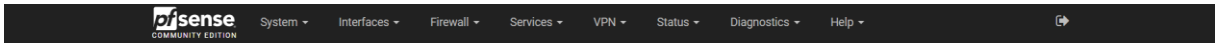
OpenVpn entre PFsense et RPI, pour serveur CUPS

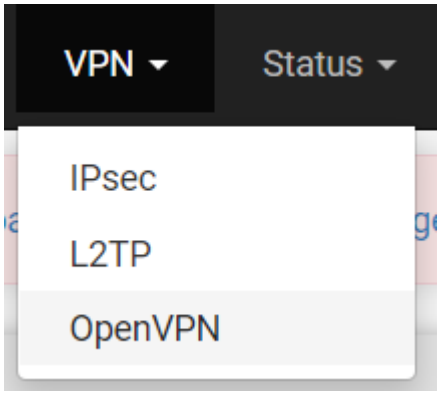
Le but est de créé un tunnel OpenVPN entre les VM client et le serveur d'impression se trouvant sur une Raspberry Pi située dans le réseau client.



I)Création du serveur et du client OpenVPN :

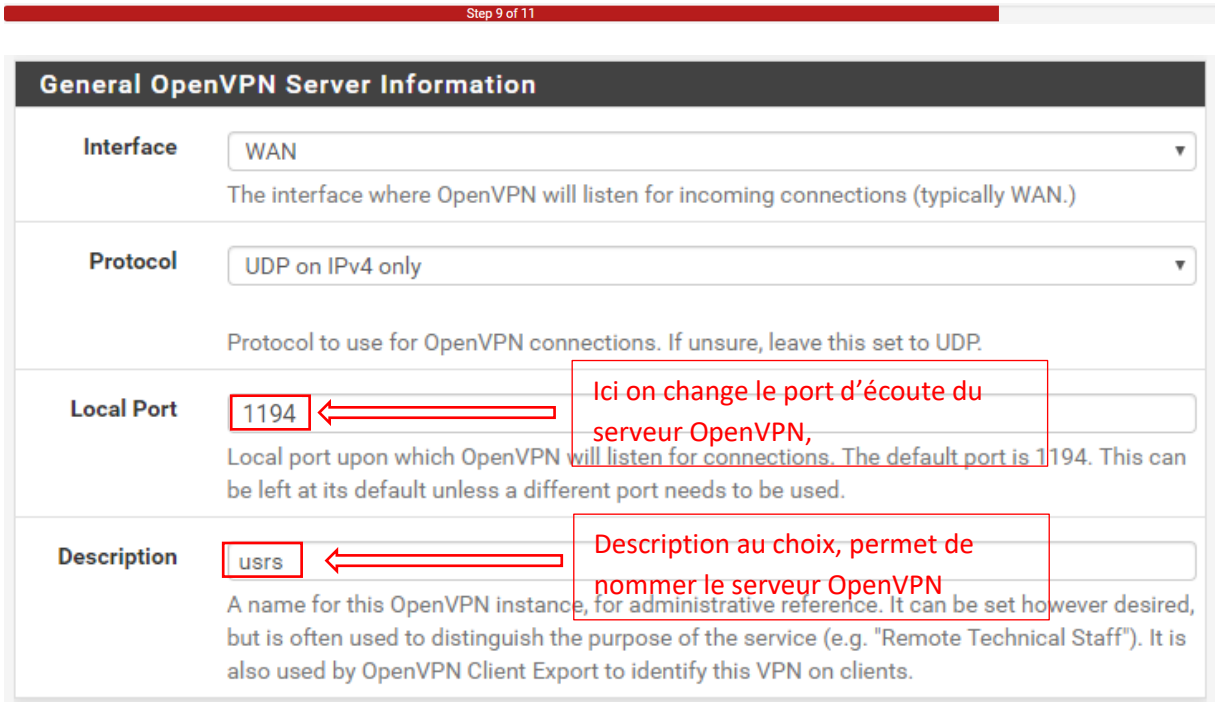
2)Serveur OpenVPN :

Pour créer un serveur OpenVPN il faut aller dans l'onglet VPN puis OpenVPN puis Wizard.

