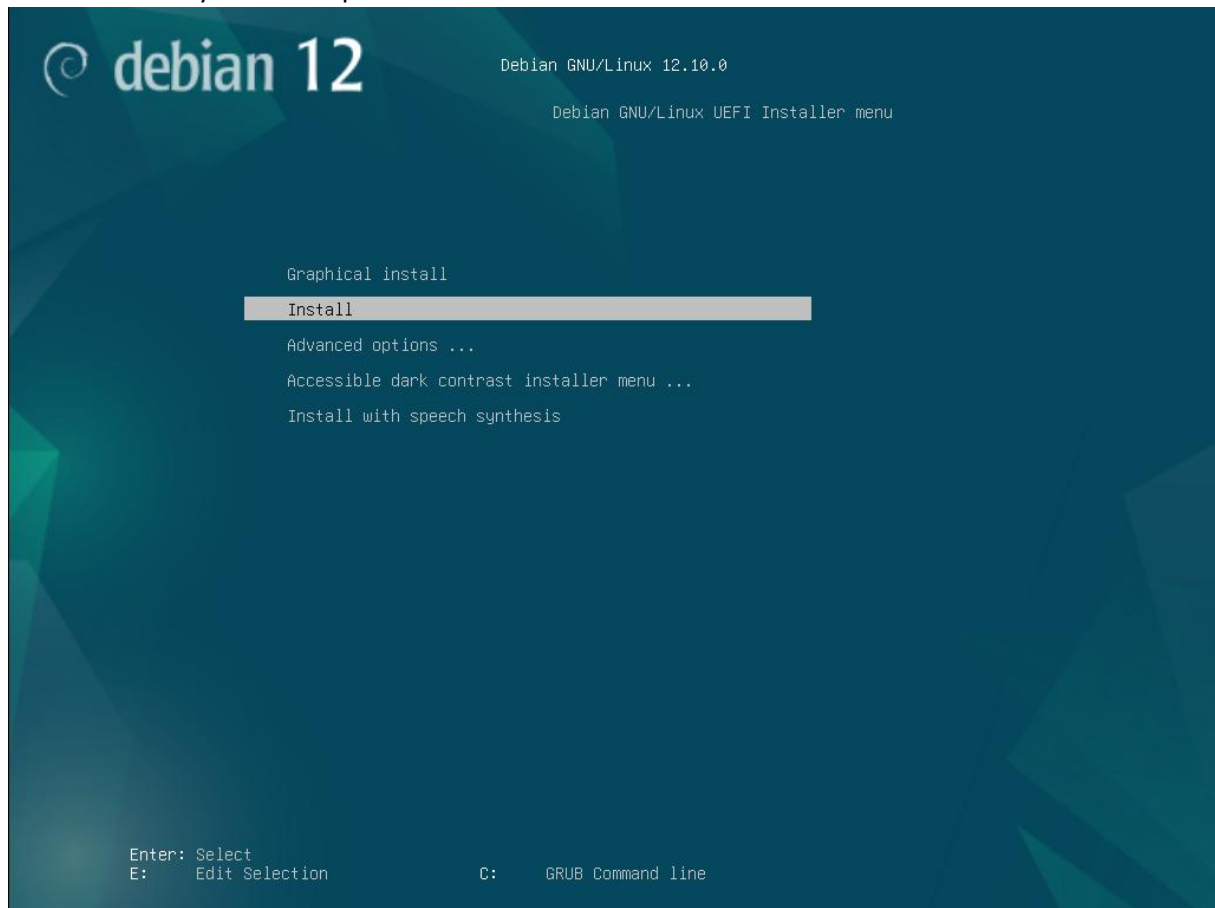


Installation et configuration Wireguard Debian :

Installation du système d'exploitation :



Attribution d'un IP statique :

[[!]] Configurer le réseau

L'adresse IP est propre à une machine et peut être constituée de :

- * quatre nombres séparés par des points (IPv4) ;
- * des blocs de caractères hexadécimaux séparés par le caractère « deux-points » (IPv6).

Il est également possible d'ajouter un masque de sous-réseau au format CIDR (par exemple « /24 »).

Si vous ne savez pas quoi indiquer, veuillez consulter l'administrateur de votre réseau.

Adresse IP :

192.168.21.200

<Revenir en arrière> <Continuer>

<Tab> déplacement; <Espace> sélection; <Entrée> activation des boutons

Masque sous réseaux :

!!! Configurer le réseau

Le masque-réseau sert à déterminer les machines locales du réseau. Si vous ne connaissez pas cette valeur, consultez votre administrateur. Le masque-réseau est une série de quatre nombres séparés par des points.

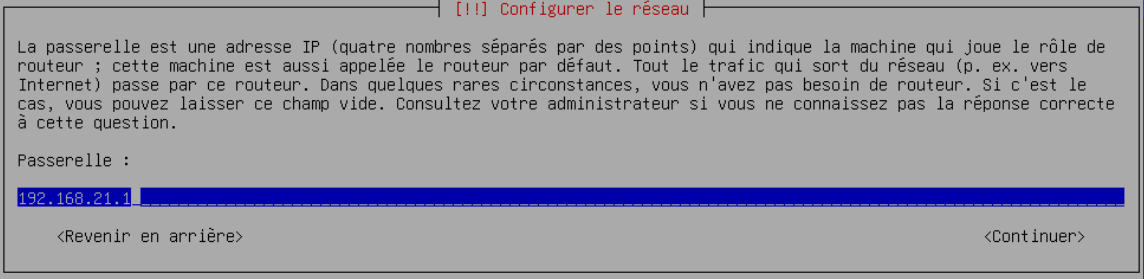
Valeur du masque-réseau :

255.255.255.0

<Revenir en arrière><Continuer>

<Tab> déplacement; <Espace> sélection; <Entrée> activation des boutons

Connection à notre routeur via la passerelle :



The screenshot shows a window titled "Configurer le réseau" (Configure the network). It contains a paragraph explaining the gateway (passerelle) as an IP address. Below the text is a label "Passerelle :" followed by a text input field containing "192.168.21.1". At the bottom of the window are two buttons: "<Revenir en arrière" (Back) and "<Continuer" (Continue). The window is set against a blue background.

[!!] Configurer le réseau

La passerelle est une adresse IP (quatre nombres séparés par des points) qui indique la machine qui joue le rôle de routeur ; cette machine est aussi appelée le routeur par défaut. Tout le trafic qui sort du réseau (p. ex. vers Internet) passe par ce routeur. Dans quelques rares circonstances, vous n'avez pas besoin de routeur. Si c'est le cas, vous pouvez laisser ce champ vide. Consultez votre administrateur si vous ne connaissez pas la réponse correcte à cette question.

Passerelle :

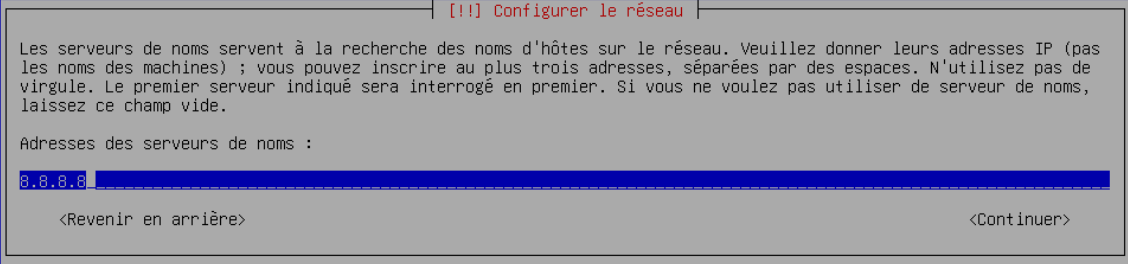
192.168.21.1

<Revenir en arrière

<Continuer

<Tab> déplacement; <Espace> sélection; <Entrée> activation des boutons

Adresse de DNS :



The screenshot shows a network configuration window with a title bar that reads "[[!]] Configurer le réseau". The window contains the following text:

Les serveurs de noms servent à la recherche des noms d'hôtes sur le réseau. Veuillez donner leurs adresses IP (pas les noms des machines) ; vous pouvez inscrire au plus trois adresses, séparées par des espaces. N'utilisez pas de virgule. Le premier serveur indiqué sera interrogé en premier. Si vous ne voulez pas utiliser de serveur de noms, laissez ce champ vide.

Adresses des serveurs de noms :

Below this text is a text input field containing "0.0.0.0".

At the bottom of the window are two buttons: "<Revenir en arrière" on the left and "<Continuer>" on the right.

At the bottom of the blue background area, there is a line of text: "<Tab> déplacement; <Espace> sélection; <Entrée> activation des boutons".

Nom de la machine :

[[!]] Configurer le réseau

Veillez indiquer le nom de ce système.

Le nom de machine est un mot unique qui identifie le système sur le réseau. Si vous ne connaissez pas ce nom, demandez-le à votre administrateur réseau. Si vous installez votre propre réseau, vous pouvez mettre ce que vous voulez.

Nom de machine :

debian

<Revenir en arrière>

<Continuer>

<Tab> déplacement; <Espace> sélection; <Entrée> activation des boutons

Mise en place du mot de passe root :

[[!]] Créer les utilisateurs et choisir les mots de passe

Vous devez choisir un mot de passe pour le superutilisateur, le compte d'administration du système. Un utilisateur malintentionné ou peu expérimenté qui aurait accès à ce compte peut provoquer des désastres. En conséquence, ce mot de passe ne doit pas être facile à deviner, ni correspondre à un mot d'un dictionnaire ou vous être facilement associé.

Un bon mot de passe est composé de lettres, chiffres et signes de ponctuation. Il devra en outre être changé régulièrement.

Le superutilisateur (« root ») ne doit pas avoir de mot de passe vide. Si vous laissez ce champ vide, le compte du superutilisateur sera désactivé et le premier compte qui sera créé aura la possibilité d'obtenir les privilèges du superutilisateur avec la commande « sudo ».

Par sécurité, rien n'est affiché pendant la saisie.

Mot de passe du superutilisateur (« root ») :

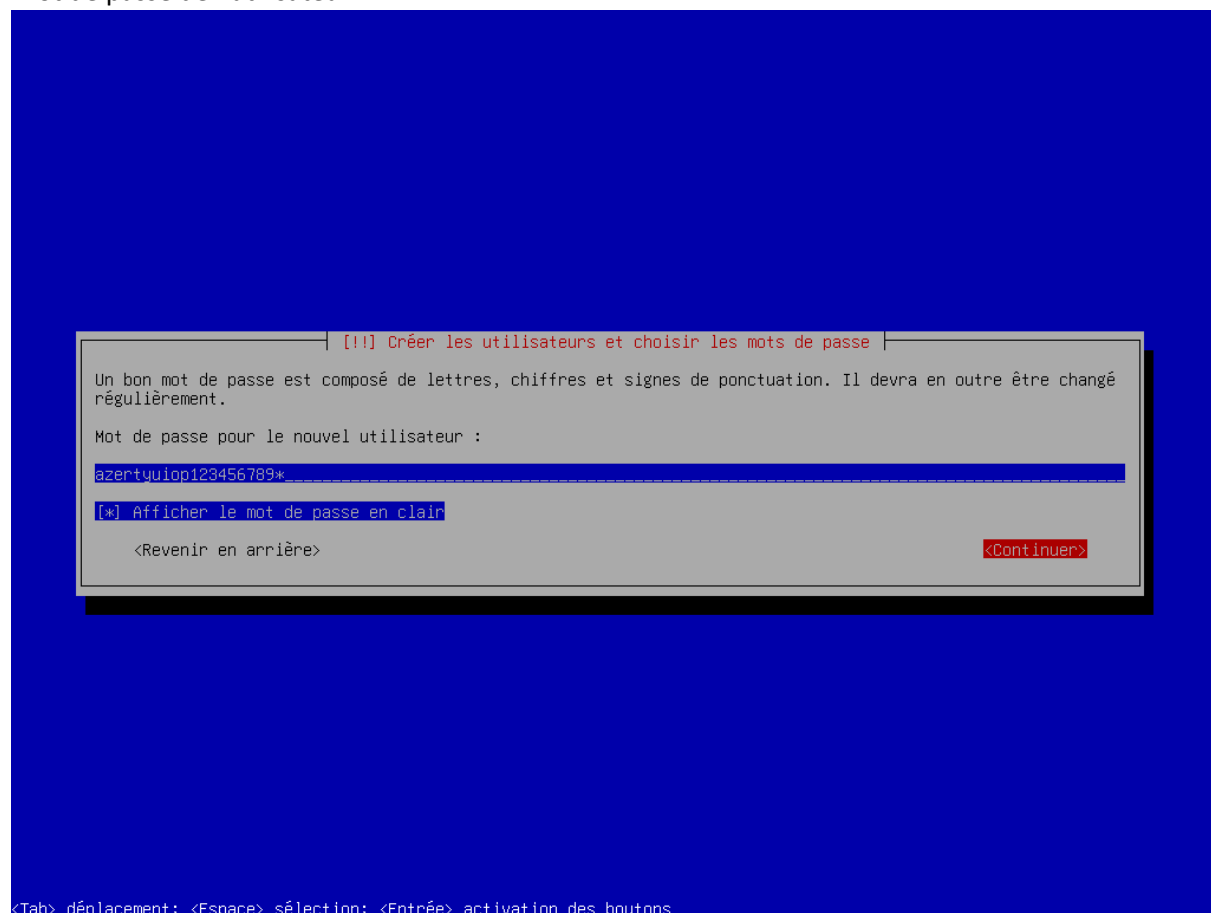
azertyuiop123456789*

☐ Afficher le mot de passe en clair

<Revenir en arrière><Continuer>

<Tab> déplacement; <Espace> sélection; <Entrée> activation des boutons

Mot de passe de l'utilisateur :



The screenshot shows a dialog box titled "[!!] Créer les utilisateurs et choisir les mots de passe". Inside the dialog, there is a text instruction: "Un bon mot de passe est composé de lettres, chiffres et signes de ponctuation. Il devra en outre être changé régulièrement." Below this, it says "Mot de passe pour le nouvel utilisateur :". A text input field contains the password "azertyuiop123456789*". Below the input field, there is a checkbox labeled "[*] Afficher le mot de passe en clair". At the bottom left of the dialog is a button labeled "<Revenir en arrière>" and at the bottom right is a button labeled "<Continuer>".

