Projet de Réseau Virtuel Paris-Perpignan

M. KHALILI (BTS SIO 2 SISR)

Professeur chargé de l'AP : Mme.GHOUA

Table des matières

1/Installation et configuration de base d'OPNsense

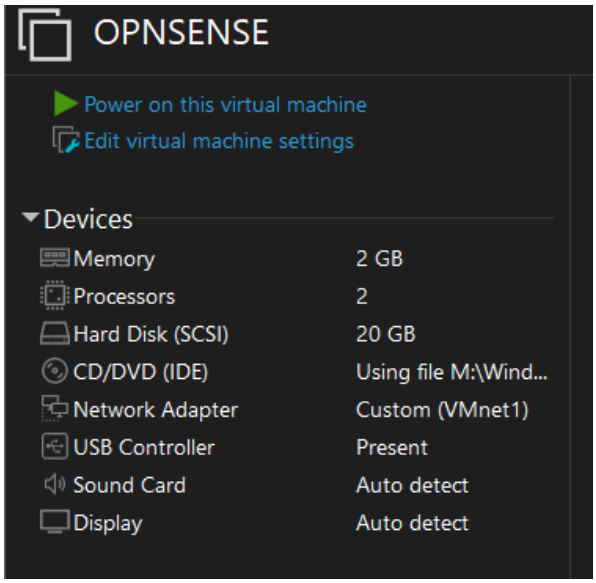
1.1/Création de la machine Virtuelle :

Pour installer OPNsense il faut récupérer l'iso depuis le site officiel :

https://opnsense.org/download/

Il faut sélectionner DVD comme ci-dessous :

Il faut faire une VM en host-only avec l'ISO téléchargé comme ci-dessous (il y a de nombreux tutos sur internet pour faire une VM). Il faut minimum 2 Go de RAM à la VM pour assurer un bon fonctionnement :



1.2/Installation d'OPNSense :

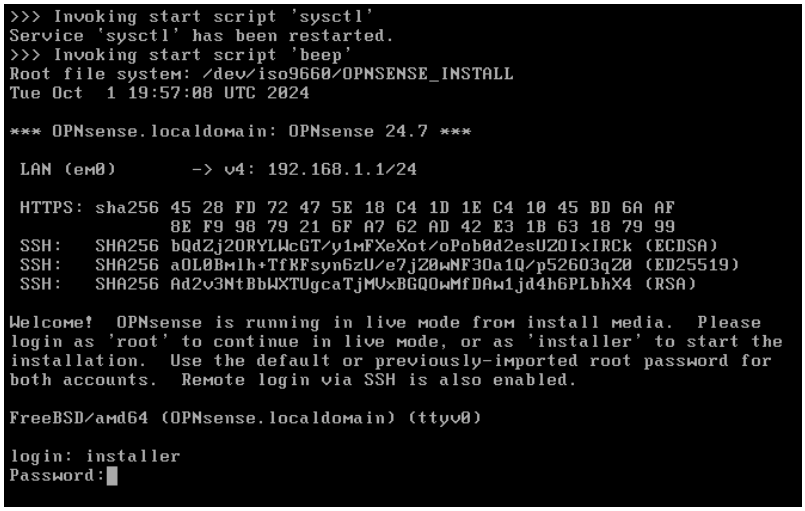
On peut la démarrer et la laisser charger.

Une fois arrivé sur la connexion, on rentre :

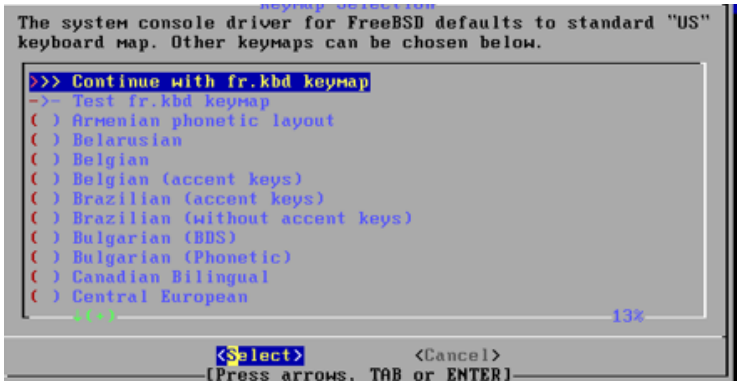
Login : installer

Password : opnsense

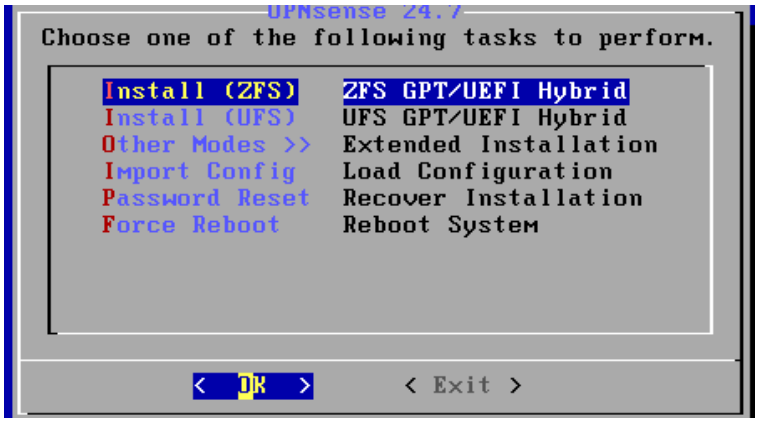
Attention, pour l'instant le clavier est en Qwerty



Ensuite, il faut choisir le « keymap », la disposition clavier : il faut descendre et sélectionner « french » et ensuite sélectionner « Continux with fr.kbd keymap ».



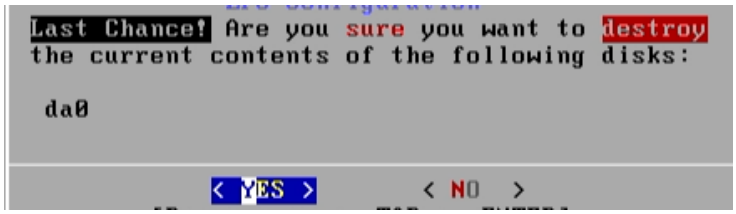
Sélectionner « Install (ZFS) ».



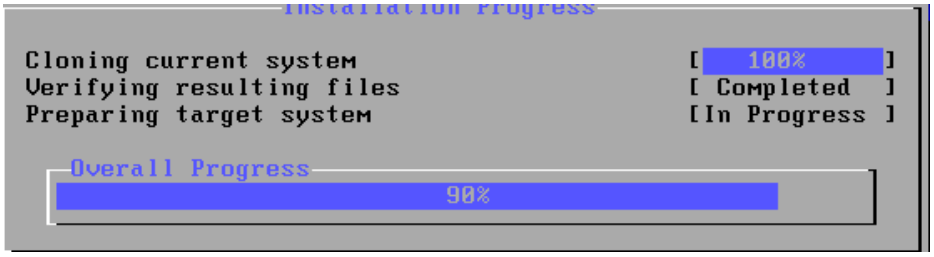
Choisir « stripe – No Redundancy » car nous voulons aucune redondance.

Choisir le disque en cliquant sur espace puis entrer.

Valider la destruction du disque. Dans notre cas, il est formaté, mais s'il y a des données dessus, il faut vérifier avant.



L'installation se lance.



Une fois fini, il demande si on veut modifier le mot de passe root, nous allons le faire pour avoir plus de sécurité, appuyez sur entrée.

Entrer votre nouveau mot de passe 2 fois.

Enfin, sélectionnez « complete install ».

La machine va redémarrer.

1.3/Configuration des interfaces :

Il faut se connecter en root et le mot de passe qu'on vient de modifier.

Pour « enter an option » appuyez sur 1.

Aux questions « Do you want to configure LAGGs now » et « Do you want to configure VLANs now » appuyez sur « n » pour non.

Pour « Enter the WAN interface … » appuyer sur entrée car nous ne l'utiliserons pas.

Pour « Enter the LAN interface … » saisir « em0 ».

Pour « Enter the Optional interface … », appuyez sur entrée car nous ne l'utiliserons pas.

Puis appuyez sur « y » pour valider.

```
Enter the WAN interface name or 'a' for auto-detection:

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): em0

Enter the Optional interface 1 name or 'a' for auto-detection
(or nothing if finished):

The interfaces will be assigned as follows:

LAN  -> em0

Do you want to proceed? [y/N]: y
```

Maintenant on va attribuée l'adresse IP.

Pour « Enter an option » appuyez sur 2.

```
Enter an option: 2
```

« Configure IPv4 adress LAN interface via DHCP ? » saisir « n » car il faut configurer l'interface en statique.

Saisissez l'adresse IP de l'interface. Cette adresse IP sera la passerelle du LAN.

Saisissez le masque en CIDR.

```
Configure IPv4 address LAN interface via DHCP? [y/N] n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.200.1


Subnet masks are entered as bit counts (like CIDR notation).
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

Pour la Gateway appuyer sur entrée pour cause que la passerelle sera elle-même.

```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

« Configure IPv6 adress LAN interface via DHCP ? » saisir « n » car nous ne voulons pas configurer l'IPv6.

Appuyez sur entrée pour sauter la configuration de l'IPV6.

« Do you want configure DHCP server on LAN ? » saisir « n » car nous ne voulons pas configurer de serveur DHCP.

« Do you want to change the web GUI protocol from HTTPS to HTTP ? » saisir « n » car nous ne voulons pas configurer le protocole HTTPS.

« Do you want to genere a new self-signed web GUI certificate ? » saisir « n » car nous ne voulons pas générer de certificat.

« Restore web GUI access default ? » appuyer sur entrée.

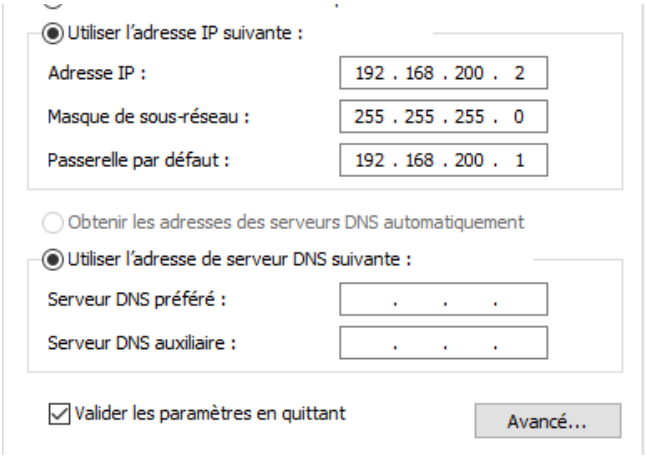
Il nous donne l'url pour configurer depuis l'interface web

```
https://192.168.200.1
```

1.4/Test :

Pour essayer, nous allons utiliser un client dans le même VMNET que notre serveur OPNSense.

Il faut changer la configuration IP du client pour quelle correspond à celle de notre serveur, la passerelle sera l'adresse IP de l'OPNSense.



Dans le navigateur, il faut saisir l'adresse IP attribuée à l'OPNSense.

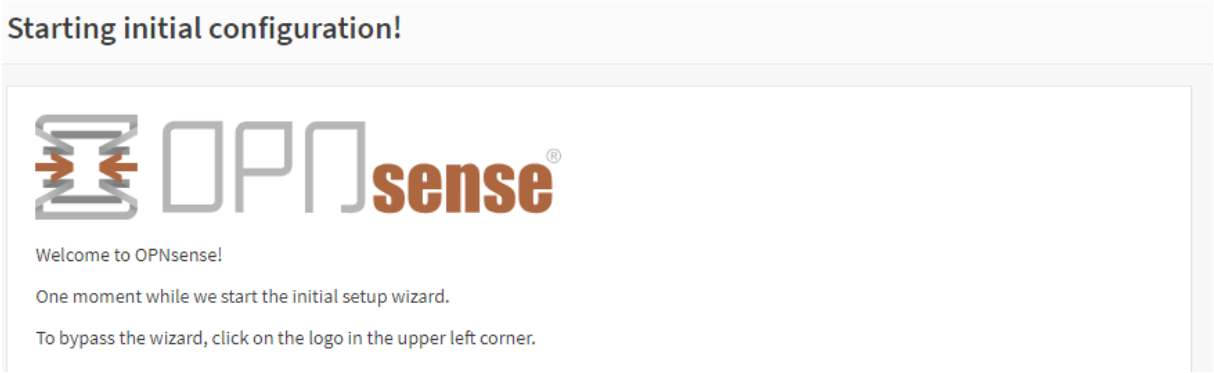
Continuer même si le certificat de sécurité n'est pas approuvé par le système d'exploitation.

Se connecter :

Login : root

Password : le mot de passe créé précédemment.

Nous arrivons sur le Wizard.



Cliquer sur « next »

Changer « Language » sur French

Le reste ne nous est pas utile.

Cliquer sur « next »

Vérifier la « Timezone »

Cliquer sur « next »

Descendez et cliquez « next »

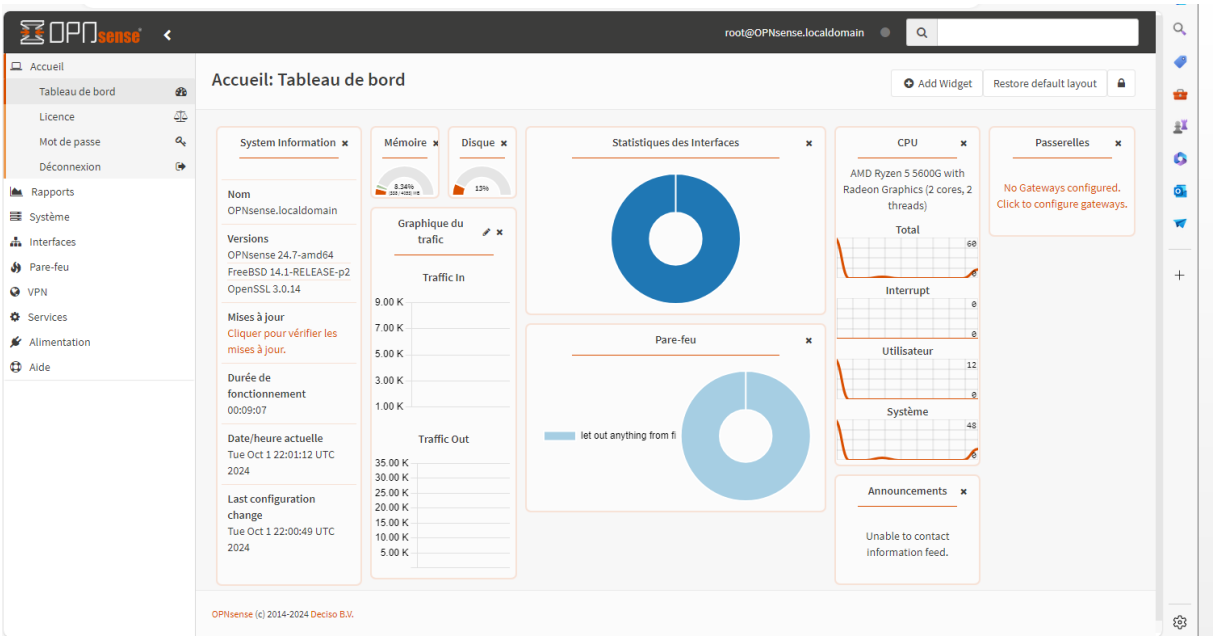
L'interface LAN est pré-configurée car nous l'avons fait avant.

Laisser vide pour le mot de passe root, nous l'avons déjà modifié.

Cliquer sur « next »

Cliquez « Recharger » pour appliquer les changements.

Nous voilà sur le tableau de bord, nous avons terminé la configuration du serveur OPNSense. Il faut maintenant configurer les différents services.



NOTE : Il faudra recommencer l'installation pour le serveur du coté Perpignan en rajoutant une carte réseau pour l'accès à internet et faire attention lors de l'assignement des interfaces de ne pas inversé les cartes réseau (mettre la carte réseau du WAN pour l'interface LAN ou l'inverse) il faut bien les identifier par leurs adresses MAC.

2/Installation et configuration de l'AD.

2.1/Configuration Nécessaire

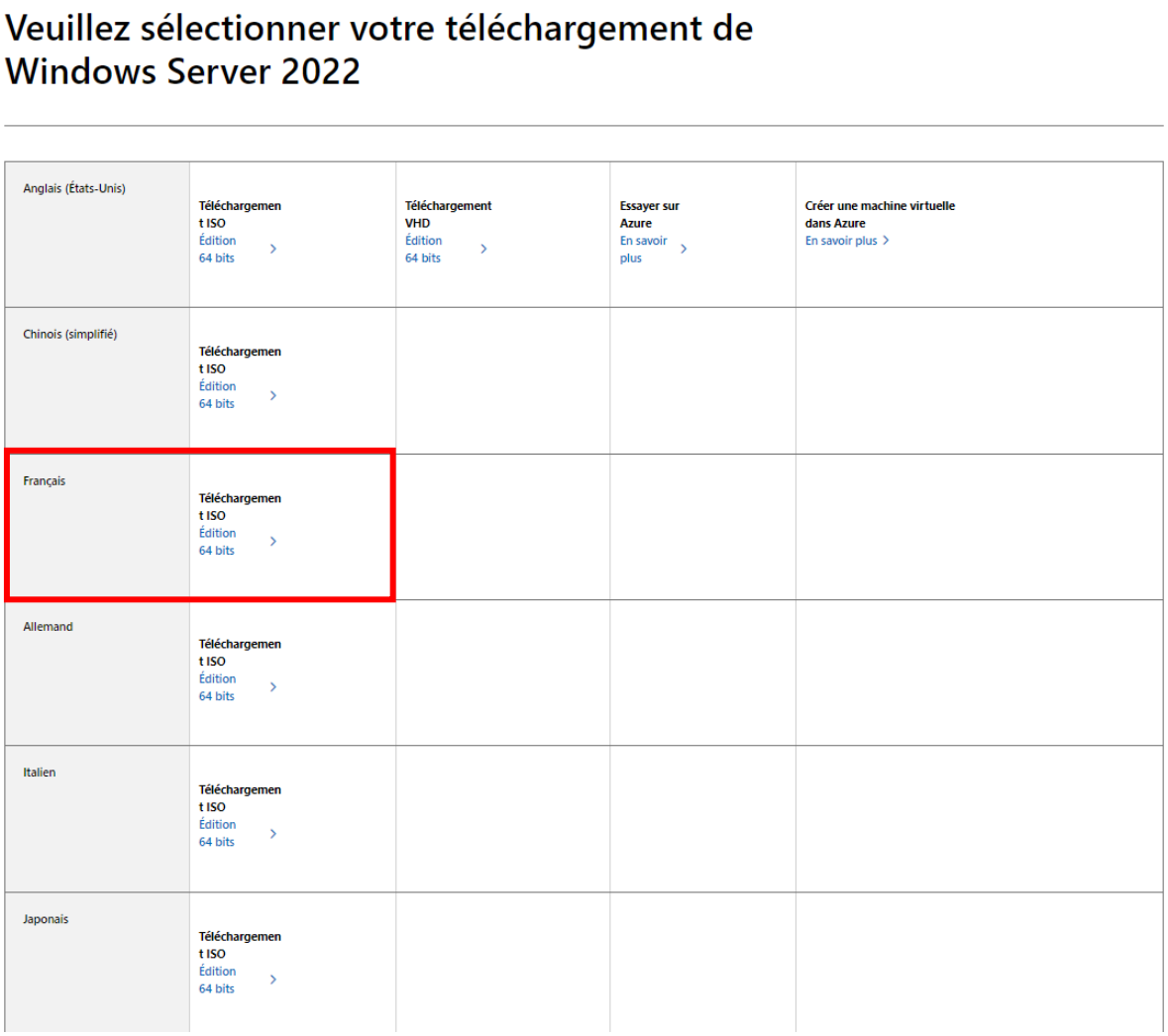
Pour la bonne réalisation de cette installation, il faudra disposer d'une configuration minimum à respecter :

- Processeur : 1.4 GHz 64-bit
    - Compatible avec le jeu d'instructions x64
    - Prend en charge NX et DEP
    - Prend en charge CMPXCHG16b, LAHF/SAHF et PrefetchW
    - Prend en charge la traduction d'adresse de deuxième niveau (EPT ou NPT)
- RAM : 512 Mo
    - ECC conseillé
- Disque : 32 Go

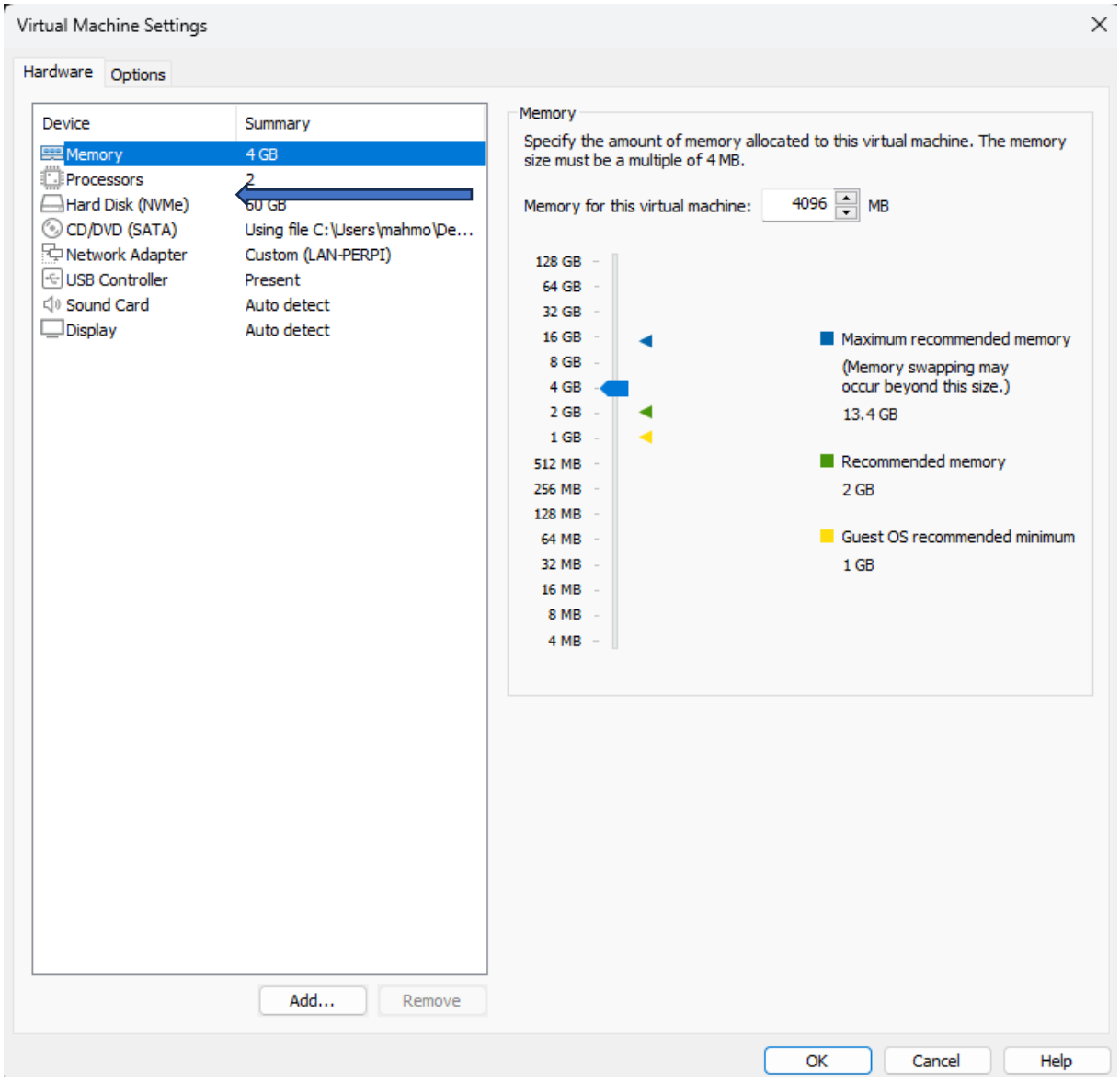
2.2/Installation de Windows Server 2022

Pour récupérer l'ISO de Windows Server, il suffit de se rendre sur le site de Microsoft :

https://www.microsoft.com/fr-fr/evalcenter/download-windows-server-2022

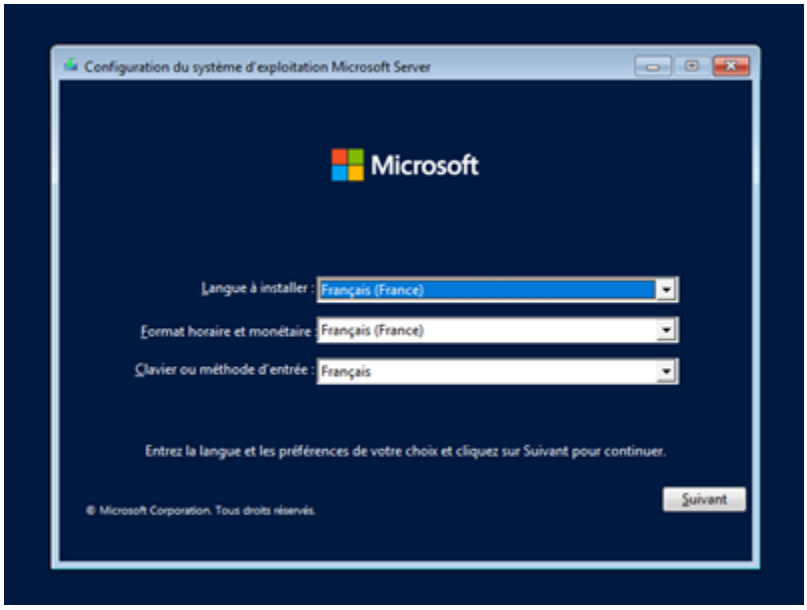


Une fois l'ISO téléchargé, l'inclure dans VMware dans la VM créée préamblement :

