

Projet VPN Maison:

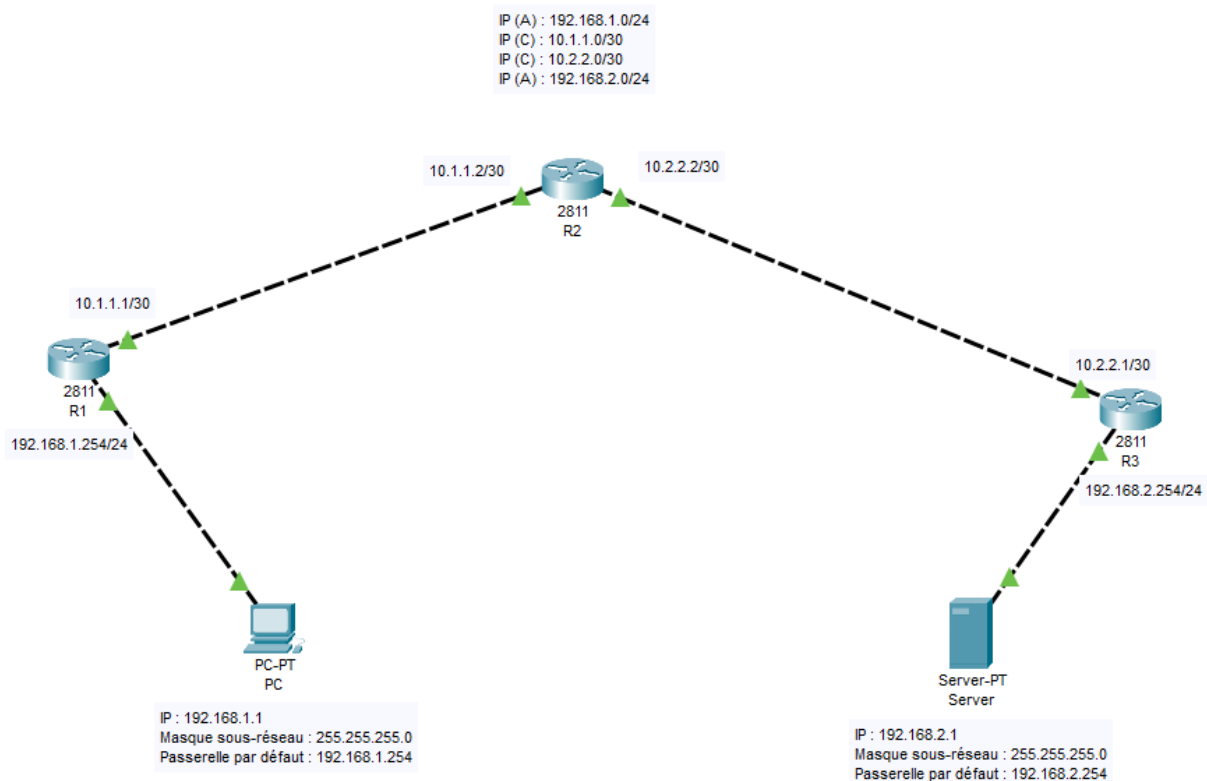
Explications générales du projet :

Le but de ce projet est de créer une connexion privée sécurisée accessible depuis un point distant via Internet. Les attendus étaient d'avoir une machine servant de serveur VPN avec un appareil pouvant s'y connecter par le biais d'un réseau externe tout en respectant les normes de sécurité et de confidentialité au sein des transmissions de données durant la connexion.

Pour se faire, nous avons décidé d'utiliser une Freebox en guise de routeur connecté à Internet ainsi qu'un ordinateur possédant Windows 11 pour le serveur VPN.

Avant de débiter le projet, nous avons décider de le réaliser sous forme d'une simulation à l'aide de Cisco Packet Tracer.

Simulation sur Cisco Packet Tracer :



