CHECCONI DORIAN
MISE EN PLACE SERVEUR VPN (LINUX)

01/11/2017

Théodore Aubanel

BTS SIO

Table des matières

PRÉSENTATION

1. Objectif du projet

Mise en place d'un réseau comportant 2 routeurs qui seront des machines sous Debian. L'objectif est qu'une machine dans un autre réseau utilise un client VPN pour être en liaison avec le serveur VPN sur la machine Debian.

2. Exigences principales

- 2 Routeurs dont un sous Debian
- Serveur VPN sur un routeur Debian

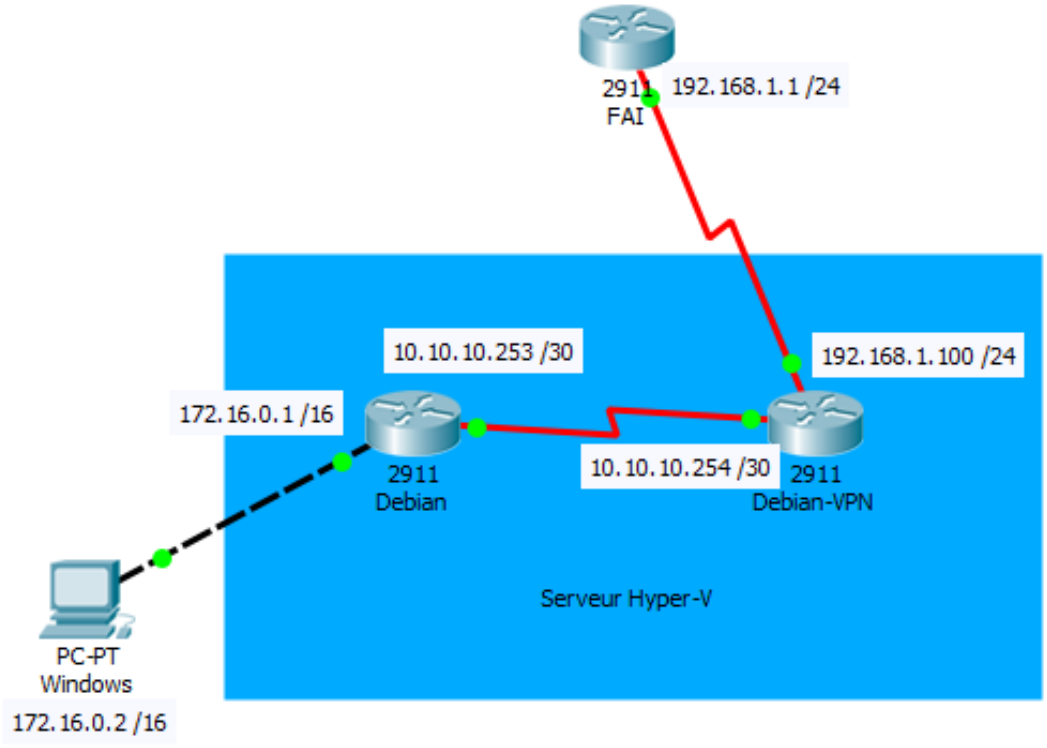
3. Matériel

Pour mettre en place ce réseau nous l'effectueront grâce à des machines virtuel et un ordinateur fixe. Les machines virtuelles peuvent êtres des machines physique si cela est possible.

Voici la liste du matériel utilisé lors de ce projet :

- Serveur Hyper-V (avec 2 cartes réseau)
- 2 Machines virtuels sous Debian (Routeur)
- 1 Machine physique sous Windows

4. Schéma du réseau



CONFIGURATIONS RÉSEAU

À partir de maintenant je nommerais « Debian » le routeur Debian simple, « Debian-VPN » le routeur Debian qui fait aussi serveur VPN et « Windows » le client VPN.

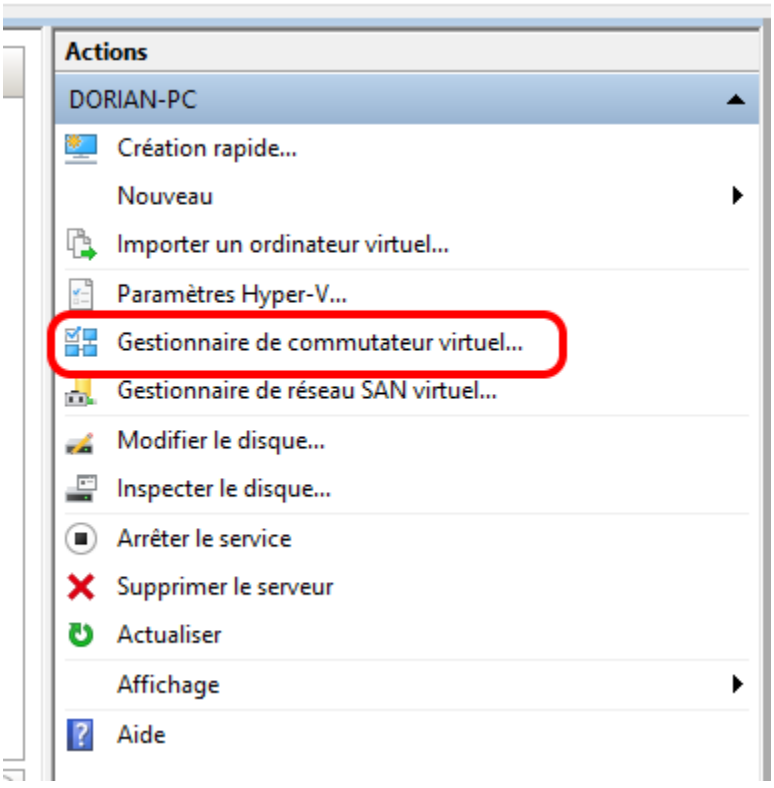
5. Configuration Hyper-V

Cette partie ne vous concerne pas si vous n'utilisé pas de machines virtuelles et/ou que vous avez votre réseau physique en place.