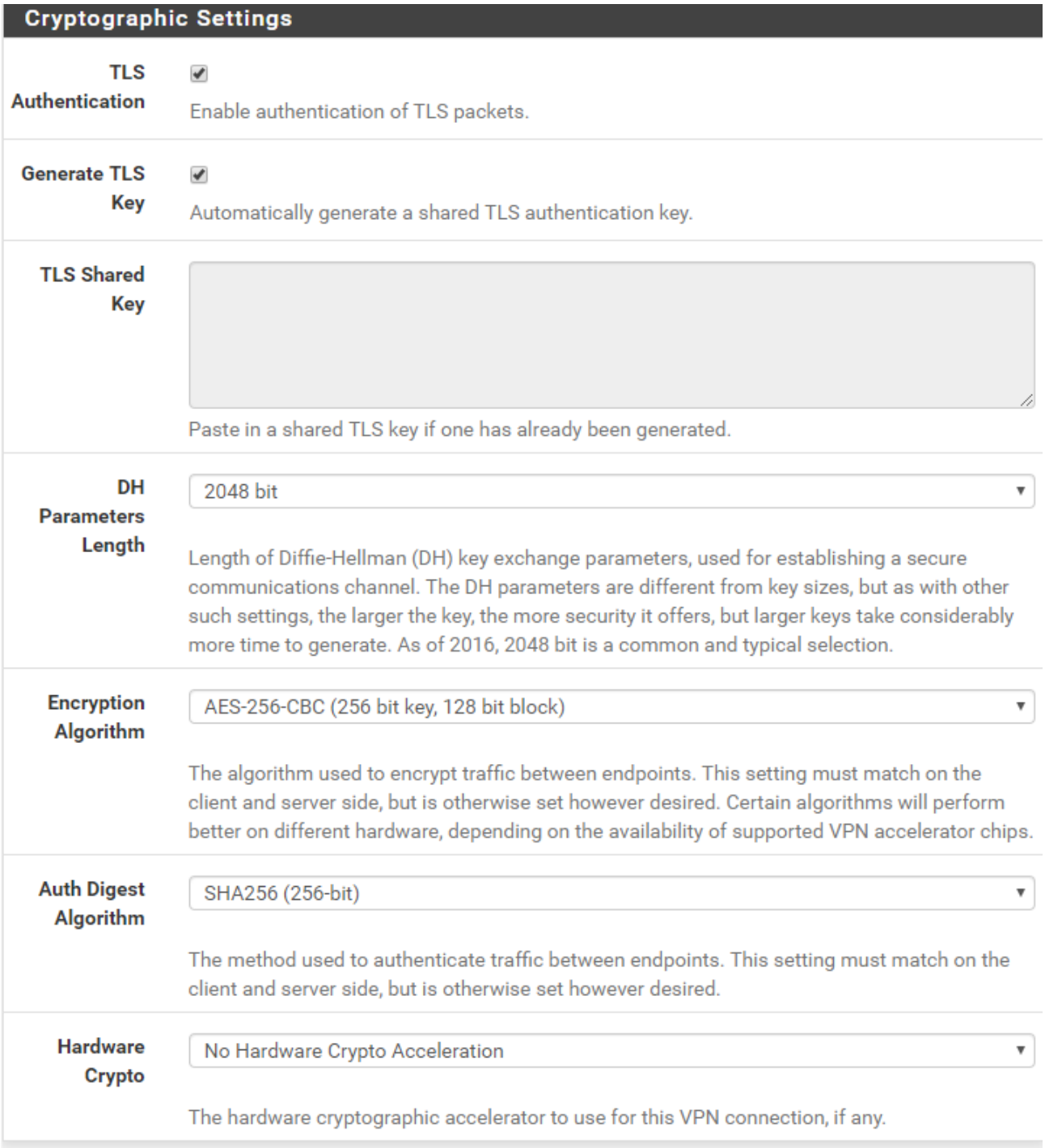


→ Wizards

On laisse tout par défaut jusqu'à l'étape 9 :



Le port OpenVPN par défaut est 1194, donc par exemple le serveur OpenVPN n°1 utilisera 1194, le n°2 1195, … .



Pour Cryptographic Settings, remplir comme ci-dessus.

Tunnel Settings

Tunnel Network

10.0.8.0/24

Réseau qui sera utilisé par le tunnel VPN (voir schéma page 11)

This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.

Redirect Gateway

☑ Force all client generated traffic through the tunnel.

Local Network

192.168.2.0/24

Réseaux VLAN1 qui accèdent au serveur d'impression (voir schéma page 11)

This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

Concurrent Connections

Specify the maximum number of clients allowed to concurrently connect to this server.

Compression

Omit Preference (Use OpenVPN Default)

Compress tunnel packets using the LZO algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.

Type-of-Service

☐ Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.