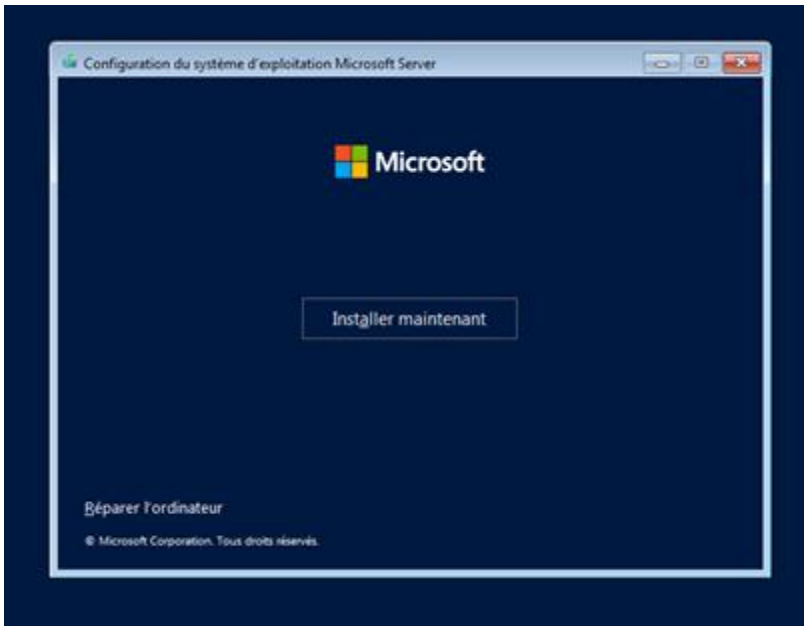


Démarrer la Machine Virtuel :

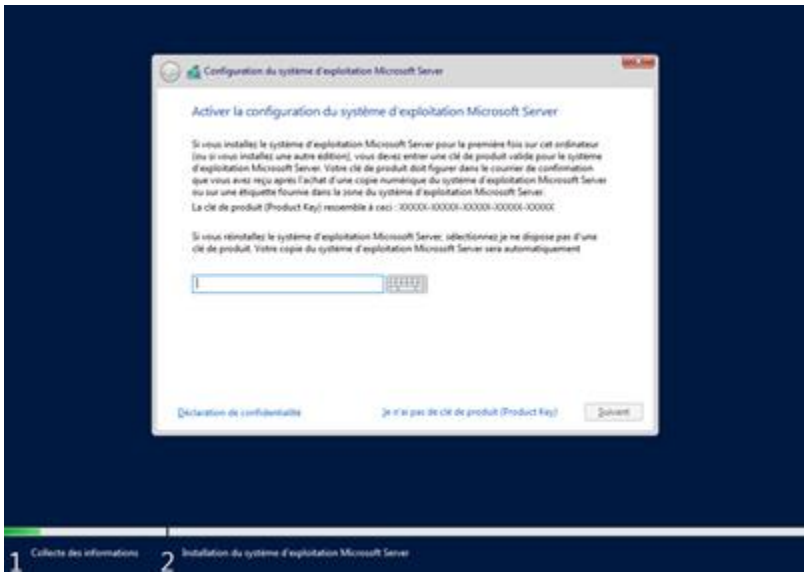
Sélectionnez la langue désirée, et cliquez sur suivant :



On clique sur Installer maintenant

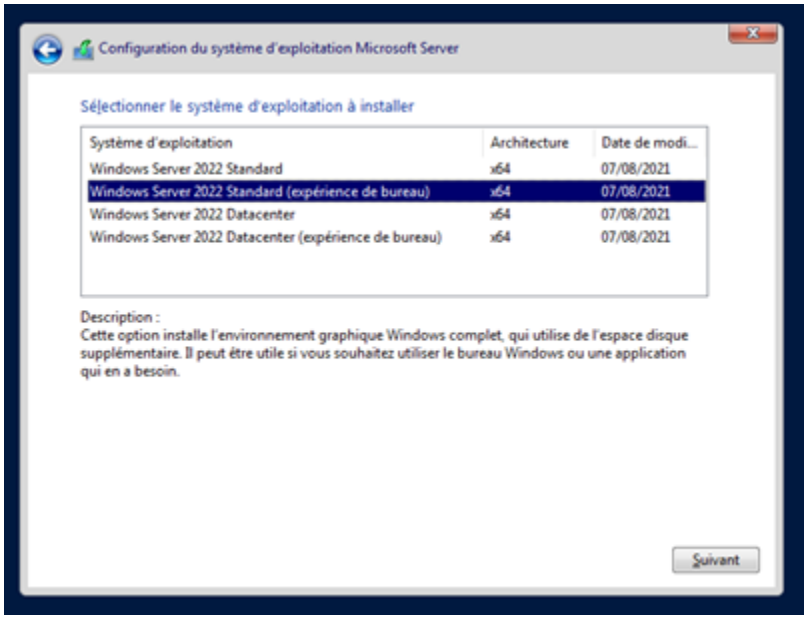


Saisissez la clef de produit (ou choisissez de la saisir plus tard) :

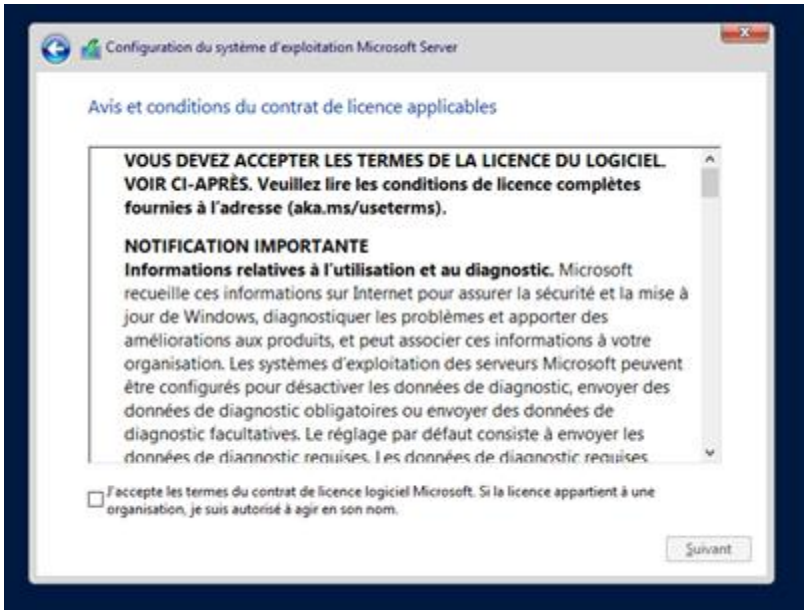


Choix du type d'installation :

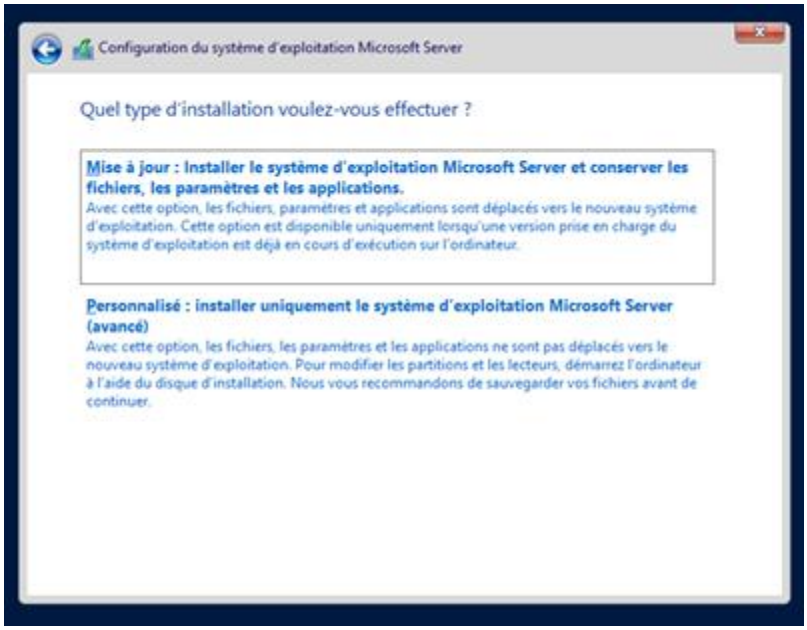
Attention le choix peut varier suivant la clef de produit saisie, ici nous allons choisir la version Windows Server 2022 Standard (expérience du bureau) :



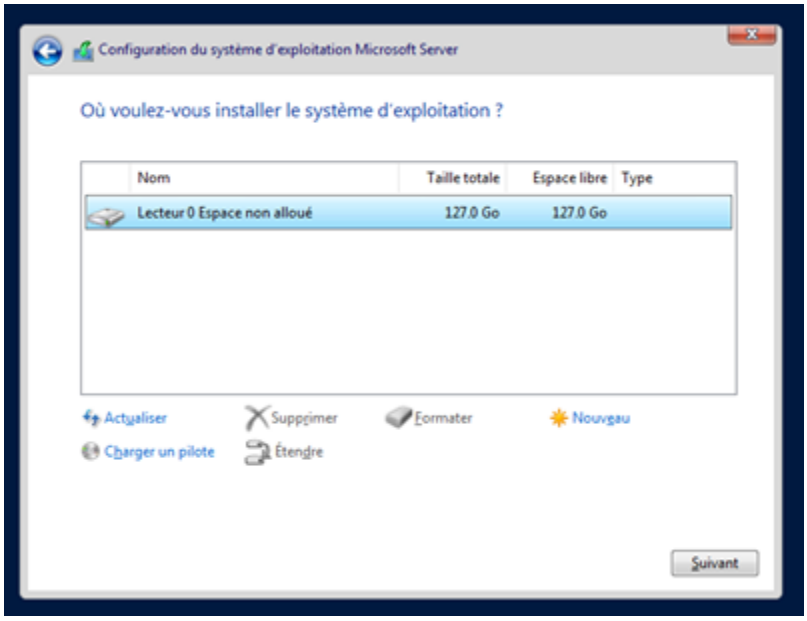
Acceptez le contrat de licence :



Sélectionnez ensuite le type d'installation, personnellement je ne vous recommande jamais de faire une mise à jour pour un serveur en production :

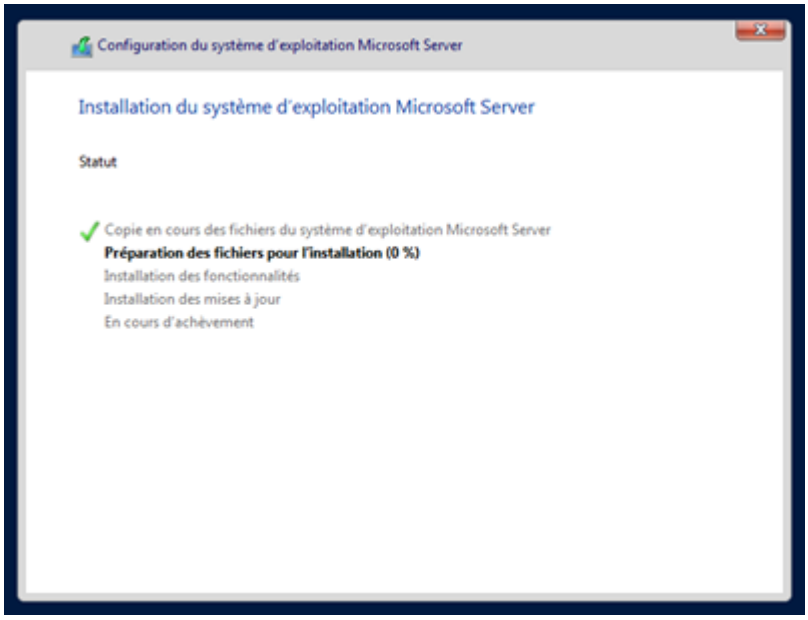


Sélectionnez le disque et la partition sur lesquels vous souhaitez installer le système (minimum 32 Go) puis cliquez sur Suivant :

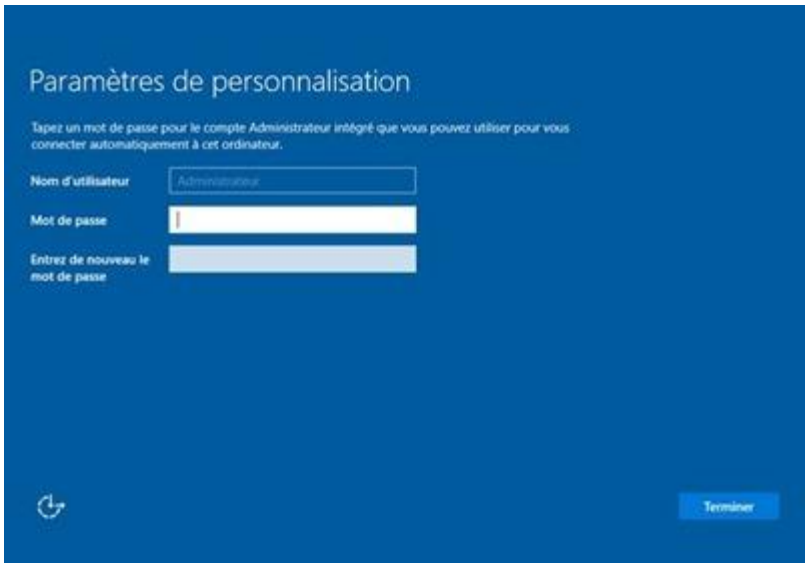


Si vous ne voyez pas de disque dans la liste, il est possible que la carte contrôleur de votre disque (SCSI, RAID, …) nécessite un pilote spécial, dans ce cas, cliquez sur “Charger un pilote”.

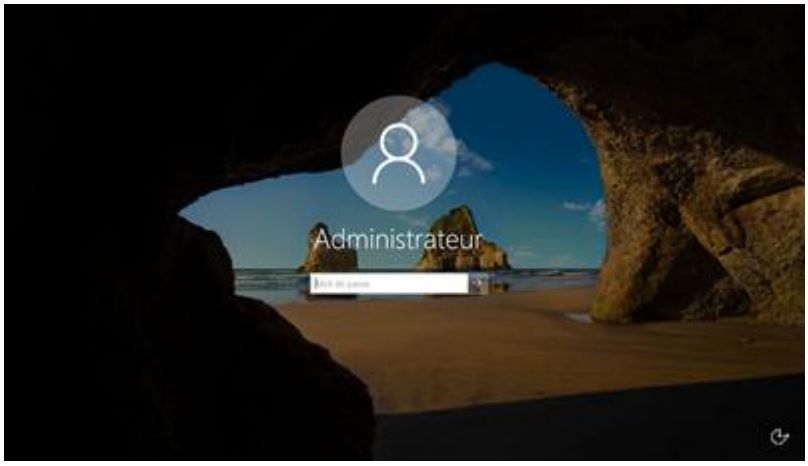
l’installation commence :



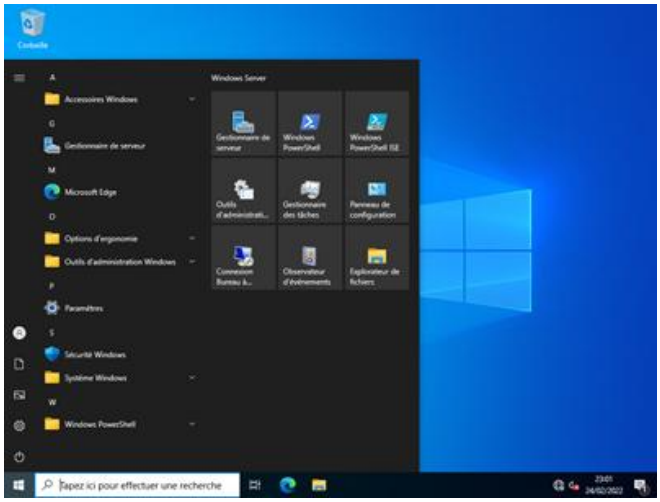
Le serveur va redémarrer… plusieurs fois.



Vous pouvez ouvrir la session en saisissant le mot de passe, taper précédemment :



Vous arrivez sur le bureau :

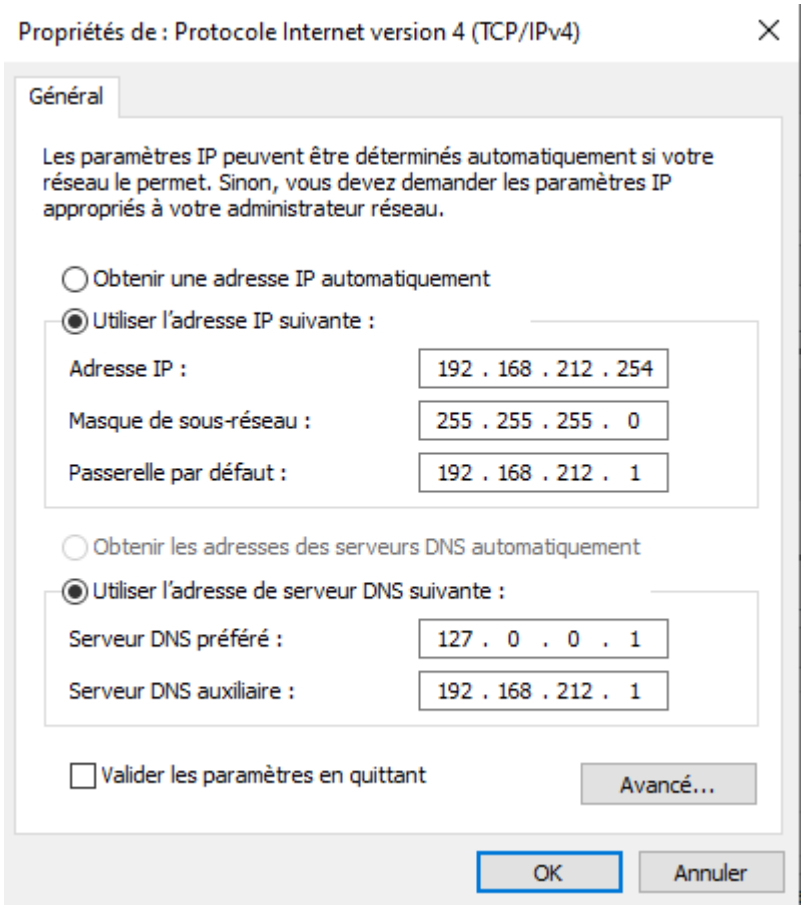


Maintenant que vous avez ouvert votre session, vous pouvez découvrir le Gestionnaire de Serveur :

Passons, maintenant à la partie la plus intéressante la configuration (;

2.4/Configuration IP de l'AD :

Premièrement, on va commencer à configurer notre carte réseau, en allant dans Panneau de configuration -> Réseau et Internet -> Centre Réseau et partage puis cliquer sur « Ethernet 0 » :

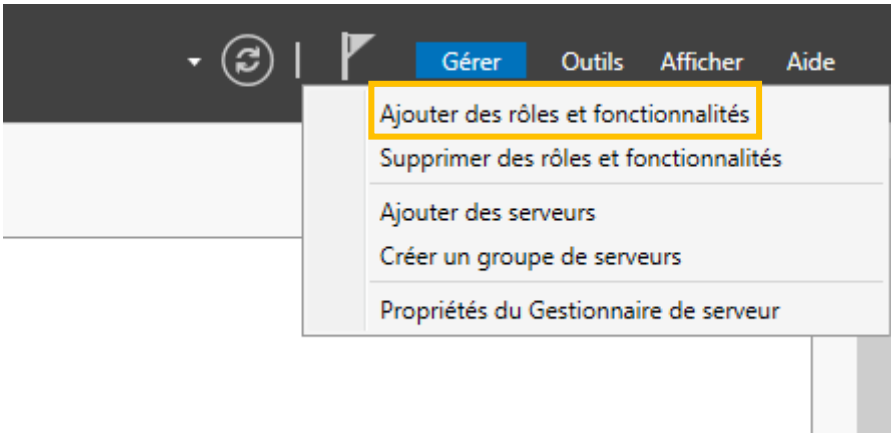


Information : Ces Informations doivent correspondre à votre schéma réseau.

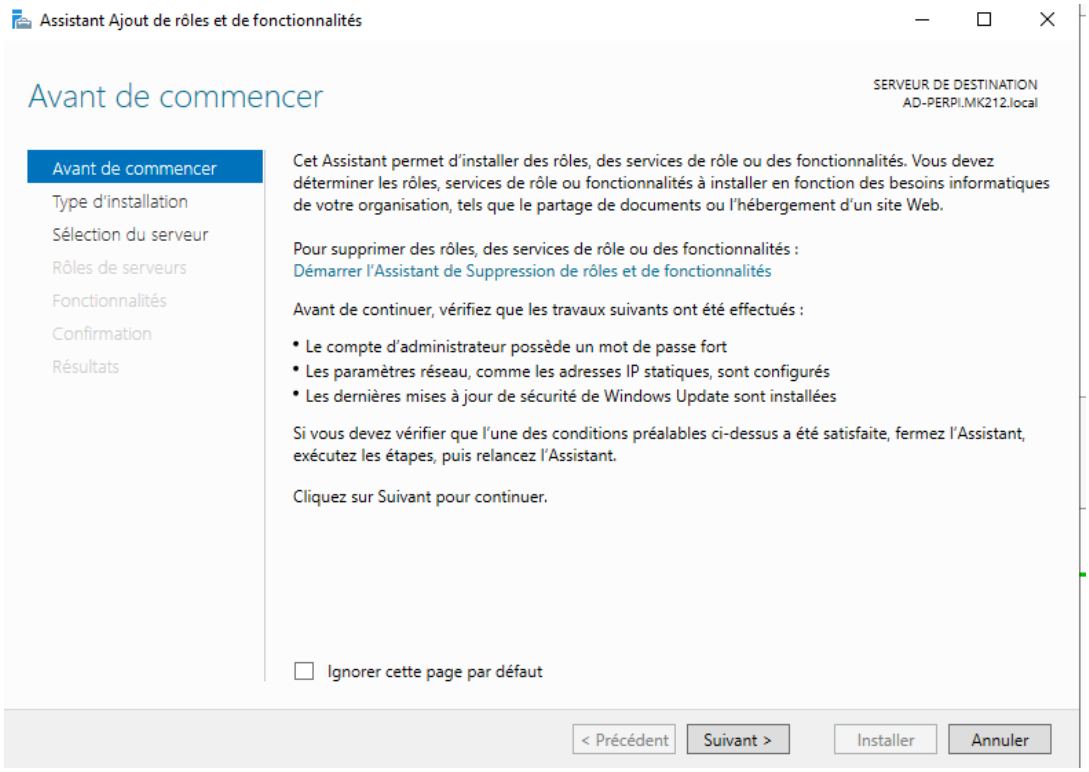
Dans mon cas « 192.168.212.1 » est ma passerelle (Lan-Perpi) OPNsense.

2.3/Crée un domaine AD DS

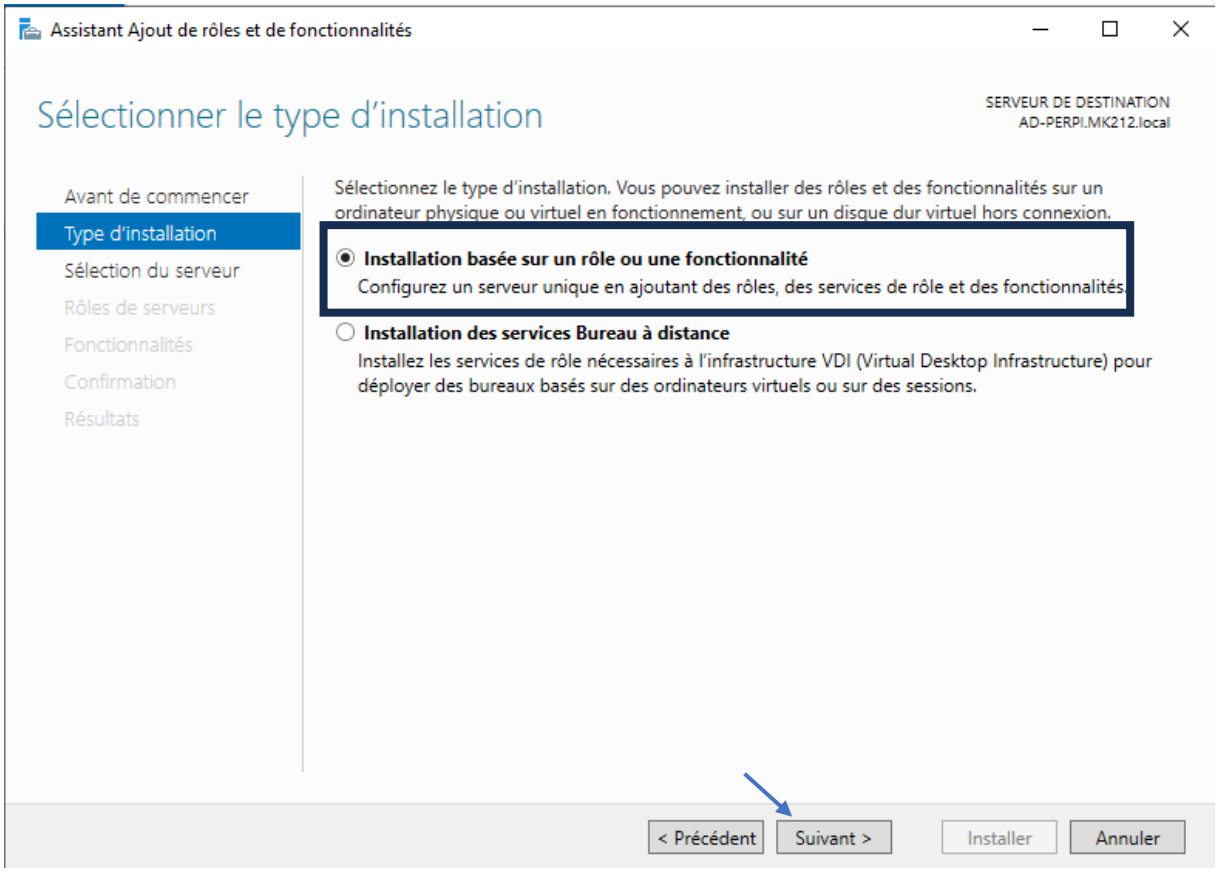
Aller dans le Gestionnaire de serveur :



Puis :



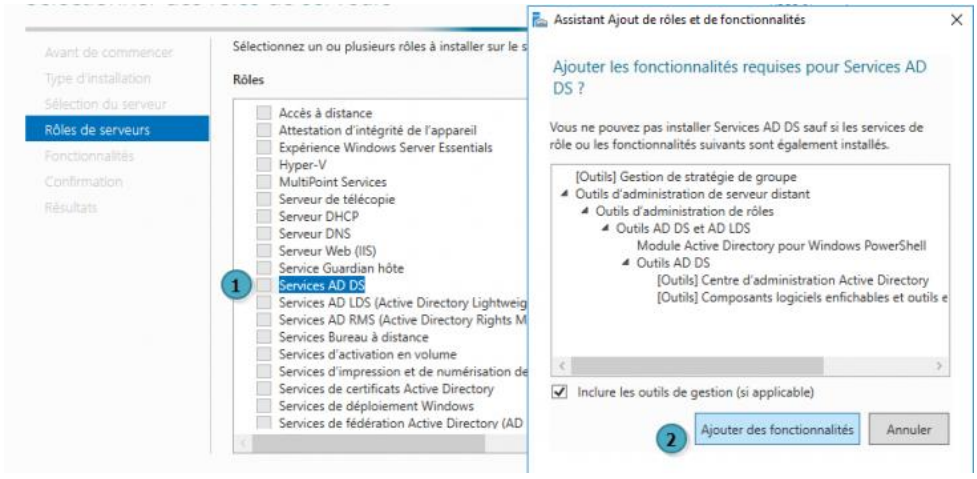
Cliquer sur « Suivant »



Continuer sur suivant à sélection du serveur.