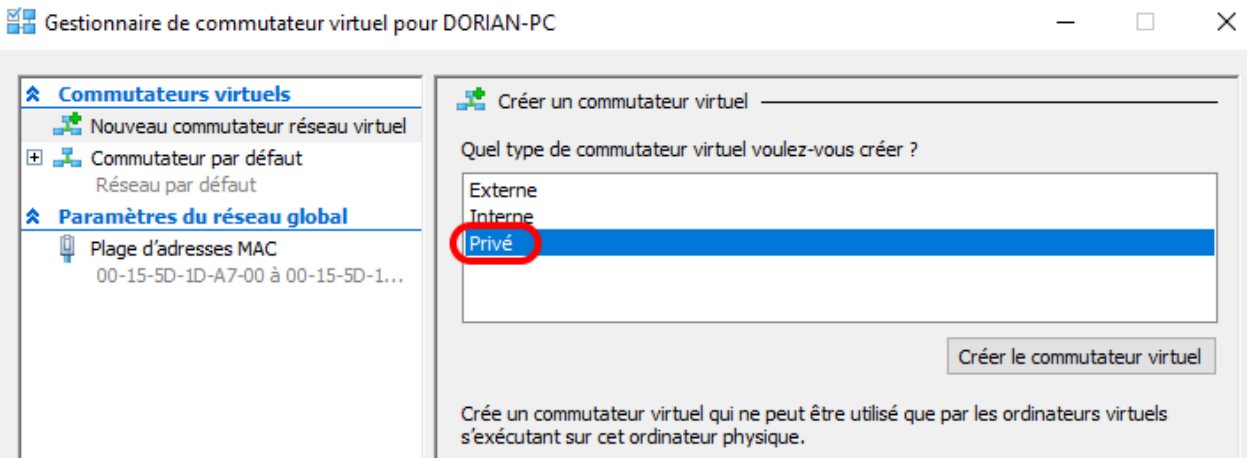
Nous allons donc commencer à configurer Hyper-V, je pars du principe que les machines virtuelles sont créées et que Debian est installé.

Première étape, nous avons besoin de créer un switch virtuel qui permettra la liaison entre nos 2 routeur.

Pour cela il faut aller dans le gestionnaire de commutateur virtuel dans le menu de droite :



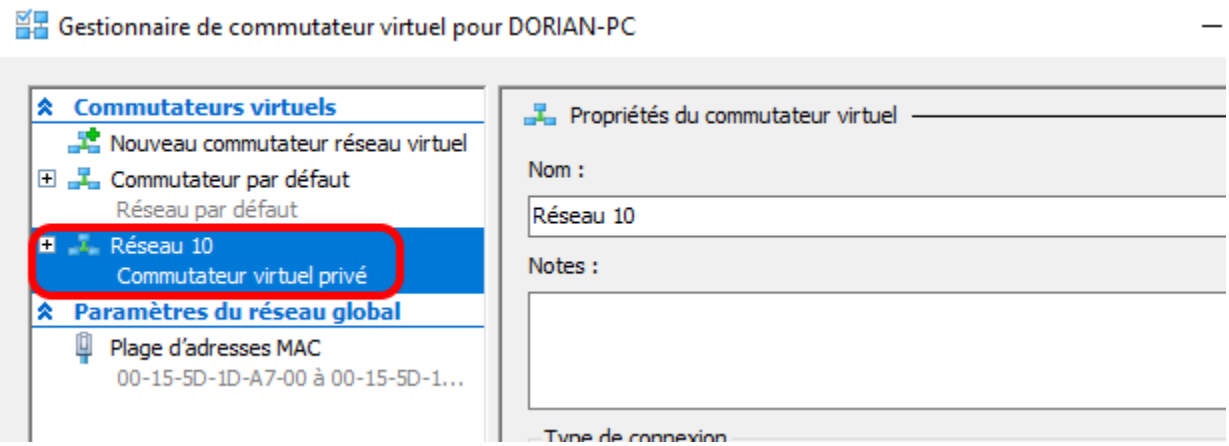
Ensuite nous devons choisir quel type de commutateur nous voulons.



Dans notre cas pour la liaison inter-routeur nous n'aurons besoin que d'un commutateur Privé qui permet une liaison seulement entre machine virtuel, ce qui est exactement ce que nous voulons !

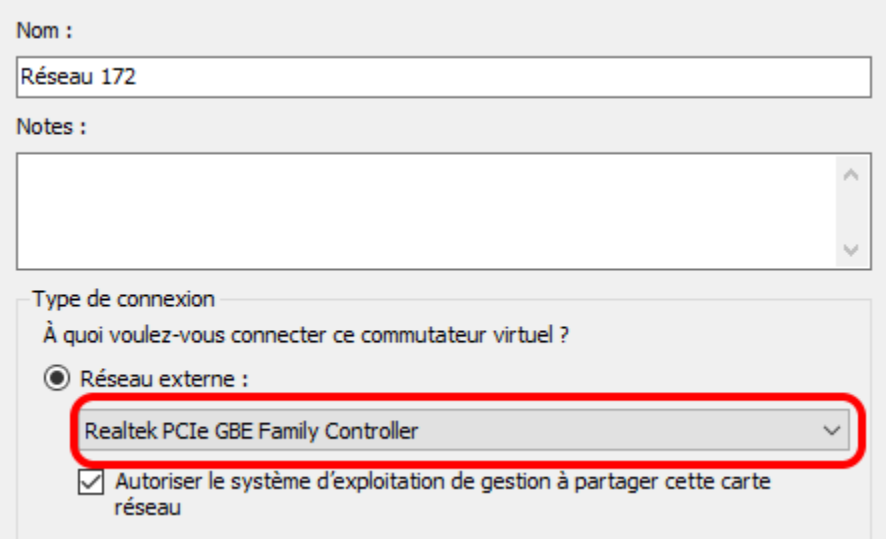
Ensuite cliquez sur « Créer le commutateur virtuel » et renseignez le nom que vous voulez lui donner. Moi je le nommerais « Réseau 10 » car mon adresse de ce réseau commence par 10.

