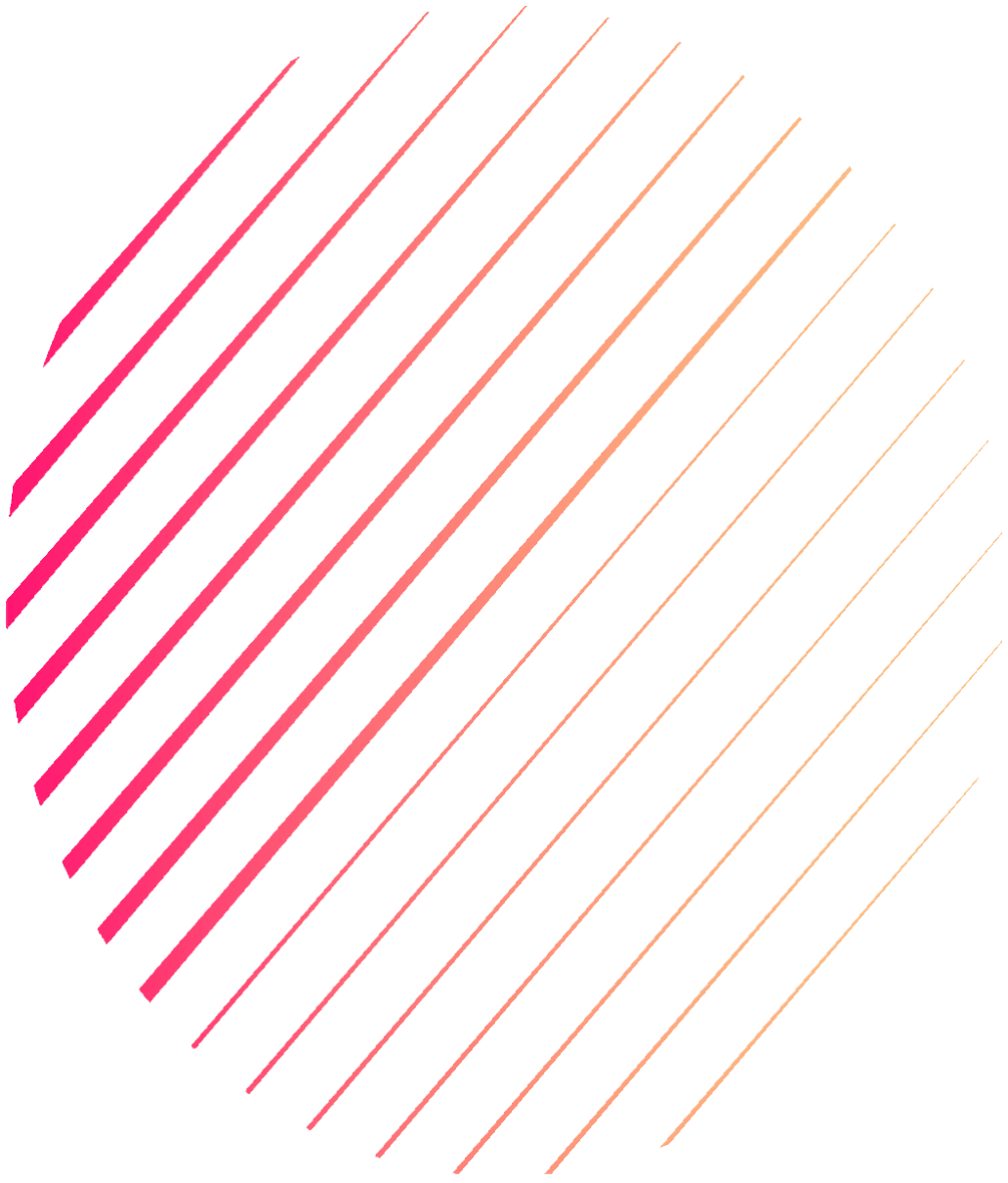
Atelier Pro 1



21/02/2024

Installation Windows Server 2019 avec VPN

Samuel THOMAS
BTS SIO 2024 – 2025

Sommaire

Contexte du Projet

Description du laboratoire GSB

Le secteur d'activité :
L'industrie pharmaceutique est un secteur très lucratif dans lequel le mouvement de fusion acquisition est très fort. Les regroupements de laboratoires ces dernières années ont donné naissance à des entités gigantesques au sein desquelles le travail est longtemps resté organisé selon les anciennes structures.
Des déboires divers récents autour de médicaments ou molécules ayant entraîné des complications médicales ont fait s'élever des voix contre une partie de l'activité des laboratoires : la visite médicale, réputée être le lieu d' arrangements entre l'industrie et les praticiens, et tout du moins un terrain d'influence opaque.

L'entreprise :
Le laboratoire Galaxy Swiss Bourdin (GSB) est issu de la fusion entre le géant américain Galaxy (spécialisé dans le secteur des maladies virales dont le SIDA et les hépatites) et le conglomérat européen Swiss Bourdin (travaillant sur des médicaments plus conventionnels), lui même déjà union de trois petits laboratoires .
En 2009, les deux géants pharmaceutiques ont uni leurs forces pour créer un leader de ce secteur industriel. L'entité Galaxy Swiss Bourdin Europe a établi son siège administratif à Paris.
Le siège social de la multinationale est situé à Philadelphie, Pennsylvanie, aux Etats-Unis.
La France a été choisie comme témoin pour l'amélioration du suivi de l'activité de visite.

Description du système informatique

Le système informatique :
Sur le site parisien, toutes les fonctions administratives (gestion des ressources humaines, comptabilité, direction, commerciale, etc.) sont présentes. On trouve en outre un service labo-recherche, le service juridique et le service communication.

La salle serveur occupe le 6ème étage du bâtiment et les accès y sont restreints (étage accessible par ascenseur à l'aide d'une clé sécurisée, portes d'accès par escalier munies d'un lecteur de badge, sas d'entrée avec gardien présent 24h/24).

Les serveurs assurent les fonctions de base du réseau (DHCP, DNS, Annuaire et gestion centralisée des environnements) et les fonctions de communication (Intranet, Messagerie, Agenda partagé, etc.).
On trouve aussi de nombreuses applications métier (base d'information pharmaceutique, serveurs dédiés à la recherche, base de données des produits du laboratoire, base de données des licences d'exploitation pharmaceutique, etc.) et les fonctions plus génériques de toute entreprise (Progiciel de Gestion Intégré avec ses modules RH, GRC, etc.).
Un nombre croissant de serveurs est virtualisé.

Constitué autour de VLAN, le réseau segmente les services de manière à fluidifier le trafic.

Les données de l'entreprises sont considérées comme stratégiques et ne peuvent tolérer ni fuite, ni destruction. L'ensemble des informations est répliqué quotidiennement aux Etats-Unis par un lien dédié. Toutes les fonctions de redondances (RAID, alimentation, lien réseau redondant, Spanning-tree, clustering, etc.) sont mises en œuvre pour assurer une tolérance aux pannes maximale.

L'équipement :
L'informatique est fortement répandue sur le site. Chaque employé est équipé d'un poste fixe relié au système central. On dénombre ainsi plus de 350 équipements terminaux et un nombre de serveurs physiques conséquent (45 en 2012) sur lesquels tournent plus de 100 serveurs virtuels.

On trouve aussi des stations de travail plus puissantes dans la partie labo-recherche, et une multitude d'ordinateurs portables (personnels de direction, service informatique, services commerciaux, etc).

Les visiteurs médicaux reçoivent une indemnité bisannuelle pour s'équiper en informatique (politique Swiss-Bourdin) ou une dotation en équipement (politique Galaxy). Il n'y a pas à l'heure actuelle d'uniformisation des machines ni du mode de fonctionnement

Chaque employé de l'entreprise a une adresse de messagerie de la forme nomUtilisateur@steph.com. Les anciennes adresses de chaque laboratoire ont été définitivement fermées au 1er janvier 2011.

Organisation du réseau

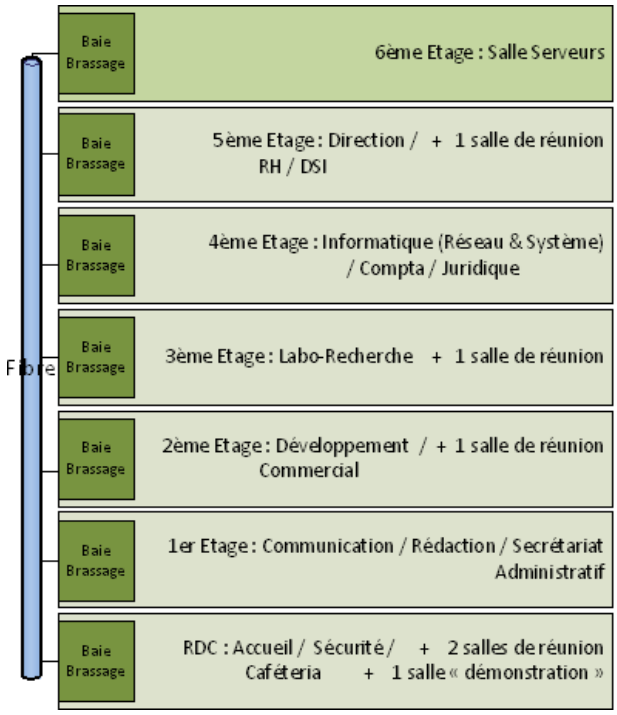
Répartition des services :
Chaque étage dispose d'une baie de brassage qui le relie par une fibre à la baie centrale de la salle serveurs.

Toutes les salles de réunion sont équipées d'un point d'accès Wifi positionné par défaut dans le VLAN "Visiteurs" qui autorise uniquement un accès Internet.
Les portables connectés en wifi à ce point d'accès reçoivent ainsi une adresse IP et n'ont, par conséquent accès qu'aux services DHCP et DNS.

Le point d'accès peut être configuré à la demande pour être raccordé à un VLAN présent au niveau de l'étage.

Chaque salle de réunion dispose d'un vidéoprojecteur, d'enceintes et d'un tableau numérique interactif.

La salle "Démonstration" est destinée à l'accueil des organismes de santé (AFSSAPS notamment) et des partenaires scientifiques. Elle dispose de paillasses et d'équipements de laboratoire, en plus d'une salle de réunion.



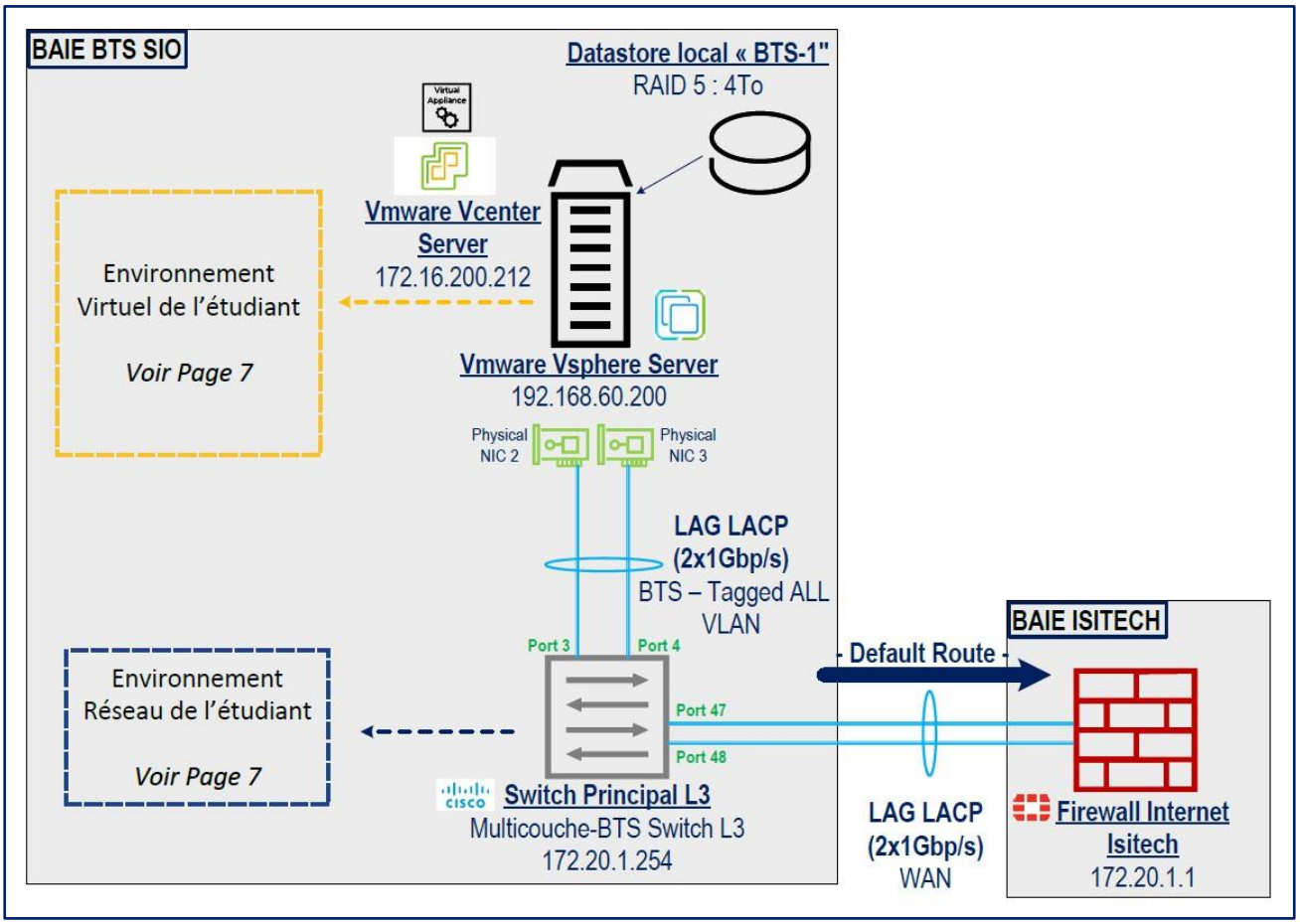
Segmentation du réseau :
L'organisation des VLAN et de l'adressage IP est la suivante :

N° VLAN	Service(s)	Adressage IP
280 : Administrateur	Serveur	192.168.1.0/24
281 : Staff	Client	192.168.10.0/24

Salle serveur et connexion internet

L'organisation des serveurs et des équipements réseaux est la suivante :

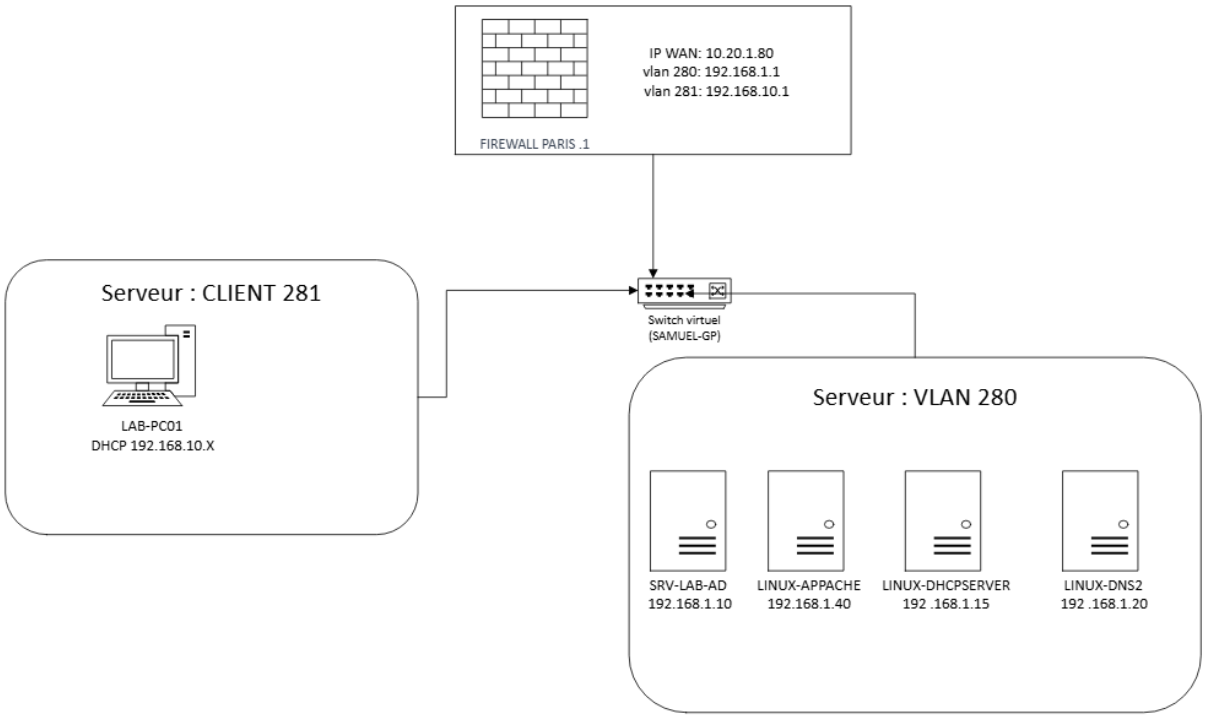
- Le serveur principal est virtualisé sous le système Vmware Vcenter 7.0
- Un Commutateur Multicouche Cisco permet l'interconnection du serveur principal et la liaison vers le firewall de proximité (Internet).
- Les Vlans sont propagés en mode Trunk sur l'interface de liaison « LAG LACP » port 3 et 4 du commutateur Multicouche et Interface Physical NIC2 et NIC3 du serveur Principal.
- L'environnement Virtuel et réseau des Projets d'Atelier de Professionnalisation sont référencées en Page X



Environnement virtuel

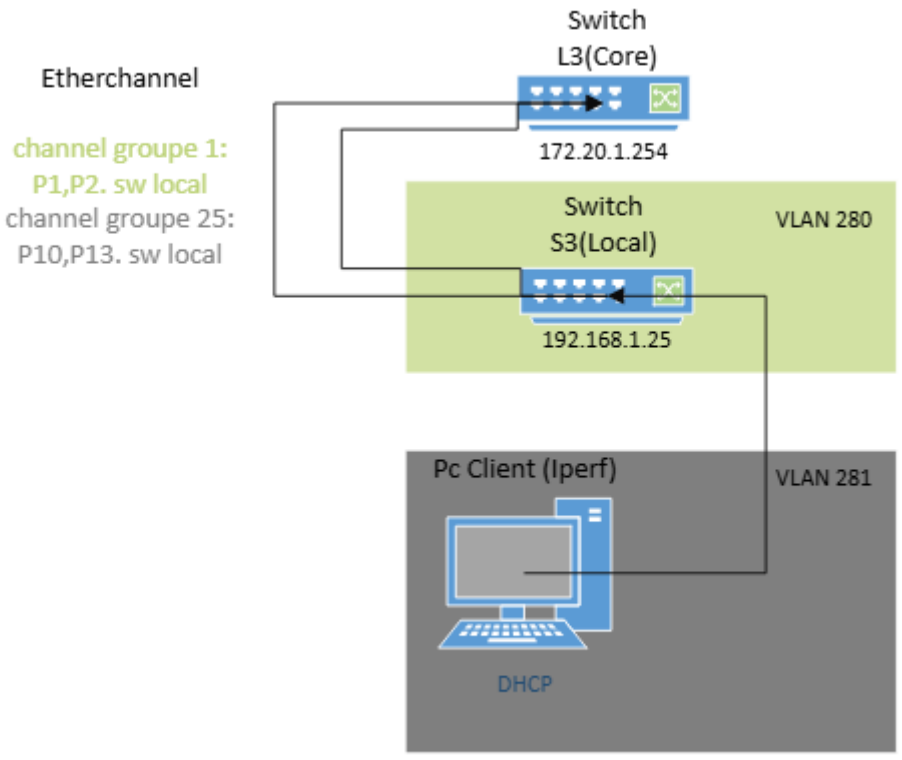
Nom de l'appareil, Système d’éxploitation

SRV- LAB-AD, win-server2022
LINUX-APPACHE, ubuntu-22.04.2-live-server
LINUX-DHCPSERVER, ubuntu-22.04.2-live-server
LINUX-DNS2, ubuntu-22.04.2-live-server
LAB-PC01, Win10_22H2_French_x64.is
FIREWALL PARIS .1, pfSense-CE-2.7.1



Environnement Réseau Physique

Nom de l'appareil,	VLAN,	Adresse IP
SRV-LAB-AD,	280,	192.168.1.10
LINUX-APPACHE	280	192.168.1.40
LINUX-DHCPSERVER	280	192 .168.1.15
LINUX-DNS2	280	192 .168.1.20
LAB-PC01	281	DHCP 192.168.10.X
FIREWALL PARIS .1	280	192.168.1.1
FIREWALL PARIS .1	281	192.168.10.1



Cahier des Charges : Installation Windows Server 2019 avec VPN

1. Contexte du projet

L'objectif de ce projet est de créer un serveur pour une entreprise. Celle-ci aura 2 utilisateurs différents sur le même poste connecté au domaine. Ils pourront se connecter à leur session sur le serveur et auront un dossier partagé sur celui-ci afin de pouvoir avoir les documents qu'ils souhaitent entre les 2 sessions. Le serveur aura un Active Directory permettant de réguler les droits qu'ils auront dessus. Il aura aussi un VPN afin de le sécuriser, ainsi que des ressources de base.

2. Objectifs du projet

Les objectifs spécifiques de ce projet sont :

-Mise en place d'un serveur Windows 2019.

-Mise en place de l'Active Directory avec plusieurs utilisateurs.

-Mise en place de droits spécifiques sur des sessions spécifiques.

-Création d'un domaine avec éventuellement un VPN.

3. Spécifications fonctionnelles

3.1 Active Directory (AD)
- Créer 2 comptes utilisateurs avec profils séparés.
- Gérer les permissions (lecture/écriture) sur un dossier partagé via Groupes AD.
- Politique de mots de passe : complexité + expiration.

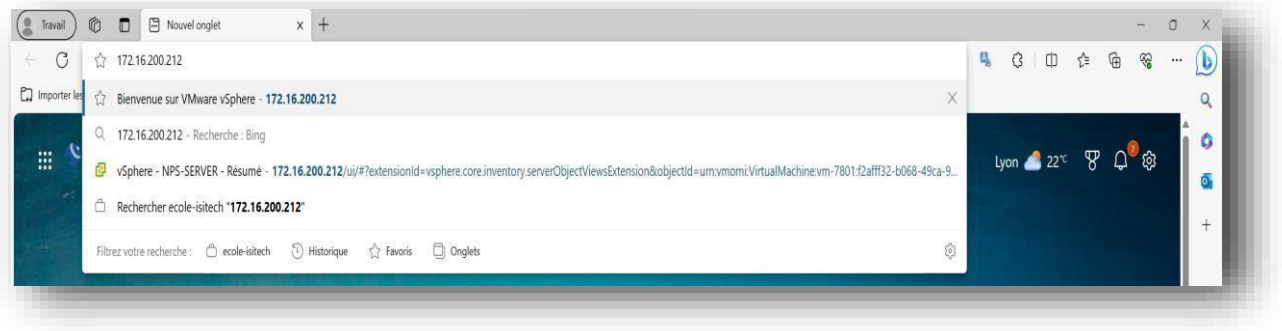
3.2 Partage de Fichiers
- Dossier partagé en SMB avec droits NTFS.
- Accès simultané pour les 2 utilisateurs.

3.3 VPN (Sécurité)
- Authentification via AD (RRAS ou OpenVPN).
- Chiffrement AES-256.
- Surveillance des connexions.

3.4 Ressources de Base
- Services : DHCP, DNS, Sauvegarde automatique.
- Maintenance : Mises à jour (WSUS) + monitoring.

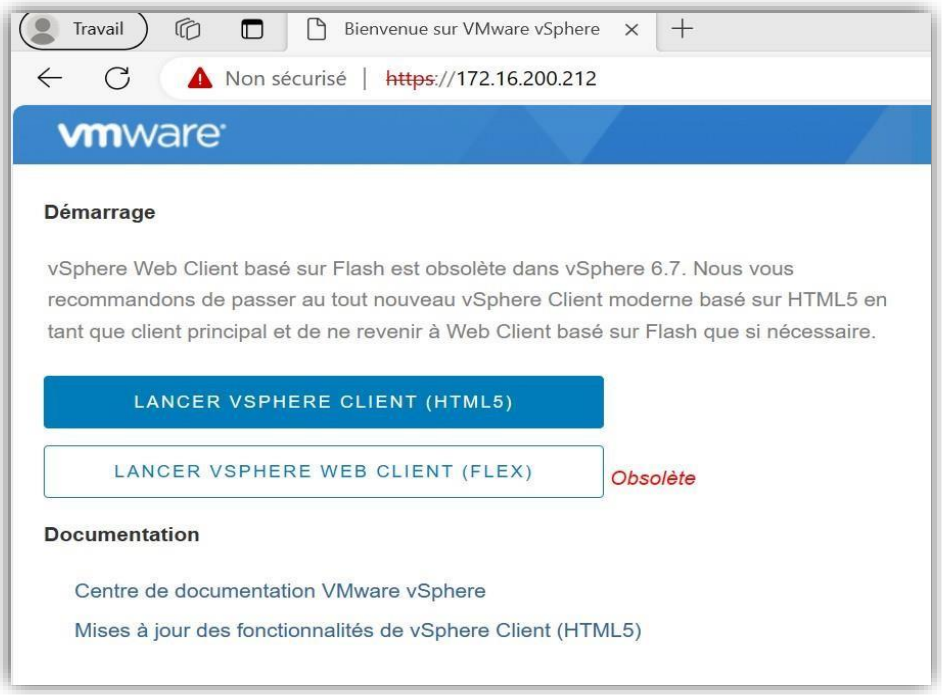
Procédure Technique : Création d'une Machine Virtuelle sous Windows 2019

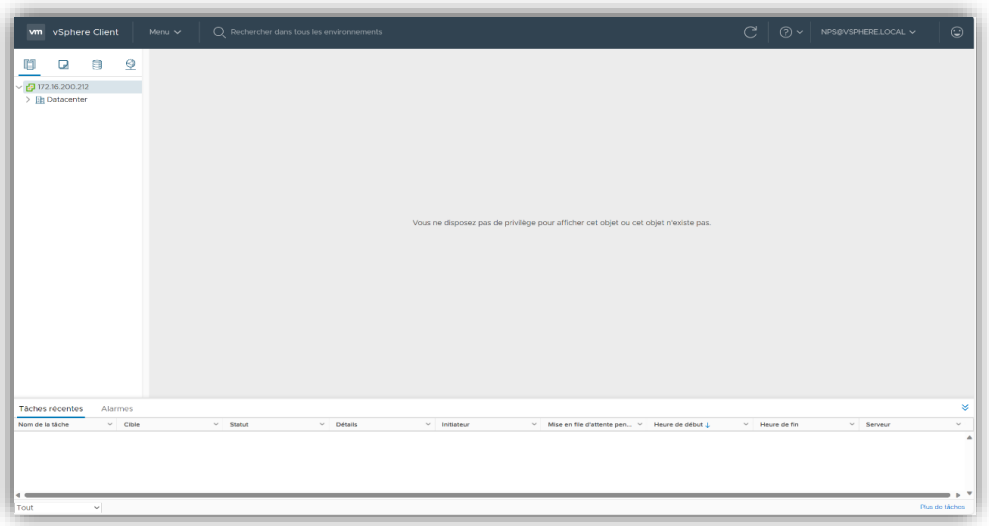
1. Ouvrir le navigateur internet et taper l'adresse IP suivante dans la barre de recherche « 172.16.200.212 », appuyer sur entrer



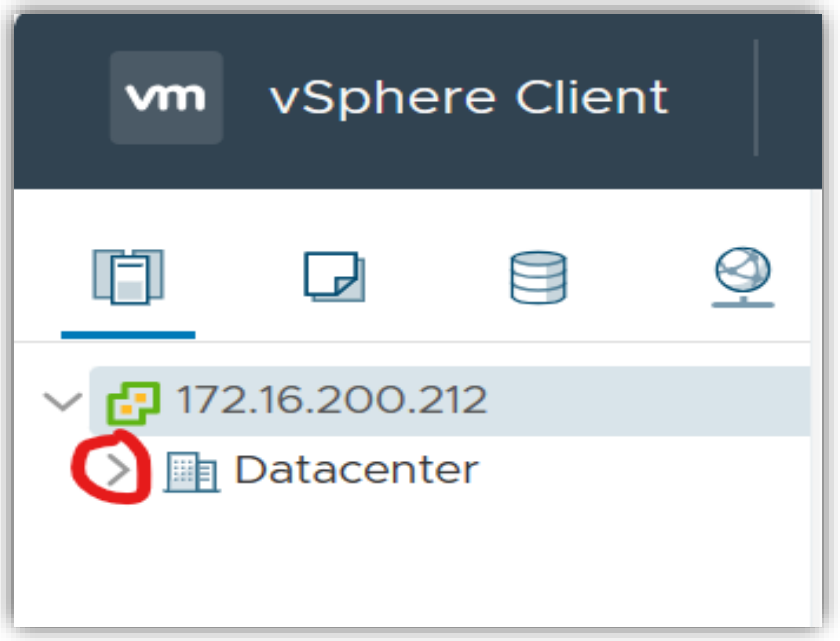
2. **On arrive sur cette page, cliquer sur « LANCER VSPHERE** CLIENT (HTML5) »

3. **On arrive sur l'espace qui va nous permettre de crée et de gérer la ou les machines virtuelles que nous allons créer**

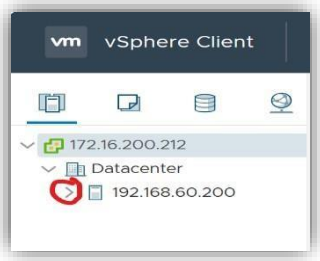


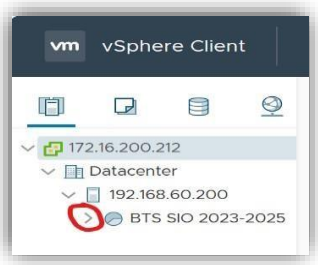


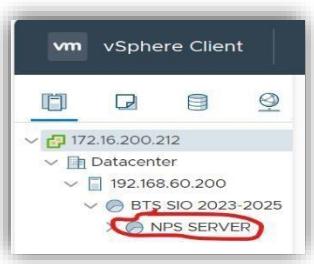
4. Cliquer sur la petite flèche sur la gauche de « Datacenter » pour afficher des informations complémentaires.