Puis :

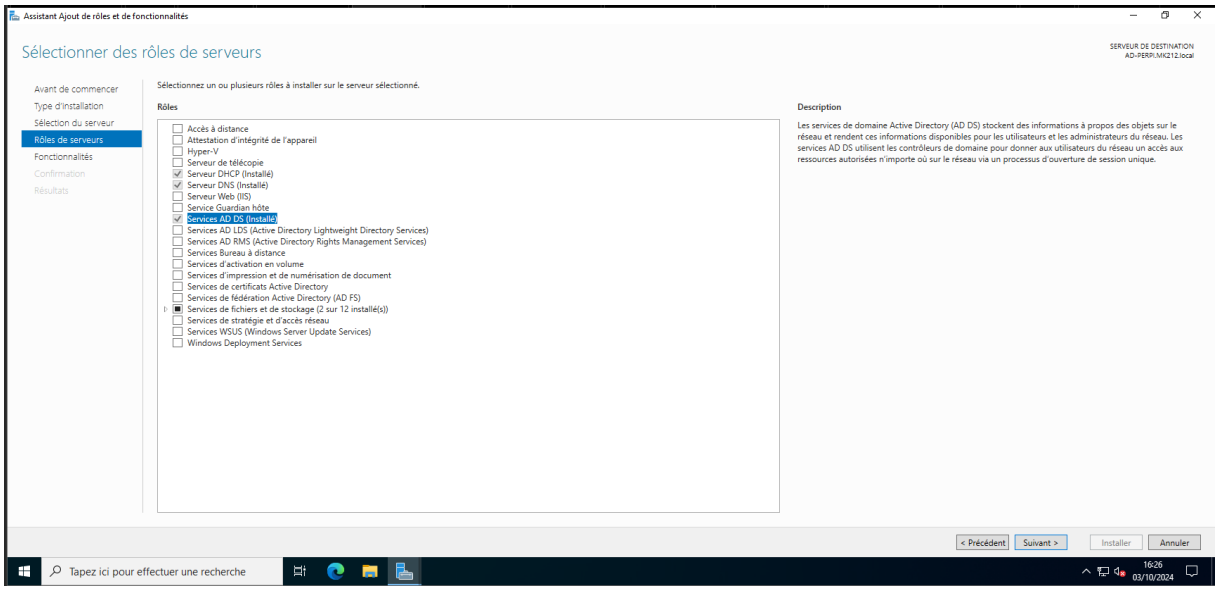
Sélectionner Services AD DS et Ajouter des fonctionnalités :

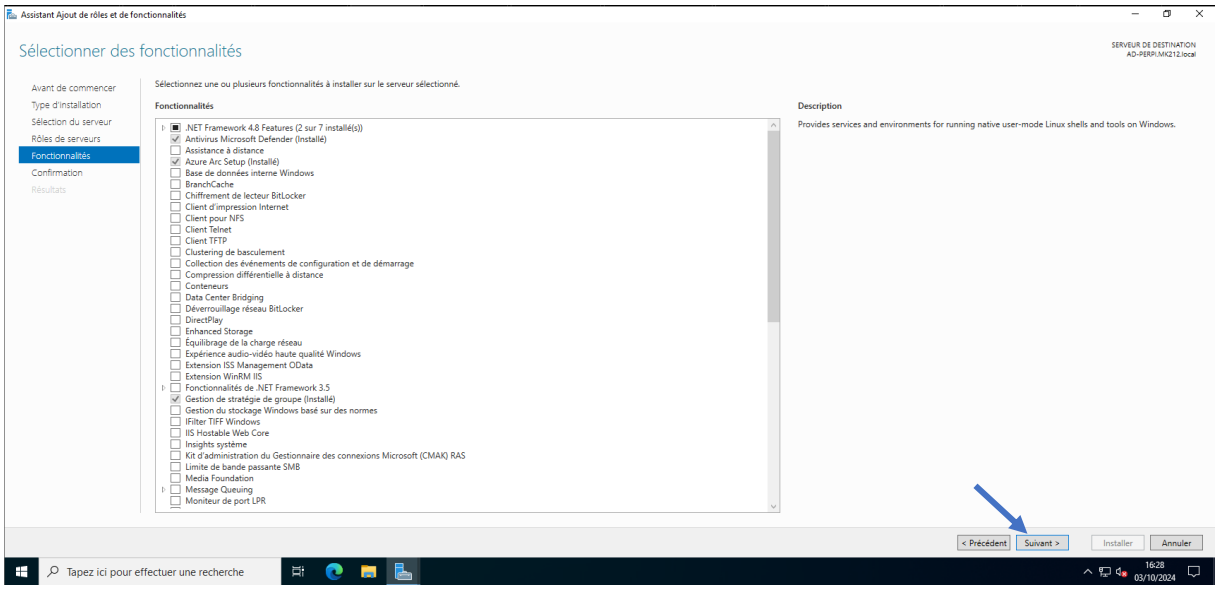


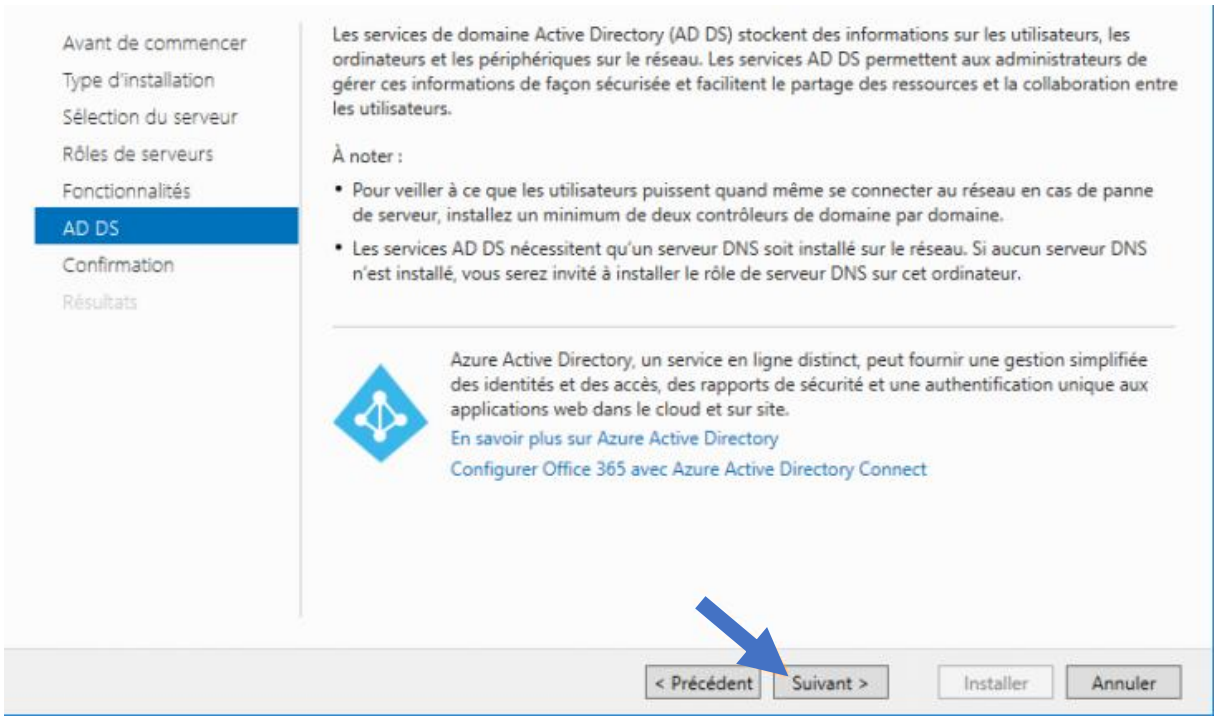
Facultatif : On peut ajouter également le « DNS » et le « DHCP » pour donner au client une configuration dynamique.

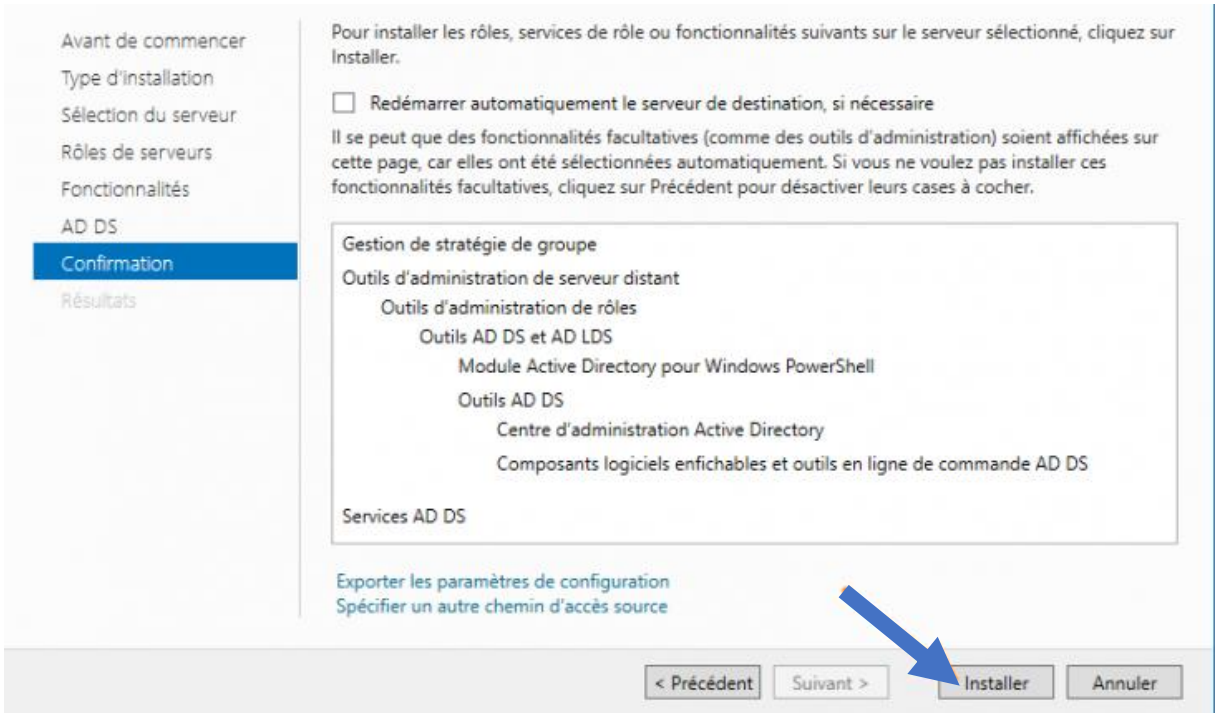
Il faudra sélectionner alors :

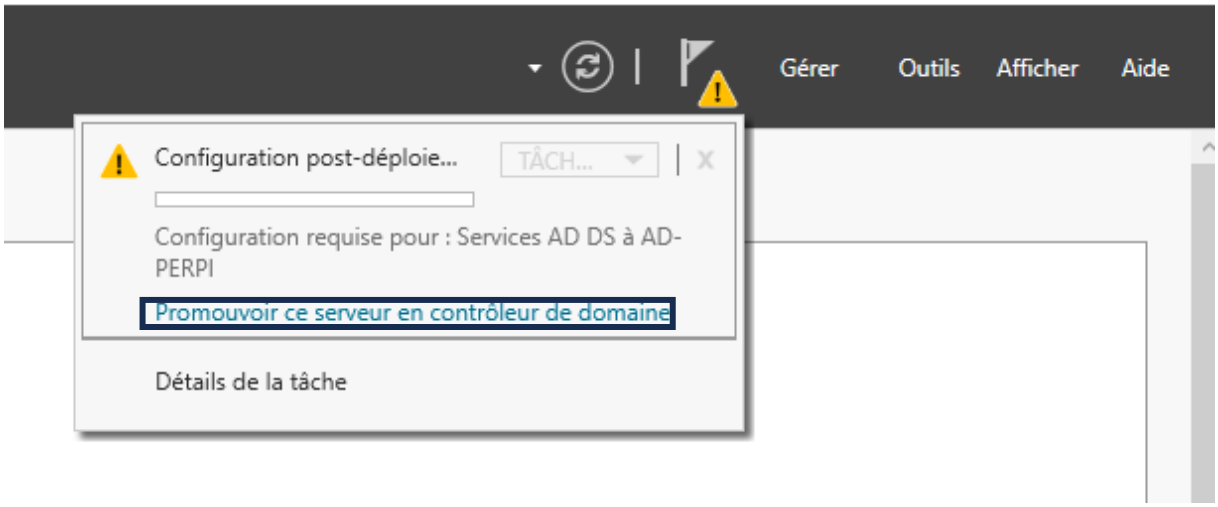
Services DHCP et DNS.



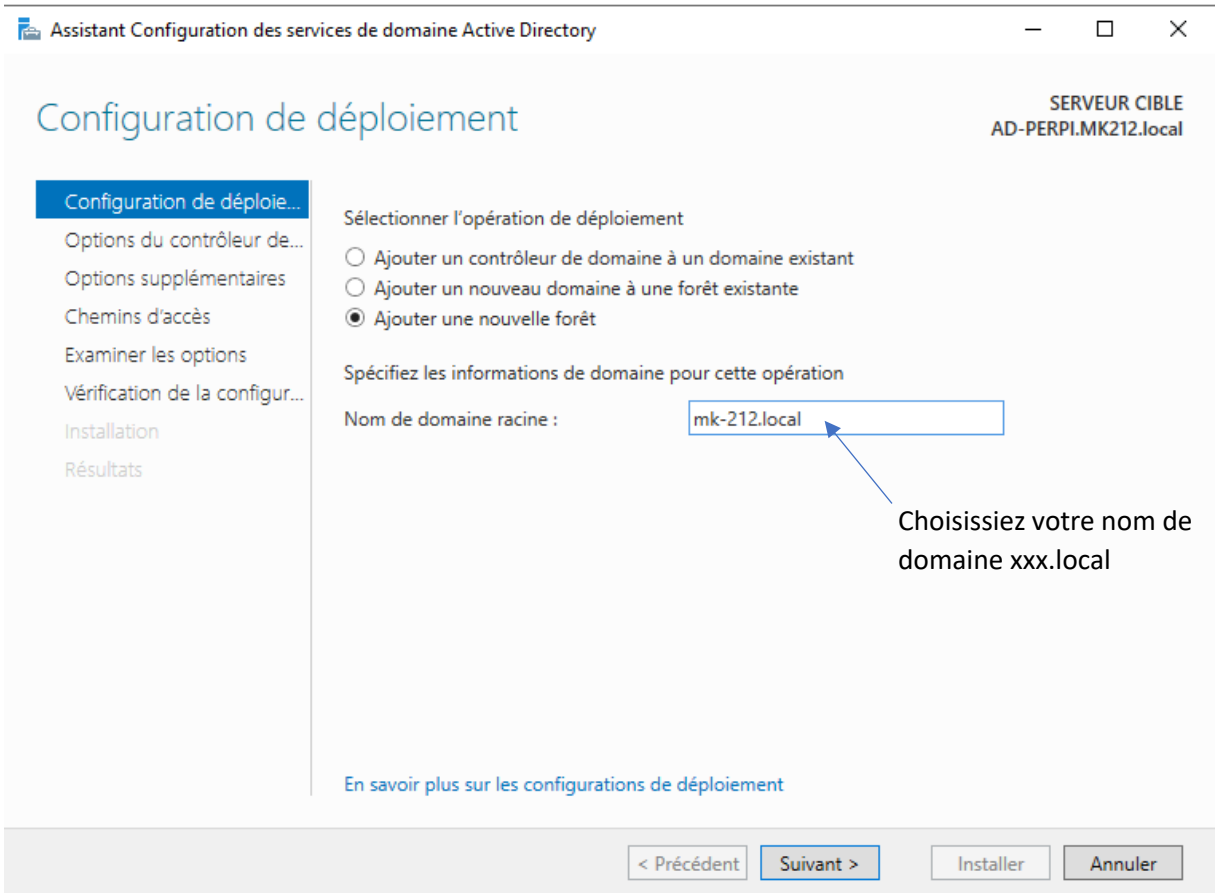



Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD DS
Confirmation
Résultats
Les services de domaine Active Directory (AD DS) stockent des informations sur les utilisateurs, les ordinateurs et les périphériques sur le réseau. Les services AD DS permettent aux administrateurs de gérer ces informations de façon sécurisée et facilitent le partage des ressources et la collaboration entre les utilisateurs.
À noter :
Pour veiller à ce que les utilisateurs puissent quand même se connecter au réseau en cas de panne de serveur, installez un minimum de deux contrôleurs de domaine par domaine.
Les services AD DS nécessitent qu'un serveur DNS soit installé sur le réseau. Si aucun serveur DNS n'est installé, vous serez invité à installer le rôle de serveur DNS sur cet ordinateur.
Azure Active Directory, un service en ligne distinct, peut fournir une gestion simplifiée des identités et des accès, des rapports de sécurité et une authentification unique aux applications web dans le cloud et sur site.
En savoir plus sur Azure Active Directory
Configurer Office 365 avec Azure Active Directory Connect
< Précédent
Suivant >
Installer
Annuler

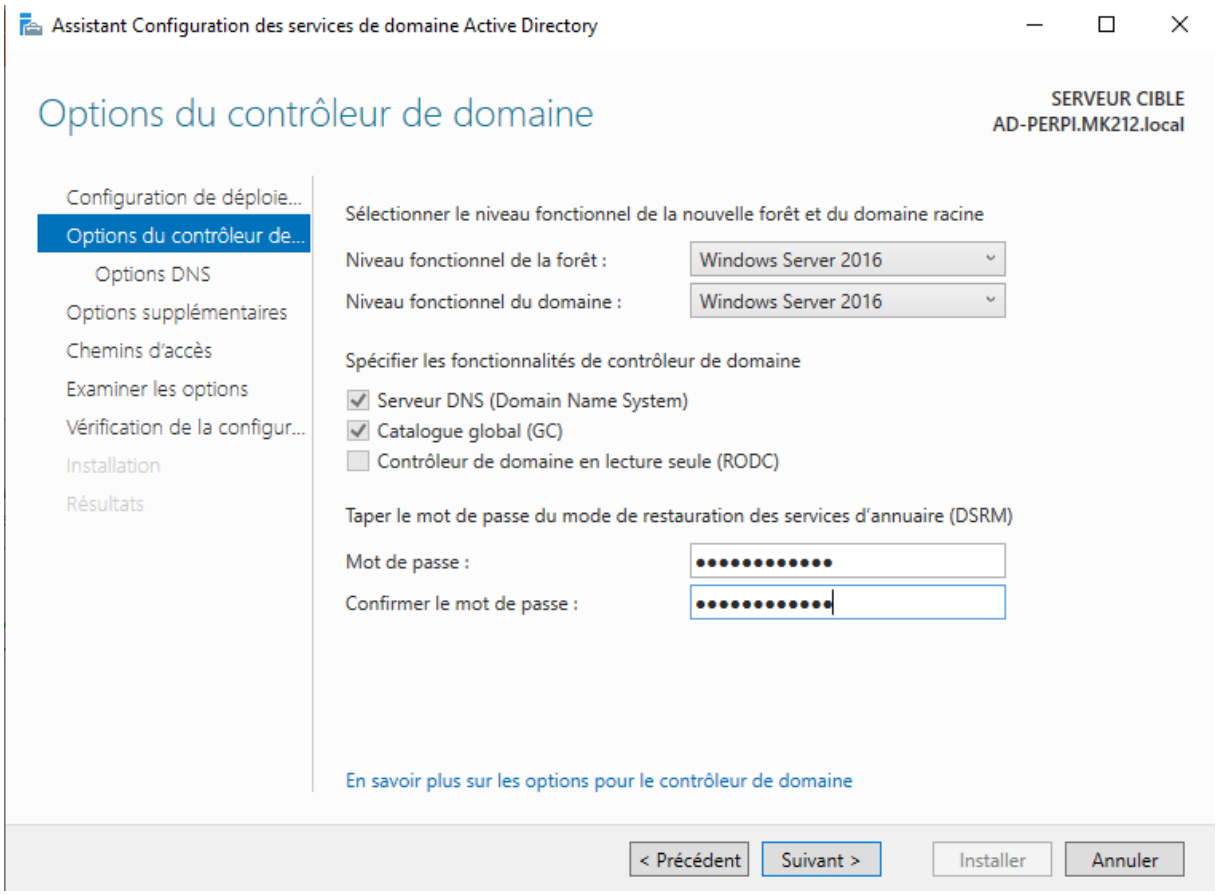

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
AD DS
Confirmation
Résultats
Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.
Redémarrer automatiquement le serveur de destination, si nécessaire
Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.
Gestion de stratégie de groupe
Outils d'administration de serveur distant
Outils d'administration de rôles
Outils AD DS et AD LDS
Module Active Directory pour Windows PowerShell
Outils AD DS
Centre d'administration Active Directory
Composants logiciels enfichables et outils en ligne de commande AD DS
Services AD DS
Exporter les paramètres de configuration
Spécifier un autre chemin d'accès source
< Précédent
Suivant >
Installer
Annuler



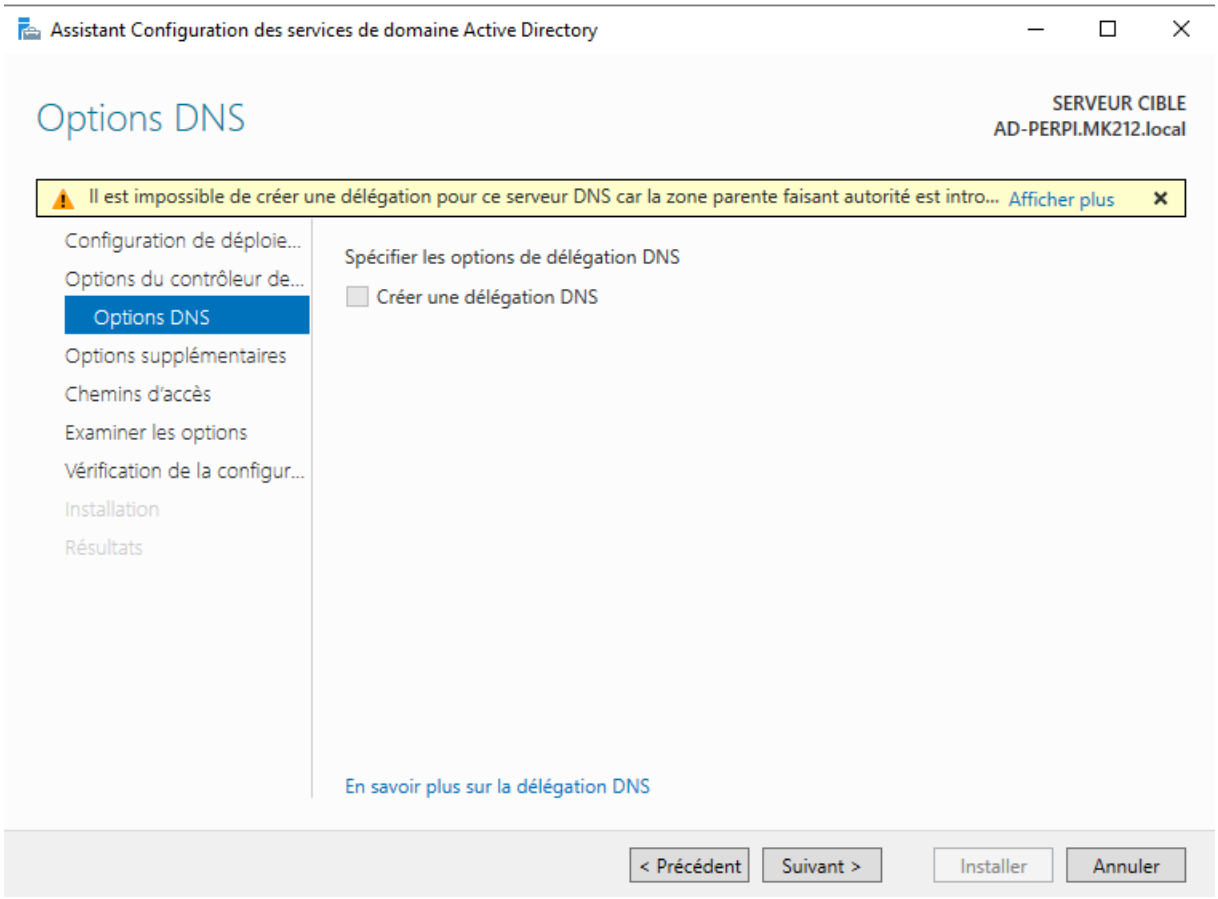
Étant donné qu'il s'agit d'un domaine inconnu au sein d'une forêt nouvellement créée, sélectionnez l'option « Ajouter une nouvelle forêt » et saisissez le nom de domaine souhaité. Il est important de noter que l'utilisation d'un nom de domaine tel que « mk-212.local » le rendra non routable, ce qui peut entraîner des complications avec des services spécifiques.



