

OpenVpn entre Pfsense et RPI, pour serveur CUPS

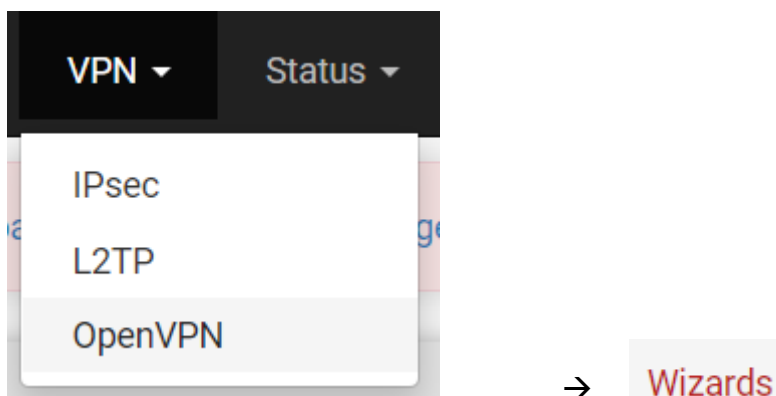
Le but est de créer un tunnel OpenVPN entre les VM client et le serveur d'impression se trouvant sur une Raspberry Pi située dans le réseau client.



1)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.



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

Step 9 of 11

General OpenVPN Server Information

| | | |
|---|------------------|---|
| Interface | WAN | |
| The interface where OpenVPN will listen for incoming connections (typically WAN.) | | |
| Protocol | UDP on IPv4 only | |
| Protocol to use for OpenVPN connections. If unsure, leave this set to UDP. | | |
| Local Port | 1194 | Ici on change le port d'écoute du serveur OpenVPN, |
| Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used. | | |
| Description | usrs | Description au choix, permet de nommer le serveur OpenVPN |
| A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients. | | |

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

| Cryptographic Settings | |
|------------------------------|---|
| TLS Authentication | <input checked="" type="checkbox"/> Enable authentication of TLS packets. |
| Generate TLS Key | <input checked="" type="checkbox"/> Automatically generate a shared TLS authentication key. |
| TLS Shared Key | <div style="border: 1px solid #ccc; height: 60px; width: 100%;"></div> <p>Paste in a shared TLS key if one has already been generated.</p> |
| DH Parameters Length | <div style="border: 1px solid #ccc; padding: 2px;">2048 bit ▼</div> <p>Length of Diffie-Hellman (DH) key exchange parameters, used for establishing a secure communications channel. The DH parameters are different from key sizes, but as with other such settings, the larger the key, the more security it offers, but larger keys take considerably more time to generate. As of 2016, 2048 bit is a common and typical selection.</p> |
| Encryption Algorithm | <div style="border: 1px solid #ccc; padding: 2px;">AES-256-CBC (256 bit key, 128 bit block) ▼</div> <p>The algorithm used to encrypt traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired. Certain algorithms will perform better on different hardware, depending on the availability of supported VPN accelerator chips.</p> |
| Auth Digest Algorithm | <div style="border: 1px solid #ccc; padding: 2px;">SHA256 (256-bit) ▼</div> <p>The method used to authenticate traffic between endpoints. This setting must match on the client and server side, but is otherwise set however desired.</p> |
| Hardware Crypto | <div style="border: 1px solid #ccc; padding: 2px;">No Hardware Crypto Acceleration ▼</div> <p>The hardware cryptographic accelerator to use for this VPN connection, if any.</p> |

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.

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

Local Network

192.168.2.0/24

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.

The screenshot shows a multi-step configuration wizard. The top section is titled "Firewall Rule Configuration" and contains the text "OpenVPN Remote Access Server Setup Wizard". Below this is another "Firewall Rule Configuration" section with explanatory text: "Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard." The next section, "Traffic from clients to server", has a "Firewall Rule" checkbox checked and the description "Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet." The final section, "Traffic from clients through VPN", has an "OpenVPN rule" checkbox checked and the description "Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel." At the bottom, there is a blue button labeled "» Next".

