08/01/2018

Léo Guilpain & Legris Thomas

TP serveur FTP

Table des matières

[Introduction 2](#_Toc502664431)

[Configuration de la Raspberry 2](#_Toc502664433)

[Mise en place du serveur FTP 3](#_Toc502664434)

[Mise en place du serveur SFTP 4](#_Toc502664435)

[Conclusion 5](#_Toc502664436)

# Introduction

L’objectif de ce TP est d’installer un serveur FTP sur une Raspberry afin d’échanger des fichiers avec un client. L’autre but est de sécuriser les messages envoyés via ce protocole. Nous réaliserons ce TP en local, sans faire de point d’accès wifi sur notre serveur.

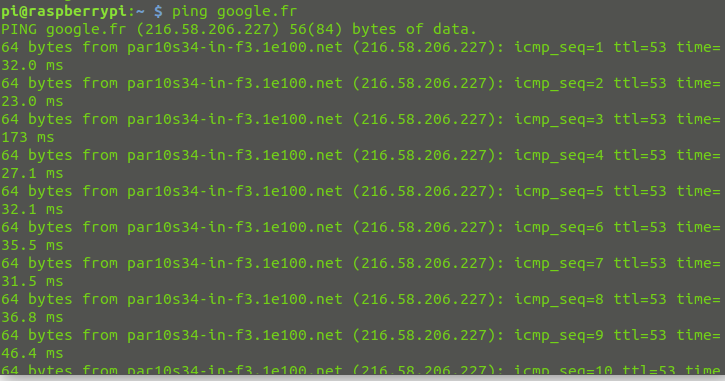
Voici le schéma fonctionnel de notre installation.

# 

# Configuration de la Raspberry

La 1ère étape est de donner une adresse IP à la Raspberry. Pour cela nous avons mis en place un serveur DHCP comme dans les séances précédentes. Cela va nous permettre d’attribuer une adresse IP automatiquement à toutes les machines se connectant sur notre réseau.

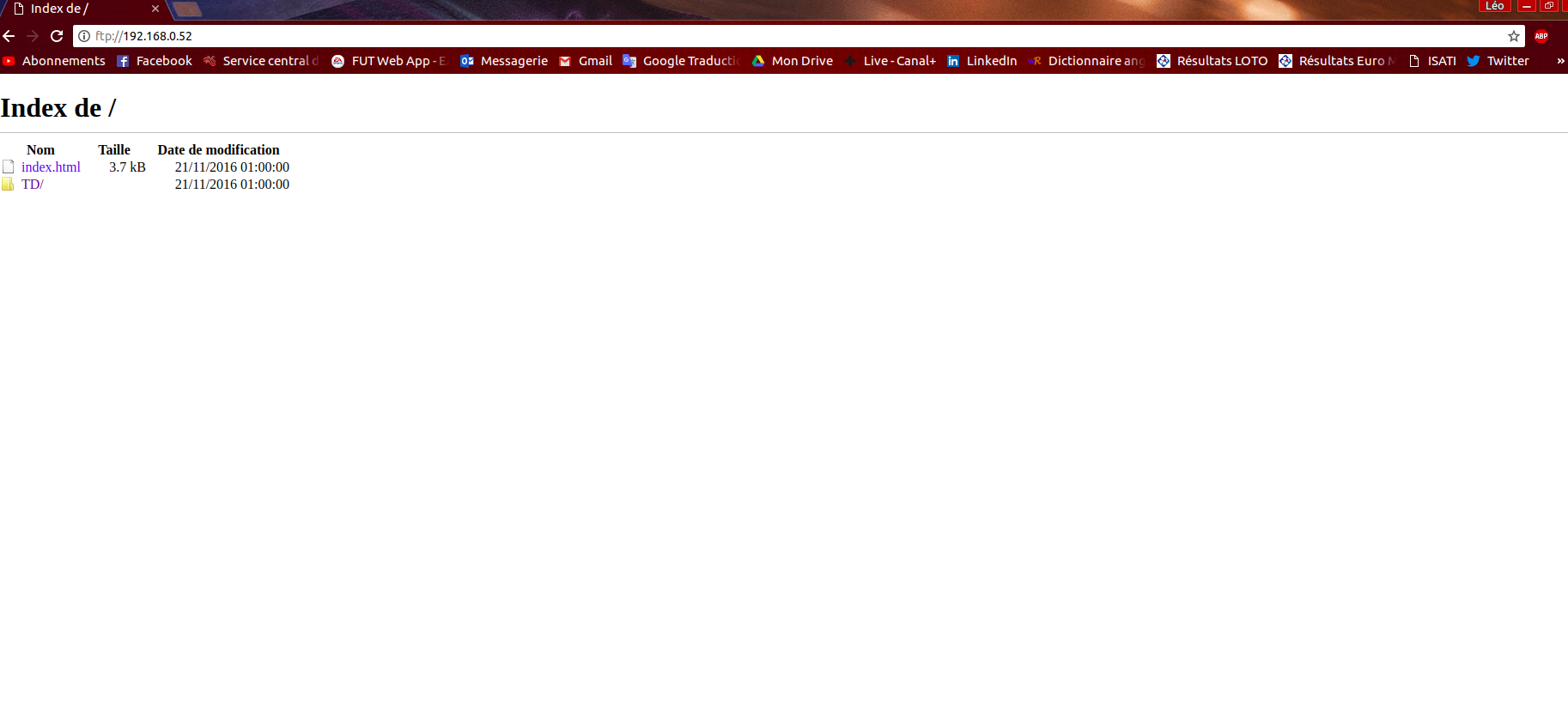
Nous avons ensuite configuré le NAT. Lorsque nous entrons dans le Shell de la Raspberry (SSH), nous avons accès à google.fr par exemple, ce qui signifie que le NAT a bien été configuré.