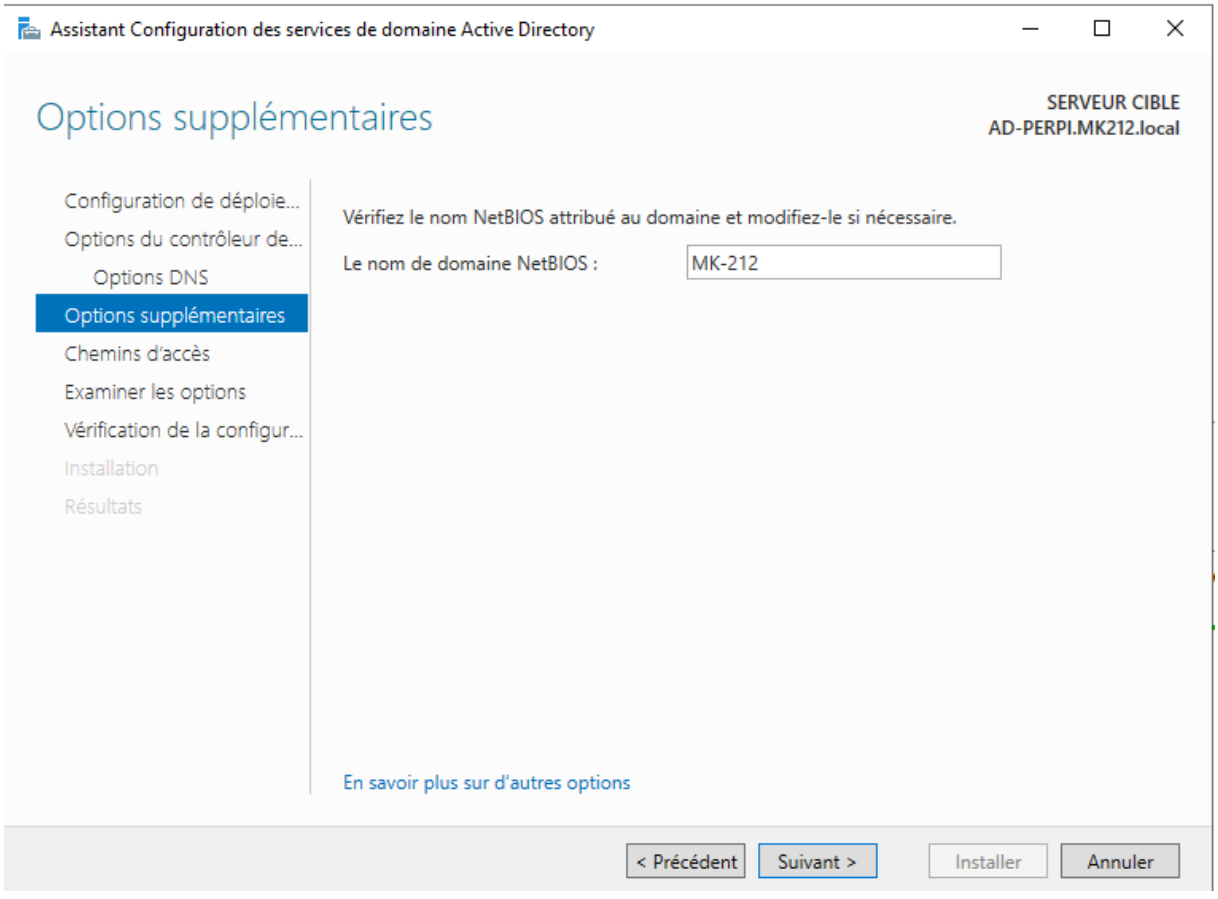
Choisissiez votre propre mot de passe.



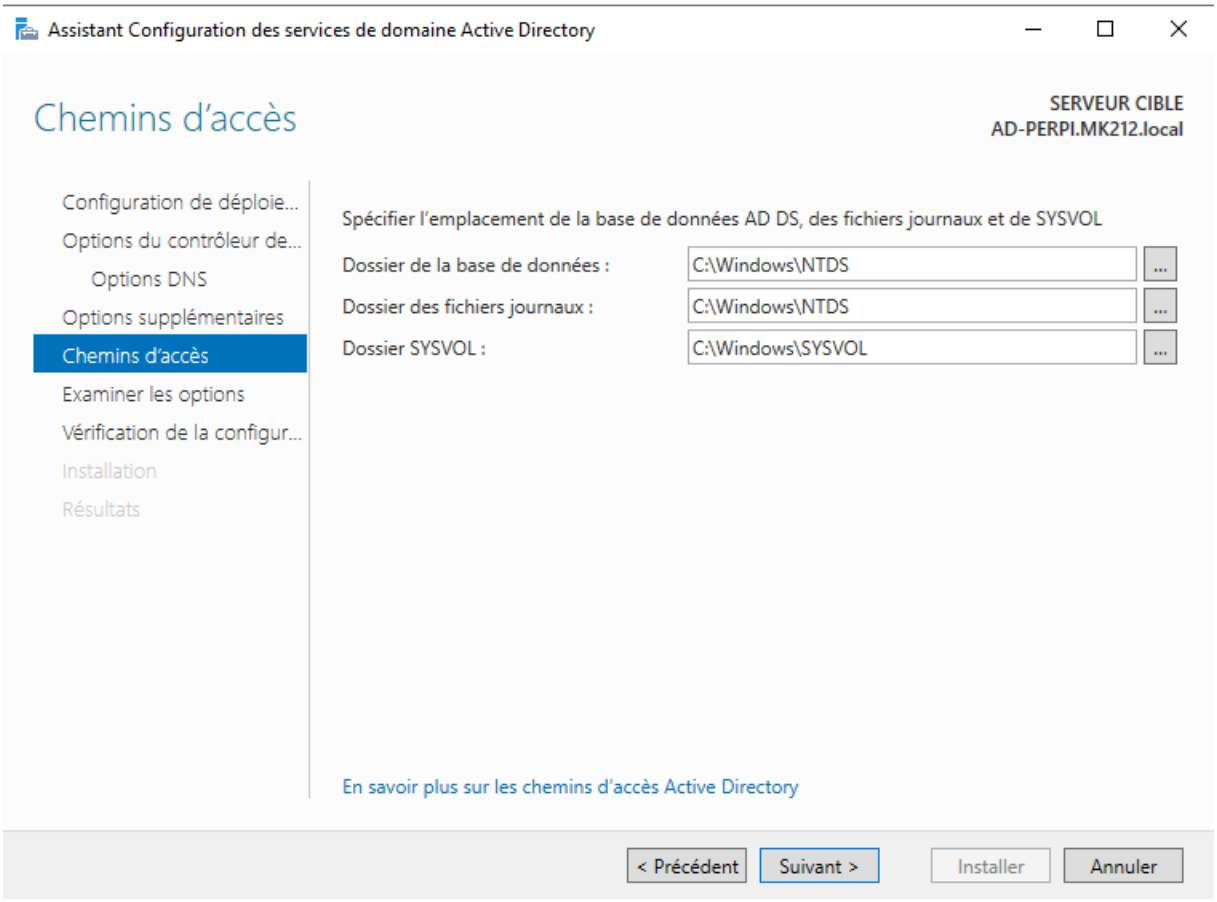
Comme il s'agit d'un nouveau serveur DNS pour une nouvelle zone, ne vous inquiétez pas pour ce message, vous pouvez poursuivre.



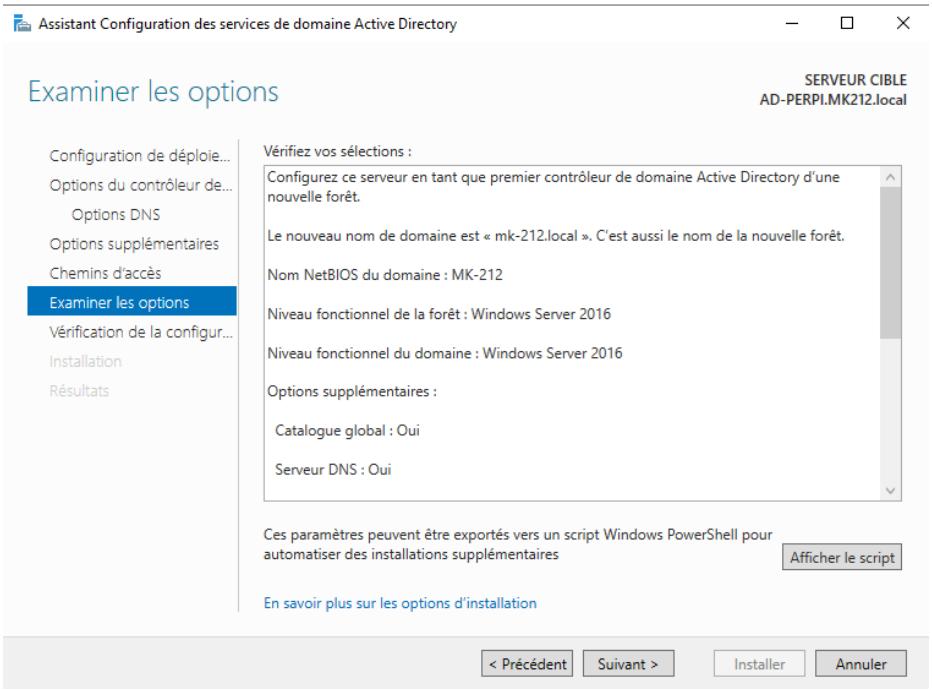
Cliquer sur « Suivant »



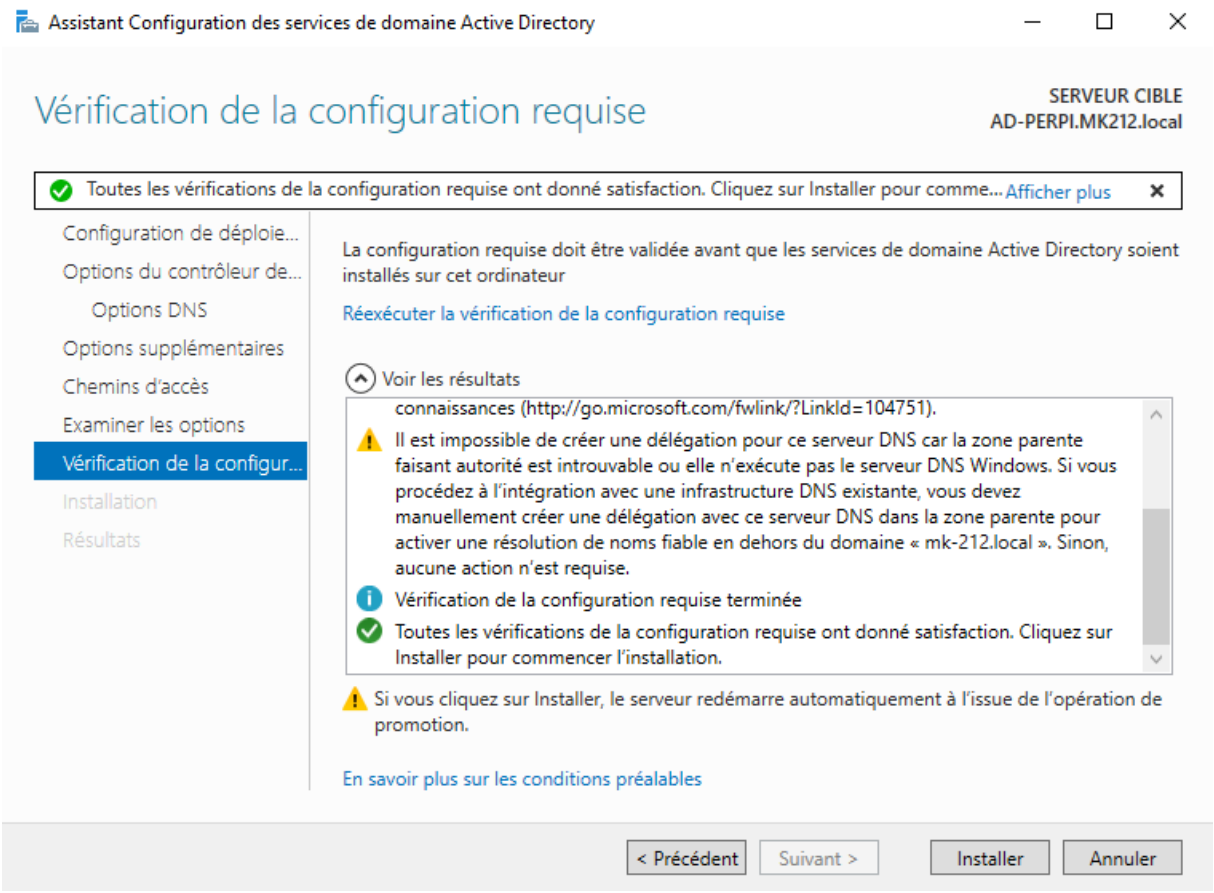
Laissez les chemins par défaut et poursuivez.



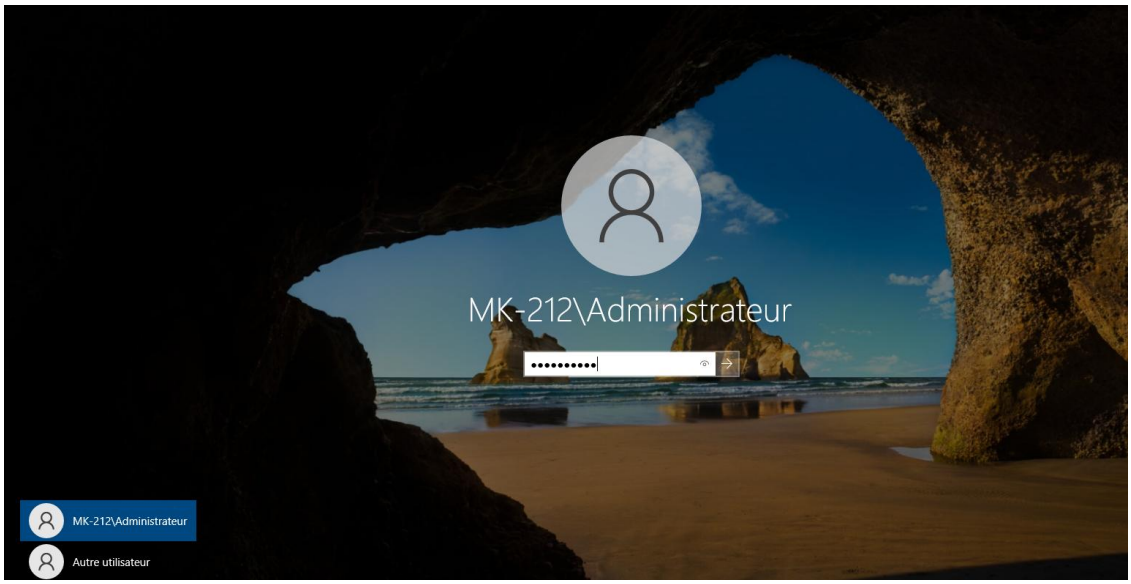
Vérifiez les options et continuez.



Finissez en cliquant sur installer pour démarrer la création de votre domaine et la configuration du DC.



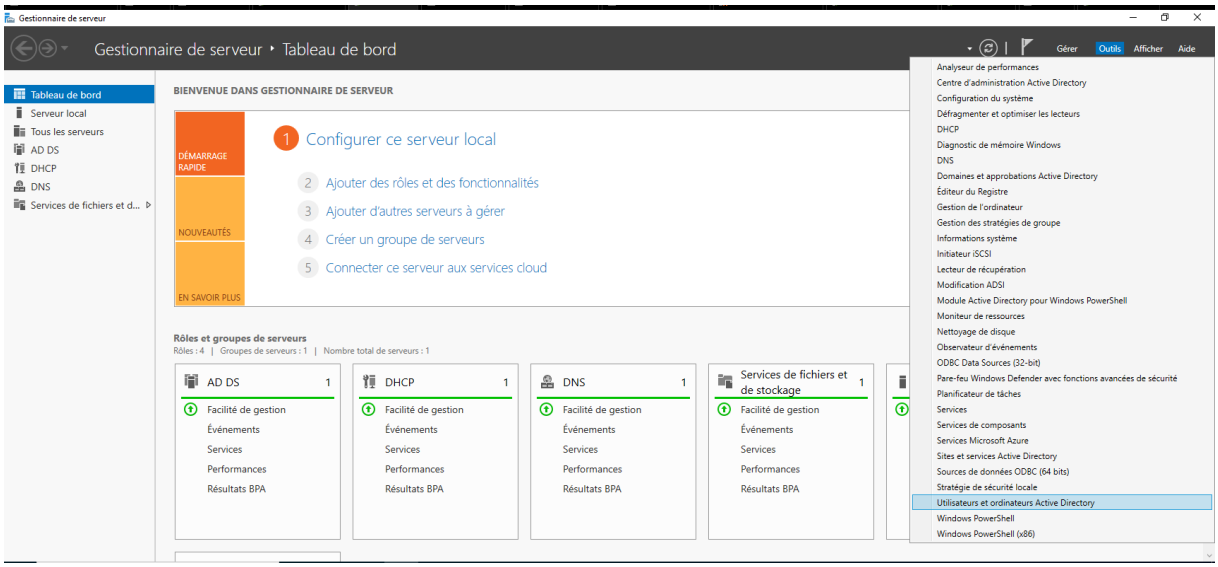
Votre serveur va redémarrer, une fois redémarrer vous verrez que votre ad est bien rentrer dans le domaine :



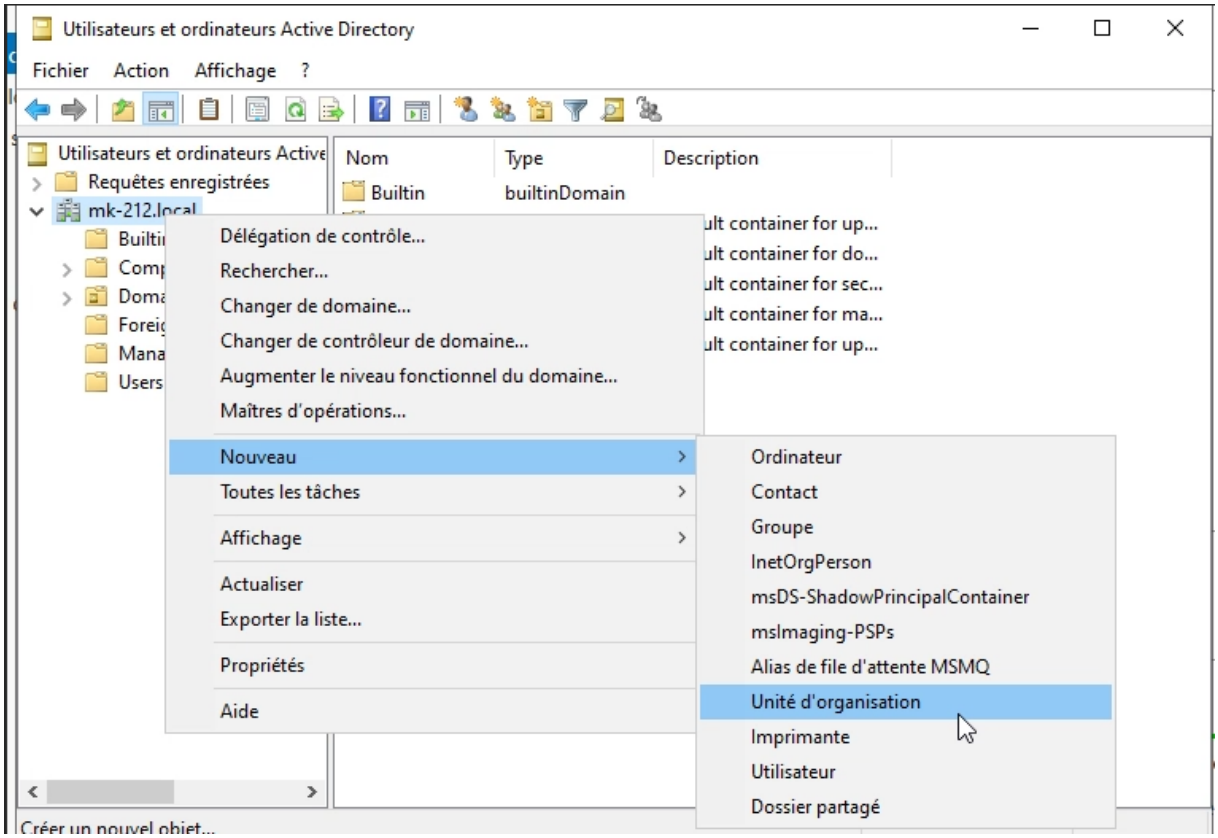
2.5/Configuration de l'AD :

Nous allons maintenant créer les utilisateurs pour notre AD.

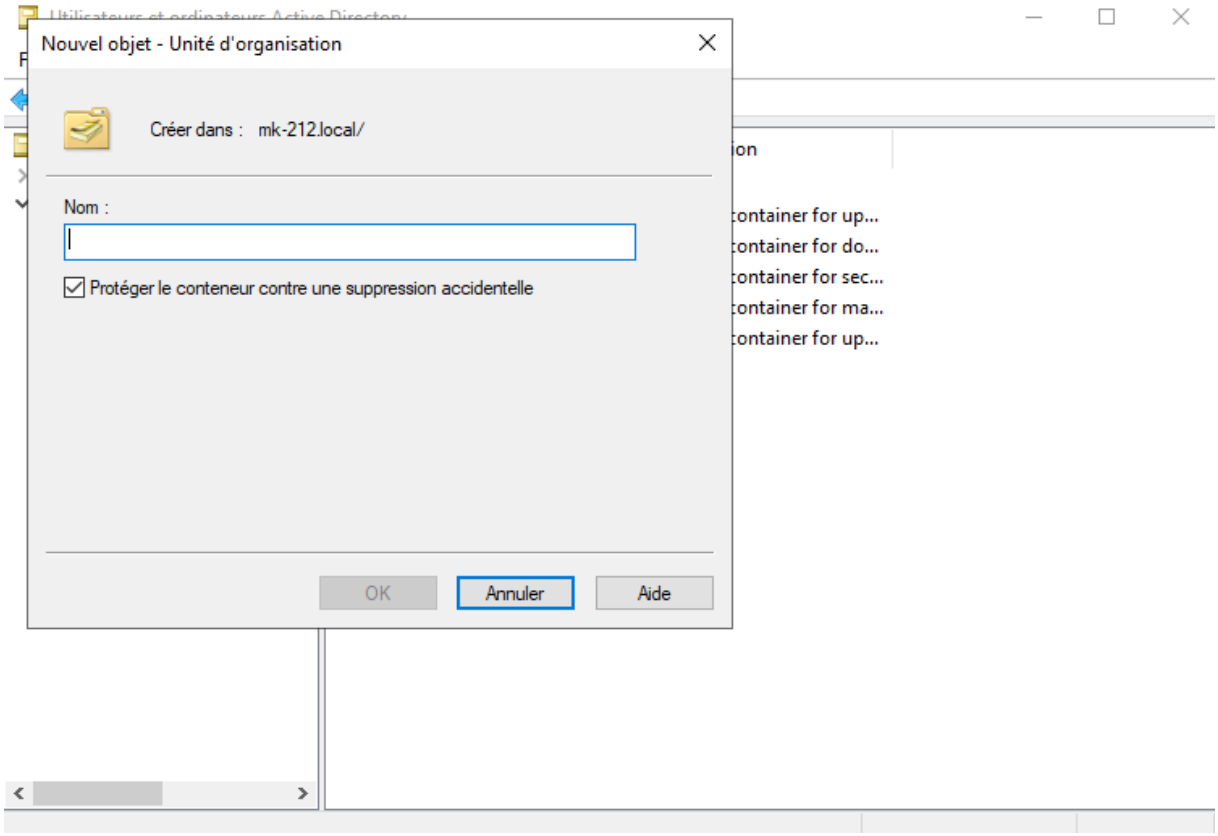
Allez dans « Utilisateurs et ordinateurs Active Directory »



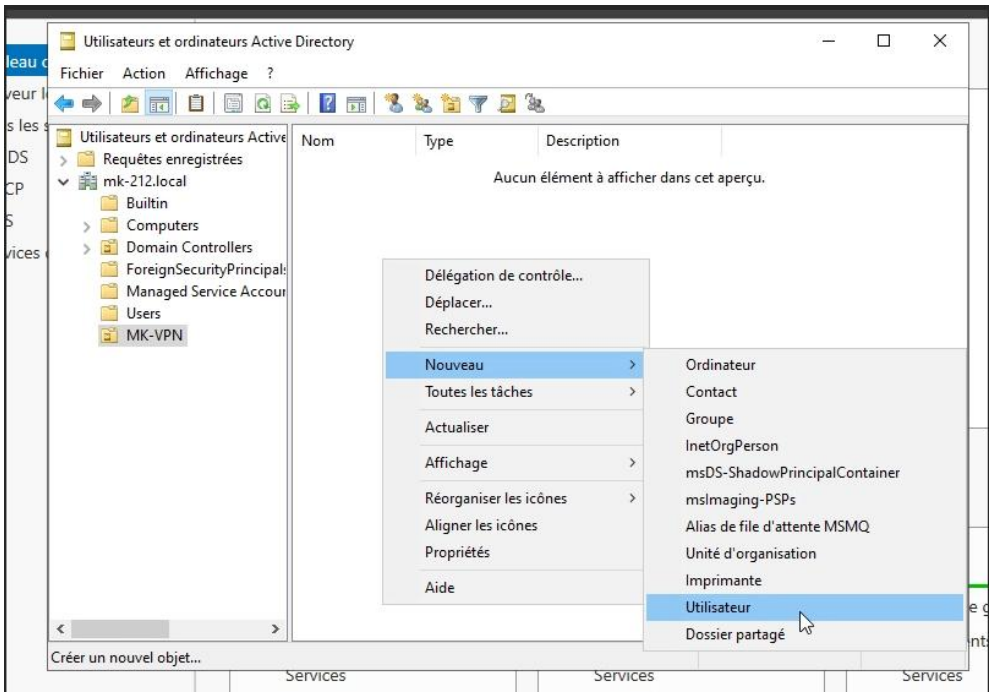
Nous devons crée une nouvelle Unité Organisation (UO)



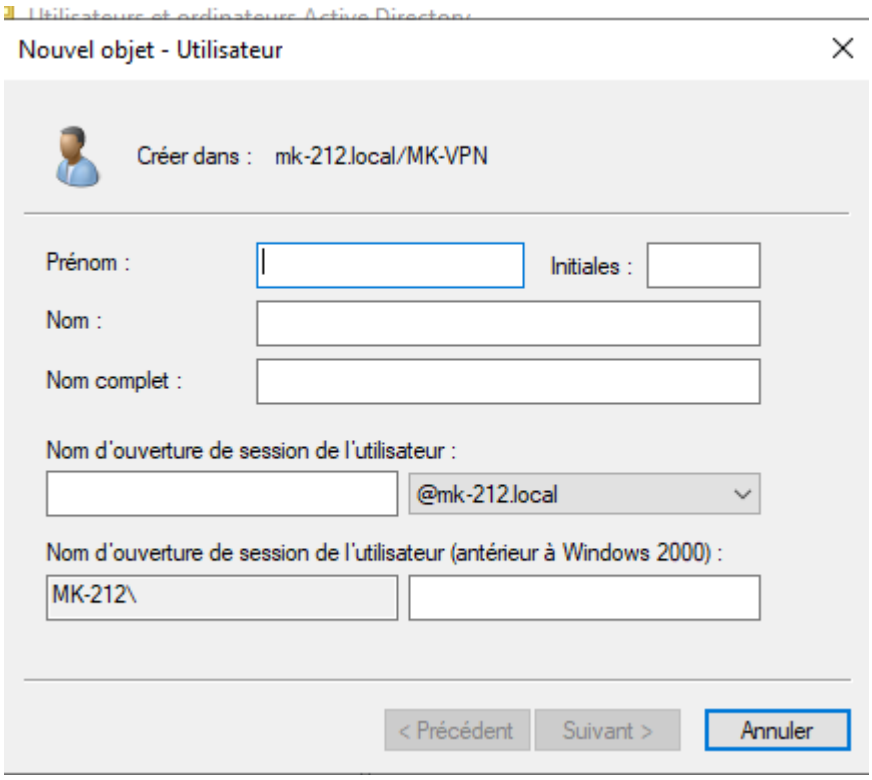
Ajouter votre nom d'organisation.