[!!] Créer les utilisateurs et choisir les mots de passe

Un bon mot de passe est composé de lettres, chiffres et signes de ponctuation. Il devra en outre être changé régulièrement.

Mot de passe pour le nouvel utilisateur :

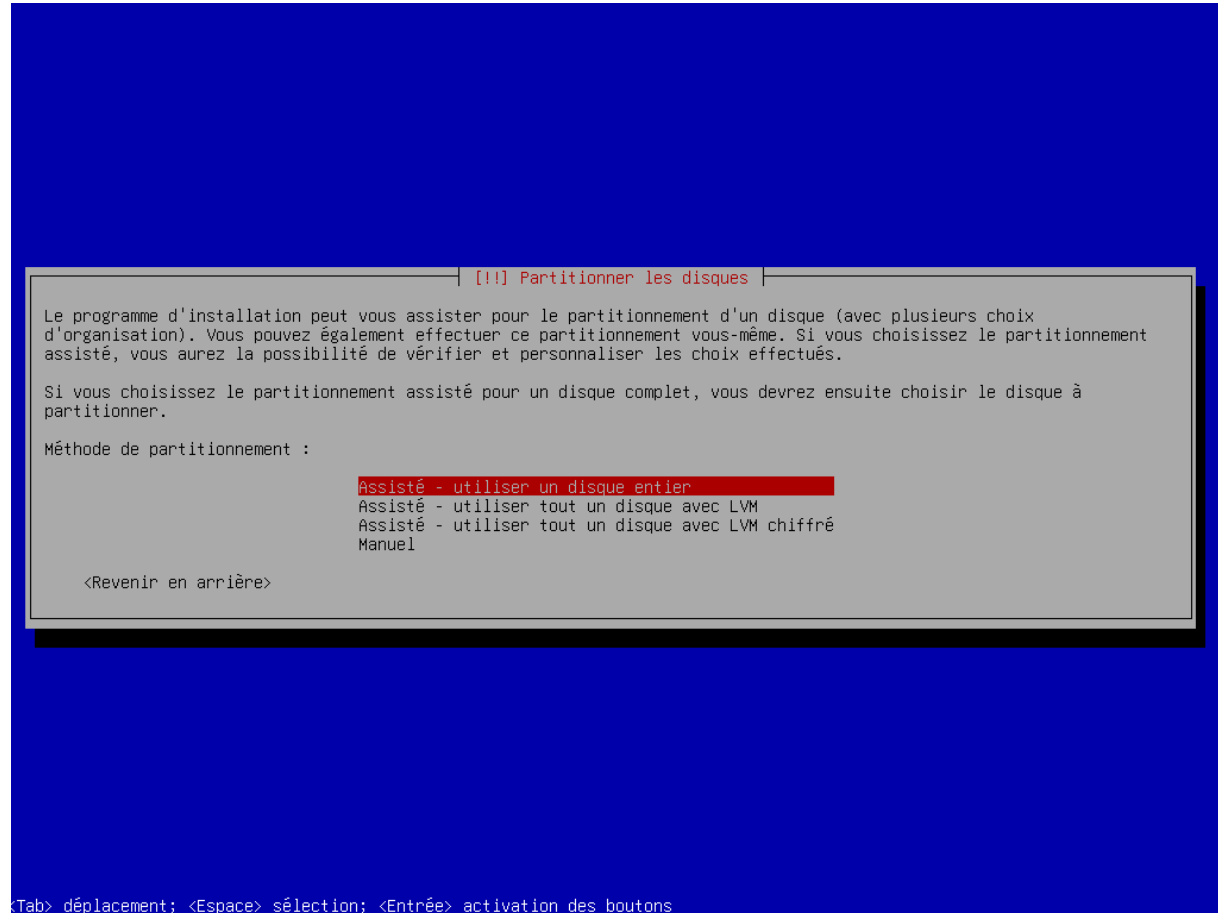
azertyuiop123456789*

[*] Afficher le mot de passe en clair

<Revenir en arrière> <Continuer>

<Tab> déplacement; <Espace> sélection; <Entrée> activation des boutons

Configuration de la partition :



[!!] Partitionner les disques

Veillez noter que toutes les données du disque choisi seront effacées mais pas avant d'avoir confirmé que vous souhaitez réellement effectuer les modifications.

Disque à partitionner :

SCSI1 (0,0,0) (sda) - 21.5 GB Msft Virtual Disk

<Revenir en arrière>

<Tab> déplacement; <Espace> sélection; <Entrée> activation des boutons

[!!] Partitionner les disques

Veillez noter que toutes les données du disque choisi seront effacées mais pas avant d'avoir confirmé que vous souhaitez réellement effectuer les modifications.

Disque à partitionner :

SCSI1 (0,0,0) (sda) - 21.5 GB Msft Virtual Disk

<Revenir en arrière>

<Tab> déplacement; <Espace> sélection; <Entrée> activation des boutons

[!!] Partitionner les disques

Voici la table des partitions et les points de montage actuellement configurés. Vous pouvez choisir une partition et modifier ses caractéristiques (système de fichiers, point de montage, etc.), un espace libre pour créer une nouvelle partition ou un périphérique pour créer sa table des partitions.

Partitionnement assisté
Configurer le RAID avec gestion logicielle
Configurer le gestionnaire de volumes logiques (LVM)
Configurer les volumes chiffrés
Configurer les volumes iSCSI

SCSI1 (0,0,0) (sda) - 21.5 GB Msft Virtual Disk

	1.0 MB			Espace libre	
n° 1	536.9 MB	B	f	ESP	
n° 2	19.9 GB		f	ext4	/
n° 3	1.0 GB		f	swap	swap
	1.0 MB			Espace libre	

Annuler les modifications des partitions
Terminer le partitionnement et appliquer les changements

<Revenir en arrière>

<E1> aide; <Tab> déplacement; <Espace> sélection; <Entrée> activation boutons

[!!] Partitionner les disques

Si vous continuez, les modifications affichées seront écrites sur les disques. Dans le cas contraire, vous pourrez faire d'autres modifications.

Les tables de partitions des périphériques suivants seront modifiées :
SCSI1 (0,0,0) (sda)

Les partitions suivantes seront formatées :
partition n° 1 sur SCSI1 (0,0,0) (sda) de type ESP
partition n° 2 sur SCSI1 (0,0,0) (sda) de type ext4
partition n° 3 sur SCSI1 (0,0,0) (sda) de type swap

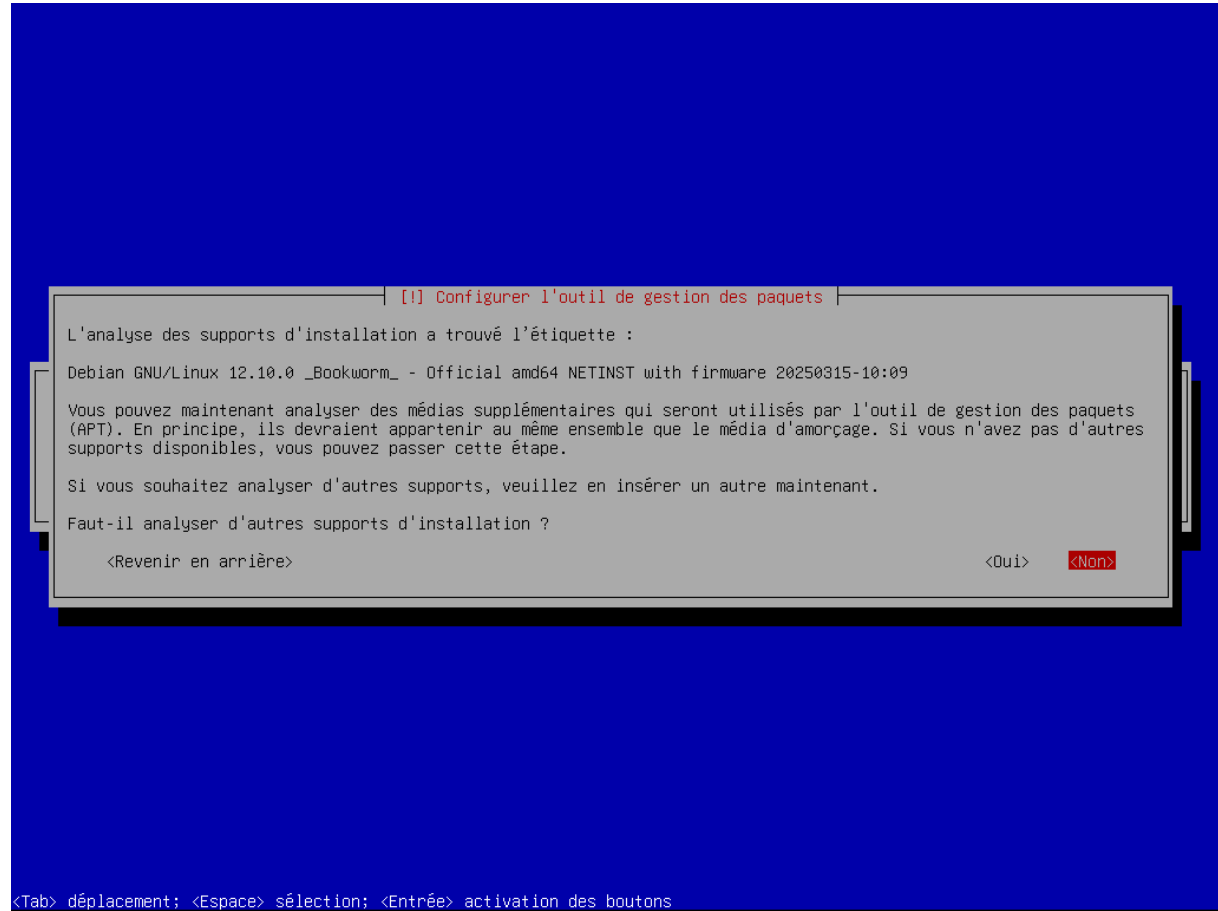
Faut-il appliquer les changements sur les disques ?

<Oui>

<Non>

<Tab> déplacement; <Espace> sélection; <Entrée> activation des boutons

Configuration l'outil de gestion des paquets :



[!] Configurer l'outil de gestion des paquets

Veuillez choisir un miroir de l'archive Debian. Vous devriez utiliser un miroir situé dans votre pays ou votre région si vous ne savez pas quel miroir possède la meilleure connexion Internet avec vous.

Généralement, deb.debian.org est un choix pertinent.

