Projet Experty 3 - Extension de l'infrastructure

BTS SIO – Option SISR

Atelier de professionnalisation

Glossaire....4
Partie 1 : Proposition technique....5
I. Schéma du domaine Experty....5
II. Liste du matériel....6
A. Serveurs....6
B. Routeur....7
C. Baie....8
D. Câbles complémentaires....8
E. Licences windows server 2022....8
III. Solutions applicatives....9
A. PFSense....9
B. GestSup....11
C. PRTG Network monitor....12
D. Veeam....13
E. Teleport....15
IV. Politique de Sauvegarde....16
Partie 2 : Proposition tarifaire....17
I. Proposition pour le matériel....17
II. Proposition pour la prestation....17
Partie 3 : Planning déploiement....18
Annexes....19
I. Procédures....19
A. Pfsense....19
1. Installation de base....19
2. OpenVPN....23
a. Créer le certificat....23
b. Créer les utilisateurs....24
c. Création du serveur OpenVPN....25
3. IPSec....32
4. Ajuster les règles des Firewalls....36
B. Linux GetSup....37
1. Installation de GestSup....37
2. Ajouter le connecteur LDAP pour la connexion à l'Active Directory....42

a. Créer un compte dédié pour Gestsup dans l'Active Directory.. 42
b. Ajout du connecteur LDAP.....44
c. Synchronisation de l'Active Directory..... 45
C. PRTG.....46
D. Bastion Teleport.....49
1. Installation de Teleport..... 49
2. Ajout du nom de l'hôte dans le DNS.....51
3. Création du compte administrateur..... 53
4. Ajouter le domaine experty.....56
a. Configurations sur le DC.....56
b. Configuration sur le serveur Teleport.....61
c. Ajouter le rôle dédié à la connection aux windows du domaine63
E. Veeam..... 64

Glossaire

Active Directory (AD) : Annuaire des utilisateurs et des ordinateurs présents dans le domaine de l'entreprise

Administrateur : Compte avec des droits supérieurs à ceux d'un utilisateur normal.

Bastion : Permet de protéger l'accès aux ressources en étant le point d'accès centralisé

DHCP : Permet l'attribution des adresses IP à chaque poste. Puis le service DNS qui agit comme un annuaire et permet de convertir les adresses IP vers des Url ou inversement.

Domaine : Structure logique regroupant des utilisateurs, ordinateurs et ressources partageant une base de données Active Directory commune et des politiques de sécurité unifiées.

DNS : Annuaire informatique permettant de convertir les adresses IP vers des URL ou inversement.

Poste de travail : Ordinateur utilisé par un utilisateur

RDP : Protocole permettant à un utilisateur de se connecter à distance sur un poste ou un serveur

Serveur : Ordinateur centralisé fournissant des services et ressources (fichiers, applications, authentification) aux postes de travail du réseau.

Utilisateur : Compte individuel créé dans Active Directory permettant à une personne de s'authentifier et d'accéder aux ressources du domaine selon ses droits.

VPN : Abréviation de Virtual Private Network, connexion sécurisée entre deux réseaux

Partie 1 : Proposition technique

Pour satisfaire aux besoins de l'entreprise Experty, plusieurs solutions doivent être mises en place, que ce soit au niveau matériel ou logiciel.

I. Schéma du domaine Experty

Dans le cadre de l'implémentation de l'infrastructure, la structure suivante avait été implémentée :

- Deux serveurs contrôleurs de domaine
- Deux serveurs de fichiers
- Un serveur d'impression
- Un serveur de sauvegarde
- Un serveur pour les outils d'administration à distance

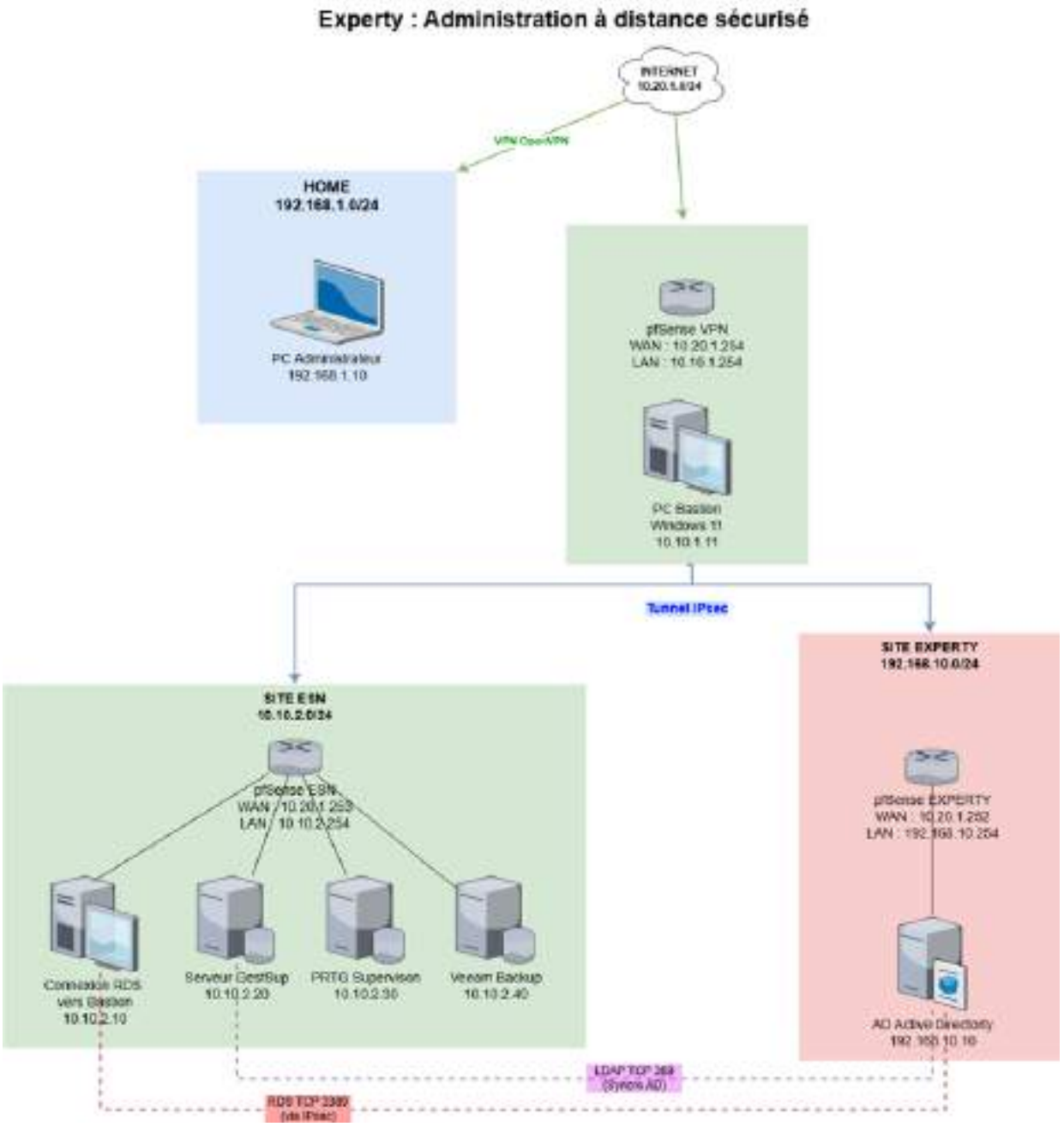
Deux onduleurs sont aussi nécessaires pour garantir un service continu en cas de coupure de courant.

Pour répondre aux nouveaux besoins de l'entreprise Experty, l'infrascture de l'ESN doit aussi évoluer

Un technicien œuvrant de chez lui ou d'un autre réseau doit pouvoir accéder en toute sécurité aux ressources de l'ESN et de Experty. Pour ce faire, des routeurs Netgate intégrant la solution PFSense doivent être mis en place. La mise en place d'un bastion est aussi nécessaire avec la solution Teleport.

Différentes ressources sont aussi nécessaires pour répondre au besoin de support technique. Pour cela, des serveurs doivent être mis en place comprenant les solutions suivantes :

- GestSup pour la gestion des tiquets
- Veeam pour sauvegarder le système GestSup
- PRTG pour la supervision des équipements réseaux



II. Liste du matériel

Plusieurs types de matériel différents sont nécessaires pour la mise en place de l'infrastructure.

A. Serveurs

Tout d'abord, quatre serveurs sont nécessaires. Pour ce faire, les serveurs DELL PowerEdge R660 Serveur rack Smart Selection ont été sélectionné. Ceux-ci ont un processeur Intel® Xeon® Silver 4410Y 2 GHz, 12C/24T, 16 GT/s, cache 30 Mo, Turbo, HT (150 W), mémoire DDR5 à 4 000 MHz, ainsi qu'une mémoire de 32 Go RDIMM, 5600 MT/s, double rangée. Ils sont aussi équipés de disques SSD 480 Go SATA lecture intensive 6 Gbit/s 512e 2,5" AG à enfichage à chaud, 1 écriture par jour.

Figure 3 Serveur DELL

B. Routeur

Comme évoqué auparavant, des routeurs Netgate 2100 sont nécessaires. Ceux-ci intègrent la solution PFSense et ont une interface web pour les configurer. Ce modèle est prévu pour des petites entreprises.

Figure 4 Routeur Netgate 2100

Voici ces performances :

PERFORMANCE	TECH SPECS
IPERF3 TRAFFIC	**IMIX TRAFFIC**
L3 Forwarding: 2.20 Gbps	**L3 Forwarding:** 594 Mbps
Firewall: 964 Mbps (10k ACLs)	**Firewall:** 249 Mbps (10k ACLs)
IPsec VPN: 254 Mbps (AES-GCM-128 / AES-NI)	**IPsec VPN:** 90 Mbps (AES-GCM-128 / AES-NI)

Figure 5 Performances Netgate 2100

C. Baie

Une baie est nécessaire pour sécuriser les serveurs, la baie APC NetShelter SX Enclosure with Sides - Rack - noir - 42U - 19" est adaptée de par sa taille et la sécurité qu'elle apporte (fermeture par clé)[1].

Figure 6 Baie APC NetShelter

D. Câbles complémentaires

Des câbles complémentaires à ceux déjà présents dans les locaux peuvent être nécessaires pour connecter les serveurs dans la baie, par exemple des câbles ethernet de 50cm, 1m ou 3m peuvent être nécessaires.

E. Licences windows server 2022

Des licences sont nécessaires pour les serveurs, ici des licences Microsoft Windows Server 2022 Standard - 16 noyaux.

[1] https://www.inmac-wstore.com/apc-netshelter-sx-enclosure-with-sides-rack-42u/p2048821.htm

Figure 7 Licence Windows Server

III. Solutions applicatives

A. PFSense

PFSense est système d'exploitation permettant la mise en place d'un parefeu. Celui-ci permet de créer des règles pour le trafic.

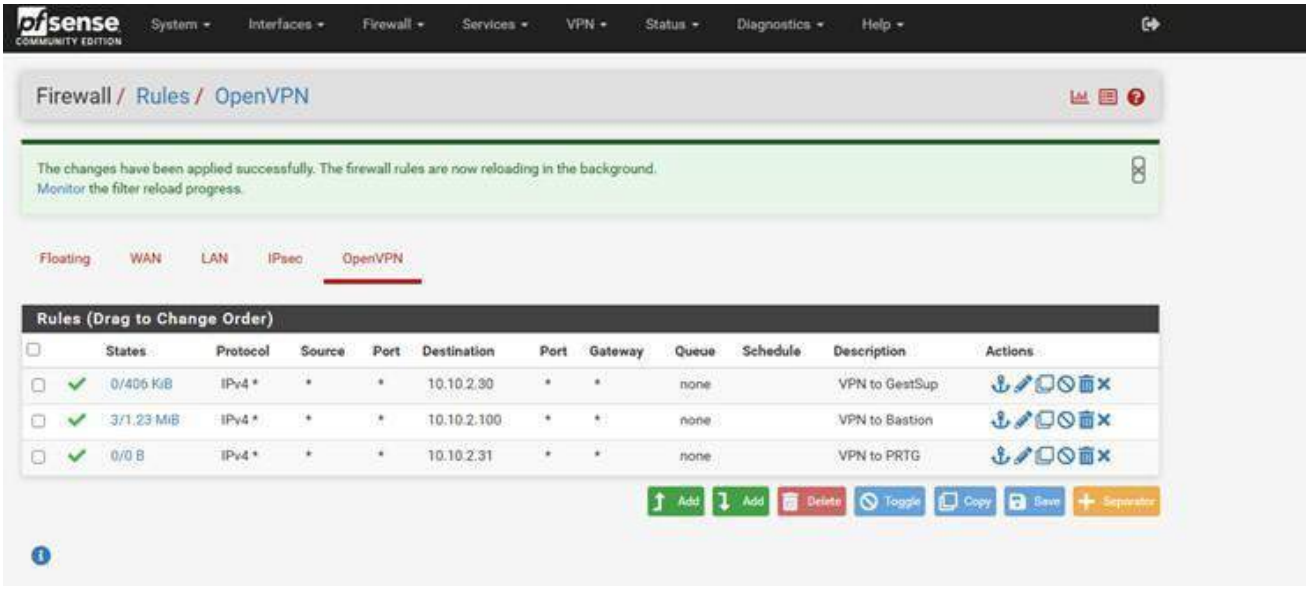


Figure 8 Règles sur le PFSense de l'ESN

Il permet aussi de faciliter la mise en place de VPN, à travers l'outil OpenVPN. La configuration est faite sur le PFSense, puis un client est créé et peut être installé sur différents systèmes d'exploitation, comme Windows 11 par exemple.

Figure 9 OpenVPN sur le PFSense de l'ESN

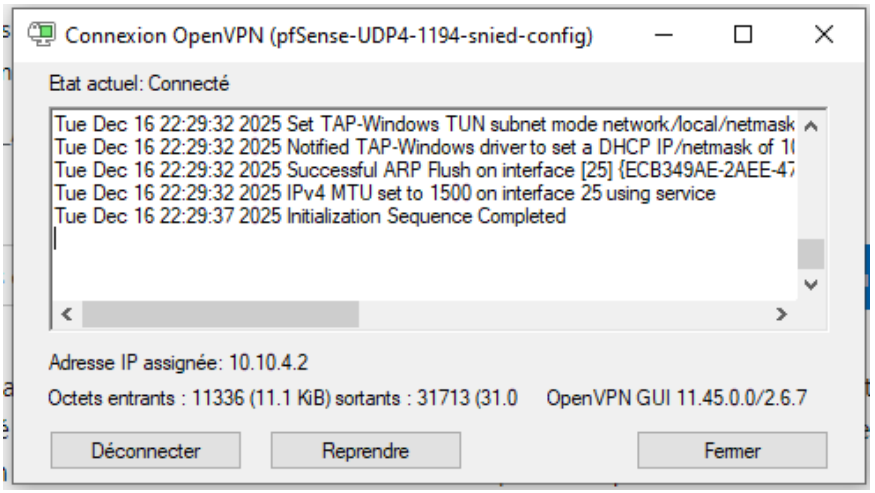


Figure 10 Client OpenVPN sur Windows

PFSense permet aussi de mettre en place des tunnels IPSec. Par exemple ici entre le réseau de l'ESN et le réseau d'Experty.

Figure 11 Tunnel IPSec

PFSense peut aussi servir de DNS si un serveur DNS n'est pas déjà présent dans le réseau.