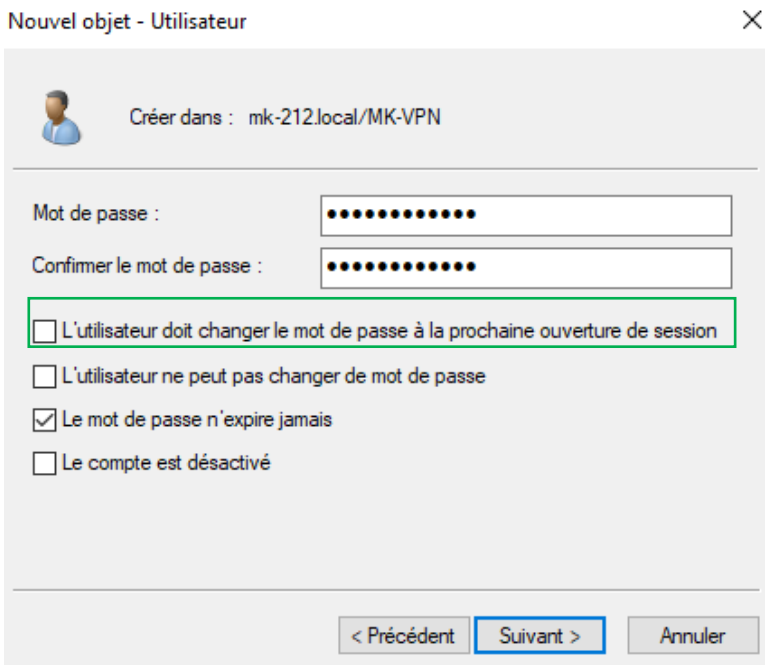
Crée maintenant, un nouvel utilisateur :



Remplissez les informations de votre nouvel utilisateur.



Puis-ajouter le mot de passe qui peut-être changer par l'utilisateur à l'ouverture de sa session (Si option coché).

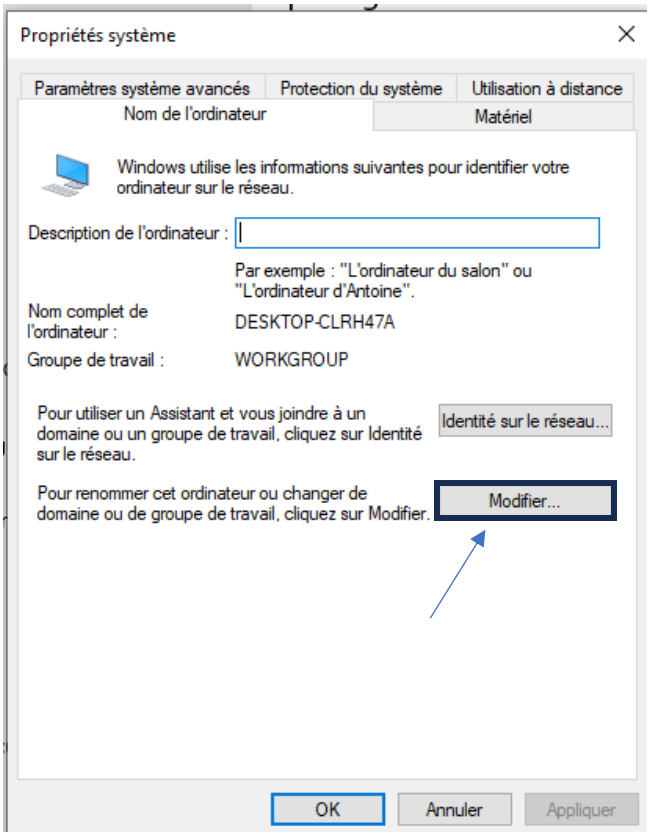


Une fois terminé, aller sur le poste client et changer l'adresse IP, si vous n'avez pas mis de DHCP sur votre AD sinon dans l'invité de commande taper « ipconfig /release puis ipconfig /renew »

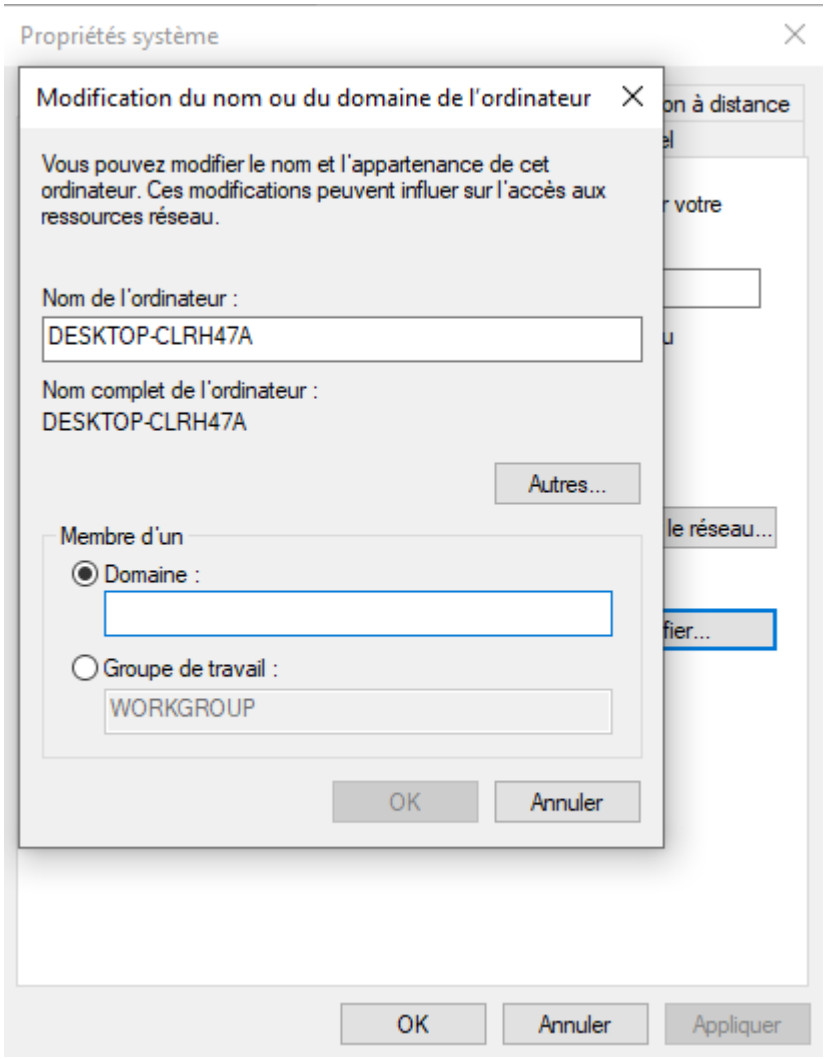
```
arte Ethernet Ethernet1 :

 Suffixe DNS propre à la connexion. . . : MK212.local
 Description. . . . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection #2
 Adresse physique . . . . . . . . . . . : 00-0C-29-95-0B-4E
 DHCP activé. . . . . . . . . . . . . . : Oui
 Configuration automatique activée. . . : Oui
 Adresse IPv6 de liaison locale. . . . .: fe80::c2c1:9c15:cce4:5b4d%31(préféré)
 Adresse IPv4. . . . . . . . . . . . . .: 192.168.212.101(préféré)
 Masque de sous-réseau. . . . . . . . . : 255.255.255.0
 Bail obtenu. . . . . . . . . . . . . . : jeudi 3 octobre 2024 17:42:28
 Bail expirant. . . . . . . . . . . . . : vendredi 11 octobre 2024 17:42:28
 Passerelle par défaut. . . . . . . . . : fe80::20c:29ff:fece:8942%31
                                         192.168.212.1
 Serveur DHCP . . . . . . . . . . . . . : 192.168.212.254
 IAID DHCPv6 . . . . . . . . . . . : 671091753
 DUID de client DHCPv6. . . . . . . . : 00-01-00-01-2E-72-1F-DC-00-0C-29-95-0B-44
 Serveurs DNS. . .  . . . . . . . . . . : 192.168.212.254
 NetBIOS sur Tcpip. . . . . . . . . . . : Activé
```

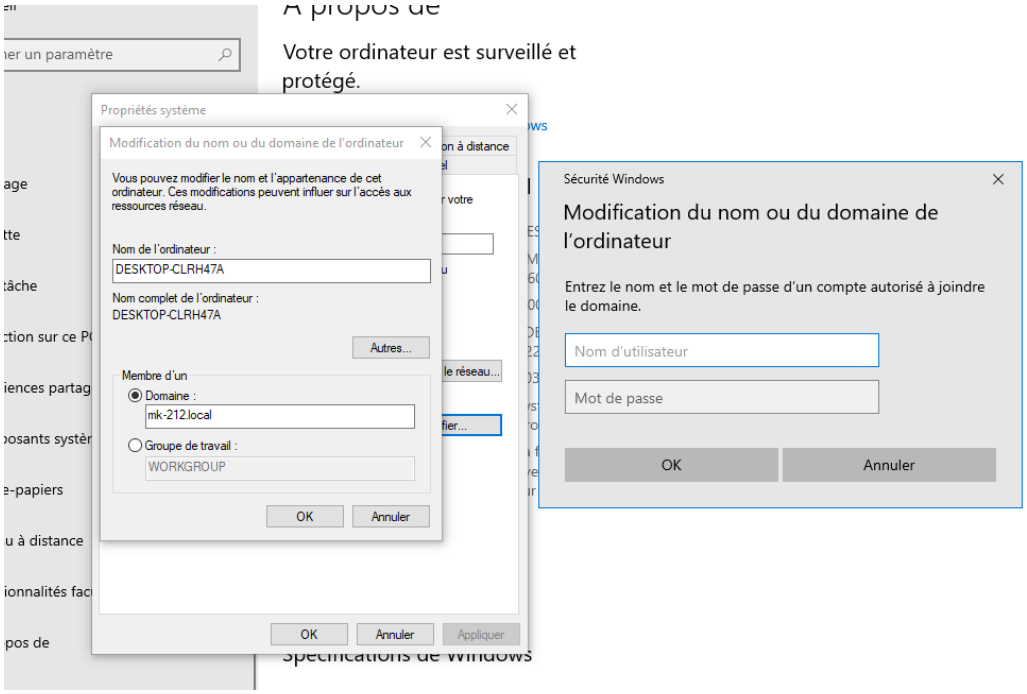
Pour rentrer dans le client dans l'AD, il faut aller dans les paramètres puis Système -> A propos de – Renommer ce PC (Avancé) :



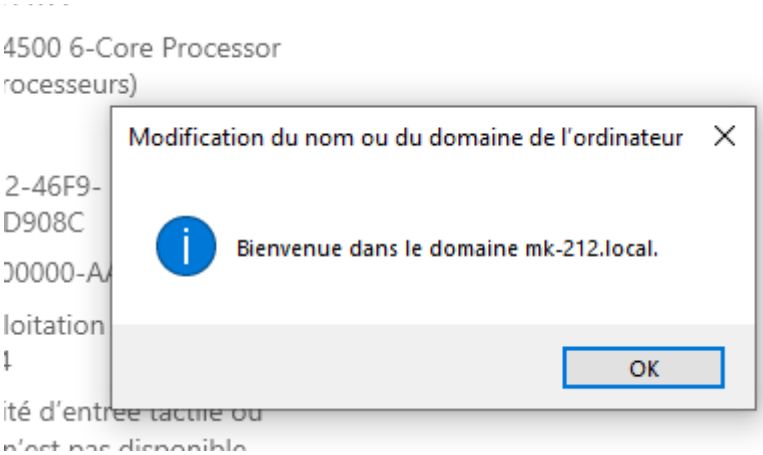
Entrer votre nom de domaine ----.local



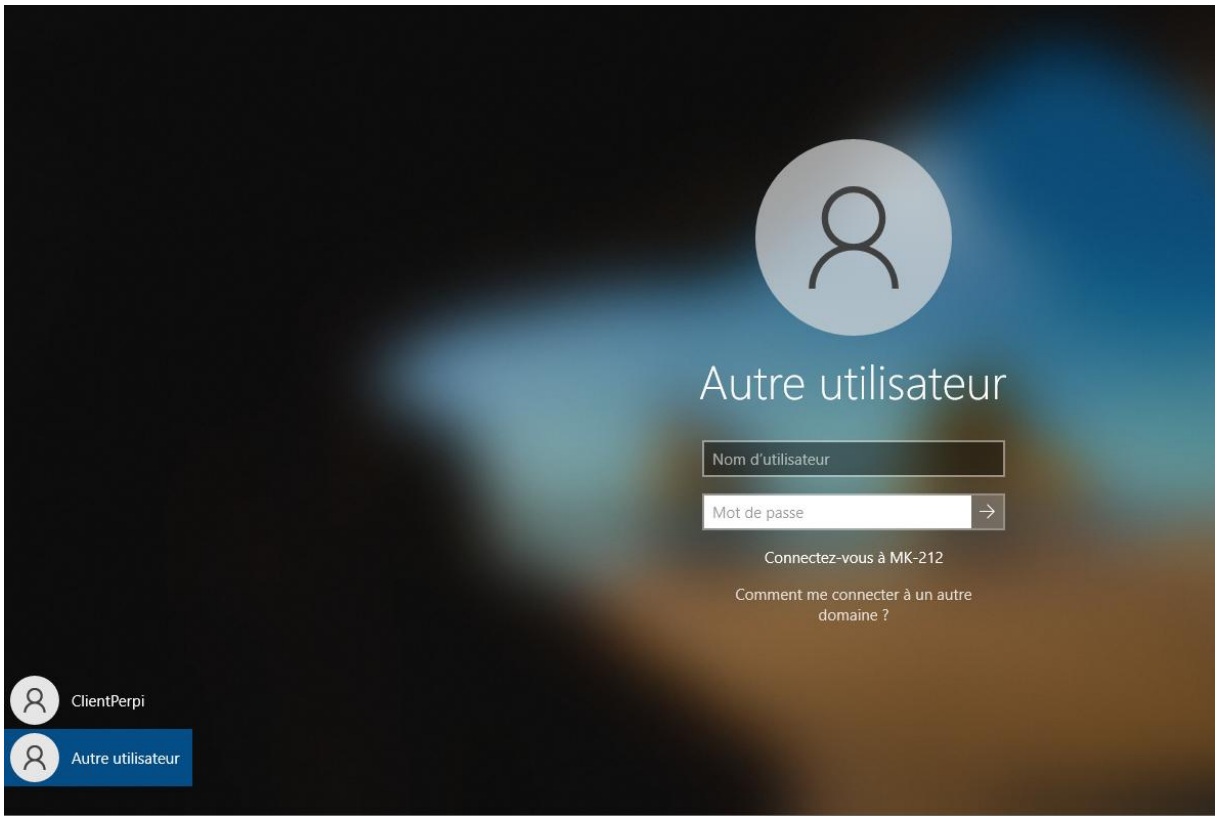
Entrer vos données de connexion :



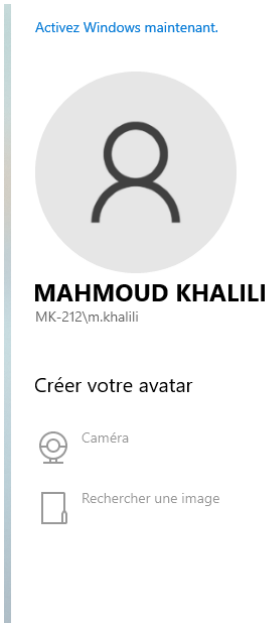
Vous devrez obtenir ça après avoir valider, cliquer sur OK puis cliquer sur « redémarrer maintenant » :



Cliquer sur autre utilisateur et entrer vos données de connexions :



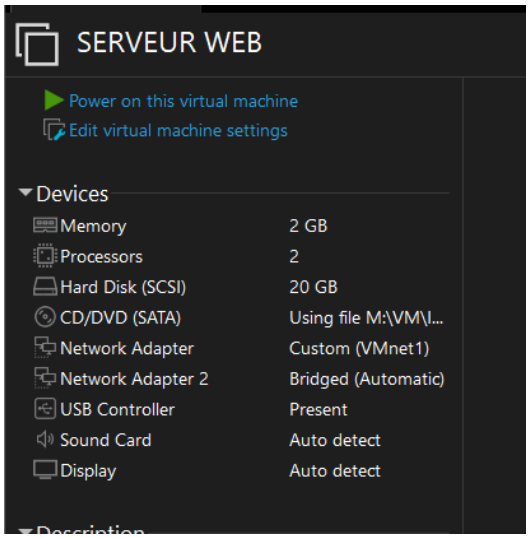
Cliquer sur paramètre puis information du compte et vous voilà dans le domaine :



3 /Configuration d'un Serveur Web sur VM Linux

3.1/Mise en place de la machine virtuelle :

Pour faire le serveur web, j'ai choisi d'utiliser une VM Linux sans interface graphique pour minimiser les consommations de ressources. Cette VM aura deux cartes réseaux : une en Host-only et une en Bridge, qui vont nous servir à la configuration en SSH, que nous retirerons à la fin de la configuration.

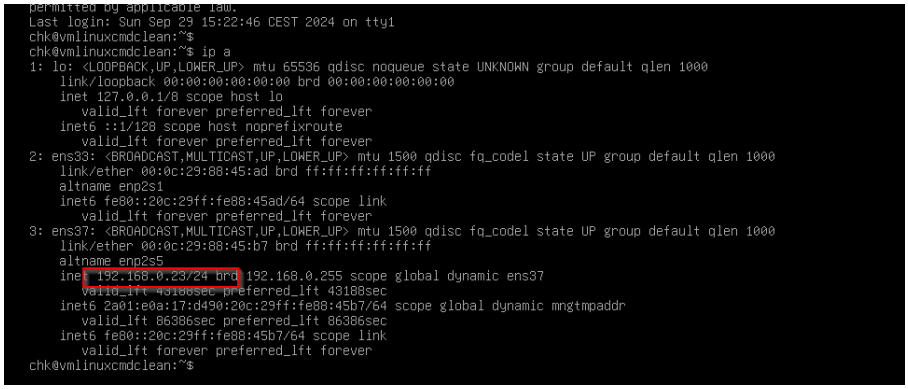


Voici un tuto pour installer Linux sans interface graphique :

https://goopensource.fr/debian-installation-sans-interface-graphique/

Une fois la VM créée, on peut la démarrer et se connecter avec l'utilisateur. Il est conseillé de vérifier l'adresse IP de l'interface Bridge en utilisant la commande :

```
ip a
```



Si vous n'avez pas d'adresse IP, il faut rajouter la carte réseau dans le fichier "/etc/network/interfaces".

```
nano /etc/network/interfaces
```

```
 GNU nano 7.2                                /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet dhcp
# This is an autoconfigured IPv6 interface
iface ens33 inet6 auto

allow-hotplug ens37
iface ens37 inet dhcp
```

Nous allons modifier l'adresse ip du host-only (ens33).

```
source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet static
        address 192.168.200.11
        netmask 255.255.255.0
        gateway 192.168.200.1
# This is an autoconfigured IPv6 interfaceiface ens33 inet6 auto

allow-hotplug ens37
iface ens37 inet dhcp
```

La gateway est l'adresse IP de l'interface LAN du firewall.

Il faut sauvegarder avec Ctrl+x.

Recharger la configuration et vérifier:

```
sudo systemctl restart networking
```

```
ip a
```

```
chk@vmlinuxcmdclean:~$ 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: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen
    link/ether 00:0c:29:88:45:ad brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.200.11/24 brd 192.168.200.255 scope global ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe88:45ad/64 scope link
       valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen
    link/ether 00:0c:29:88:45:b7 brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    inet 192.168.0.23/24 brd 192.168.0.255 scope global dynamic ens37
       valid_lft 43197sec preferred_lft 43197sec
    inet6 2a01:e0a:17:d490:20c:29ff:fe88:45b7/64 scope global dynamic mngtmpaddr
       valid_lft 86393sec preferred_lft 86393sec
    inet6 fe80::20c:29ff:fe88:45b7/64 scope link
       valid_lft forever preferred_lft forever
chk@vmlinuxcmdclean:~$ _
```

3.2/Installation de MobaXtream :

Pour activer l'accès root via SSH, commencer par installer le serveur SSH:

```
sudo apt-get update
```

```
sudo apt-get install openssh-server
```

Ensuite, éditez le fichier de configuration SSH pour permettre la connexion root. Ouvrez le fichier "/etc/ssh/sshd_config" avec un éditeur de texte :

```
sudo nano /etc/ssh/sshd_config
```

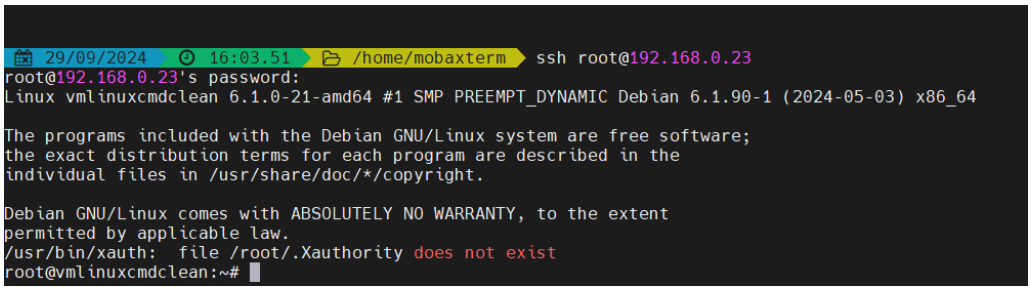
Modifier la ligne “PermitRootLogin” en :
PermitRootLogin yes

Ensuite, redémarrez le service SSH pour appliquer les modifications:

```
sudo systemctl restart ssh
```

Une fois ici, vous pouvez vous connecter en root à la VM depuis le PC physique grâce au logiciel MobaXterm.

Vous pouvez facilement installer MobaXtrem sur Windows grâce à ce lien :
https://mobaxterm.mobatek.net/download.html



3.3/Installation d’Apache :

Installez Apache avec la commande suivante :

```
sudo apt-get install apache2
```

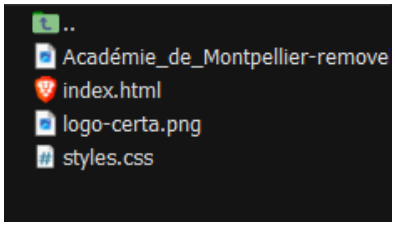
Accédez au répertoire où se trouvent les fichiers du site :

```
cd /var/www/hml
```

Supprimez la page par défaut :

```
sudo rm index.html
```

Cliquez sur « Follow terminal Folder » en bas à gauche et faites glisser-déposer les pages de votre site.



Redémarrer le serveur web :

```
systemctl restart apache2
```

Si on tape l'adresse IP du serveur web dans un navigateur depuis un client dans le même vmnet (vmnet 1) avec la bonne configuration IP, on tombe sur le site web.

3.4/Activation du HTTPS :

Activer le module SSL d'Apache :

```
a2enmod ssl
```

Activer le site « default-ssl » d'Apache :

```
a2ensite default-ssl
```

A2ensite default-ssl

Recharger apache2 :

```
systemctl reload apache2
```

Installer openssl :

```
apt-get update
apt-get install openssl
```

Générer un certificat :

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -sha256 -out /etc/apache2/server.crt -keyout /etc/apache2/server.key
```

Cela permetrra d'obtenir un certificat valable 1 ans.

Il faut rentrer les informations pour le certificat comme par exemple :

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:FR
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:Perpignan
Organization Name (eg, company) [Internet Widgits Pty Ltd]:MC-212.fr
Organizational Unit Name (eg, section) []:IT
Common Name (e.g. server FQDN or YOUR name) []:CHK
Email Address []:contact@mlc.fr
root@vmlinuxcmdclean:~#
```

Il faut modifier les droits sur la clé :

```
chmod440 /etc/apache2/server.crt
```

Indiquer à Apache2 où se trouve le certificat :

```
nano /etc/apache2/sites-available/default-ssl
```

```
#   A self-signed (snakeoil) certificate can be created by installing
#   the ssl-cert package. See
#   /usr/share/doc/apache2/README.Debian.gz for more info.
#   If both key and certificate are stored in the same file, only the
#   SSLCertificateFile directive is needed.
SSLCertificateFile      /etc/apache2/server.crt
SSLCertificateKeyFile   /etc/apache2/server.key
```

Enregistrer et quitter.

Active le module SSL :

```
a2enmod ssl
```

Activer le site HTTPS :

```
a2ensite default-ssl
```

Redémarrer apache2 :

```
systemctl reload apache2
```

Le https est activé.

3.5/Retrait de la carte réseau bridge :

Il est possible de retirer la carte réseau qui est en bridge.

Enlever les lignes de configuration avec:

```
nano /etc/network/interfaces
```

```
# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet static
    address 192.168.200.11
    netmask 255.255.255.0
    gateway 192.168.200.1


root@vmlinuxcmdclean:~# systemctl restart networking
root@vmlinuxcmdclean:~#
```

Redémarrer le service networking :

```
systemctl restart networking
```

1. **<u>Verification :</u>**

Nous avons toujours accès au serveur web depuis le VMnet 1.

La configuration du serveur web est terminée.