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 est 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 :

Cryptographic Settings

TLS Configuration Use a TLS Key

A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack unauthorized connections. The TLS Key does not have any effect on tunnel data.

TLS Key

```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
db6dd283dbd30f67a950c5c35dd59838
4ee5fe39b8792012d909fa52ee98a216
660f06c5064f5279882a18fff8bca588
4b663956f2f3a32a07ffab672b0e8e2
676da26475c5bd14afa130998b608f6f
45752a04a53fde09a358ea565638a9a1
4aa30c393ed0c0c9ebbead95bd1aa72
877b466e1efe46281aab2b394edc0ec8
6f4b9cfa15c8283fdd4e067c4b67e62f
96b1cde2d90eca02deb3d5346de951d
2ec08f7a42b01bf8cc36fe0204a4e0e4
2d171671197bf40cc1b9f3fb042ec1e2
b2e4b8f820f8c7561aed03e11d4c3d7c
bb7b41851fa1c3f31166449eb1d0e971
b8349b362e7271dee6eb11a234f10953
cd469a8a0bae1894bef33c6d37456f43
-----END OpenVPN Static key V1-----
```

← Clé TLS à copier

Paste the TLS key here.
This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.

Serveur n°X :

TLS Key



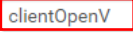

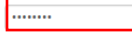
```
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
8a7ef8a28b63c1f6760d4c330c9d0017
aa810e164fe6be0f2a00e8c0a36d3b82
101ff7d6094a48b3411067bd37eb1f6b
9bb1a2efb7f6d81b3463ed8cf536a1f7
70c851a610af46244ae5853c85c56106
792b484f5352dcfdc80a38d9603fca79
aec65d31deda927d1dd4eef3faa65afa
7429f51b12e6710b498a39555276cbc5
56fdcbf33ab543a4d5e7607dd3cedfdf
1668d9db3c4208dbd0f54ef2fa484e51
eaed82c5e74d2f9fd858651b36c4aab6
abdebf086c0f98824986ec06e6cb9105
ac8dc04266d444fea8e26b8ef1213f4b
3bedadae2eb3ecaf2f7ebf0fc93aaf67
3052c2ffa483b51a983d4cbf58301cf8
7c3dbca3325c07ff360b3a21207f1672
-----END OpenVPN Static key V1-----
```

← Supprimer la clé présente, et copier celle du serveur n°1

Paste the TLS key here

2) Client OpenVPN :

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

| General Information | |
|-------------------------------|--|
| Disabled | <input type="checkbox"/> Disable this client Set this option to disable this client without removing it from the list. |
| Server mode | Peer to Peer (SSL/TLS) |
| Protocol | UDP on IPv4 only |
| Device mode | tun - Layer 3 Tunnel Mode "tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platform "tap" mode is capable of carrying 802.3 (OSI Layer 2.) |
| Interface | WAN The interface used by the firewall to originate this OpenVPN client connection |
| Local port | <input type="text"/> Set this option to bind to a specific port. Leave this blank or enter 0 for a random dynamic port. |
| Server host or address | 192.168.0.39  IP du PFsense hébergeant le Serveur OpenVPN |
| Server port | 1194  Port d'écoute du serveur OpenVPN |
| Proxy host or address | <input type="text"/> The address for an HTTP Proxy this client can use to connect to a remote server. TCP must be used for the client and server protocol. |
| Proxy port | <input type="text"/> |
| Proxy Authentication | none |
| Description | clientOpenV  Nom du Client A description may be entered here for administrative reference (not parsed). |
| User Authentication Settings | |
| Username | PI  Identifiant du client lors de la connexion Leave empty when no user name is needed |
| Password |  Mot de passe Leave empty when no password is needed <input type="text"/> Confirm |

Pour **Cryptographic Settings** :

On laisse tout par défaut sauf la clé TLS si un client a déjà été créé précédemment (comme vu 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:

General Information

Server List ← Serveur où le client va se connecter

Select the servers that will utilize this override. When no servers are selected, the override will apply to all servers.