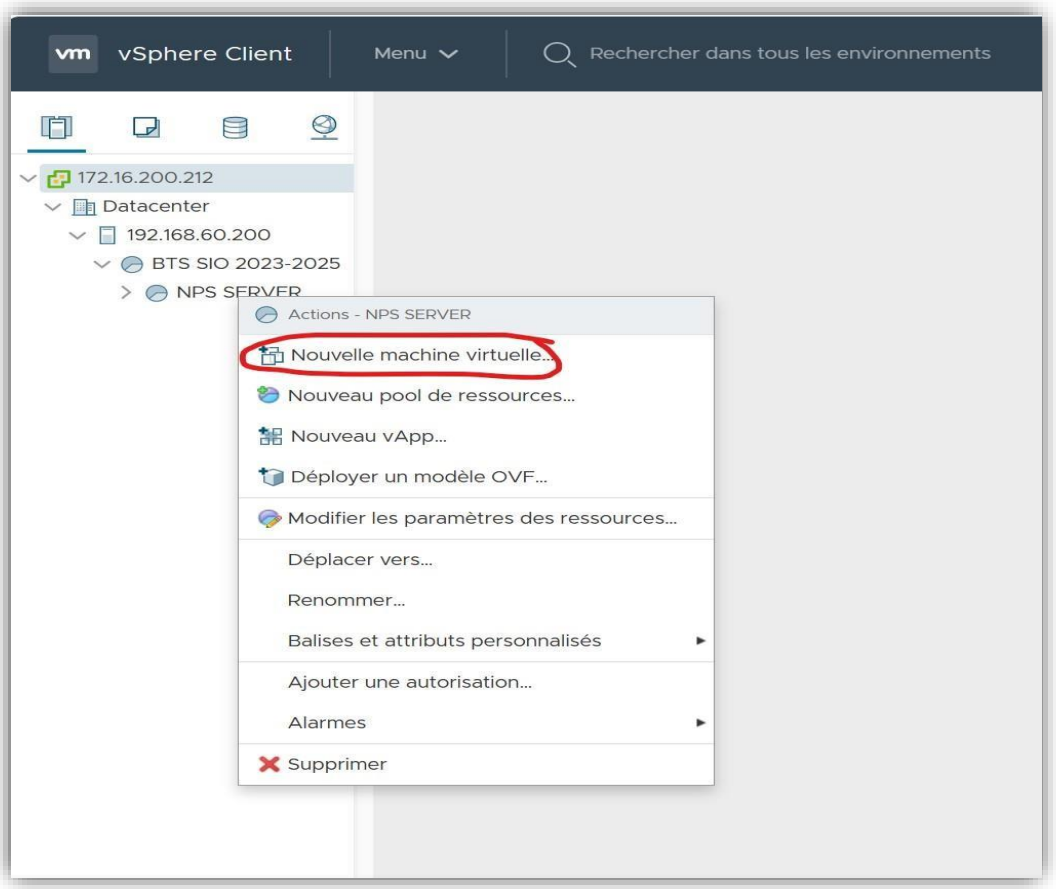
Répéter l'étape précédente avec la nouvelle information qui apparait jusqu'à ce que « LAB SERVER » apparaisse



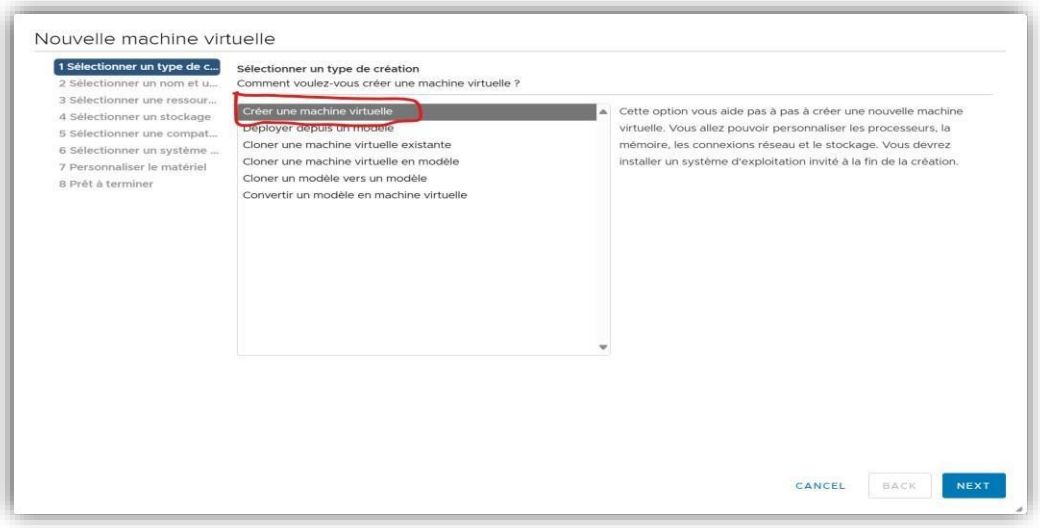




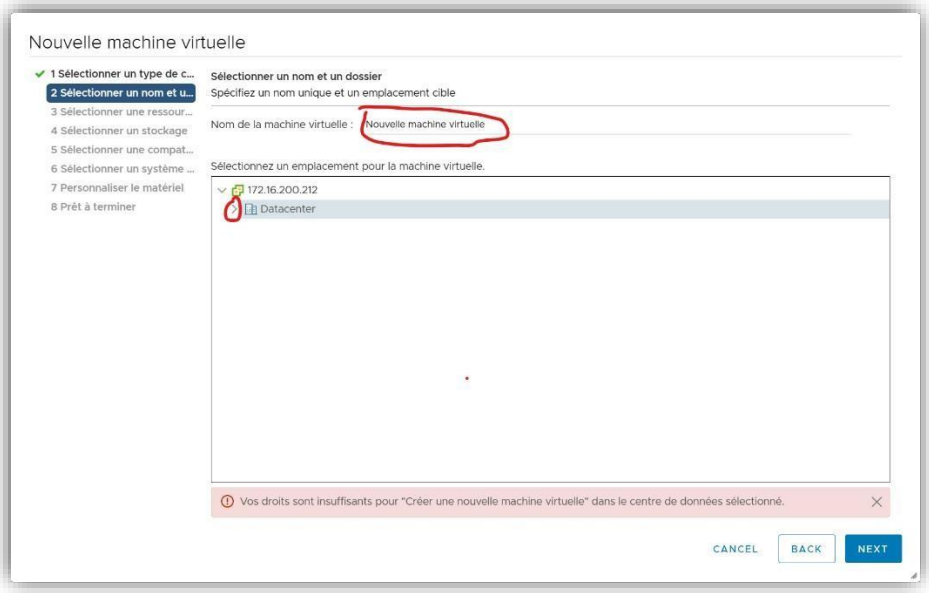
Clic droit sur « LAB SERVER » puis cliquer sur « Nouvelle Machine Virtuelle »

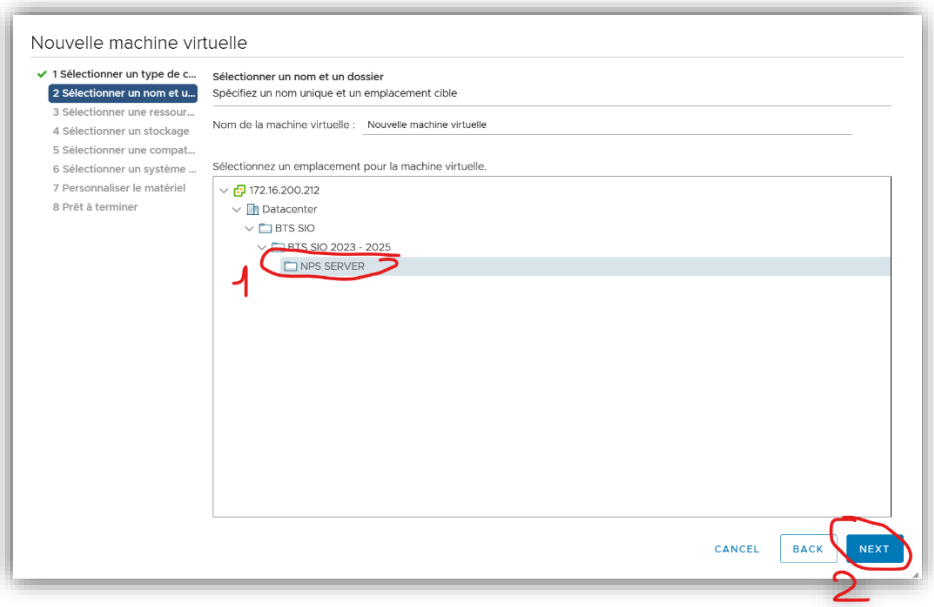


Une nouvelle page qui apparait, afin de procéder à la configuration la Machine Virtuelle. Cliquer sur Créer une machine virtuelle puis sur Next en bas à droite de la page

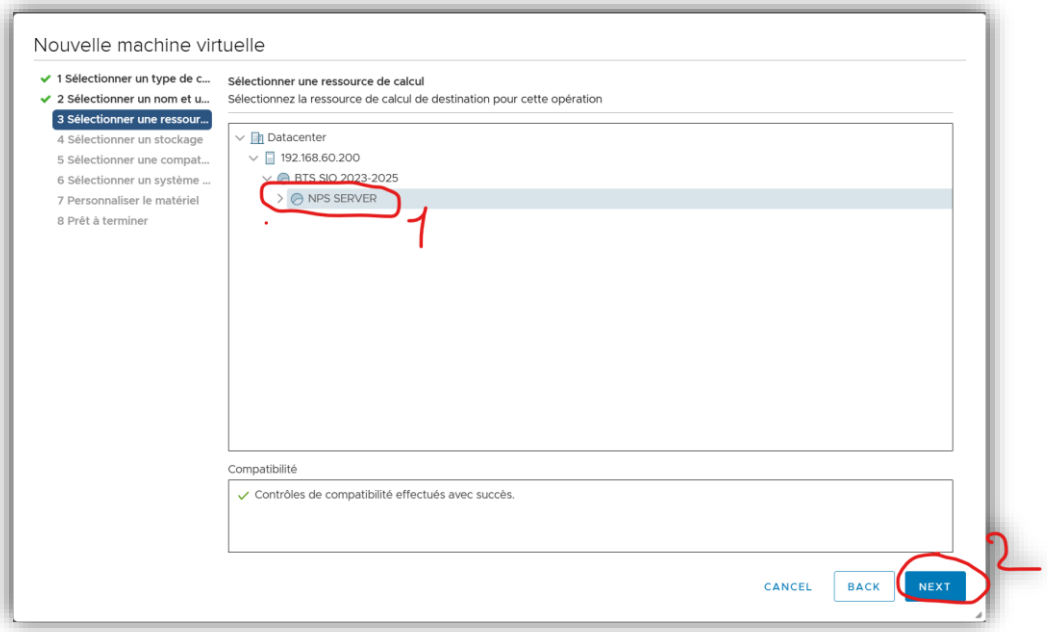


Entrer le nom que vous souhaitez donner à votre machine virtuelle puis cliquer sur la flèche à gauche de « Datacenter ».
Faire la même procédure jusqu'à ce que « LAB SERVER » soit affiché, le selectionner puis appuyer sur Next en bas à droite de la page

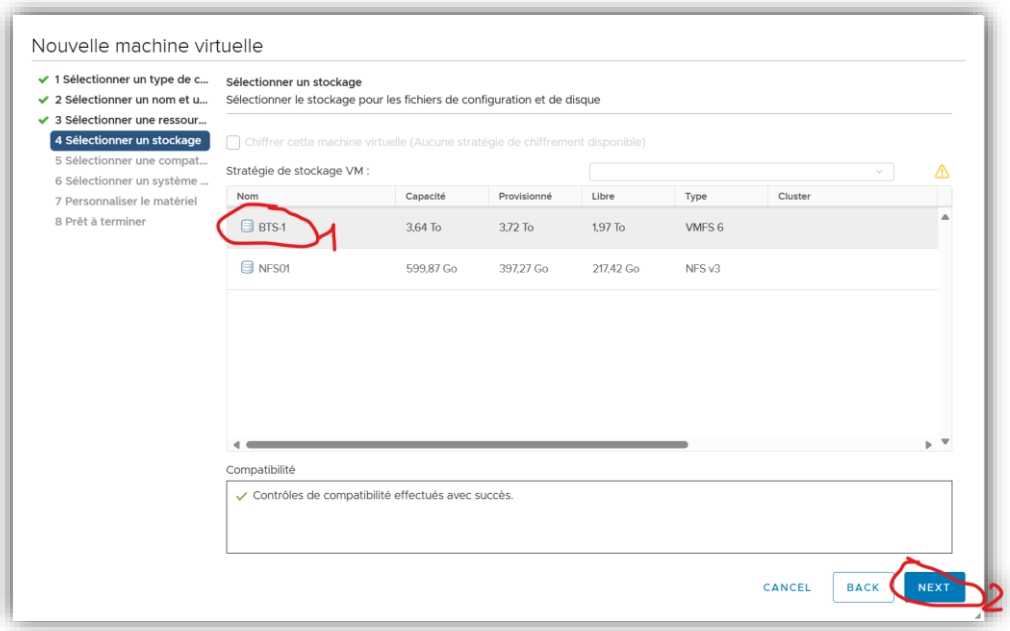




Sélectionner une ressource de calcul : sélectionner « LAB SERVEUR » puis cliquer sur NEXT

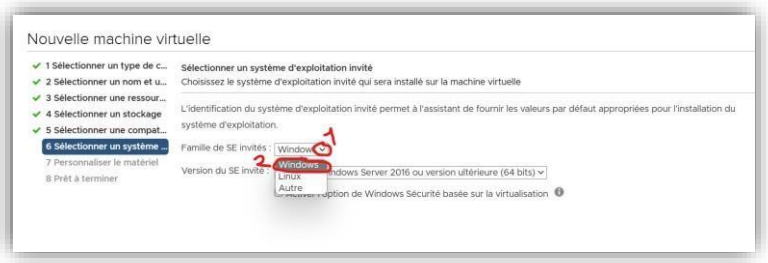


Sélectionner un stockage : cliquer sur « BTS 1 » puis cliquer sur NEXT pour passer à l'étape suivante

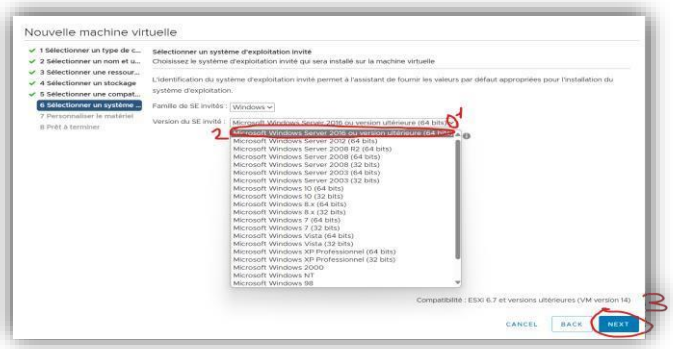


Sélectionner une compatibilité : cliquer sur la petite flèche vers le bas pour afficher un menu déroulant, sélectionner « ESXi 6.7 et versions ultérieures », cliquer sur NEXT pour passer à la suite.

Sélectionner un système d'exploitation : choisir le système d'exploitation qui sera installé sur la machine
Famille de SE invités : Cliquer sur la flèche vers le bas et choisir « Windows »



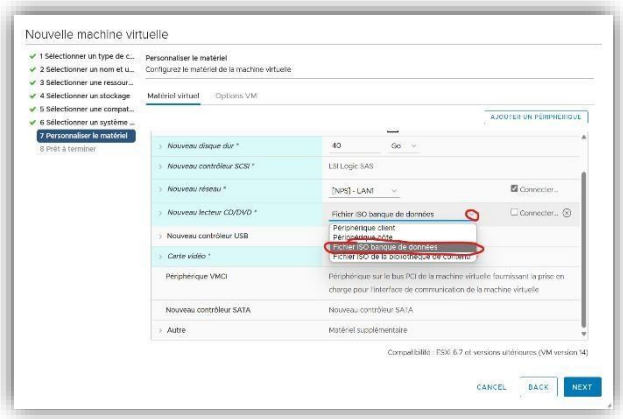
Version du SE invités : Cliquer sur la flèche vers le bas et choisir « Microsoft Windows Server 2016 ou version ultérieur (64 bits) puis cliquer sur NEXT pour poursuivre la procédure.



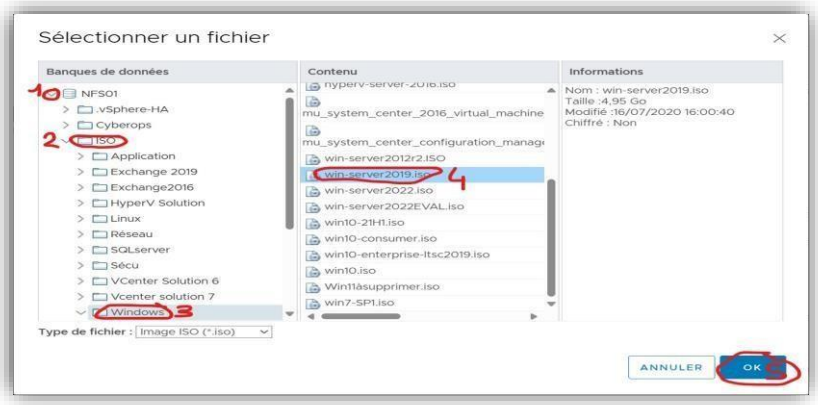
Personnaliser le matériel : sur la page ci-dessous, il est possible de configurer sa machine virtuelle avec les paramètres que l'on souhaite : nombre de CPU, mémoire, réseau … En fonction de ce que l'on souhaite faire sur la machine, il faudra des paramètres spécifiques.

Dans notre cas, il va falloir installer sur notre machine, une « image » de Windows 2019 à partir d'un « fichier d'archive » trouvé sur un serveur, une base de données.

Voici la procédure à suivre :
Dans la partie intitulé « nouveau lecteur CD/DVD » cliqué sur la petite flèche vers le bas et sélectionner Fichier ISO banque de données » et cocher la case « connecté » qui est juste à côté (à droite)



Une Nouvelle page s'ouvre, sélectionner « NFS01 » puis « ISO », choisir le dossier « Windows », cliquer sur le fichier « win- server2019.iso » et cliquer sur OK

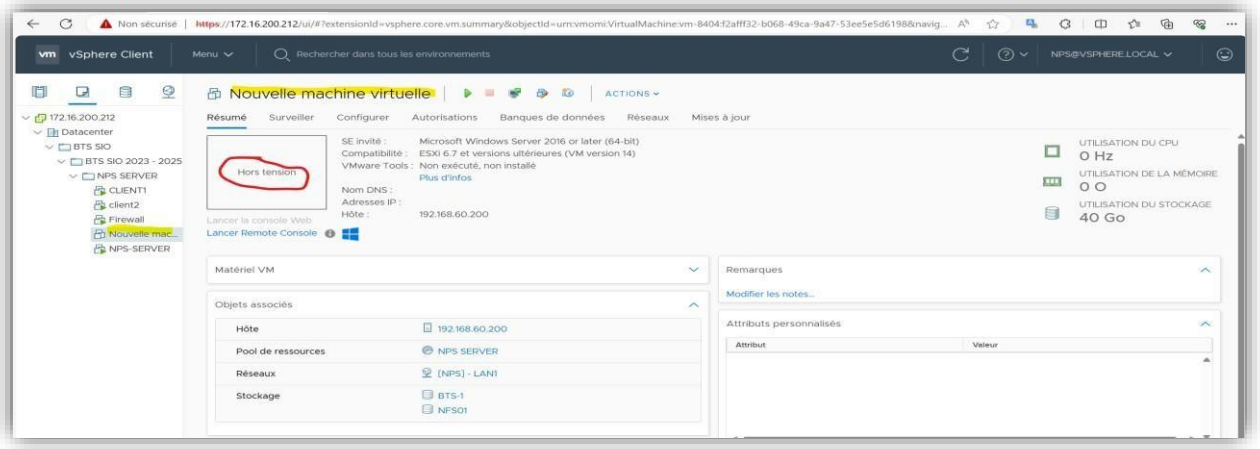


Cela nous ramène sur la page pour personnalisé le matériel, cliquer sur NEXT pour continuer.

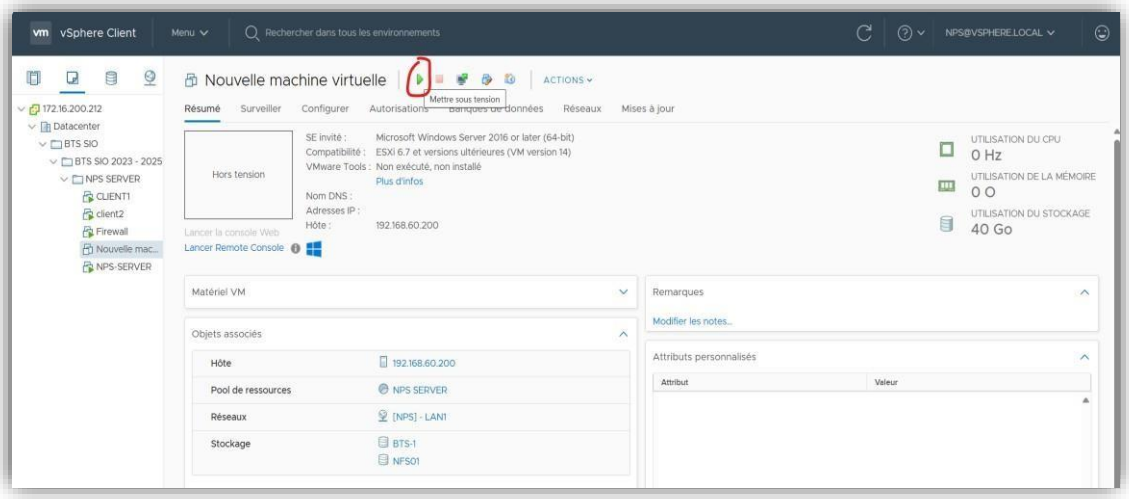
La dernière page apparait, elle vous permet de vérifier tout les paramètres de la Machine Virtuelle

Si il y'a une erreur, il est possible de la modifier en sélectionnant, sur le côté gauche de la page, la catégorie concerné, et modifier le paramètre en question.
Si il n'y a pas d'erreur, il faut cliquer sur « FINISH », la Machine Virtuelle est créer et configurer.

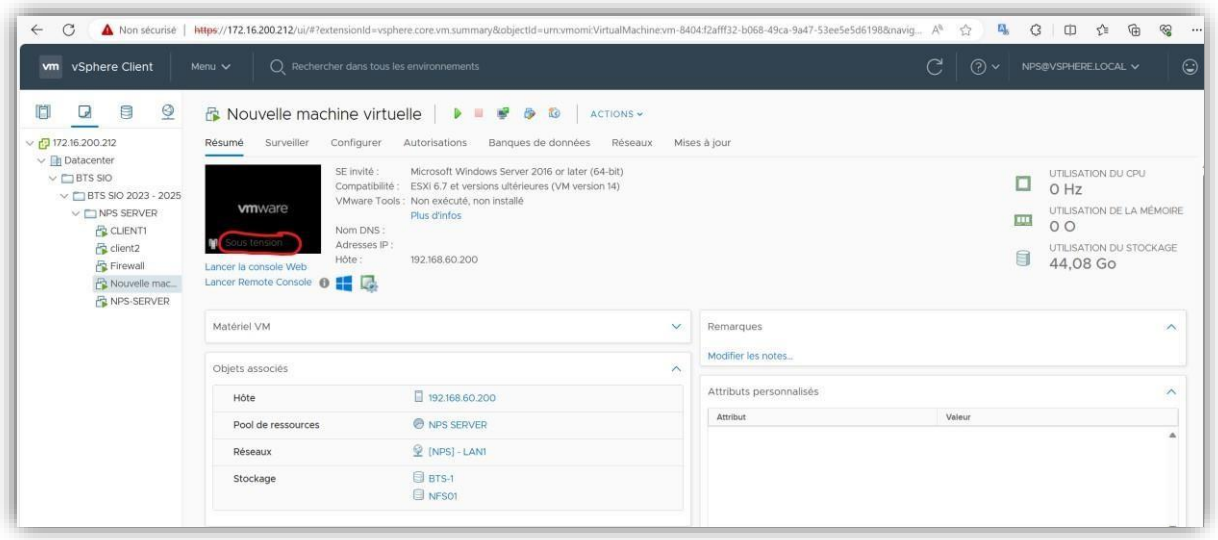
Une fois la configurations terminé, cela nous ramène sur l'interface.
On voit bel et bien que la Machine existe, en effet, elle fait
partie de la liste de l'ensemble des différents Machines Virtuelles que nous avons créée dans le cadre de notre projet.
En Revanche on constate qu'elle est pas alimenté : « hors tension », par conséquent on ne peut l'utiliser pour le moment.



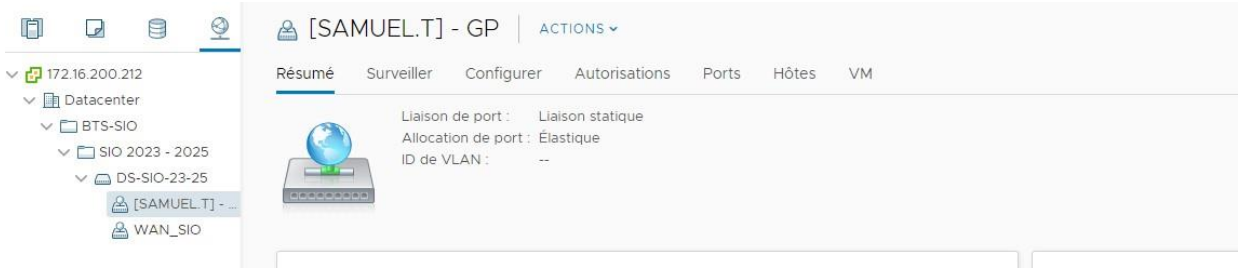
Pour la mettre sous tension, et ainsi, pouvoir utiliser la machine, il faut cliquer sur le bouton Vert « Mettre sous tension »



Une fois que nous avons appuyé sur le bouton « Mettre sous tension », la machine est alimenté et nous pouvons donc
l'utiliser en cliquant sur la vignette.



Ensuite nous avons créé notre réseau spécifique avec les vlans sur mon switch



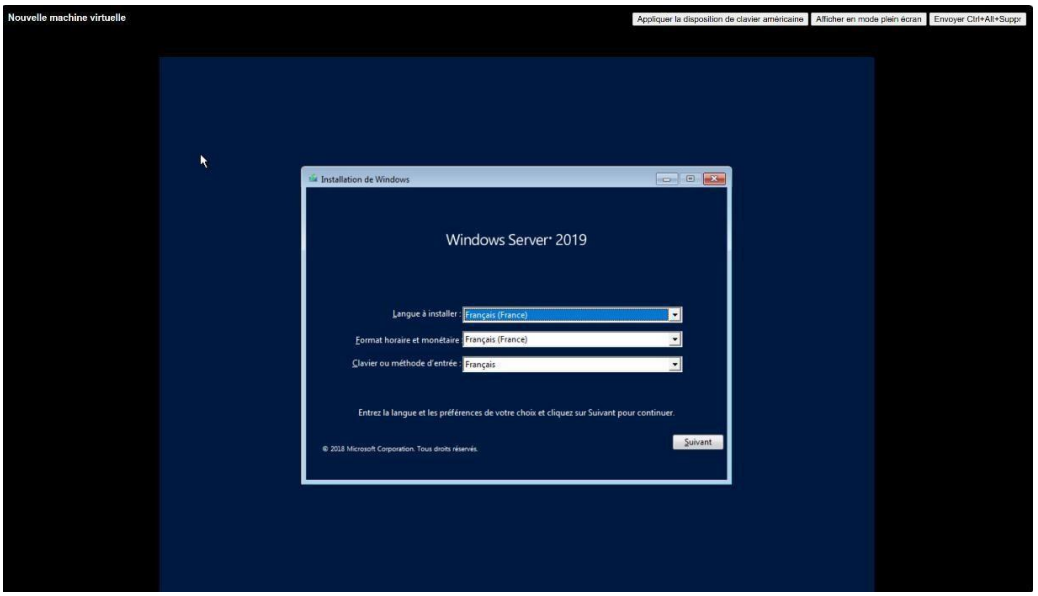
Dans celui si mettre les vlan sur les port spécifiques des appareils client et des appareils serveurs

[SAMUEL.T]FIREWALL	--	[SAMUEL.T] - GP	Raccordé	Accès VLAN : 280
[SAMUEL.T]LAB-PC02	--	[SAMUEL.T] - GP	Raccordé	Accès VLAN : 281
[SAMUEL.T]SRV-LAB-AD	--	[SAMUEL.T] - GP	Raccordé	Accès VLAN : 280
[SAMUEL.T]LAB-PC01	--	[SAMUEL.T] - GP	Raccordé	Accès VLAN : 281
[SAMUEL.T]FIREWALL	--	[SAMUEL.T] - GP	Raccordé	Accès VLAN : 281
[THOMAS]-SRV-GLPI	--	[SAMUEL.T] - GP	Raccordé	Accès VLAN : 280

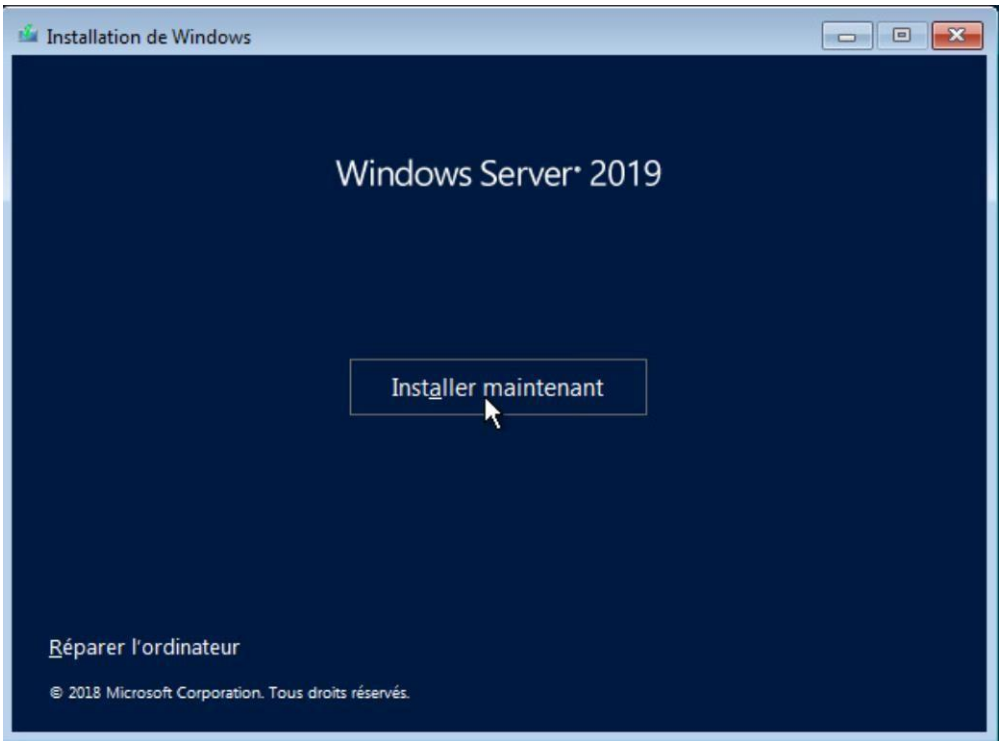
Installation de Windows serveur 2019

Lors du démarrage appuyé sur un n'importe quel touche afin de boot sur le CD virtuel de la VM ayant l'ISO

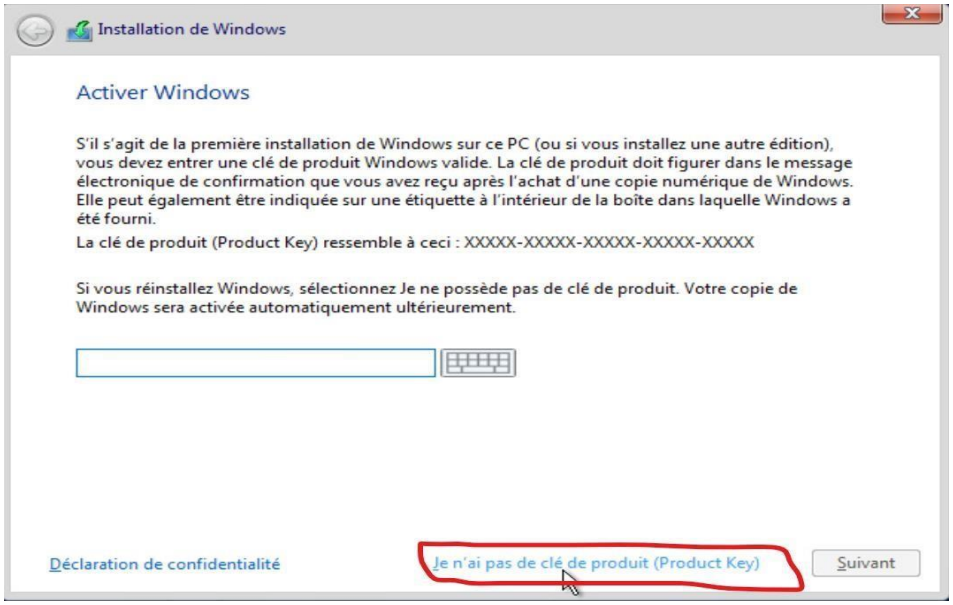
On arrive sur cette page, il faut compléter ce qui nous est demandé puis cliquer sur suivant.