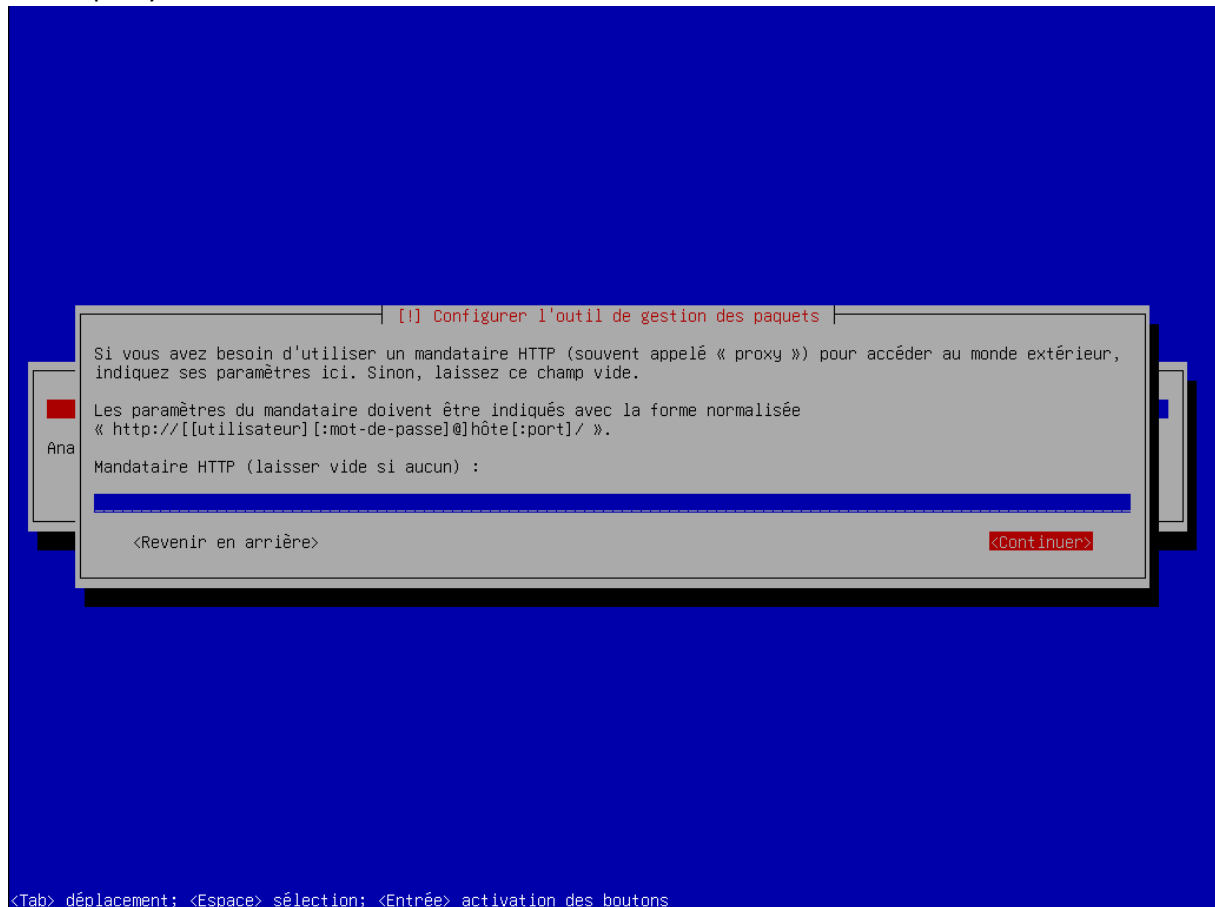
Miroir de l'archive Debian :

deb.debian.org
ftp.fr.debian.org
debian.proxad.net
ftp.ec-m.fr
deb-mir1.naitways.net
miroir.univ-lorraine.fr
ftp.u-picardie.fr
ftp.u-strasbg.fr
mirror.plusserver.com
debian.univ-tlse2.fr
ftp.univ-pau.fr
mirrors.ircam.fr
ftp.lip6.fr
debian.polytech-lille.fr
debian.apt-mirror.de
debian.obspm.fr
mirror.johnnybegood.fr
apt.tetaneutral.net
mirror.gitoyen.net
debian.mirrors.ovh.net
debian-archive.trafficmanager.net

<Revenir en arrière>

<Tab> déplacement; <Espace> sélection; <Entrée> activation des boutons

Pas de proxy donc on ne met rien :



[!] Configurer l'outil de gestion des paquets

Si vous avez besoin d'utiliser un mandataire HTTP (souvent appelé « proxy ») pour accéder au monde extérieur, indiquez ses paramètres ici. Sinon, laissez ce champ vide.

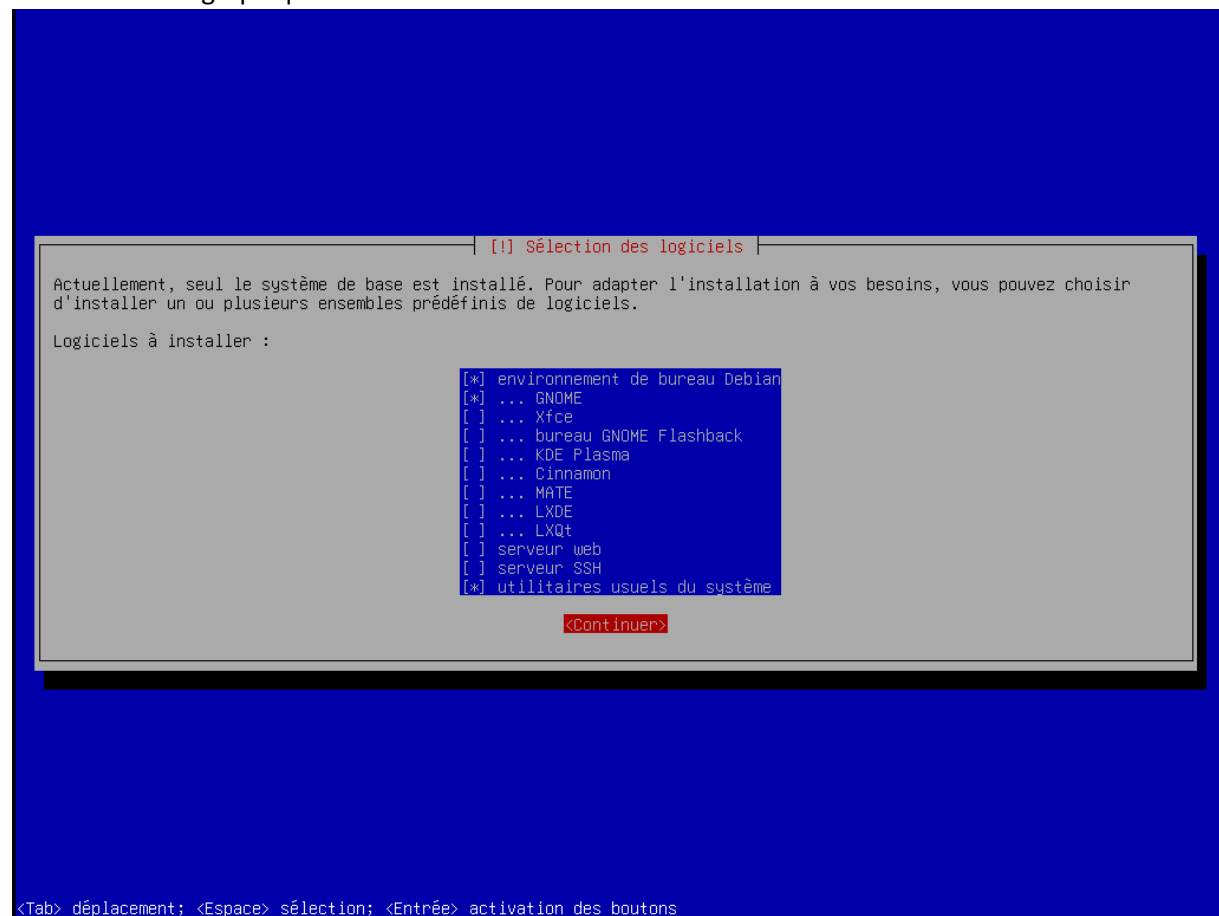
Les paramètres du mandataire doivent être indiqués avec la forme normalisée
« http://[utilisateur][:mot-de-passe]@hôte[:port]/ ».

Mandataire HTTP (laisser vide si aucun) :