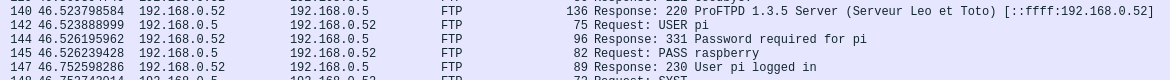
# Mise en place du serveur FTP

Nous avons installé et configuré « Proftpd » sur la Raspberry pi, c’est un serveur libre et relativement puissant. Le fichier de configuration s’ouvre avec la commande :

sudo nano /etc/proftpd/proftpd.conf

Nous sommes maintenant connectés au serveur placé sur la Raspberry :

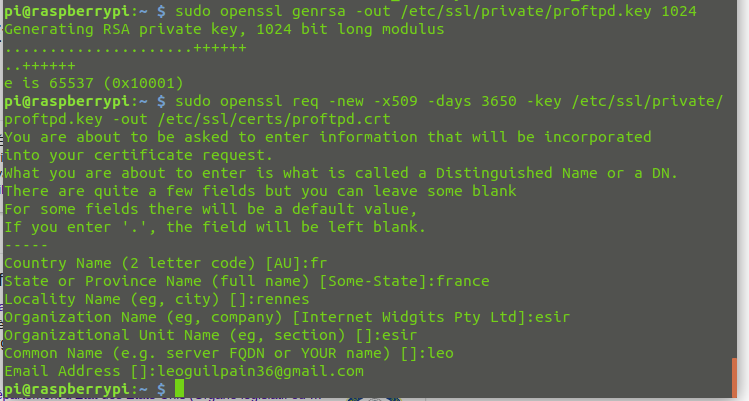
Les utilisateurs peuvent alors communiquer via la protocole FTP mais il n’y a pas de chiffrage, c’est-à-dire qu’une simple écoute nous permet de repérer les informations clés.

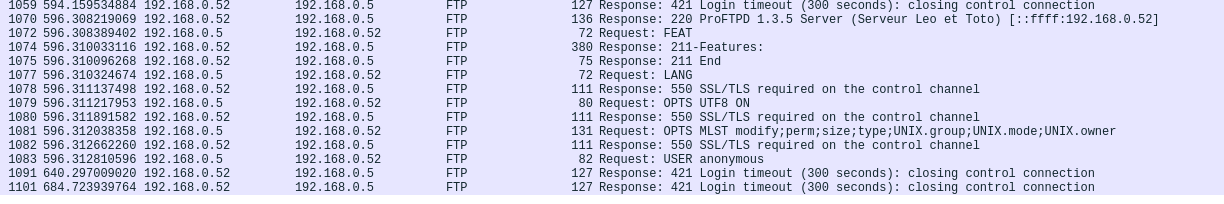


Avec l’outil Wireshark, nous avons accès aux noms d’utilisateurs (pi) et aux mots de passes (raspberry) qui sont échangés via le protocole. C’est pourquoi il est nécessaire de sécuriser le protocole.

# Mise en place du serveur SFTP

Pour remédier au problème de sécurité, nous utilisons le système de chiffrement RSA, en générant une clé publique et une clé privée, de façon à chiffrer et déchiffrer les messages envoyés. Ce chiffrement se fait grâce à la librairie Openssl comme on peut le voir ci-dessous.



Comme nous pouvons le constater, nous avons rentré nos informations pour la connexion, tout en générant des clés grâce à open SSL. Nos informations ne sont plus en claires comme nous pouvons le voir ci-dessous, la connexion au serveur est sécurisée. Les mots de passes et les noms d’utilisateurs ne sont plus en clairs.

# Conclusion

Ce TP nous a permis de réaliser du transfert de fichier de manière sécurisé entre un client et un serveur FTP. Il nous a également permis de configurer le NAT sur notre Raspberry pi.