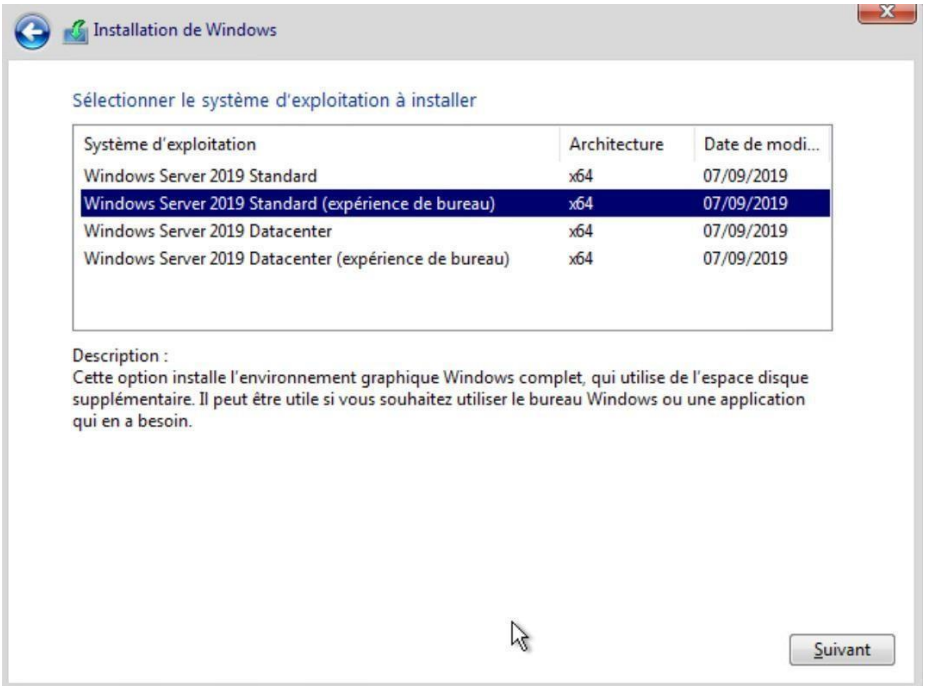
Cliquer sur « installer Maintenant », le programme d'installation va se lancer.



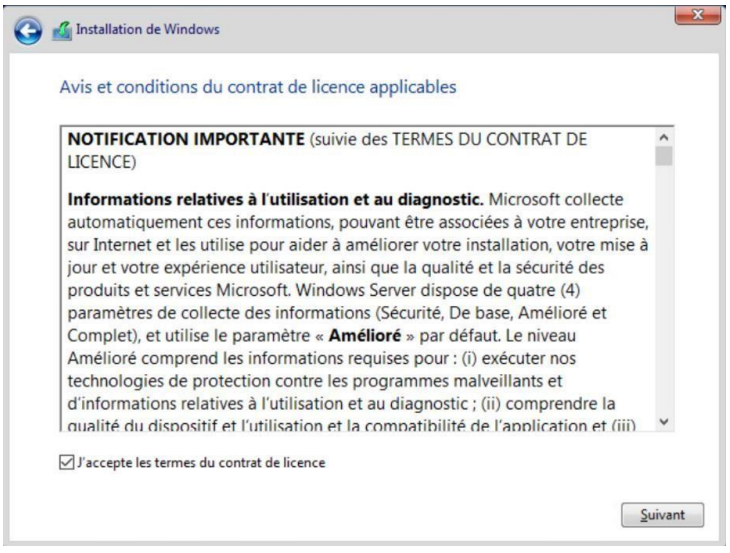
Cliquer sur « je n'ai pas de clé de produit »



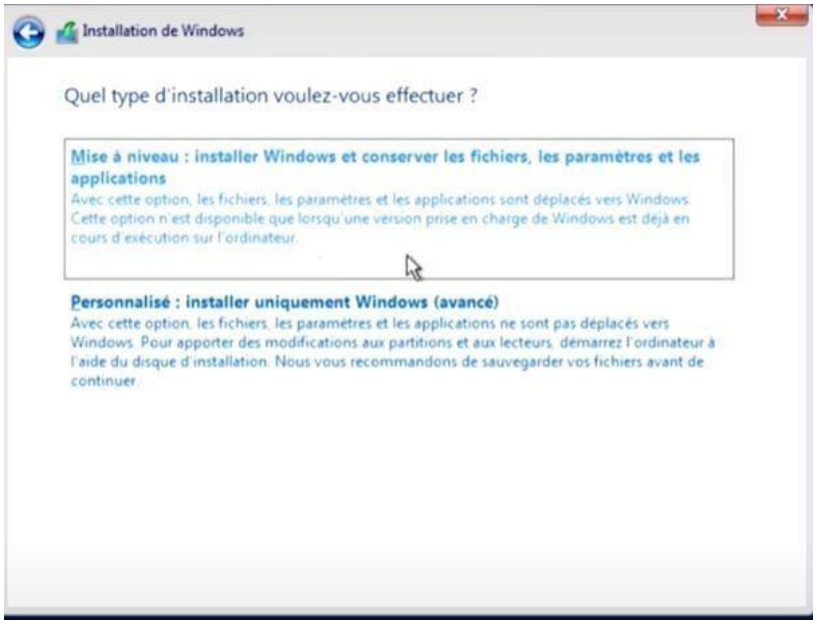
Choisir « Windows Server 2019 Standard (expérience de bureau) » pour avoir l'interface graphique. Puis cliquer sur suivant.



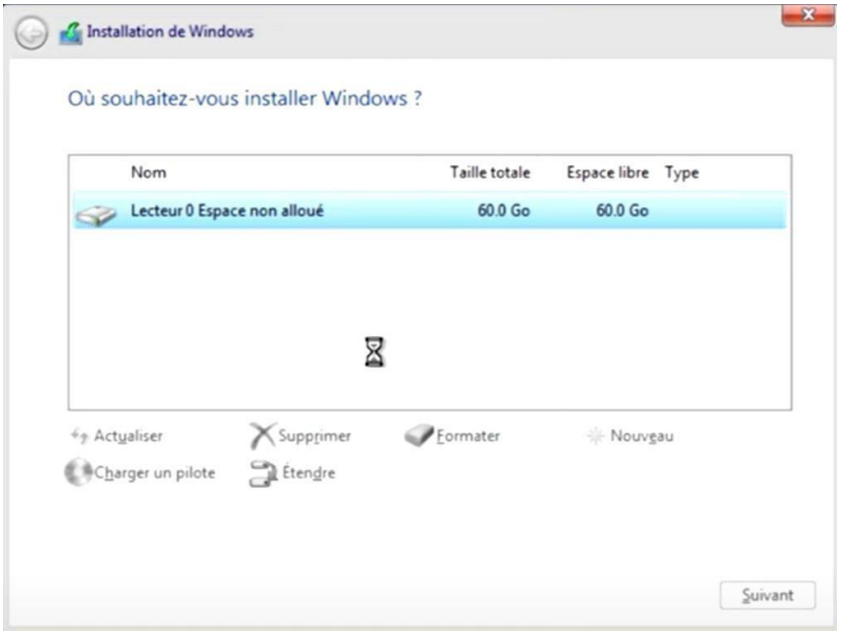
Une page va s'afficher, il faut accepter les termes du contrat de licence puis cliquer sur suivant.



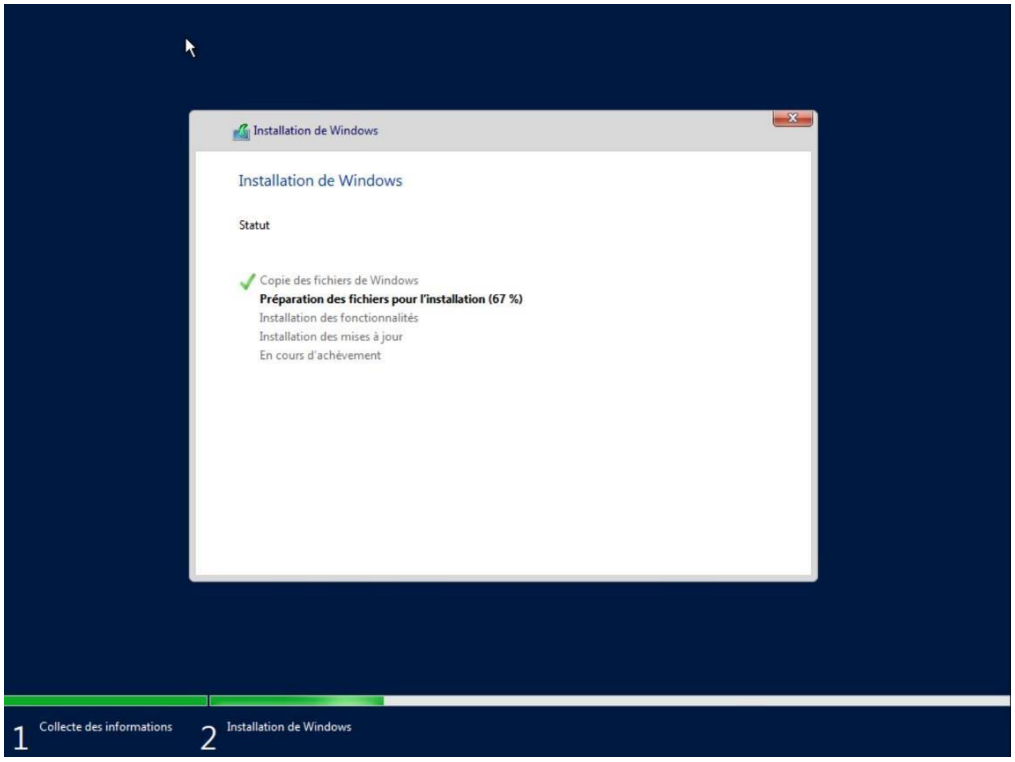
Avant de démarrer l'installation, ils vont proposer 2 méthodes d'installation, dans notre cas, on choisit la 2ème option.



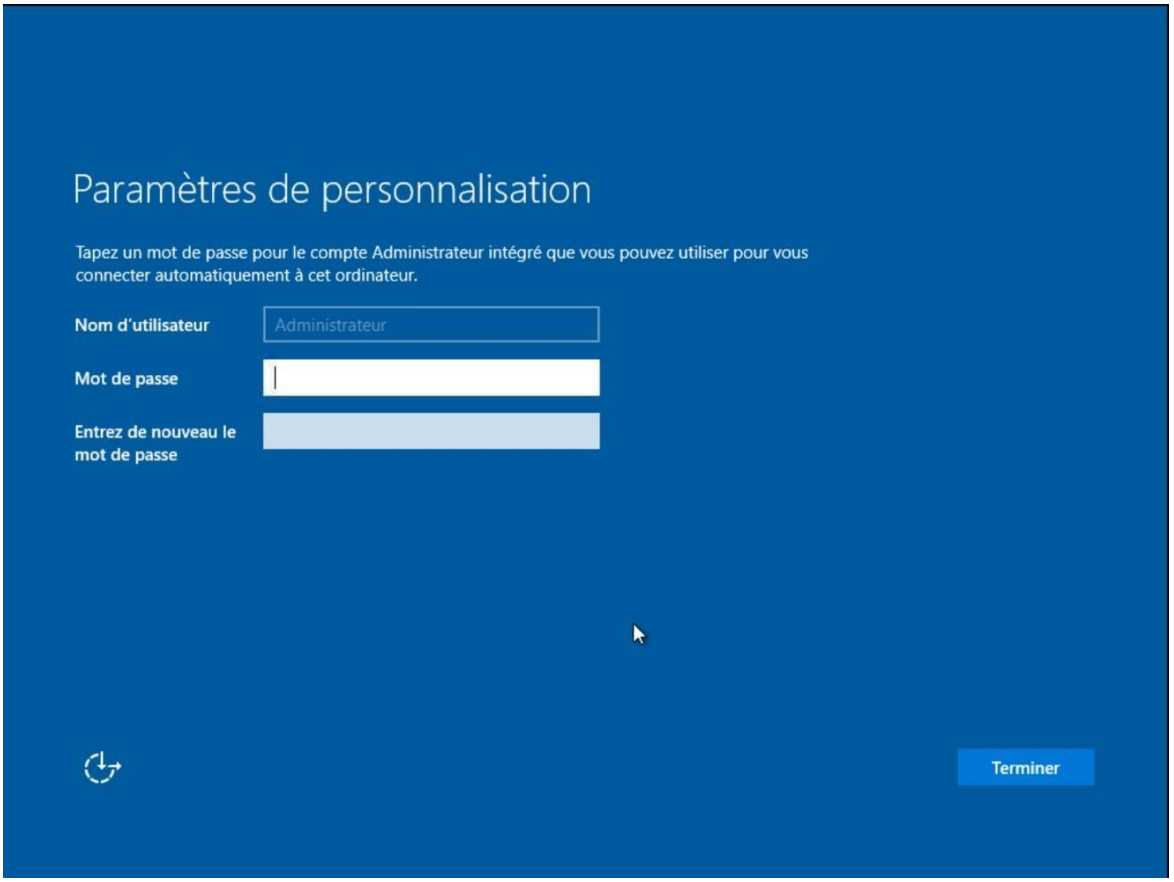
De plus, ça va également vous demander l'endroit ou installer Windows, cliquer sur suivant. (Image prise sur internet, le lecteur était de 40go dans notre cas)



L'installation est en cours, il faut patienter



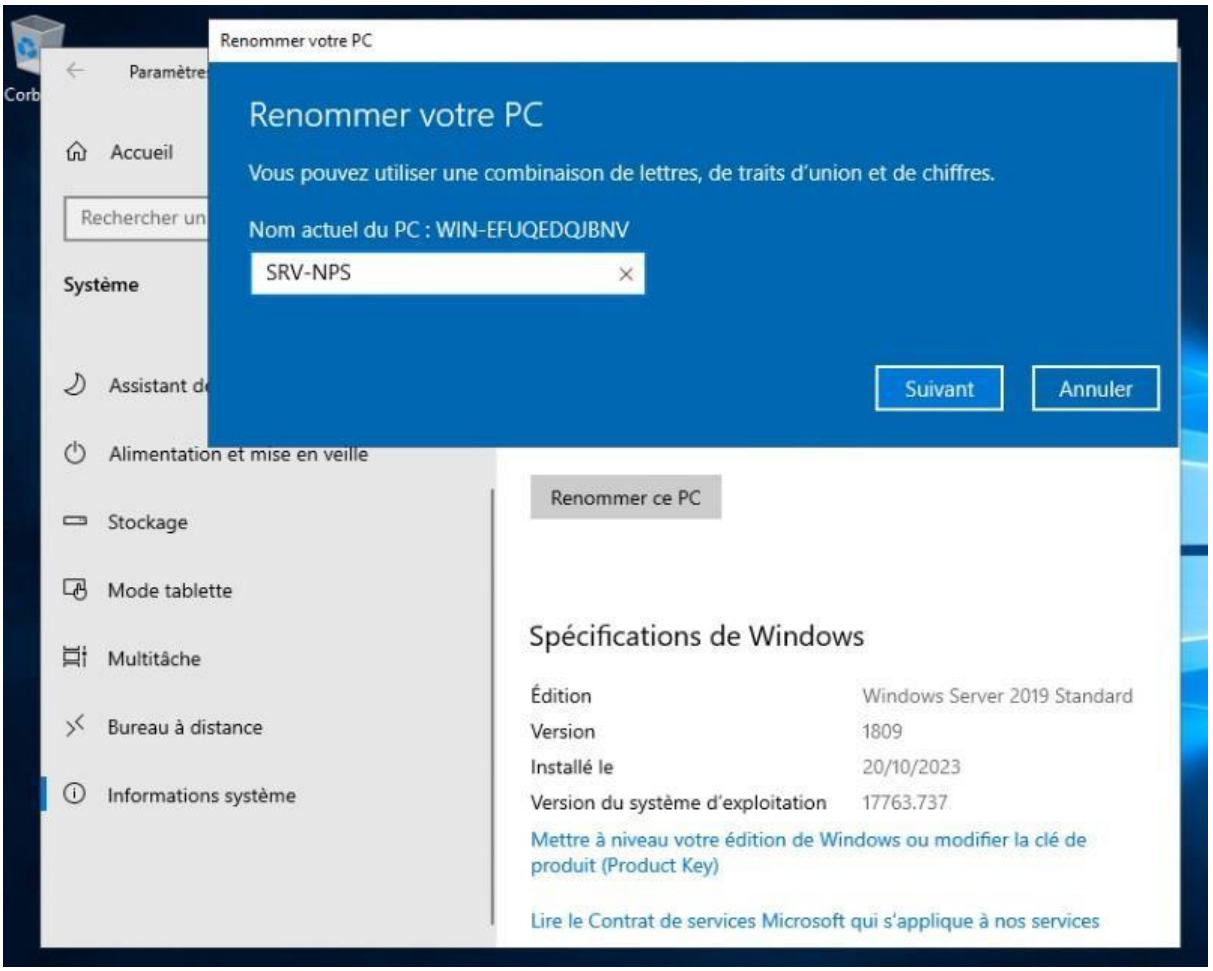
On arrive sur la fin, il faut remplir les informations demandé



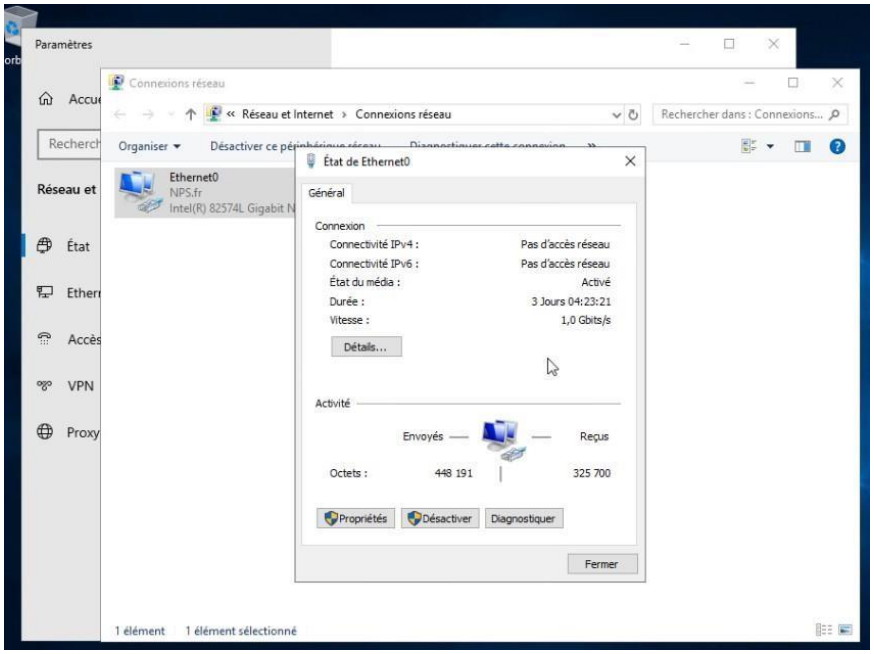
L'installation de Windows est terminée

Installations active directory, DNS, DHCP

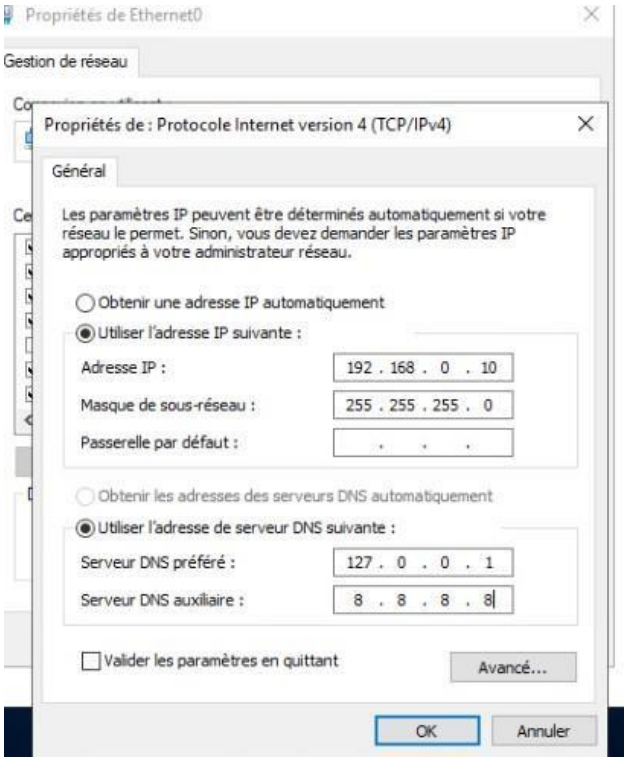
Tout d'abord, il faudra renommer le poste afin d'y ajouter un domaine avec le nom souhaité. Pour cela, il faudra se rendre dans les paramètres système « information système ».



Ensuite, il faudra définir une adresse IP statique pour le serveur, généralement en choisissant la dernière ou l'une des premières adresses telles que .254 ou .10. Pour ce faire, il est nécessaire de se rendre dans les paramètres réseau et de modifier l'adresse IPv4.



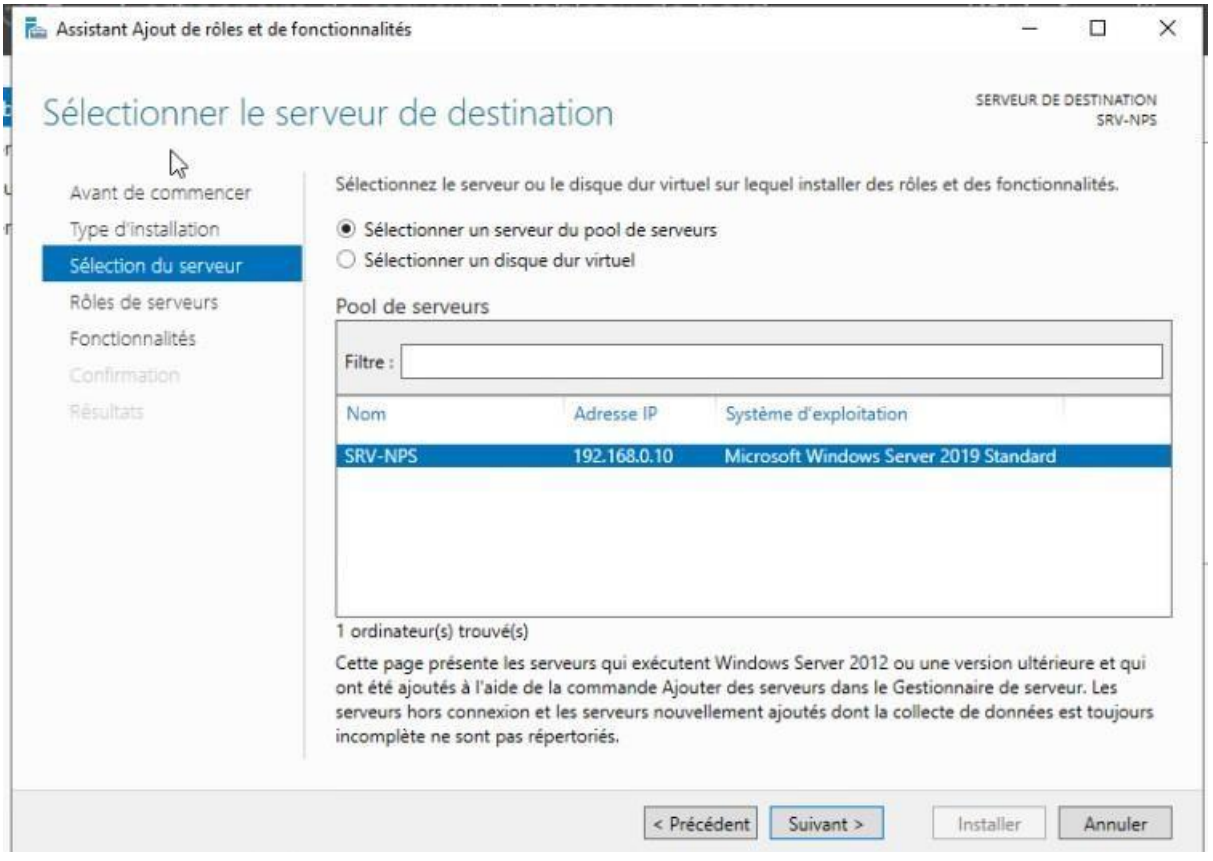
Comme notre serveur vas servir de DNS on lui attribue le DNS



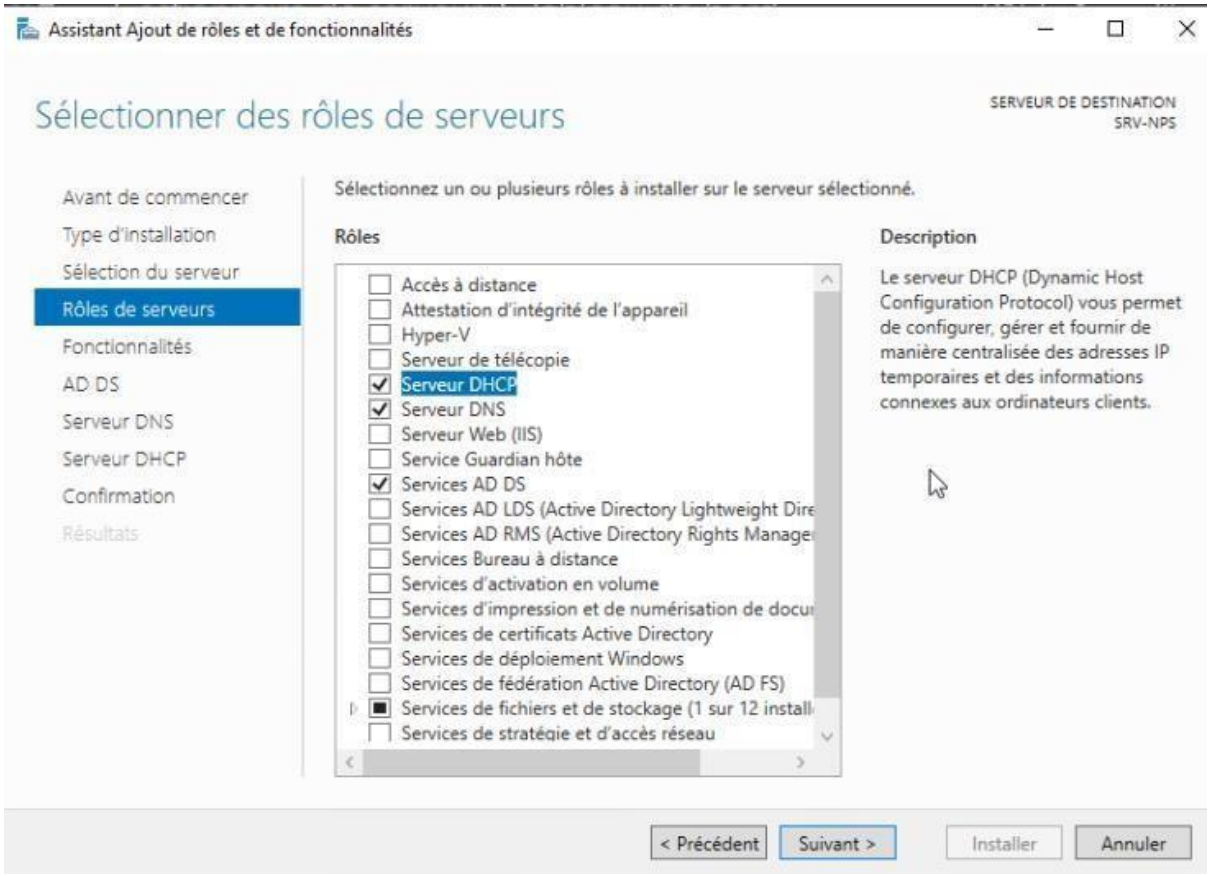
127.0.0.1 qui correspond à lui-même.

Suite a sa il faut se rendre dans la gestionnaire de serveur afin d'y ajouté des rôles et fonctionnalités.

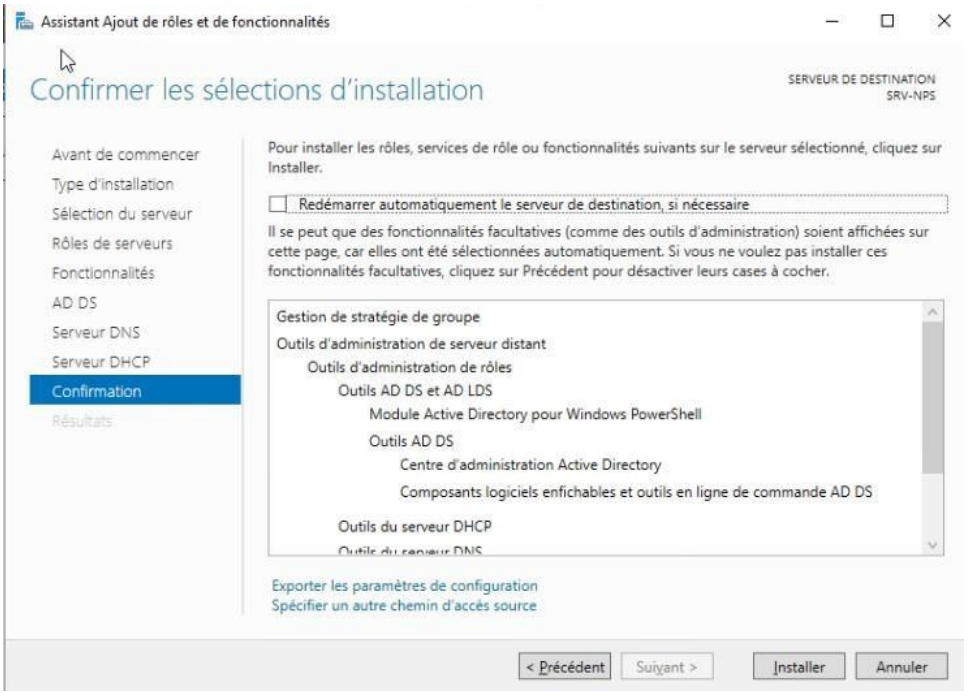
Nous allons ajouter les rôles active directory DNS et DHCP. On retrouve dans le domaine le nom de notre serveur.