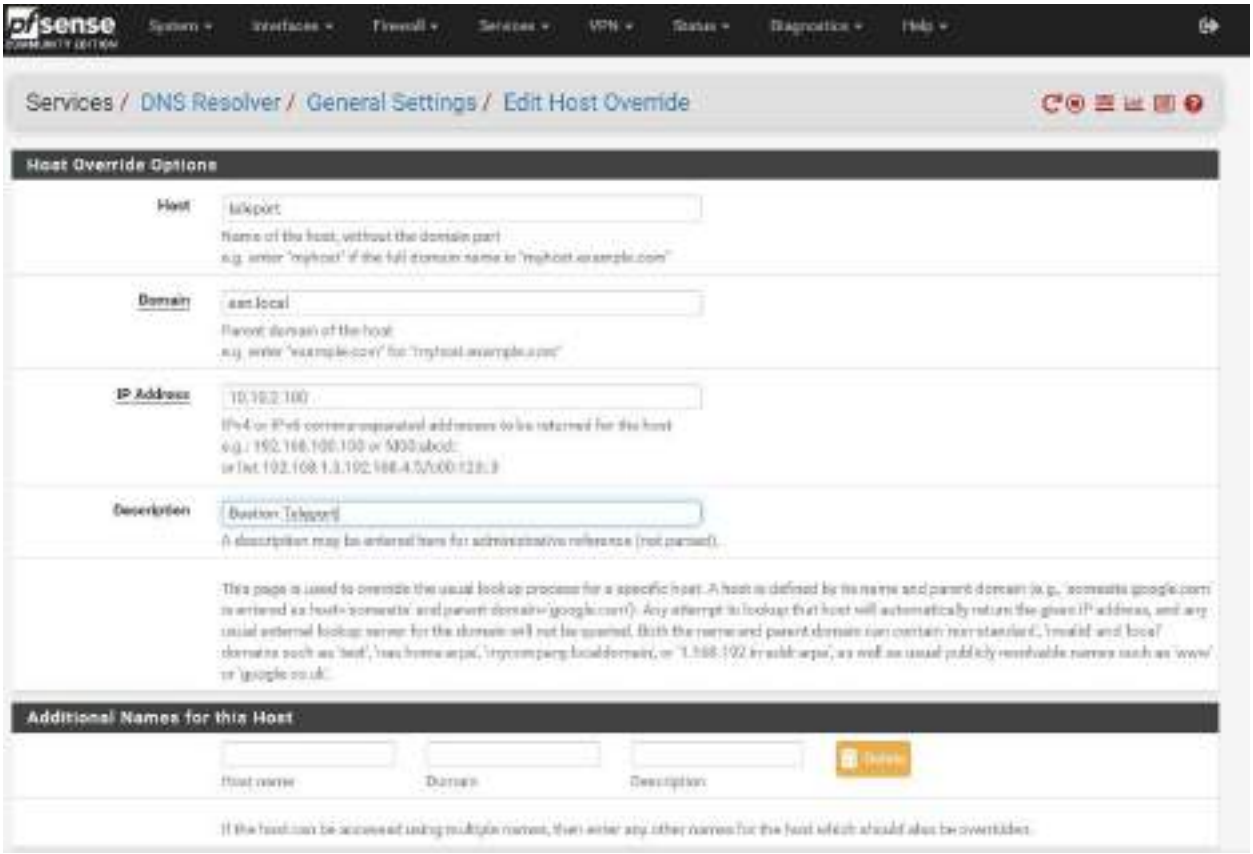


Figure 12 Configuration d'un Host avec le DNS Resolver du PFSense de l'ESN

B. GestSup

GestSup est une solution de gestion de tickets de supports et d'équipements. Elle permet aux utilisateurs d'experty d'ouvrir des tickets lorsqu'un incident survient ou lorsqu'ils ont des requêtes techniques. Les techniciens de l'ESN peuvent alors gérer ces tickets.

Cette solution est connectée à l'active directory d'Experty pour permettre aux utilisateurs de s'identifier avec leurs logins habituels.

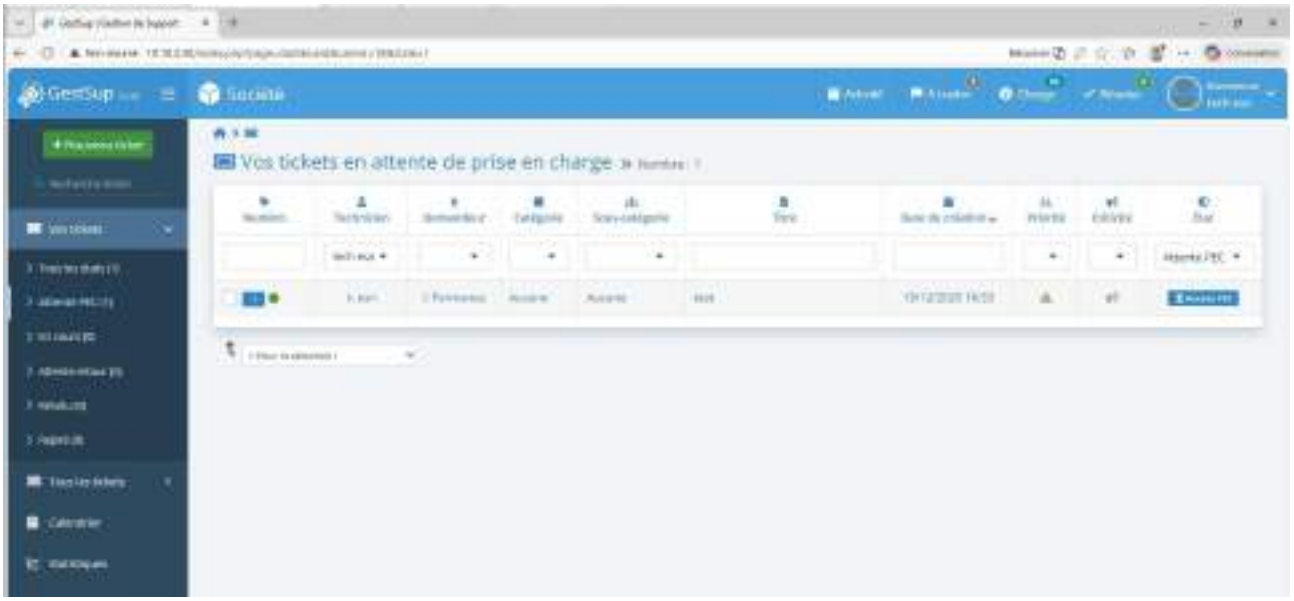


Figure 13 Accueil de GestSup avec le compte technicien de l'ESN

C. PRTG Network monitor

PRTG Network Monitor est une solution permettant la supervision des équipements réseaux. Elle permet de surveiller l'état des équipements et d'alerter si un incident survient. Ici, l'infrastructure réseau de l'ESN est celle surveillée, mais il est aussi possible de superviser celle d'Experty si besoin est.

Figure 14 Accueil de la solution PRTG

La solution génère automatiquement une carte réseau, ce qui peut être très pratique pour la documentation ou pour résoudre des incidents.

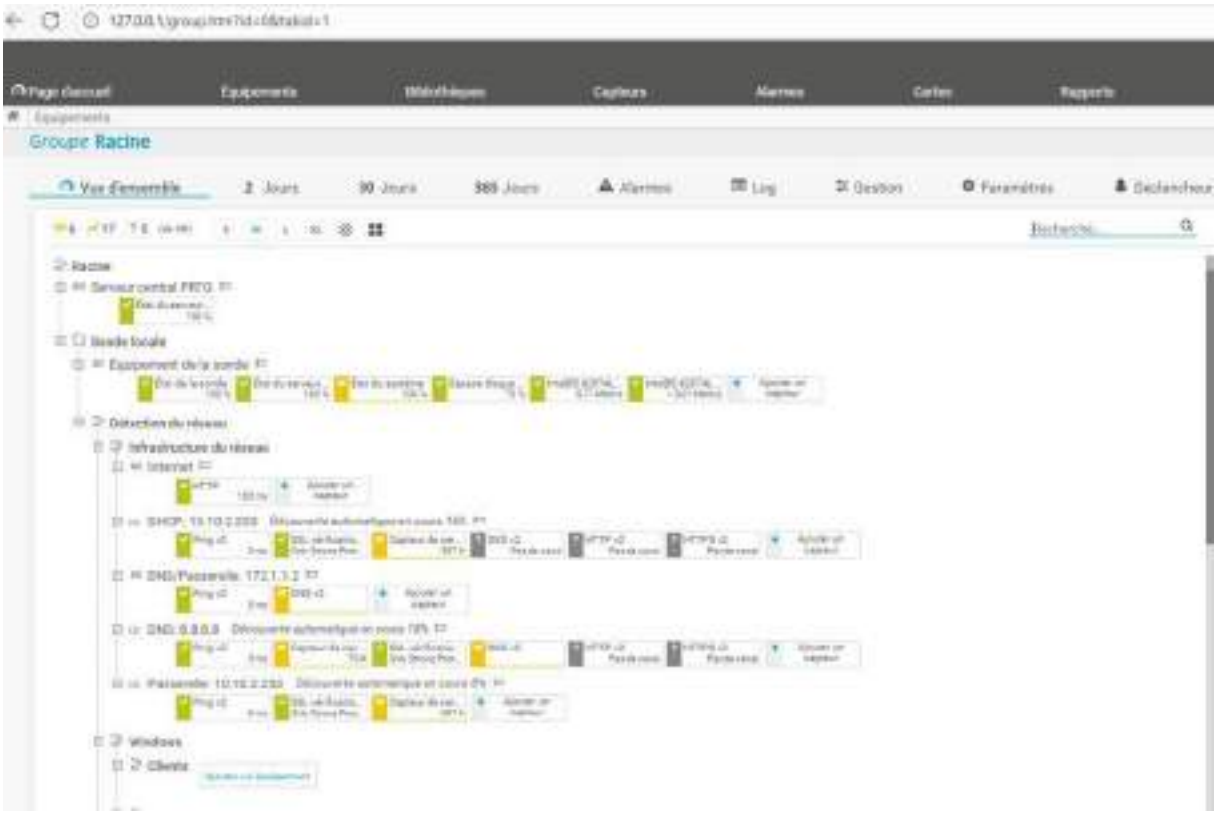


Figure 15 Carte réseau de l'ESN

D. Veeam

Veeam est une solution de sauvegarde et récupération. Veeam va permettre de sauvegarder des systèmes entiers ou juste certains volumes ou fichiers au choix, pour permettre une récupération en cas d'incident.

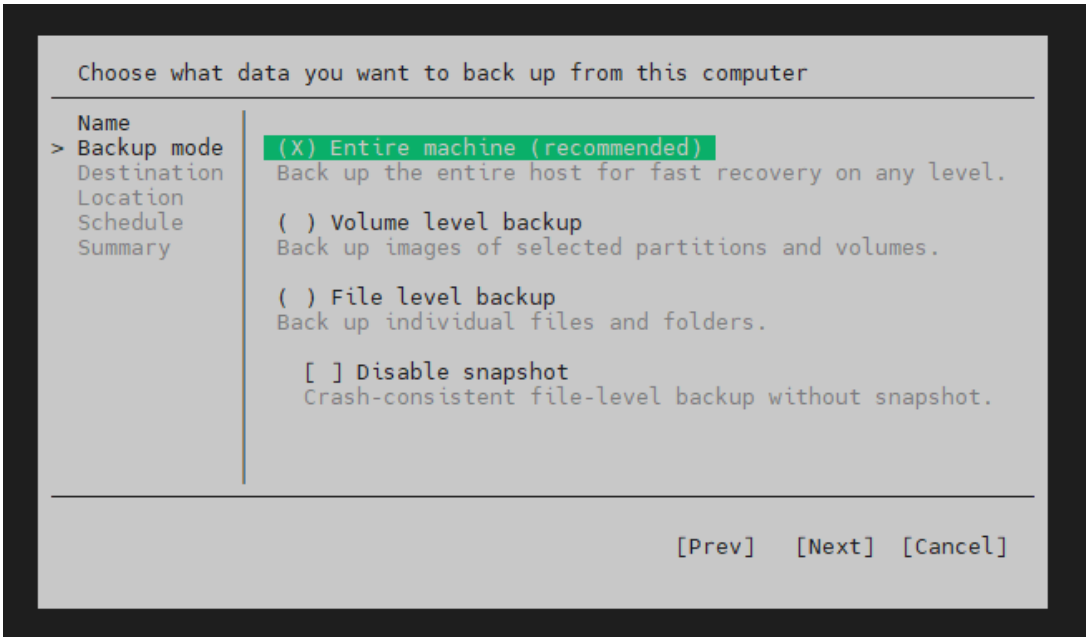


Figure 16 Choix des supports à sauvegarder

Un agent Veeam est installé sur chaque système dont une sauvegarde est souhaitée. Cette sauvegarde peut être faite au rythme souhaité.

Figure 17 Choix du rythme de la sauvegarde dans Veeam

Elle peut être sauvegardée sur le serveur concerné en local (non recommandé pour des raisons de sécurité), sur un support externe ou dans un dossier partagé, hébergé sur un autre serveur.

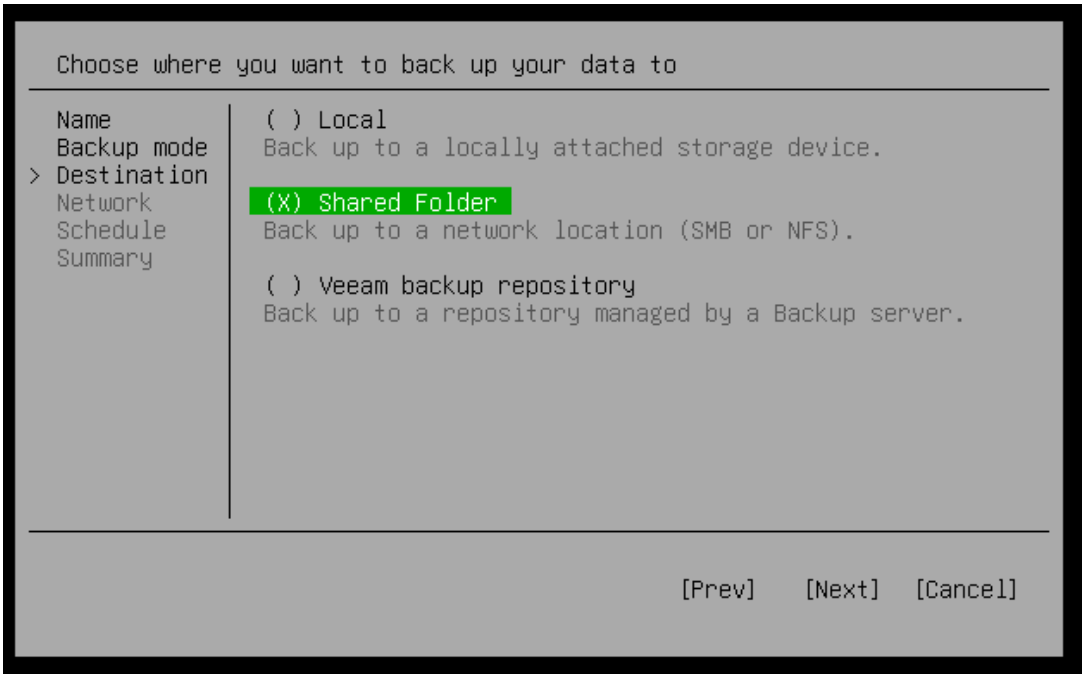


Figure 18 Choix de la destination de la sauvegarde

Pour l'ESN, le choix a été fait de sauvegarder le serveur hébergeant la solution GestSup dans un dossier partagé, hébergé sur un serveur windows dans le même réseau.