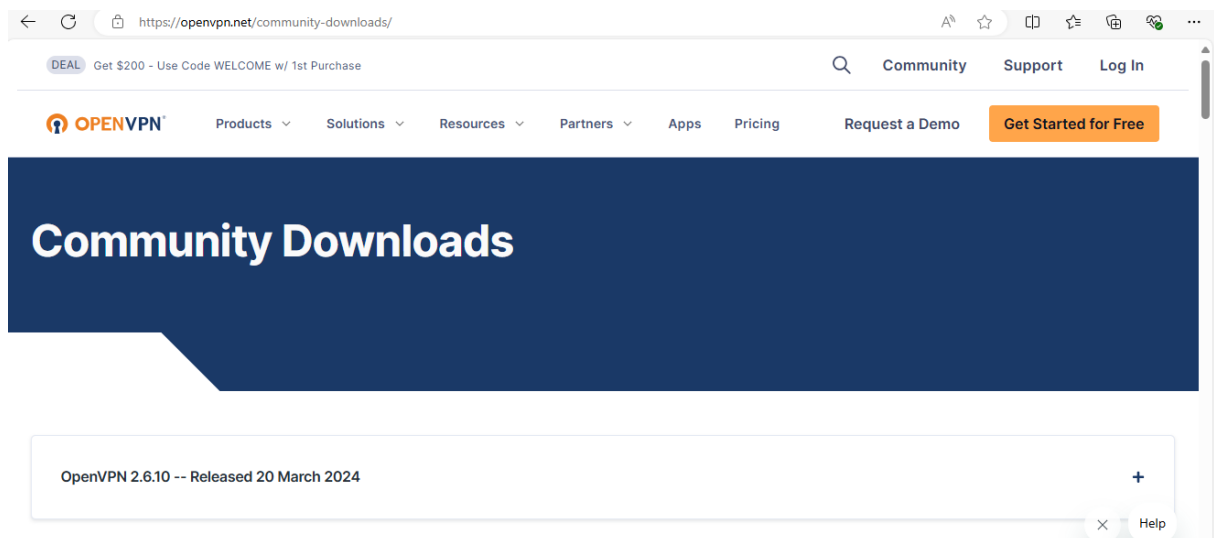
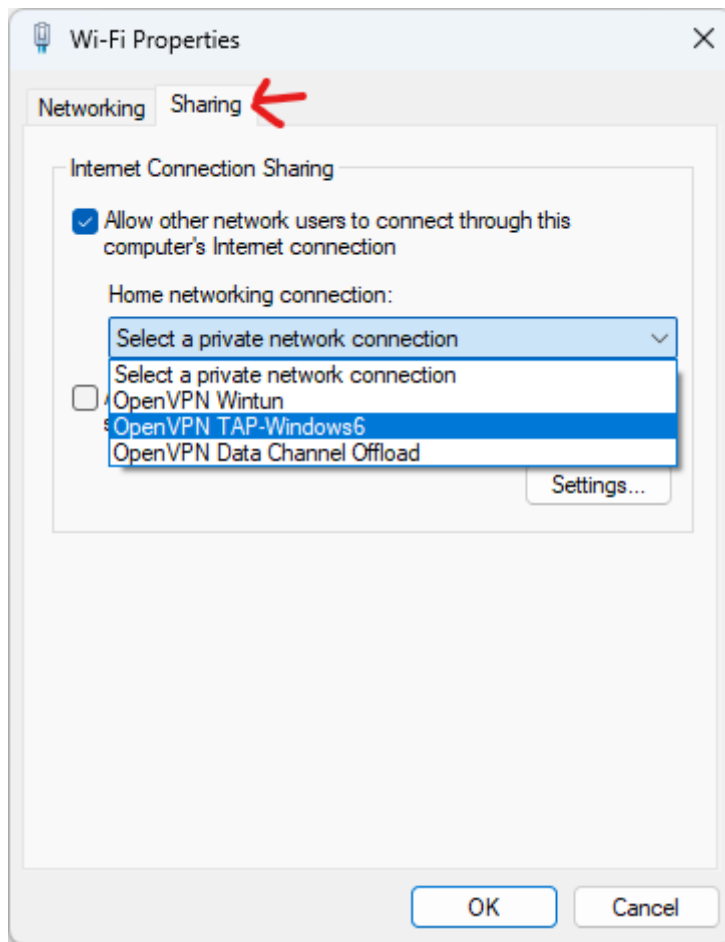
Configuration sur cette simulation :

