
Préparation du dépaquetage de .../libnfnetlink0_1.0.2-2_amd64.deb ...
Dépaquetage de libnfnetlink0:amd64 (1.0.2-2) ...
Sélection du paquet libnetfilter-conntrack3:amd64 précédemment désélectionné.
Préparation du dépaquetage de .../libnetfilter-conntrack3_1.0.9-3_amd64.deb ...
Dépaquetage de libnetfilter-conntrack3:amd64 (1.0.9-3) ...
Sélection du paquet iptables précédemment désélectionné.
Préparation du dépaquetage de .../iptables_1.8.9-2_amd64.deb ...
Dépaquetage de iptables (1.8.9-2) ...
Sélection du paquet ufw précédemment désélectionné.
Préparation du dépaquetage de .../archives/ufw_0.36.2-1_all.deb ...
Dépaquetage de ufw (0.36.2-1) ...
Paramétrage de libip6tc2:amd64 (1.8.9-2) ...
Paramétrage de libnfnetlink0:amd64 (1.0.2-2) ...
Paramétrage de libnetfilter-conntrack3:amd64 (1.0.9-3) ...
Paramétrage de iptables (1.8.9-2) ...
update-alternatives: utilisation de « /usr/sbin/iptables-legacy » pour fournir « /usr/sbin/iptables » (iptables) en mode automatique
update-alternatives: utilisation de « /usr/sbin/ip6tables-legacy » pour fournir « /usr/sbin/ip6tables » (ip6tables) en mode automatique
update-alternatives: utilisation de « /usr/sbin/iptables-nft » pour fournir « /usr/sbin/iptables » (iptables) en mode automatique
```

4.8 Ouvrez les ports nécessaires :

ufw allow 21/tcp (port du FTP/FTPS)

ufw allow 22/tcp (port du SSH)
ufw allow 40000:50000/tcp (mode passif du FTP/FTPS)

```
root@srv-FTP:~# ufw allow 21/tcp
Rules updated
Rules updated (v6)
root@srv-FTP:~# ufw allow 40000:50000/tcp
Rules updated
Rules updated (v6)
root@srv-FTP:~#
```

4.9 Active et Vérifie que UFW est bien actif :

ufw enable

```
root@srv-FTP:~# ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
```

ufw status

```
root@srv-FTP:~# ufw status
Status: active
```

4.10 Vérification du Fonctionnement

Testez la connexion avec un client FTP comme FileZilla.

Voir les transactions FTP en temps reel :

tail -f /var/log/vsftpd.log

Ton serveur FTP est prêt

Attention : Ce serveur FTP fonctionne, mais il n'est pas sécurisé !
Tout transite en clair, donc si quelqu'un intercepte les données, il verra tout (y compris les mots de passe).
Si tu veux un serveur sécurisé avec FTPS (chiffrement TLS/SSL), passe à la partie suivante.

5. Passage de FTP à FTPS (FTP Sécurisé avec TLS/SSL)

5.1 Génération d'un Certificat SSL/TLS

Créez un certificat auto-signé :

openssl req -x509 -nodes -days 365 -newkey rsa:2048 \
-keyout /etc/ssl/private/vsftpd.pem \
-out /etc/ssl/private/vsftpd.pem

exemple :
Country Name → Code du pays sur 2 lettres (France = FR).

State or Province Name → Région (ex : Île-de-France).

Locality Name → Ville (Paris).

Organization Name → Nom de l'organisation (LPRS).

Organizational Unit Name → Département (ex : IT, Informatique ou autre).

Common Name → Nom du serveur ou domaine (L'ip du serveur FTP "172.29.68.96").