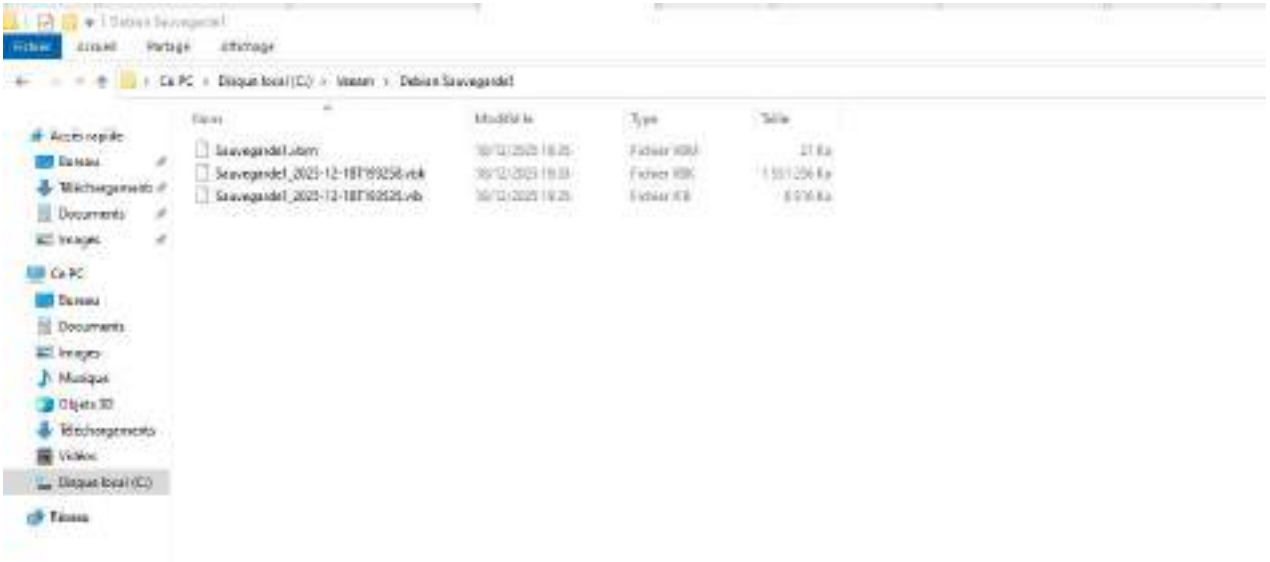


Figure 19 Dossier partagé de sauvegarde veeam

E. Teleport

Teleport est solution permettant un accès Zero Trust aux serveurs et aux applications grâce à différents protocoles. Les utilisateurs ont un utilisateur avec des rôles dédiés dans Teleport leur donnant l'accès que à certaines ressources.

Pour le technicien de l'ESN, celui-ci a accès à Teleport seulement au travers du VPN et a son utilisateur dédié lui permettant seulement l'accès avec son utilisateur de l'Active Directory au domain controller de Experty avec un bureau à distance (RDP).

Figure 20 Accueil de Teleport pour l'administrateur

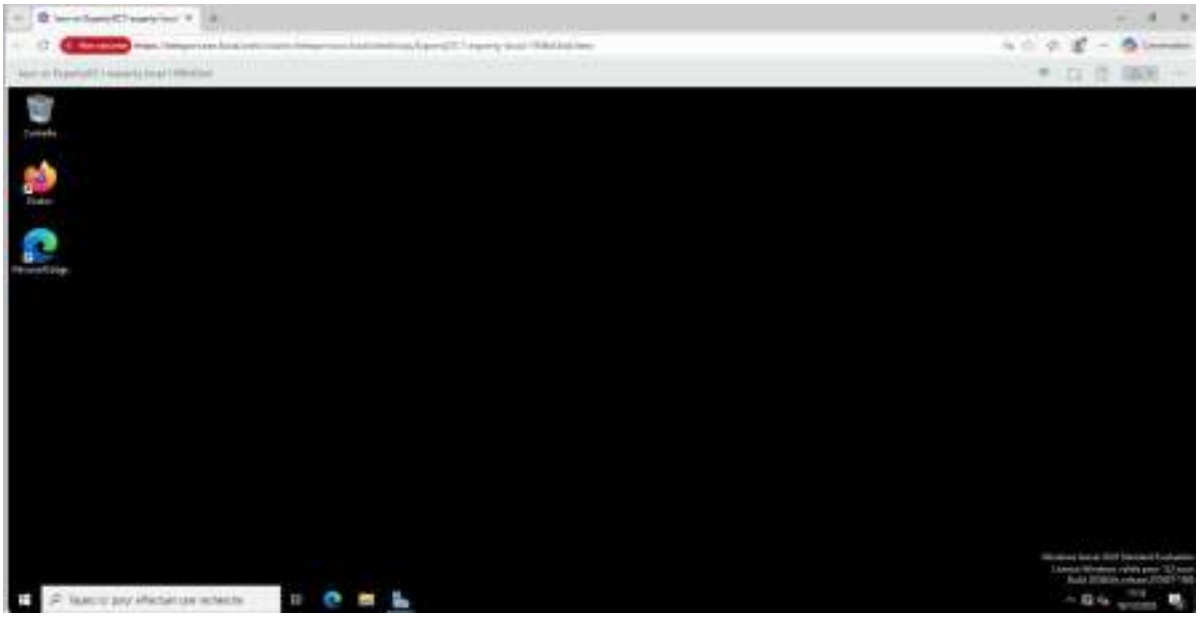


Figure 21 Accès au bureau à distance du DC1 Experty

Teleport permet d'enregistrer les sessions des utilisateurs et de faire des logs des actions.

IV. Politique de Sauvegarde

Tout comme pour le premier projet Experty, une politique de sauvegarde doit être déterminée. Ici il est important de garantir la sécurité du système de support pour avoir un suivi sans encombre.

Pour cela le système GestSup est sauvegardé avec la solution Veeam.

La solution sauvegarde le système entier tous les jours à 00 :40 et la sauvegarde est retenue pendant une période de 7 jours. Cela permet de rétablir le système en cas d'incident.

Partie 2 : Proposition tarifaire

Au sein de la proposition tarifaire doivent être distingués la proposition pour le matériel comprenant les coûts de chaque solution matérielle et la proposition tarifaire pour la prestation réalisée.

I. Proposition pour le matériel

Nom	Quantité	Prix
Serveur	4	25 735 €
Routeurs	2	630 €
Baie	1	1 901,61€
Licences Windows Server 2022	2	748,88€

II. Proposition pour la prestation

Nom	Quantité	Prix
Réalisation de la documentation	1	1 000€
Intervention technicien	2	3 000€
Support technique	1	1 901,61€/ an

Partie 3 : Planning déploiement

Au niveau du déploiement, celui-ci est prévu sur deux jours.

Etape	Nombre de technicien	Durée	Date
Installation physique de la baie avec les serveurs et routeur	1	2h	1er jour
Déploiement PFSense	1	5h	1er jour
Déploiement de GestSup et la sauvegarde	1	3h	2eme jour
Déploiement Teleport	1	3h	2eme jour
Déploiement PRTG	1	2h	2eme jour

Annexes

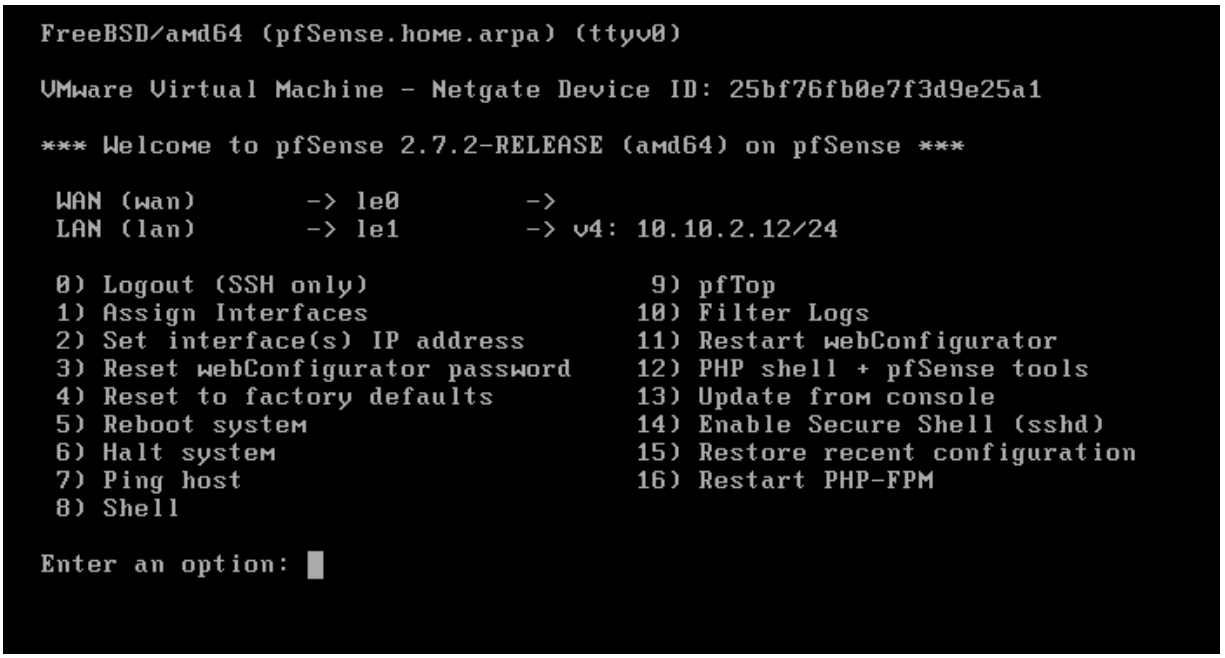
I. Procédures

Les procédures qui suivent ont été faites pour le déploiement des différentes solutions évoquées plus haut.

A. Pfsense

1. Installation de base

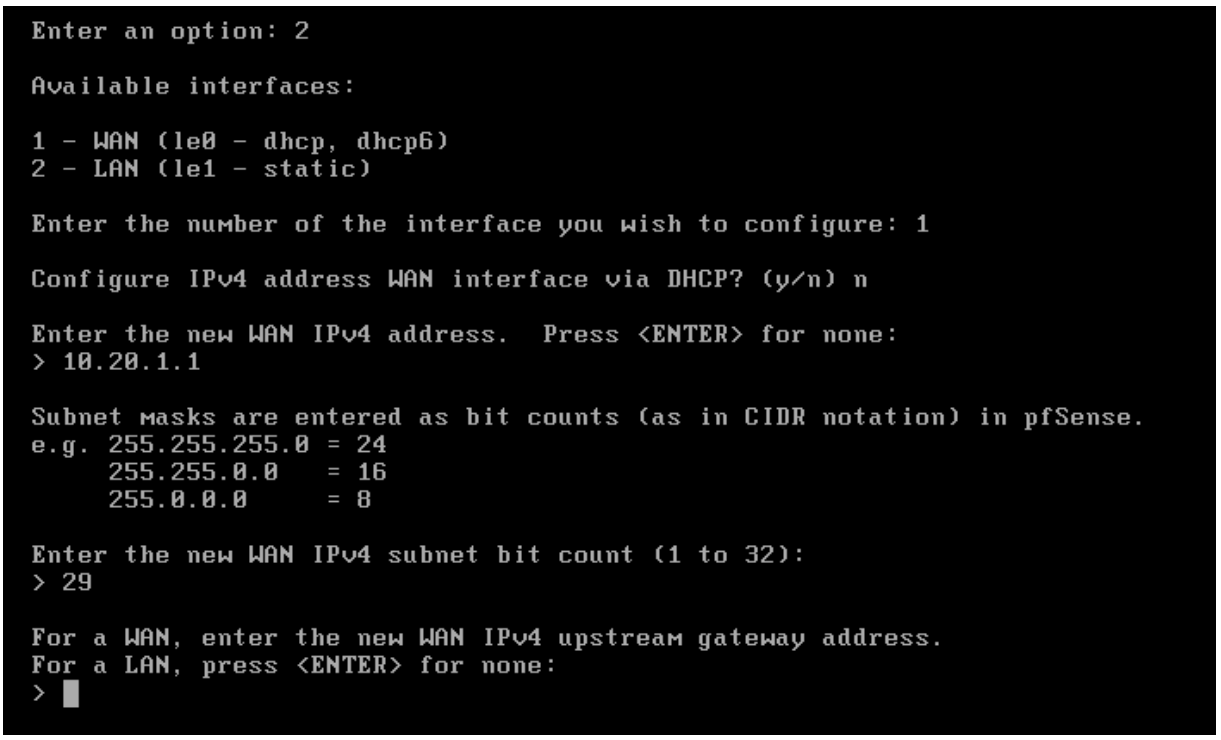
Assigner les adresses IP aux interfaces LAN et WAN :



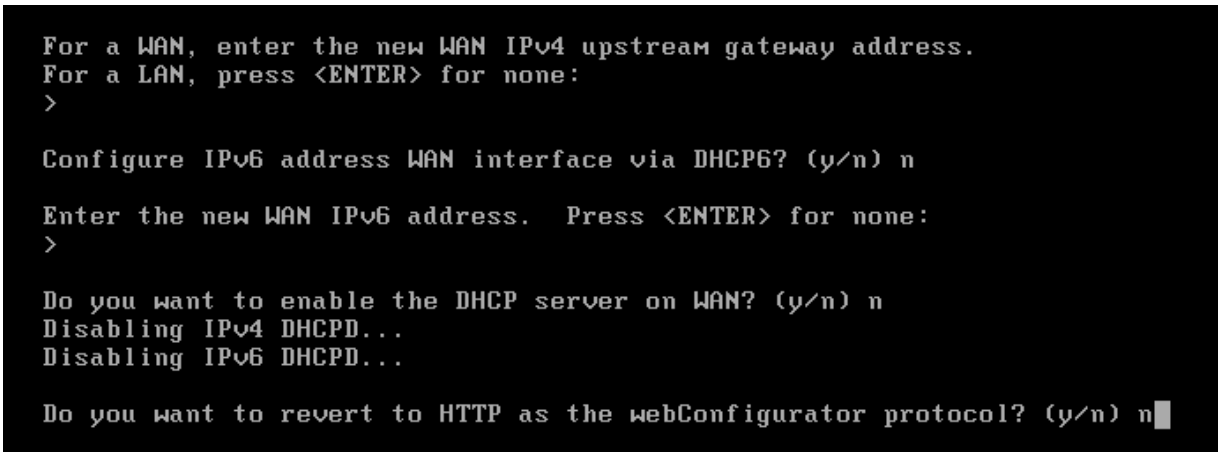
Assigner à l'interface WAN :

Entrer 2 comme option. Ensuite taper 1 pour accéder aux paramètres de l'intrerface WAN. Mettre n pour le DHCP, puis renseigner l'adresse WAN du pfsense ainsi que le masque de sous-réseau en notation CIDR. Puis renseigner l'adresse de la passerelle

du WAN pour l'upstream gateway adress.