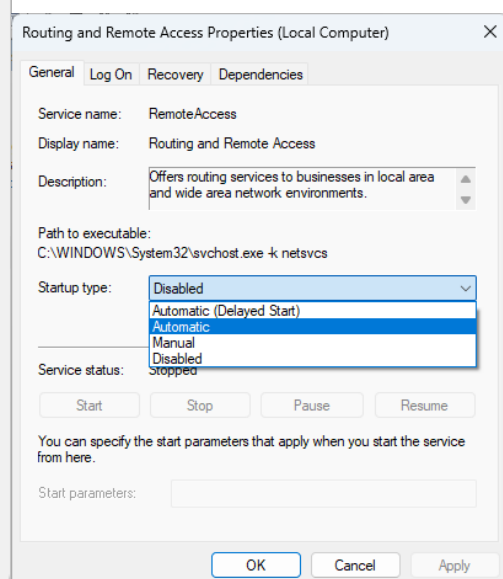
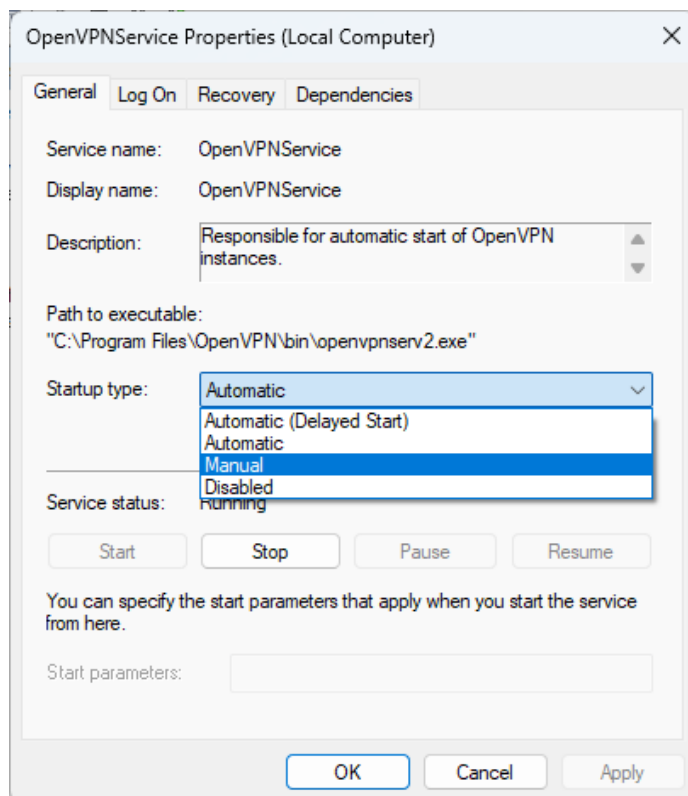
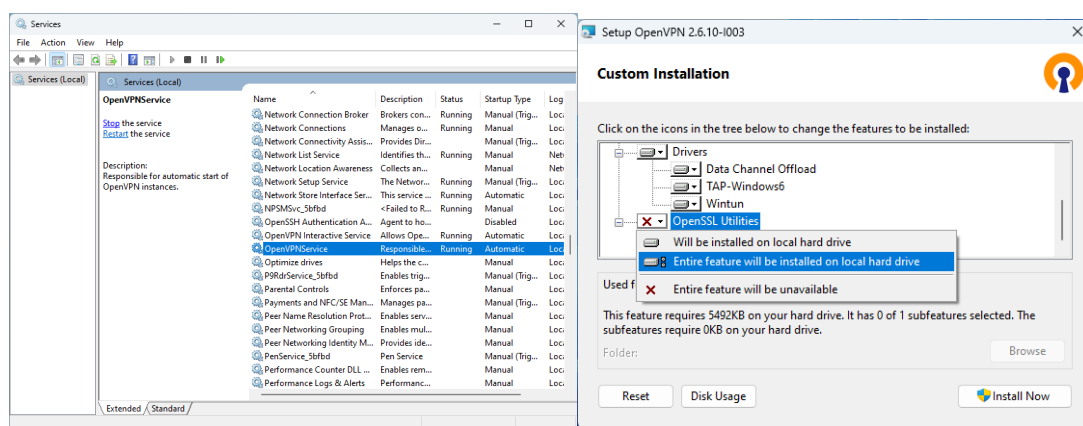
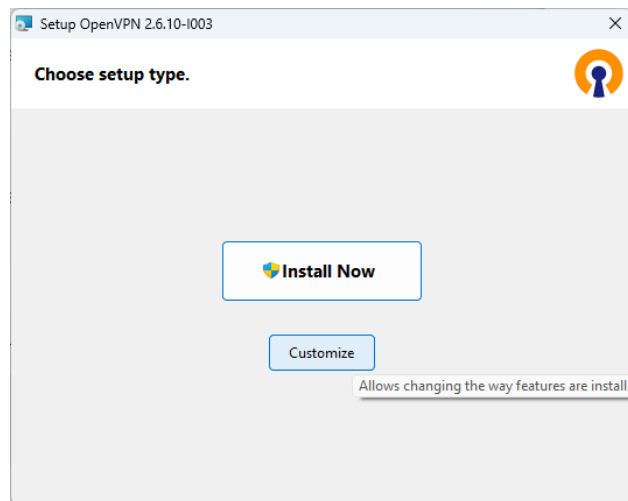
Nous avons débuté par la mise en place d'un réseau basique contenant un ordinateur, un serveur et trois routeurs où le premier sous-réseau représente le réseau de l'utilisateur avec son ordinateur et son routeur à domicile, un routeur central reliant les deux sous- réseaux et le réseau d'entreprise contenant un routeur avec le serveur du VPN.

Pour se faire, il fallait réaliser l'adressage IP ainsi que la mise en place des masques sous-réseau et des passerelles par défaut. Pour les routeurs, il fallait configurer les ports et les routes. Une fois le réseau configuré, il fallait passer à l'aspect de la tunnelisation. On a donc configuré le chiffrement ainsi que le hachage des données via le protocole ISAKMP pour ensuite passer à la configuration IP Sec et à la création d'une ACL à partir des adresses IP.