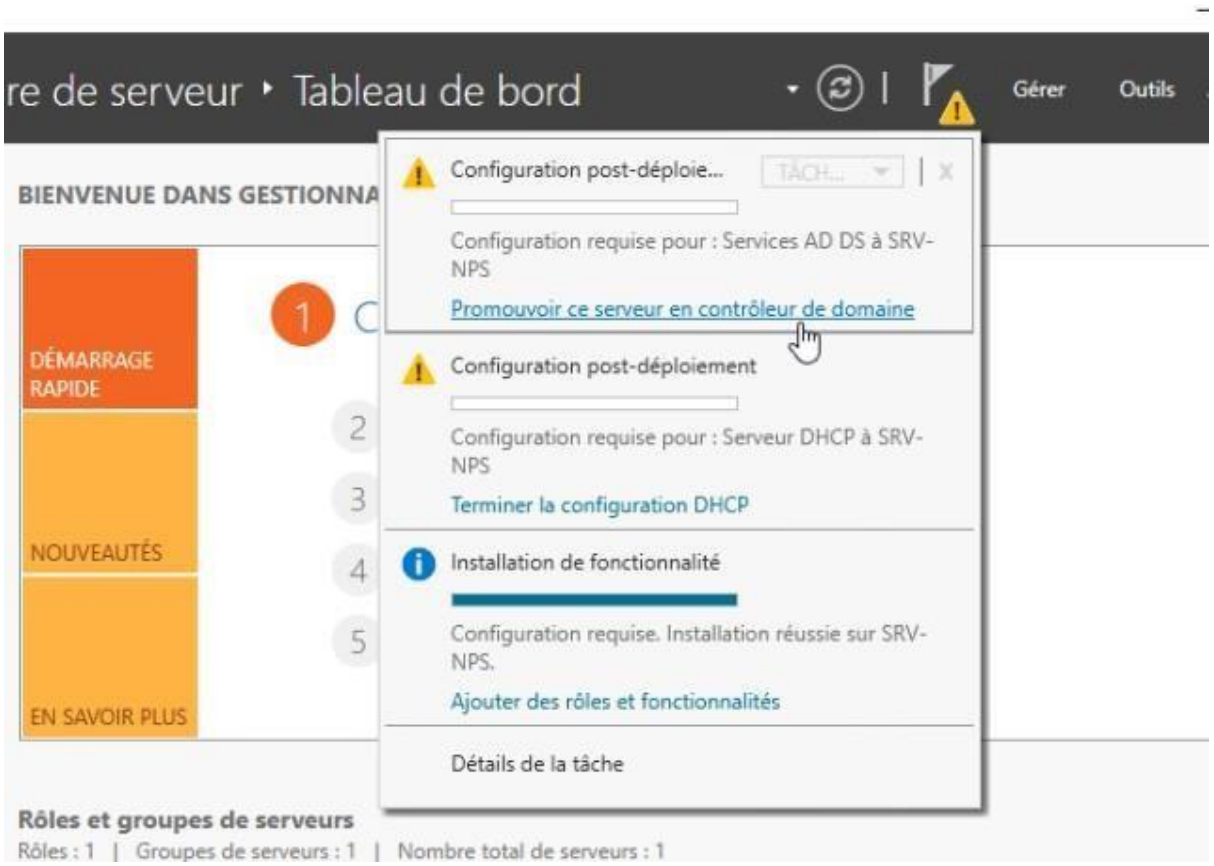
Faire suivant et cocher les rôles a ajouté. A chaque fois faire
« ajouté les fonctionnalités.



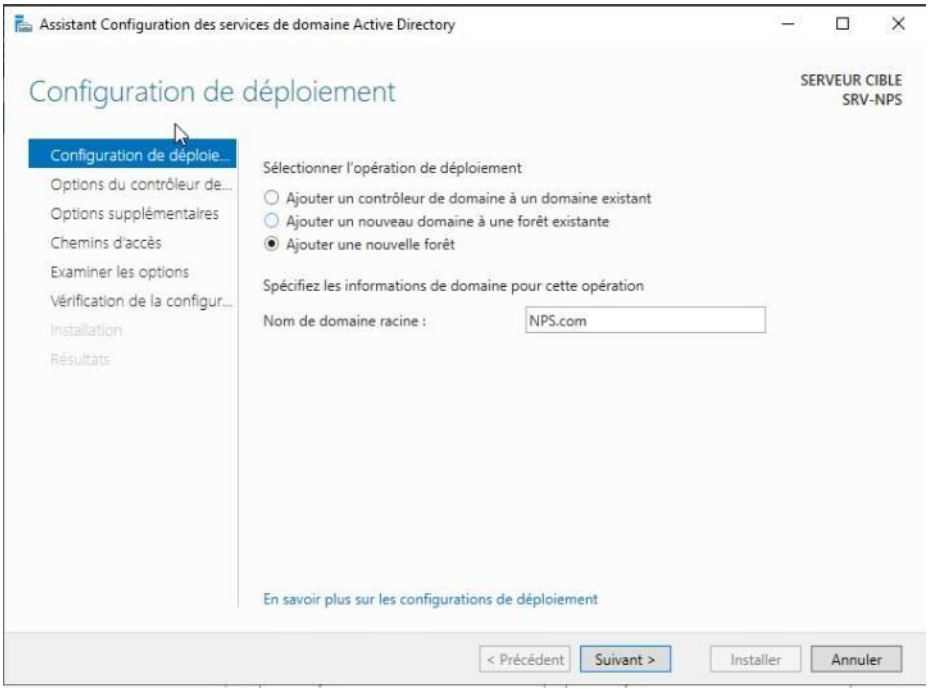
Faire suivant jusqu'à arriver ici et cliqué sur « installer » :



Suite a sa cliqué sur le drapeau et cliqué sur promouvoir ce serveur en contrôleur de domaine.

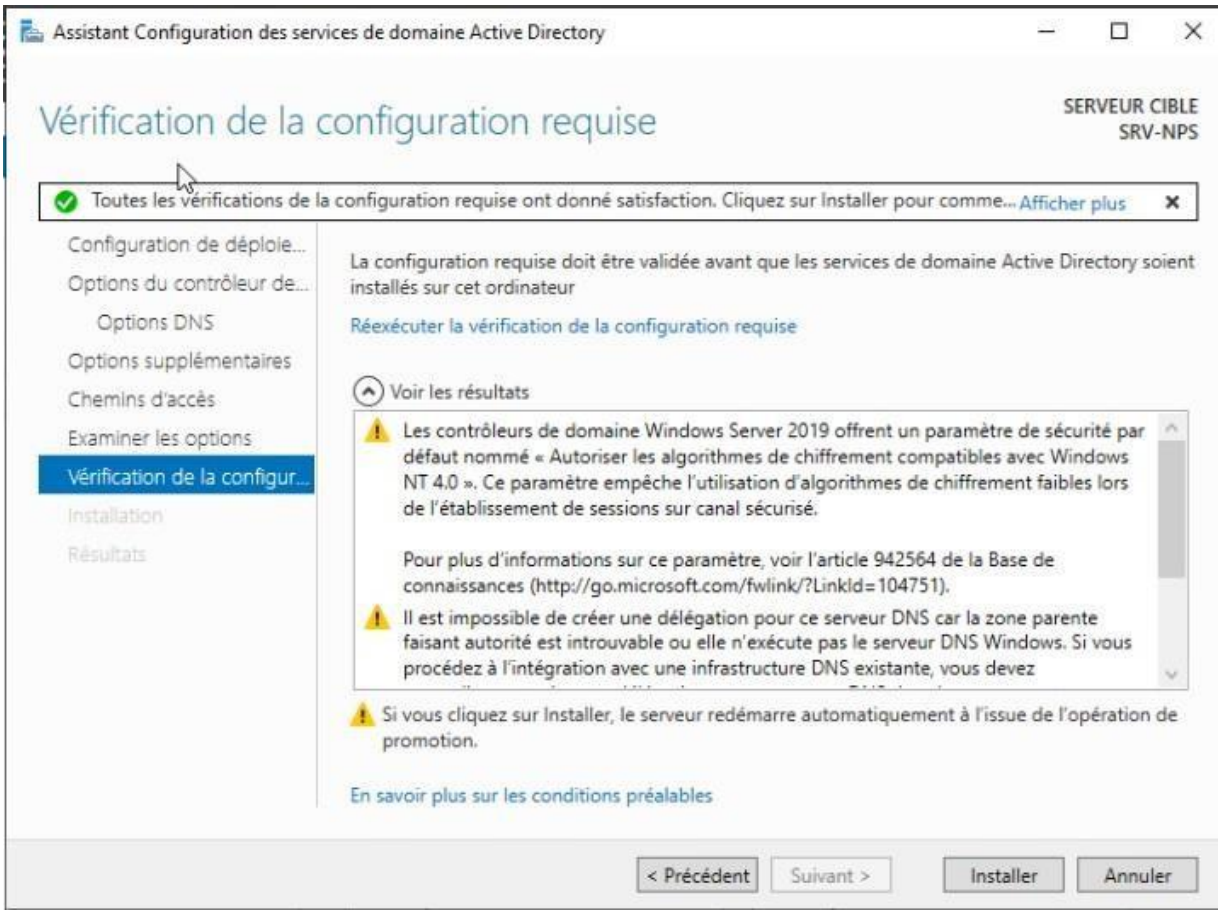


Remplir de cette manière pour avoir notre domaine ne tant que LAB.com. cliqué sur « suivant ».



Suite a sa ne rien changer entrée juste un mdp et cliqué sur « suivant »

Continué de cliquer sur « suivant » jusqu'à arriver sur cette page.
Cliqué sur « installé ».

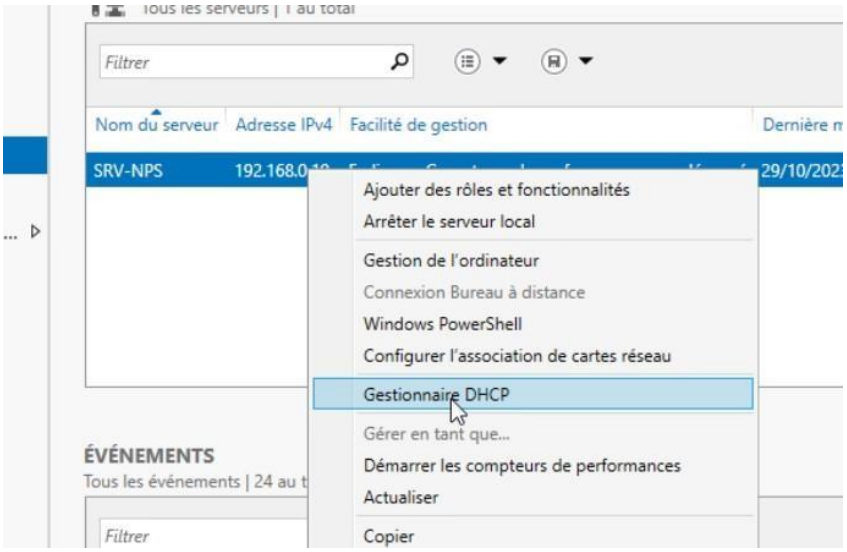


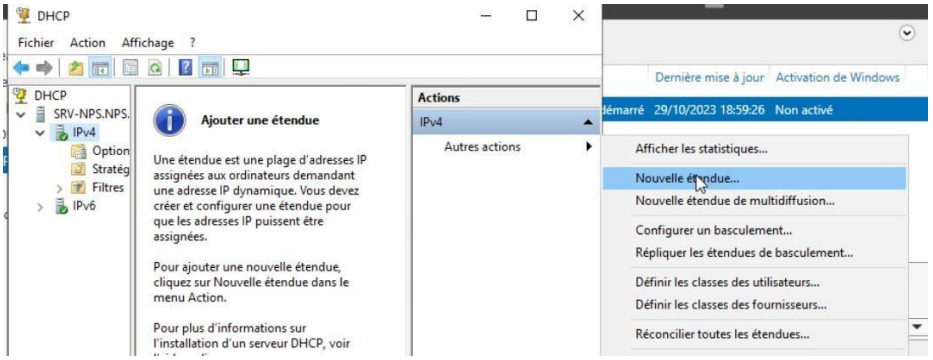
Le redémarrage est nécessaire afin de prendre en compte l'active directory.

Apres cela il faudra donc configuré le serveur DHCP. Cliqué sur « terminé la configuration » puis « suivant » et
« validé » et « fermé ».

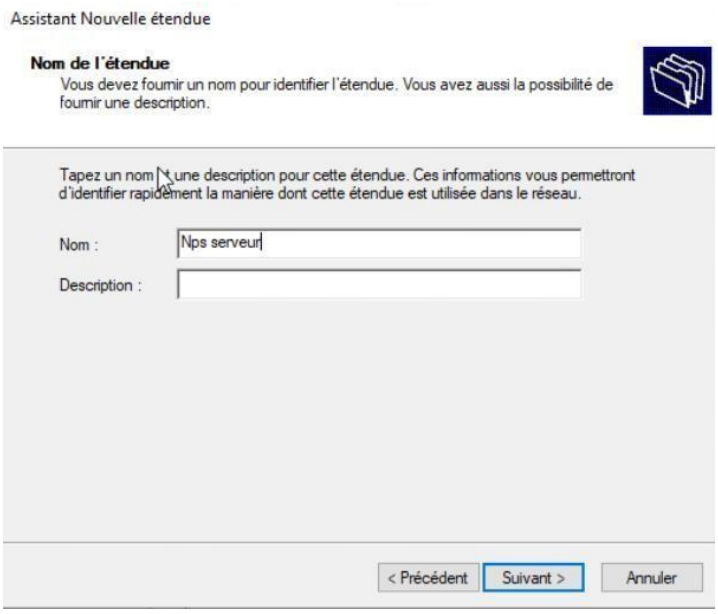
Pour le serveur DHCP il faudra définir ce qu'on appelle un
« pool d'adresse » afin d'attribuer une adresse ip automatiquement et définir un bail pour celles-ci.

Pour cela il faudra allez dans gestionnaire de DHCP et créer une étendue en allant dans ipv4.

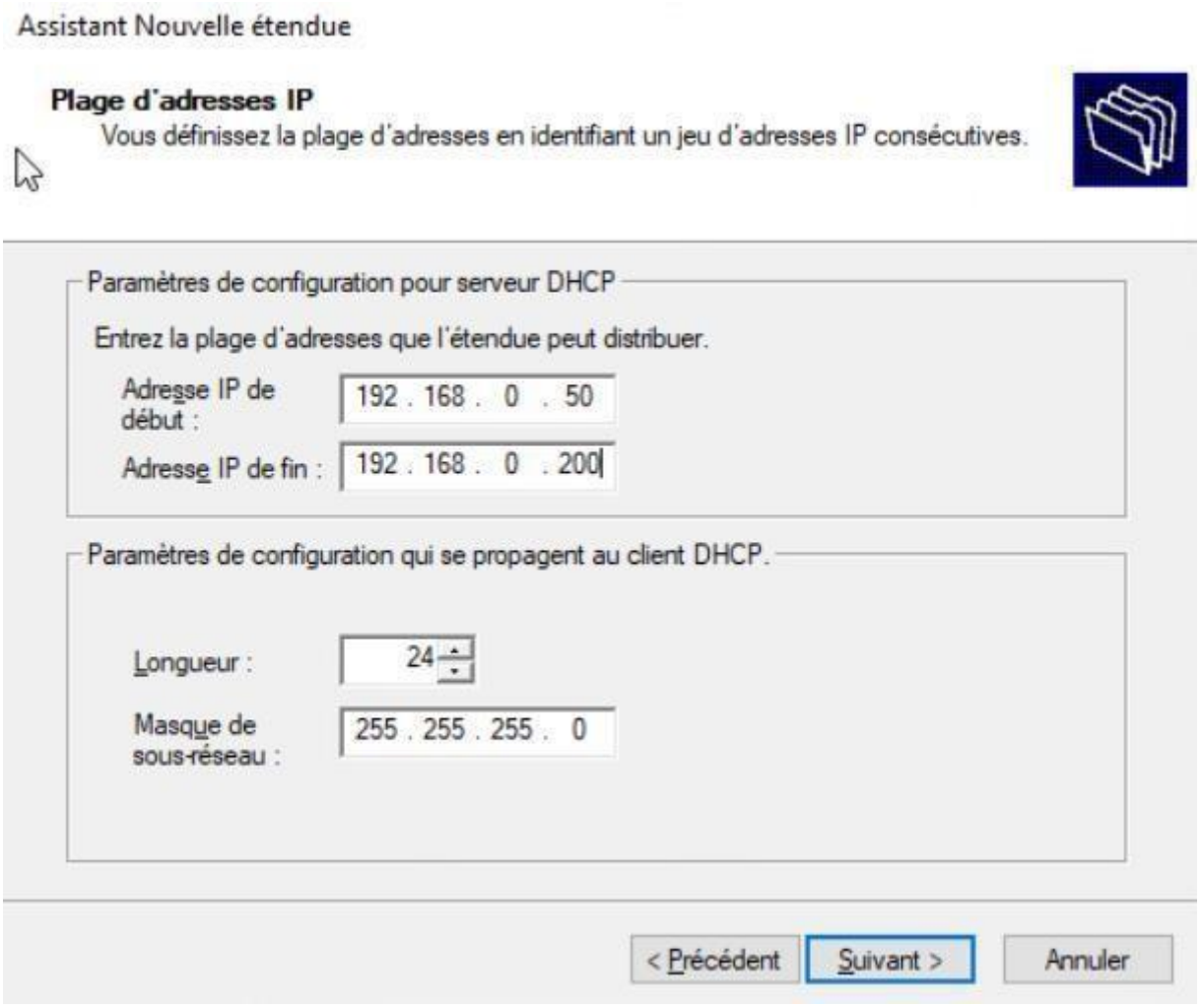




Cliqué sur «suivant» puis mettre le nom souhaité puis «suivant».

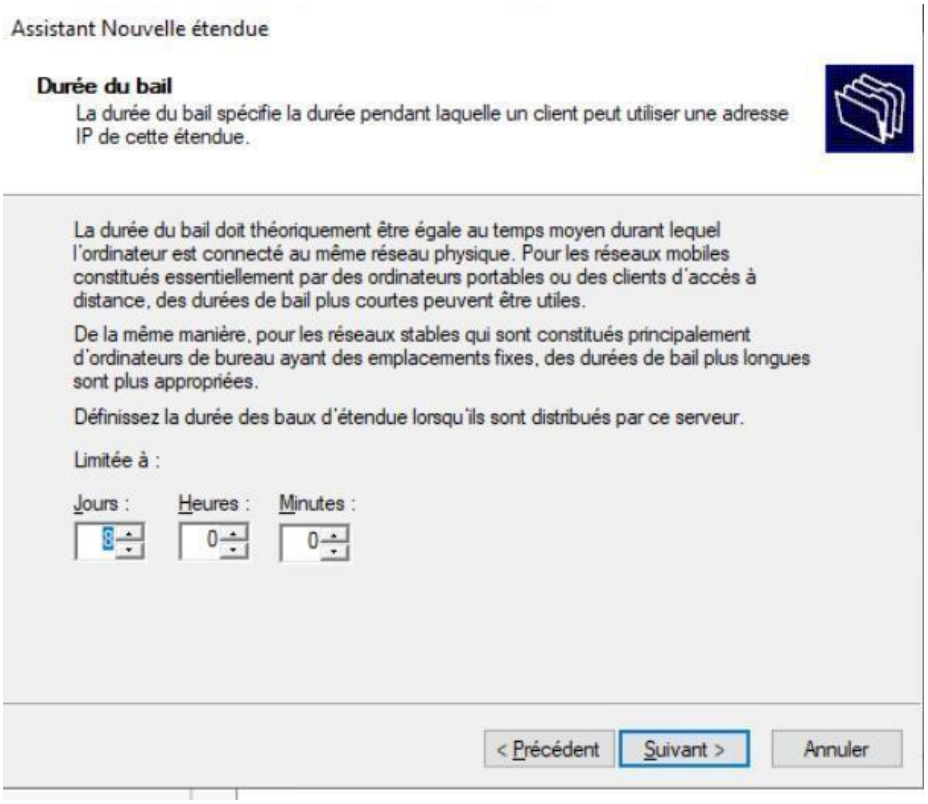


Et enfin attribué le pool que l'on veut avec le masque.



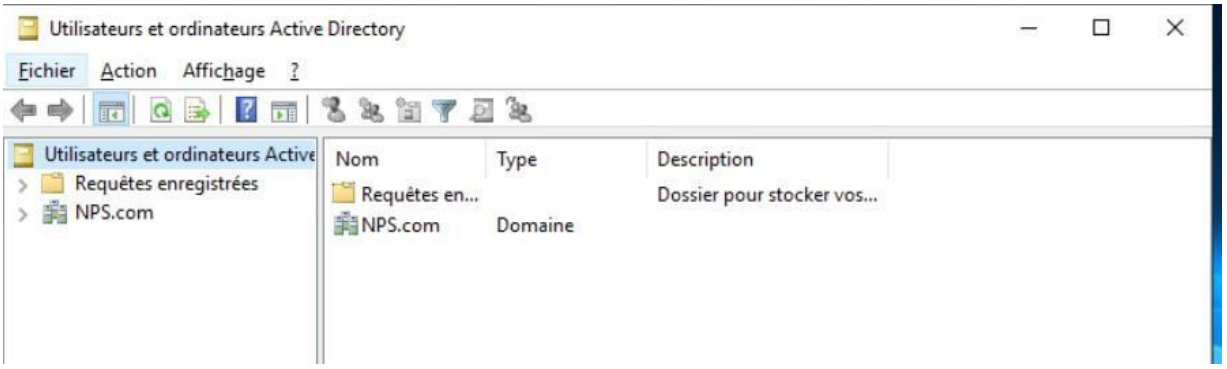
Ensuite vous pouvais exclure du DHCP des ip souhaité cela ne nous intéresse pas alors nous faisant « suivant ».

Ensuite nous pouvons définir le bail.

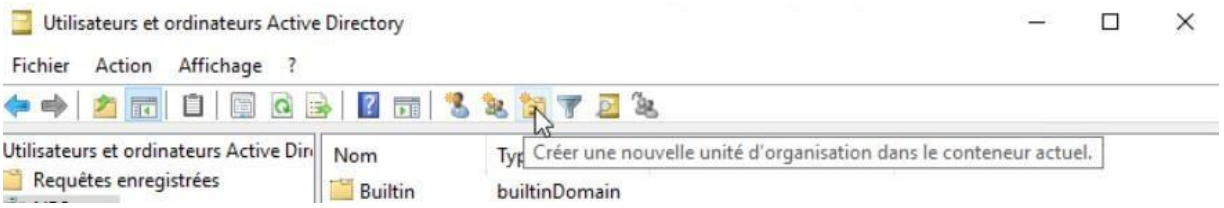


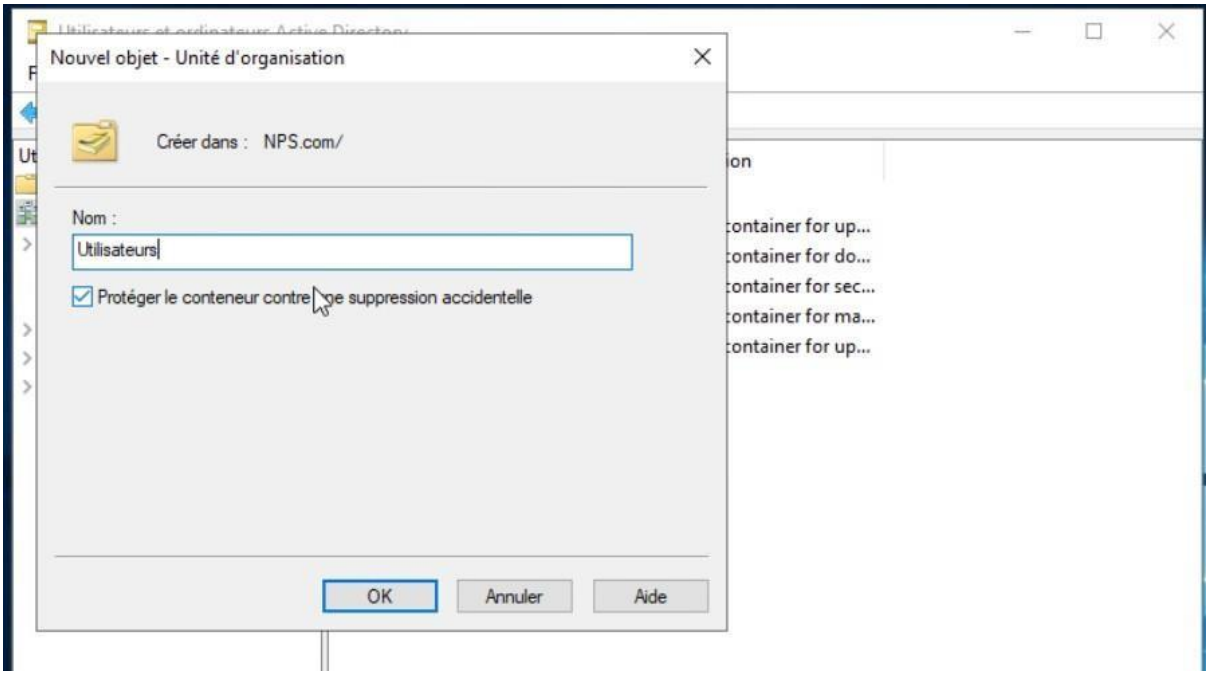
Puis suivant jusqu'à « terminé ».

Passons à la configuration d'utilisateur et de groupe :
Tout d'abord il faudra allez dans la gestionnaire d'utilisateur active directory.

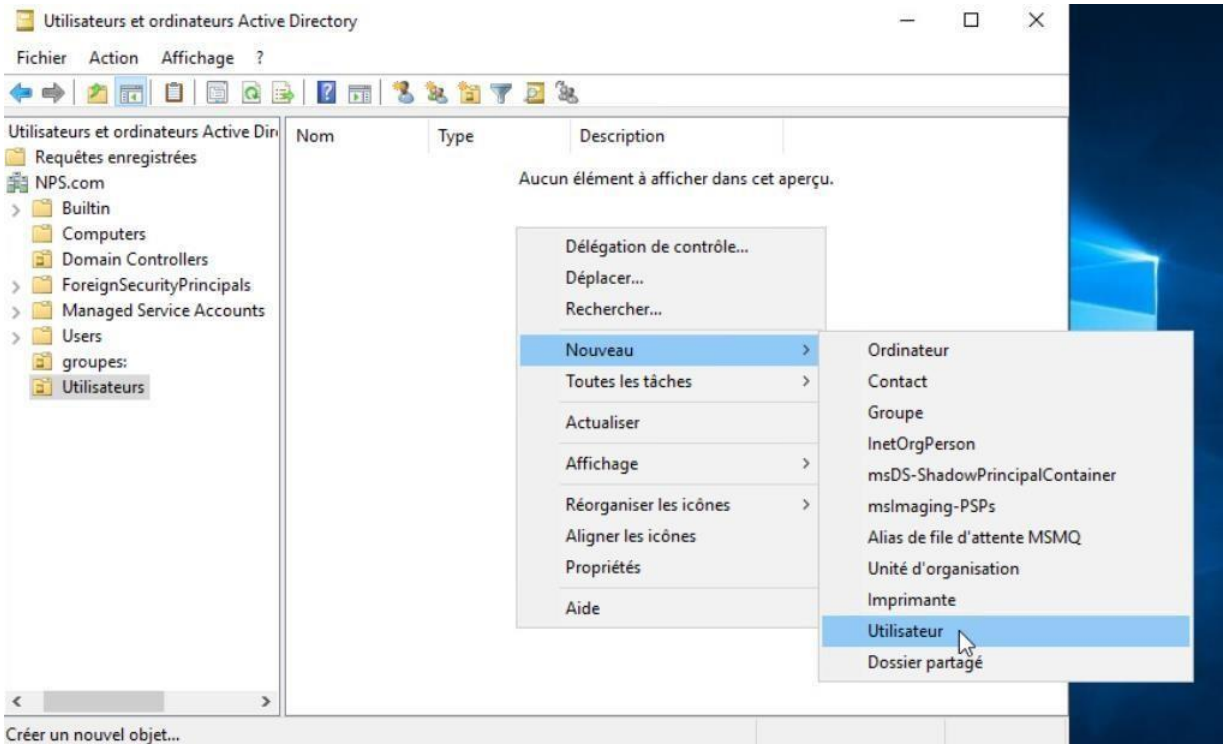


Ce rendre dans le domaine qui nous intéresse et créer un dossier pour nos utilisateurs et un autres pour nos groupes.

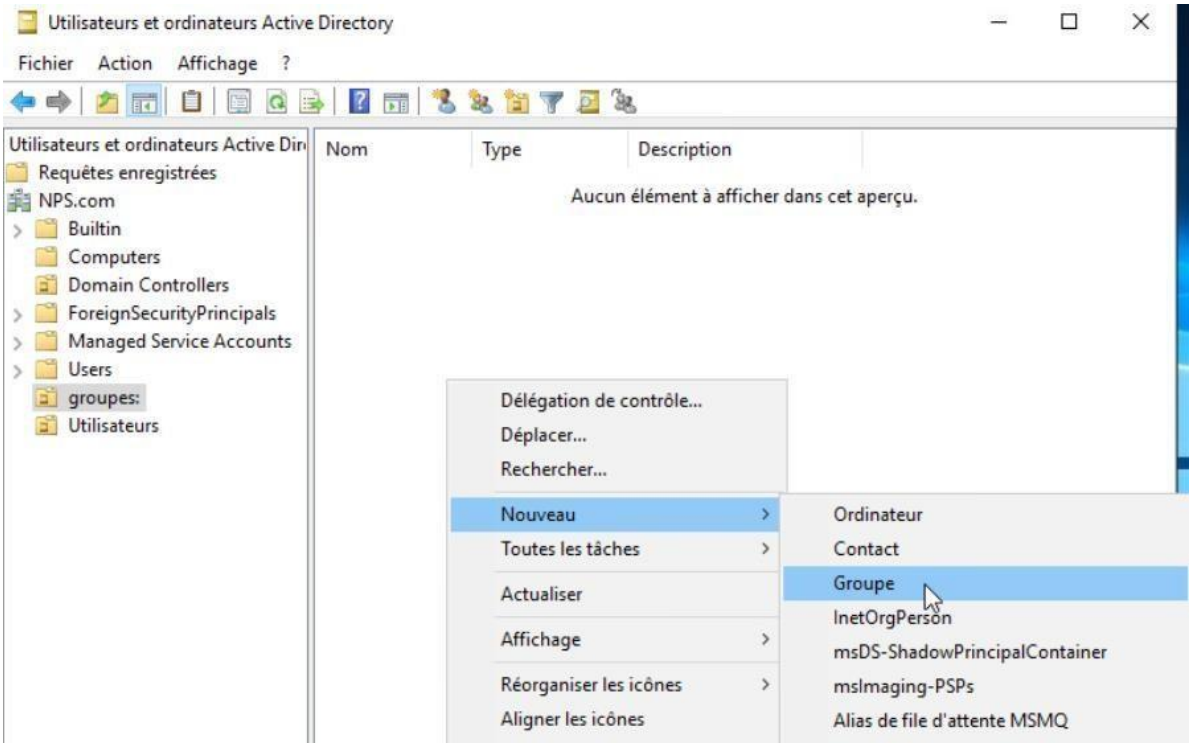


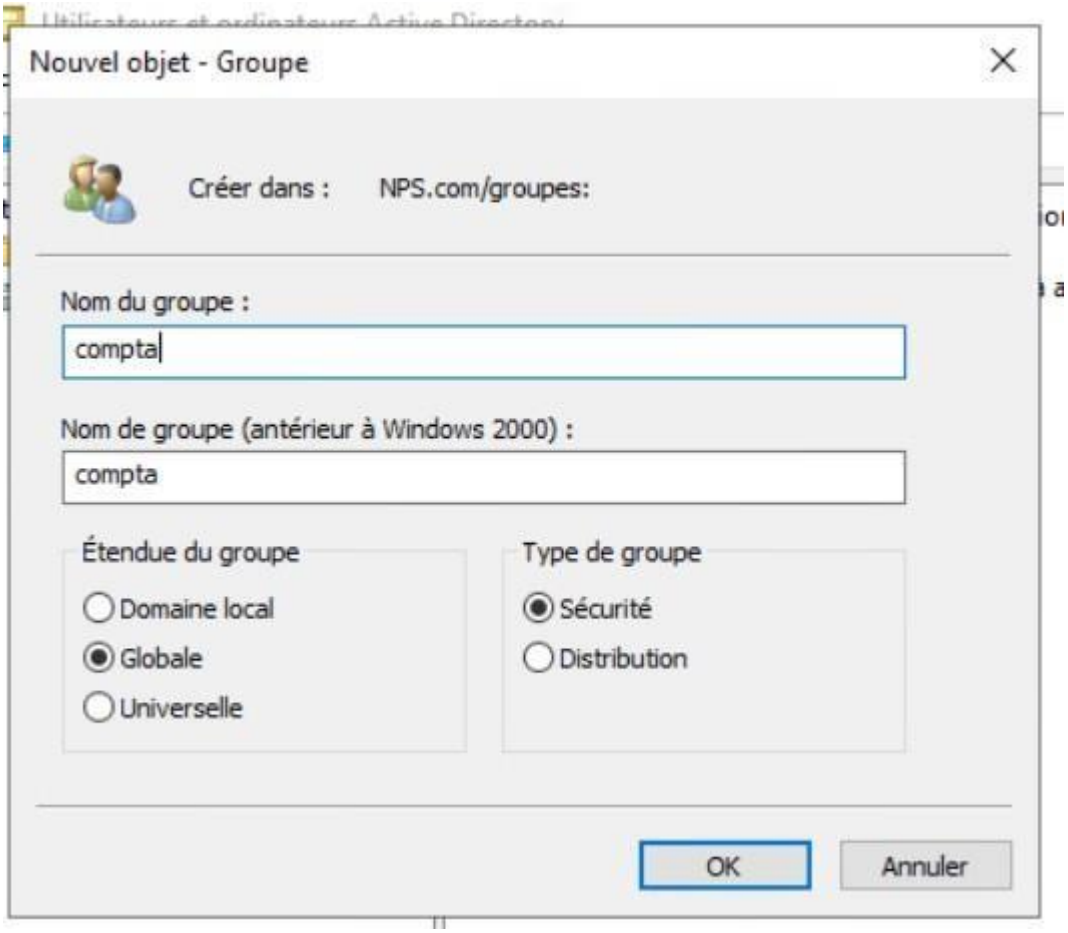


Dans ces dossiers nous allons créer un user et un groupe afin de donné un exemple.