```
root@srv-FTP:~# openssl req -x509 -nodes -days 365 -newkey rsa:2048 \
-keyout /etc/ssl/private/vsftpd.pem \
-out /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]:Ile-de-France
Locality Name (eg, city) []:Paris
Organization Name (eg, company) [Internet Widgits Pty Ltd]:LPRS
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:172.29.68.96
```

5.2 Configuration de vsftpd pour FTPS

Modifiez /etc/vsftpd.conf et ajoutez :

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

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

ssl_enable=YES

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

6 Ajout d'une Protection avec fail2ban

🔥 Comment Fail2Ban bloque les attaques ?

Fail2Ban est un outil qui surveille les logs et **bloque automatiquement** les IP malveillantes après plusieurs tentatives de connexion échouées. Il est très efficace contre les attaques par **force brute** et certains types de scans.

📌 Explication des paramètres :

✔ **maxretry = 5**	Si une IP échoue **5 fois**, elle est bloquée.
✔ **bantime = 3600**	L'IP sera bloquée **pendant 1 heure**.
✔ **findtime = 600**	L'analyse se fait **sur 10 minutes**.

6.1 Installez fail2ban :

apt install fail2ban -y

```
root@srv-FTP:~# apt install fail2ban -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  python3-pyinotify python3-systemd whois
Paquets suggérés :
  mailx system-log-daemon monit sqlite3 python-pyinotify-doc
Les NOUVEAUX paquets suivants seront installés :
  fail2ban python3-pyinotify python3-systemd whois
0 mis à jour, 4 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 589 ko dans les archives.
Après cette opération, 2 901 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://deb.debian.org/debian bookworm/main amd64 fail2ban all 1.0.2-2 [451 kB]
Réception de :2 http://deb.debian.org/debian bookworm/main amd64 python3-pyinotify all 0.9.6-2 [27,4 kB]
Réception de :3 http://deb.debian.org/debian bookworm/main amd64 python3-systemd amd64 235-1+b2 [39,3 kB]
Réception de :4 http://deb.debian.org/debian bookworm/main amd64 whois amd64 5.5.17 [70,8 kB]
589 ko réceptionnés en 0s (12,0 Mo/s)
Sélection du paquet fail2ban précédemment désélectionné.
(Lecture de la base de données... 38533 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../fail2ban_1.0.2-2_all.deb ...
Dépaquetage de fail2ban (1.0.2-2) ...
Sélection du paquet python3-pyinotify précédemment désélectionné.
Préparation du dépaquetage de .../python3-pyinotify_0.9.6-2_all.deb ...
Dépaquetage de python3-pyinotify (0.9.6-2) ...
Sélection du paquet python3-systemd précédemment désélectionné.
Préparation du dépaquetage de .../python3-systemd_235-1+b2_amd64.deb ...
Dépaquetage de python3-systemd (235-1+b2) ...
Sélection du paquet whois précédemment désélectionné.
Préparation du dépaquetage de .../whois_5.5.17_amd64.deb ...
Dépaquetage de whois (5.5.17) ...
Paramétrage de whois (5.5.17) ...
Paramétrage de fail2ban (1.0.2-2) ...
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /lib/systemd/system/fail2ban.service.
Paramétrage de python3-pyinotify (0.9.6-2) ...
Paramétrage de python3-systemd (235-1+b2) ...
Traitement des actions différées (« triggers ») pour man-db (2.11.2-2) ...
```

6.2 Crée une règle pour protéger vsftpd

nano /etc/fail2ban/jail.local

6.3 Ajoute ces lignes :

[vsftpd]

enabled = true

port = ftp,ftps

filter = vsftpd

logpath = /var/log/vsftpd.log

maxretry = 5

bantime = 3600

```
[vsftpd]
enabled = true
port = ftp,ftps
filter = vsftpd
logpath = /var/log/vsftpd.log
maxretry = 5      # Nombre de tentatives avant le bannissement
bantime = 3600    # Temps de bannissement en secondes (1h)
findtime = 600    # Temps d'analyse des tentatives (10 min)
```

6.4 Redémarre fail2ban :

systemctl restart fail2ban

```
root@srv-FTP:~# systemctl restart fail2ban
```

6.5 Test de la Connexion FTPS

Connectez-vous avec FileZilla, WinSCP ou MobaXterm en utilisant FTPS Explicite sur le port 21.

7. Conclusion : FTP vs FTPS

FTP (Non Sécurisé)	**FTPS (Sécurisé avec TLS/SSL)**
Transmission en clair	Chiffrement des données
Vulnérable aux attaques	Protégé contre les interceptions
Risque de fuite d'identifiants	Connexion et transferts sécurisés

Si vous voulez un serveur fiable et sécurisé, utilisez FTPS !