Voilà notre nouveau commutateur est ici :

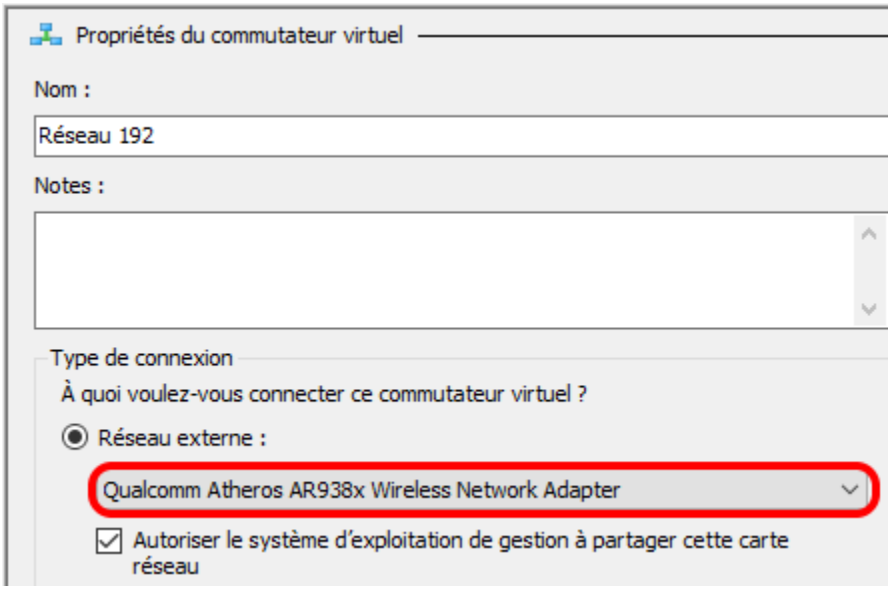


Mon serveur possède 2 cartes réseau physique, il me faudra donc créer 2 commutateur externe pour que mes machines virtuelles puissent aussi accéder au réseau externe (physique).

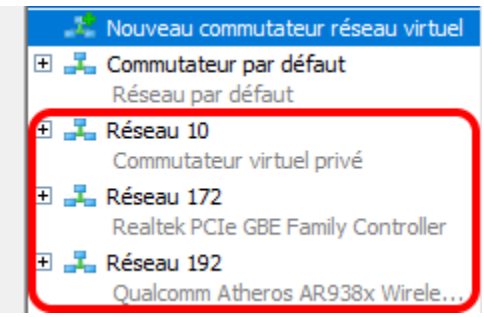
Je crée donc mon premier commutateur externe pour le réseau 172 pour qui j'affecte ma carte Ethernet (Filaire).



Et un deuxième commutateur externe pour le réseau 192 pour qui j'affecte ma carte Wifi.

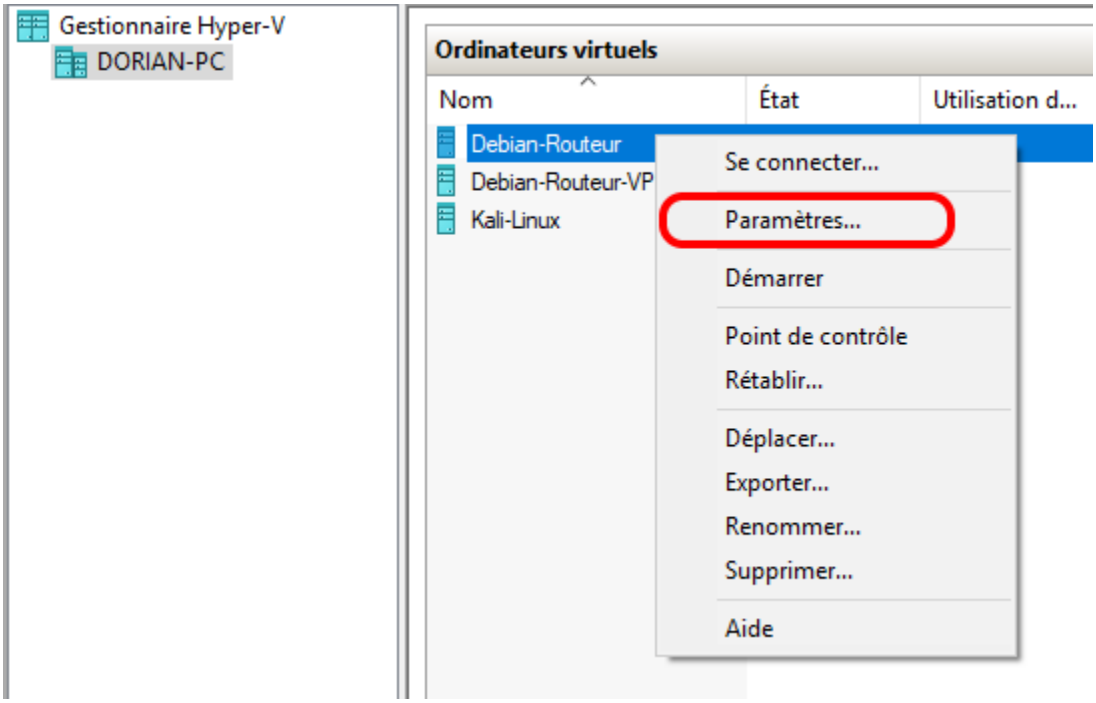


Nos commutateurs étant créé :

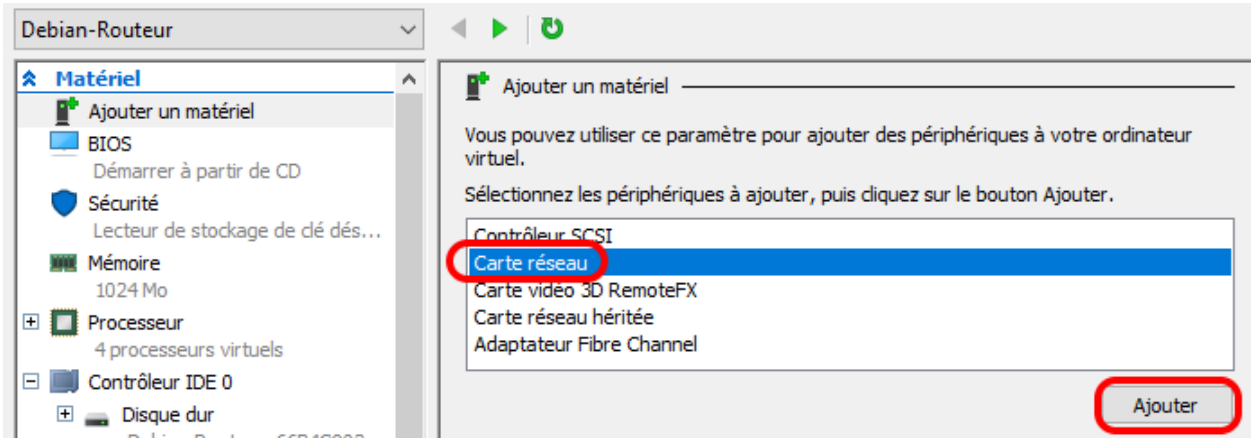


Nous allons maintenant rajouter une nouvelle carte réseau sur nos 2 machines virtuels pour le réseau inter-routeur.