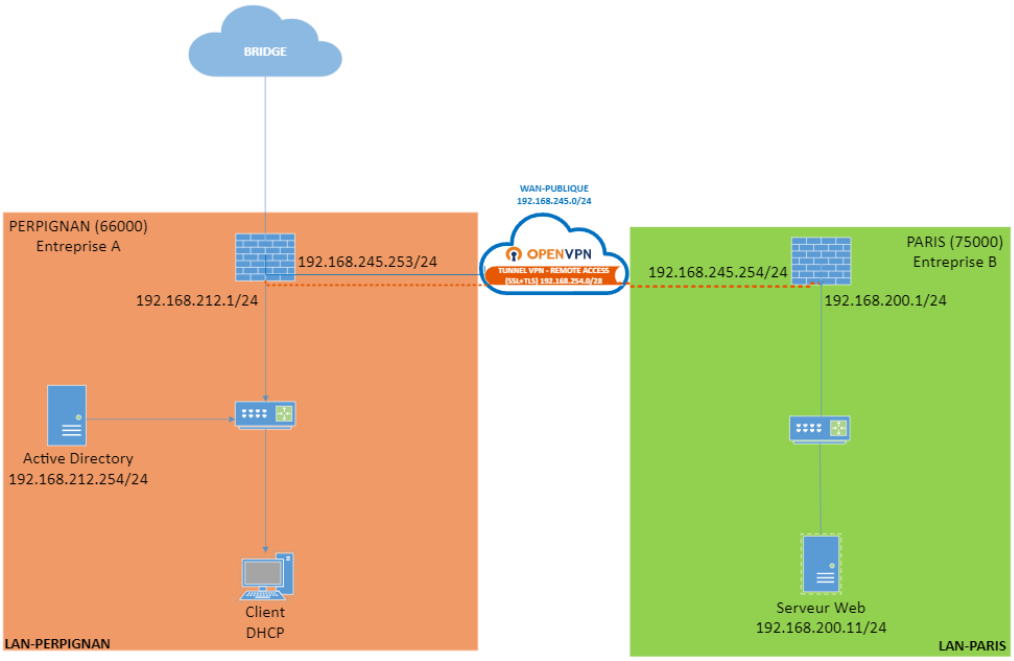
4/Installation et Configuration de l'OpenVPN sur Paris.

i Information : Sous OpnSense, on peut mettre en place plusieurs types de VPN

- **Peer to peer (SSL/TLS)** : pour monter un VPN site-à-site en utilisant une authentification par certificat.
- **Peer to peer (Shared Key)** : pour monter un VPN site-à-site en utilisant une authentification par clé partagée.
- **Remote Access (SSL/TLS)** : pour monter un accès distant pour clients nomades en utilisant une authentification par certificat.
- **Remote Access (User Auth)** : pour monter un accès distant pour clients nomades en utilisant une authentification par login/password.
- **Remote Access (SSL/TLS + User Auth)** : pour monter un accès distant pour clients nomades en utilisation une authentification par certificat et par login/password.

Dans notre Atelier Professionnel, nous allons utiliser « Remote Access (SSL/TLS + User Auth) »

4.1/Mise en œuvre OpenVPN – SSL/TLS – Rappel



Le module VPN permet de créer un client, un serveur ou les deux. Lors de l'activation du service VPN, une carte OPT virtuelle est générée, facilitant la transmission des paquets vers le VPN distant.

Il est également possible d'établir différents types de serveurs sur un système PfSense, à condition d'utiliser des réseaux ou des tunnels distincts.

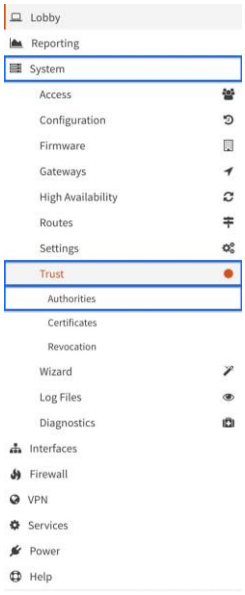
OpenVPN fonctionne sur un modèle client-serveur. Lors de la liaison de deux sites, l'un fonctionne comme client tandis que l'autre sert de serveur, permettant ainsi la connexion de plusieurs sites distants à un emplacement central.

Le serveur conserve à la fois le certificat de l'autorité et son propre certificat ainsi que la clé privée correspondante.

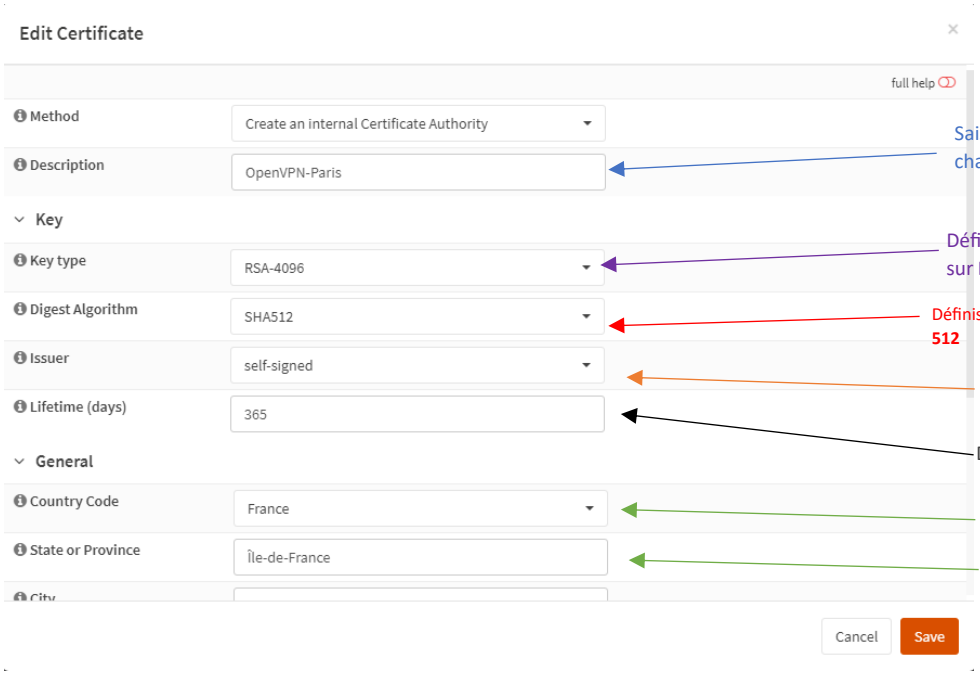
À partir du serveur, nous générons également les fichiers essentiels requis pour les clients, notamment un certificat client, une clé et le fichier client OpenVPN, qui varie en fonction de la plate-forme du client (Android, Windows ou Mac).

4.2/Génération de l'autorité de certification (CA)

Pour commencer, nous allons générer notre autorité de certification (CA) pour valider l'identité du serveur OpenVPN et authentifier les certificats utilisateur :



Puis Cliquez sur le signe **+** . La page de configuration **des autorités** s'affiche.



Saisissez un nom pour votre CA dans le champ **Nom descriptif**.

Définissez le **type de clé et sa longueur** sur **RSA**

Définissez l'algorithme **de digestion** sur **SHA-512**

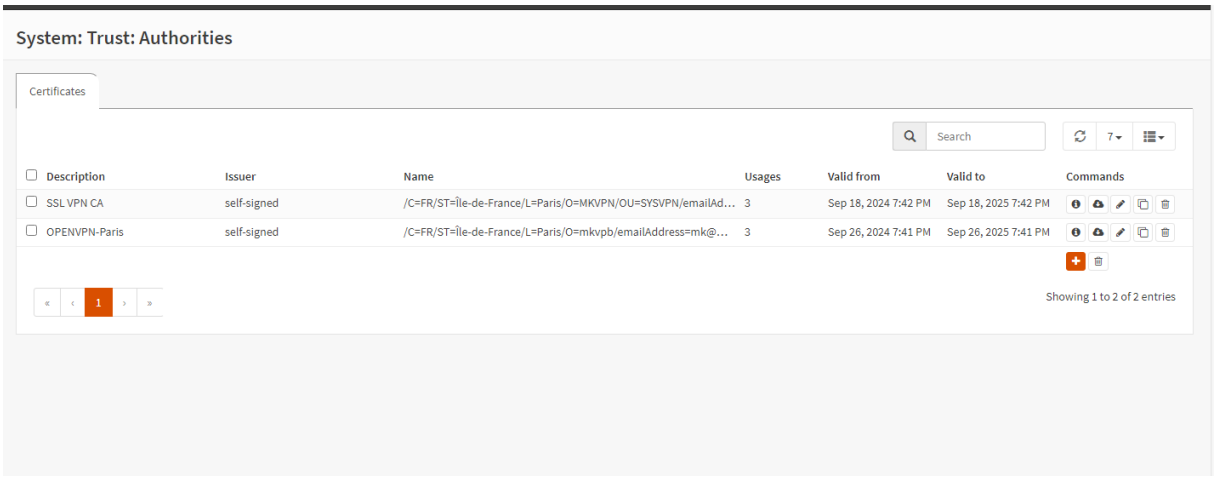
Laissez par défaut

Définissez la **durée de vie** sur **365** jours.

Vous pouvez définir des valeurs aléatoires pour les champs **Code du pays** , **État ou province** , **Ville** , **Organisation** et **Adresse e-mail**

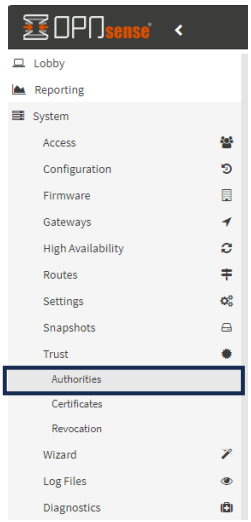
Cliquez sur **Enregistrer** en bas de la page.

Vous êtes ramené à la page principale **des autorités** et nous pouvons voir que notre autorité de certification nouvellement créée est affichée.

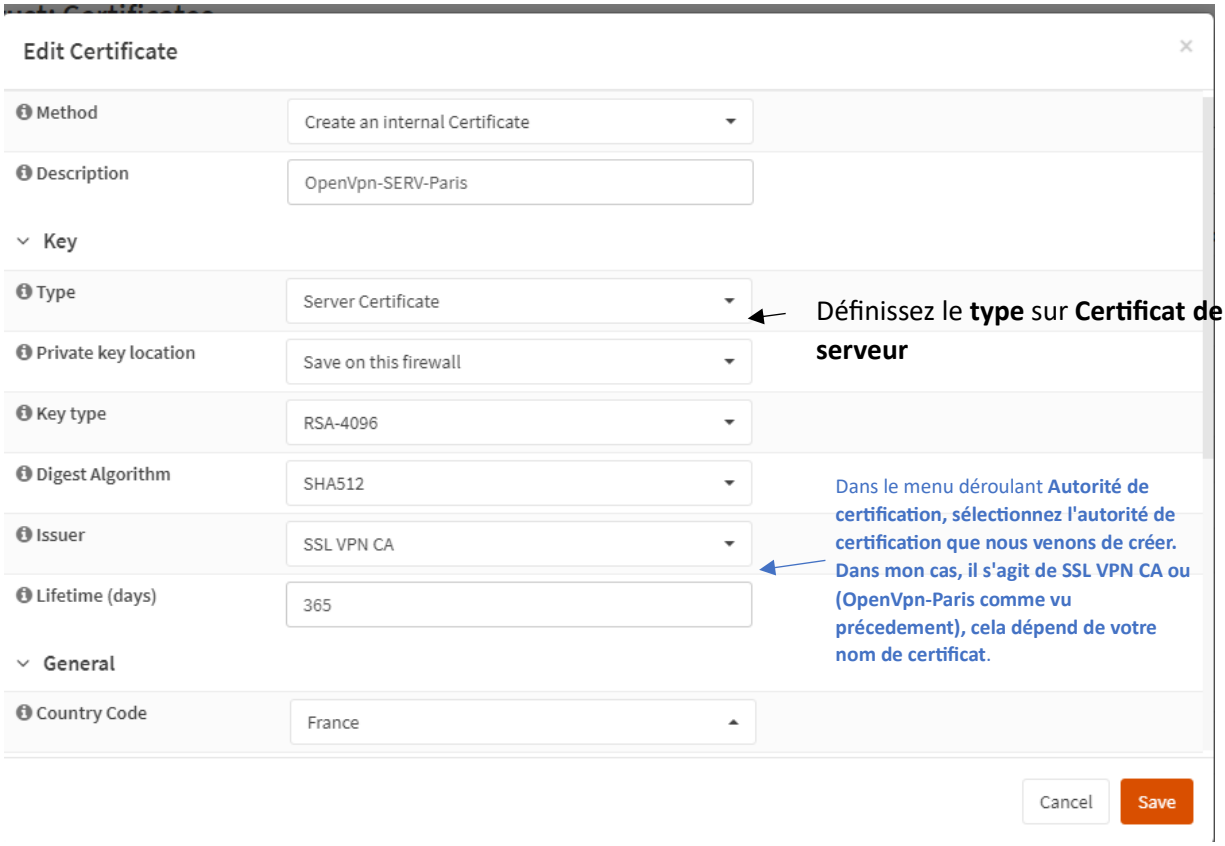


4.3/Génération du certificat du serveur

Dans les menus latéraux, sélectionnez **Certificats** (nous sommes déjà dans la section **Système** > **Confiance** de l'interface utilisateur). La page principale **Certificats** s'affiche.



Cliquez sur le signe **+** . La page de configuration **des certificats** s'affiche.

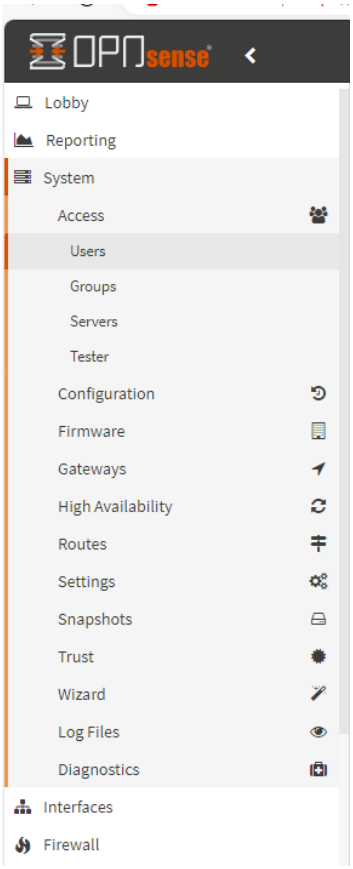


Replisser la suite, comme nous l'avons fait précédemment.

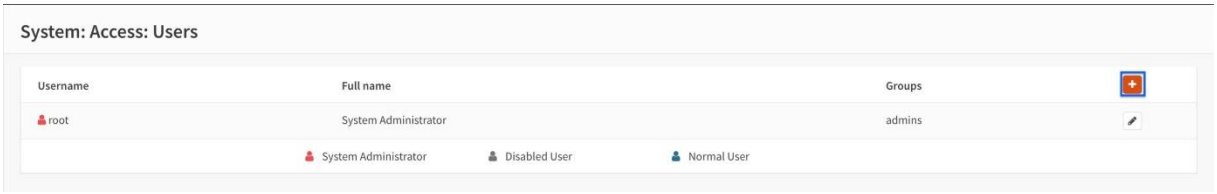
4.4/Créer un utilisateur VPN et son certificat utilisateur associé

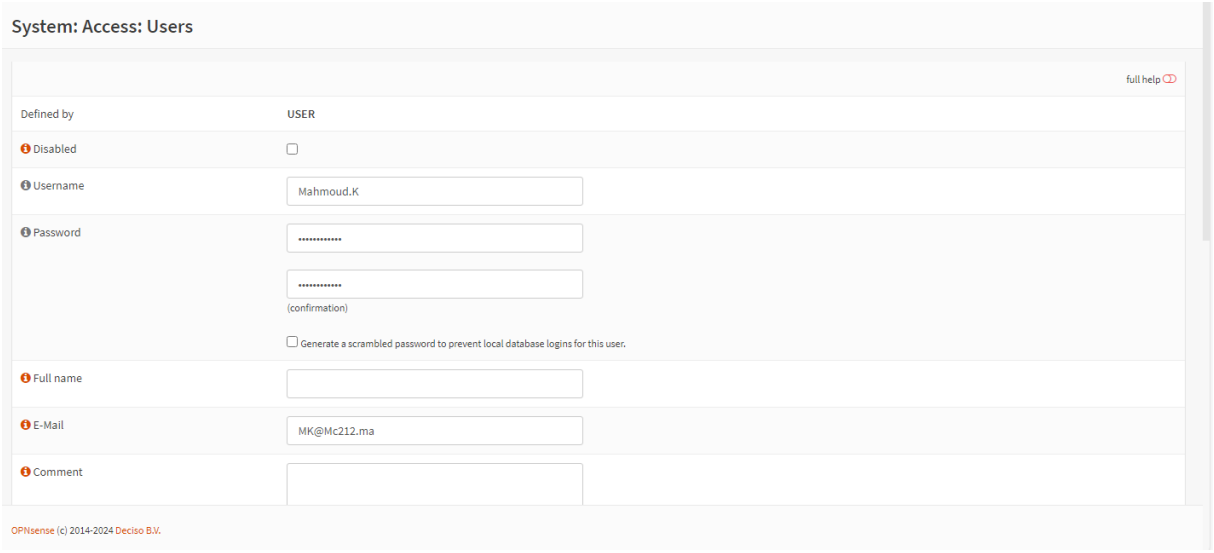
Nous allons maintenant créer un utilisateur pour accéder à notre serveur OpenVPN.

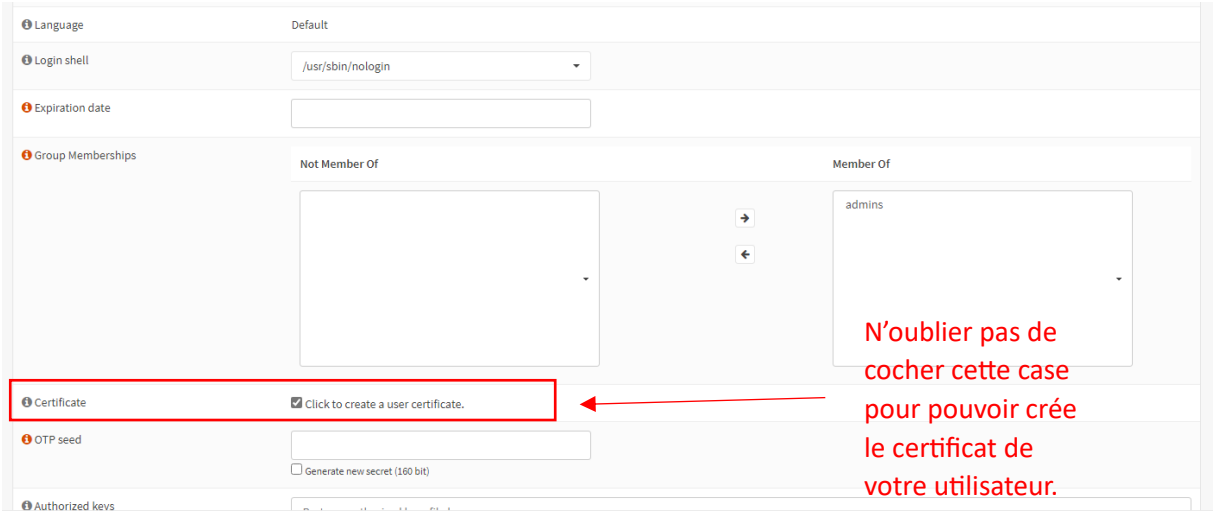
Dans les menus latéraux, sélectionnez **Système** > **Accès** > **Utilisateurs** . La page principale **Utilisateurs** s'affiche :



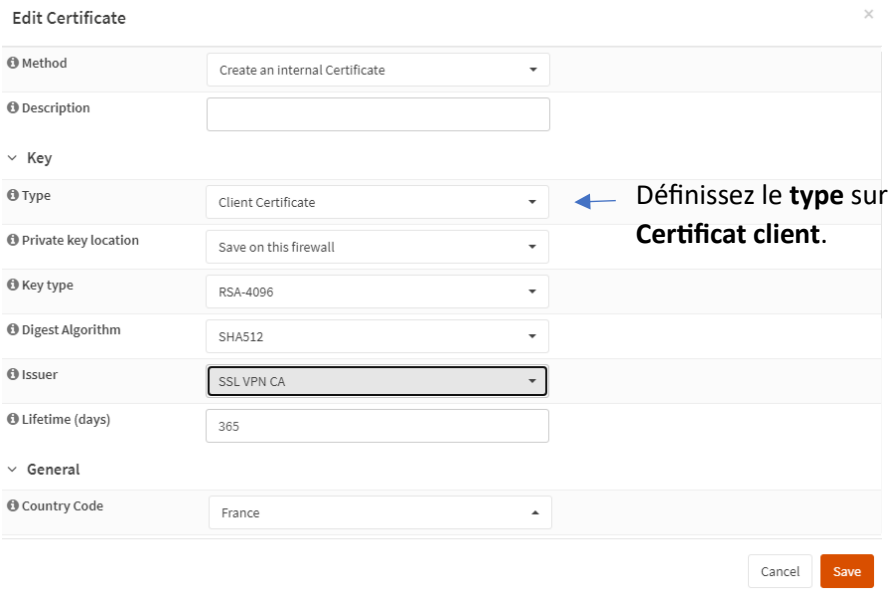
Cliquez sur le signe **+** . La page **de configuration des utilisateurs** s'affiche.







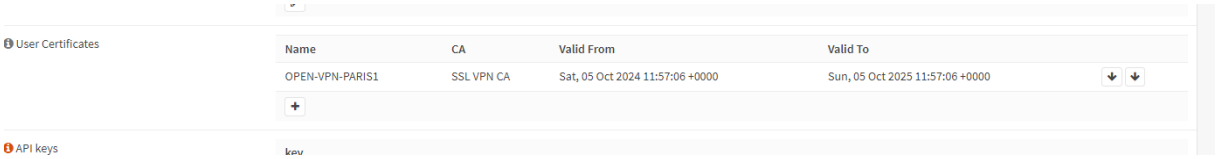
Vous arrivez sur cette page



Définissez le **type** sur **Certificat client**.

Une fois rempli toutes les informations et vérifier qu'elles sont bien correctes cliquer sur enregistrer

Vous revenez à la page de configuration **de l'utilisateur** et nous pouvons voir que notre certificat client nouvellement créé a été ajouté au profil utilisateur. Cliquez à nouveau sur **Enregistrer**

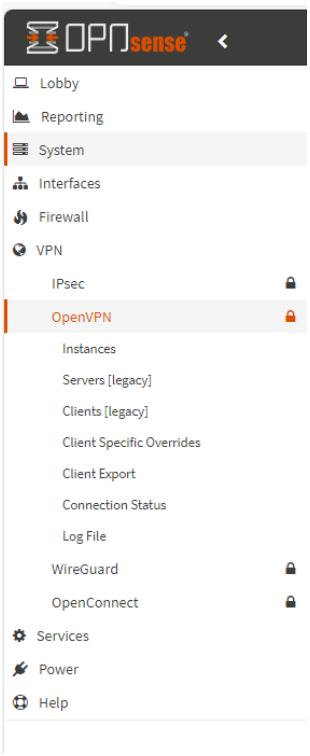


Les modifications sont enregistrées et vous devriez voir Les modifications ont été appliquées avec succès en haut de la page.

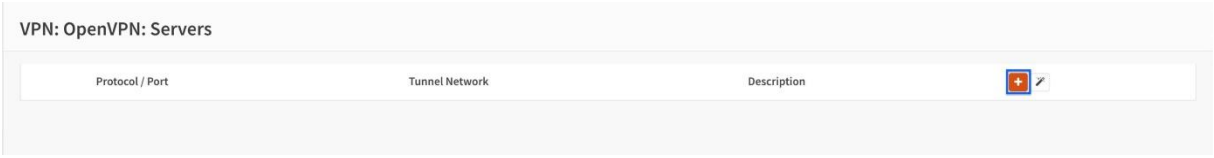
4.5/Création du serveur OpenVPN

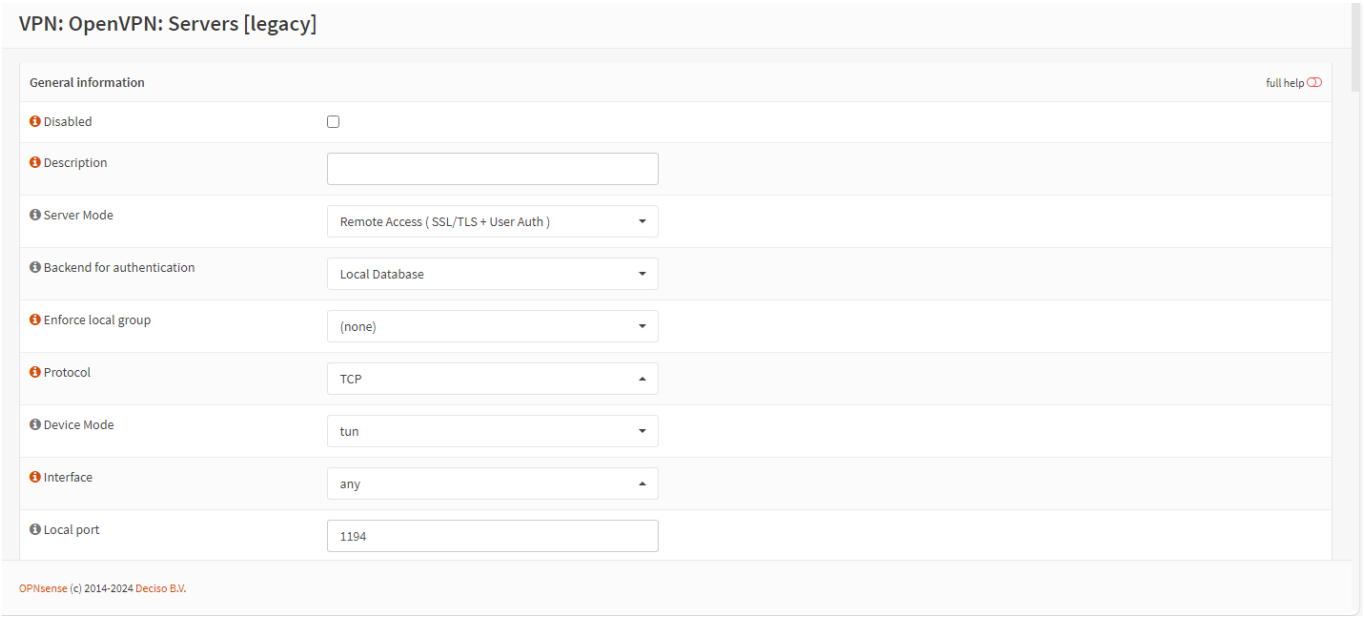
Nous avons maintenant tout ce dont nous avons besoin pour créer le serveur OpenVPN.

