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

SOMMAIRE :

[1. Introduction 2](#_Toc191759185)

[2. Mettre à jour le système 2](#_Toc191759186)

[3. Configurer une adresse IP statique 3](#_Toc191759187)

[3.1 ma configuration : 3](#_Toc191759188)

[3.2 Redémarre les services réseau pour appliquer la nouvelle configuration : 3](#_Toc191759189)

[4. Installation d'un Serveur FTP 3](#_Toc191759190)

[4.1 Installation de vsftpd 3](#_Toc191759191)

[4.2 Verifier la version de vsftpd : 4](#_Toc191759192)

[4.3 Lancer le service FTP : 4](#_Toc191759193)

[4.4 Lancer le service FTP à chaque démarrage du serveur: 4](#_Toc191759194)

[4.5 Vérifie l'état du service FTP : 4](#_Toc191759195)

[4.6 Configuration de vsftpd 5](#_Toc191759196)

[Redémarre vsftpd pour appliquer les changements : 5](#_Toc191759197)

[4.7 Configuration du Pare-feu (UFW) 6](#_Toc191759198)

[4.8 Ouvrez les ports nécessaires : 6](#_Toc191759199)

[4.9 Active et Vérifie que UFW est bien actif : 6](#_Toc191759200)

[4.10 Vérification du Fonctionnement 7](#_Toc191759201)

[Ton serveur FTP est prêt 7](#_Toc191759202)

[5. Passage de FTP à FTPS (FTP Sécurisé avec TLS/SSL) 8](#_Toc191759203)

[5.1 Génération d'un Certificat SSL/TLS 8](#_Toc191759204)

[5.2 Configuration de vsftpd pour FTPS 8](#_Toc191759205)

[6 Ajout d'une Protection avec fail2ban 9](#_Toc191759206)

[6.1 Installez fail2ban : 9](#_Toc191759207)

[6.2 Crée une règle pour protéger vsftpd 10](#_Toc191759208)

[6.3 Ajoute ces lignes : 10](#_Toc191759209)

[6.4 Redémarre fail2ban : 10](#_Toc191759210)

[6.5 Test de la Connexion FTPS 11](#_Toc191759211)

[7. Conclusion : FTP vs FTPS 11](#_Toc191759212)

## 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

Mon fichier sources list :

# deb cdrom:[Debian GNU/Linux 12.7.0 \_Bookworm\_ - Official amd64 DVD Binary-1 with firmware 20240831-10:40]/ bookworm contrib main non-free-firmware

deb http://deb.debian.org/debian/ bookworm main non-free-firmware

deb-src http://deb.debian.org/debian/ bookworm main non-free-firmware

deb http://security.debian.org/debian-security bookworm-security main non-free-firmware

deb-src http://security.debian.org/debian-security bookworm-security main non-free-firmware

# bookworm-updates, to get updates before a point release is made;

# see https://www.debian.org/doc/manuals/debian-reference/ch02.en.html#\_updates\_and\_backports

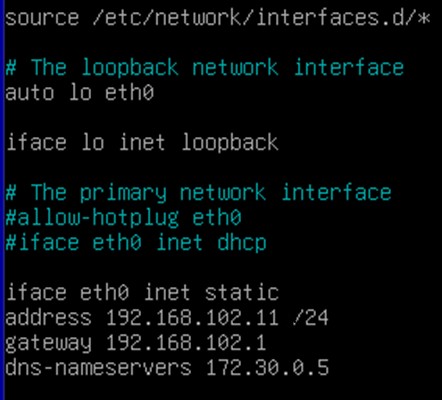
deb http://deb.debian.org/debian/ bookworm-updates main non-free-firmware

deb-src http://deb.debian.org/debian/ bookworm-updates main non-free-firmware

## 3. Configurer une adresse IP statique

Ouvre le fichier de configuration des interfaces réseau pour édition :

nano /etc/network/interfaces

3.1 ma configuration :  


### 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

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

### 4.2 Verifier la version de vsftpd :

vsftpd -version



### 4.3 Lancer le service FTP :

**systemctl start vsftpd**



### 4.4 Lancer le service FTP à chaque démarrage du serveur:

systemctl enable vsftpd

****

### 4.5 Vérifie l'état du service FTP :

**systemctl status vsftpd**

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

### 4.6 Configuration de vsftpd

Ouvrez le fichier de configuration :

nano /etc/vsftpd.conf

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Les changements à faire:  
décommenter :

write\_enable=YES

chroot\_local\_user=YES

Rajouter :

pasv\_enable=YES

pasv\_min\_port=40000

pasv\_max\_port=50000

max\_clients=10

max\_per\_ip=2

allow\_writeable\_chroot=YES

### Redémarre vsftpd pour appliquer les changements :

systemctl restart vsftpd

### 4.7 Configuration du Pare-feu (UFW)

Installer UFW:

apt install ufw

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

### 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)

Une image contenant texte, Police, capture d’écran

Le contenu généré par l’IA peut être incorrect.

### 4.9 Active et Vérifie que UFW est bien actif :

ufw enable



ufw status



### 4.10 Creer un user FTP

useradd -m ftpuser



passwd ftpuser

Une image contenant texte, Police, capture d’écran, ligne

Le contenu généré par l’IA peut être incorrect.

### 4.11 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.**

Une image contenant texte, Appareils électroniques, capture d’écran, affichage

Le contenu généré par l’IA peut être incorrect.

## 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”).

Une image contenant texte, capture d’écran

Le contenu généré par l’IA peut être incorrect.

### 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



## 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

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

### 6.2 Crée une règle pour protéger vsftpd

nano /etc/fail2ban/jail.local

**Ajoute ces lignes :**

[vsftpd]

enabled = true

port = ftp,ftps

filter = vsftpd

logpath = /var/log/vsftpd.log

maxretry = 5

bantime = 3600

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

### 6.4 Redémarre fail2ban :

systemctl restart fail2ban



### 6.5 Test de la Connexion FTPS

Faites un reboot et connectez-vous avec FileZilla, WinSCP ou MobaXterm en utilisant FTPS Explicite sur le port 21.

Une image contenant texte, Appareils électroniques, capture d’écran, affichage

Le contenu généré par l’IA peut être incorrect.

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Le contenu généré par l’IA peut être incorrect.

## Félicitations, vous avez réussi à faire un serveur FTPS avec un certificat privé.

## 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 !