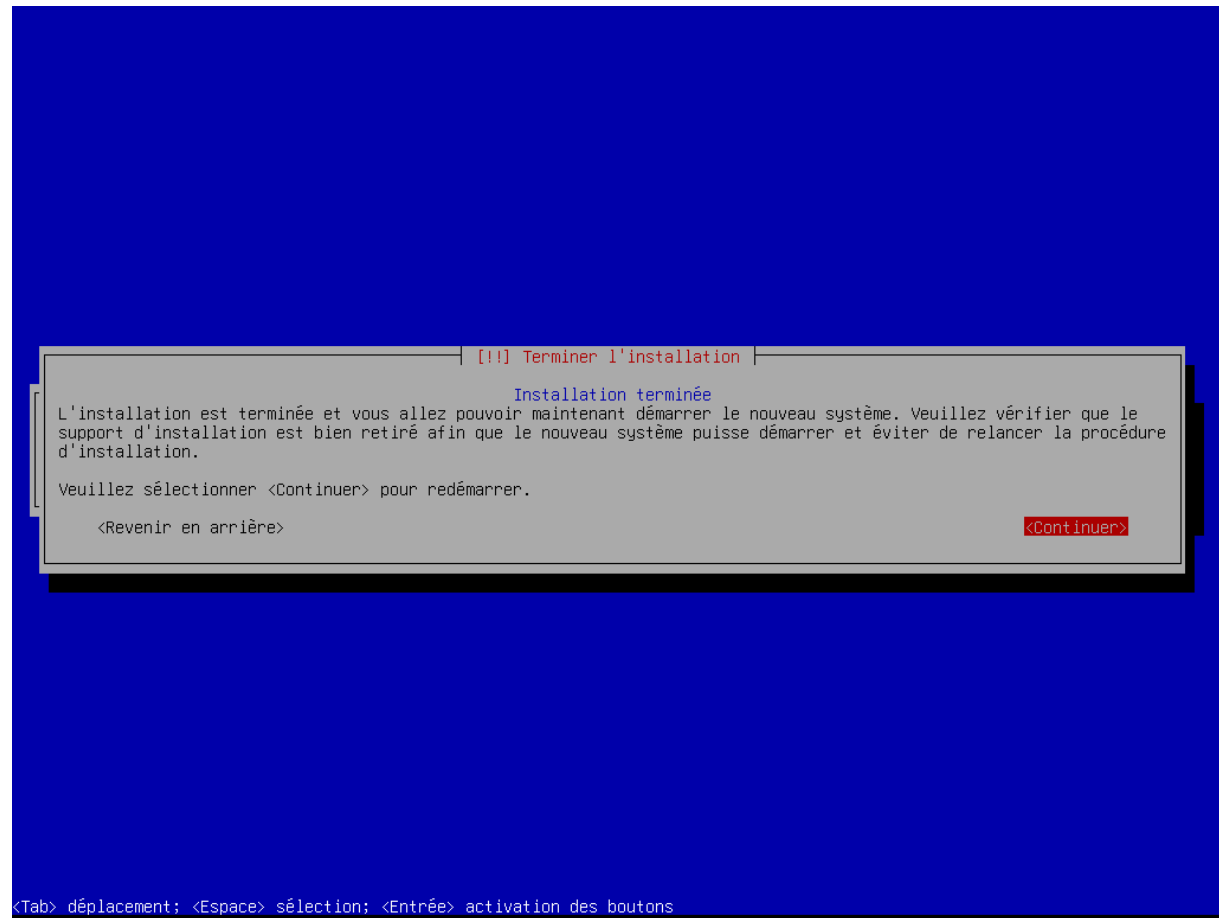
<Revenir en arrière> <Continuer>

<Tab> déplacement; <Espace> sélection; <Entrée> activation des boutons

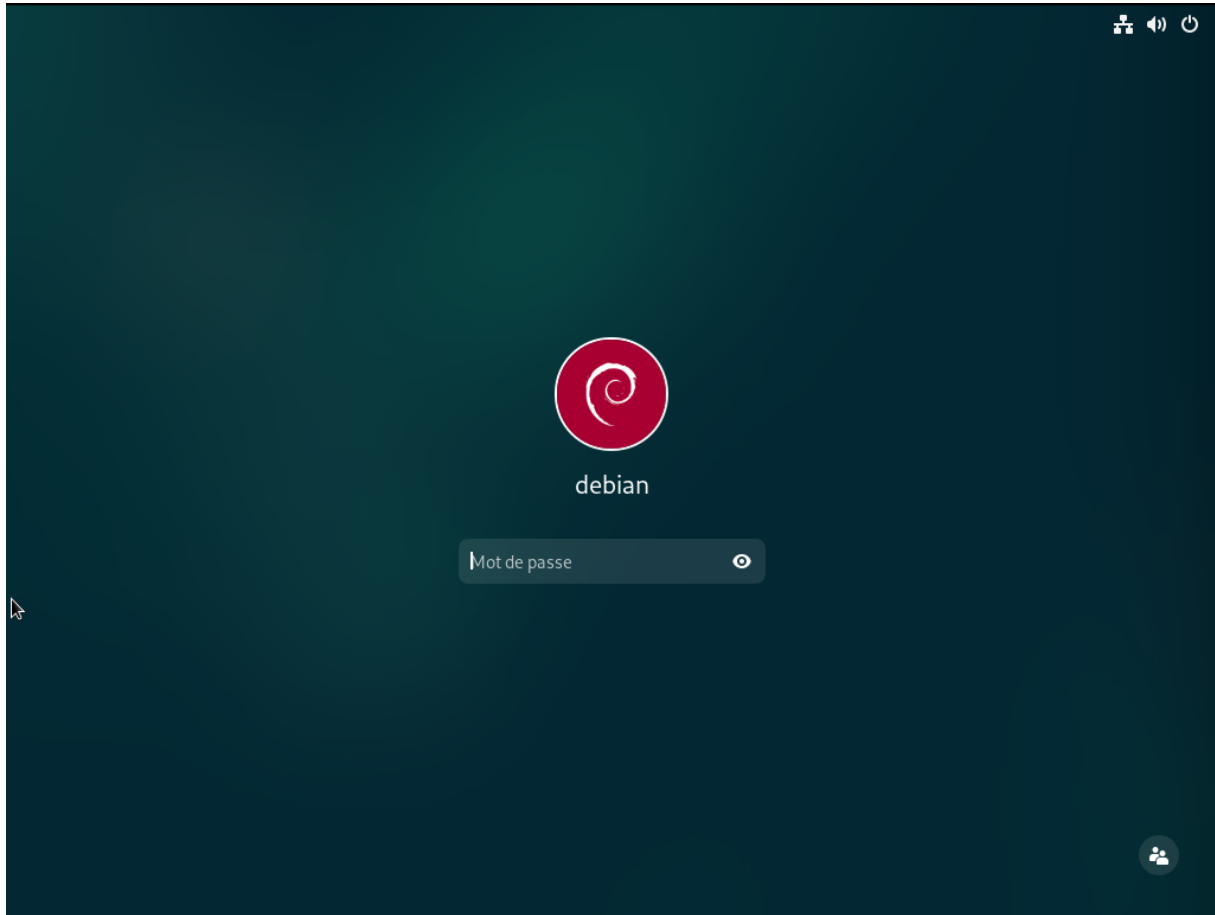
Logiciel à installer : on installera plus tard le serveur SSH car ça prend du temps + GNOME pas besoin d'une interface graphique



Fin de l'installation :



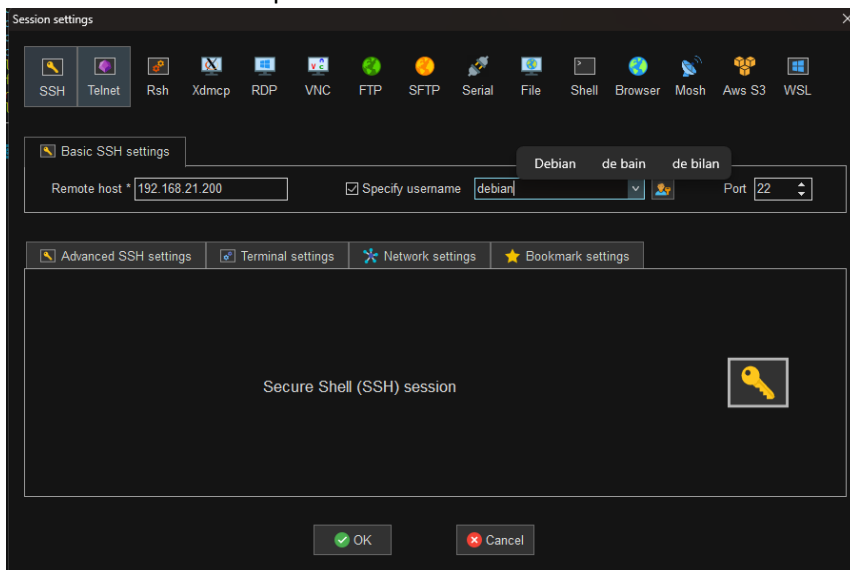
Nous voila sur debian :

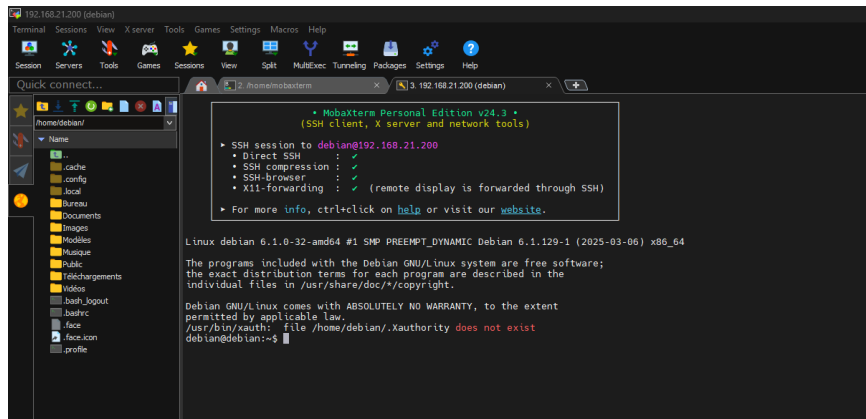


Installation du server SSH pour qu'on puisse avoir une connection sécurisé :

```
root@debian:/home/debian# sudo apt install wireguard
```

Connection via SSH depuis mobaXterm :





Nous voila connecter en SSH depuis mobaXterm

Installation de wireguard :

```
debian@debian:~$ su
Mot de passe :
root@debian:/home/debian# sudo apt install wireguard
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
wireguard est déjà la version la plus récente (1.0.20210914-1).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@debian:/home/debian#
```

Génération de la clé public et privé :

```
root@debian:/home/debian# wg genkey | sudo tee /etc/wireguard/server.key | wg pubkey | sudo tee /etc/wireguard/server.pub
P8p/uC32l0k8zJXAT2ka+R5xZbFr+130mQ0pnFA280s=
```

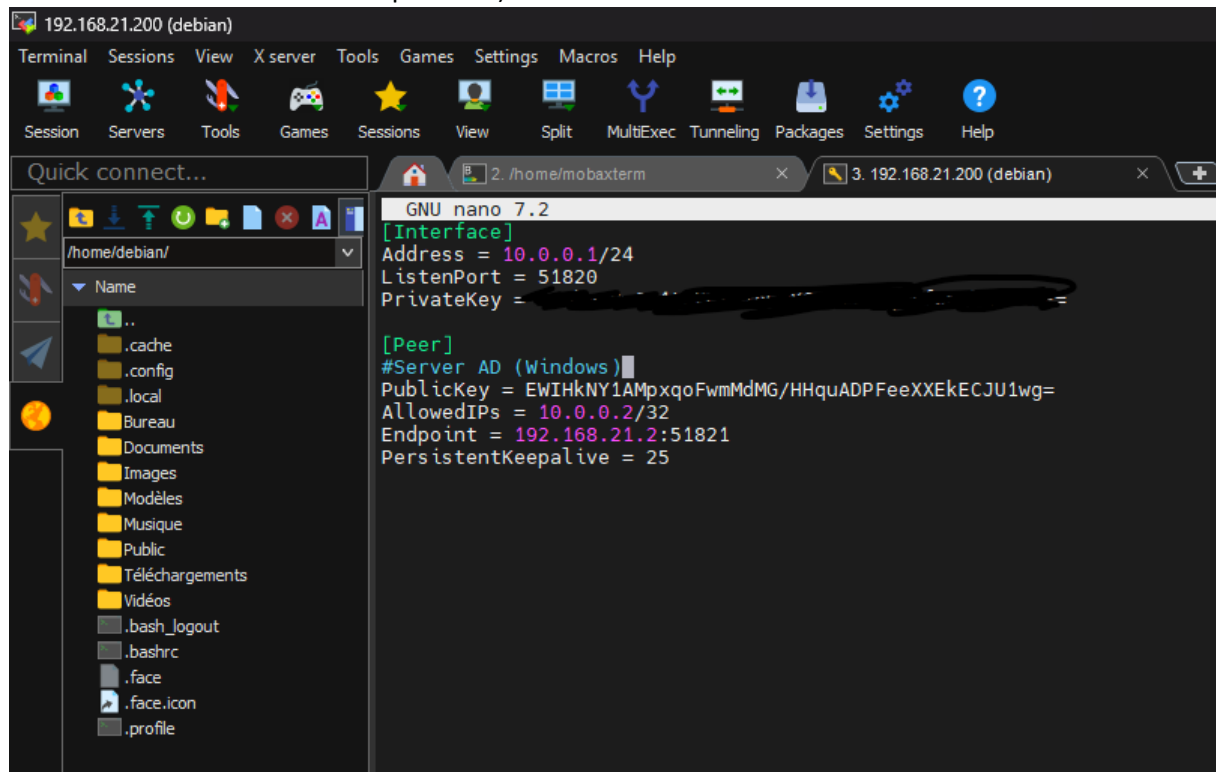
Pour afficher la clé publique :

```
root@debian:/home/debian# sudo cat /etc/wireguard/server.pub
P8p/uC32l0k8zJXAT2ka+R5xZbFr+130mQ0pnFA280s=
```

Configuration du server Wireguard :

```
root@debian:/etc/wireguard# sudo nano /etc/wireguard/wg0.conf
```

Mise en place des clé privé et des clés publiques pour la configuration du server Wireguard (on mettra celle du server windows plus tard)



Activation du routage sur debian : `echo 'net.ipv4.ip_forward=1' | sudo tee -a /etc/sysctl.conf` `sudo sysctl -p`

```

root@debian:/etc/wireguard# echo 'net.ipv4.ip_forward=1' | sudo tee -a /etc/sysctl.conf
root@debian:/etc/wireguard#
  
```

Démarrage dy server WireGuard : `sudo systemctl enable wg-quick@wg0` `sudo systemctl start wg-quick@wg0`

```

root@debian:~# sudo systemctl enable wg-quick@wg0
root@debian:~# sudo systemctl start wg-quick@wg0
root@debian:~# sudo wg
interface: wg0
  public key: P8p/uC32l0k8zJXAT2ka+R5xZbFr+130mQ0pnFA280s=
  private key: (hidden)
  listening port: 51820
root@debian:~#
root@debian:~#
  
```

On peut voir que le Wireguard est bien en place.

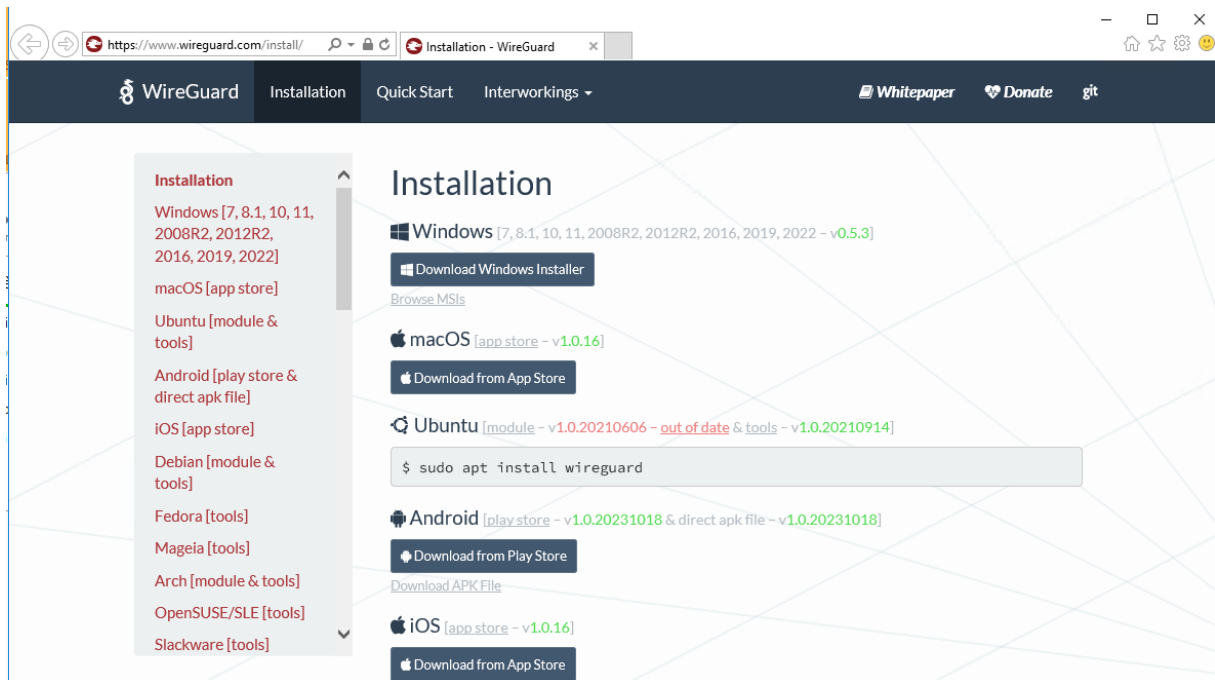
```

root@debian:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:01:be:1f brd ff:ff:ff:ff:ff:ff
    inet 192.168.21.200/24 brd 192.168.21.255 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::215:5dff:fe01:be1f/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
5: wg0: <POINTOPOINT,NOARP,UP,LOWER_UP> mtu 1420 qdisc noqueue state UNKNOWN group default qlen 1000
    link:none
    inet 10.0.0.1/24 scope global wg0
        valid_lft forever preferred_lft forever
root@debian:~#
  