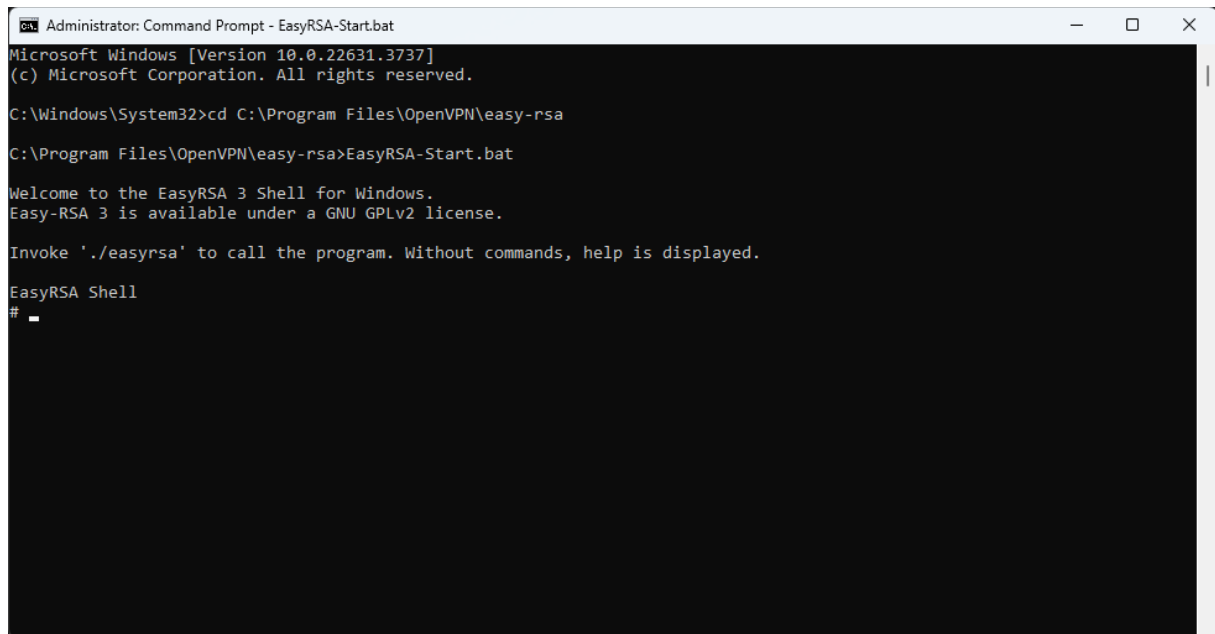
Mise en place physique du VPN :

Pour débiter la création du VPN, nous avons mis en place le serveur VPN en configurant son adresse IP par le biais du logiciel Open VPN.