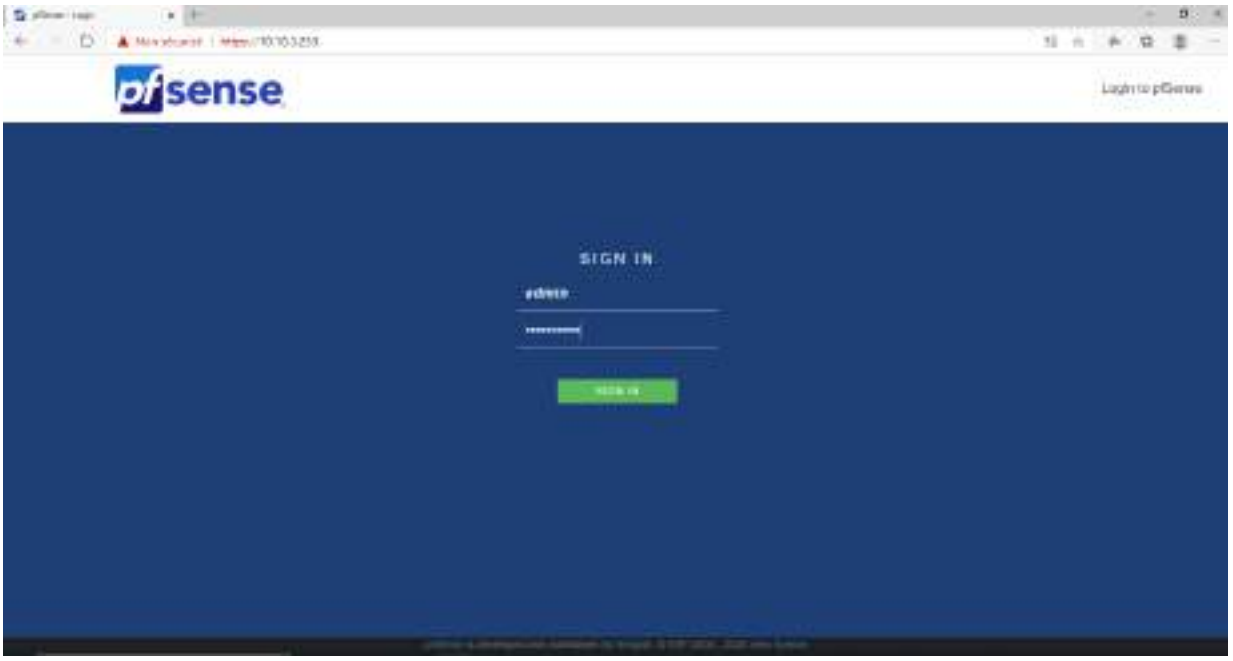
Ensuite faire non pour tout ce qui concerne l'IPv6 et refuser l'activation du DHCP sur le WAN :



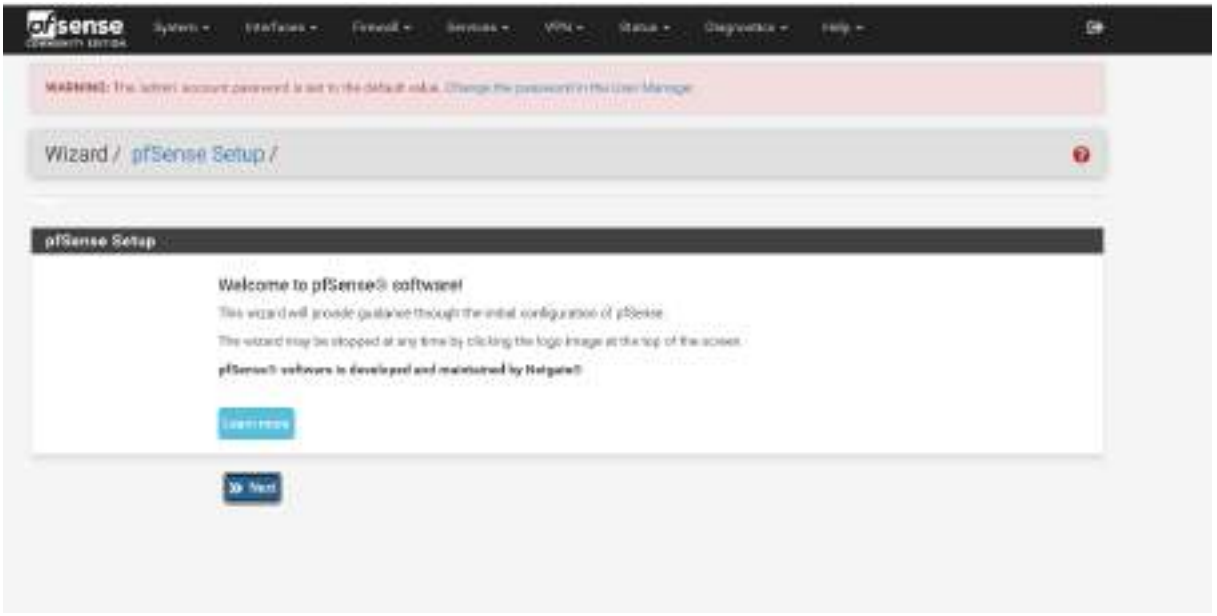
Faire de même avec l'interface LAN. Résultat :

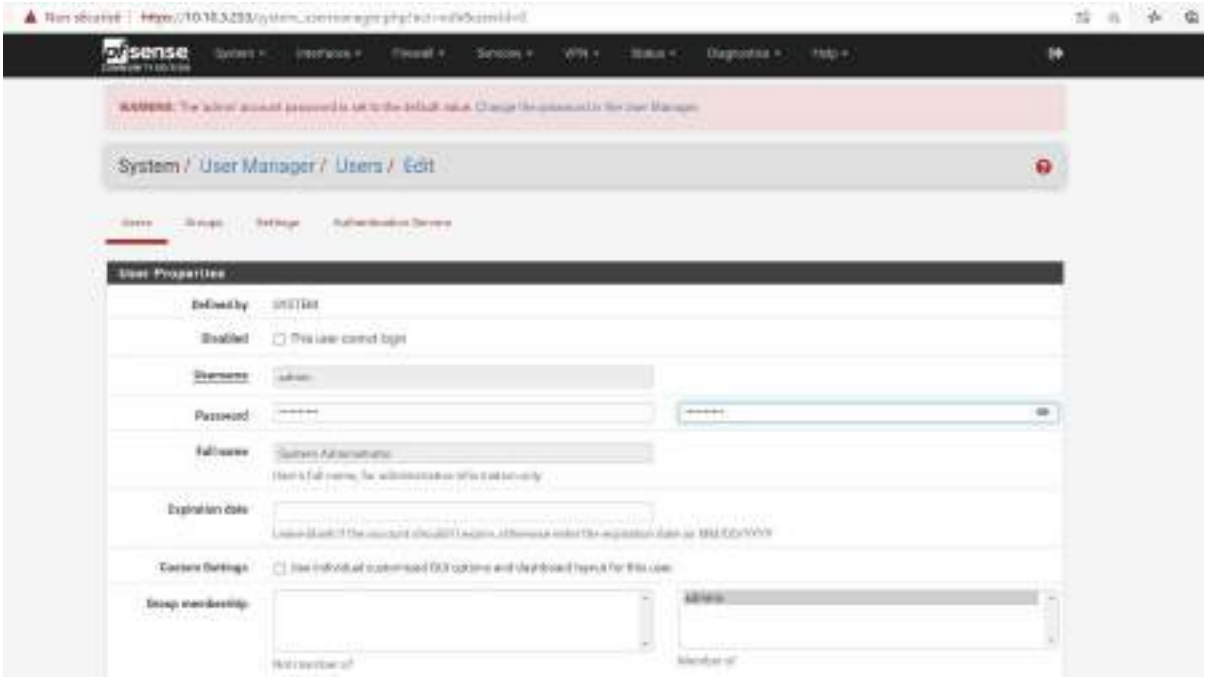
```
The IPv4 LAN address has been set to 10.10.1.253/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://10.10.1.253/

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: 25bf76fb0e7f3d9e25a1

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> le0        -> v4: 10.20.1.1/29
 LAN (lan)       -> le1        -> v4: 10.10.1.253/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: S
```

Aller sur un ordinateur/serveur dans le même réseau, sur un navigateur et entrer l'adresse IP LAN du PFSense pour accéder à la page de connexion, utiliser admin/pfsense en login :



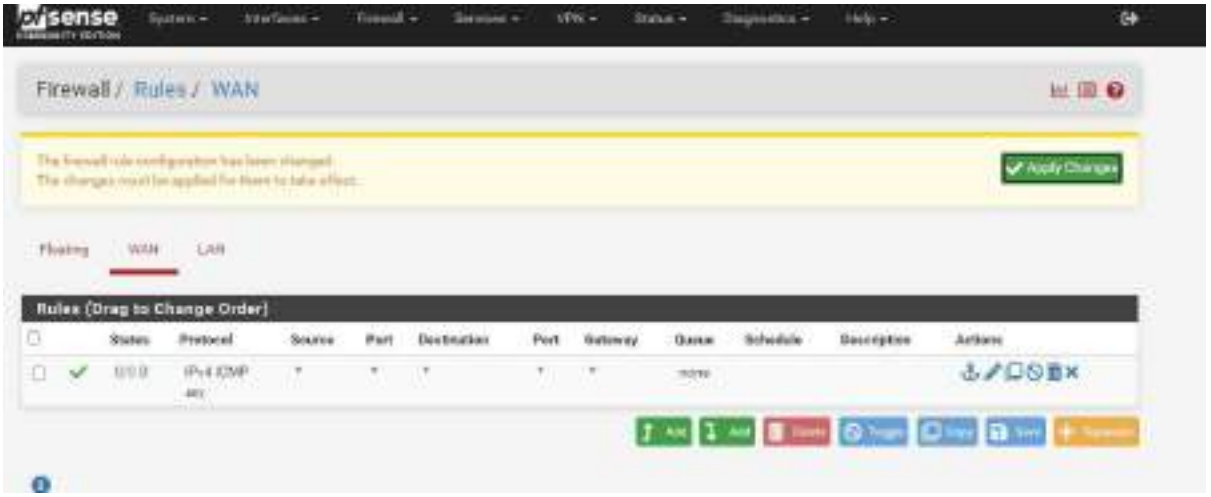
Cliquer sur « Change the password in the User Manager" et changer le mot de passe :





Aller dans Interface, WAN, défiler la dernière section intitulée Reserved Networks et désactiver Block private networks et Block bogon networks :

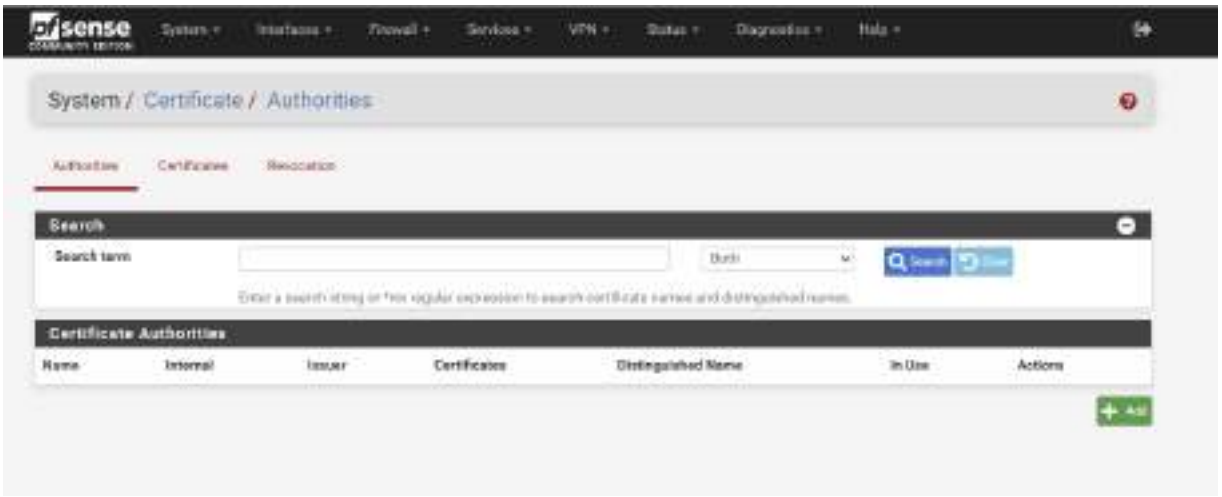
Pour tester si la connexion est bien possible entre les pfsense, rajouter pour le WAN dans Firewall, Rules, WAN, la règle IPv4 ICMP Any et faire un ping :



2. OpenVPN

a. Créer le certificat

Aller dans System, certificates, Authorities et cliquer sur Add :



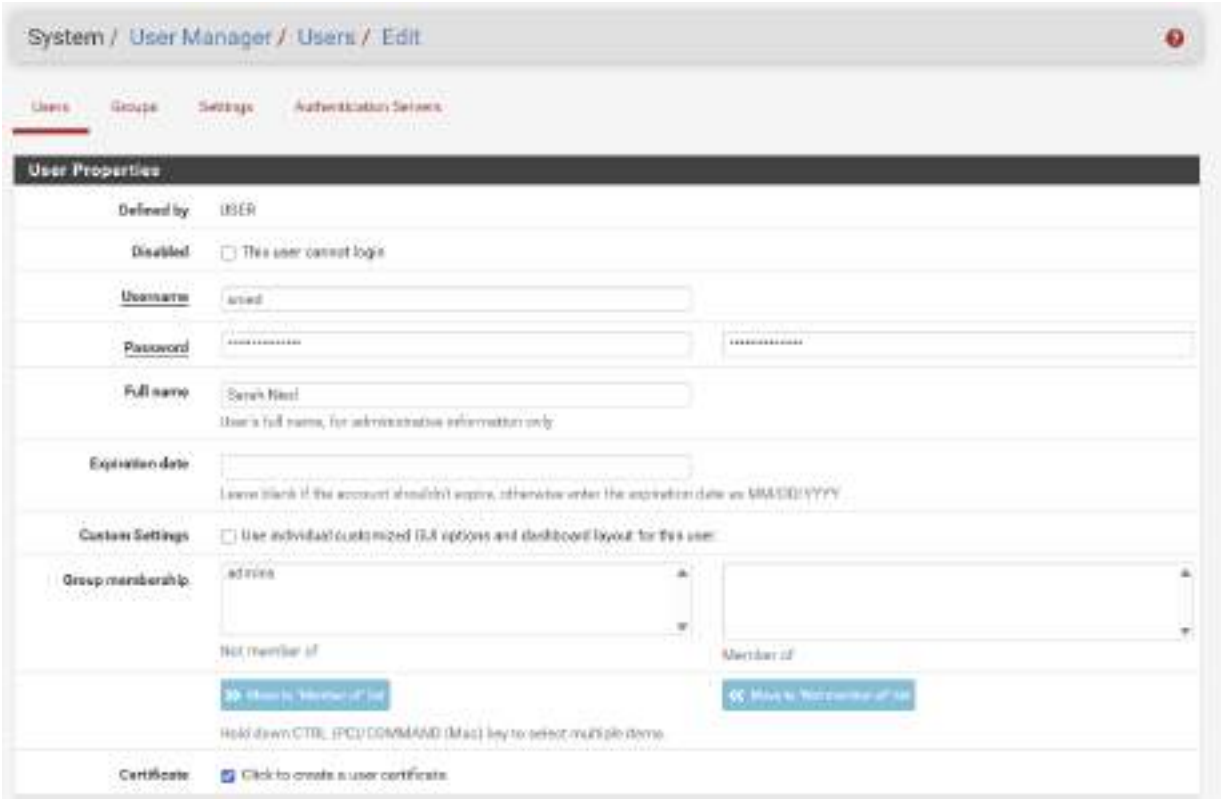
Renseigner les informations comme suit :

Résultat :

b. Créer les utilisateurs

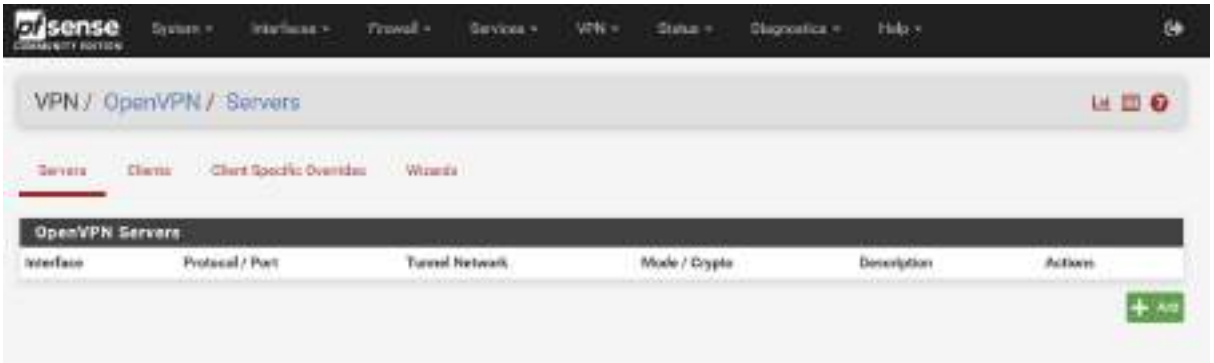
Aller dans System, User Manager, Users :