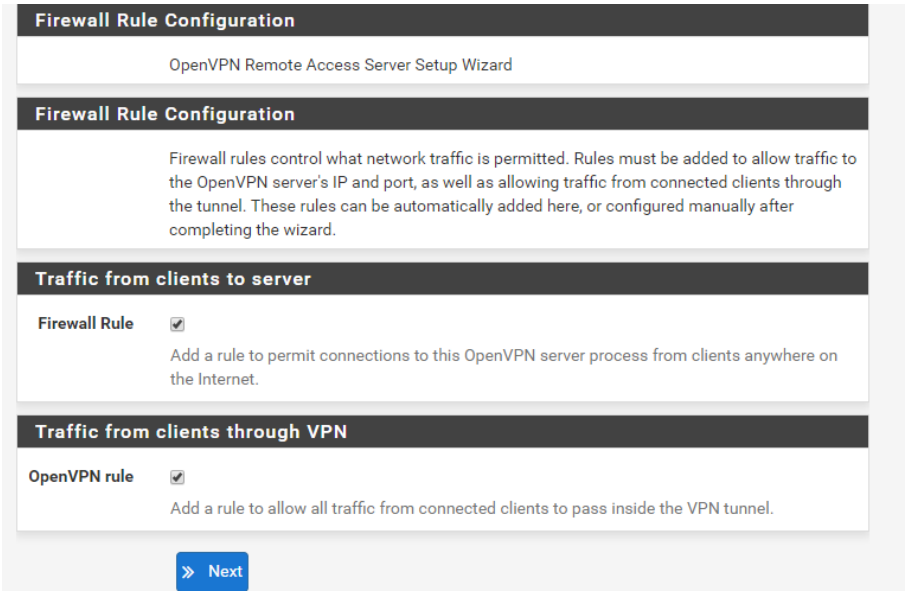
Inter-Client Communication

☐ Allow communication between clients connected to this server.

Duplicate Connections

☐ Allow multiple concurrent connections from clients using the same Common Name.
NOTE: This is not generally recommended, but may be needed for some scenarios.

Pour le firewall cochez les deux cases afin de créer automatiquement les règles de firewall associer au serveur.



Pour finir, nous devons modifier 1 ou 2 choses dans la conf du serveur .

Pour ce faire aller dans VPN→OpenVPN→Servers

Et cliquer sur le petit crayon afin de modifier le serveur.

Décocher cette case :

«

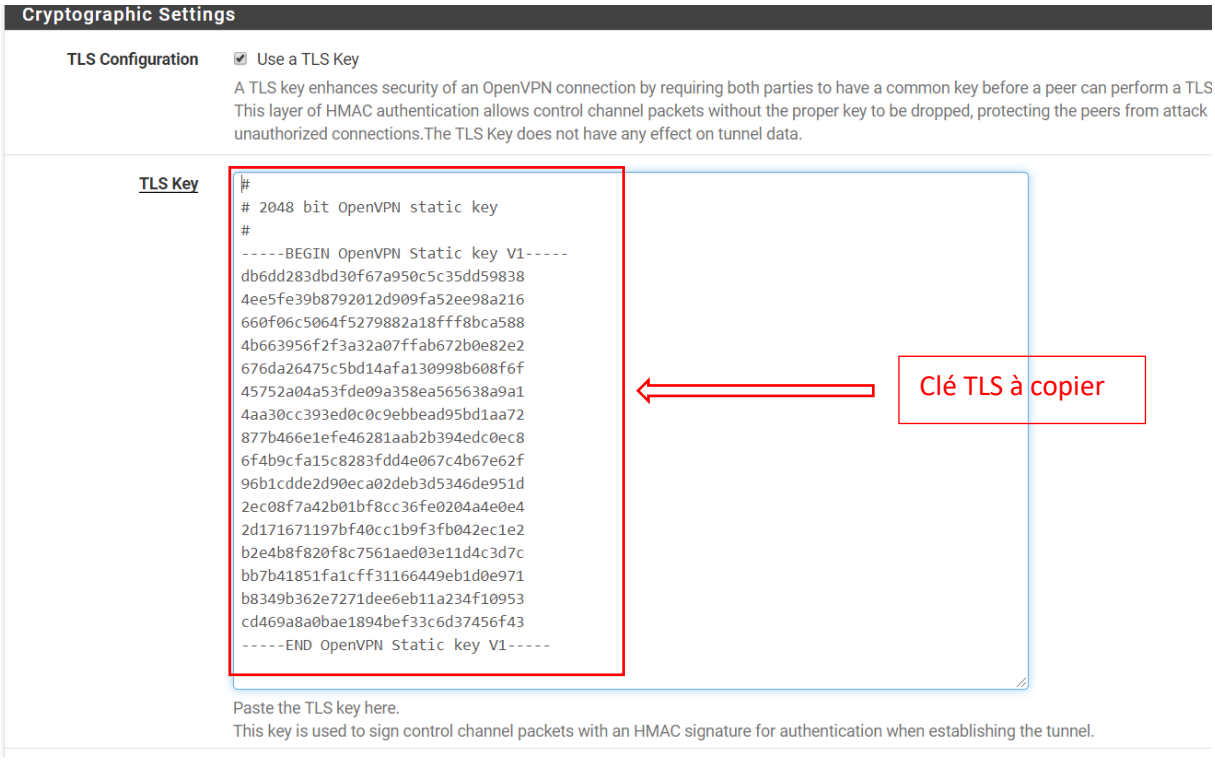
Force all client-generated IPv4 traffic through the tunnel.

»

Si le serveur VPN que vous venez de créer et le premier alors passer directement à la création d'un client (page 6).