Nous sommes ensuite passés à la génération des clés et des certificats pour les clients à l'aide de Easy RSA.



```
Administrator: Command Prompt - EasyRSA-Start.bat
Microsoft Windows [Version 10.0.22631.3737]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd C:\Program Files\OpenVPN\easy-rsa

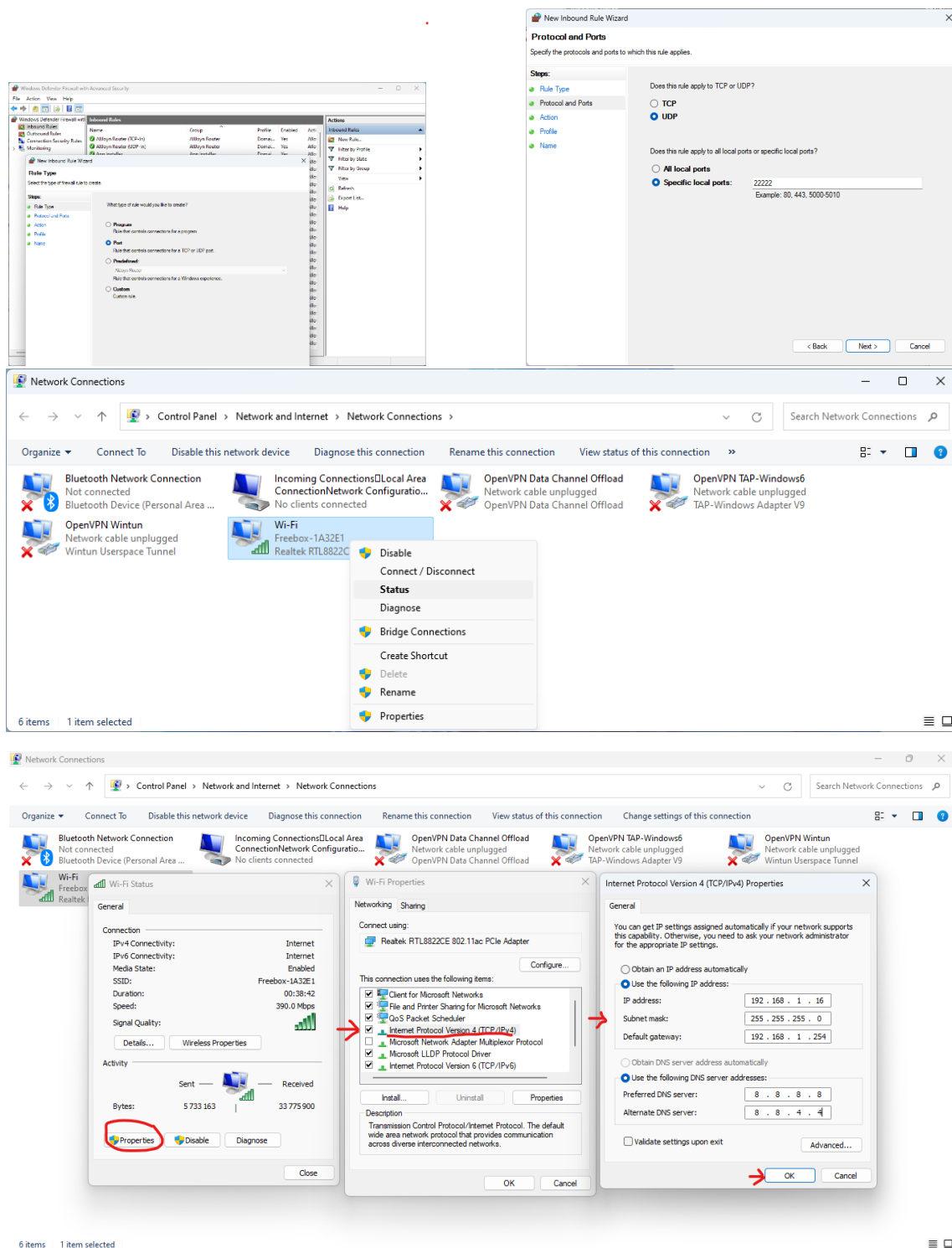
C:\Program Files\OpenVPN\easy-rsa>EasyRSA-Start.bat

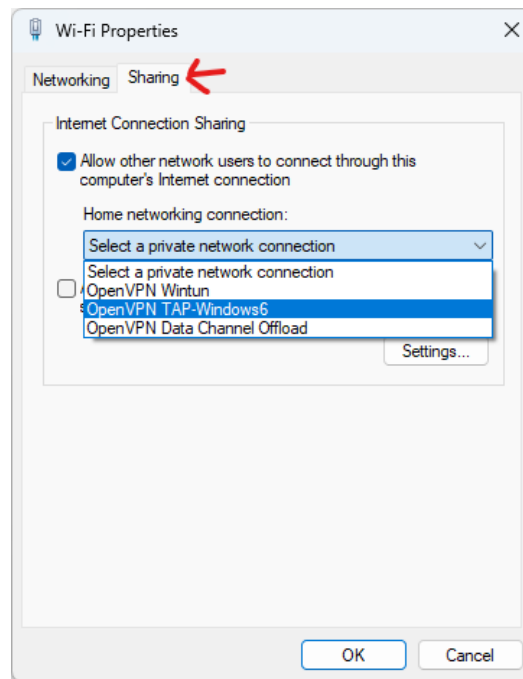
Welcome to the EasyRSA 3 Shell for Windows.
Easy-RSA 3 is available under a GNU GPLv2 license.

Invoke './easysrsa' to call the program. Without commands, help is displayed.

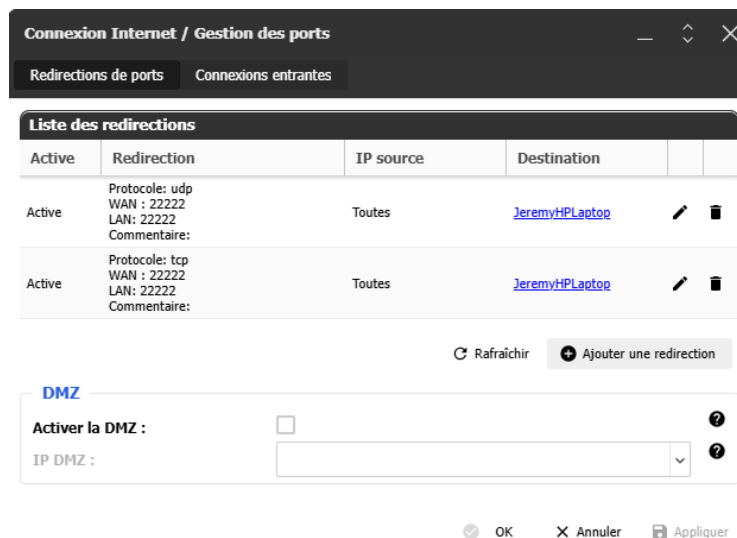
EasyRSA Shell
# _
```