Cliquer sur Add, remplir les informations nécessaires et cocher Click to create a user certificate :

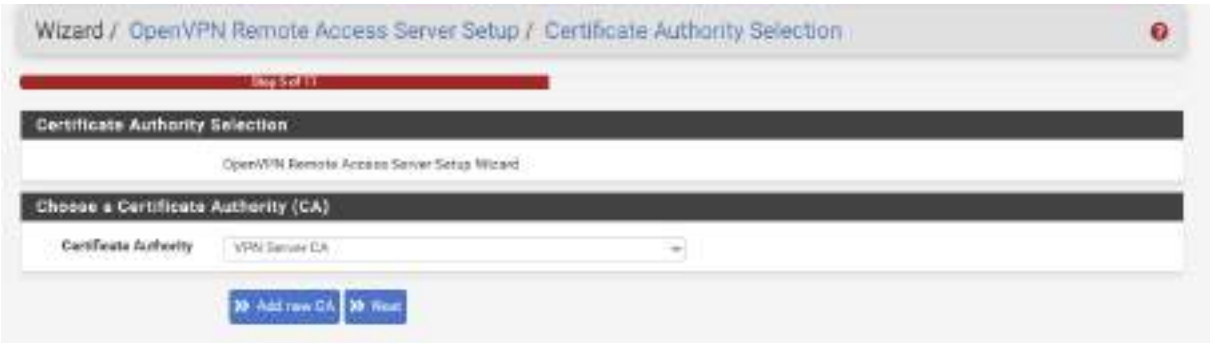


c. Création du serveur OpenVPN

Aller dans VPN, OpenVPN et cliquer sur Wizards :



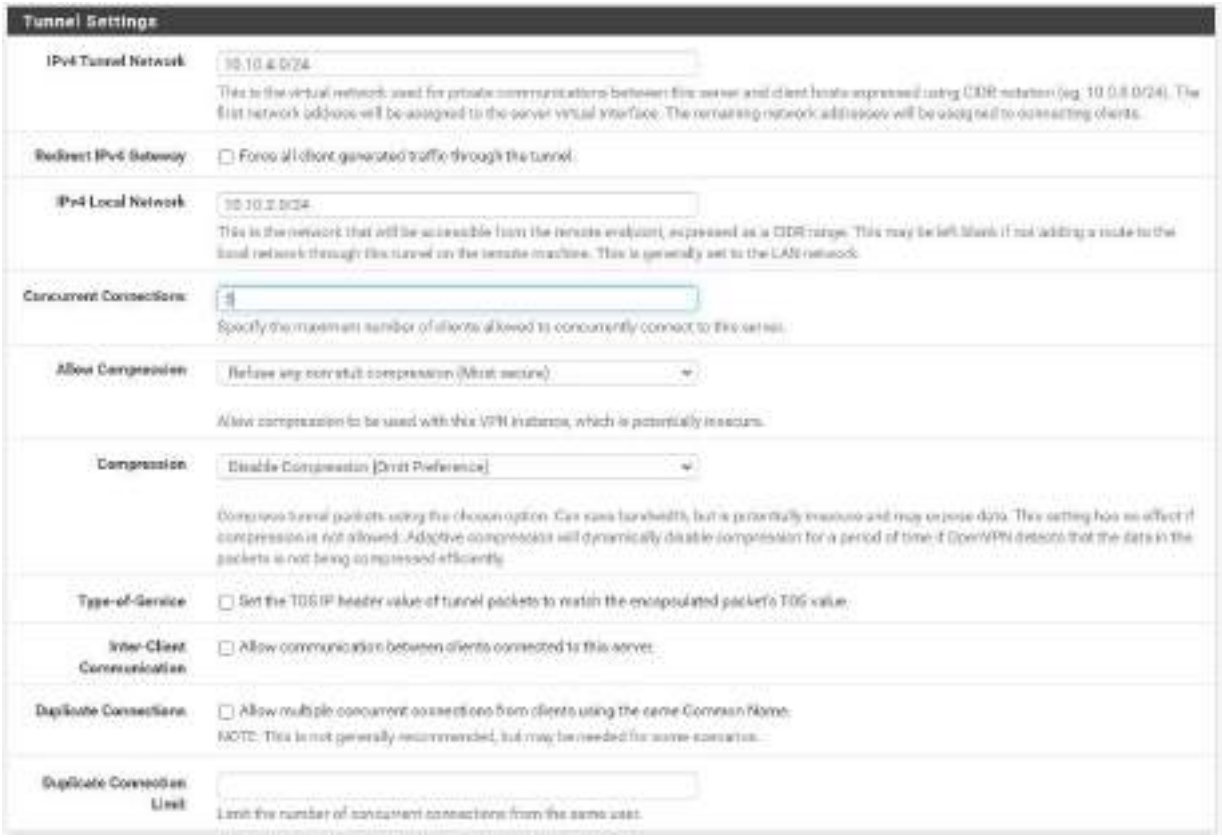
Suivre le wizard :



Ensuite cliquer sur Add new certificate :

Renseigner le nom :

Renseigner la partie Tunnel settings comme suit :



Indiquer l'adresse 10.10.2.254 en serveur DNS et faire next :

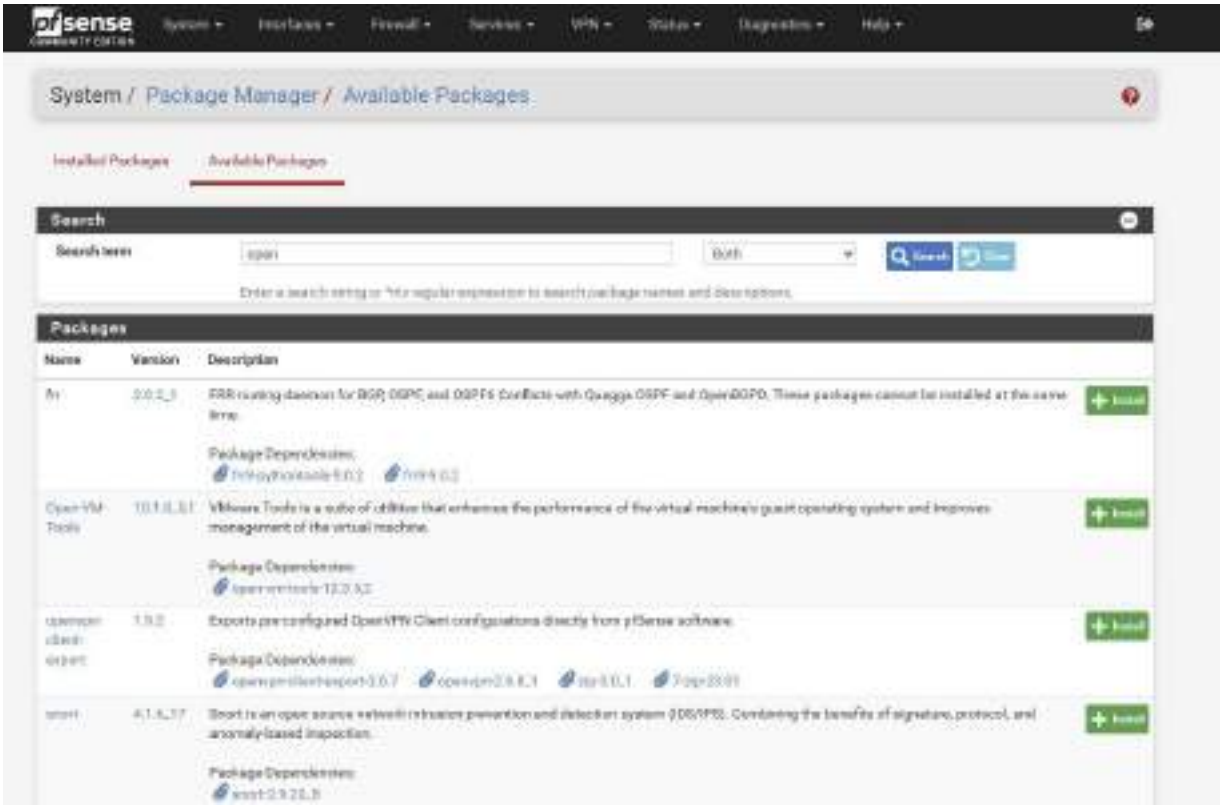
Cocher Firewall Rule et OpenVPN Rule:

Terminer le wizard:

Résultat:

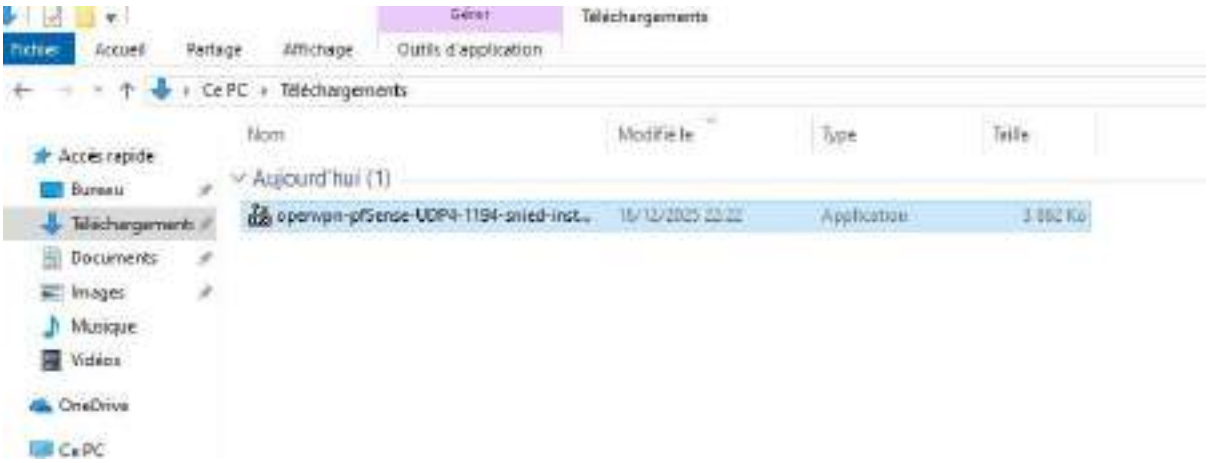
Ensuite vérifier que la règle concernant le VPN s'est bien créée dans Firewall, Rules, WAN :

Aller dans System, Package Manager, Available packages et installer openvpn-client-export en cliquant sur install :

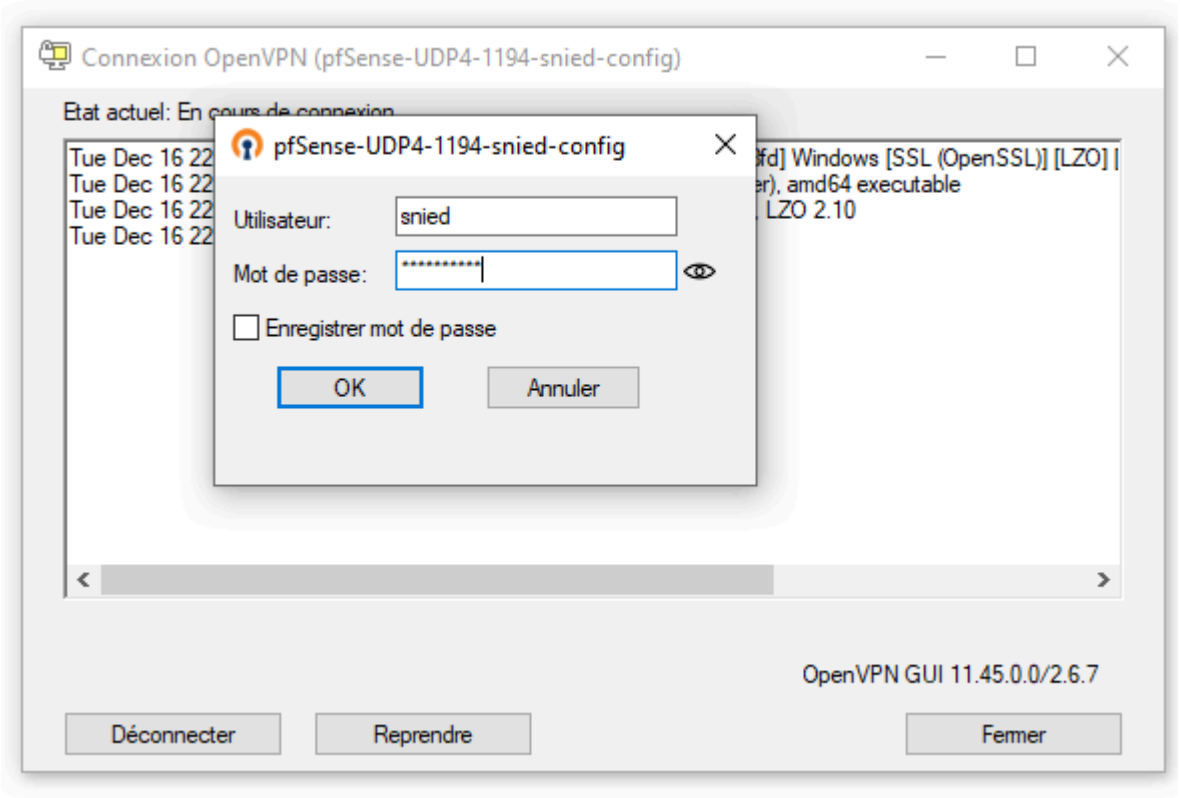


Ensuite aller dans VPN, OpenVPN, Client export et défiler jusqu'à OpenVPN Clients :

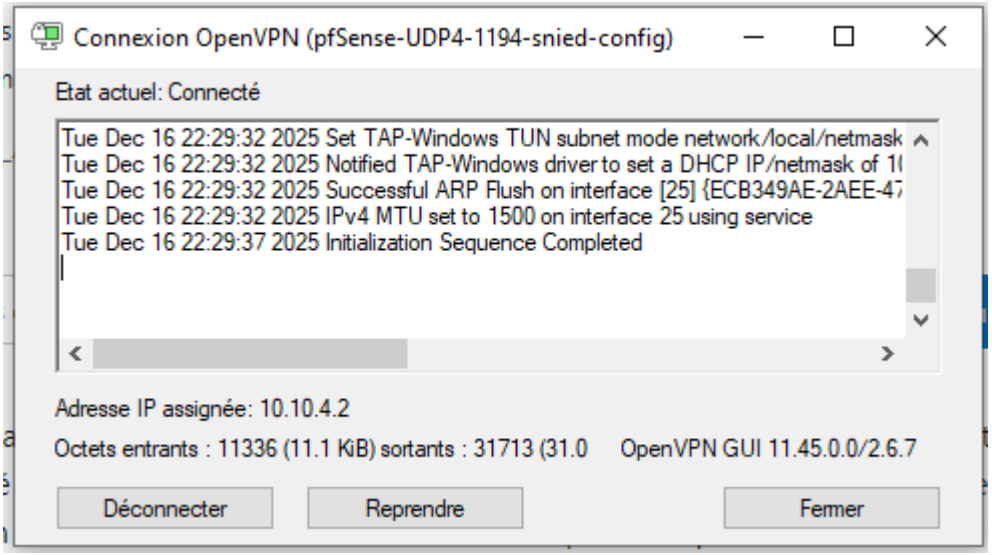
Télécharger le client adapté et l'installer sur le poste cible :



Une fois l'installation terminée, ouvrir OpenVPN GUI et renseigner les identifiants de connexion :