```

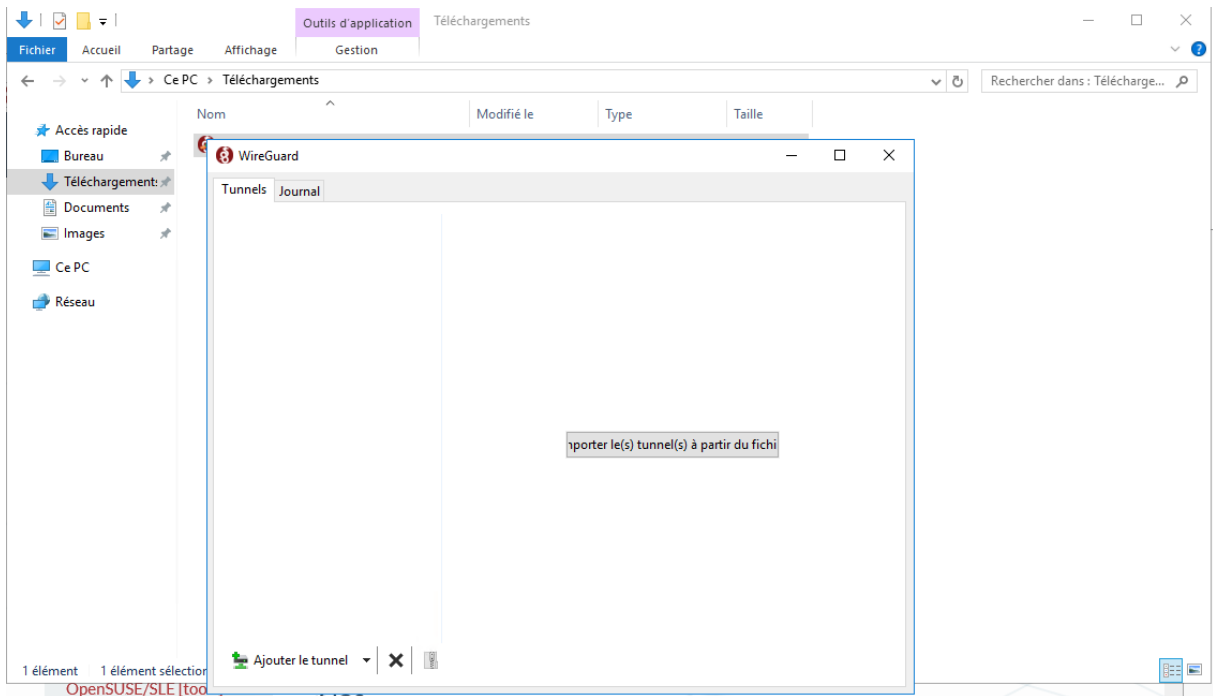
On peut voir depuis un IP → il y a une nouvelle connection.

Maintenant configuration du VPN sur la machine windows :

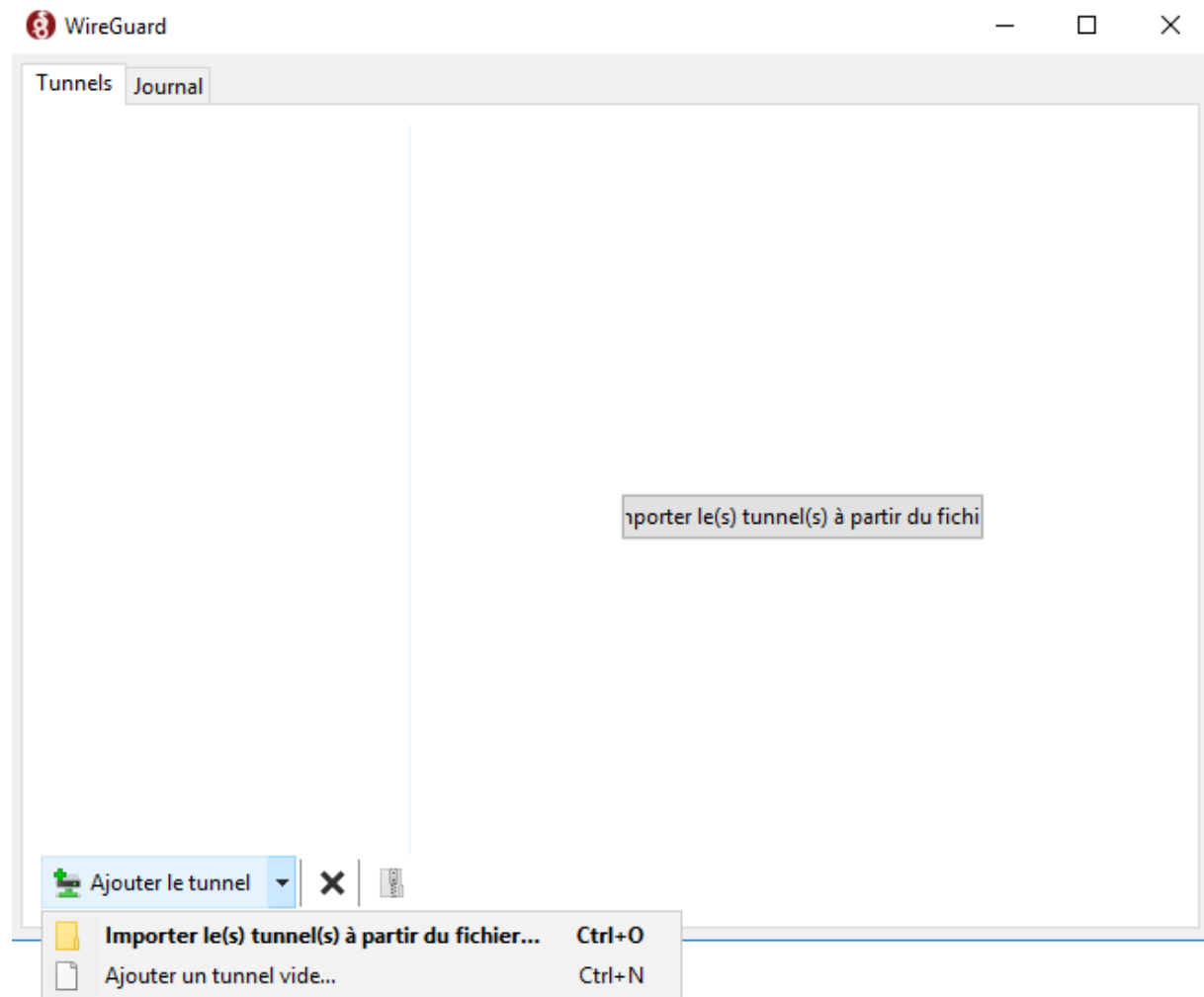
Depuis le site officiel de Wireguard : <https://www.wireguard.com/install/> on installe l'application :



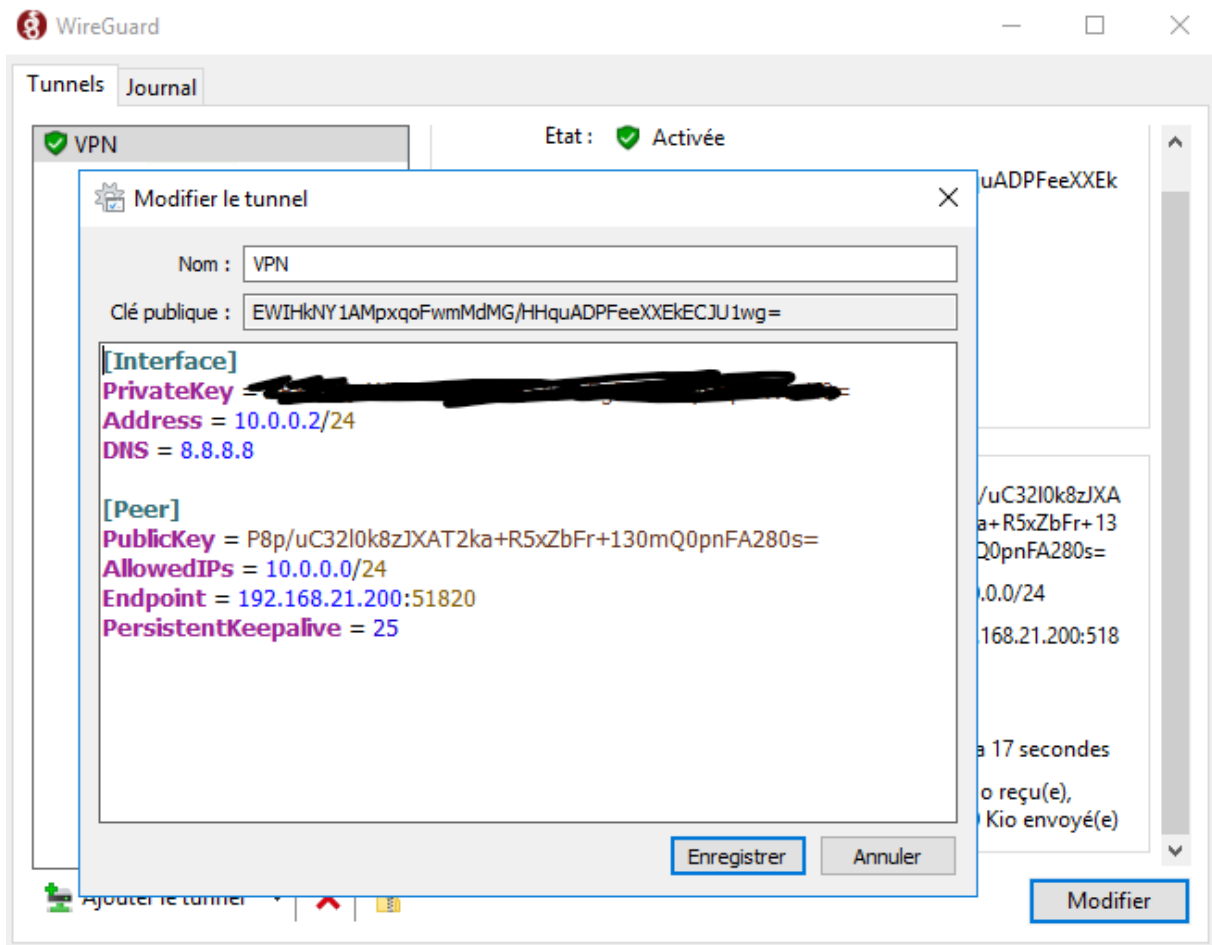
Wireguard installé :



Cliquer sur ajouter un tunnel vide :



Configuration du tunnel :



Sur le server Debian regardons la connection :

```
root@debian:/etc/wireguard# wg
interface: wg0
  public key: P8p/uC32l0k8zJXAT2ka+R5xZbFr+130mQ0pnFA280s=
  private key: (hidden)
  listening port: 51820

peer: EWIhKkNY1AMpxqoFwmMdMG/HHquADPFeeXXEkECJU1wg=
  endpoint: 192.168.21.2:51821
  allowed ips: 10.0.0.2/32
  transfer: 0 B received, 148 B sent
  persistent keepalive: every 25 seconds
root@debian:/etc/wireguard#
```

```

root@debian:/etc/wireguard# ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=128 time=0.415 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=128 time=0.618 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=128 time=0.611 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=128 time=0.597 ms
64 bytes from 10.0.0.2: icmp_seq=5 ttl=128 time=0.488 ms
64 bytes from 10.0.0.2: icmp_seq=6 ttl=128 time=0.502 ms
^C
--- 10.0.0.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5104ms
rtt min/avg/max/mdev = 0.415/0.538/0.618/0.075 ms
root@debian:/etc/wireguard#

```

connection en vpn operationnel sur le server debian, on arrive a ping le server windows

```

C:\Users\Administrateur.WIN-V1KTGI8K1CV>ping 10.0.0.1

Envoi d'une requête 'Ping' 10.0.0.1 avec 32 octets de données :
Réponse de 10.0.0.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.0.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.0.1 : octets=32 temps<1ms TTL=64
Réponse de 10.0.0.1 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 10.0.0.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\Administrateur.WIN-V1KTGI8K1CV>

```

fonctionnement dans les deux sens. Le VPN est bien configuré

```

C:\Users\Administrateur.WIN-V1KTGI8K1CV>ipconfig

Configuration IP de Windows

Carte inconnue VPN :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv4. . . . . : 10.0.0.2
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :

Carte Ethernet Ethernet :

    Suffixe DNS propre à la connexion. . . :
    Adresse IPv6 de liaison locale. . . . : fe80::6415:baae:9ef2:dd28%8
    Adresse IPv4. . . . . : 192.168.21.2
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.21.1

Carte Tunnel isatap.{A7C489E6-8980-409A-8DDC-1F6B77EA834B} :

    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . :

Carte Tunnel Teredo Tunneling Pseudo-Interface :

    Statut du média. . . . . : Média déconnecté

```

Si on arrive pas a communiquer le pare feu peut bloquer on active donc ufw cela nous permettre d'ouvrir un port spécifique.