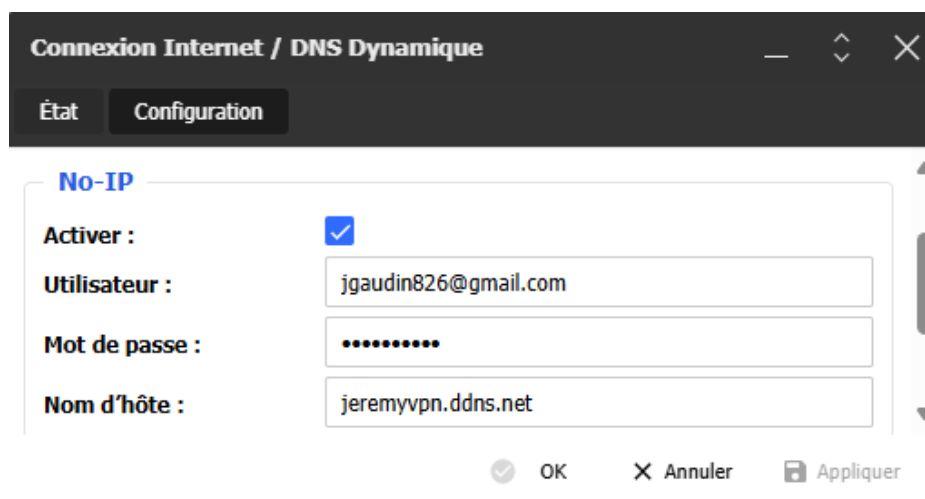
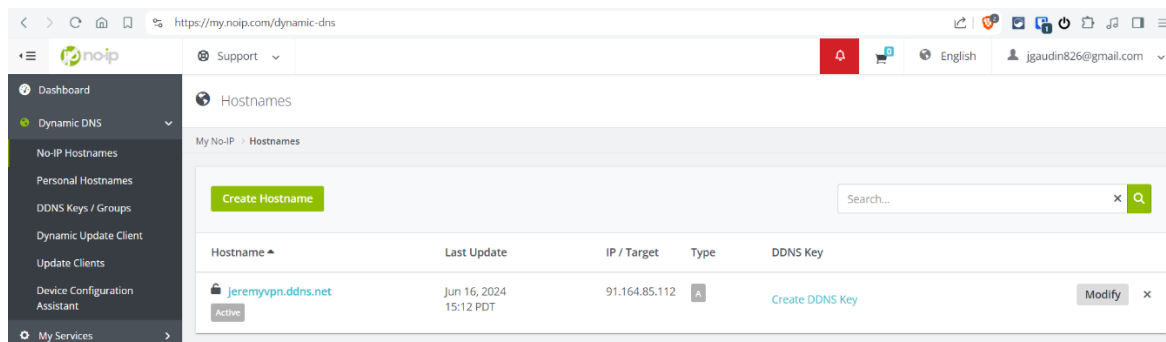
On a ensuite ouvert les ports 22222 et le port 445 au sein des règles du pare-feu de l'ordinateur avant de débiter la configuration du réseau en assignant une adresse IP au serveur et en activant le paramètre « file sharing » tout en sélectionnant Open VPN pour sa prise en charge.



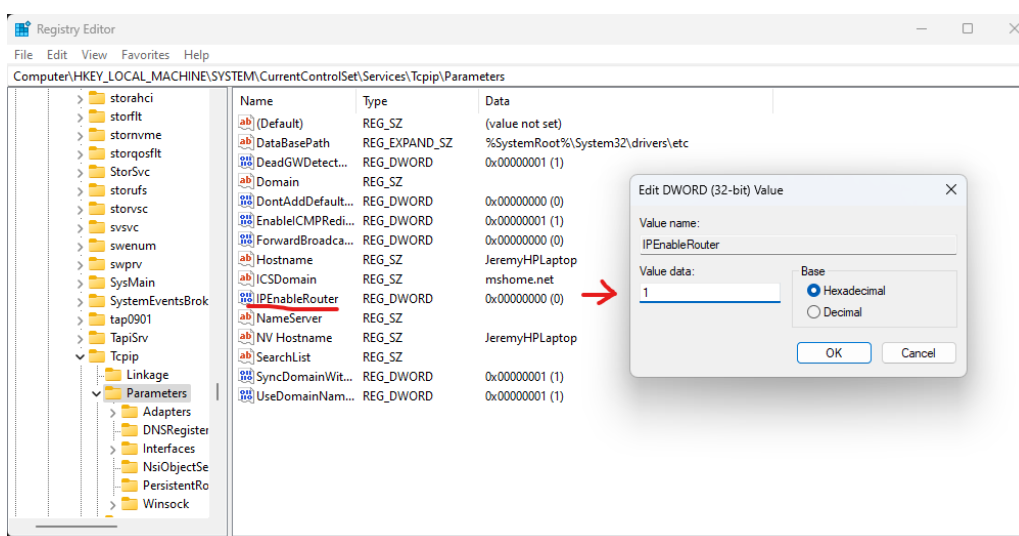


Il était également nécessaire de configurer une redirection de port sur le routeur pour accéder au serveur puis de mettre en place un DDNS en utilisant No IP.