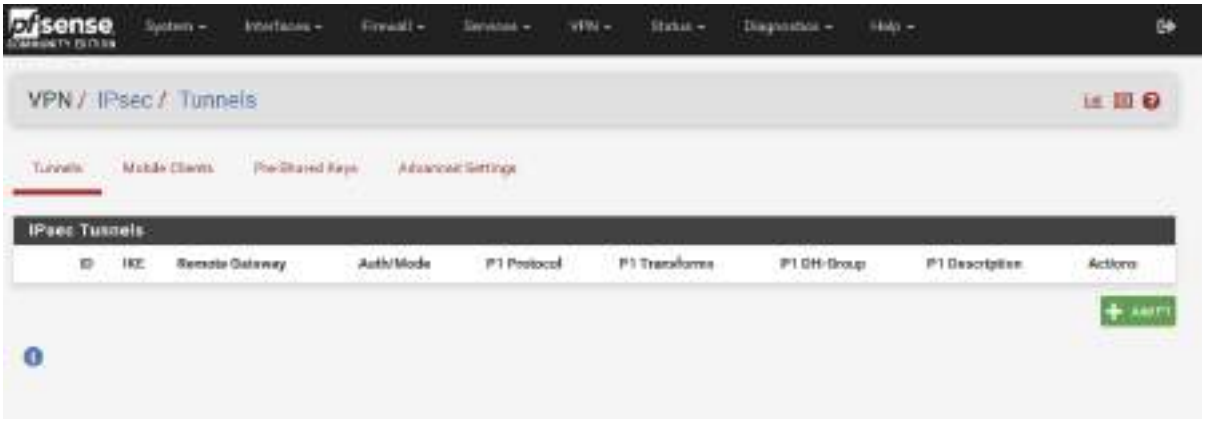
La connexion se fera alors :



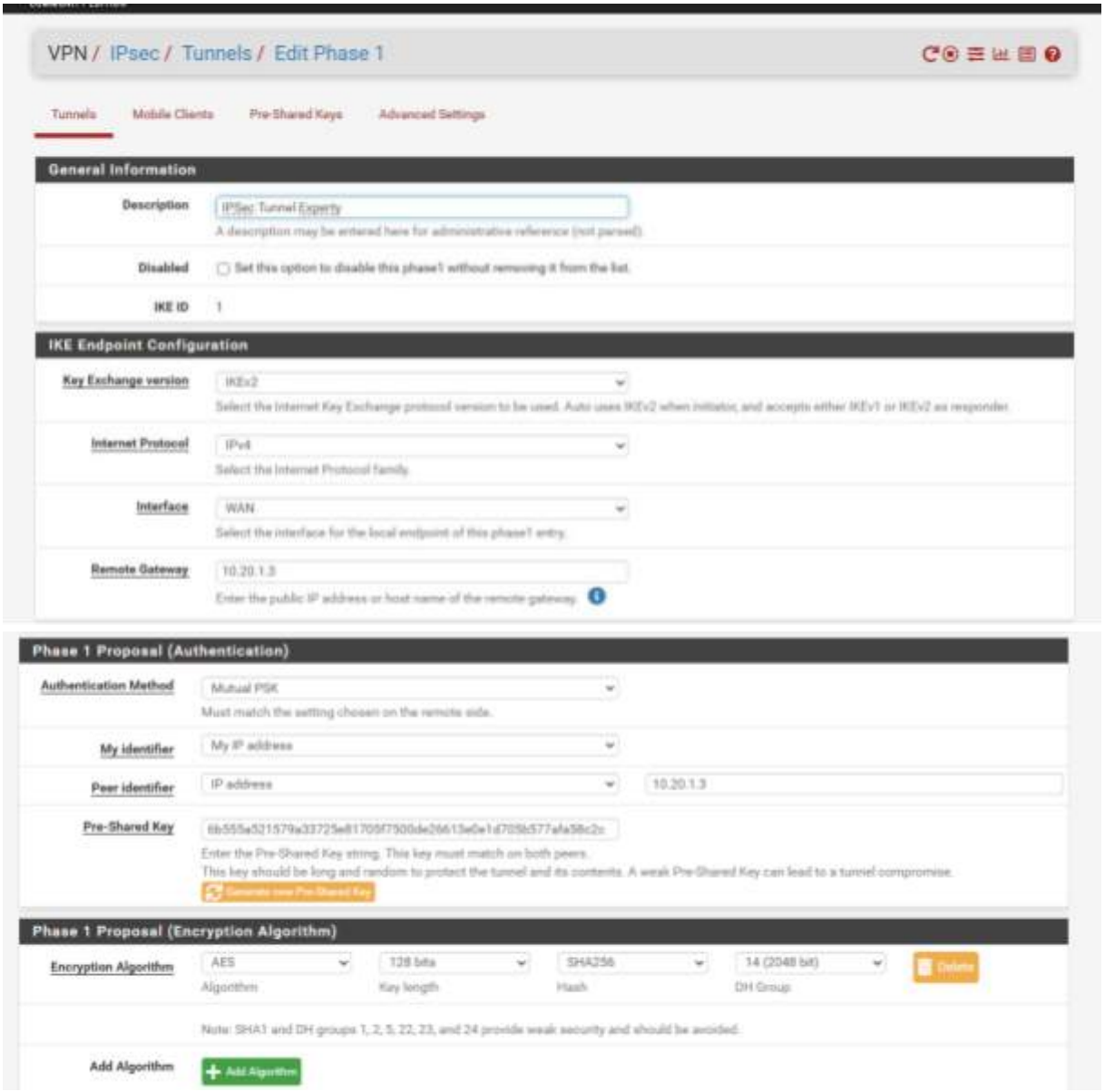
Le PC aura alors accès aux ressources du réseau spécifié lors de la création du VPN.

3. IPSec

Aller dans VPN, IPSec :

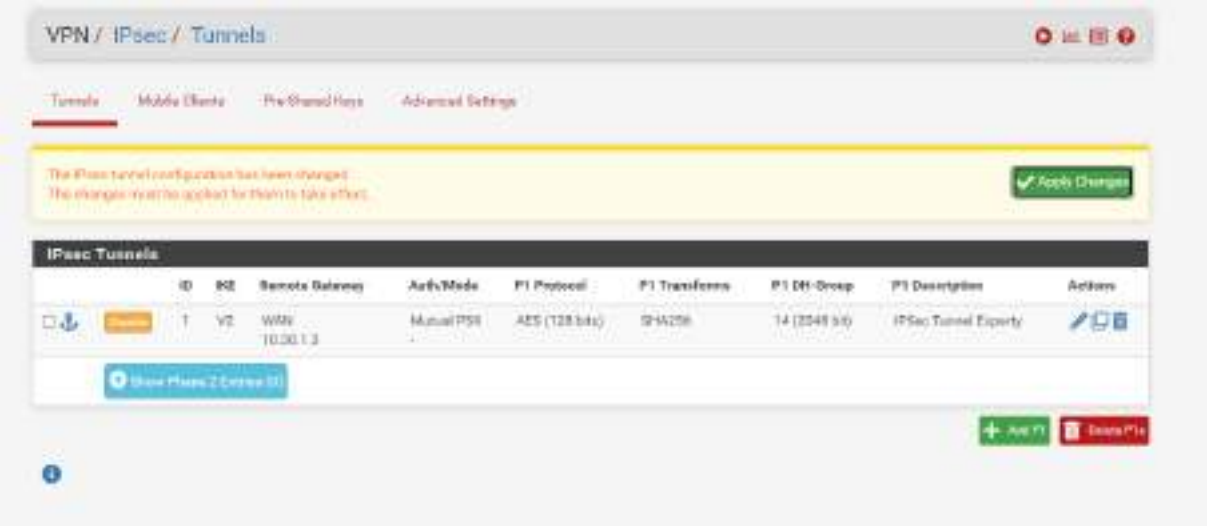


Le renseigner de la manière suivante en faisant bien attention aux adresses réseaux :

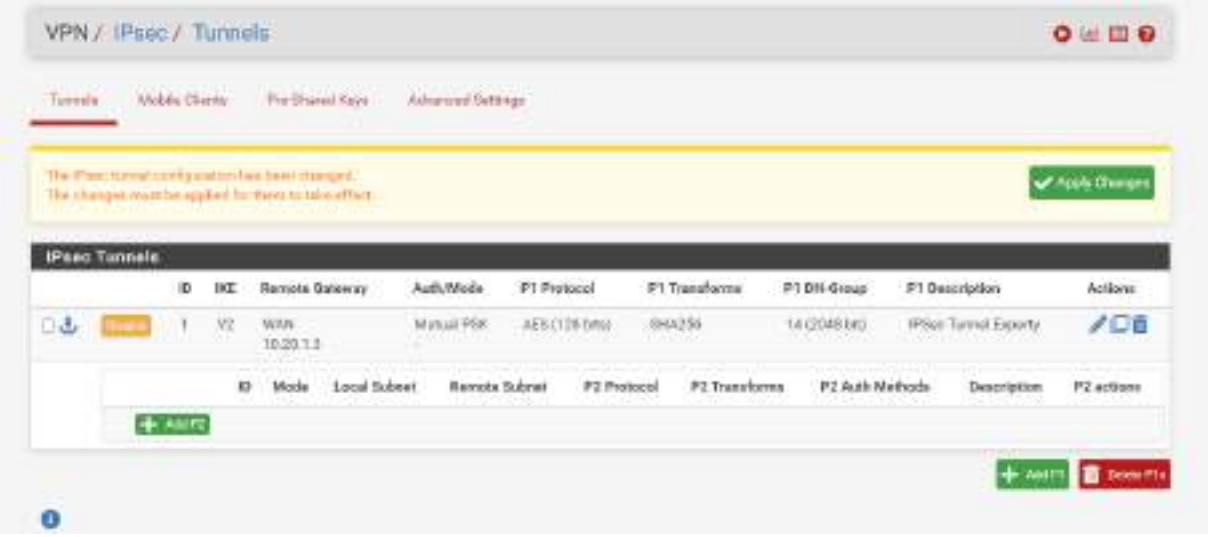


Copier la Pre-Shared Key pour l'utiliser lors de la création du P1 sur l'autre PFSense. Valider.

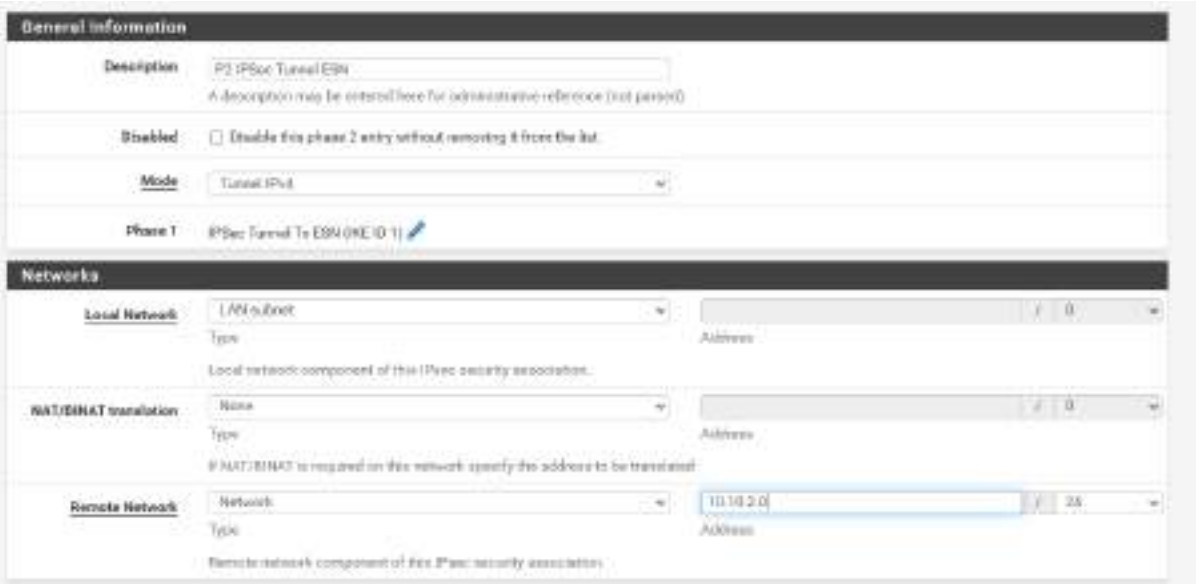
Retourner sur VPN, IPSec si ce n'est pas déjà le cas, puis cliquer sur Show Phase 2 Entries :



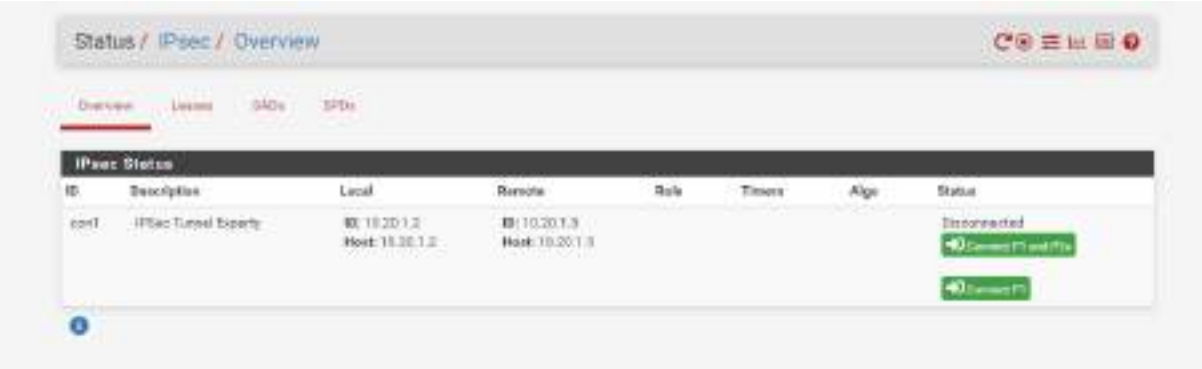
Ensuite cliquer Add P2 :



Renseigner les informations suivantes en faisant bien attention au réseau choisi :

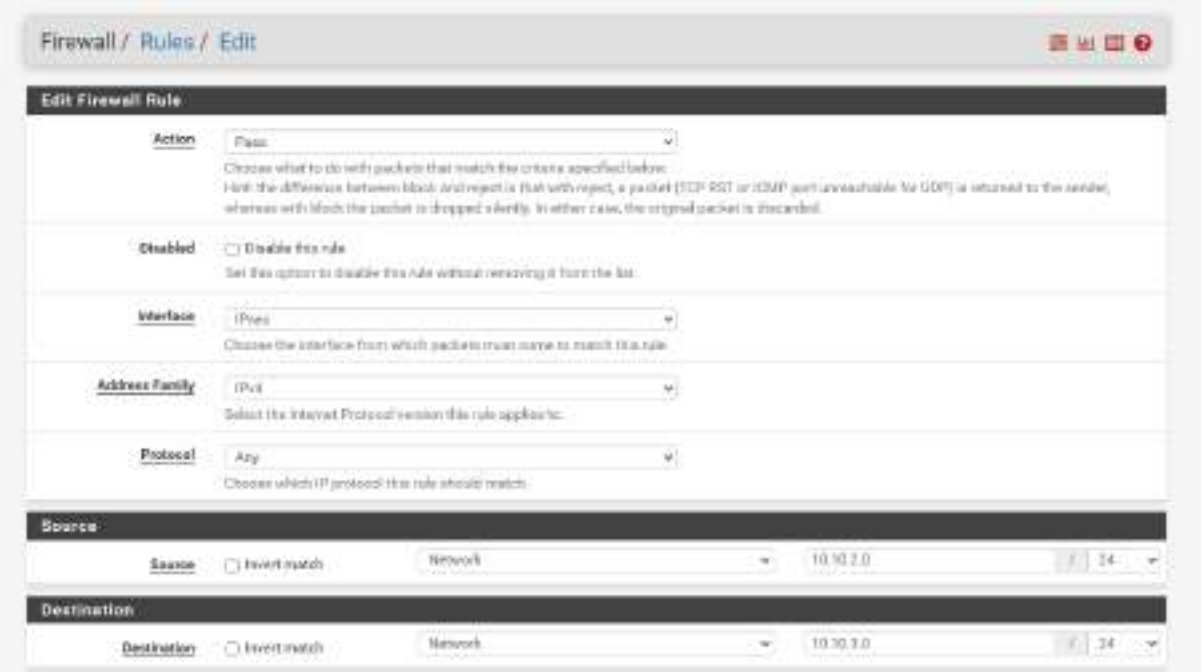


Valider et faire la même démarche sur l'autre PFSense. Puis aller dans Status, IPSec et cliquer sur Connect P1 and P2s :