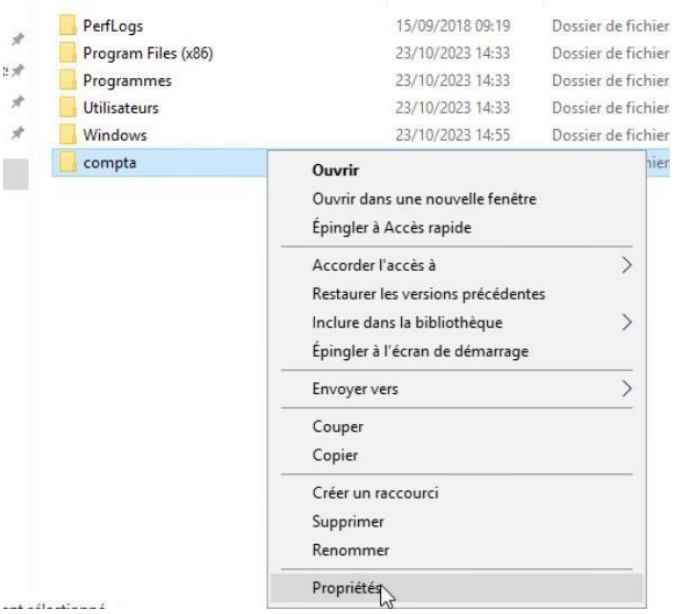


L'user s'appellera « comptabilité01 » et aura comme identifiant « compta01 ». Cet user sera dans le groupe compta qui permettra d'avoir accès au dossier partagé uniquement au membre de la compta.

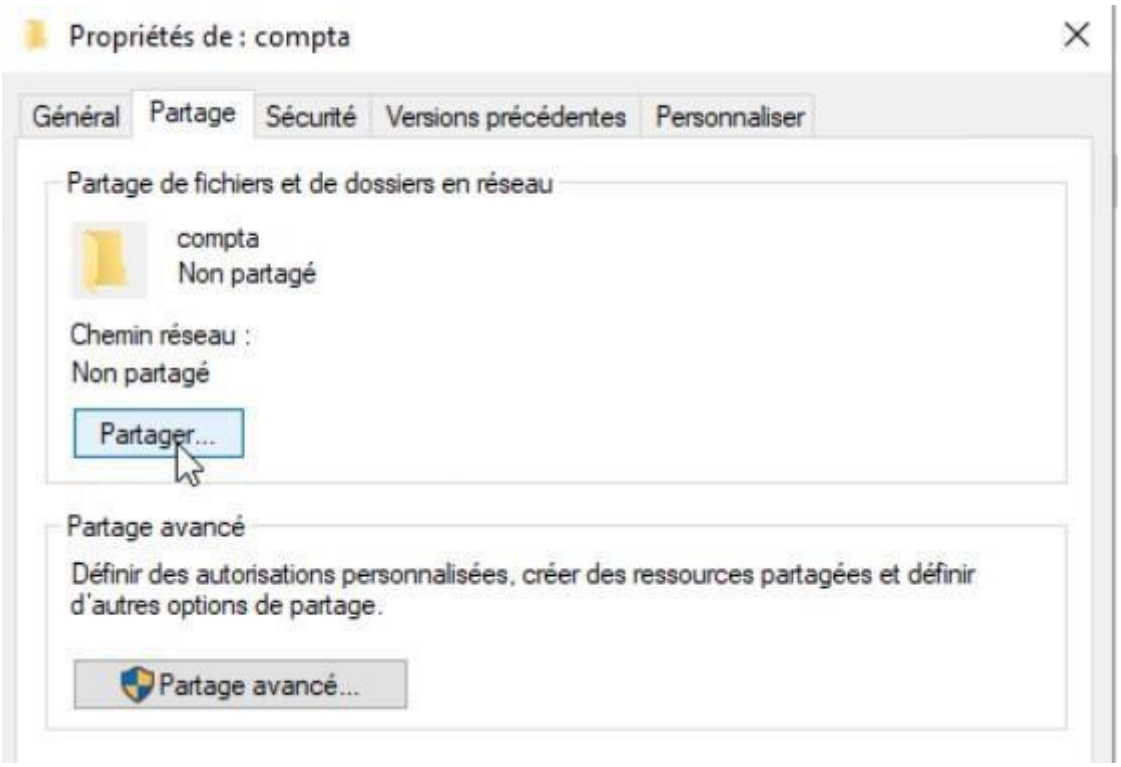




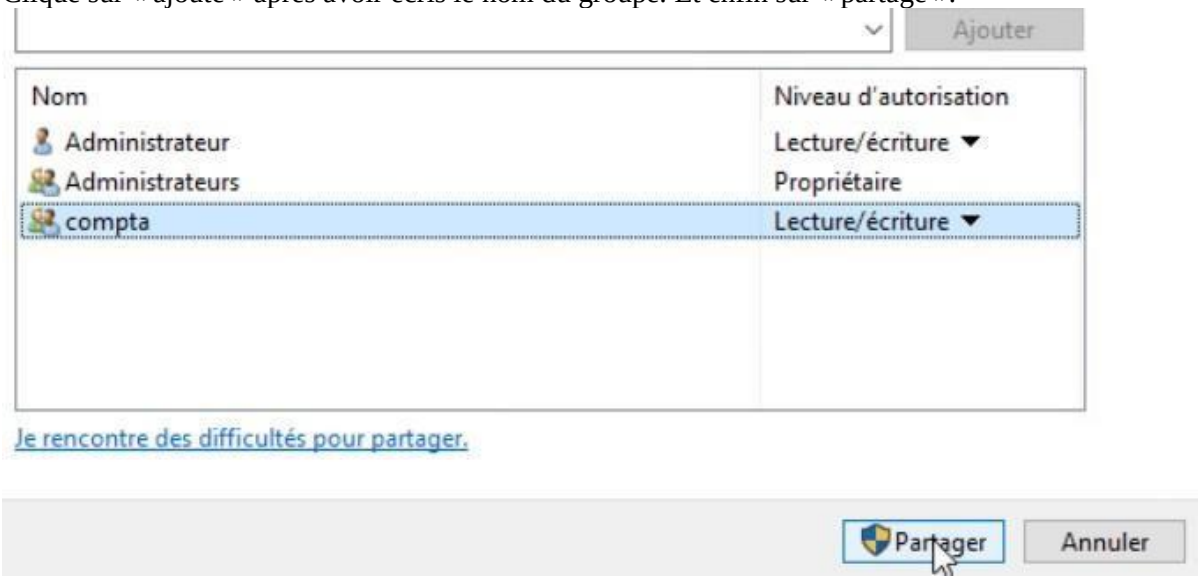
Pour le partage du dossier il suffit de se rendre dans l'onglet partage et donné les droits que l'on souhaite aux membres du groupe.



Cliqué sur « partagé » .



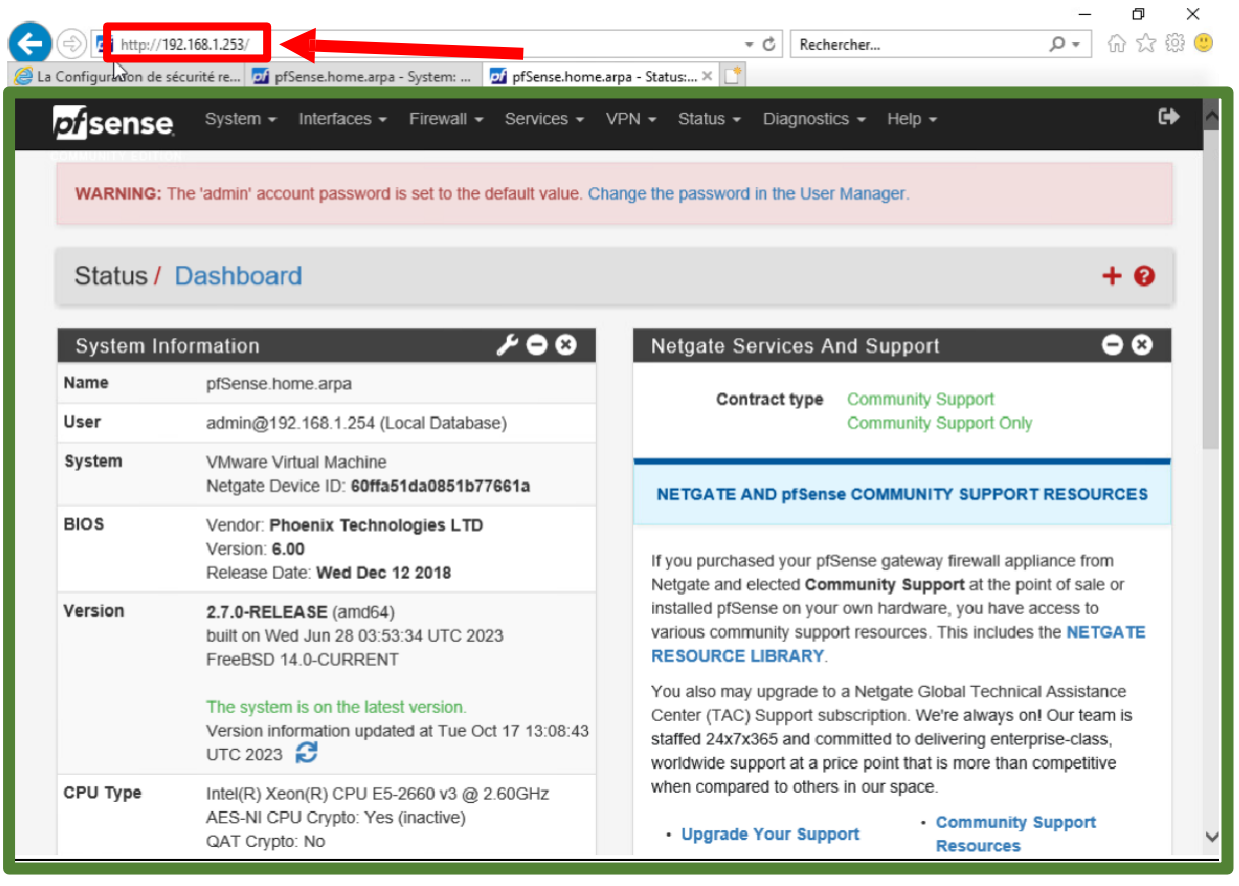
Cliqué sur « ajouté » après avoir écris le nom du groupe. Et enfin sur « partagé ».



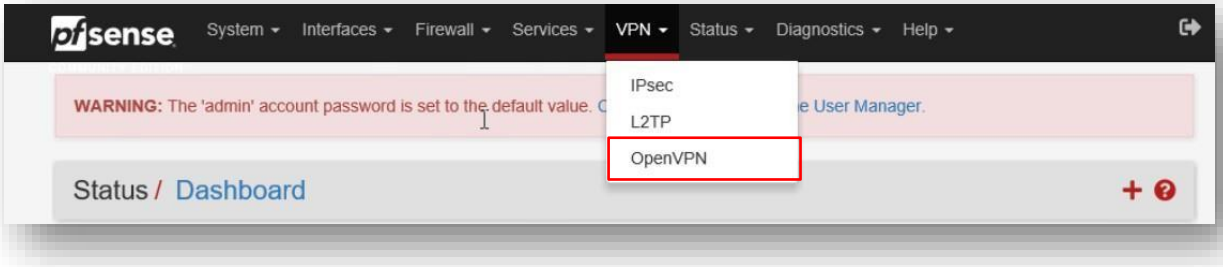
Installation et Setup d'un VPN avec nom d'utilisateur et mot de passe avec pfsense et OpenVPN sur vSphere

Configuration dpfsense :

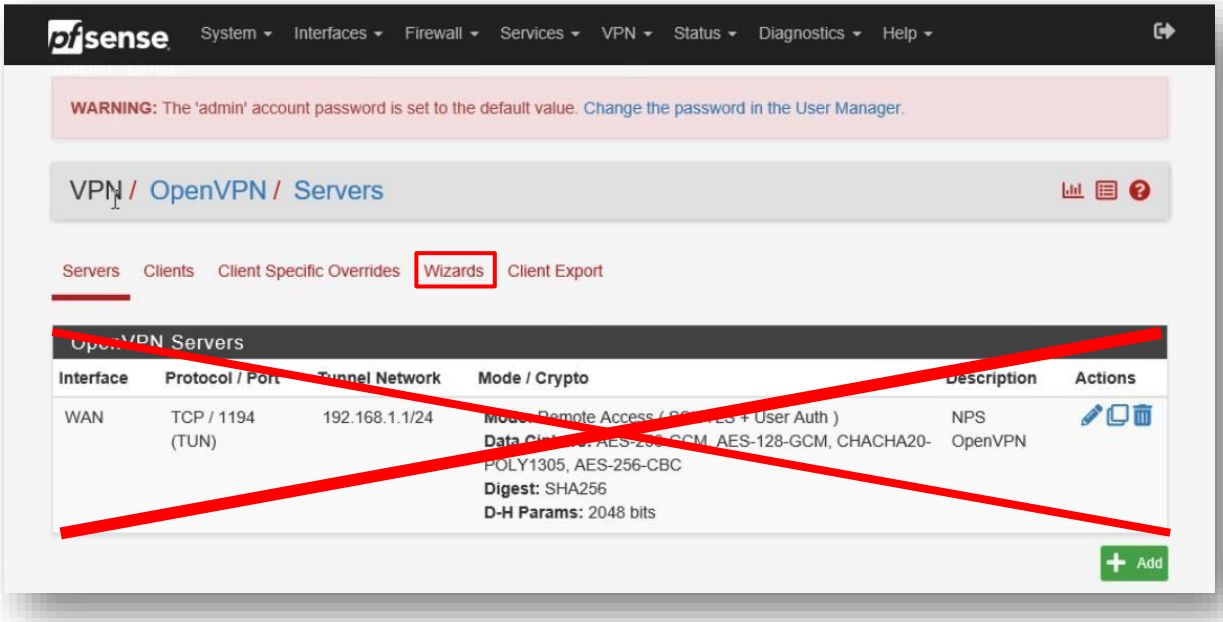
Étape 1 : Taper son adresse réseau en local sur le navigateur Internet de la machine virtuelle, si pfsense est installé on devrait tomber sur cette page ci-dessous encadrée en vert



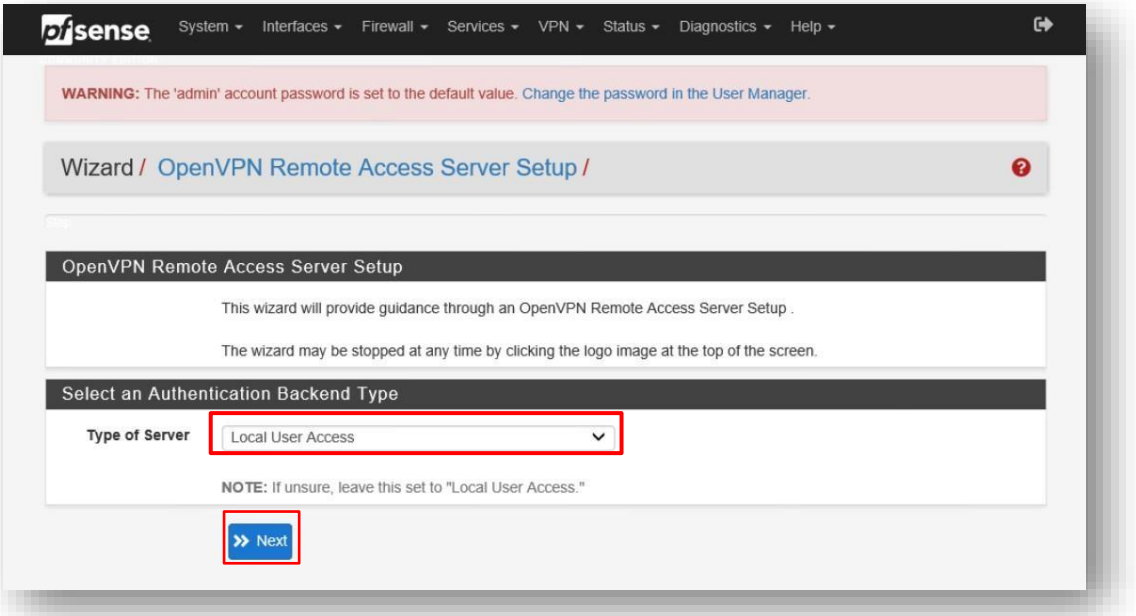
Étape 2 : Cliquer sur VPN puis sur OpenVPN



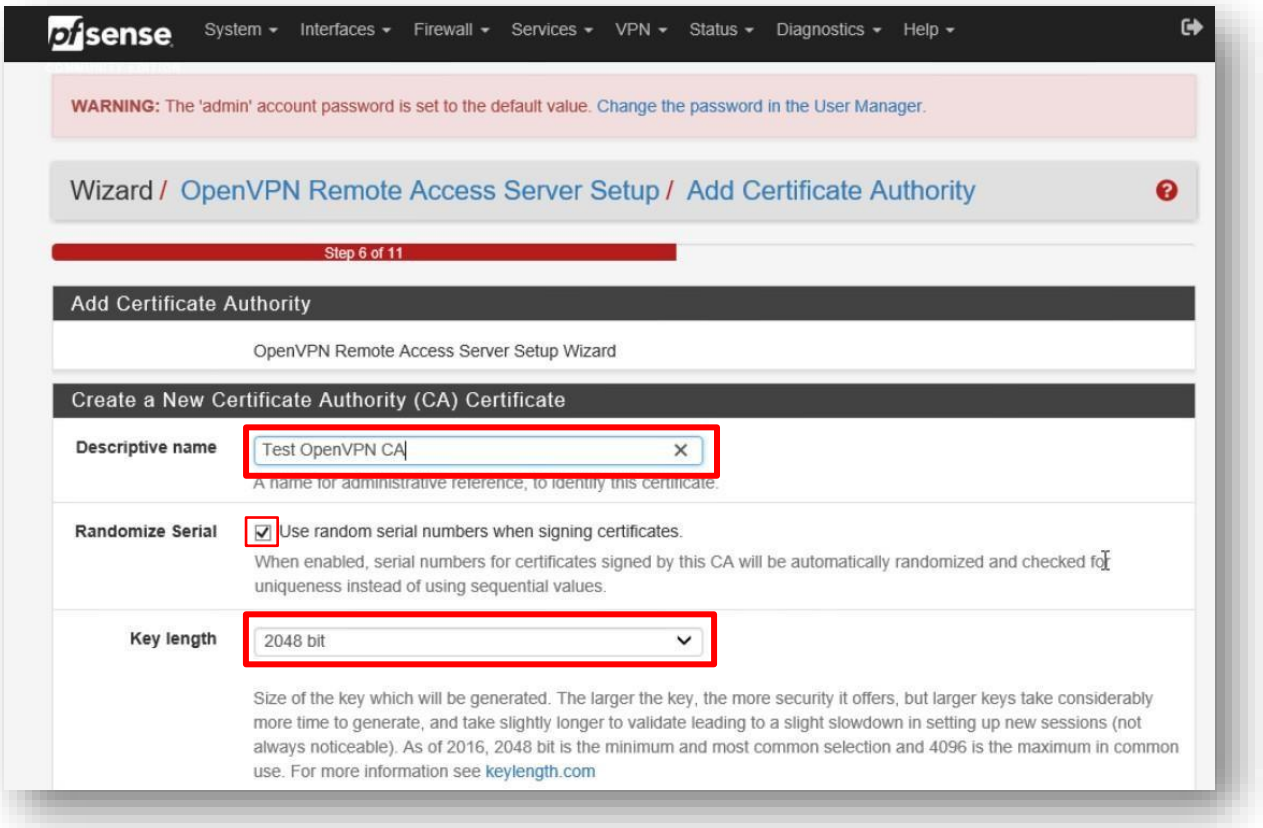
Étape 3 : Une fois sur la page d'OpenVPN, cliquer sur « Wizards » (par défaut aucun server OpenVPN ne devrait exister)



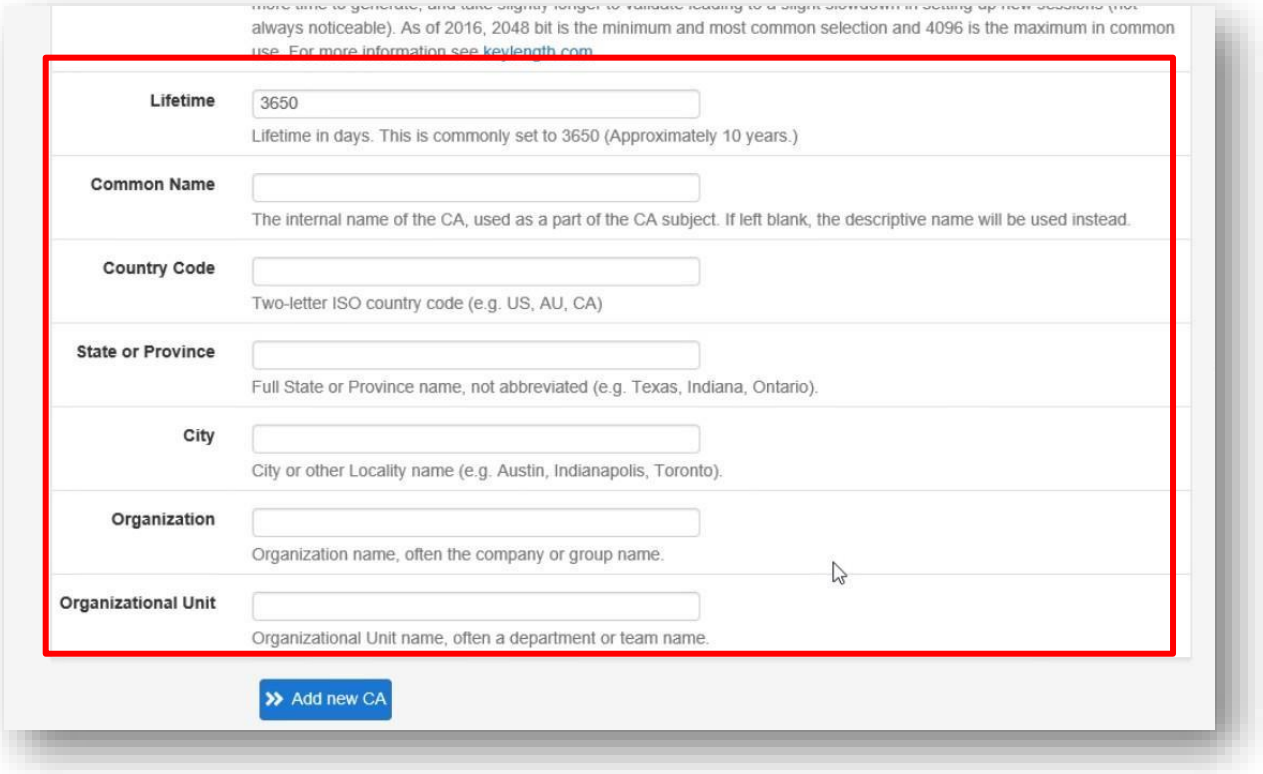
Étape 4 : Sélectionner Local User Access et cliquer sur Next



Étape 5 : Création d'un Certificate Authority

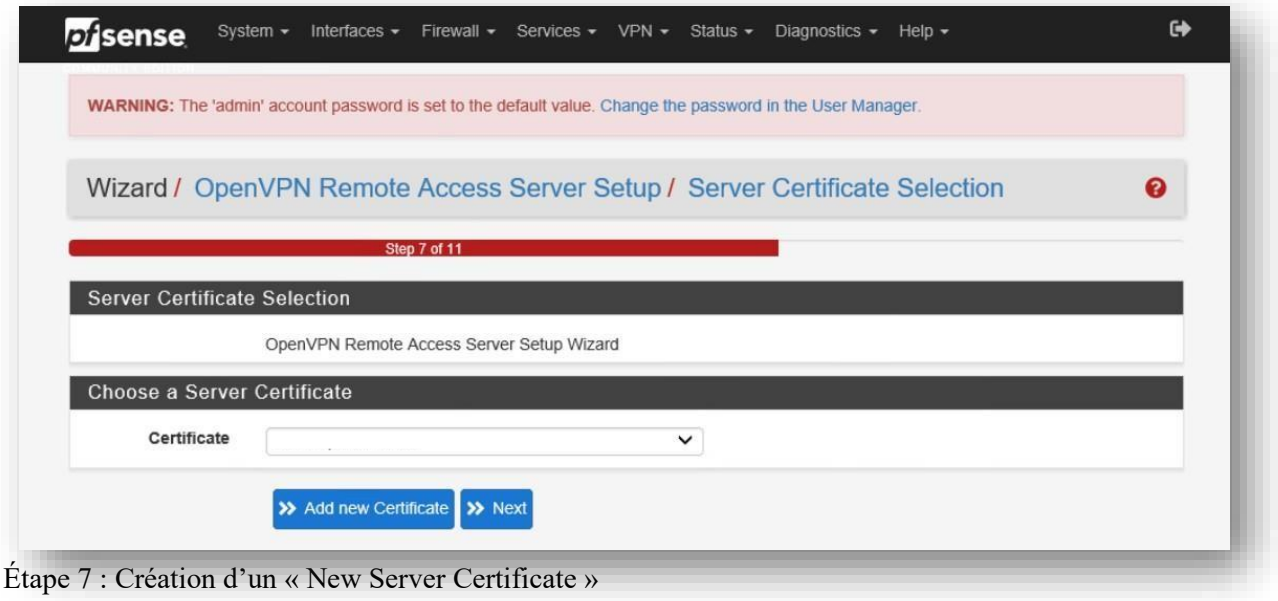


Laisser cocher « Randomize Serial » et sélectionner 2048 bit en « Key length »



Les options ci-dessus sont optionnelles, cliquer sur « Add new CA »

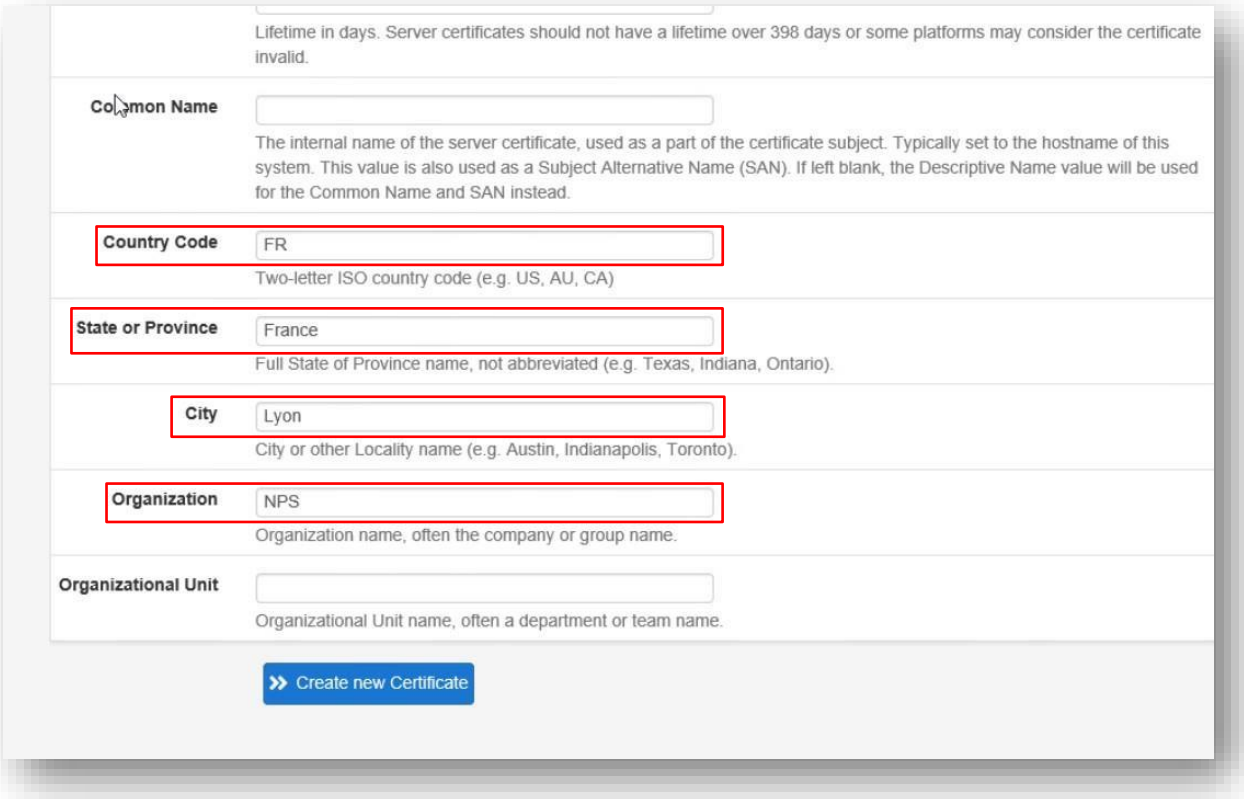
Étape 6 : Cliquer sur « Add new Certificate »



Étape 7 : Création d'un « New Server Certificate »

Donner un nom de référence dans « Descriptive name », laisser 2048 bit et 398 jours