Si le serveur que vous venez de créer n'est pas le premier alors il faut se rendre dans le premier serveur créé et copier la clé TLS du serveur et la coller dans le nouveau serveur :

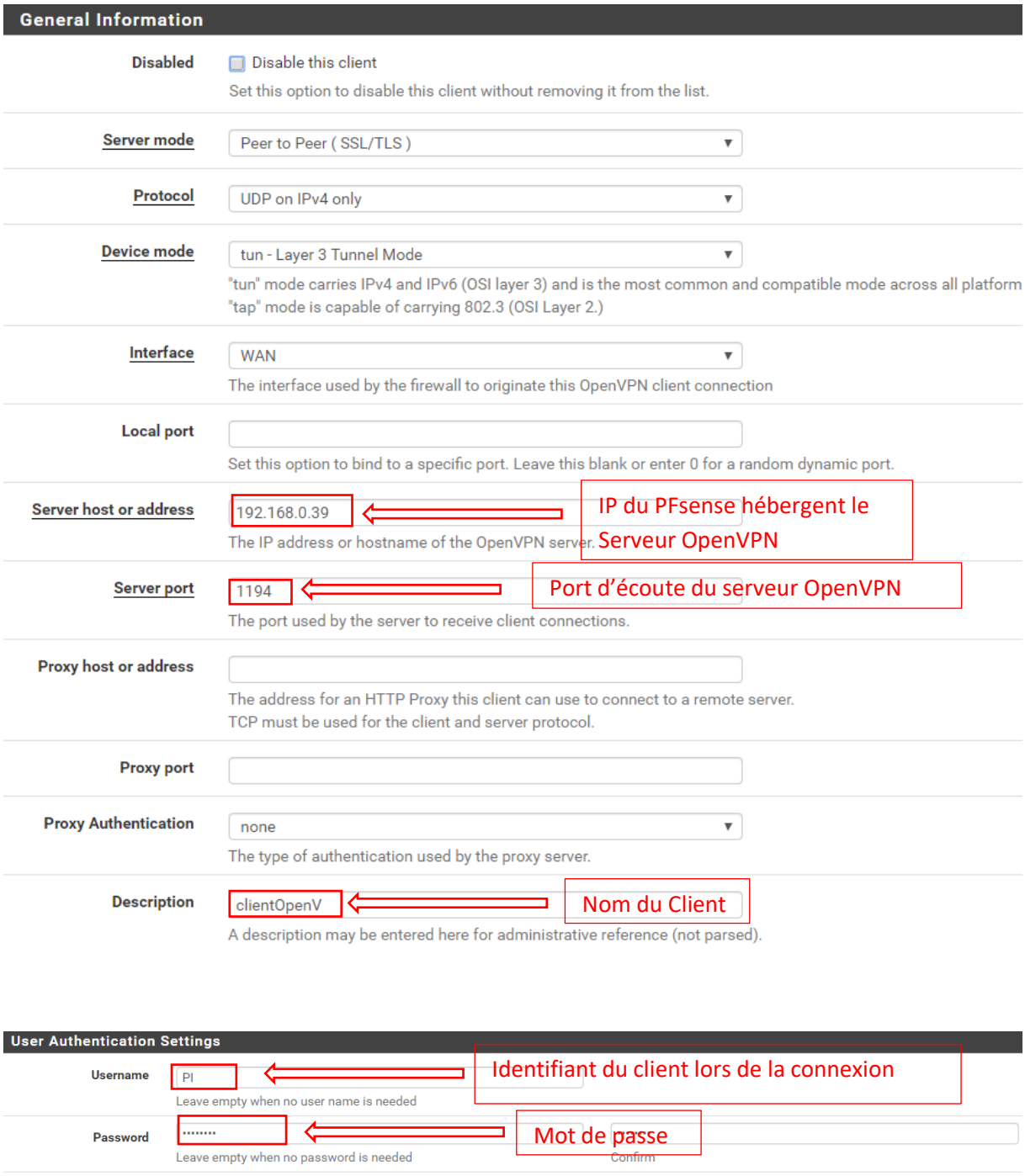
Serveur n°1 :



Serveur n°X :

2)Client OpenVPN :

Pour créer un client OpenVPN il faut aller dans l'onglet VPN puis OpenVPN puis client :