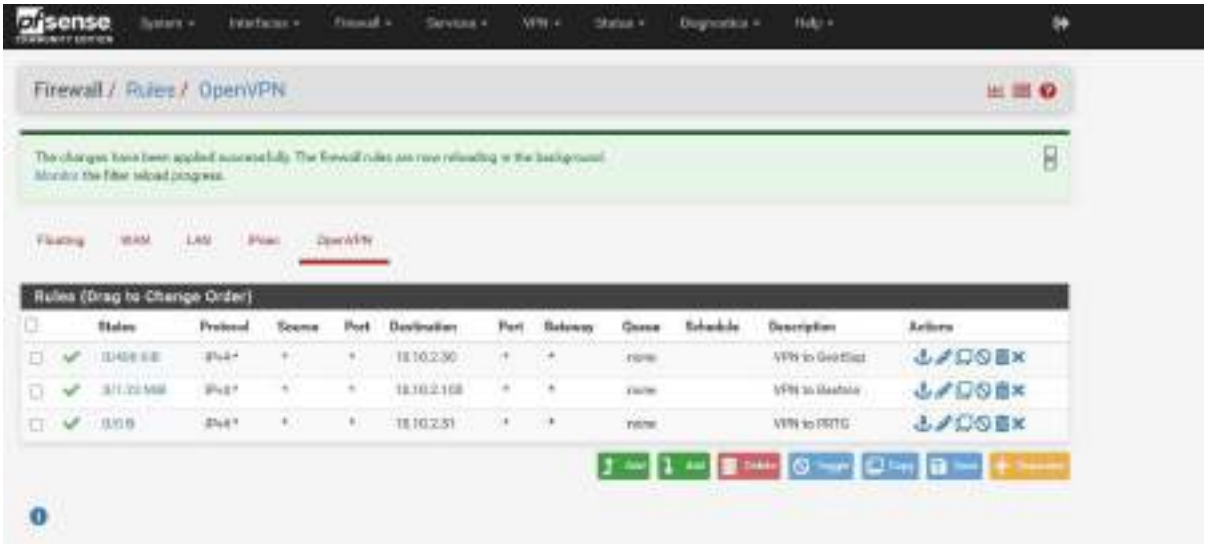
Le tunnel s'établit alors :

Aller dans Firewall, Rules et ajouter sur les deux Pfsense une règle permettant tout trafic d'un réseau à l'autre. Pour cela cliquer sur Add et renseigner la règle ainsi (en adaptant les réseaux) :



4. Ajuster les règles des Firewalls

Pour le Pfsense de l'ESN, aller dans Firewall, Rules, OpenVPN et renseigner des règles permettant le trafic vers chacun des serveurs qui doivent pouvoir être accessibles à partir du VPN, faire Add et renseigner la règle avec l'adresse de destination du serveur :



Pour le PFSense de Experty, aller dans Firewall, Rules, IPsec et créer une règle pour permettre le trafic du réseau de l'ESN vers le domaine controller :

B. **Linux GetSup**

1. Installation de GestSup

Installer une debian 12, la mettre à jour.

Soit faire une installation automatique en exécutant la commande : apt install curl -y && curl -s https://gestsup.fr/install.deb12.sh | bash

Ou alors faire une installation manuelle :

Installer les dépendances nécessaires :

apt install apache2 mariadb-server unzip curl ntp

cron -y apt install php libapache2-mod-php -y

apt install

php-{common,curl,gd,imap,intl,ldap,mbstring,mysql,xml,zip} -y

Créer l'utilisateur de la base de données dans MariaDB :

```
mariadb -u root
CREATE USER 'gestsup'@'localhost' IDENTIFIED BY
'password'; GRANT ALL PRIVILEGES ON *.* TO
'gestsup'@'localhost'; FLUSH PRIVILEGES;
exit
```

```
root@Debian:/home/debian# mariadb -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.14-MariaDB-0+deb12u2 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE USER 'gestsup'@'localhost' IDENTIFIED BY 'password';
Query OK, 0 rows affected (0,001 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON *.* TO 'gestsup'@'localhost';
Query OK, 0 rows affected (0,000 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,000 sec)

MariaDB [(none)]> exit
```

Faire mysql_secure_installation pour sécuriser la base de données :

```
root@Debian:/home/debian# mysql_secure_installation

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
haven't set the root password yet, you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password or using the unix_socket ensures that nobody
can log into the MariaDB root user without the proper authorisation.

You already have your root account protected, so you can safely answer 'n'.

Switch to unix_socket authentication [Y/n] n
 ... skipping.

You already have your root account protected, so you can safely answer 'n'.

Change the root password? [Y/n] n
 ... skipping.

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them.  This is intended only for testing, and to make the installation
go a bit smoother.  You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
 ... Success!

Normally, root should only be allowed to connect from 'localhost'.  This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
 ... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access.  This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
 - Dropping test database...
 ... Success!
 - Removing privileges on test database...
 ... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.
```

Aller dans nano /etc/php/8.2/apache2/php.ini et modifier les paramètres suivants :

max_execution_time = 480

memory_limit = 512M

upload_max_filesize = 8M

date.timezone =

Europe/Paris

```
; Maximum execution time of each script, in seconds
; https://php.net/max-execution-time
; Note: This directive is hardcoded to 0 for the CLI SAPI
max_execution_time = 480
```

```
; Maximum amount of memory a script may consume
; https://php.net/memory-limit
memory_limit = 512M
```

```
; Maximum allowed size for uploaded files.
; https://php.net/upload-max-filesize
upload_max_filesize = 8M
```

```
[Date]
; Defines the default timezone used by the date functions
; https://php.net/date.timezone
;date.timezone = Europe/Paris
```

Puis modifier le fichier de configuration MariaDB nano /etc/mysql/mariadb.conf.d/50-server.cnf en modifiant ceci, sachant que pour le innodb, cela doit représenter minimum 25% de la RAM du serveur :

innodb_buffer_pool_size =
1G skip-name-resolve

```
#
# * InnoDB
#

# InnoDB is enabled by default with a 10MB datafile in /var/lib/mysql/.
# Read the manual for more InnoDB related options. There are many!
# Most important is to give InnoDB 80 % of the system RAM for buffer use:
# https://mariadb.com/kb/en/innodb-system-variables/#innodb_buffer_pool_size
innodb_buffer_pool_size = 1G
```

```
# Broken reverse DNS slows down connections considerably and name resolve is
# safe to skip if there are no "host by domain name" access grants
skip-name-resolve
```

Télécharger le fichier zip de GestSup : wget -P /var/www/html https://gestsup.fr/downloads/versions/current/version/gestsup_3.2.55.zip (ne pas oublier d'ajuster le numéro de version à celle voulue)

Dézipper le fichier : unzip /var/www/html/gestsup_3.2.55.zip -d

/var/www/html Une fois le fichier dézippé, supprimer le fichier zip et

l'index par défaut :

rm
/var/www/html/gestsup_3.2.55.zip
rm /var/www/html/index.html

Ajouter l'utilisateur gestsup avec son mot de passe : adduser gestsup

--ingroup www-data (si le debian renvoie adduser : command not found, faire export PATH="$PATH:/sbin:/usr/sbin:usr/local/sbin" et la commande marchera)

Puis modifier les droits :

chown -R gestsup:www-data /var/www/html/
find /var/www/html/ -type d -exec chmod 750 {} \; find /var/www/html/ -type f -exec chmod 640 {} \; chmod 770 -R /var/www/html/upload
chmod 770 -R /var/www/html/images/model chmod 770 -R /var/www/html/backup chmod 770 -R /var/www/html/_SQL
chmod 660 /var/www/html/connect.php

Attribuer une adresse statique à la vm en allant dans /etc/network/interfaces : allow-hotplug ens37
iface ens37 inet static
address 10.10.2.100/24
gateway 10.10.2.253

Redémarrer le service networking : systemctl restart networking et vérifier en faisant ip a que l'adresse IP a bien été prise en compte.

Ensuite aller sur l'adresse IP/install et suivre l'installateur, bien mettre l'utilisateur gestsup et son mot de passe (ici password) comme utilisateur:

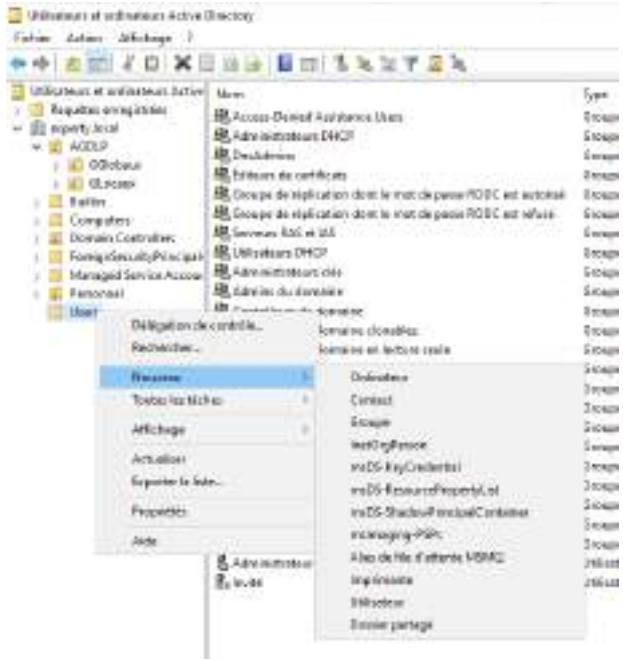
Ensuite supprimer le répertoire install : rm -rf /var/www/html/install/

Se connecter à l'adresse IP du serveur avec le mot de passe indiqué à la fin de l'installation, puis un pop-up s'ouvre pour demander de changer le mot de passe :

2. Ajouter le connecteur LDAP pour la connexion à l'Active Directory

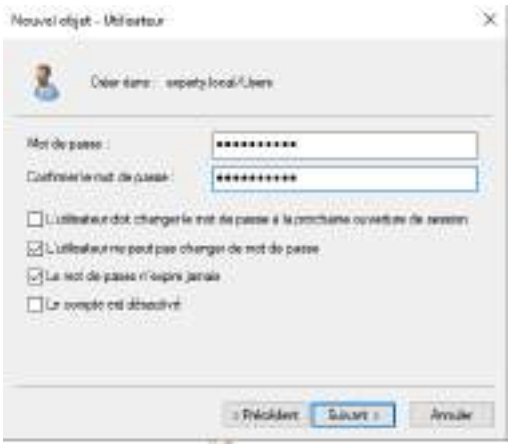
a. Créer un compte dédié pour Gestsup dans l'Active Directory Aller sur le DC et ouvrir Utilisateurs et ordinateurs Active Directory :

Dérouler experty.local et faire un clic droit sur Users, Nouveau, et cliquer sur Utilisateur :



Renseigner les informations suivantes :

Renseigner le mot de passe, décocher l'utilisateur doit changer et cocher L'utilisateur ne peut pas changer de mot de passe et Le mot n'expire jamais :



Admin.202212

Récupérer le Distinguished Name de cet utilisateur, soit en faisant Affichage, Fonctionnalités Avancées, clic droit sur l'utilisateur, Propriétés, Editeurs d'attributs, distinguishedName, soit en allant sur Powershell et faire cette commande :

```
Get-ADUser -Identity gestsup-ldap | Select-Object
```

DistinguishedName Résultat: CN=GestSup,CN=Users,DC=experty,DC=local

Pour vérifier si le compte marche bien et que la connexion est bien établie, faire apt install ldap-utils -y puis :

```
ldapsearch -x -H ldap://10.10.3.10:389 -D
"CN=GestSup,CN=Users,DC=experty,DC=local"
-w "Admin.202212"                    -b "DC=experty,DC=local"

CN=GestSup Service Account,OU=SVC,OU=Experty,DC=experty,DC=local
```

b. Ajout du connecteur LDAP

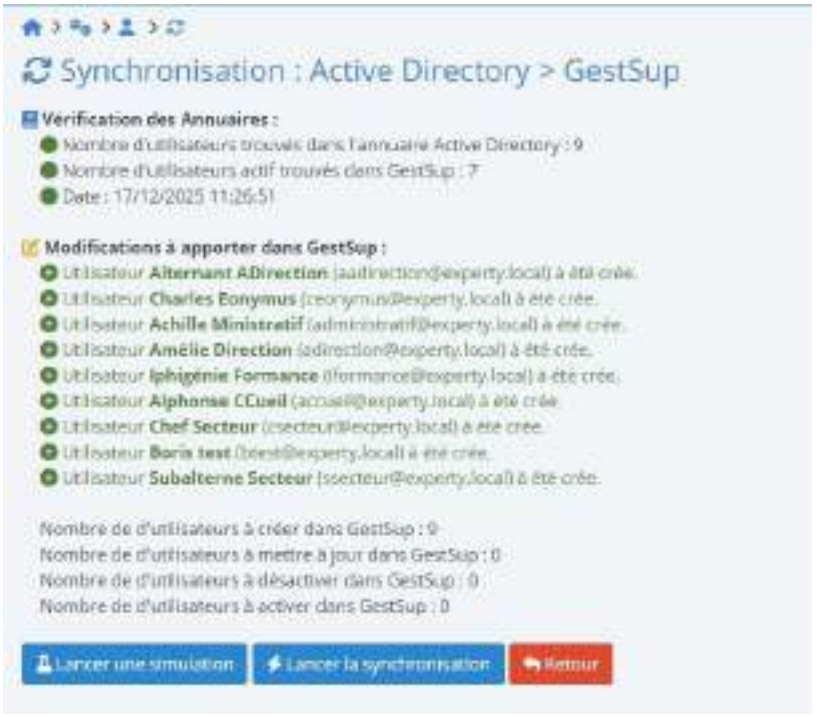
Ensuite retourner sur GestSup, aller dans Administration, Paramètres, Connecteurs, LDAP et renseigner les informations suivantes (bien vérifier dans quelle OU se situent les employés) :

Cliquer sur Test du connecteur LDAP pour vérifier que tout est fonctionnel :

Puis cliquer sur valider.

c. Synchronisation de l'Active Directory

Ensuite aller dans Administration, Utilisateurs et cliquer sur Synchronisation LDAP :



Les utilisateurs peuvent désormais se connecter avec les identifiants de l'Active Directory de Experty. Attention, le serveur AD doit pouvoir être constamment joignable.