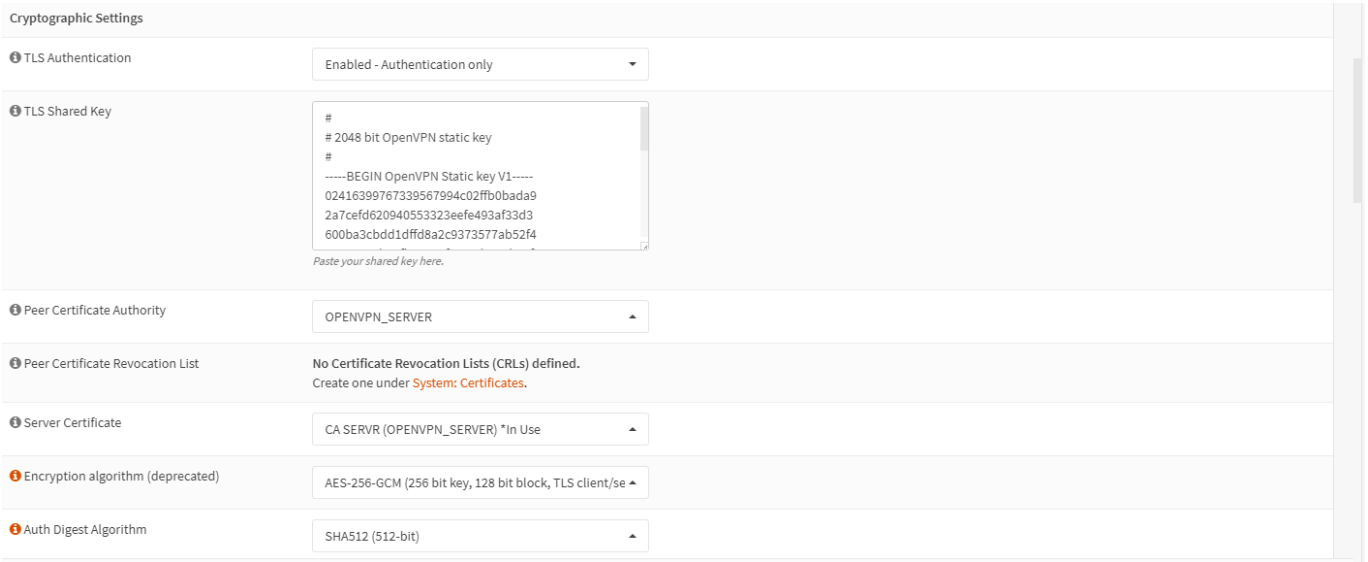
Dans les menus latéraux, sélectionnez **VPN** > **OpenVPN** > **Serveurs** . La page principale **des serveurs OpenVPN** s'affiche.

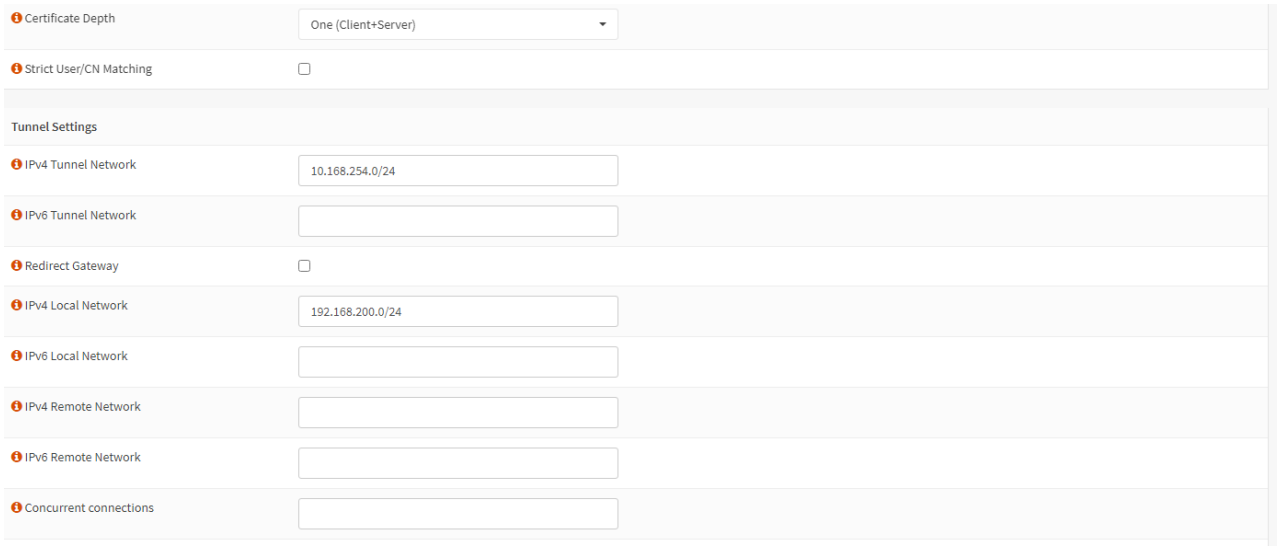


Cliquez sur le signe **+** pour ajouter un nouveau serveur OpenVPN. La page principale de configuration du serveur OpenVPN s'affiche.








Certificate Depth
One (Client+Server)
Strict User/CN Matching
Tunnel Settings
IPv4 Tunnel Network
10.168.254.0/24
IPv6 Tunnel Network
Redirect Gateway
IPv4 Local Network
192.168.200.0/24
IPv6 Local Network
IPv4 Remote Network
IPv6 Remote Network
Concurrent connections


No Preference
Type-of-Service
Inter-client communication
Duplicate Connections
Client Settings
Dynamic IP
Topology

Informations générales

1. Indiquez un nom pour votre serveur OpenVPN dans le champ **Description** .
2. Définissez le **mode serveur** sur **Accès à distance (SSL/TLS + authentification utilisateur)** .
3. Définissez le **backend pour l'authentification** sur **la base de données locale** .
4. Définissez le **protocole** sur **TCP4 (TCP en mode IPv4)** .
5. Réglez le **mode de l'appareil** sur **tun** .
6. Réglez l' **interface** sur **WAN** (afin que nous puissions nous connecter depuis l'extérieur).
7. Définissez le **port local** sur le port que vous souhaitez utiliser. Je le laisserai à **1194** , le port par défaut pour OpenVPN.

Paramètres cryptographiques

1. Dans le menu déroulant **Authentification TLS , sélectionnez Activé – Authentification et chiffrement** .
2. Cochez la case **Générer automatiquement une clé d'authentification TLS partagée** .
3. Définissez l' **autorité de certification homologue** sur l'autorité de certification que nous avons créée précédemment.
4. Dans le menu déroulant **Certificat de serveur , sélectionnez le certificat de serveur que nous avons créé précédemment.**
5. Dans le menu déroulant **Algorithme de chiffrement , sélectionnez AES-256-GCM** .
6. Définissez l'algorithme Auth Digest sur **SHA512 (512 bits)** .
7. Définissez la **profondeur du certificat** sur **un (client + serveur)** .
8. Cochez la case **Correspondance stricte utilisateur/CN**

Paramètres du tunnel

1. Saisissez un sous-réseau qui n'est pas utilisé sur votre système dans le champ **Réseau de tunnel IPv4** .
2. Cochez la case **Rediriger la passerelle** .
3. Sélectionnez **Activé – Algorithme de stub (–compress stub)** dans le menu déroulant **Compression .**
4. Cochez la case **communication inter-clients**

Paramètres du client

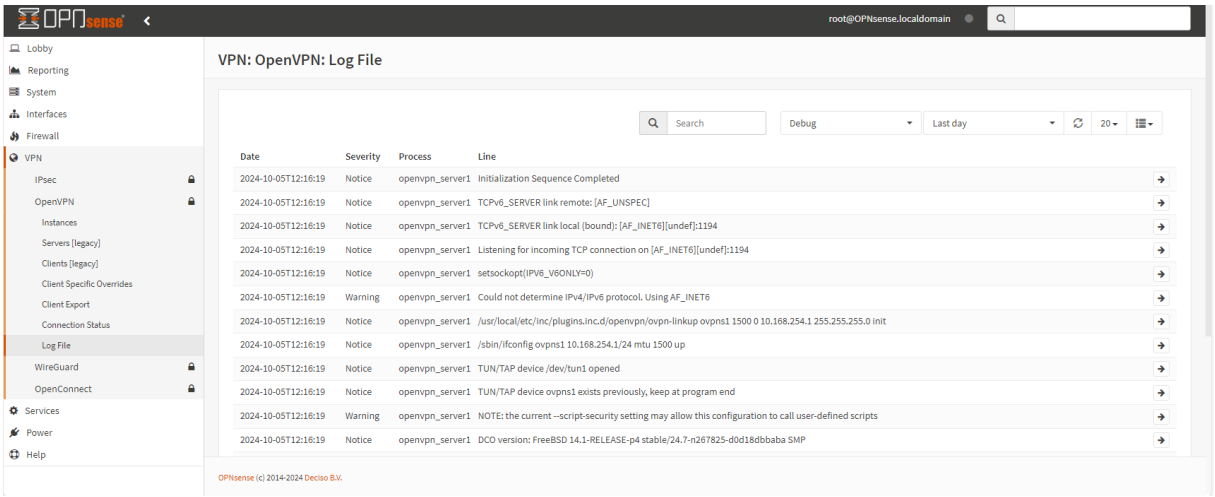
1. Cochez la case **IP dynamique** .
2. Cochez la case **Topologie** .
3. Cliquez sur **Enregistrer** en bas de la page.

Vous êtes ramené à la page principale des serveurs OpenVPN et nous pouvons voir notre serveur nouvellement créé affiché dans la liste.

Vérification de la configuration du serveur OpenVPN

1. Vérifions les journaux OpenVPN pour nous assurer que notre serveur est correctement configuré. Dans les menus latéraux, accédez à VPN > OpenVPN > Journaux système . La page Journaux OpenVPN s'affiche.

Vous devriez voir **la séquence d'initialisation terminée** dans les journaux si tout est correctement configuré.

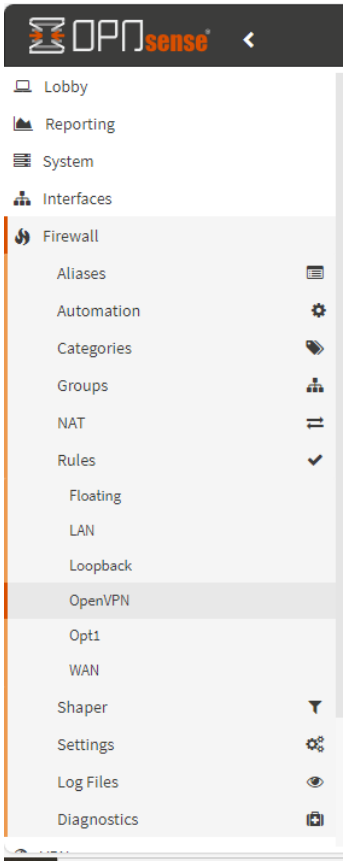


4.6/Création de règles de pare-feu

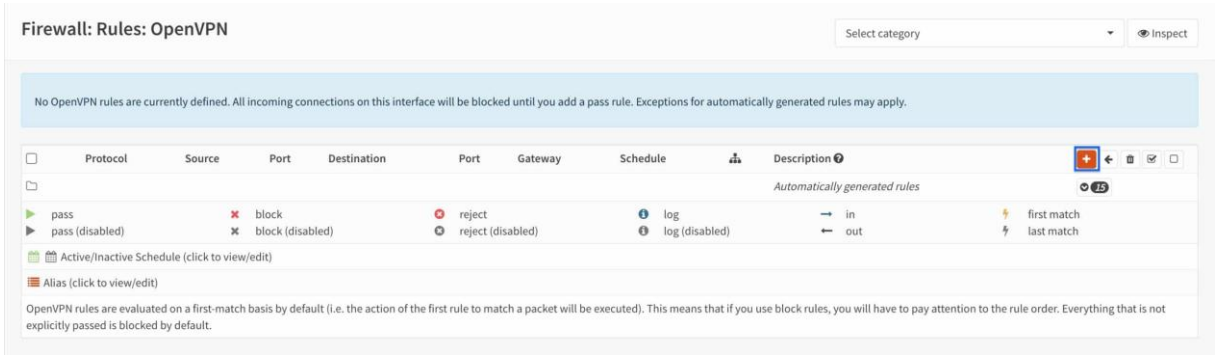
Maintenant que nous avons configuré notre serveur OpenVPN, nous devons créer une règle de pare-feu pour autoriser le trafic vers et depuis notre serveur.

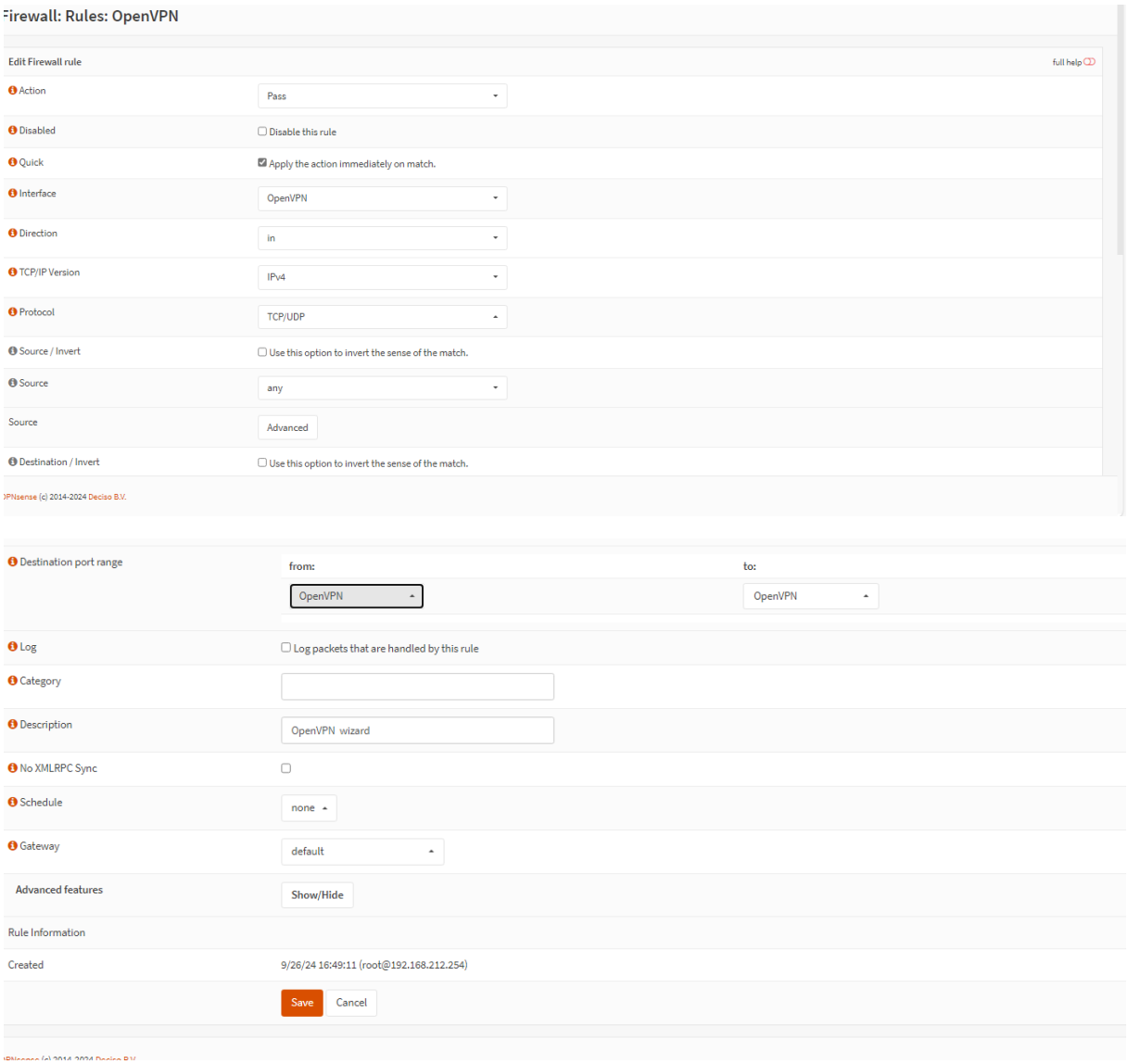
Règle OpenVPN

Dans les menus latéraux, sélectionnez Pare-feu > Règles > OpenVPN . La page Règles de l'interface OpenVPN s'affiche



Cliquez sur le signe + pour créer une nouvelle règle. La page Configuration de la règle de pare-feu s'affiche.

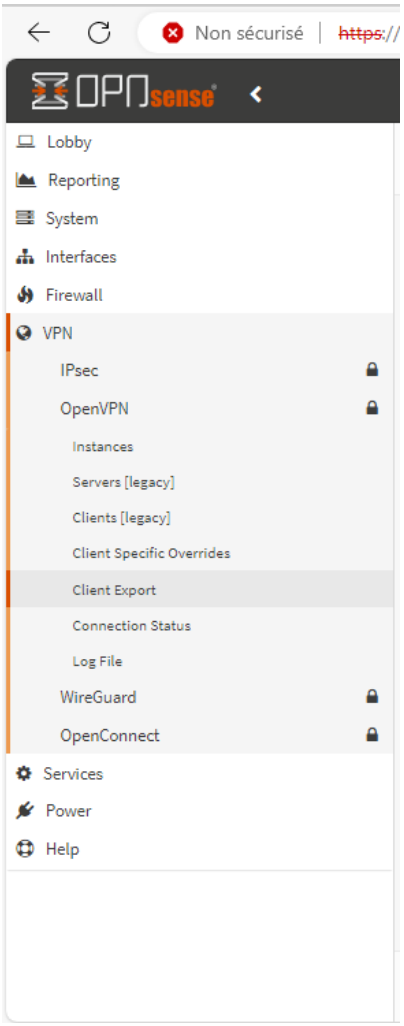



Firewall: Rules: OpenVPN
Edit Firewall rule
full help
Action
Pass
Disabled
Disable this rule
Quick
Apply the action immediately on match.
Interface
OpenVPN
Direction
in
TCP/IP Version
IPv4
Protocol
TCP/UDP
Source / Invert
Use this option to invert the sense of the match.
Source
any
Source
Advanced
Destination / Invert
Use this option to invert the sense of the match.
OPNsense (c) 2014-2024 Deciso B.V.
Destination port range
from:
to:
OpenVPN
OpenVPN
Log
Log packets that are handled by this rule
Category
Description
OpenVPN wizard
No XMLRPC Sync
Schedule
none
Gateway
default
Advanced features
Show/Hide
Rule Information
Created
9/26/24 16:49:11 (root@192.168.212.254)
Save
Cancel

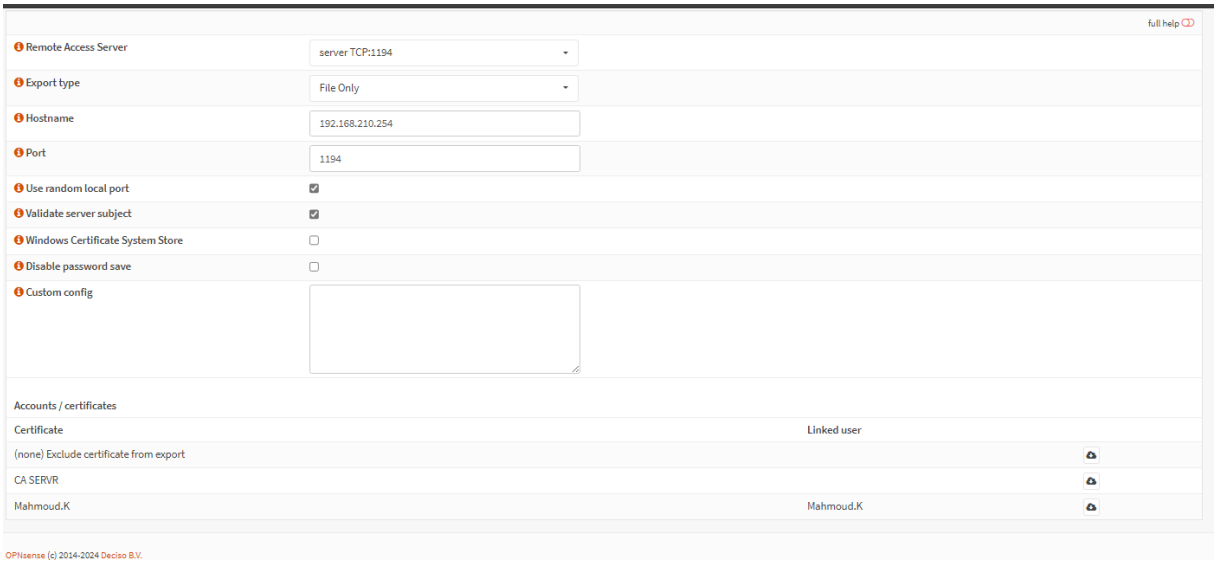
4.7/Exporter la configuration du client OpenVPN

Nous avons créé notre CA et nos certificats, notre serveur OpenVPN et nos règles de pare-feu. Il ne nous reste plus qu'à exporter notre configuration utilisateur et à nous connecter à notre serveur.

Dans les menus latéraux, accédez à **VPN** > **OpenVPN** > Exportation **du client** . La page **Exportation du client** s'affiche.



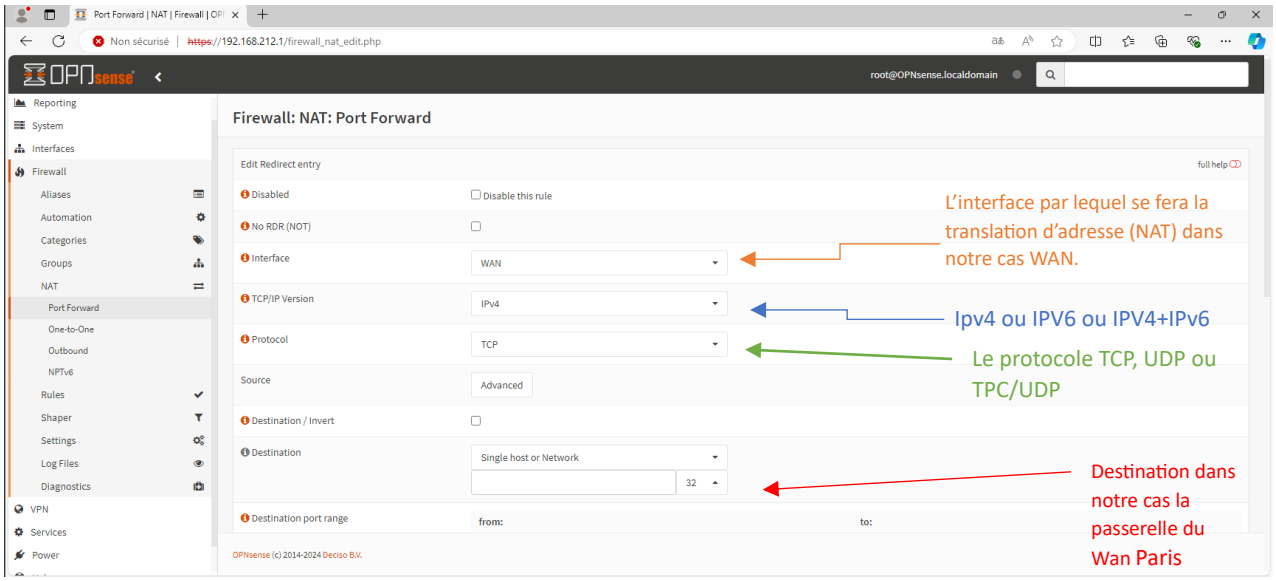
- Sélectionnez le serveur OpenVPN que nous avons créé dans le menu déroulant **Serveur d'accès à distance.**
- Définissez le **type d'exportation** sur **Fichier uniquement**.
- Saisissez votre **adresse IP WAN** publique dans le champ **Nom d'hôte.** Si vous utilisez un DNS dynamique pour accéder à l'interface WAN d'OPNsense, vous pouvez saisir votre nom d'hôte DNS dynamique dans ce champ et vous connecter en utilisant ce nom d'hôte comme adresse de serveur.
- Saisissez le port que vous avez sélectionné lors de la création du serveur dans le champ **Port**.
- Cliquez sur le bouton **Télécharger** à côté du nom d'utilisateur OpenVPN.



4.8/Configuration du NAT

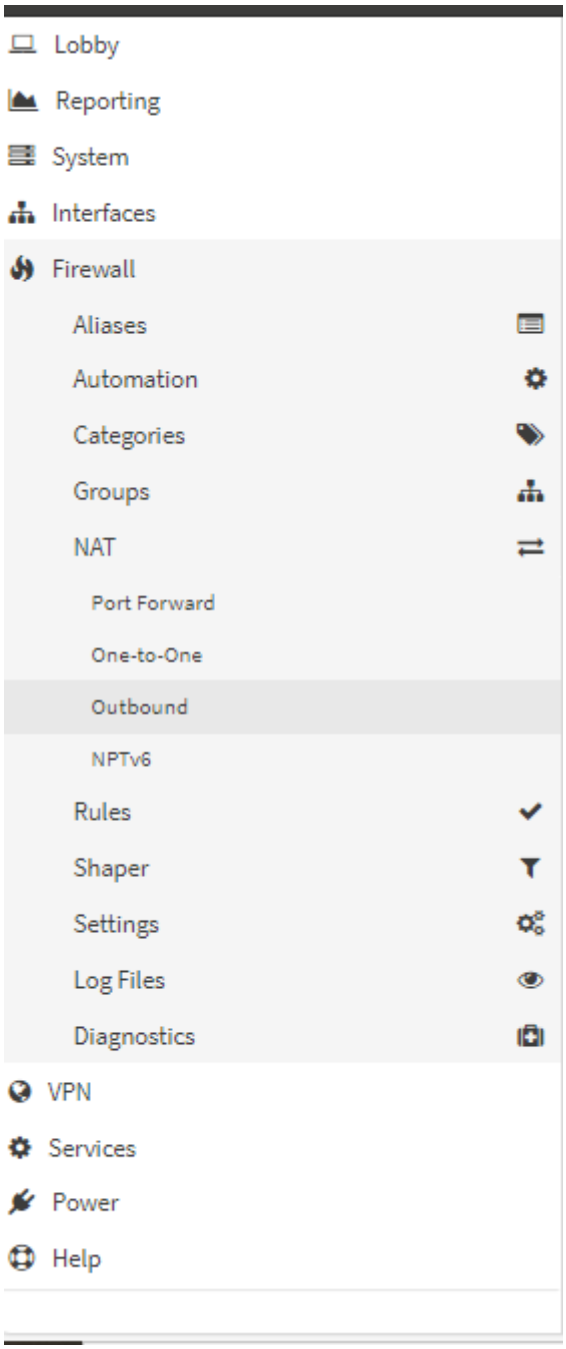
La traduction d'adresses réseau (NAT) est utilisée pour traduire des adresses IP privées en adresses IP publiques. OpnSense propose plusieurs options NAT, notamment le transfert de port, le NAT 1:1 et le NAT sortant. Vous pouvez configurer NAT en accédant à Pare-feu > NAT.