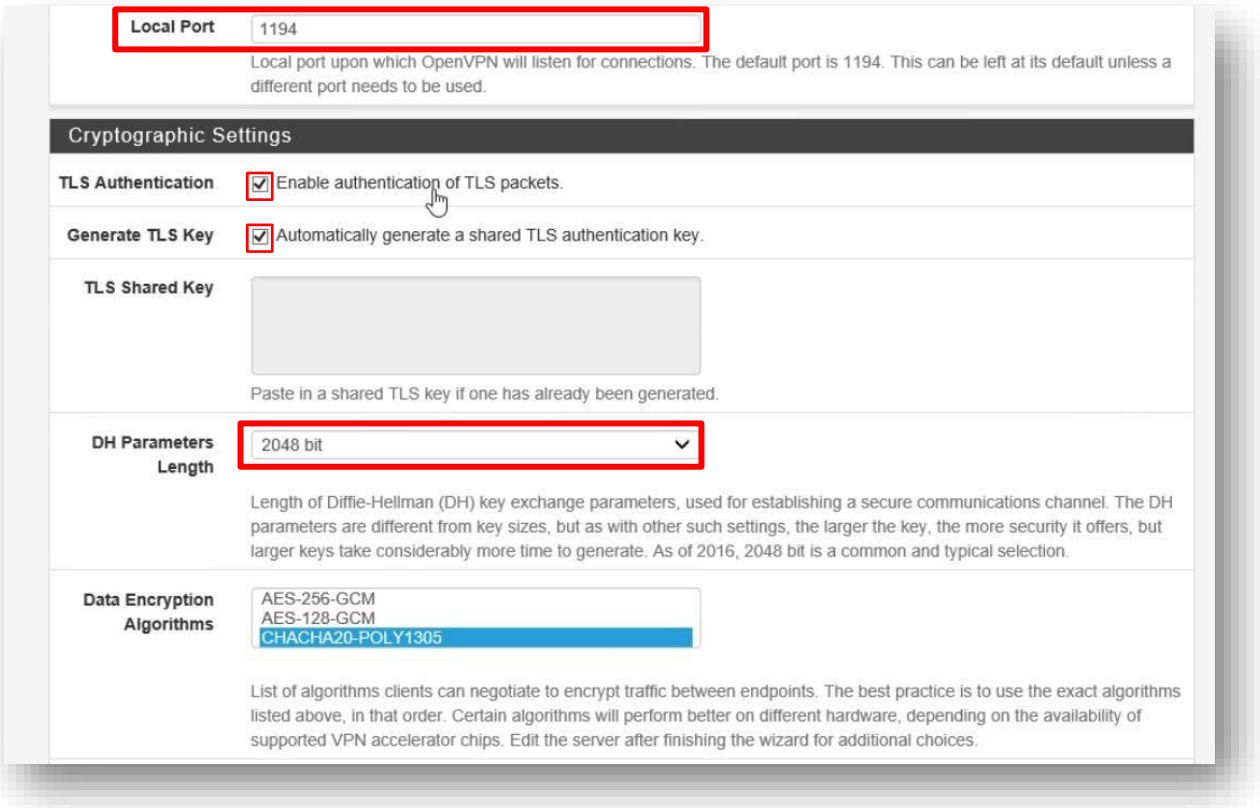
↓Compléter les champs suivants ↓

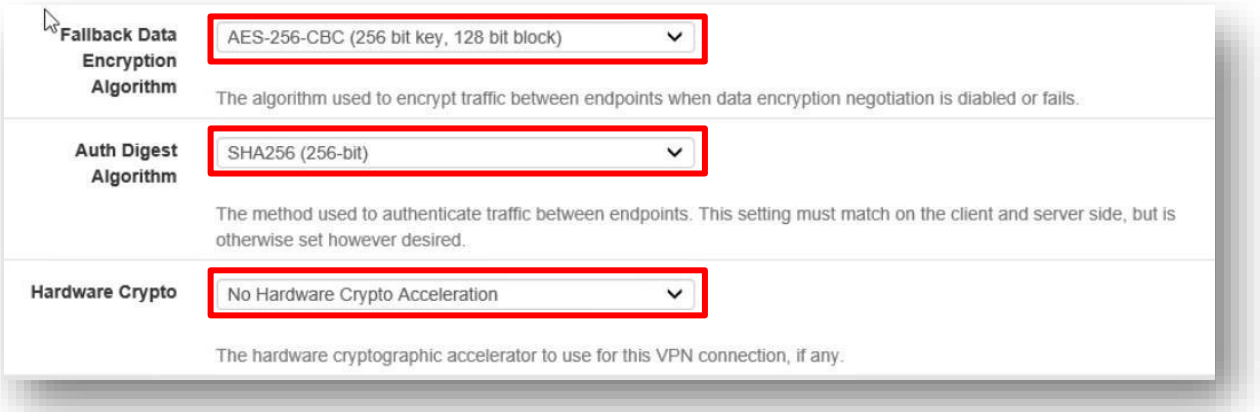


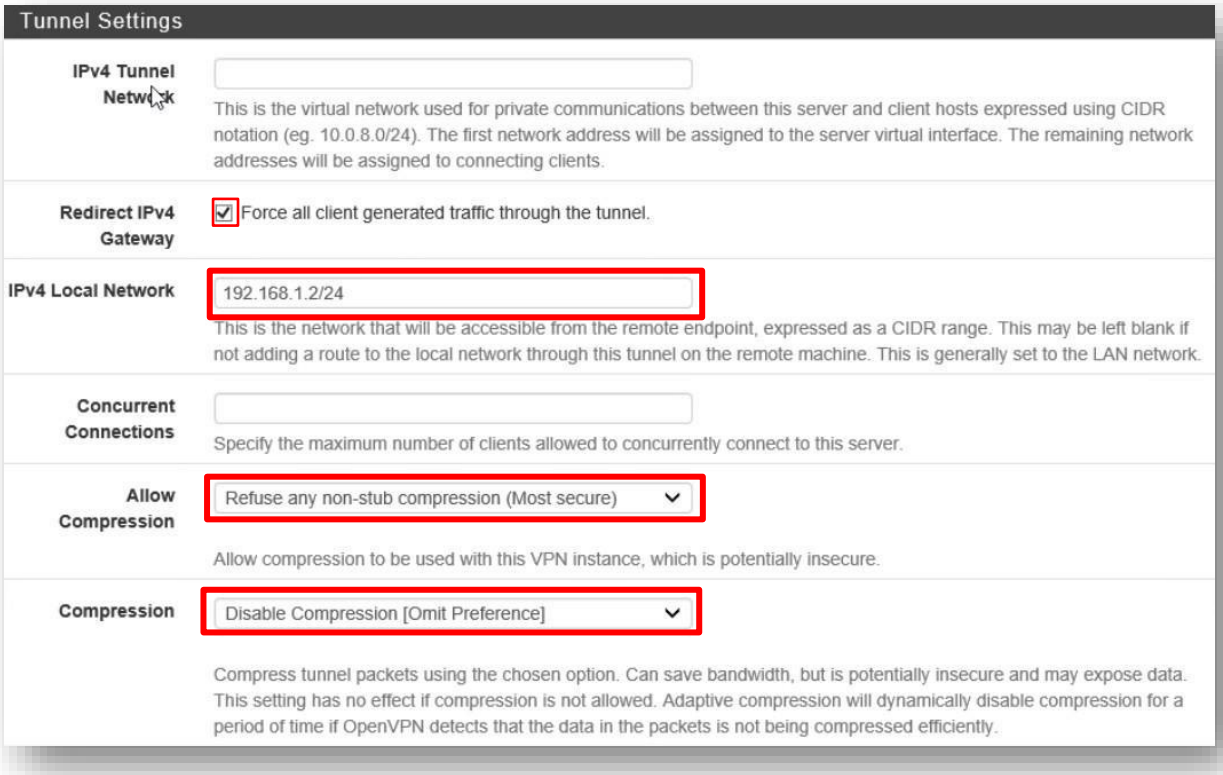
Étape 8 : Setup de l'OpenVPN

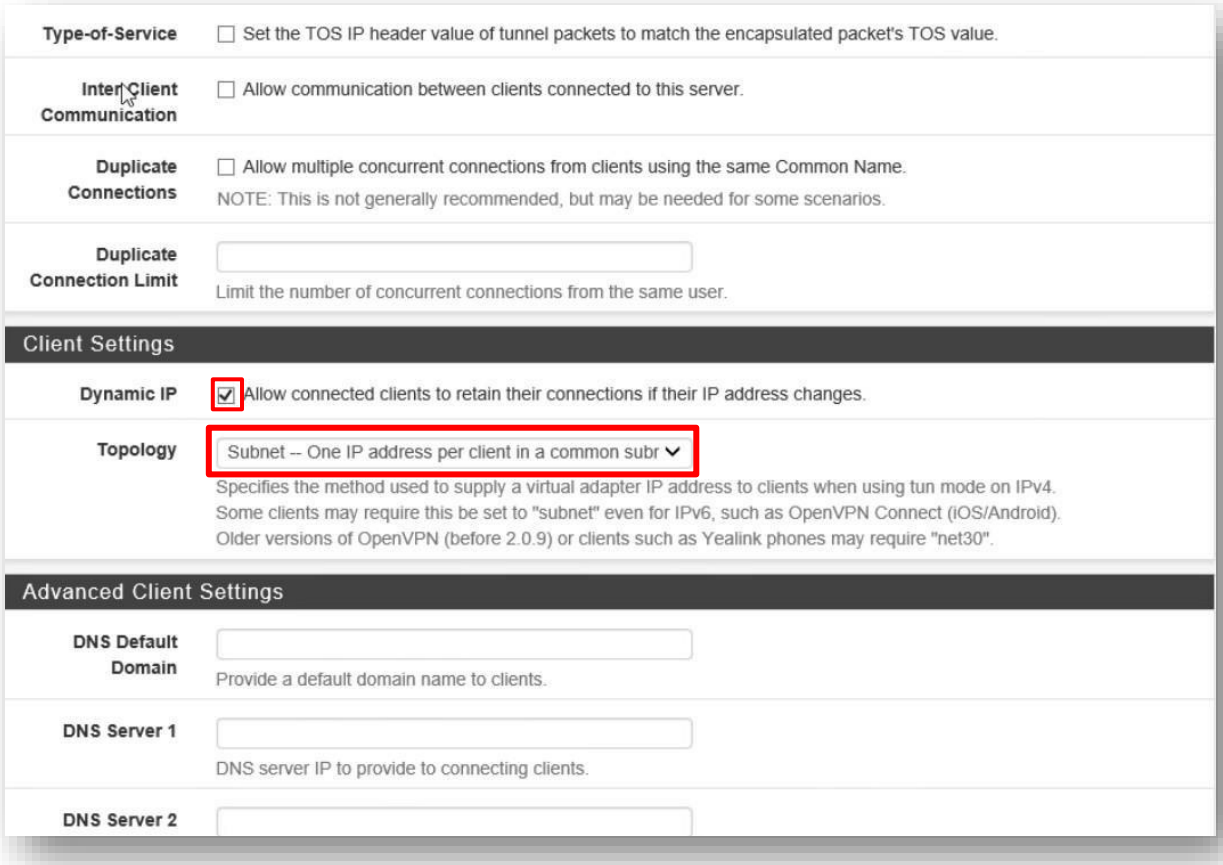
↑ Compléter les champs ci-dessus avec le Protocol sélectionné et l'interface WAN ↑

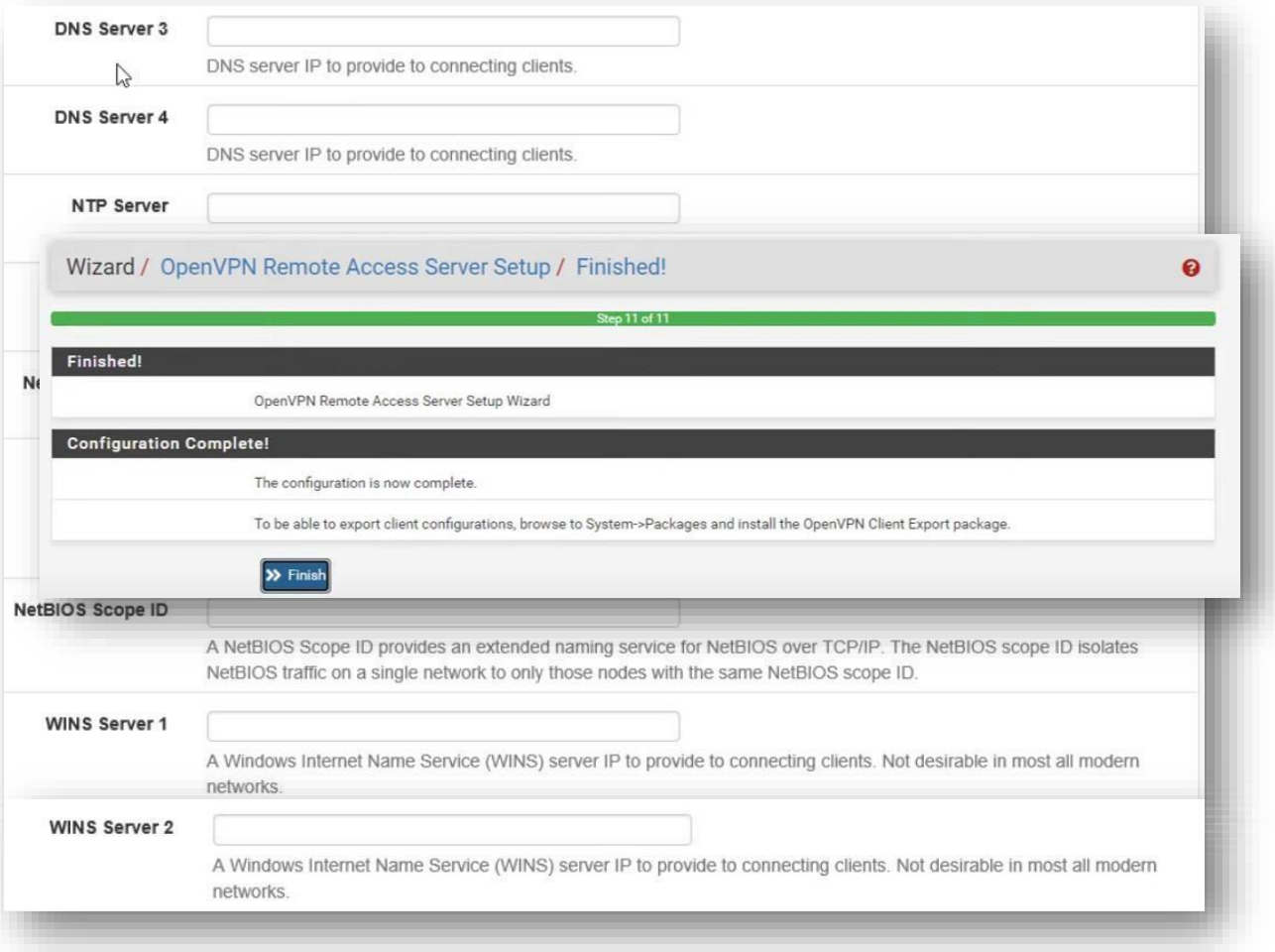
↓ Suivre les instructions avec les captures d'écran ci-dessous ↓



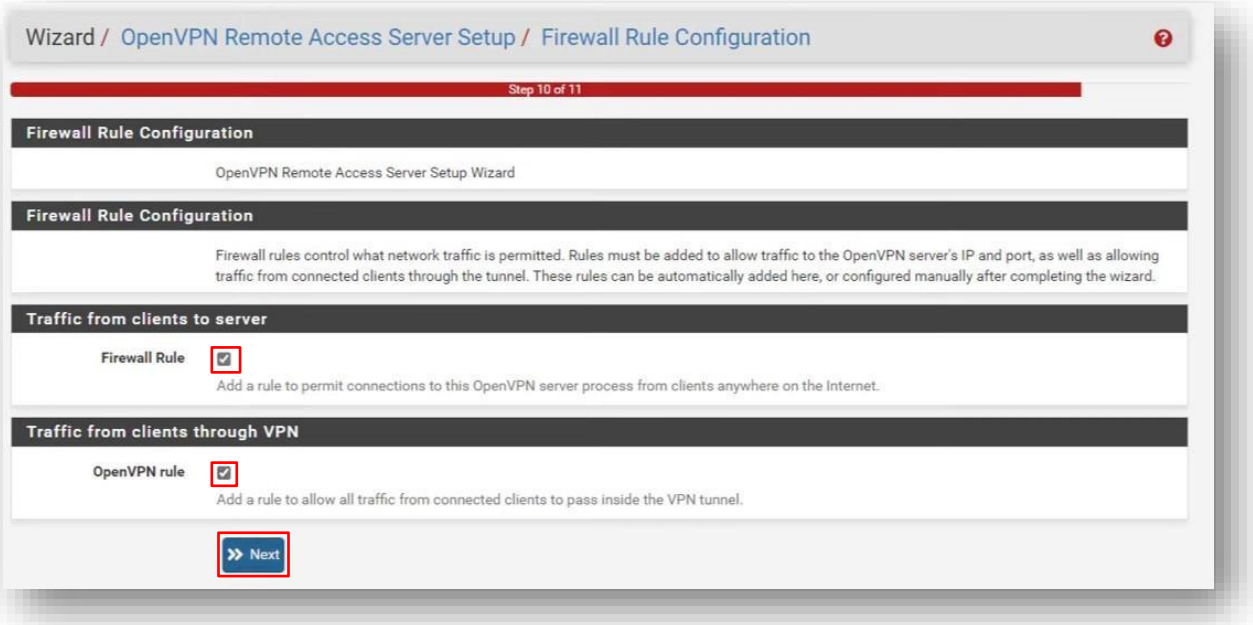



Tunnel Settings
IPv4 Tunnel Network
This is the virtual network used for private communications between this server and client hosts expressed using CIDR notation (eg. 10.0.8.0/24). The first network address will be assigned to the server virtual interface. The remaining network addresses will be assigned to connecting clients.
Redirect IPv4 Gateway
Force all client generated traffic through the tunnel.
IPv4 Local Network
192.168.1.2/24
This is the network that will be accessible from the remote endpoint, expressed as a CIDR range. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
Concurrent Connections
Specify the maximum number of clients allowed to concurrently connect to this server.
Allow Compression
Refuse any non-stub compression (Most secure)
Allow compression to be used with this VPN instance, which is potentially insecure.
Compression
Disable Compression [Omit Preference]
Compress tunnel packets using the chosen option. Can save bandwidth, but is potentially insecure and may expose data. This setting has no effect if compression is not allowed. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.


Type-of-Service
Set the TOS IP header value of tunnel packets to match the encapsulated packet's TOS value.
Inter-Client Communication
Allow communication between clients connected to this server.
Duplicate Connections
Allow multiple concurrent connections from clients using the same Common Name.
NOTE: This is not generally recommended, but may be needed for some scenarios.
Duplicate Connection Limit
Limit the number of concurrent connections from the same user.
Client Settings
Dynamic IP
Allow connected clients to retain their connections if their IP address changes.
Topology
Subnet -- One IP address per client in a common subr
Specifies the method used to supply a virtual adapter IP address to clients when using tun mode on IPv4.
Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android).
Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".
Advanced Client Settings
DNS Default Domain
Provide a default domain name to clients.
DNS Server 1
DNS server IP to provide to connecting clients.
DNS Server 2

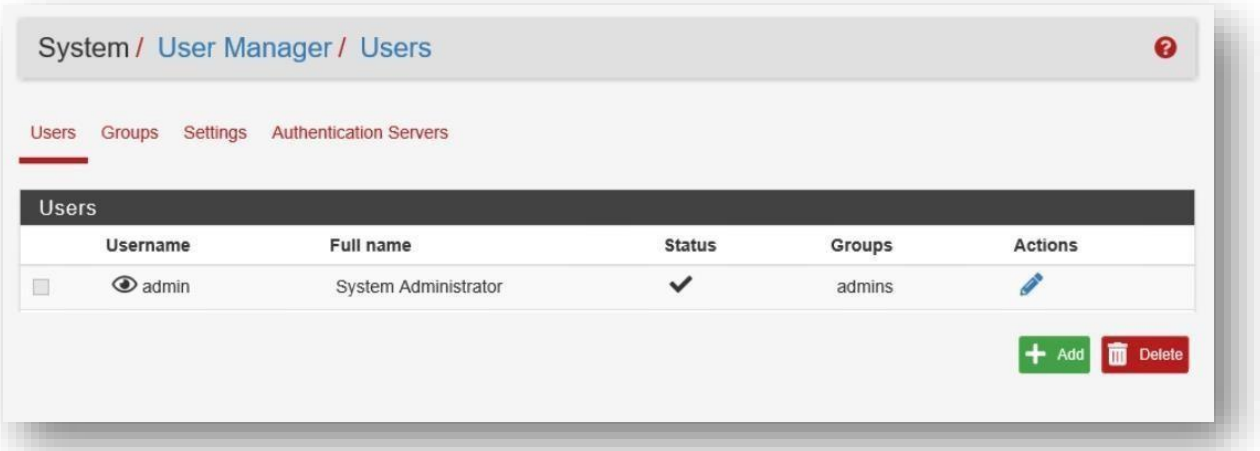


Étape 9 : Configuration du Firewall



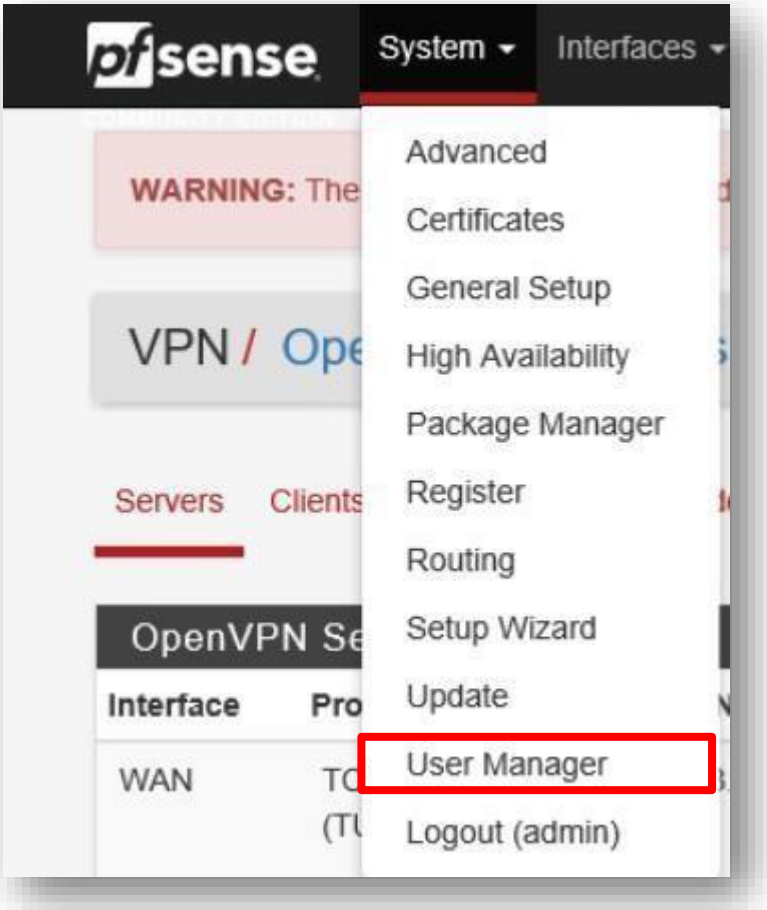
↑ Cocher « OpenVPN rule » et « Firewall rule » puis cliquer sur Next ↑

↓ Une fois le Setup fini on devrait tomber sur cette page, cliquer sur Finish ↓



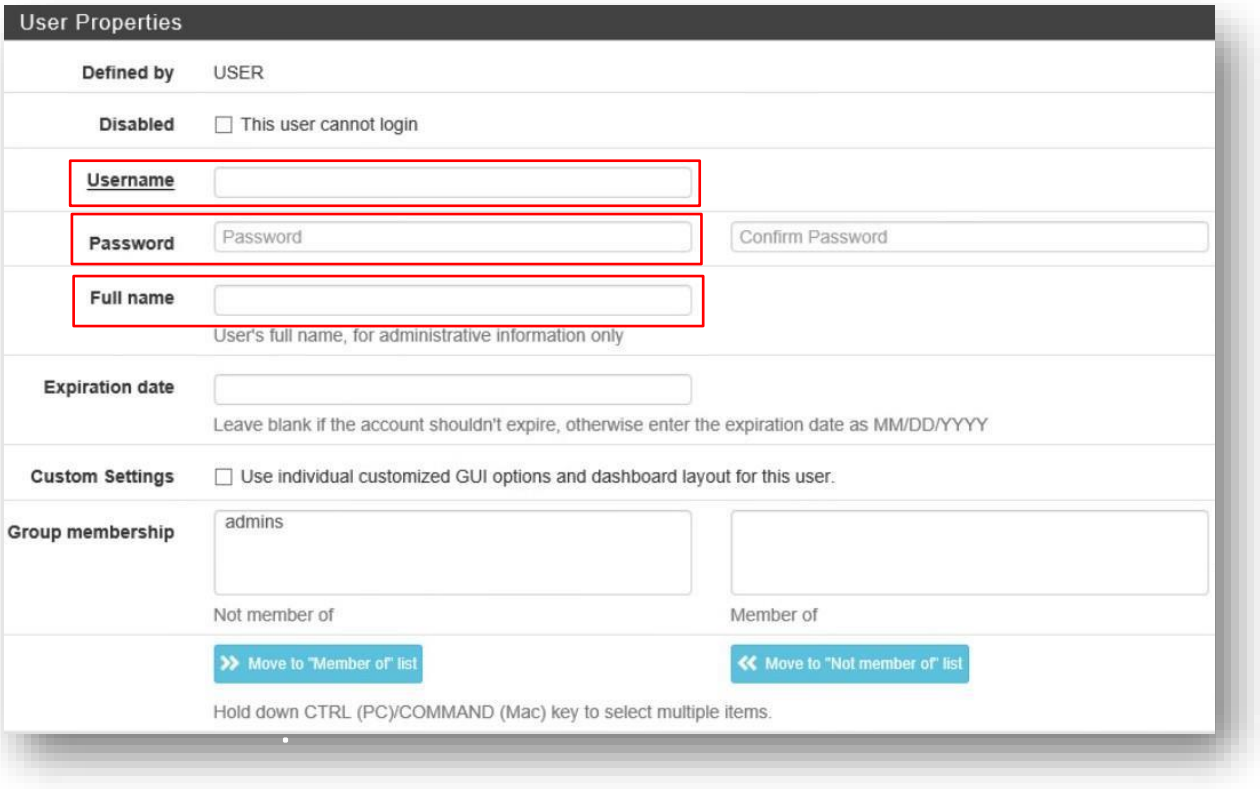
Étape 10 : Configuration de l'utilisateur

↓ Aller dans System puis sur User Manager ↓



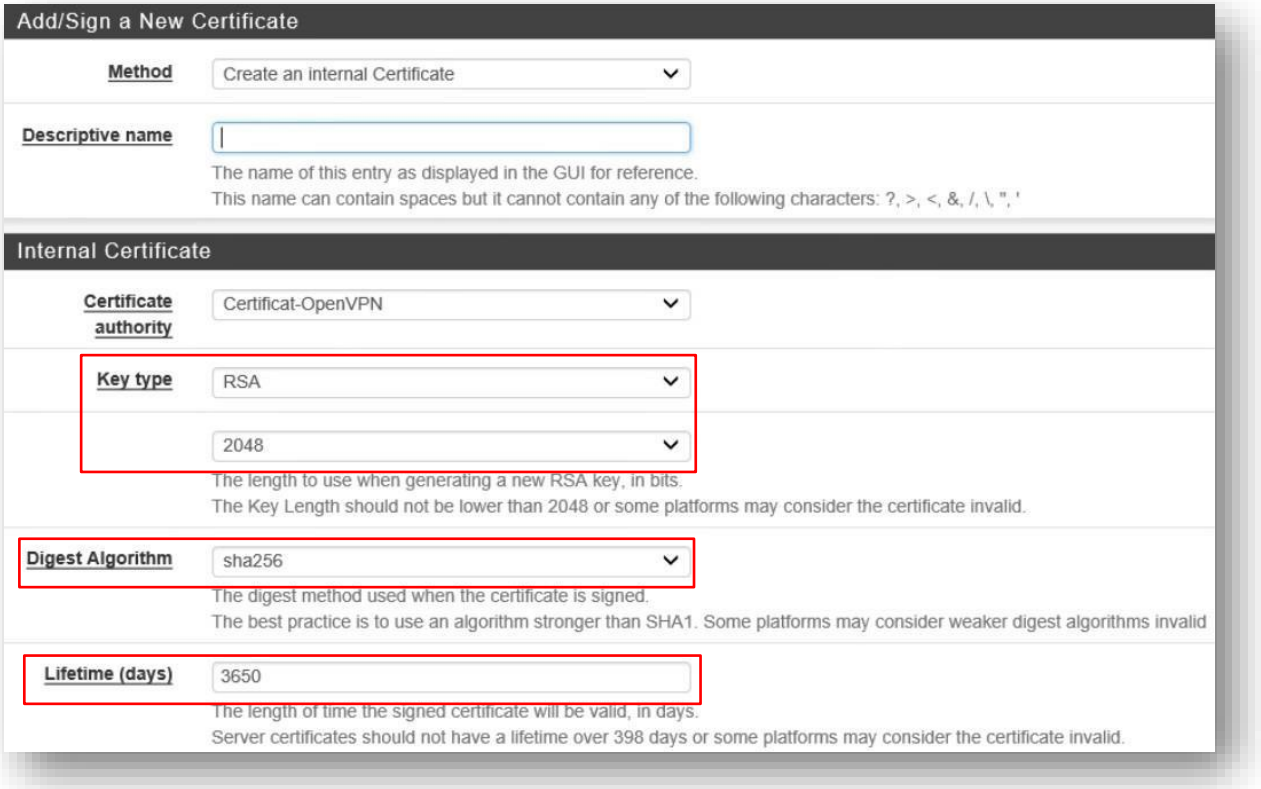
Cliquer sur « Add » pour ajouter un nouvel utilisateur

↓ Compléter les champs ci-dessous encadrés en rouge, on en aura besoin plus tard pour le Login ↓

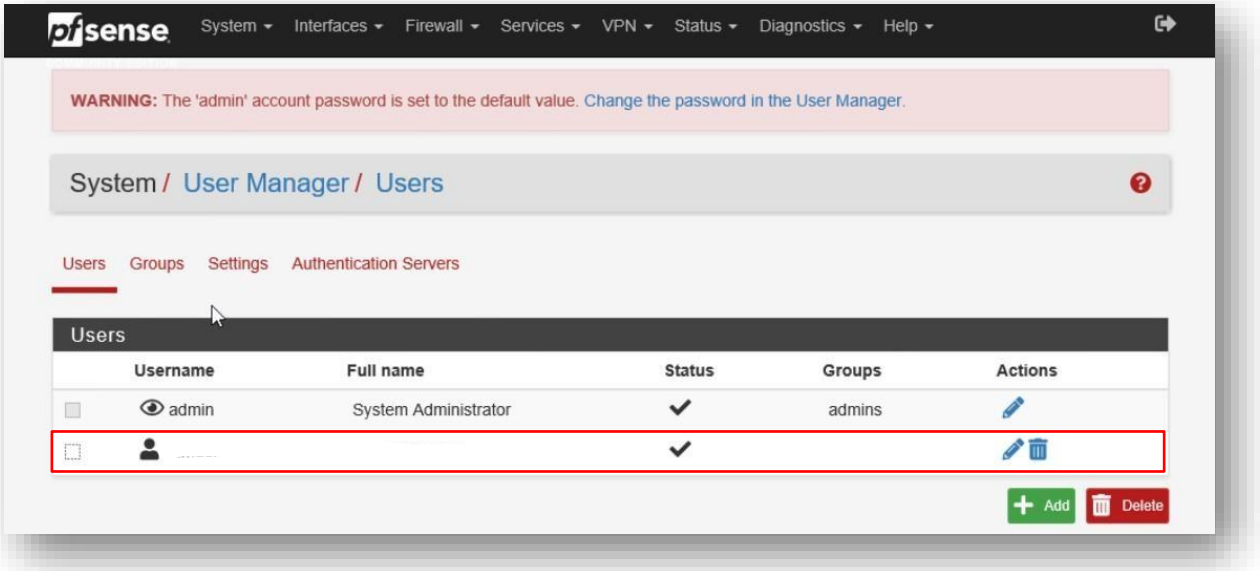


↑ Définir un nom d'utilisateur et un mot de passe puis cliquer sur Save ↑

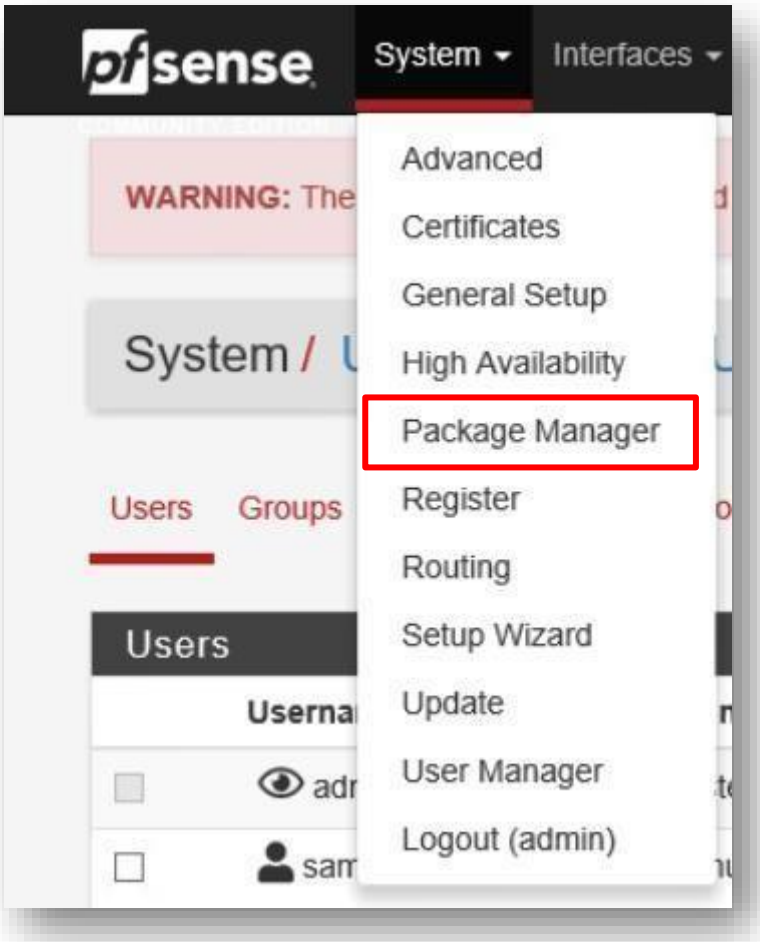
↓ Ajouter un nom de description et sélectionner les options des champs ci-dessous encadrés en rouge puis cliquer sur Save ↓