Disable Disable this override
Set this option to disable this client-specific override without removing it from the list.

Common Name
Enter the X.509 common name for the client certificate, or the username for VPNs utilizing password authentication. This match is case sensitive.

Description
A description for administrative reference (not parsed).

Client Settings

Server Definitions Prevent this client from receiving any server-defined client settings.

DNS Default Domain Provide a default domain name to clients

DNS Servers Provide a DNS server list to clients

NTP Servers Provide an NTP server list to clients

NetBIOS Options Enable NetBIOS over TCP/IP
If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.

Advanced ← Cette ligne permet donc d'attribuer une IP statique au Client.

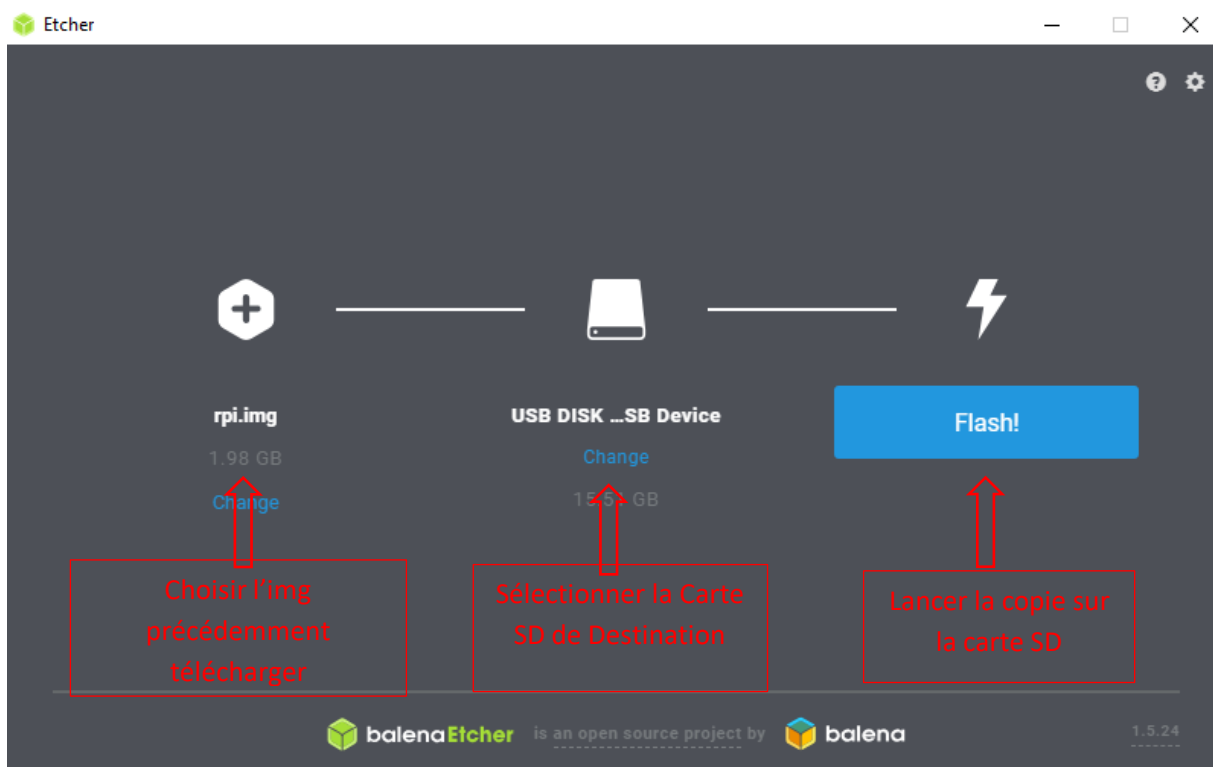
II) Raspberry :

1) Installation de la Raspberry :

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

Ensuite on télécharge et installe le logiciel BalenaEtcher : « <https://www.balena.io/etcher/> »

Une fois le logiciel installé, il suffit de choisir l'image à FLASH, le lecteur (donc la carte SD de destination), et cliquer sur FLASH, une fois l'opération terminée il ne reste plus qu'à mettre la carte SD dans la Raspberry et la démarrer.