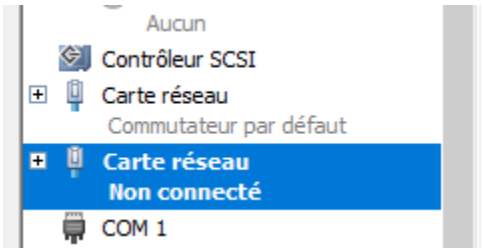
Vous allez maintenant dans les paramètres de votre machine virtuel :



Une fois dans les paramètres vous arrivez directement sur la page d'ajout de périphérique. Vous ajoutez donc une nouvelle carte réseau :



Vous avez maintenant 2 cartes réseau :



Voici les configurations de chaque cartes réseau des machines virtuels :

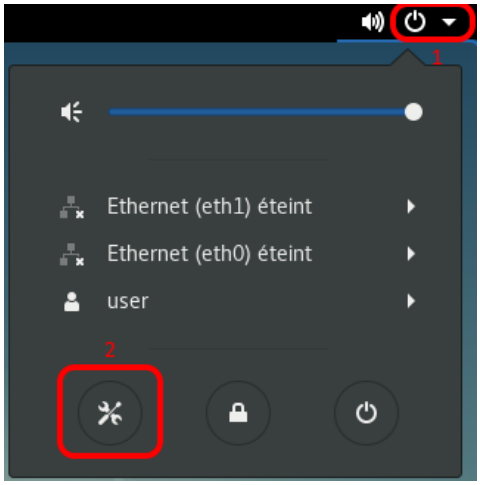
Cartes Réseau	Debian	Debian-VPN
Carte Réseau 1	Commutateur « Réseau 172 »	Commutateur « Réseau 192 »
Carte Réseau 2	Commutateur « Réseau 10 »	Commutateur « Réseau 10 »

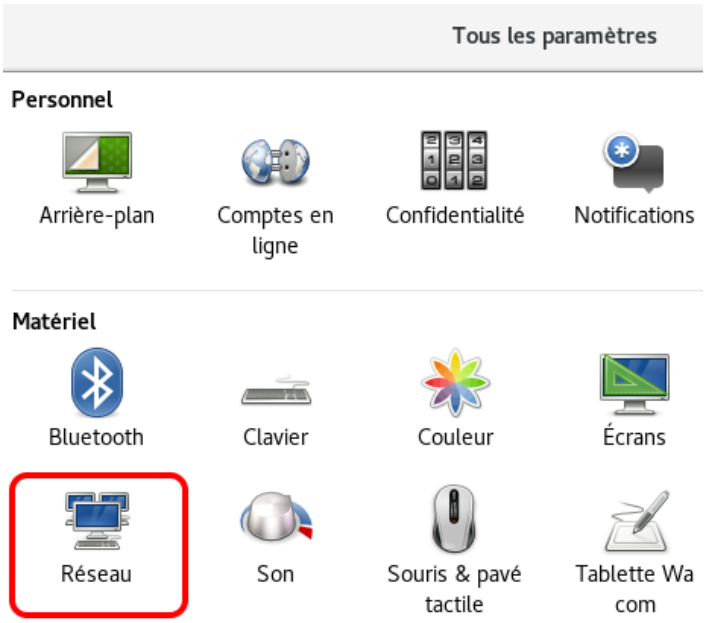
La configuration d'Hyper-V est maintenant terminée.

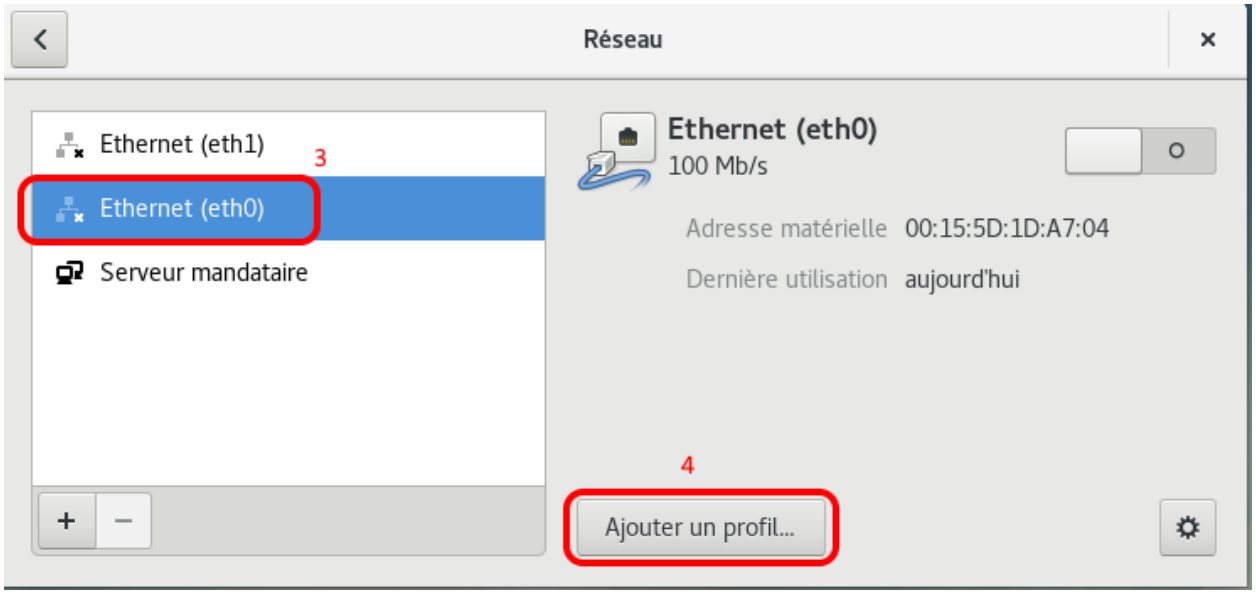
6. Configuration des routeurs (Debian)