Si la connection ne marche pas ouvrir le port 51820 :

```
root@debian:~# sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
root@debian:~# ufw status
bash: ufw : commande introuvable
root@debian:~# sudo ufw status
Status: active
root@debian:~# sudo ufw allow 51820/udp
Rule added
Rule added (v6)
root@debian:~# sudo ufw status
Status: active
```

To	Action	From
--	-----	----
51820/udp	ALLOW	Anywhere
51820/udp (v6)	ALLOW	Anywhere (v6)

Ecrire cette commande dans le fichier rules.

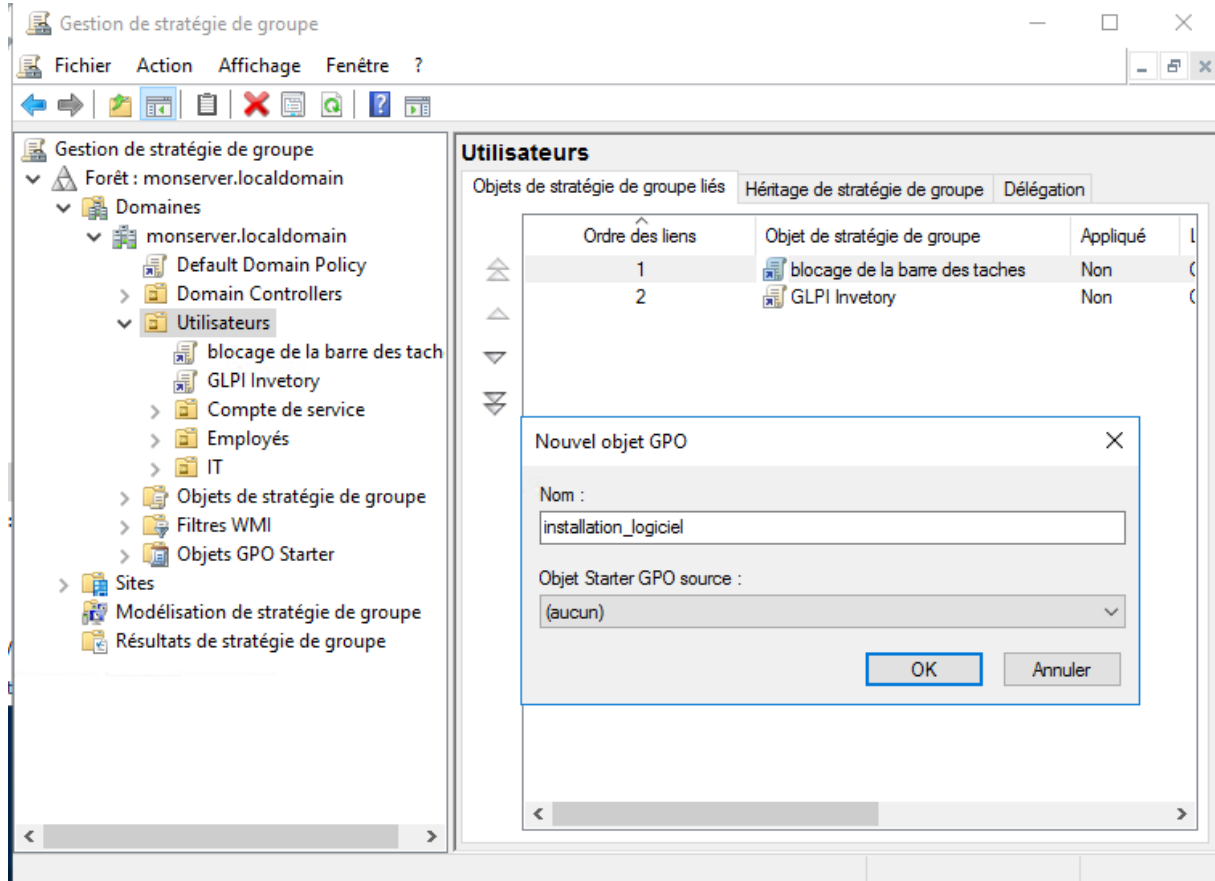
```
root@debian:~# sudo nano /etc/ufw/before.rules
```

```
# Autoriser ICMP (ping) sur wg0
-A ufw-before-input -i wg0 -p icmp --icmp-type echo-request -j ACCEPT
```

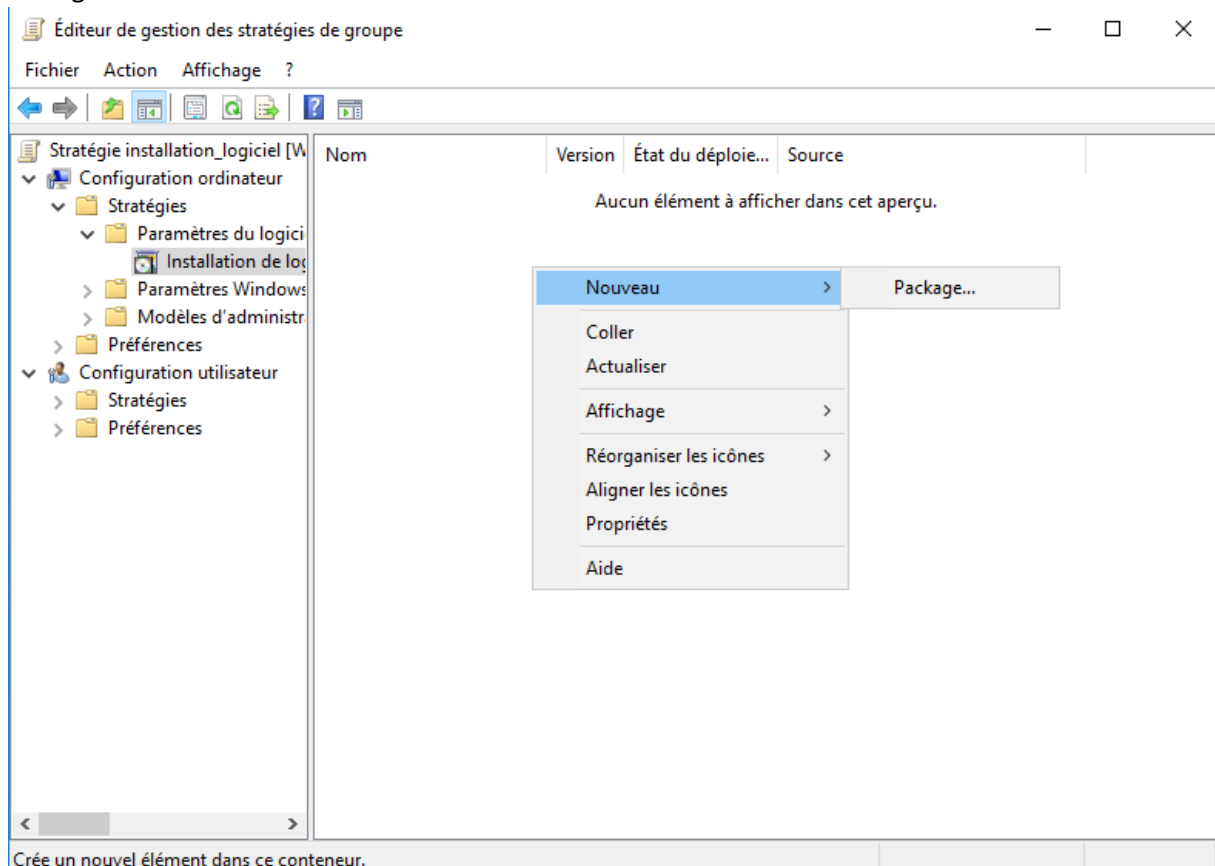
Mise en place d'un GPO pour installation de wireguard automatiquement sur les postes client windows :

Lieu de partage pour récupérer les fichiers partager en .msi [\\SRV-1\application\\$](#)

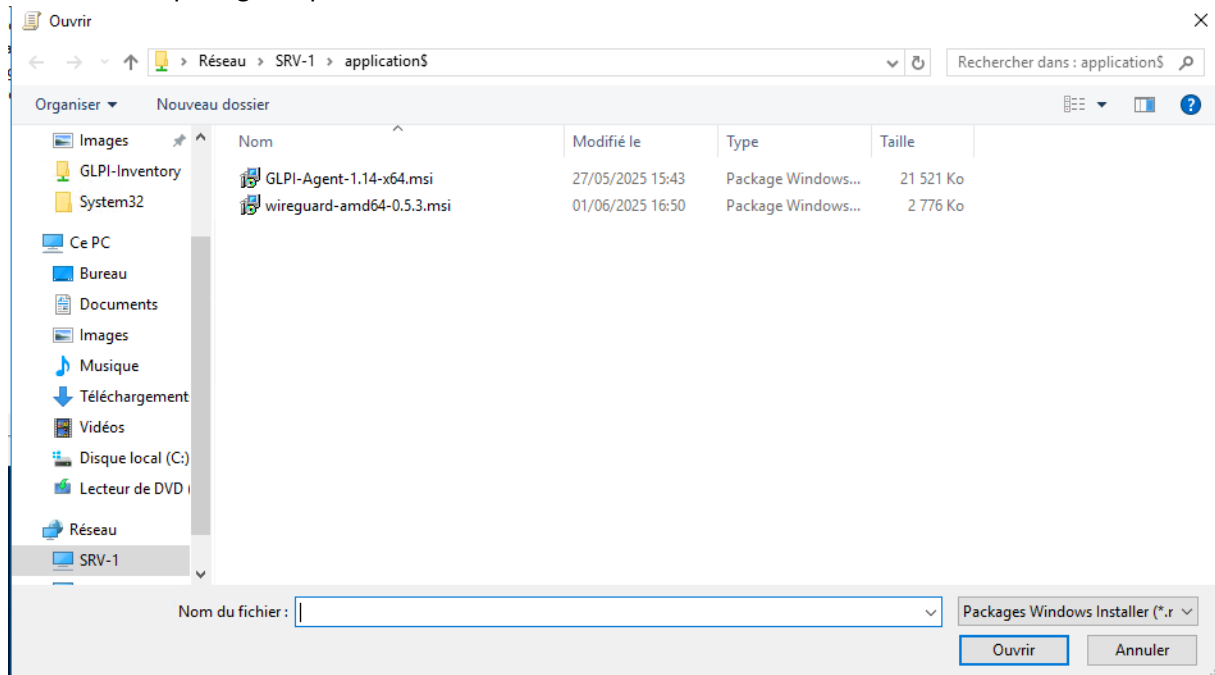
Création de la GPO :