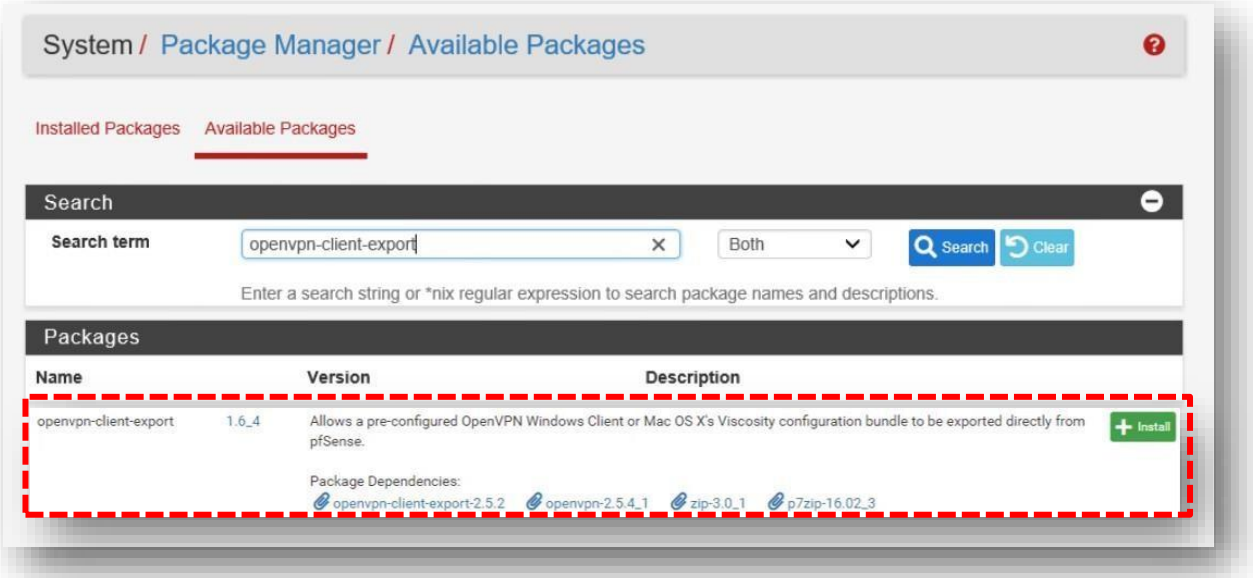


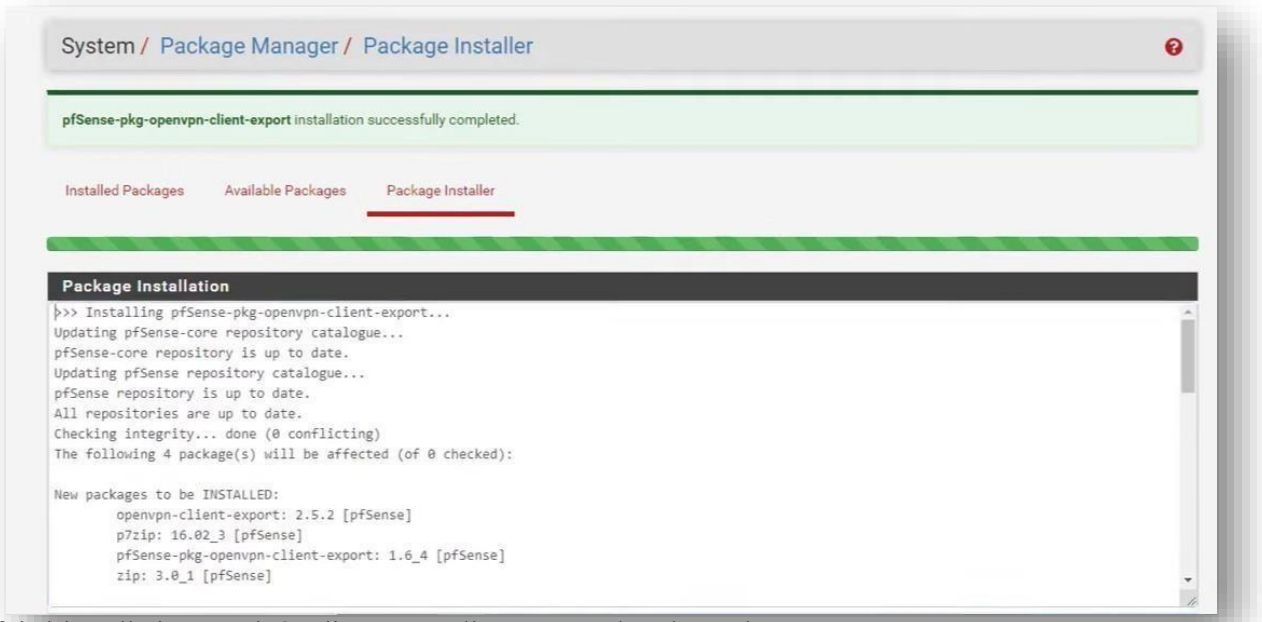
Un nouvel utilisateur doit normalement apparaitre dans les « Users »



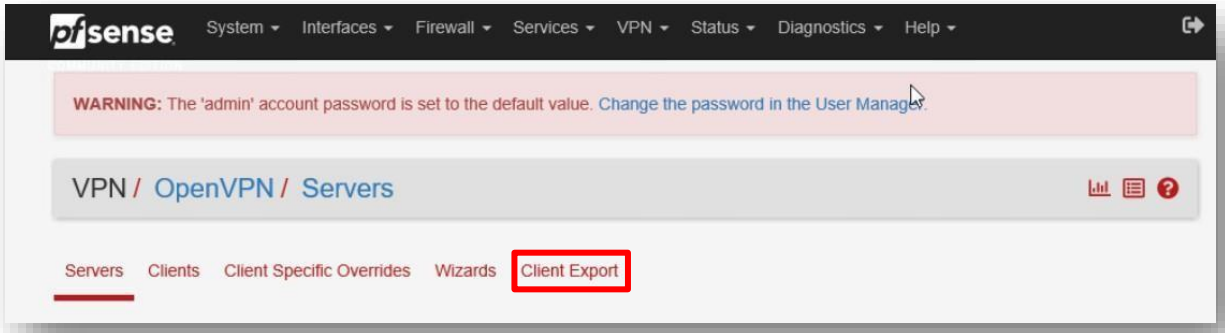
Étape 11 : Installation du package OpenVPN-CLIENT-EXPORT Aller dans System puis cliquer sur Package Manager
Cliquer sur « Available Packages » et installer openvpn-client-export



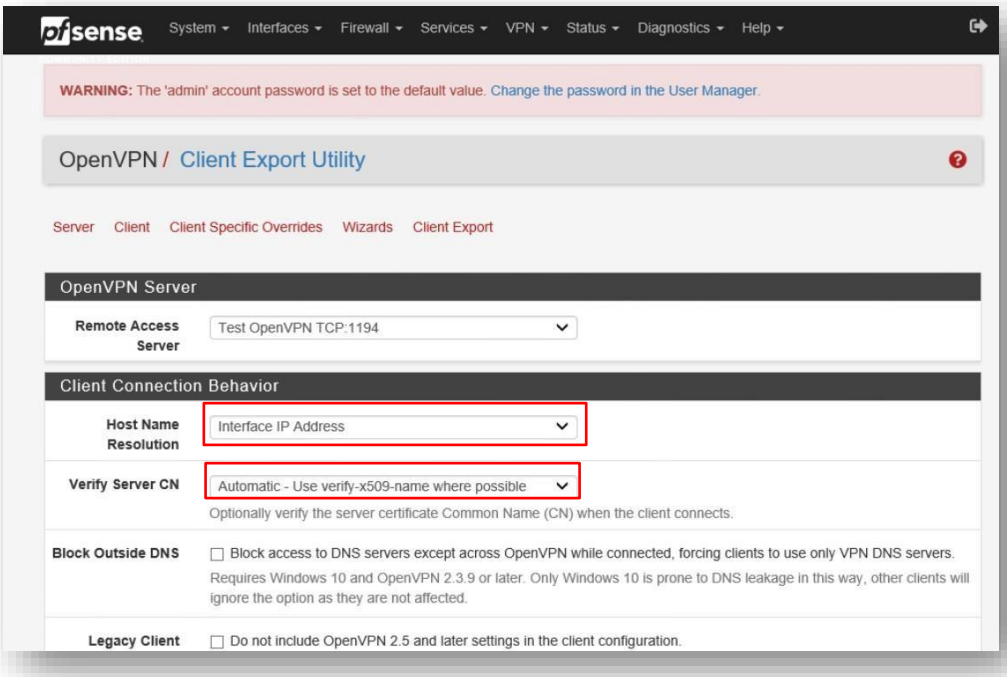


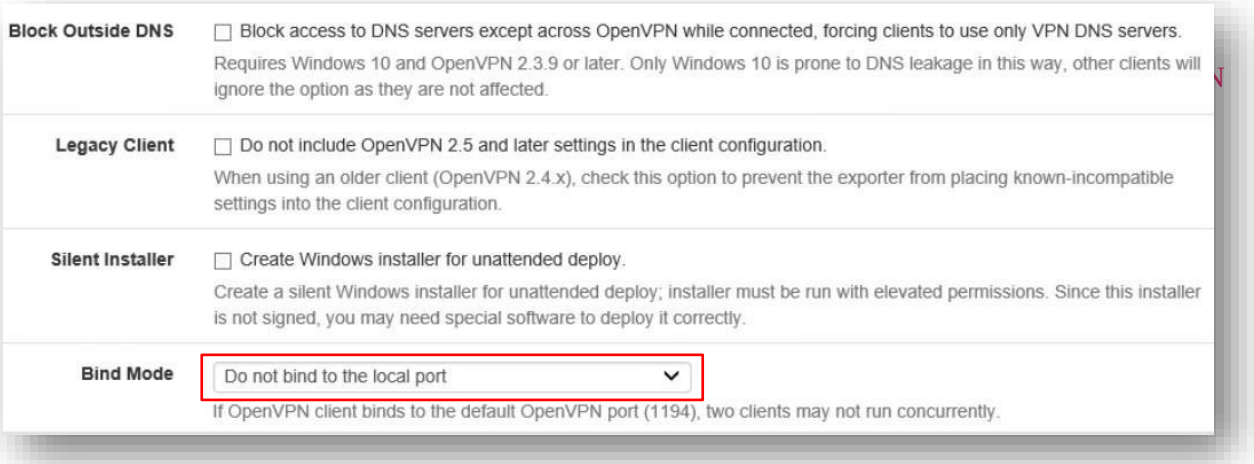


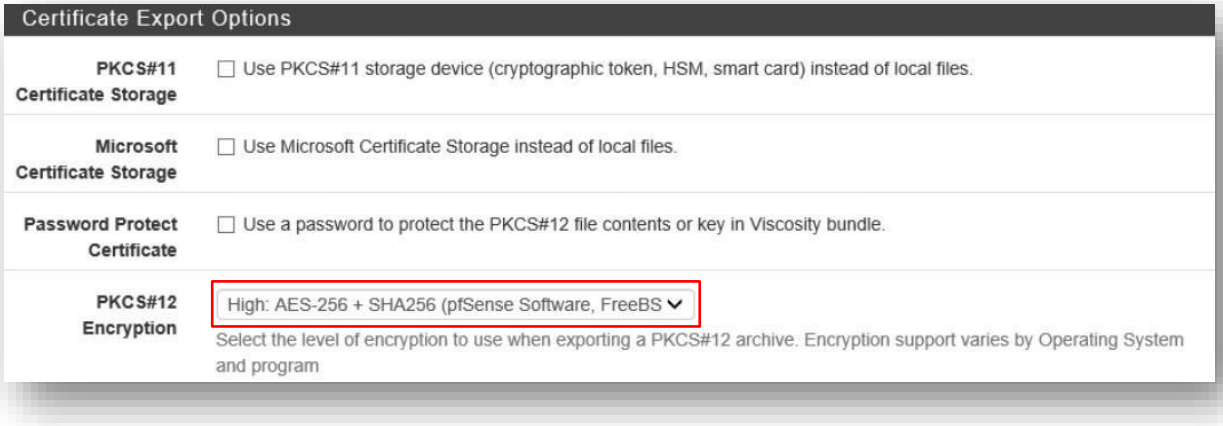
Une fois l'installation terminée cliquer sur Client Export dans la section OpenVPN



Sélectionner les paramètres ci-dessous

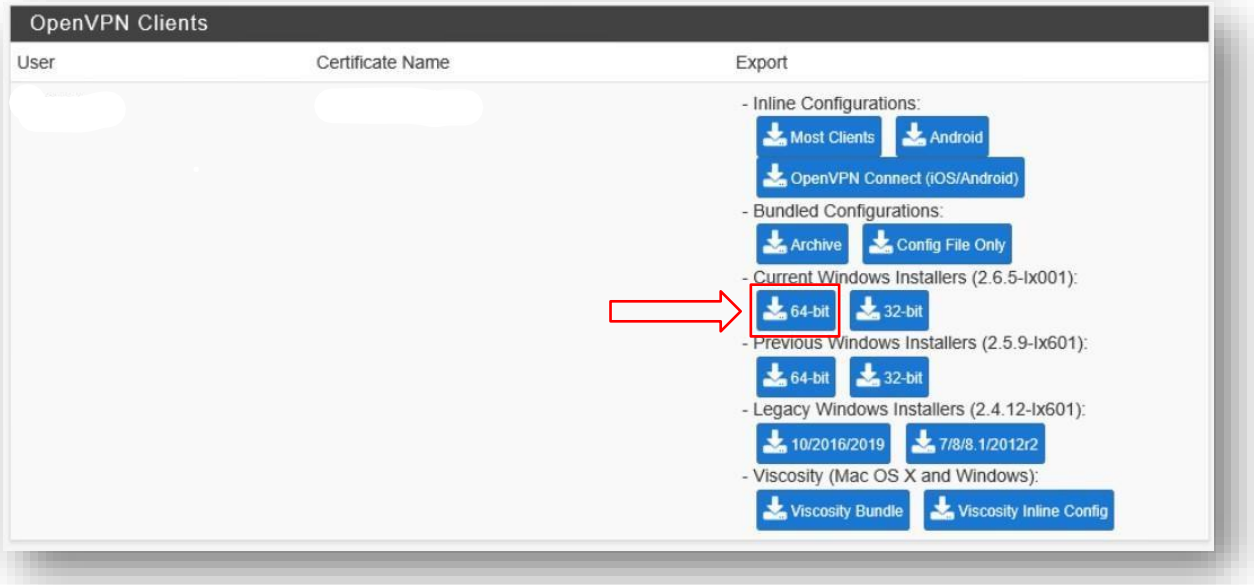




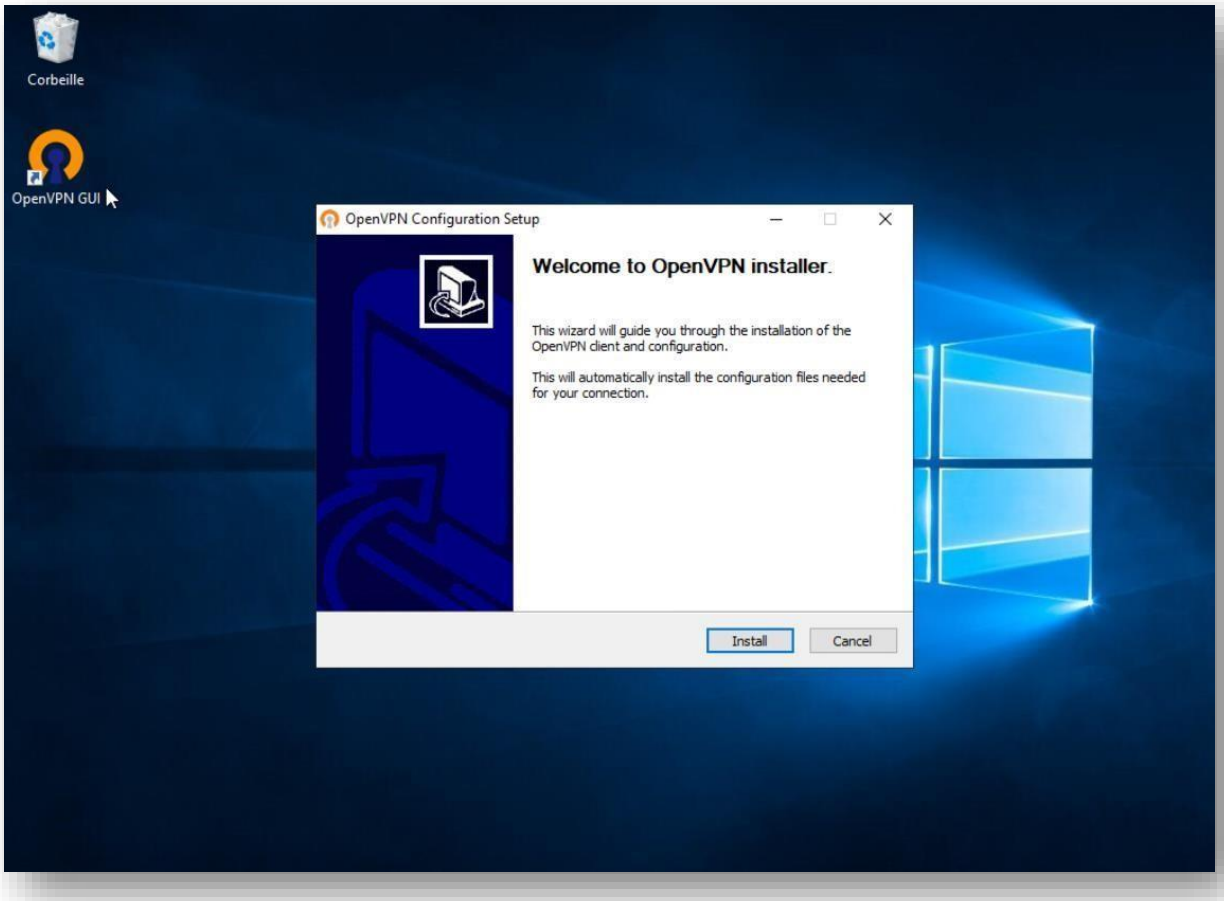


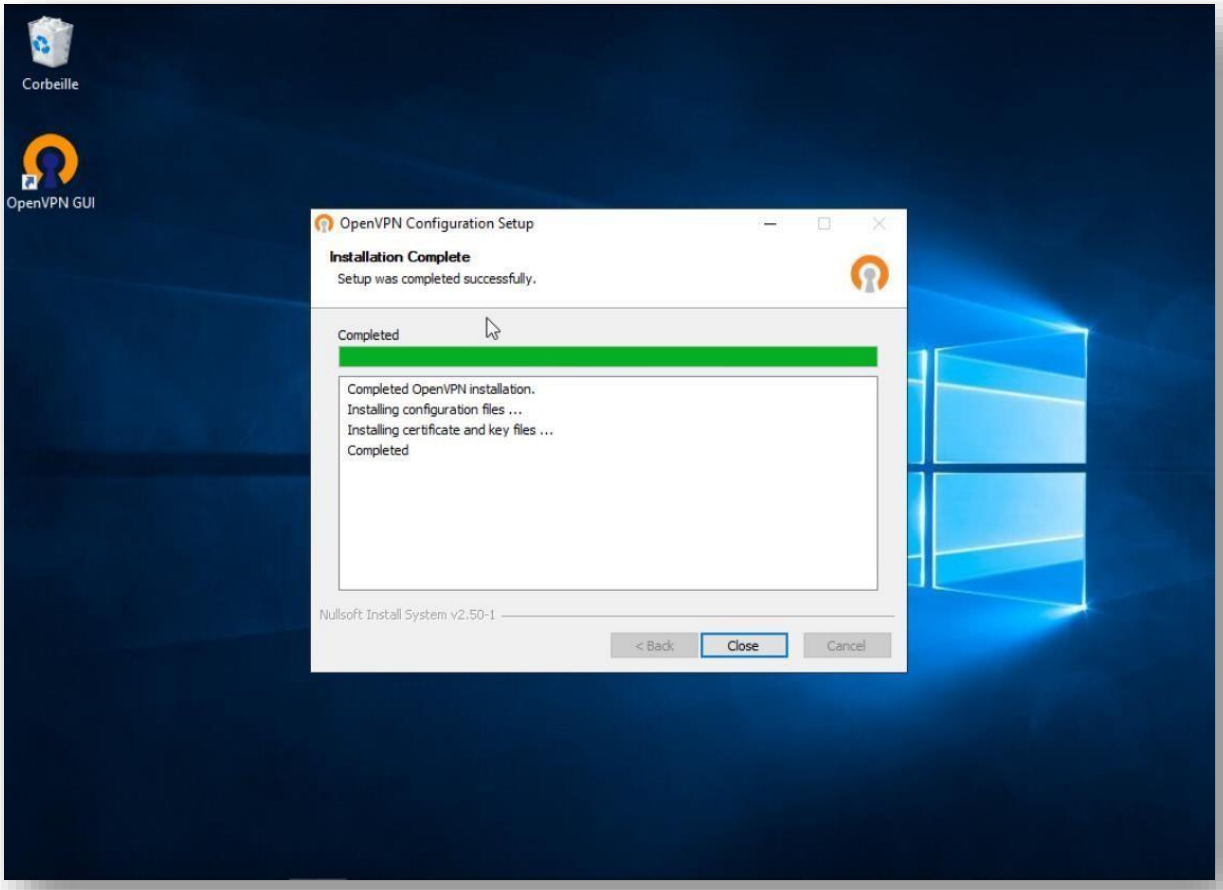
En bas de la page il devrait y avoir des installations pour l'OpenVPN,

sélectionner le 64-bit

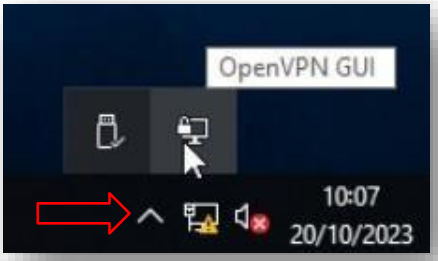


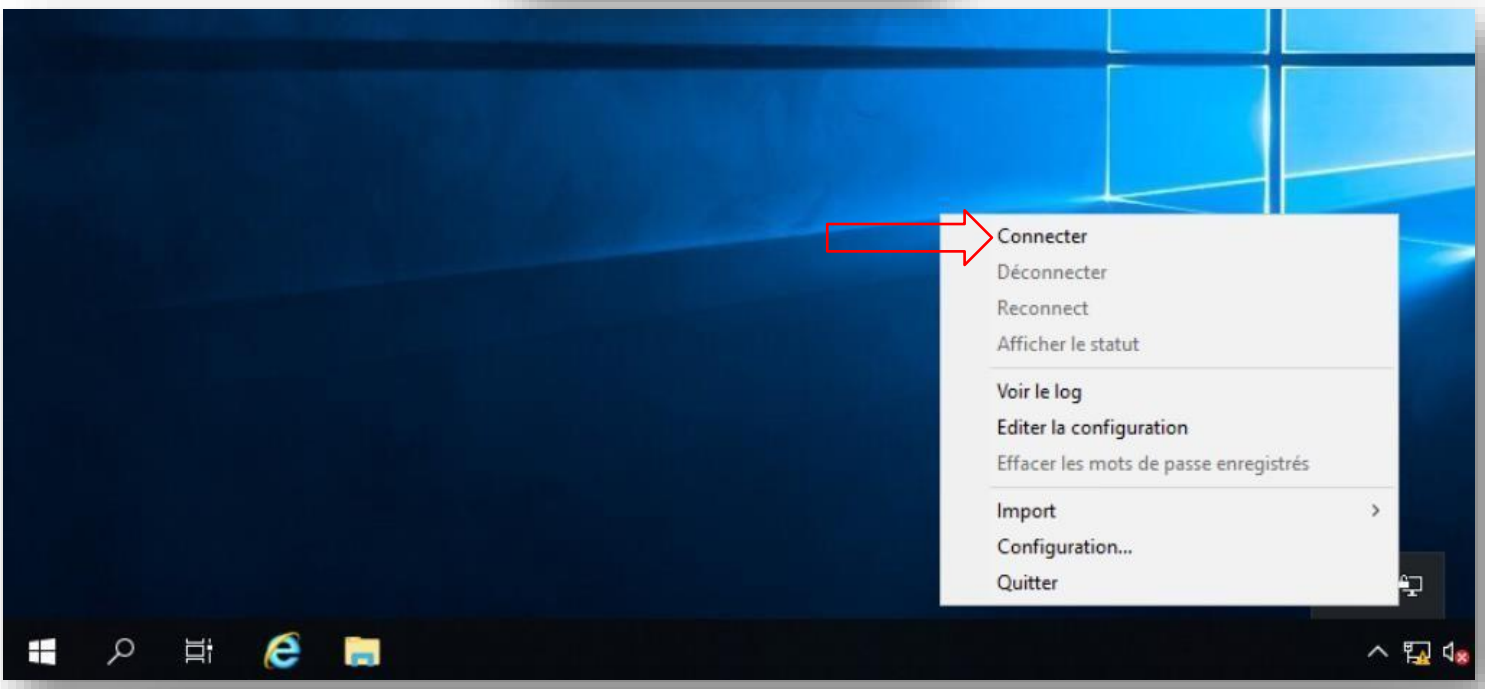
Une fois le client OpenVPN installé ouvrir OpenVPN GUI et démarrer l'installation

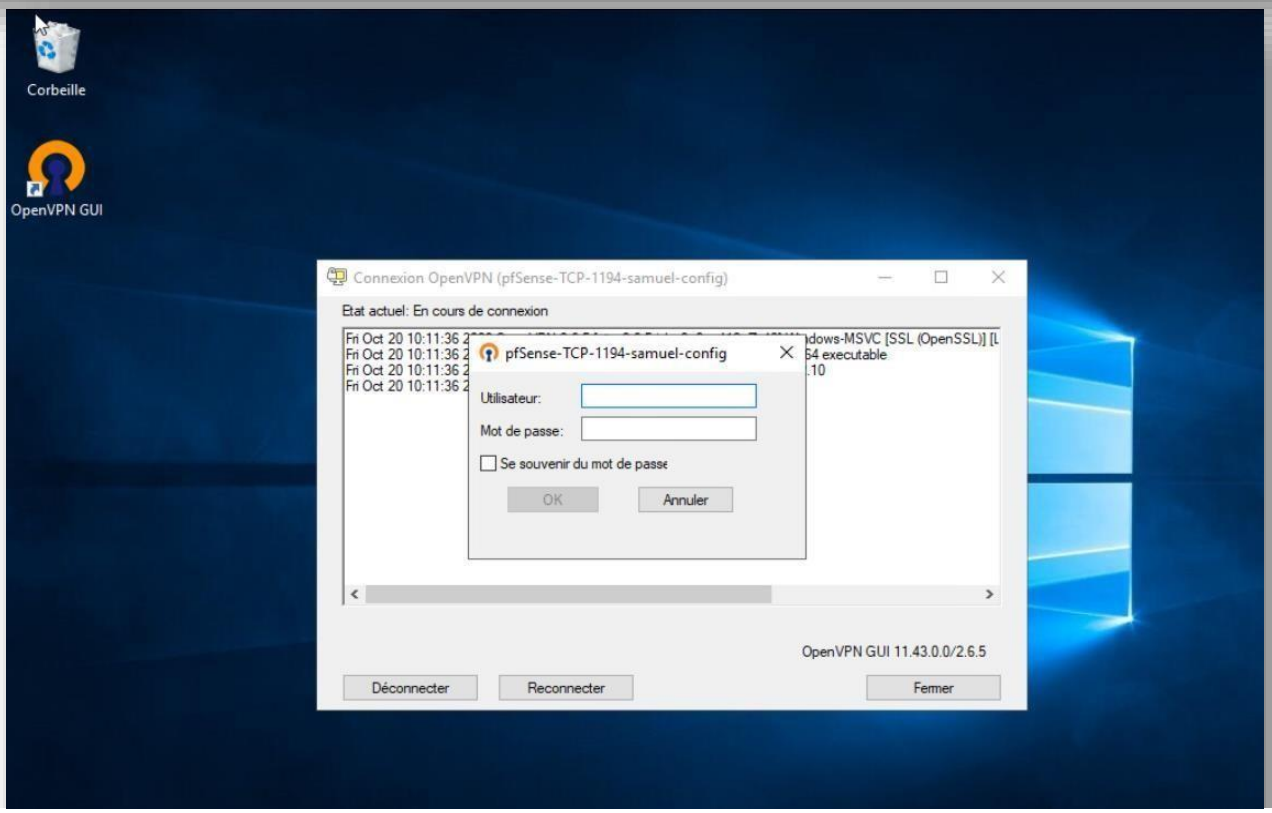




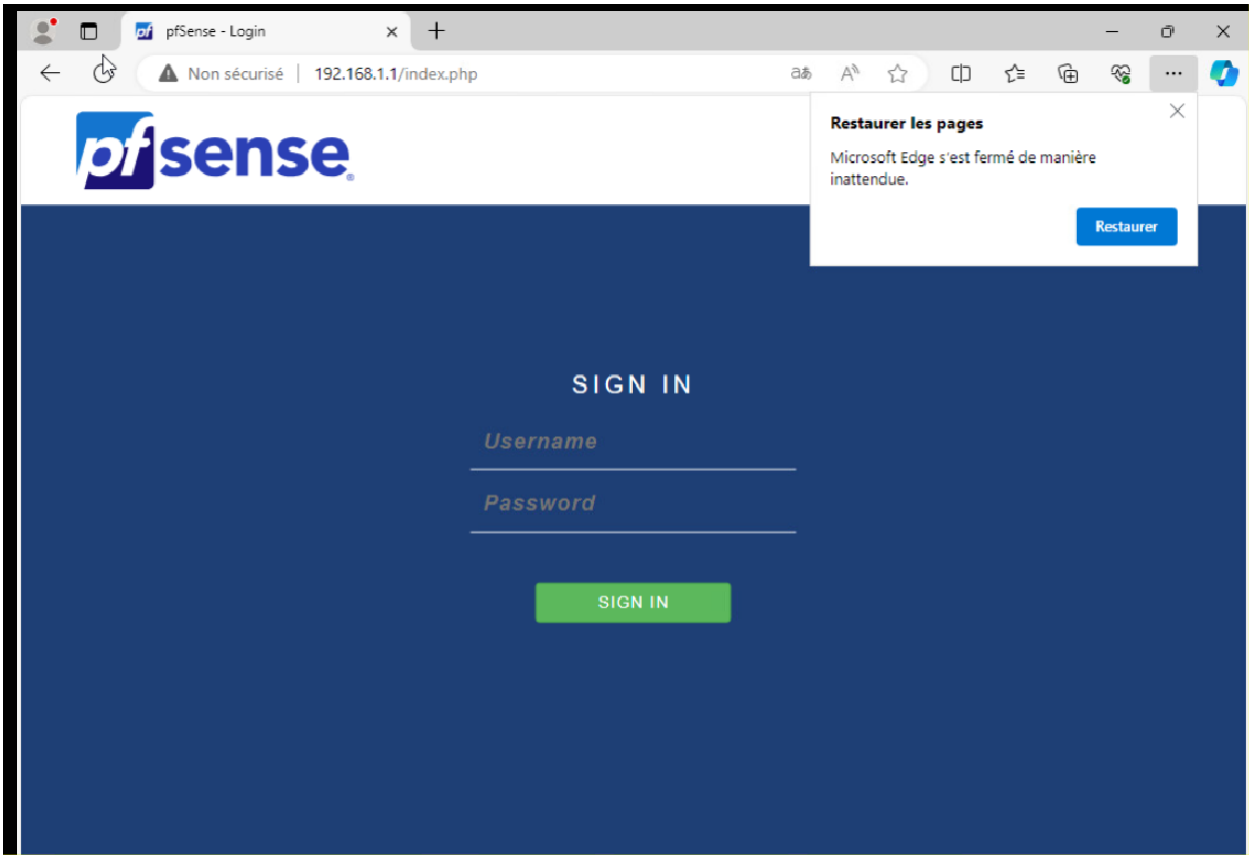
Pour ouvrir le client, cliquer sur l'icône pour voir les applications en arrière-plan, OpenVPN GUI devrait apparaître, faire un clic droit dessus puis « Connecter »