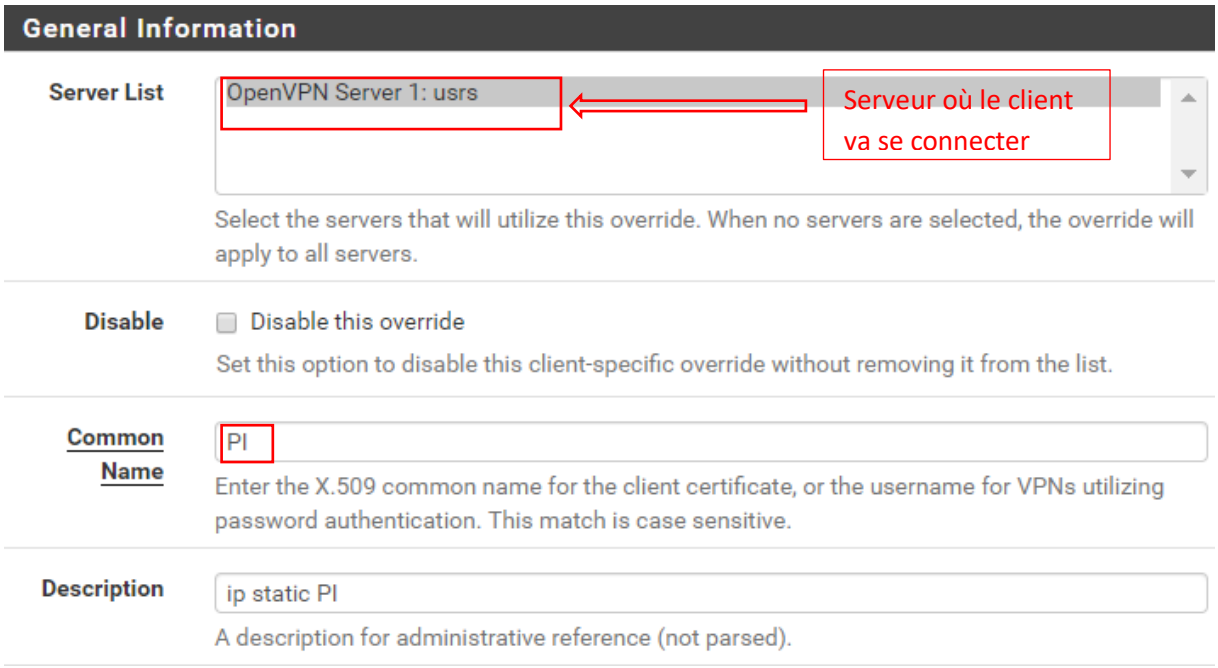


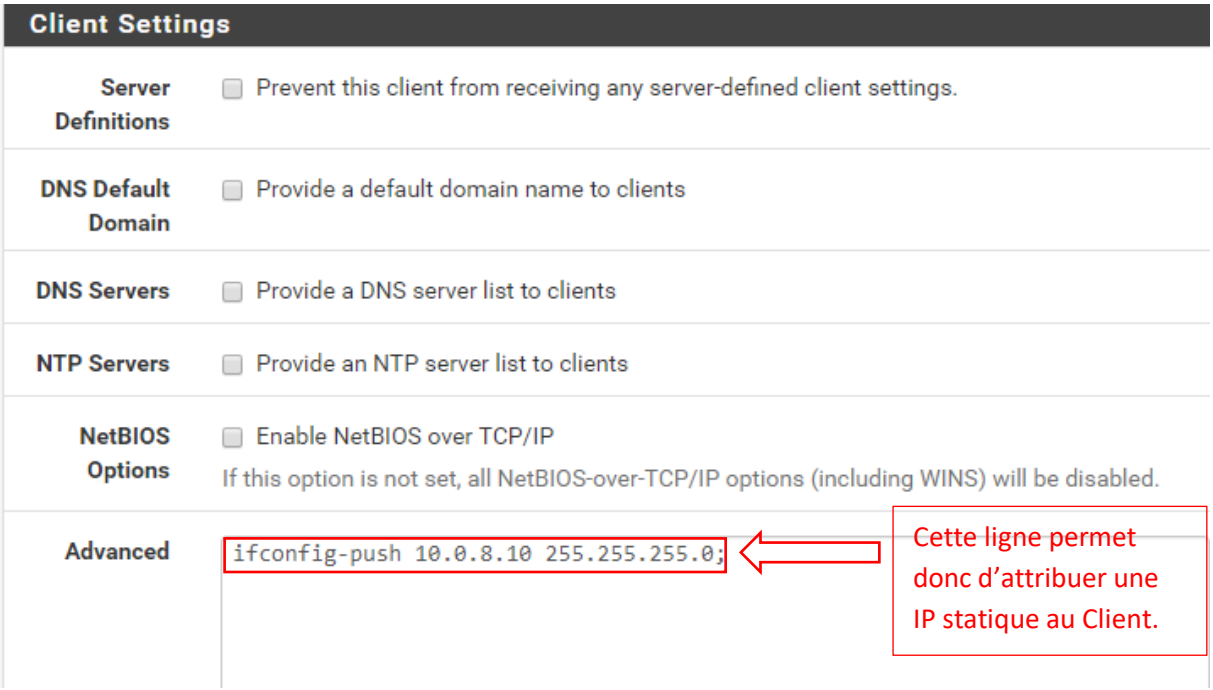
Pour Cryptographic Settings :