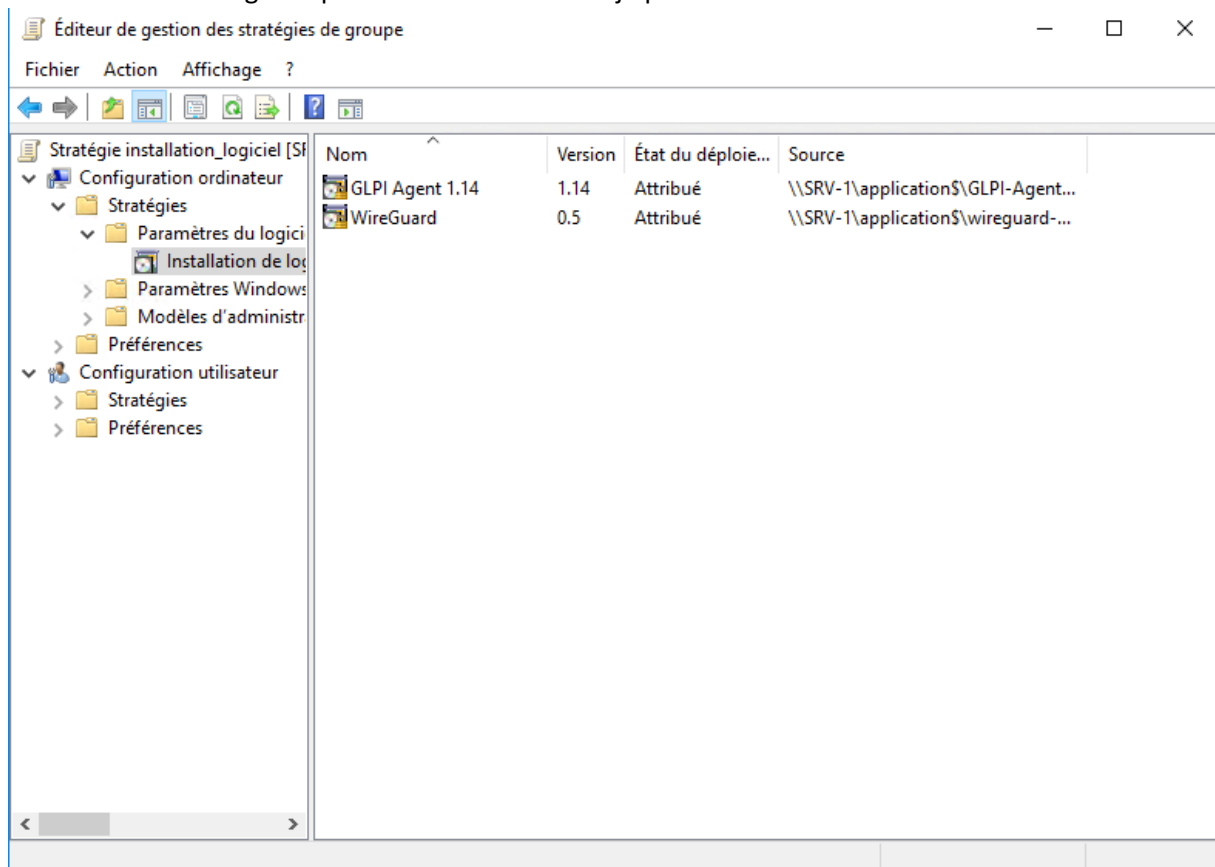
Configuration de la GPO :



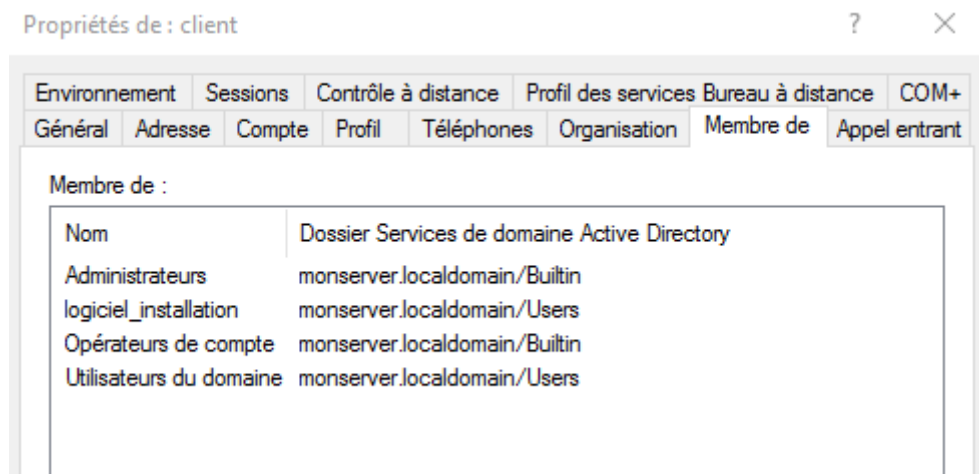
Via le dossier partagé on peut retrouver les fichiers .msi :



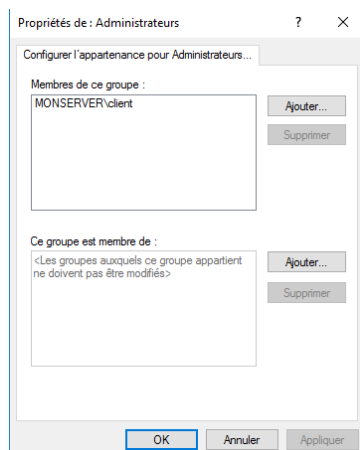
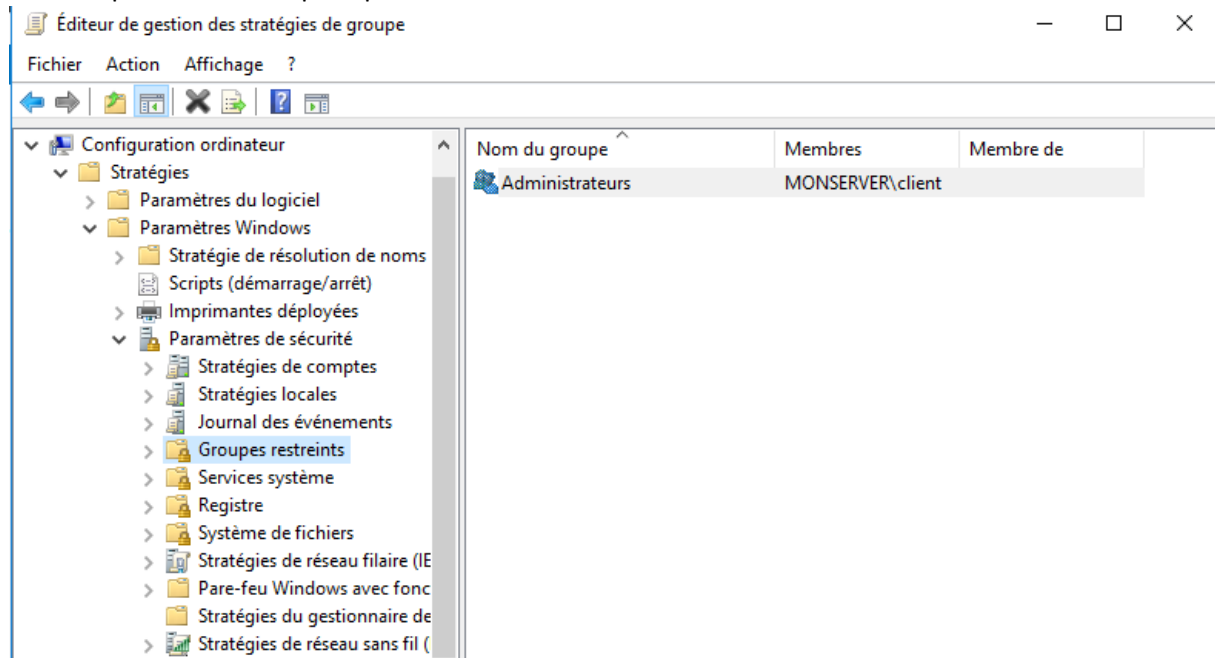
On sélectionne le logiciel qu'on veut dans mon cas je prends les deux :



On met les droits pour que le client ai acces à l'active directory (mettre le droit admin sur le poste local):



Mise en place d'un GPO pour permettre l'automatisation des droits admin sur un domain :



Script pour bloquer l'accès local au server ad : # Bloquer tout accès local au serveur AD :

New-NetFirewallRule -DisplayName "Bloquer accès LAN AD" `

-Direction Inbound -Action Block `

-RemoteAddress 192.168.0.0/16 `

-Protocol TCP `

-LocalPort 389,445,139,135,88 `

-Profile Any

Script pour autoriser uniquement les connexions depuis le VPN wireguard :

New-NetFirewallRule -DisplayName "Autoriser VPN vers AD" `

-Direction Inbound -Action Allow `

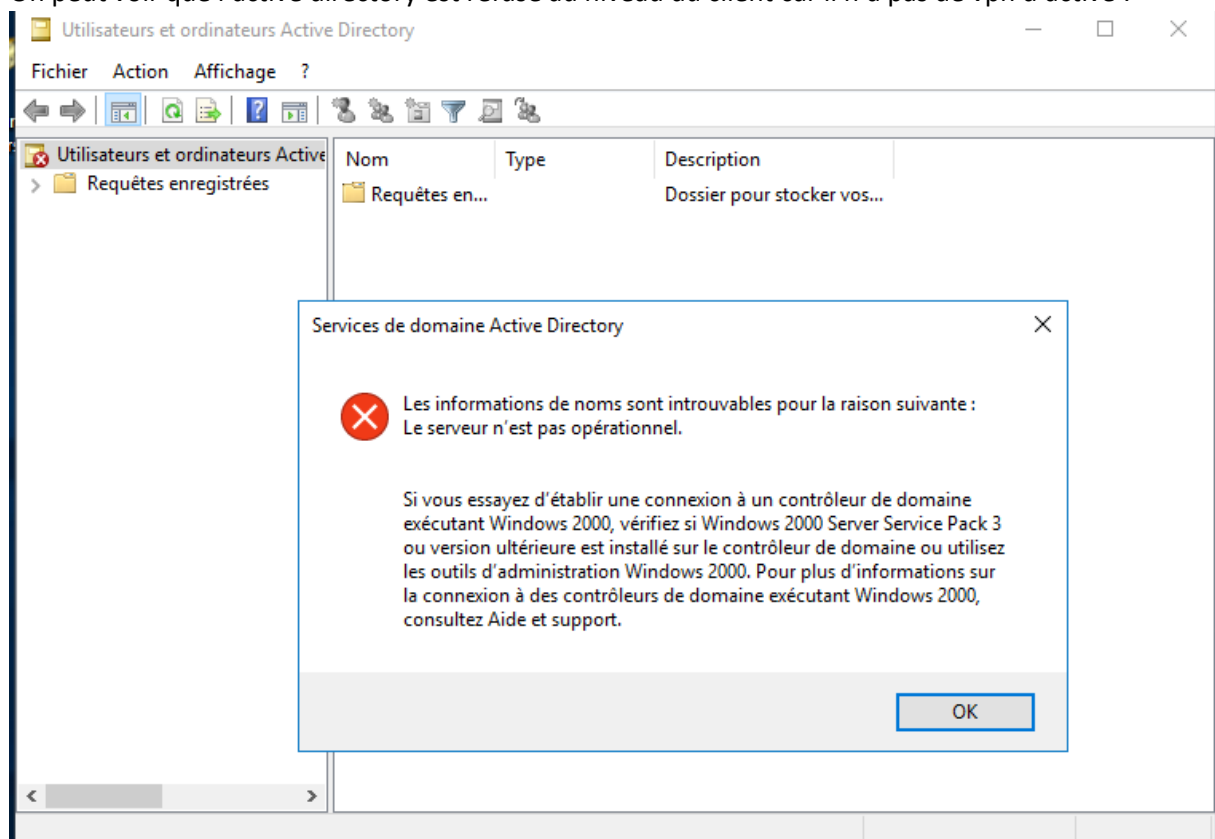
-RemoteAddress 10.0.0.0/24 `

-Protocol TCP `

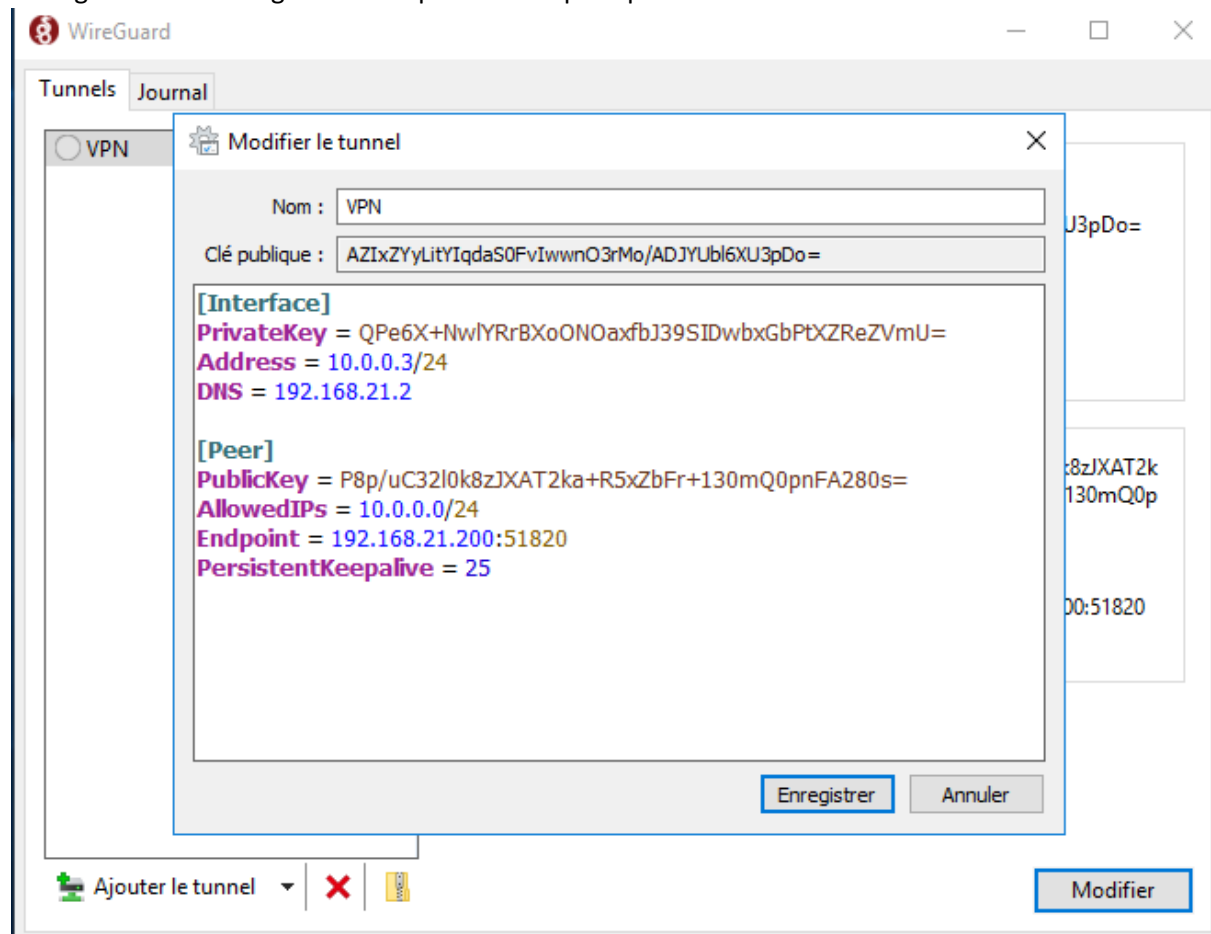
-LocalPort 389,445,139,135,88 `

-Profile Any

On peut voir que l'active directory est refusé au niveau du client car il n'a pas de vpn d'activé :