Sur l'OPNsense de Perpignan et de Paris, il faudra ajouter une règle NAT (Network Address Translation) :



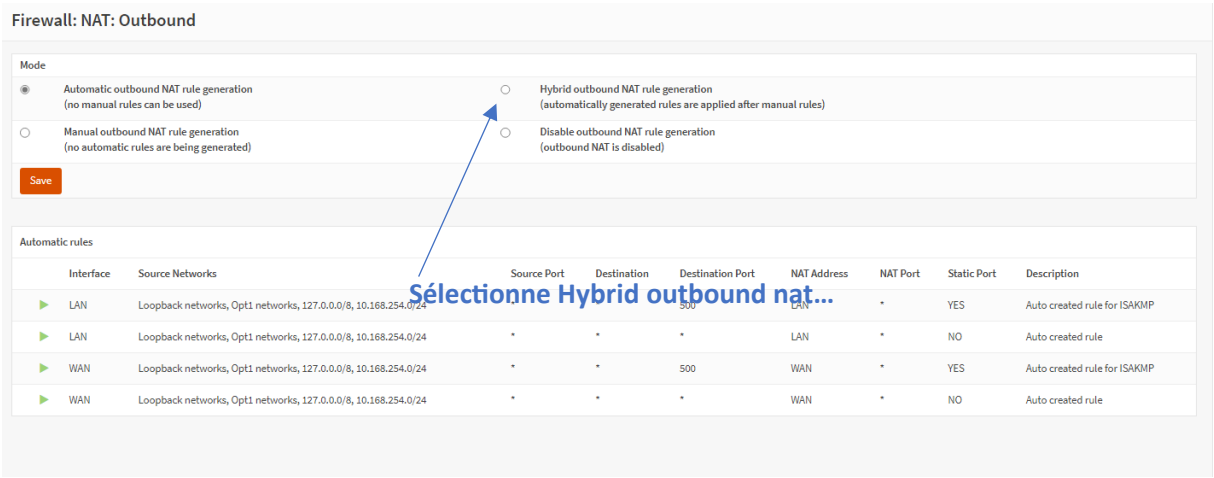
4.9/Outbound (NAT)

Allez dabns Firewall -> NAT -> Outbound.

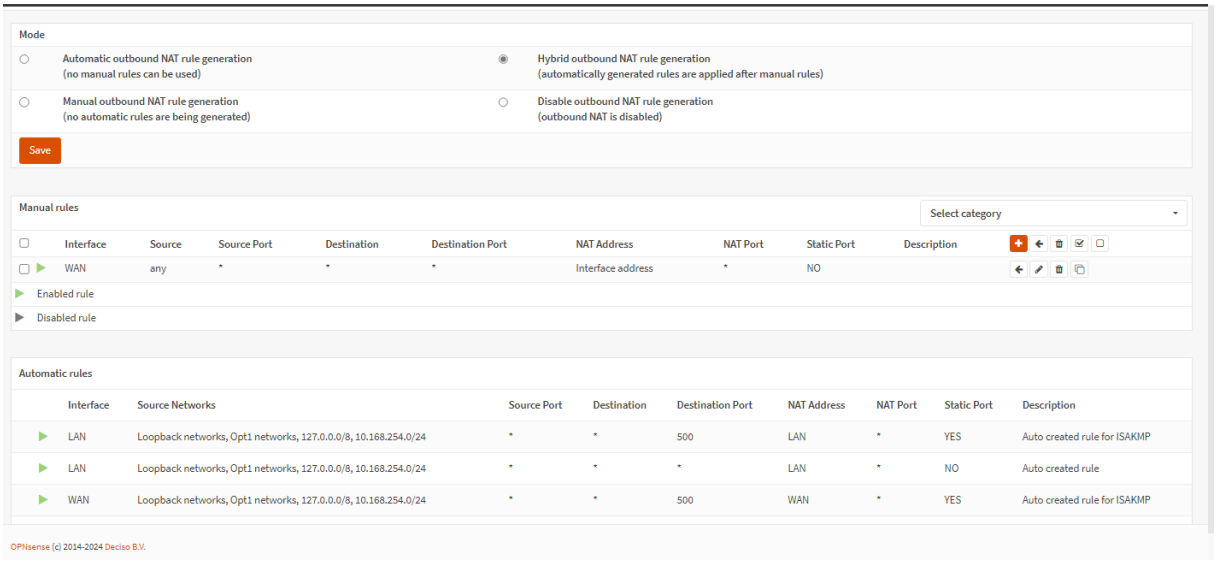


Par défaut il existe ces règles, il faudra ajouter une nouvelle.

Tout d’abord



Sélectionne Hybrid outbound nat…



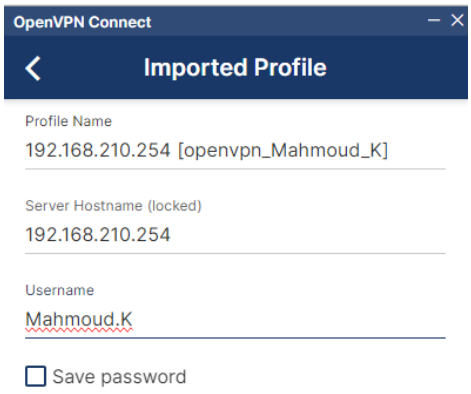
Configurer selon vos réseaux.

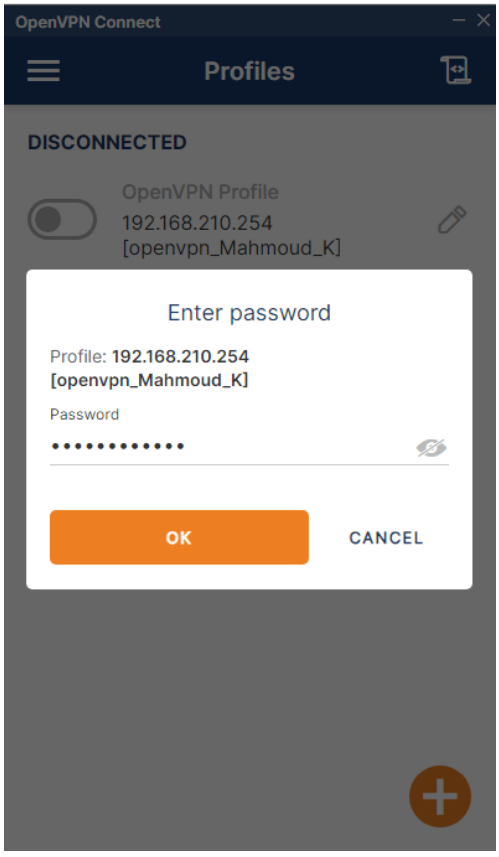
4.10/Connexion au tunnel sécurisé sur le client coté perpignan.

Installer OpenVPN sur internet (https://openvpn.net/community-downloads/)

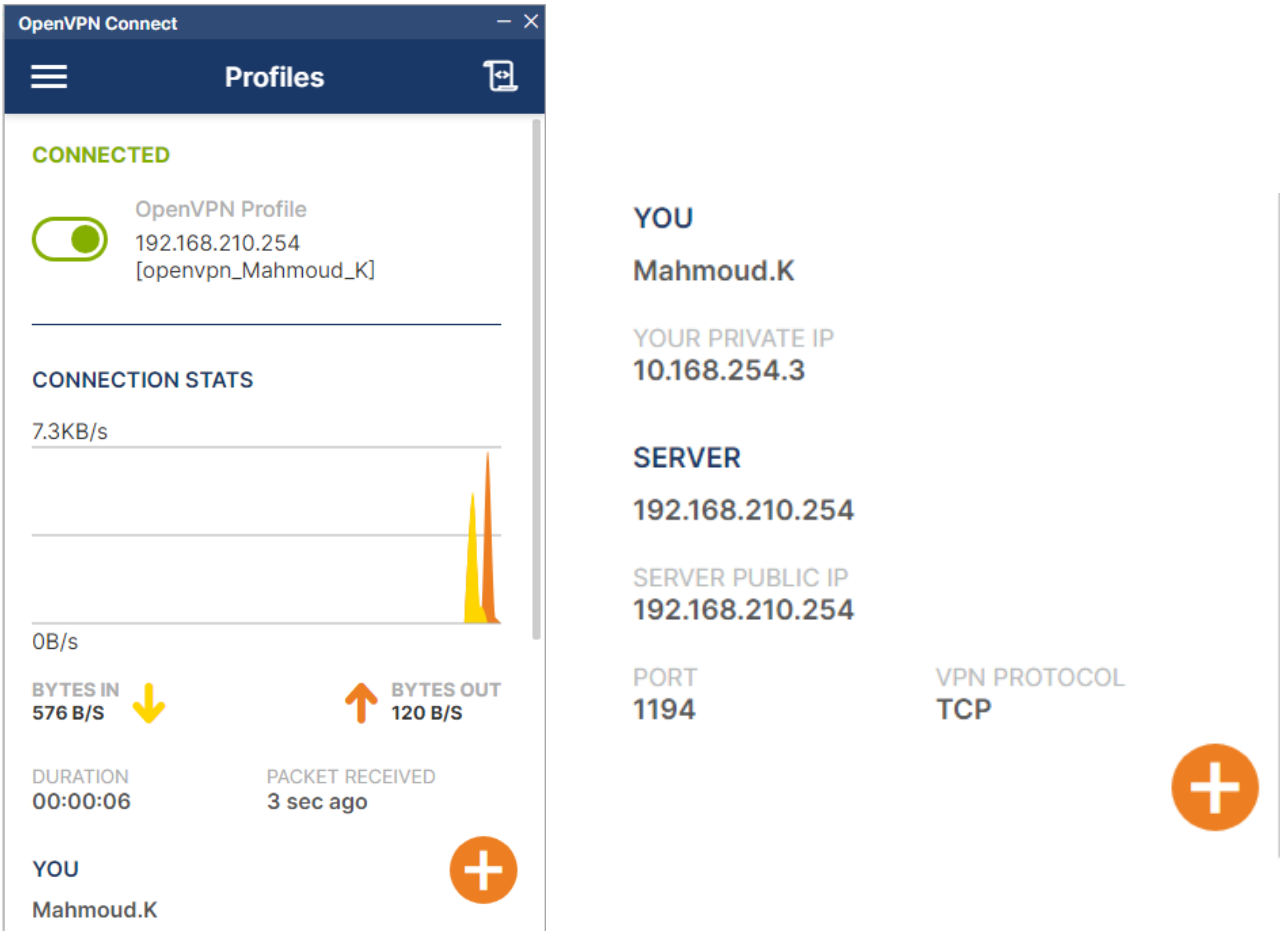
Lancer et importer la configuration.

Connecter-vous avec vos identifiants.





Et vous voilà connecter !

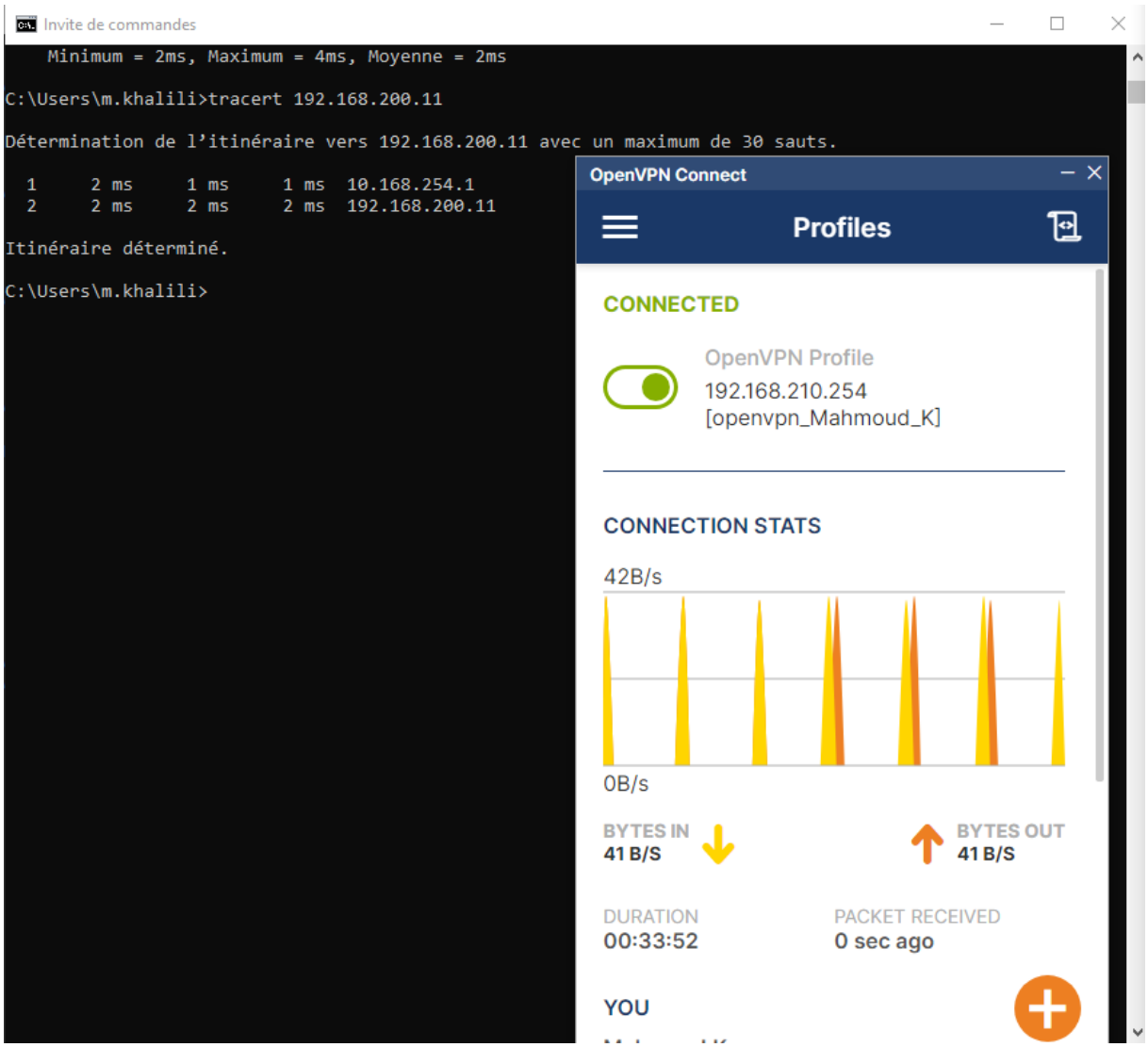


On va voir, si on accéder bien à notre site distant :

Dans mon cas l'adresse sera : https://192.168.200.11

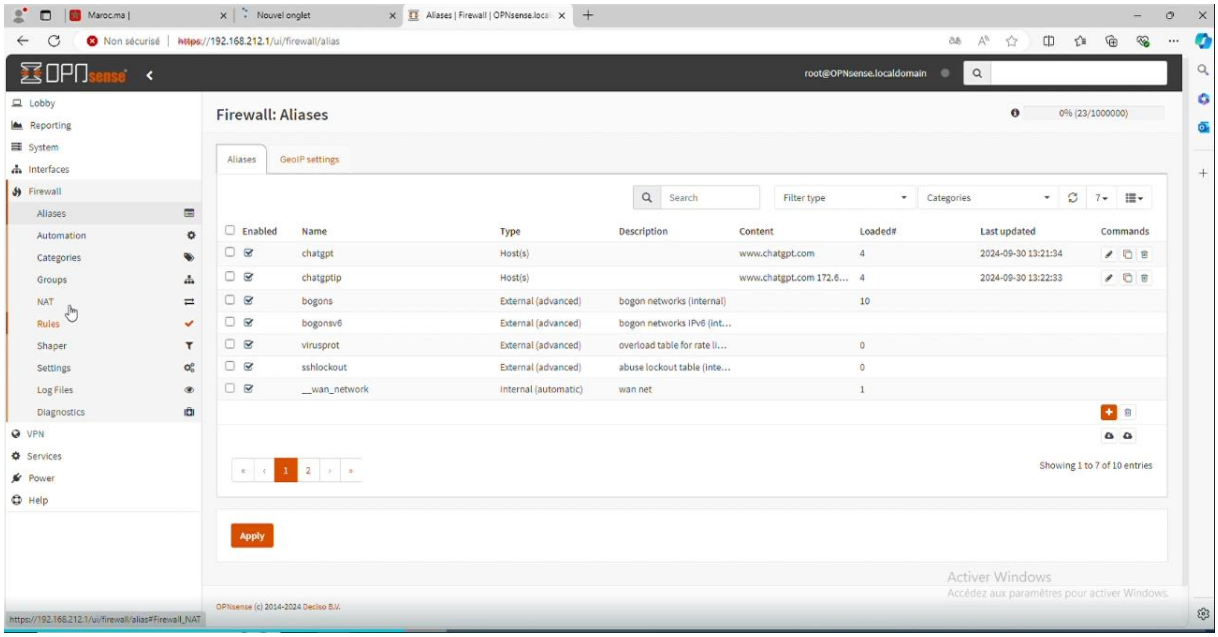
On peut réaliser égalament un tracert pour voir le chemin emprunter :

CMD -> tracert @IP



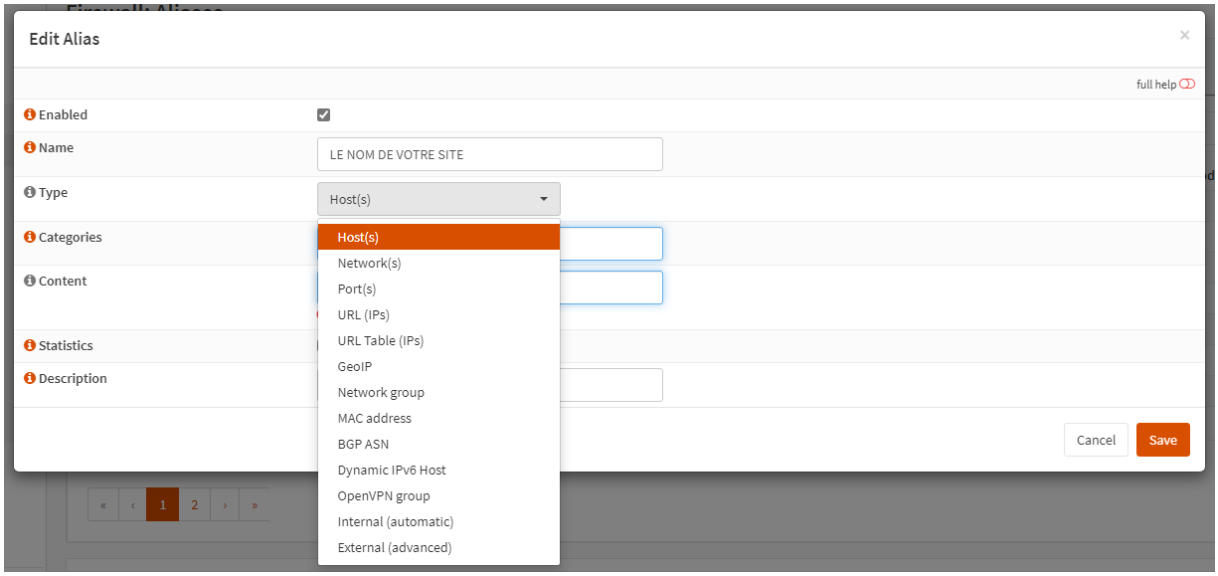
4.11/Règles pour bloquer un site

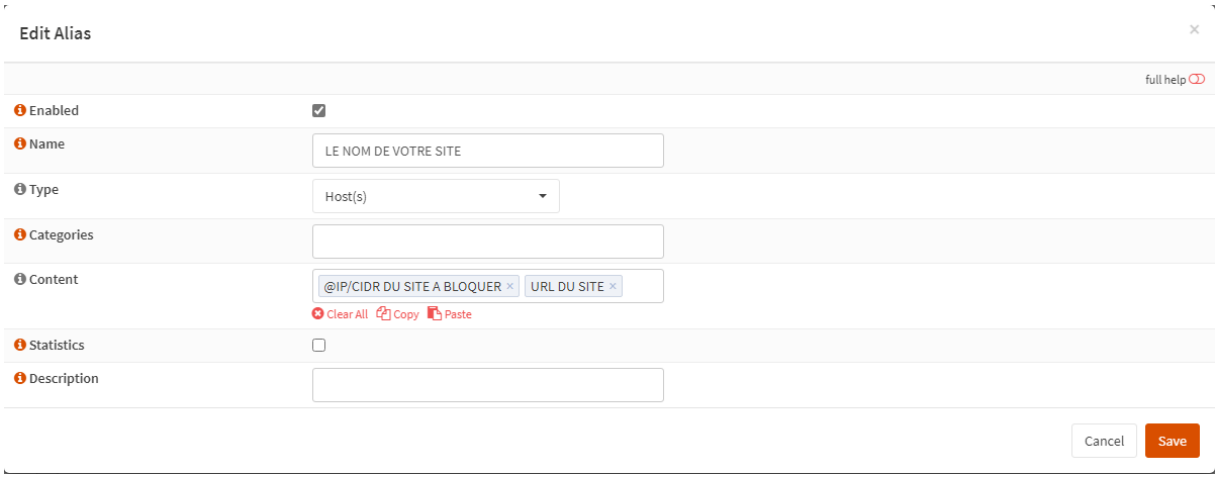
Il vous suffit tout d'abord d'aller dans Aliases dans FireWall -> Aliases puis Crée un nouveau Aliases



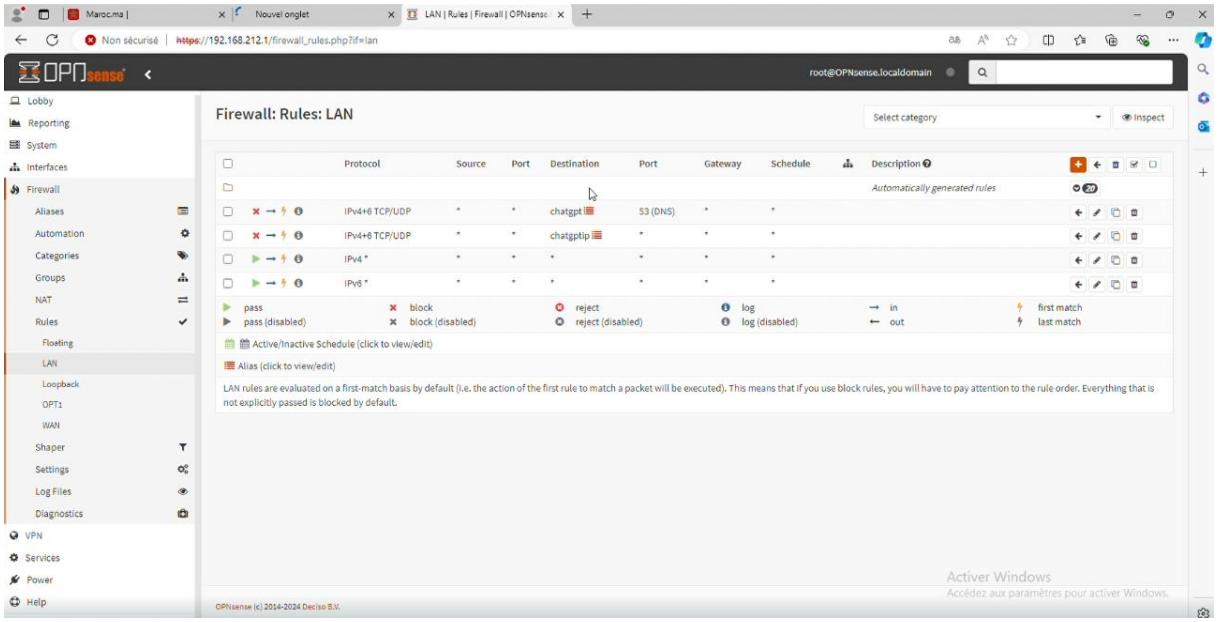
Par quel type, souhaitez-vous bloquer :

Pour ma part pour ChatGpt, ça sera Host(s)

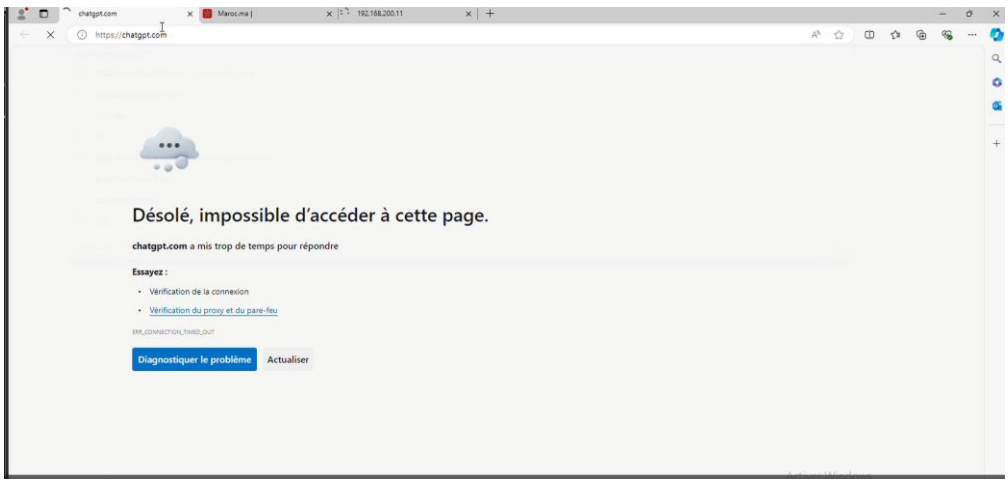




Maintenant ajouter une règle sur le réseau ou vous voulez le bloquer :



Chatgpt est désormais bloquer.



5/Merci pour votre lecture !