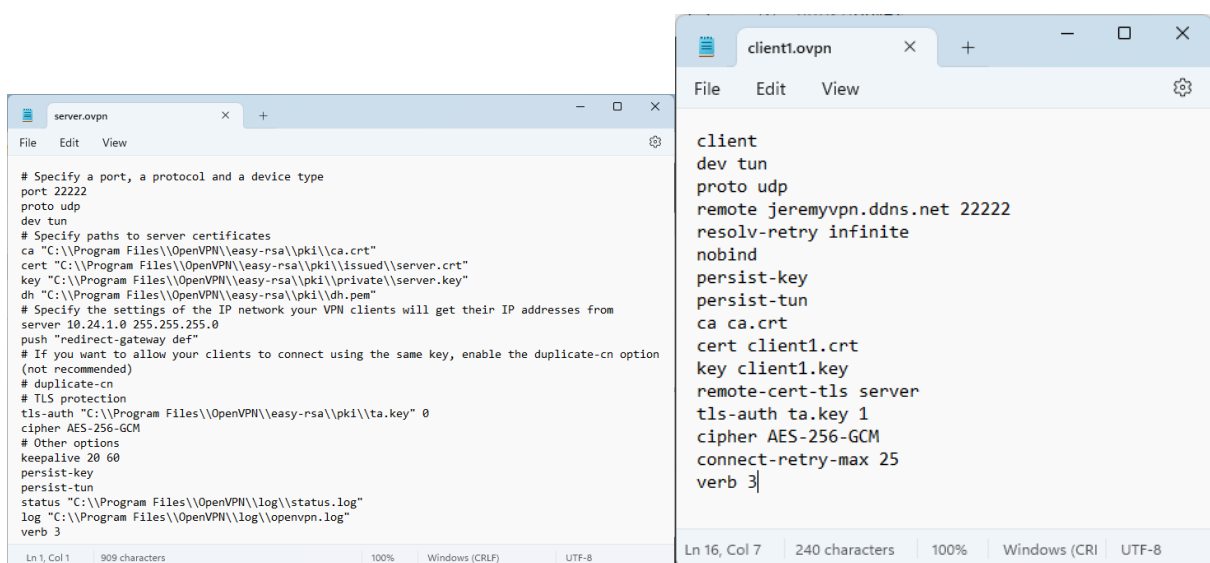
On a ouvert le « Registry Editor » afin d'activer le paramètre « IPEnableRouter » qui est nécessaire au fonctionnement de notre VPN pour passer à l'ouverture de la connexion avec l'interface Open VPN GUI.



On a ensuite récupéré les fichiers de connexion pour le client (credentials, certificats et clés) afin de les stocker dans un dossier client.

Name	Date modified	Type	Size
 ca	19/06/2024 14:37	Security Certificate	2 KB
 client1	19/06/2024 14:38	Security Certificate	5 KB
 client1.key	19/06/2024 14:38	KEY File	2 KB
 dh.pem	19/06/2024 14:39	PEM File	1 KB
 ta.key	19/06/2024 14:40	KEY File	1 KB
 client1	19/06/2024 15:11	OpenVPN Config ...	1 KB