On laisse tout par défaut sauf la clé TLS si un client a déjà était créé précédemment (comme vue lors de la création du serveur page 5)

Pour finir la configuration du client, nous allons attribuer une adresse IP statique au client OpenVPN :

Aller dans l'onglet VPN puis OpenVPN puis client spécifique Overrides:





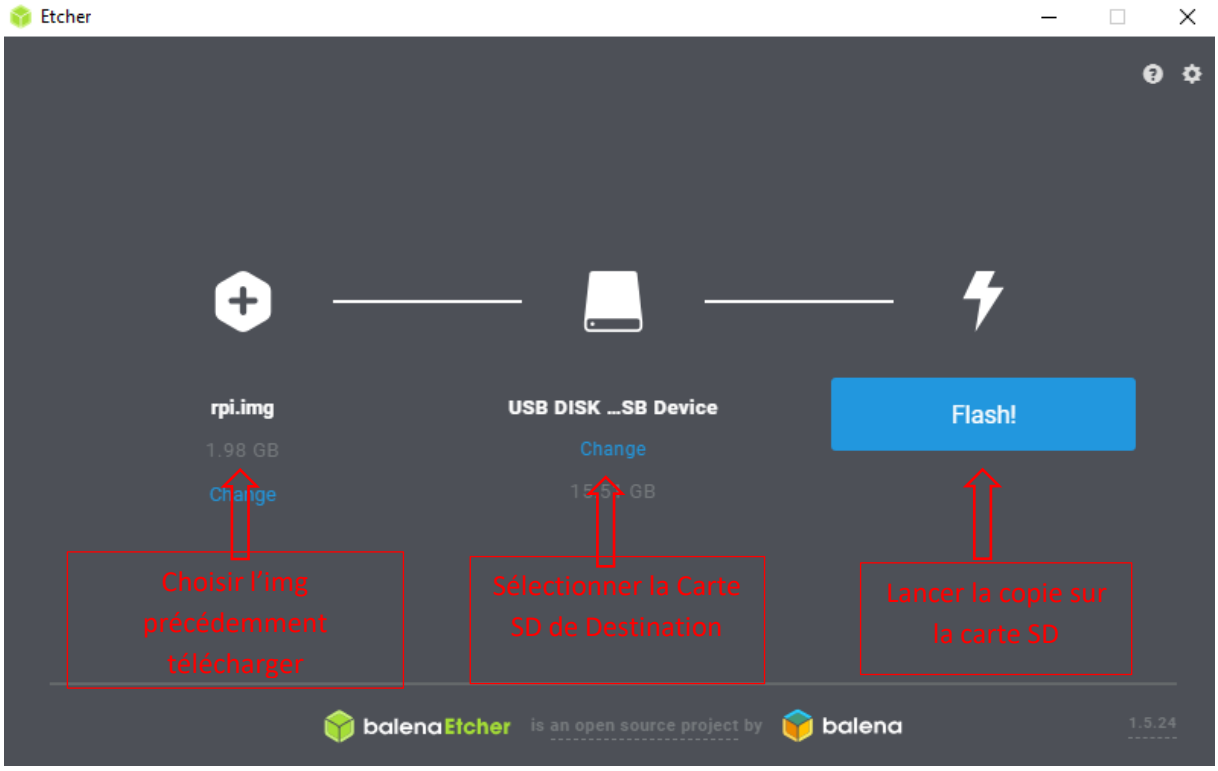
II)Raspberry :

1)Installation de la Raspberry :

On va tout d'abord télécharger l'image de la Raspberry : « »

Ensuite on télécharge est installer le logiciel BalenaEtcher : «https://www.balena.io/etcher/ »