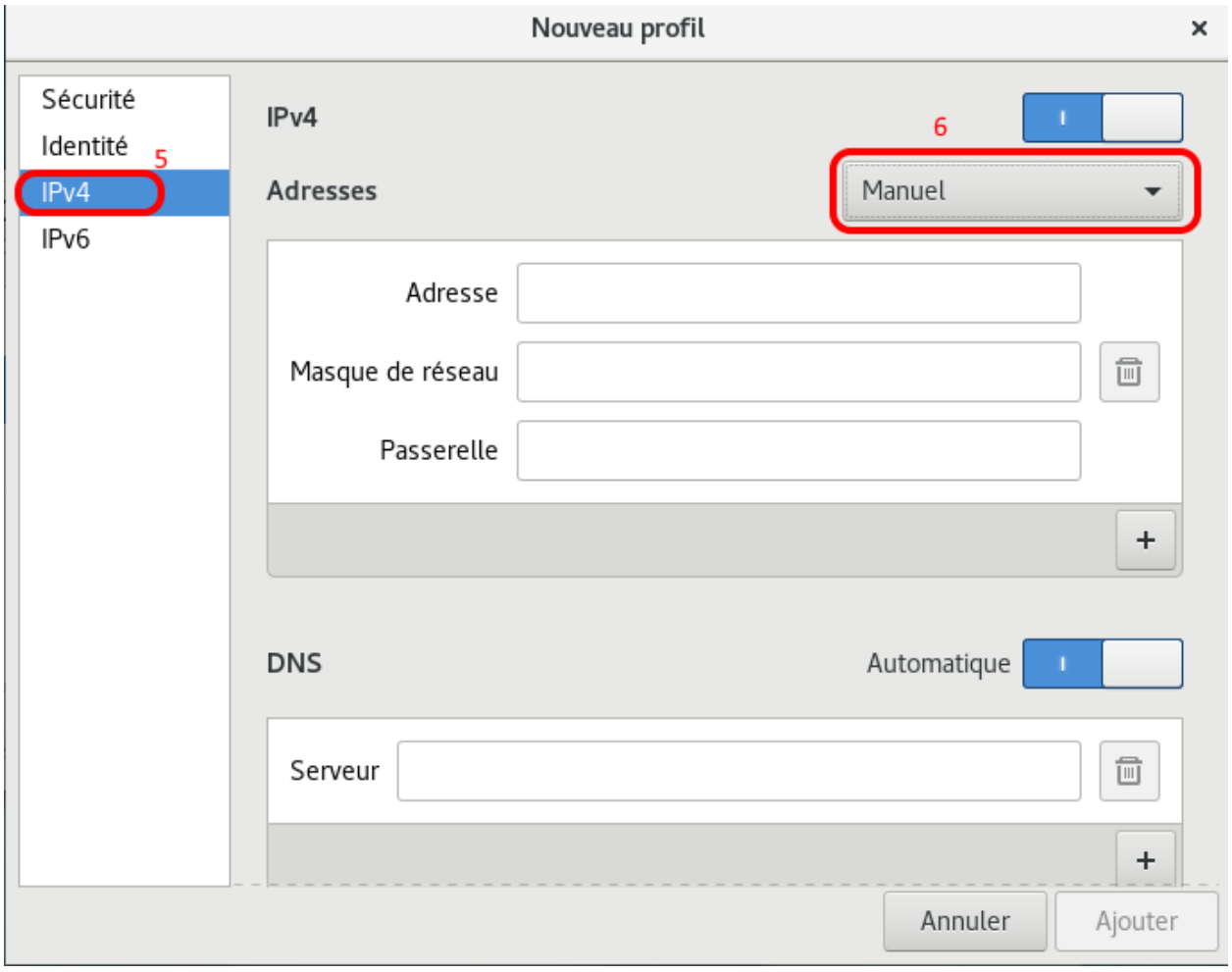
Les étapes si dessous ne sont montrés qu'une seule fois mais sont bien à faire sur les 2 machines : « Debian » et « Debian-VPN »

Pour commencer nous devons configurer les cartes réseau avec une adresse Ip statique. Rendez-vous dans les paramètres de cartes :









Voilà comment mettre une carte réseau en statique. Maintenant il faut ajouter les profils en leur donnant un nom dans « Identité » puis appliquer les configurations aux cartes souhaitées.

Voici les configurations de mes cartes :

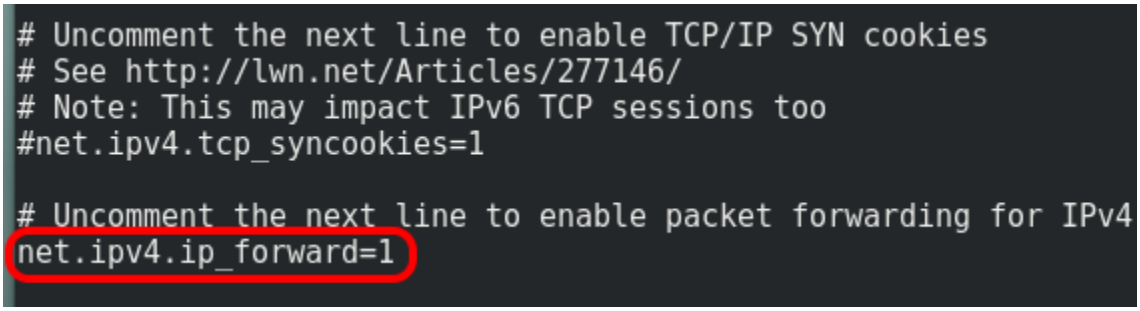
- Carte 1 dans Hyper-V = eth0
- Carte 2 dans Hyper-V = eth1

Cartes Réseau	Debian	Debian-VPN
Carte Réseau 1	Ip : 172.16.0.1 Masque : 255.255.0.0 Passerelle : Aucune	Ip : 192.168.1.100 Masque : 255.255.255.0 Passerelle : Aucune
Carte Réseau 2	Ip : 10.10.10.253 Masque : 255.255.255.252 Passerelle : Aucune	Ip : 10.10.10.254 Masque : 255.255.255.252 Passerelle : Aucune

Maintenant que nos cartes réseau sont configuré nous allons devoir nous occuper du routage entre les 2 routeurs pour que l'on puisse communiquer d'un réseau à l'autre.