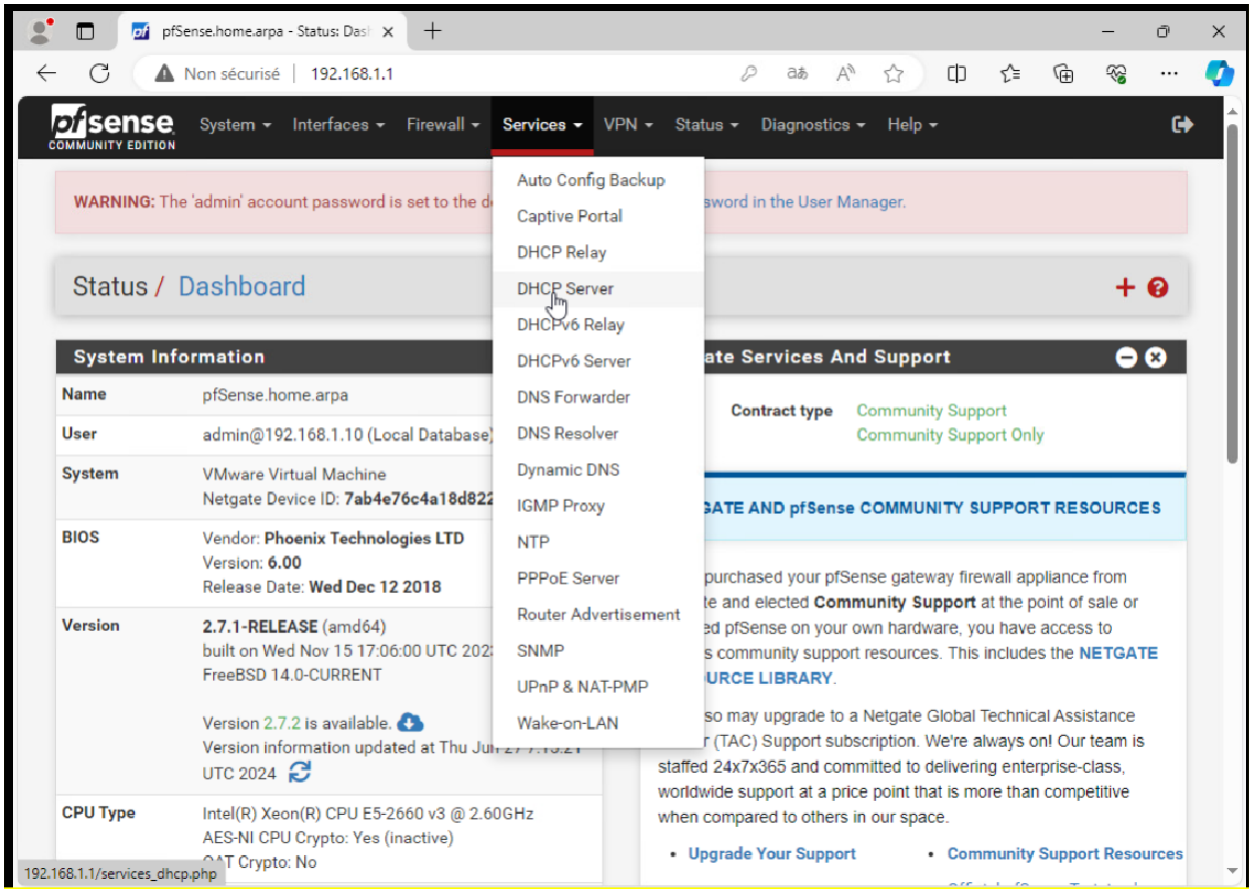




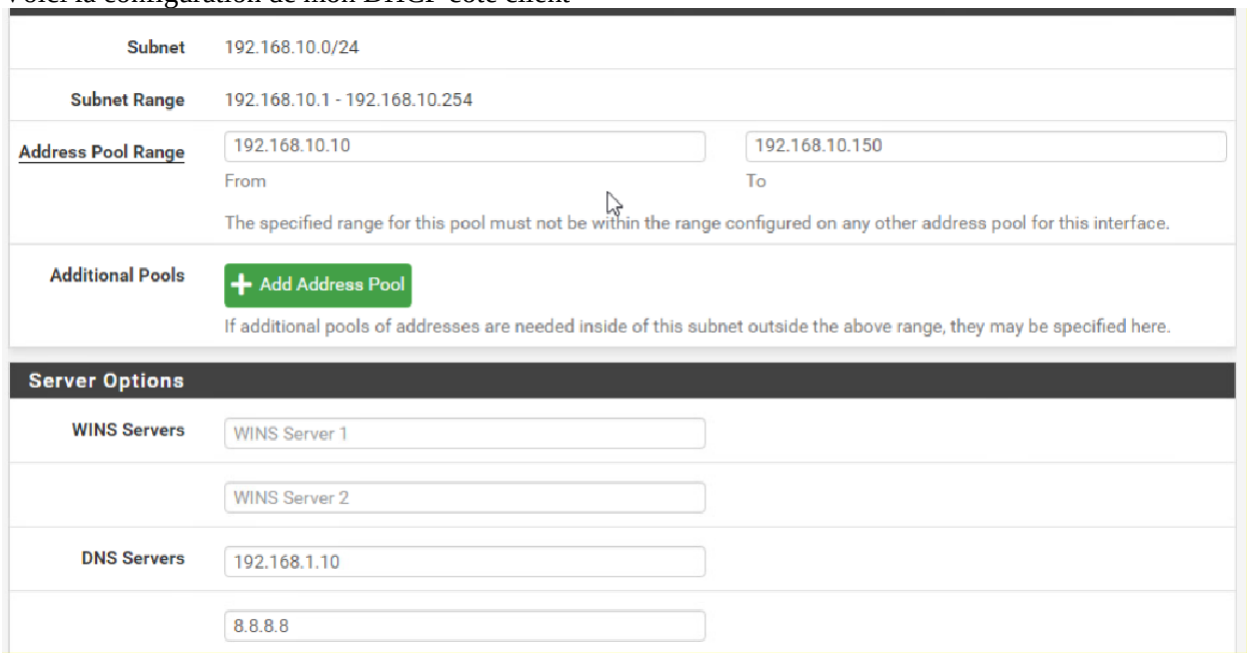
Suite à quelque problème des correctifs était nécessaire dont l'installation du DHCP client sur le firewall via l'environnement graphique



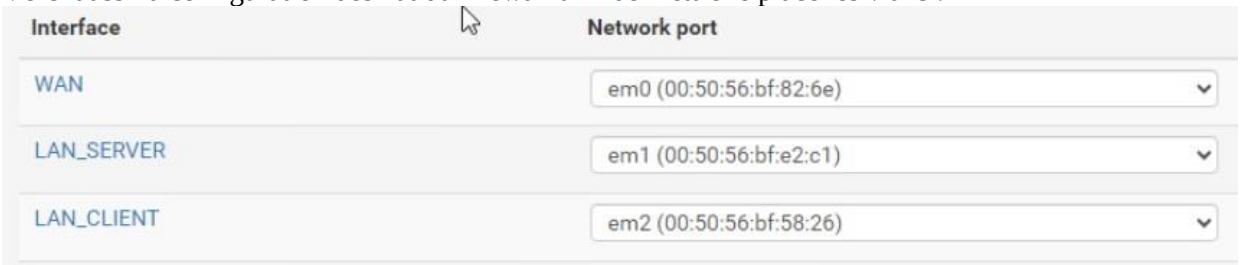
Puis service : DHCP server



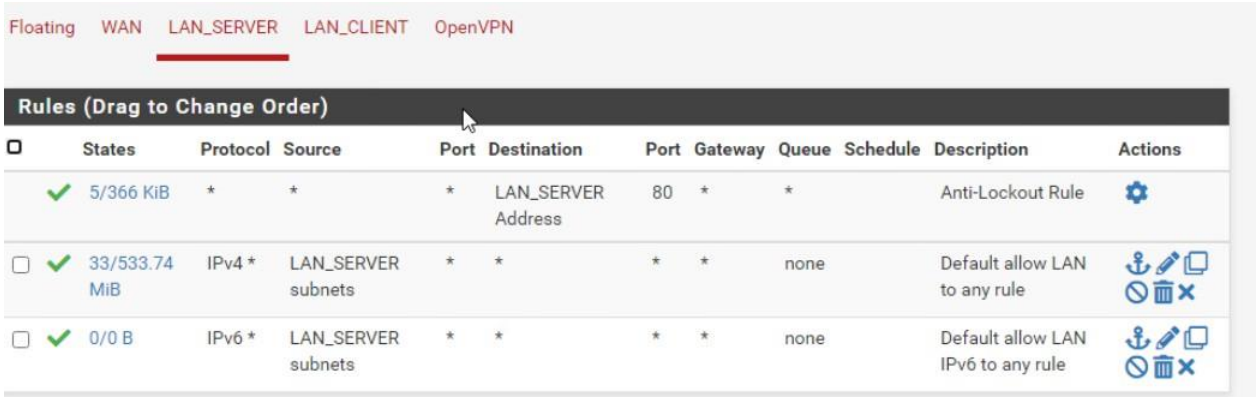
Voici la configuration de mon DHCP coté client

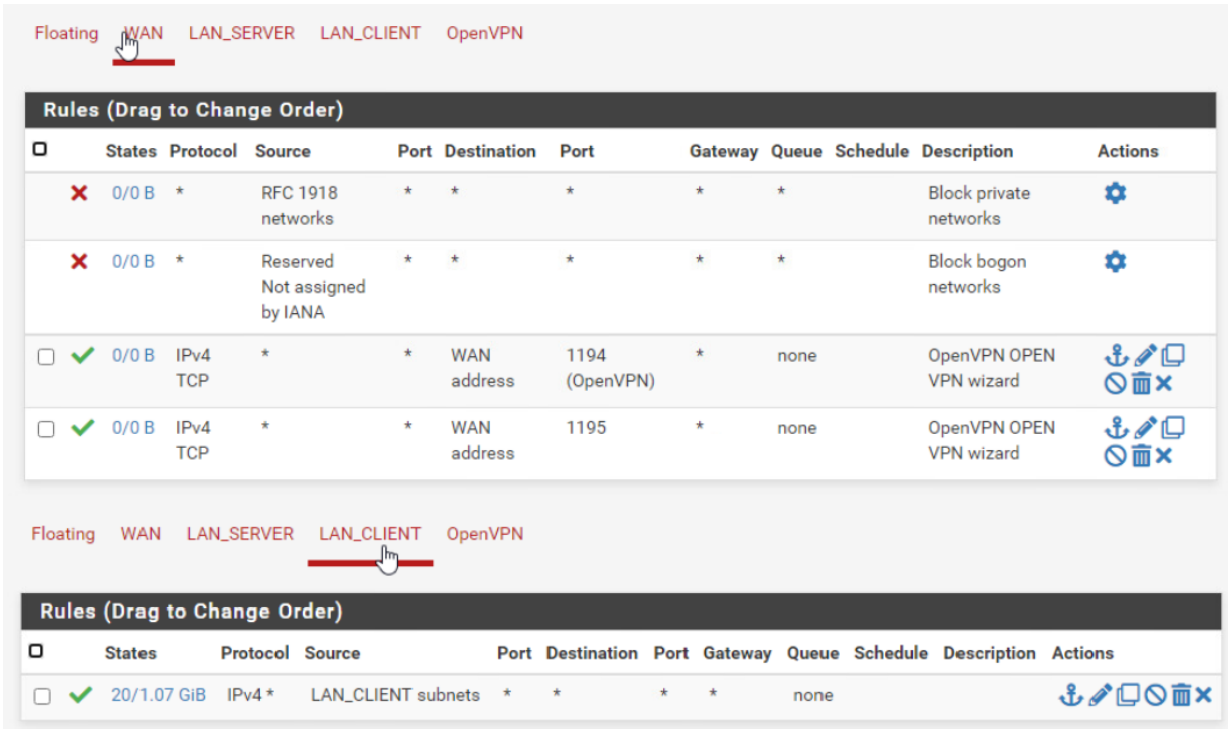


Voici aussi la configuration des nat du firewall afin de mettre le place les vlans :

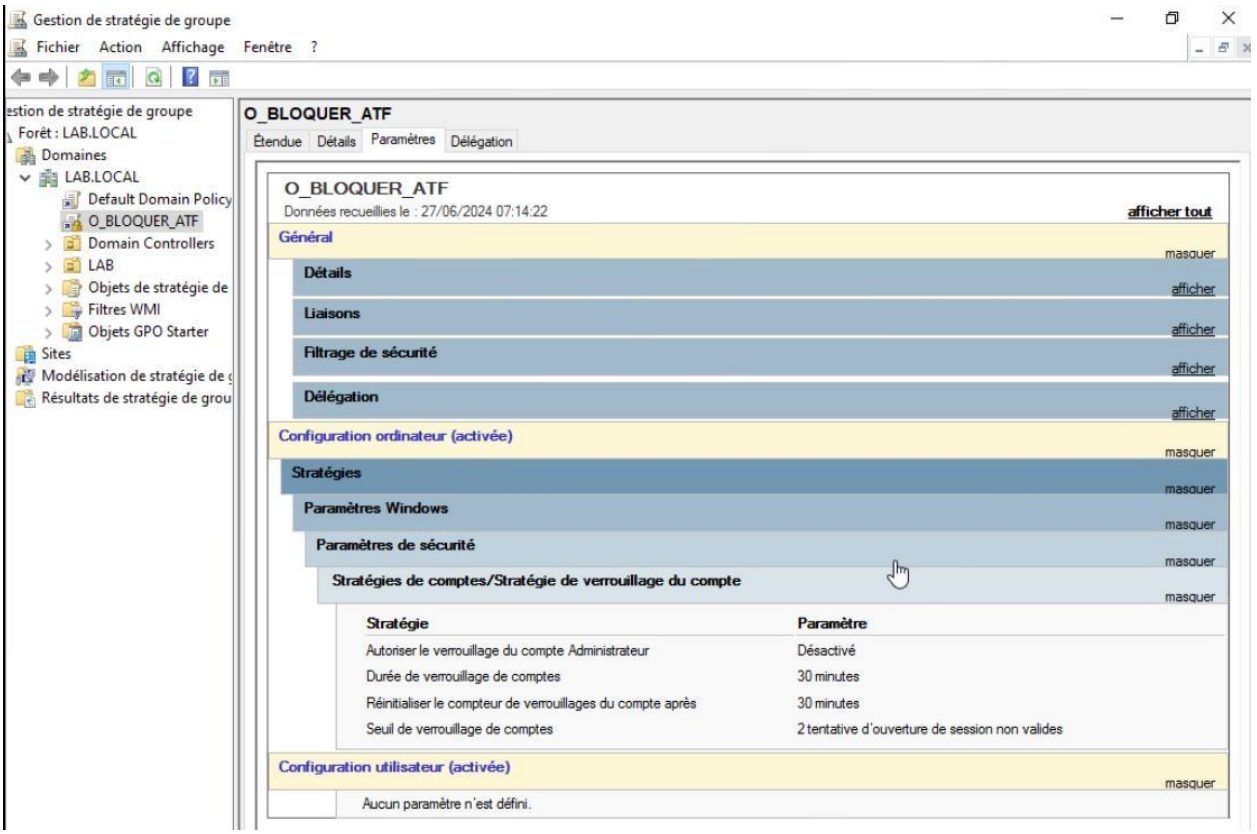


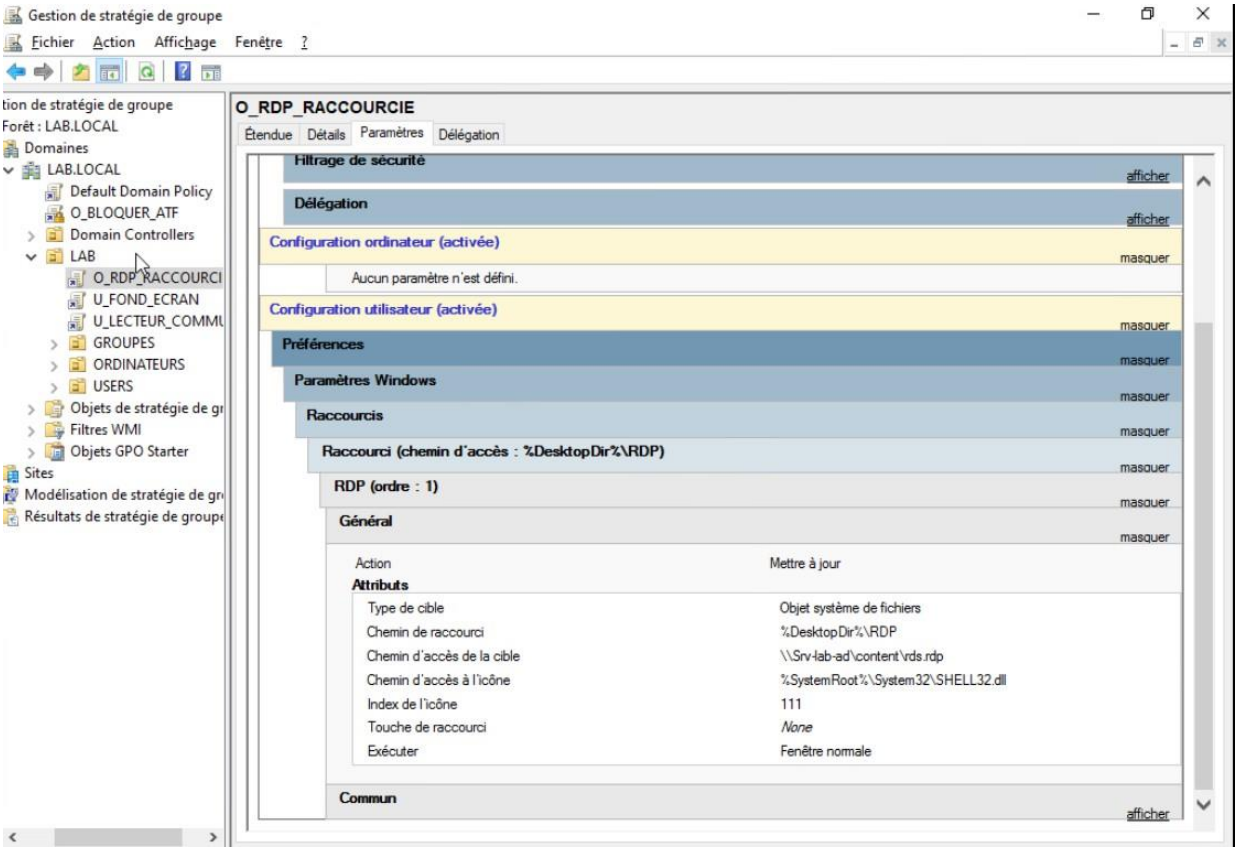
Ainsi que leurs regles de parefeu afin d'autorisé la liaison :

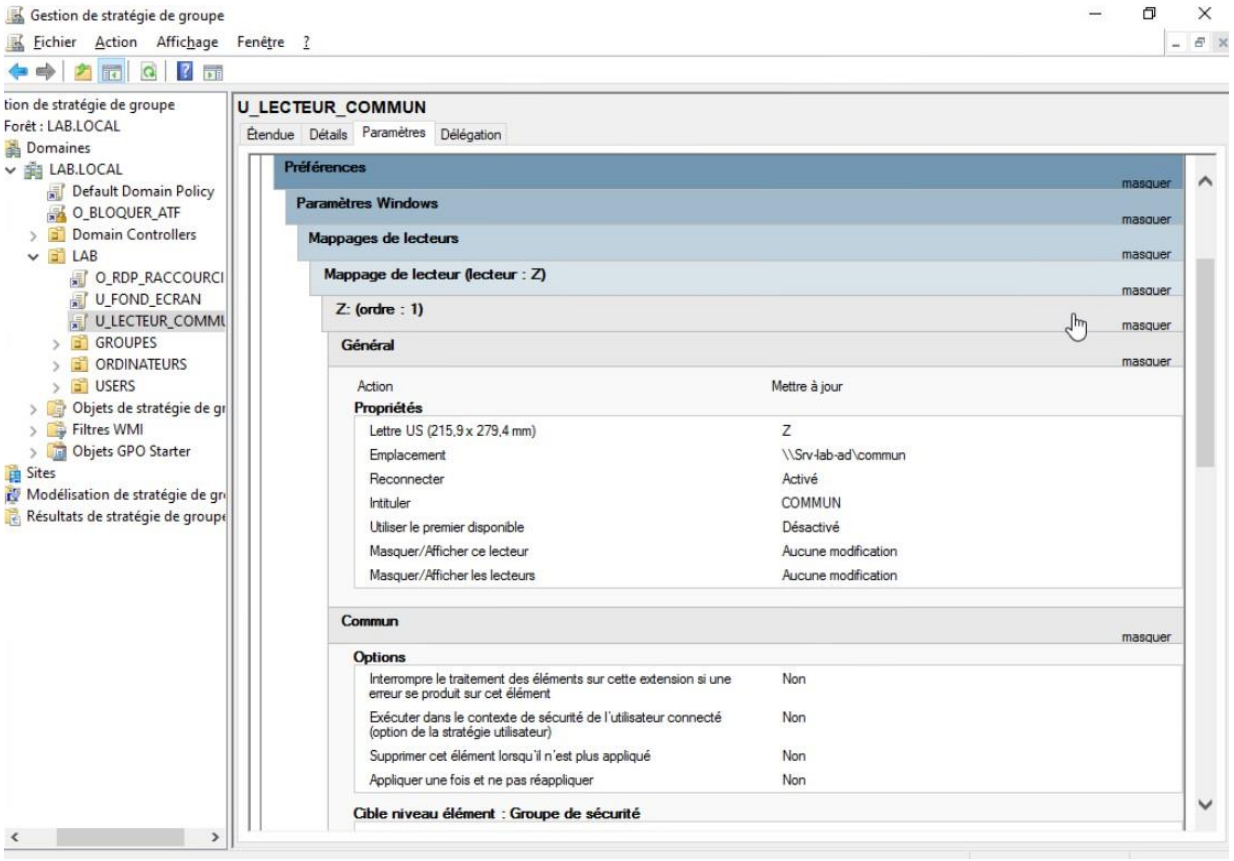


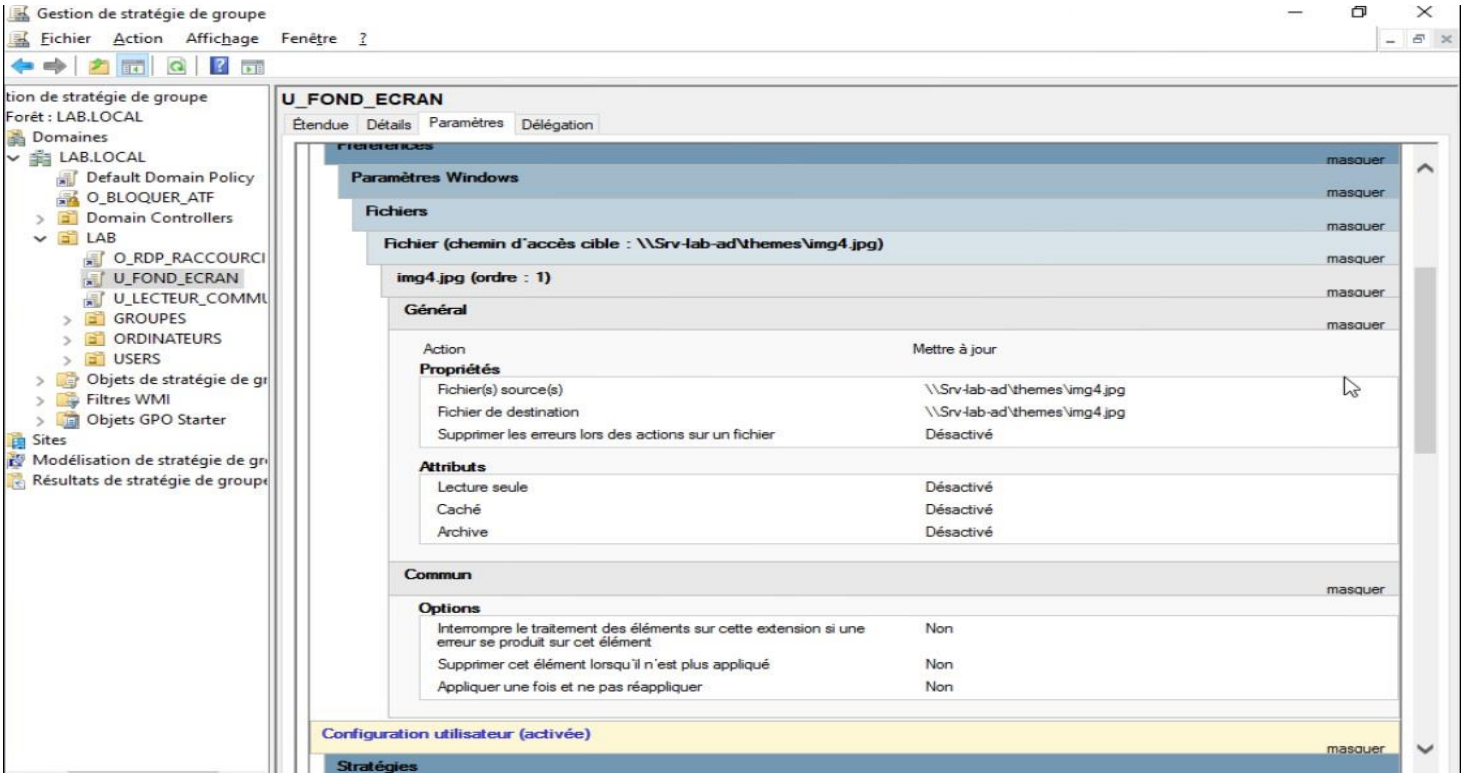


Installations GPO (BONUS) :






Gestion de stratégie de groupe
Fichier Action Affichage Fenêtre ?
tion de stratégie de groupe
Forêt : LAB.LOCAL
Domaines
LAB.LOCAL
Default Domain Policy
O_BLOQUER_ATF
Domain Controllers
LAB
O_RDP_RACCOURCI
U_FOND_ECRAN
U_LECTEUR_COMMU
GROUPES
ORDINATEURS
USERS
Objets de stratégie de gr
Filtres WMI
Objets GPO Starter
Sites
Modélisation de stratégie de gr
Résultats de stratégie de groupe
U_LECTEUR_COMMUN
Étendue Détails Paramètres Délégation
Préférences
masquer
Paramètres Windows
masquer
Mappages de lecteurs
masquer
Mappage de lecteur (lecteur : Z)
masquer
Z: (ordre : 1)
masquer
Général
masquer
Action Mettre à jour
Propriétés
Lettre US (215,9 x 279,4 mm) Z
Emplacement \\Srv-lab-ad\commun
Reconnecter Activé
Intituler COMMUN
Utiliser le premier disponible Désactivé
Masquer/Afficher ce lecteur Aucune modification
Masquer/Afficher les lecteurs Aucune modification
Commun
masquer
Options
Interrompre le traitement des éléments sur cette extension si une erreur se produit sur cet élément Non
Exécuter dans le contexte de sécurité de l'utilisateur connecté (option de la stratégie utilisateur) Non
Supprimer cet élément lorsqu'il n'est plus appliqué Non
Appliquer une fois et ne pas réappliquer Non
Cible niveau élément : Groupe de sécurité


Gestion de stratégie de groupe
Fichier Action Affichage Fenêtre ?
tion de stratégie de groupe
Forêt : LAB.LOCAL
Domaines
LAB.LOCAL
Default Domain Policy
O_BLOQUER_ATF
Domain Controllers
LAB
O_RDP_RACCOURCI
U_FOND_ECRAN
U_LECTEUR_COMMU
GROUPES
ORDINATEURS
USERS
Objets de stratégie de gr
Filtres WMI
Objets GPO Starter
Sites
Modélisation de stratégie de gr
Résultats de stratégie de groupe
U_FOND_ECRAN
Étendue Détails Paramètres Délégation
masquer
Paramètres Windows
masquer
Fichiers
masquer
Fichier (chemin d'accès cible : \\Srv-lab-ad\themes\img4.jpg)
masquer
img4.jpg (ordre : 1)
masquer
Général
masquer
Action Mettre à jour
Propriétés
Fichier(s) source(s) \\Srv-lab-ad\themes\img4.jpg
Fichier de destination \\Srv-lab-ad\themes\img4.jpg
Supprimer les erreurs lors des actions sur un fichier Désactivé
Attributs
Lecture seule Désactivé
Caché Désactivé
Archive Désactivé
Commun
masquer
Options
Interrompre le traitement des éléments sur cette extension si une erreur se produit sur cet élément Non
Supprimer cet élément lorsqu'il n'est plus appliqué Non
Appliquer une fois et ne pas réappliquer Non
Configuration utilisateur (activée)
masquer
Stratégies

Conclusion

Ce projet a permis de mettre en place une infrastructure réseau sécurisée et performante, centrée sur l'installation et la configuration d'un serveur Windows Server 2019 ainsi que la déployabilité d'un VPN via pfSense et OpenVPN dans un environnement virtualisé (vSphere).

Les étapes clés ont inclus :

- **La virtualisation du serveur sous VMware, garantissant flexibilité et scalabilité.**
- **La configuration avancée du VPN pour un accès distant sécurisé, avec authentification par nom d'utilisateur et mot de passe.**
- **L'optimisation du réseau via des stratégies de groupe (GPO), simplifiant la gestion des utilisateurs et des politiques de sécurité.**

En conclusion, cette infrastructure répond aux exigences initiales tout en offrant une base solide pour des évolutions futures.