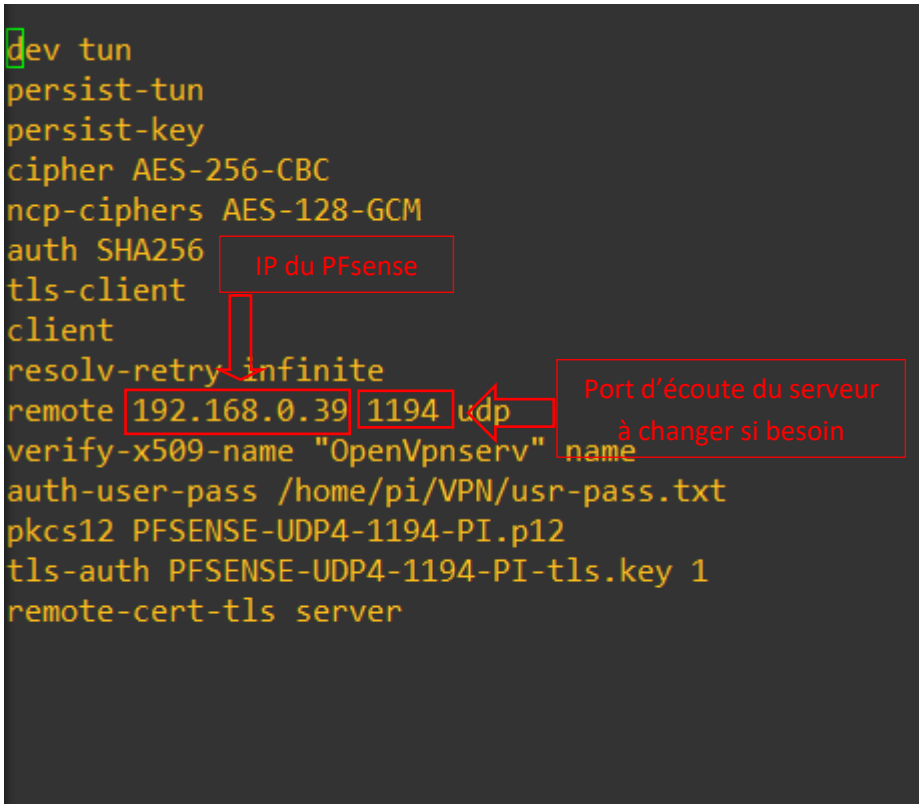
Une fois le logiciel installer, il suffit de choisir l'img a FLASH, le lecteur(donc la carte sd de destination), et cliquer sur FLASH, une fois l'opération terminer il ne reste plus qu'à mettre la carte sd dans la raspberry et la démarrer.



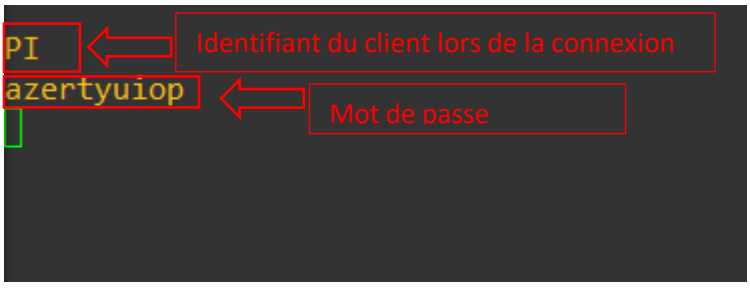
2)Configuration du client OpenVPN :

Aller dans le dossier VPN → cd /home/pi/VPN)

Ouvrer le fichier « PFSENSE-UDP4-1194-PI.ovpn » avec un éditeur de texte (nano PFSENSE-UDP4-1194-PI.ovpn) :



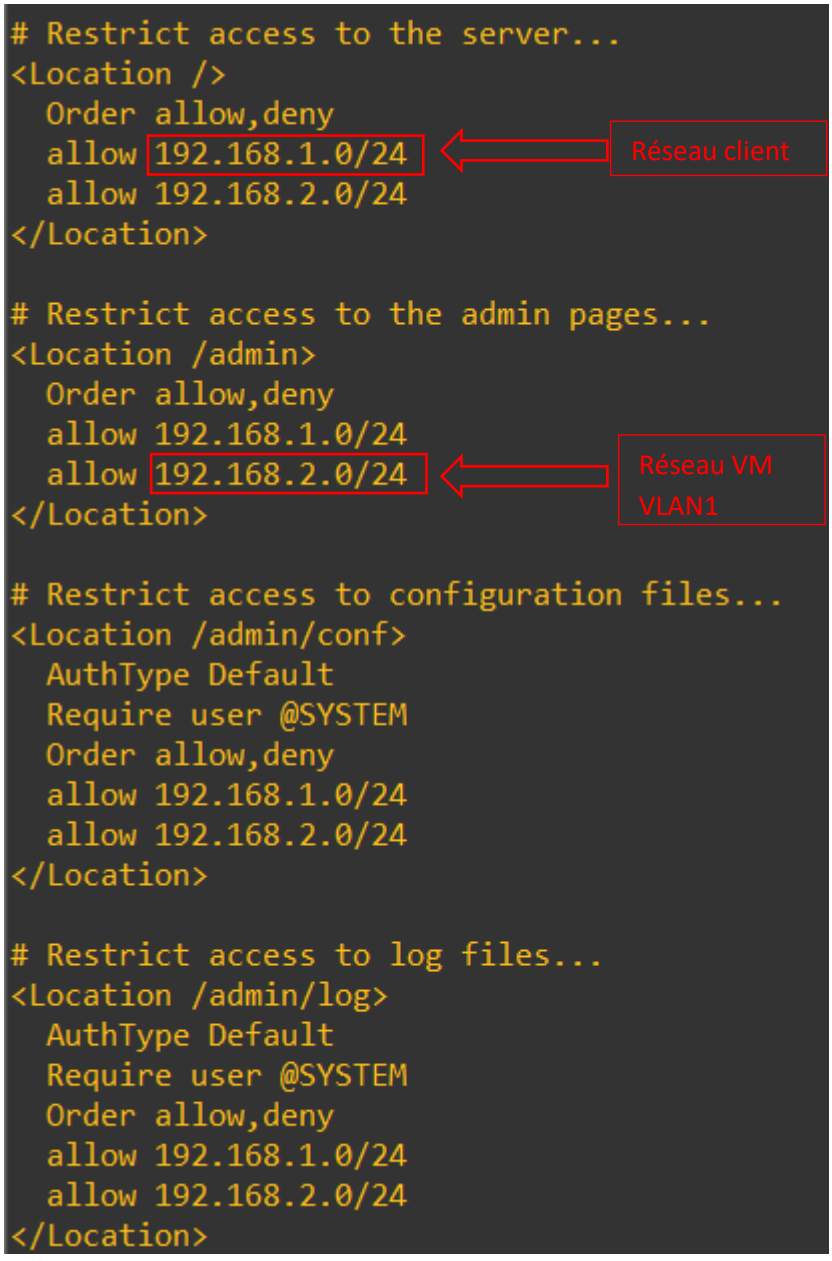
Ensuite il faut modifier le fichier usr-pass.txt (nano usr-pass.txt) :