Pour activer la fonction de routage il n'y a rien de compliquer.

1. Ouvrez le fichier « /etc/sysctl.conf »
2. Rechercher la ligne « # sysctl net.ipv4.ip_forward=1 »
3. Décommenté la en retirant le « # » au début de la ligne



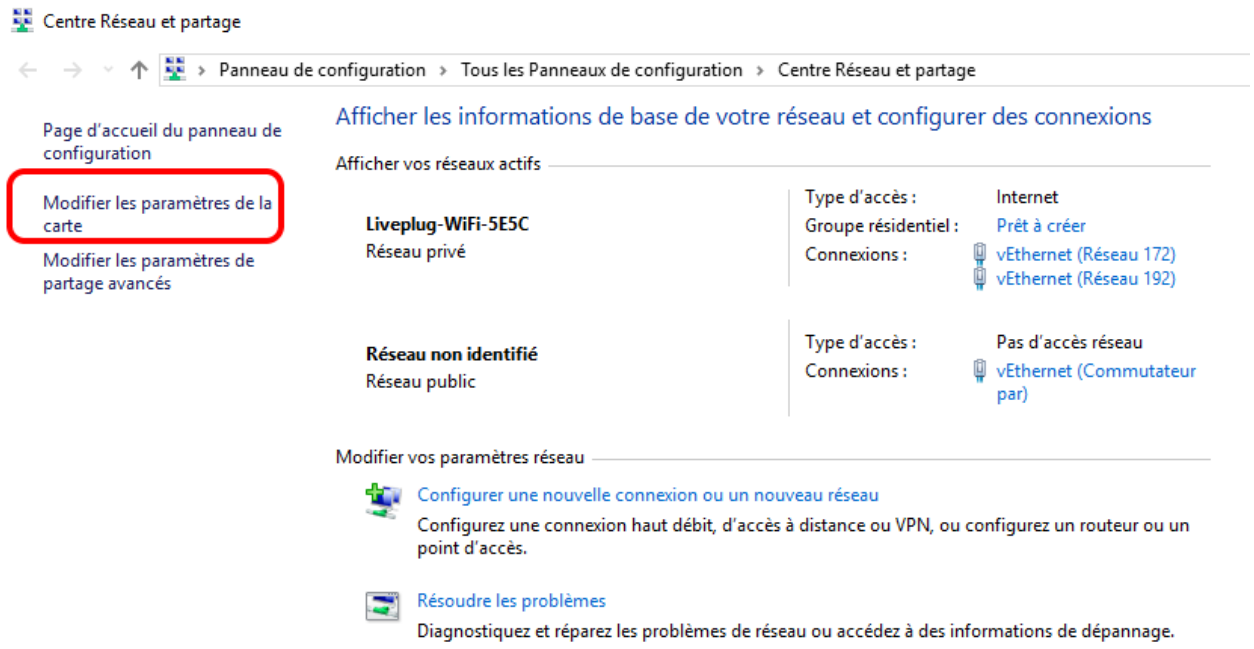
Une fois modifier, vous n'avez plus qu'à redémarrer votre machine virtuelle. (Après redémarrage, vérifiez que les bons profils de vos cartes réseau sont appliqué)

Je rappelle que ces manipulations sont à faire sur les 2 machines virtuelles Debian ainsi que tout ce qui va suivre jusqu'à que nous arrivions à la partie VPN.

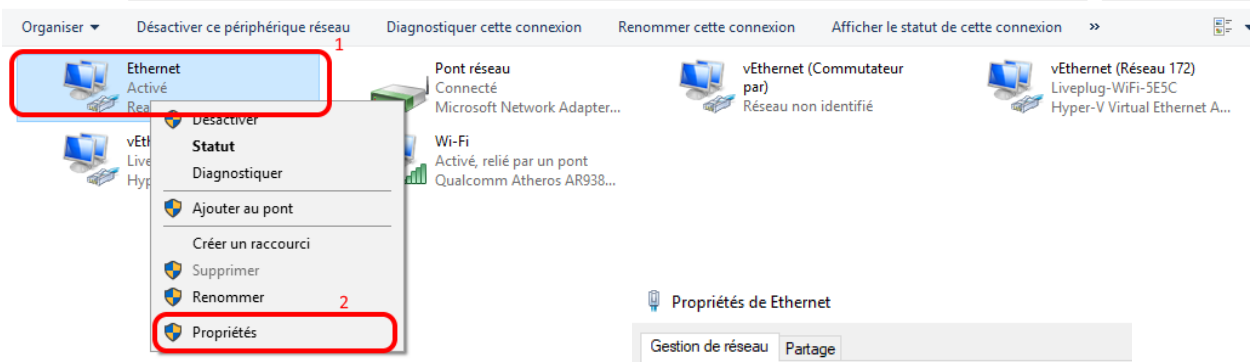
Maintenant que c'est fait nous allons rajouter Windows !