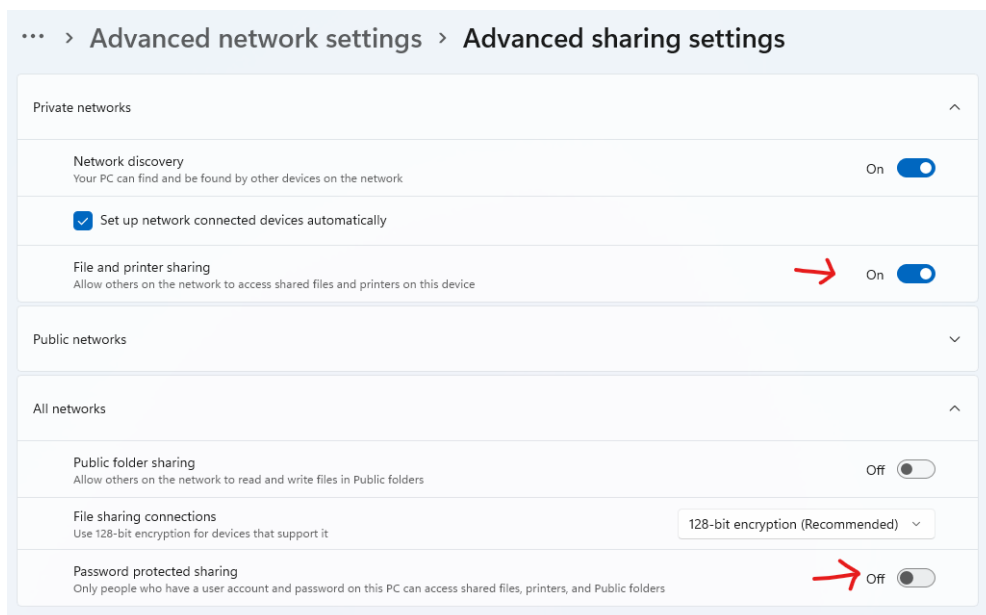
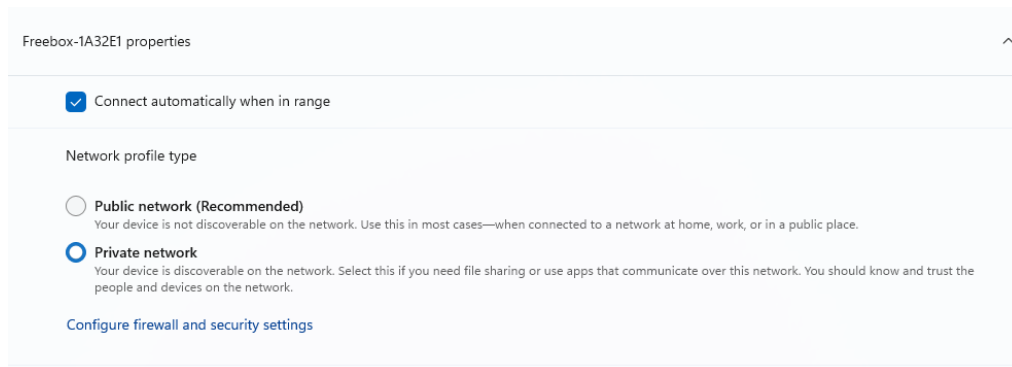
Vient ensuite la configuration du client au sein du VPN en prenant en compte le port et l'adresse IP.



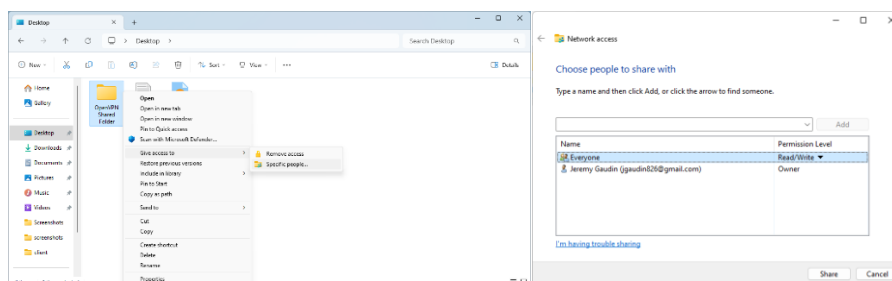
```
# Specify a port, a protocol and a device type
port 22222
proto udp
dev tun
# Specify paths to server certificates
ca "C:\Program Files\OpenVPN\easy-rsa\pk1\ca.crt"
cert "C:\Program Files\OpenVPN\easy-rsa\pk1\issued\server.crt"
key "C:\Program Files\OpenVPN\easy-rsa\pk1\private\server.key"
dh "C:\Program Files\OpenVPN\easy-rsa\pk1\dh.pem"
# Specify the settings of the IP network your VPN clients will get their IP addresses from
server 10.24.1.0 255.255.255.0
push "redirect-gateway def"
# If you want to allow your clients to connect using the same key, enable the duplicate-cn option
(not recommended)
# duplicate-cn
# TLS protection
tls-auth "C:\Program Files\OpenVPN\easy-rsa\pk1\ta.key" 0
cipher AES-256-GCM
# Other options
keepalive 20 60
persist-key
persist-tun
status "C:\Program Files\OpenVPN\log\status.log"
log "C:\Program Files\OpenVPN\log\openvpn.log"
verb 3
```

```
client
dev tun
proto udp
remote jeremyvpn.ddns.net 22222
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert client1.crt
key client1.key
remote-cert-tls server
tls-auth ta.key 1
cipher AES-256-GCM
connect-retry-max 25
verb 3
```

Il fallait passer le réseau en privé et aller dans les paramètres avancés pour activer tous les paramètres du réseau privé.



On clôture le tout avec la création du dossier partagé sur le réseau et en sa mise en accès avec le VPN en activant le partage dans les propriétés.



Autre point important, pour éviter que le serveur n'entre en « hibernation », il faut régler les paramètres au sein des « Power Options »