3)Configuration de CUPS :

Aller dans le dossier cups → cd /etc/cups)

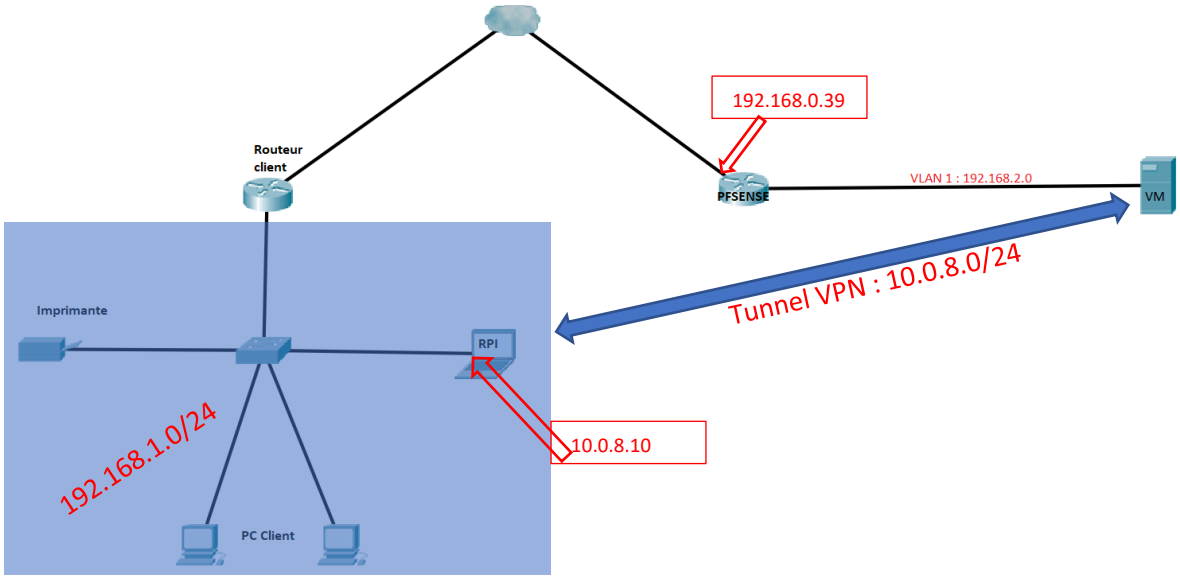
Il faut modifier le fichier cupsd.conf (nano cupsd.conf) :




```
# Restrict access to the server...
<Location />
  Order allow,deny
  allow 192.168.1.0/24
  allow 192.168.2.0/24
</Location>

# Restrict access to the admin pages...
<Location /admin>
  Order allow,deny
  allow 192.168.1.0/24
  allow 192.168.2.0/24
</Location>

# Restrict access to configuration files...
<Location /admin/conf>
  AuthType Default
  Require user @SYSTEM
  Order allow,deny
  allow 192.168.1.0/24
  allow 192.168.2.0/24
</Location>

# Restrict access to log files...
<Location /admin/log>
  AuthType Default
  Require user @SYSTEM
  Order allow,deny
  allow 192.168.1.0/24
  allow 192.168.2.0/24
</Location>
```

Il faut ici modifier les réseaux ou adresses IP autorisées à accéder au site WEB de cups,

Il faut donc modifier les lignes « allow » selon le besoin (ajouter, supprimer, modifier)


192.168.0.39
Routeur client
PFSENSE
VLAN 1 : 192.168.2.0
VM
Tunnel VPN : 10.0.8.0/24
Imprimante
RPI
10.0.8.10
192.168.1.0/24
PC Client