7. Configuration Windows

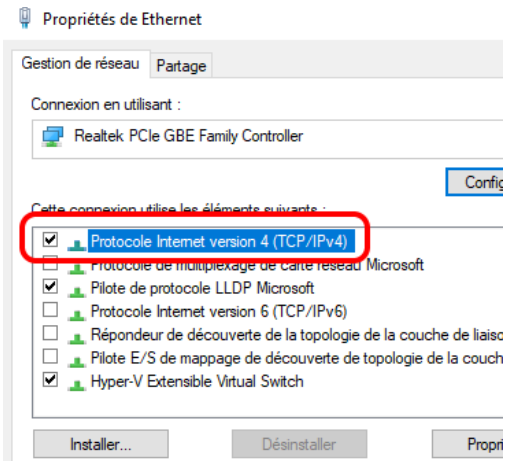
Pour configurer Windows rendez-vous dans le centre de réseau et partage puis dans le gestionnaire de carte :



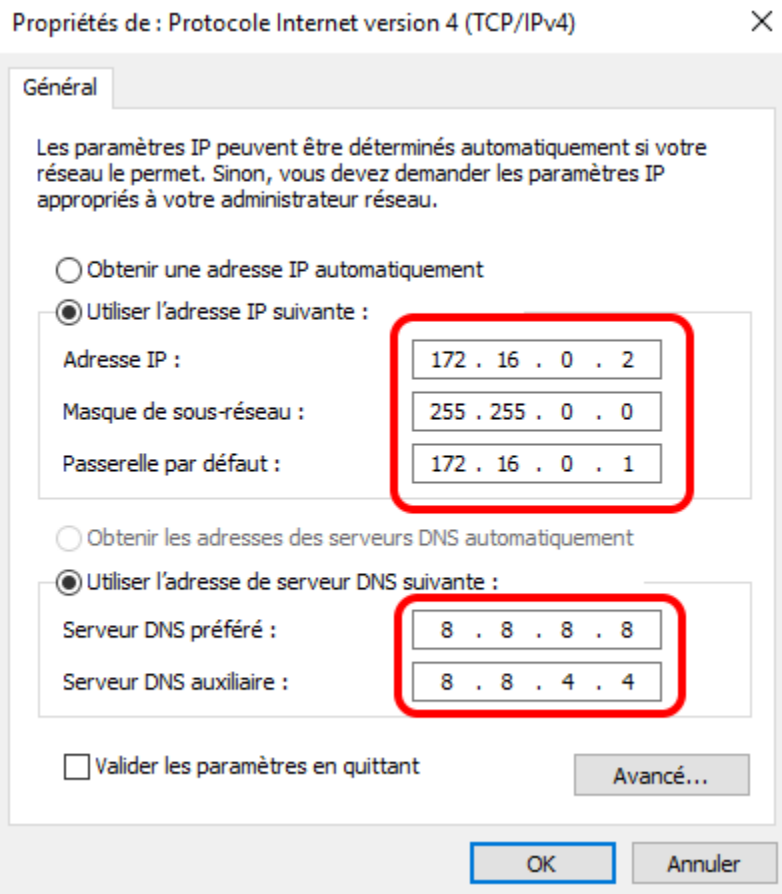
Une fois que vous y êtes, faites un clic droit sur votre carte réseau puis propriété :



Un double clic ici pour ouvrir les paramètres IPV4 :



Puis on renseigne les informations de notre carte pour terminer et on valide :



Si tout est bon vous pouvez passer à la mise en place du VPN sinon reprenez au début du tuto et vérifiez vos configurations.

INSTALLATIONS ET CONFIGURATIONS VPN

8. Installation du serveur VPN

 À partir de maintenant nous ne travaillerons que sur Debian-VPN.

Nous utiliserons OpenVPN comme application VPN.

Voici la liste des commandes à exécuter pour l'installation d'OpenVPN sur Debian-VPN :

```
# apt-get install openvpn easy-rsa
```

Vous faites oui et vous laissez terminer. C'est fini pour l'installation.

9. Configuration du serveur VPN

On se prépare à installer les certificats :

```
# cp -a /usr/share/easy-rsa /etc/openvpn/easy-rsa

# cd /etc/openvpn/easy-ras
```

On nettoie les fichiers inutiles puis on génère les certificats de l'autorité :

```
# source vars

# ./clean-all

# ./build-ca
```

Des informations vous seront demandé, vous pouvez laisser par défaut ou les remplacer :

```
Country Name (2 letter code) [US]:

State or Province Name (full name) [CA]:

Locality Name (eg, city) [SanFrancisco]:

Organization Name (eg, company) [Fort-Funston]:

Organizational Unit Name (eg, section) [MyOrganizationalUnit]:

Common Name (eg, your name or your server's hostname) [Fort-Funston CA]:

Name [EasyRSA]:

Email Address [me@myhost.mydomain]:
```

Ensuite il faut générer la clé Diffie-Hellman qui permet de sécuriser les échanges :

```
# ./build-dh
```

Une fois terminé on génère les certificats pour le serveur :

```
# ./build-key-server srvcert
```

Tout comme l'autre certificat il vous sera demandé des informations que vous pourrez modifier :

```
countryName             :PRINTABLE:'US'

stateOrProvinceName     :PRINTABLE:'CA'

localityName            :PRINTABLE:'SanFrancisco'

organizationName        :PRINTABLE:'Fort-Funston'

organizationalUnitName:PRINTABLE:'MyOrganizationalUnit'

commonName              :PRINTABLE:'debian-facile'

name                    :PRINTABLE:'EasyRSA'

emailAddress            :IA5STRING:'me@myhost.mydomain'
```

Répondez « y » aux 2 questions qui vous seront poser à la fin.

On récupère des fichiers de configuration exemples pour les modifier :

```
# gunzip -c /usr/share/doc/openvpn/examples/sample-config-
files/server.conf.gz > /etc/openvpn/server.conf
```

Il faut maintenant configurer ce fichier de configuration pour nous :

```
# nano /etc/openvpn/server.conf
```

Voici les modifications à faire :

```
#On limite les droits à l'utilisateur nobody et au groupe nogroup. Attention
cela n'est bon que pour les clients qui sont sur linux/unix.
#Pour les clients windows il faut commenter ces deux lignes

user nobody
group nogroup
---
#On limite le nombres de client simultanées

max-clients 5
---

#On active la compression ça permet de gagner de la bande passante et la
vitesse pour tout ce qui est binaire.
#Attention il faut aussi que cette ligne soit dans le fichier de
configuration du client openvpn

comp-lzo
---

ca /etc/openvpn/easy-rsa/keys/ca.crt
cert /etc/openvpn/easy-rsa/keys/srvcert.crt
key /etc/openvpn/easy-rsa/keys/srvcert.key  # This file should be kept secret
---

dh /etc/openvpn/easy-rsa/keys/dh2048.pem
---

push "redirect-gateway def1 bypass-dhcp"
push "dhcp-option DNS 8.8.8.8"
push "dhcp-option DNS 8.8.4.4"
```

Maintenant on test la configuration en stoppant le service puis en démarrant notre configuration :

```
# service openvpn stop

# Openvpn /etc/openvpn/server.conf

# service openvpn start
```

Si vous obtenez « Initialization Sequence Completed » à la deuxième commande c'est que la configuration est bonne !