Configuration de wireguard sur le poste client pour pouvoir avoir accès a l'ad :



fichier .conf

[Interface]

Address = 10.0.0.1/24

ListenPort = 51820

PrivateKey = iAHky/QwJa4tgXEkA/eEuYGuGTtnpg8xfQMYlluz63E=

[Peer]

PublicKey = EWIHkNY1AMpxqoFwmMdMG/HHquADPFeeXXEkECJU1wg=

AllowedIPs = 10.0.0.2/32

Endpoint = 192.168.21.2:51821

PersistentKeepalive = 25

[Peer]

#CLIENT

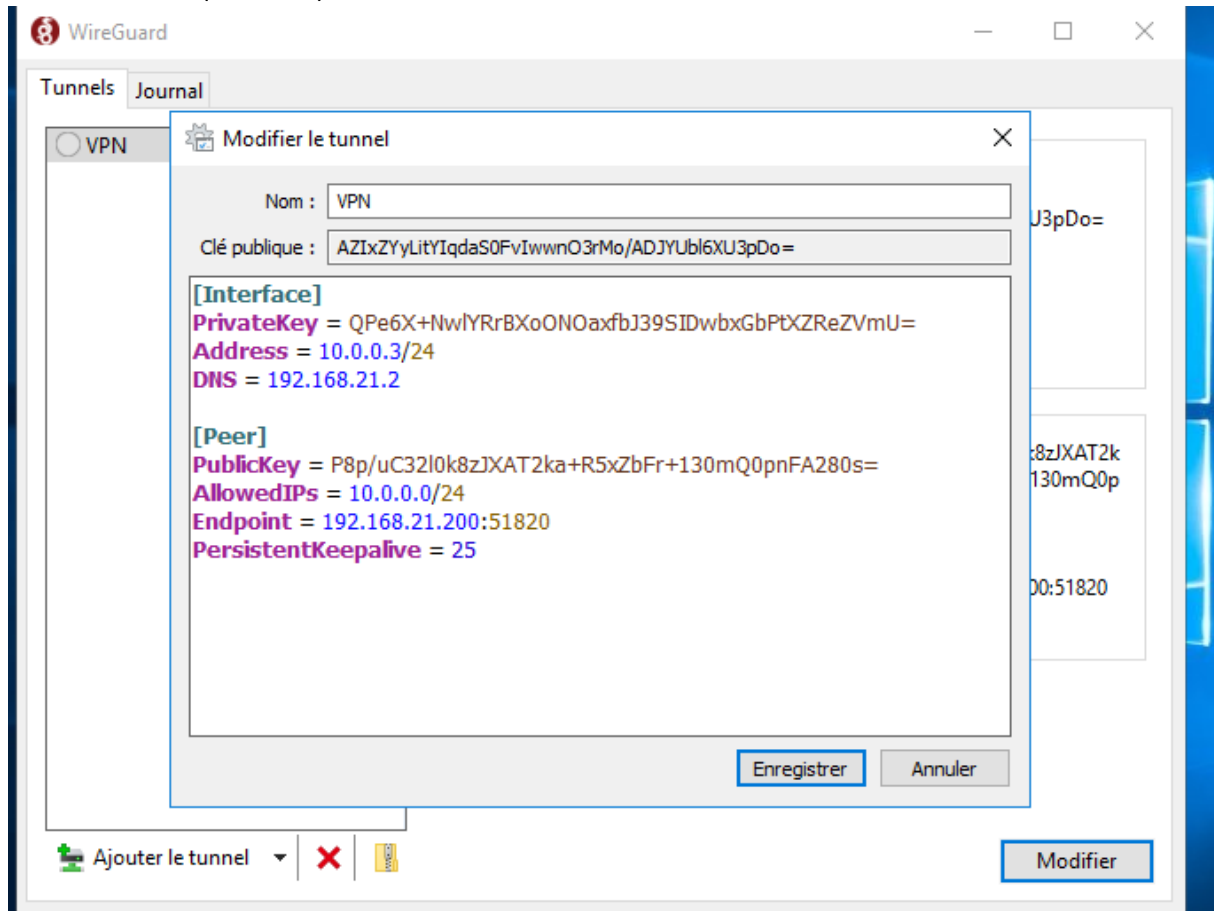
PublicKey = AZlxZYyLitYlqdaS0FvlwwnO3rMo/ADJYUbl6XU3pDo=

AllowedIPs = 10.0.0.3/32

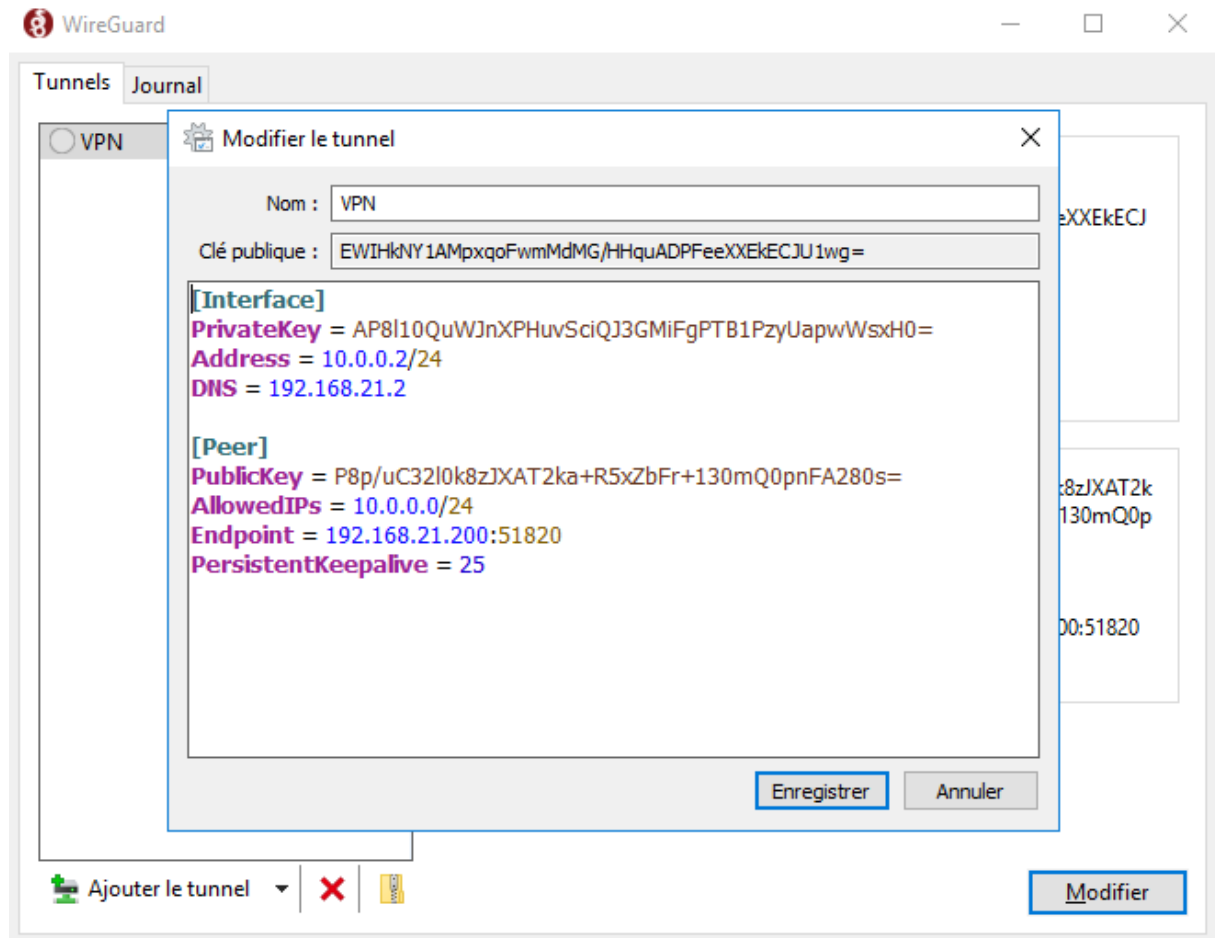
Endpoint = 192.168.21.200:51821

PersistentKeepalive = 25

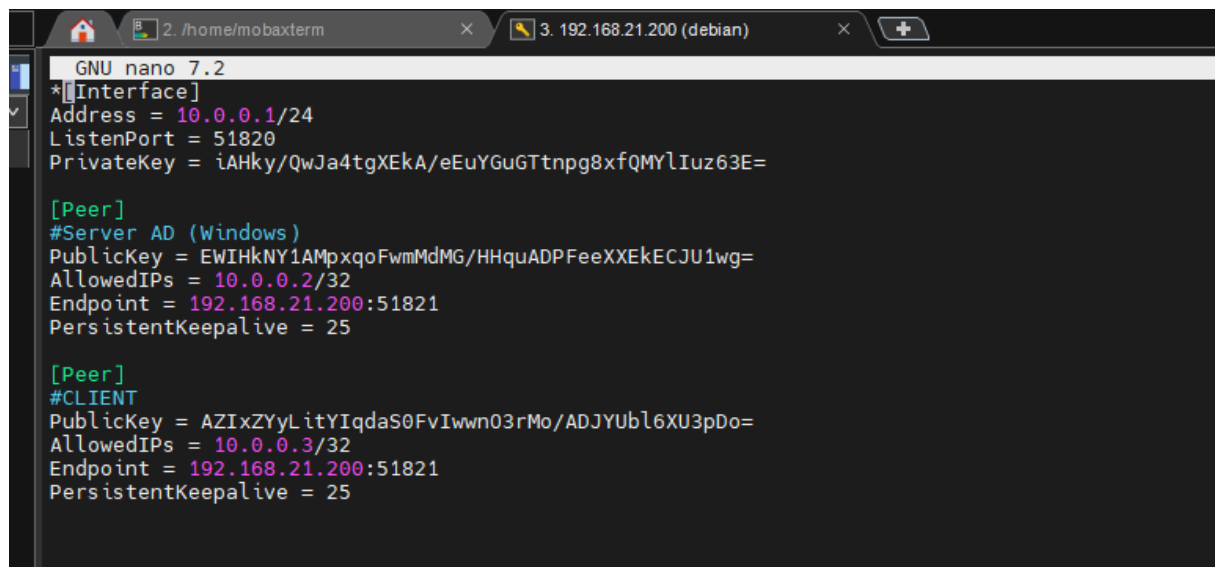
Conf VPN client (windows) :



Conf VPN server ad (windows) :



Conf VPN wireguard (debian) :



Clé privé wireguard :

iAHky/QwJa4tgXEkA/eEuYGuGTtnpg8xfQMYlluz63E=

clé public wireguard :

P8p/uC32l0k8zJXAT2ka+R5xZbFr+130mQ0pnFA280s=

Clé privé windows (ad) :

AP8l10QuWJnXPHuvSciQJ3GMiFgPTB1PzyUapwWsxH0=

Clé public windows (ad) :

EWIHkNY1AMpxqoFwmMdMG/HHquADPFeeXXEkeCJU1wg=