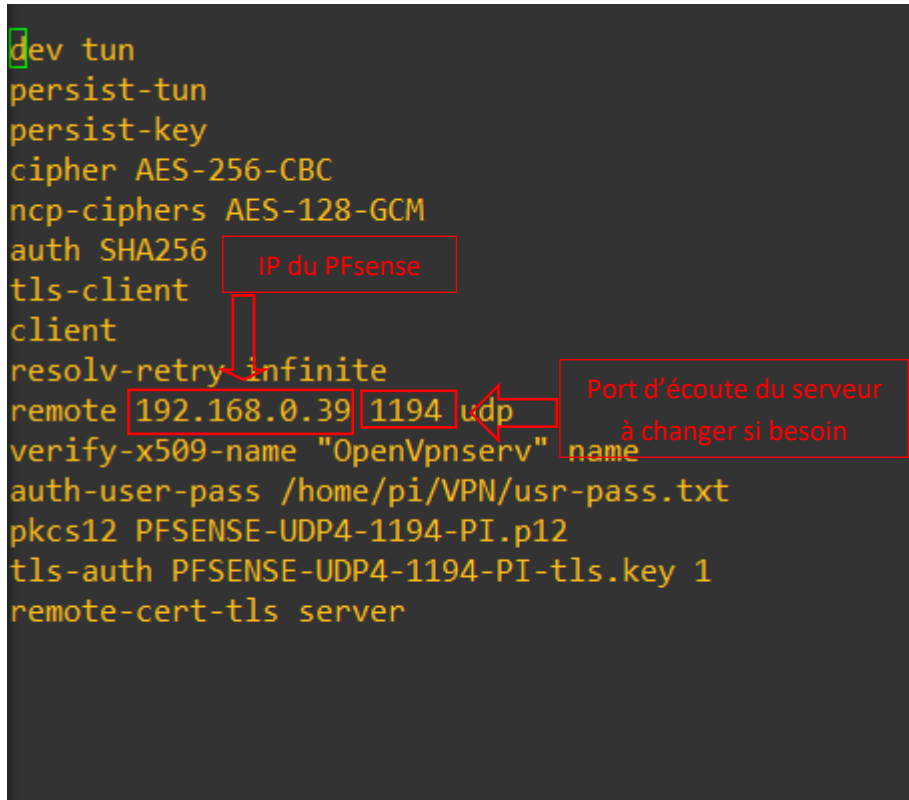


2) Configuration du client OpenVPN :

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

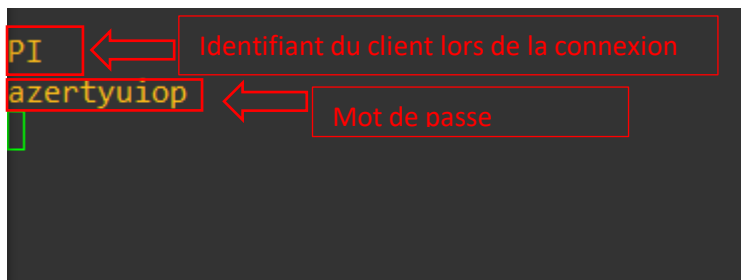
Ouvrir le fichier « PFSense-UDP4-1194-PI.ovpn » avec un éditeur de texte (nano PFSense-UDP4-1194-PI.ovpn) :

```
dev tun
persist-tun
persist-key
cipher AES-256-CBC
ncp-ciphers AES-128-GCM
auth SHA256
tls-client
client
resolv-retry infinite
remote 192.168.0.39 1194 udp
verify-x509-name "OpenVpnserv"
auth-user-pass /home/pi/VPN/usr-pass.txt
pkcs12 PFSense-UDP4-1194-PI.p12
tls-auth PFSense-UDP4-1194-PI-tls.key 1
remote-cert-tls server
```