Nous allons maintenant générer les certificats pour notre client VPN :

```
# cd /etc/openvpn/easy-rsa

# source vars

# ./build-key clientCerti
```

Comme pour le certificat serveur il vous sera demandé des informations que vous pourrez modifier :

```
countryName             :PRINTABLE:'US'

stateOrProvinceName     :PRINTABLE:'CA'

localityName            :PRINTABLE:'SanFrancisco'

organizationName        :PRINTABLE:'Fort-Funston'

organizationalUnitName:PRINTABLE:'MyOrganizationalUnit'

commonName              :PRINTABLE:'debianFacile'

name                    :PRINTABLE:'EasyRSA'

emailAddress            :IA5STRING:'me@myhost.mydomain'
```

Répondez « y » aux 2 questions qui vous seront poser à la fin.

Maintenant que vous avez vos certificats pour le client gardez les de côté pour les mettre sur votre machine client.

Les certificats sont : « ca.crt », « clientCerti.key » et « clientCerti.crt »

Il faut maintenant faire du NAT sur nos Debian pour que l'on puisse simuler une connexion internet.


Cette commande est à faire sur vos deux routeurs Debian en mettant comme interface celle qui est dans le réseau 10.

```
# iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
```

Voilà la configuration de Debian-VPN est terminé.

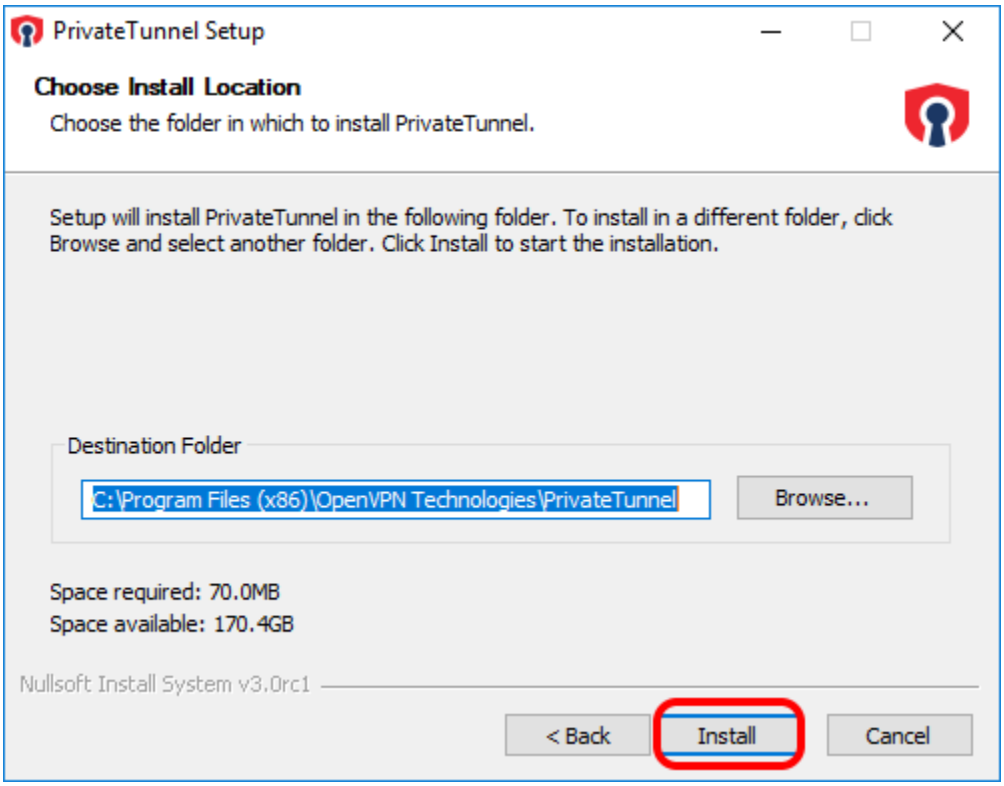
10. Installation du client VPN

Nous travaillons maintenant sur notre machine Windows.

Téléchargez OpenVPN pour Windows à cette adresse : https://openvpn.net/index.php/open-source/downloads.html

Puis exécutez-le.

Vous pouvez changer le chemin d'installation ou le laisser par défaut, ce que je vais faire. Puis vous faites « Install » :



11. Configuration du client VPN

Il faut aller dans le dossier « C:\Program Files (x86)\OpenVPN\config\ » où nous allons créer notre fichier de configuration.

Créer un fichier avec l'extension « .ovpn ».

Dans ce fichier mettez cette configuration que vous pouvez modifier en fonction de que vous avez mis coté serveur :

```
remote 10.10.10.254 1193

client
dev tun
proto tcp
nobind
cipher AES-256-CBC
comp-lzo
auth-user-pass
tls-client
persist-key
persist-tun
persist-remote-ip
verb 3
pull
<cert>
-----BEGIN CERTIFICATE-----
VOTRE VERTIFICAT « clientCerti.crt »
-----END CERTIFICATE-----
</cert>
<key>
-----BEGIN RSA PRIVATE KEY-----
VOTRE VERTIFICAT « clientCerti.key »
-----END RSA PRIVATE KEY-----
</key>
<ca>
-----BEGIN CERTIFICATE-----
VOTRE VERTIFICAT « ca.crt »
-----END CERTIFICATE-----
</ca>
```

Ce qui est en rouge est à remplacer par les clés de certificat qui sont dans les fichier que vous avez normalement mis de côté comme je l'ai dit 😉.

Maintenant Dans le plateau de la barre des tâches dans le coin inférieur droit de l'écran, faites click du bouton droit sur l'icône OpenVPN GUI et choisissez votre fichier de configuration et faite « connecter ».

Voila maintenant vôtres client VPN et connecté à votre serveur PVN.
J'espère que ce tuto vous aura aider et merci d'avoir lu jusqu'au bout 😊