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

```
PI
azertyuiop
```



3) Configuration de CUPS :

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

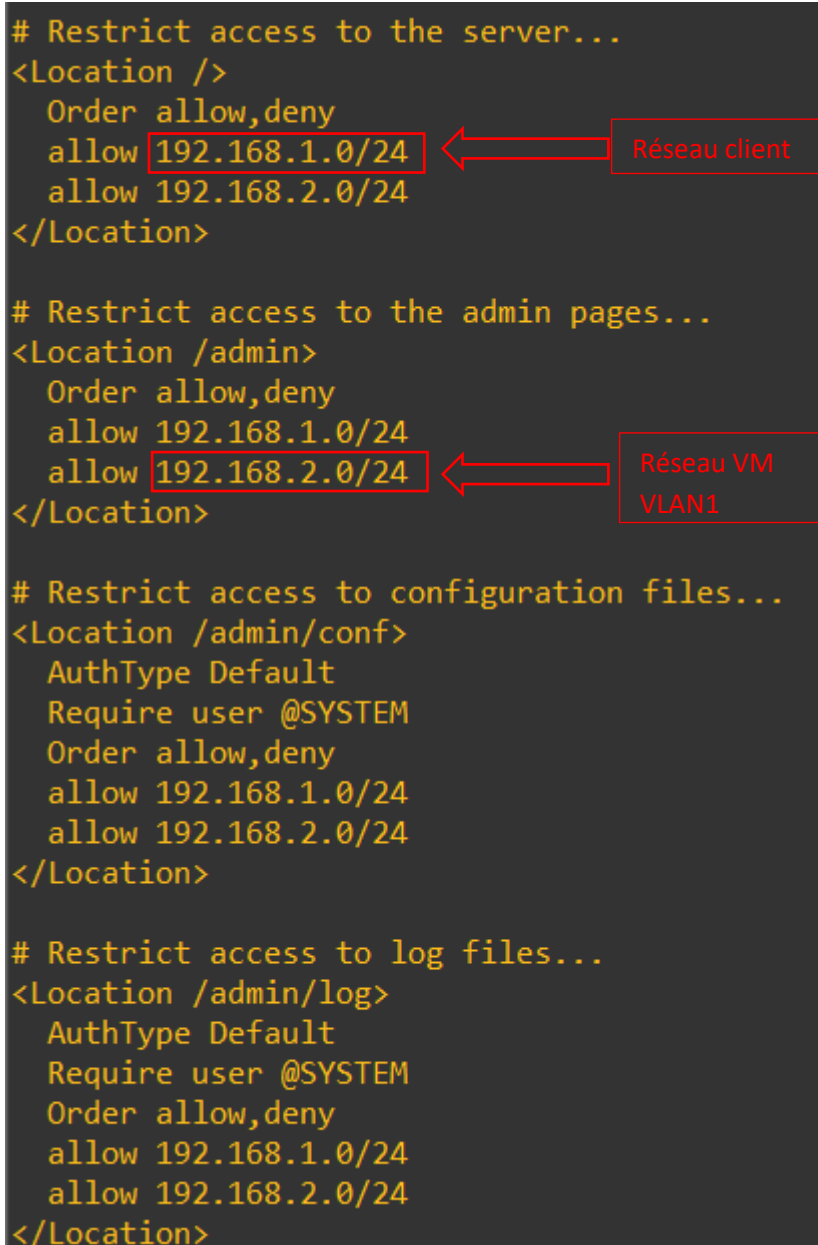
Il faut modifier le fichier cupsd.conf (nano cupsd.conf) :

```
# 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)