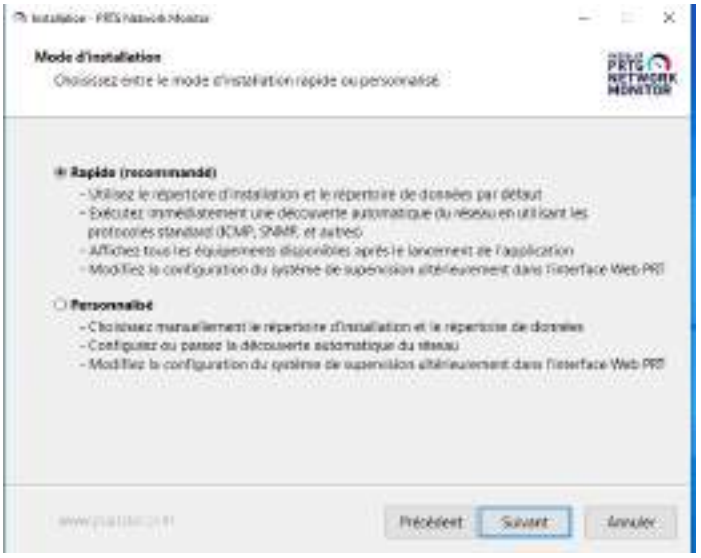
C. **PRTG**

Installer un windows server 2022 et lui attribuer une adresse statique, puis aller sur Download and Install et télécharger PRTG :

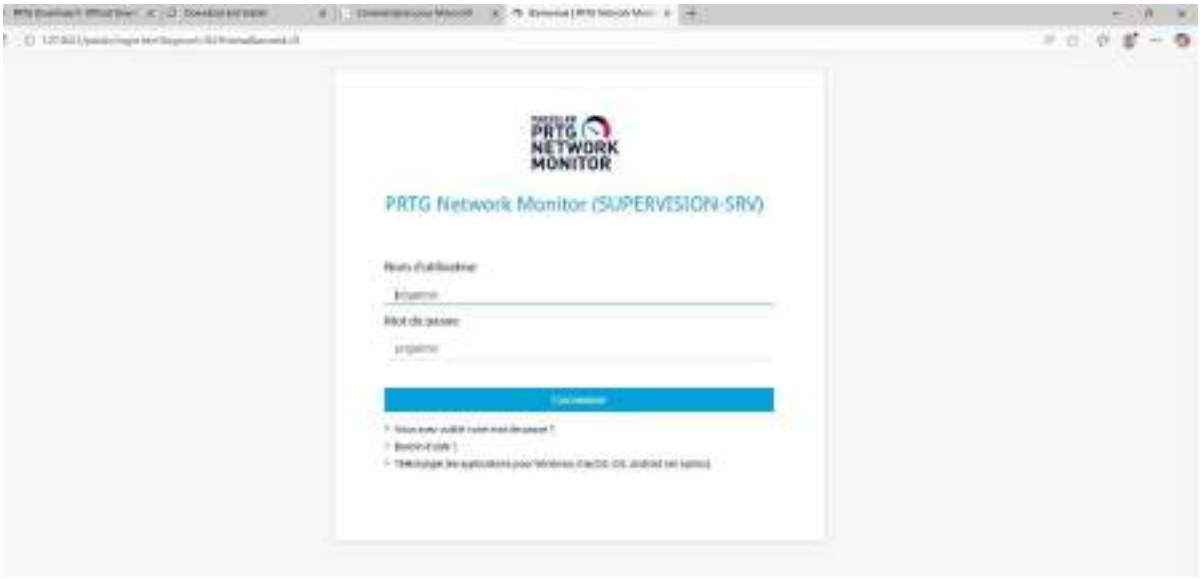
Noter la clé de licence et son nom :

Puis lancer l'assistant d'installation :

Suivre l’installateur et choisir Rapide en mode d’installation :

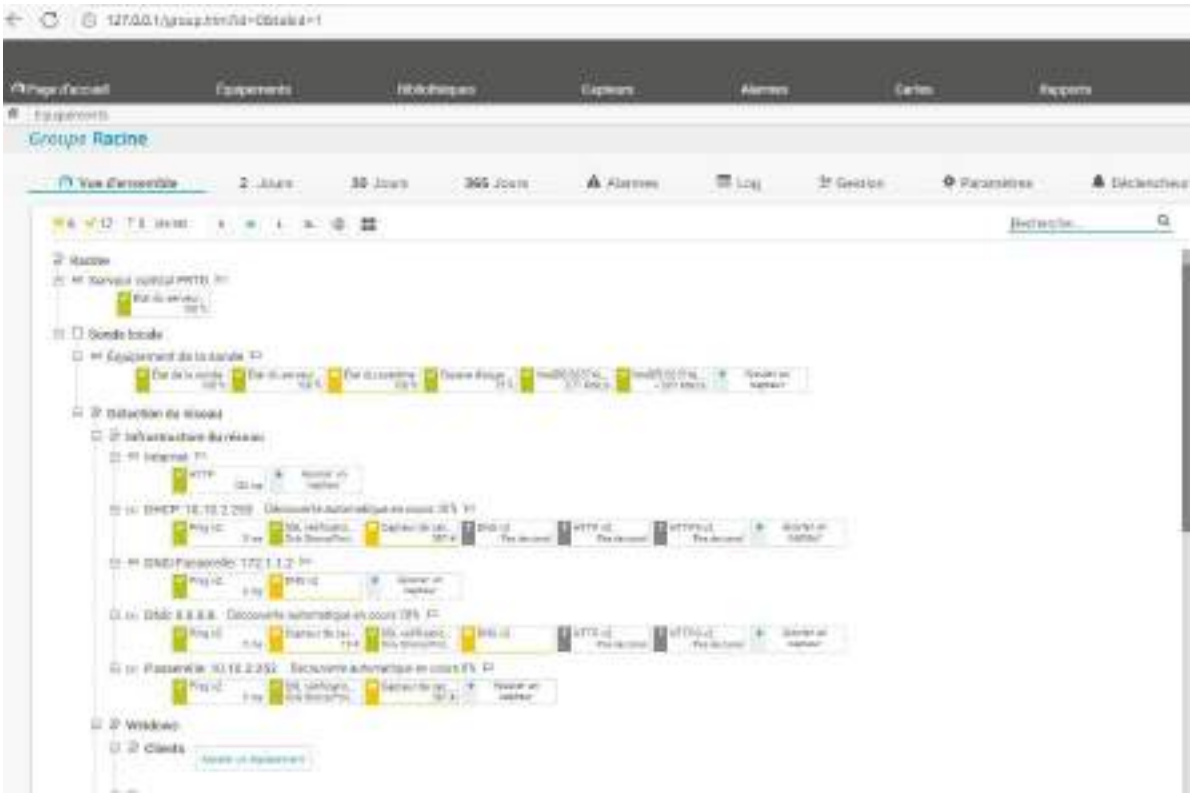


L’installation se poursuit toute seule et se termine en ouvrant cette page :



Faire connexion après avoir modifié le mot de passe pour accéder à la page d'accueil :

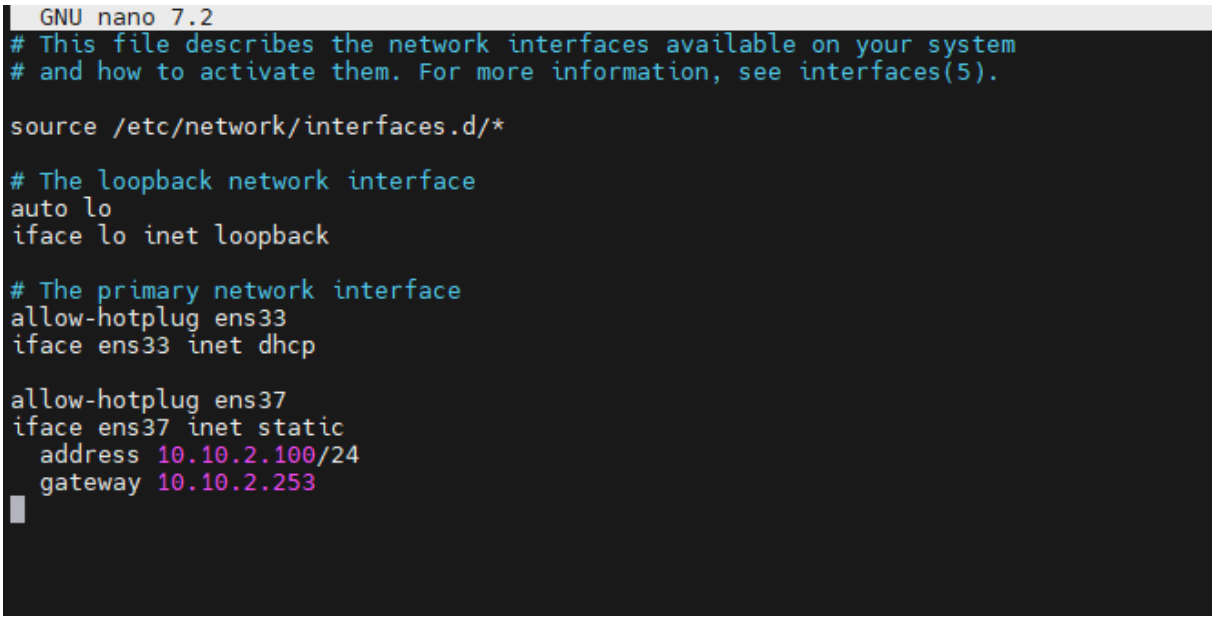
Aller sur Equipements pour voir la carte réseau avec les différents équipements détectés par PRTG :



D. **Bastion Teleport**

1. Installation de Teleport

Installer une debian 12 et lui assigner une adresse IP statique en faisant nano /etc/network/interfaces :



allow-hotplug ens37
iface ens37 inet static
address 10.10.2.100/24
gateway 10.10.2.253
dns-nameserver

10.10.2.253 Faire apt-get install

resolvconf.

Redémarrer le networking : systemctl restart

networking Ensuite créer un répertoire teleport dans

lequel tout sera mis :

mkdir -p
/var/lib/teleport cd
/var/lib/teleport

Puis générer une clé privée : openssl genrsa -out privkey.pem 2048

Ensuite créer un fichier de configuration OpenSSL nano cert_config.cnf et y coller ceci en adaptant le nom de domaine et l'adresse IP:

[req]
default_bits = 2048
prompt = no
default_md =

```
sha256
distinguished_name = dn
req_extensions = v3_req
```

[dn]
C = FR
ST = Grand Est
L = Strasbourg
O = ESN
CN = teleport.esn.local

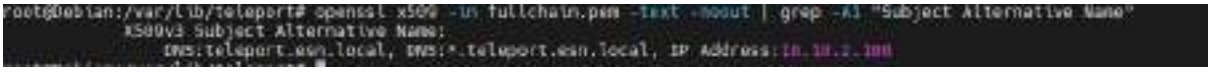
[v3_req]
subjectAltName = @alt_names

[alt_names]
DNS.1 = teleport.esn.local
DNS.2 = *.teleport.esn.local
IP.1 = 10.10.2.100

Puis générer le certificate openssl:

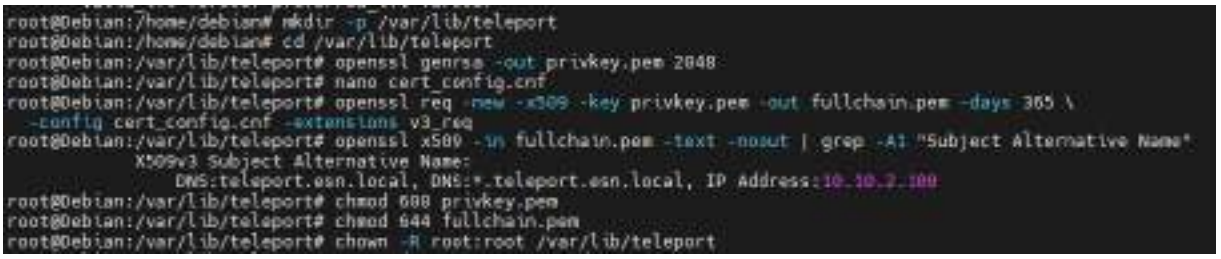
```
openssl req -new -x509 -key privkey.pem -out fullchain.pem -days 365 \
  -config cert_config.cnf -extensions v3_req
```

Pour verifier si le certificat s'est bien généré : openssl x509 -in fullchain.pem -text - noout | grep -A1 "Subject Alternative Name"

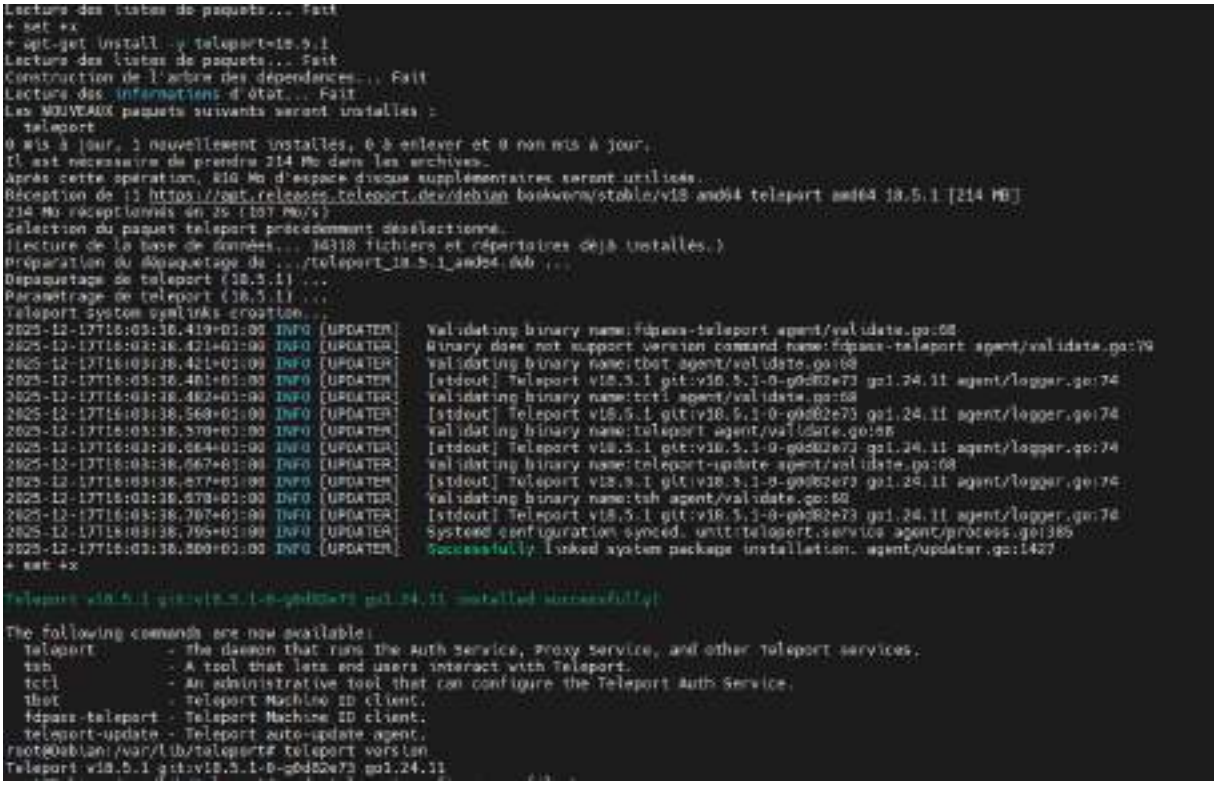


Ensuite accorder les bons droits :

```
chmod 600 privkey.pem
chmod 644 fullchain.pem
chown -R root:root /var/lib/teleport
```

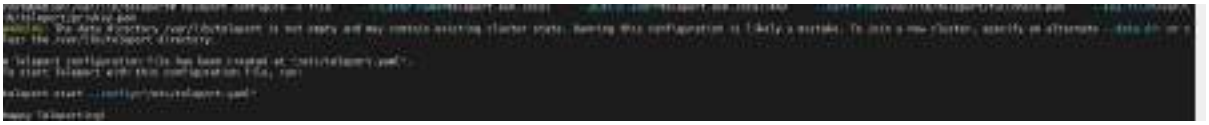


Puis télécharger teleport: wget -O- https://cdn.teleport.dev/install.sh | bash -s 18.5.1



Ensuite faire:

teleport configure -o file --cluster-name=teleport.esn.local
--public-addr=teleport.esn.local:443
--cert-file=/var/lib/teleport/fullchain.pem
--key-file=/var/lib/teleport/privkey.pem

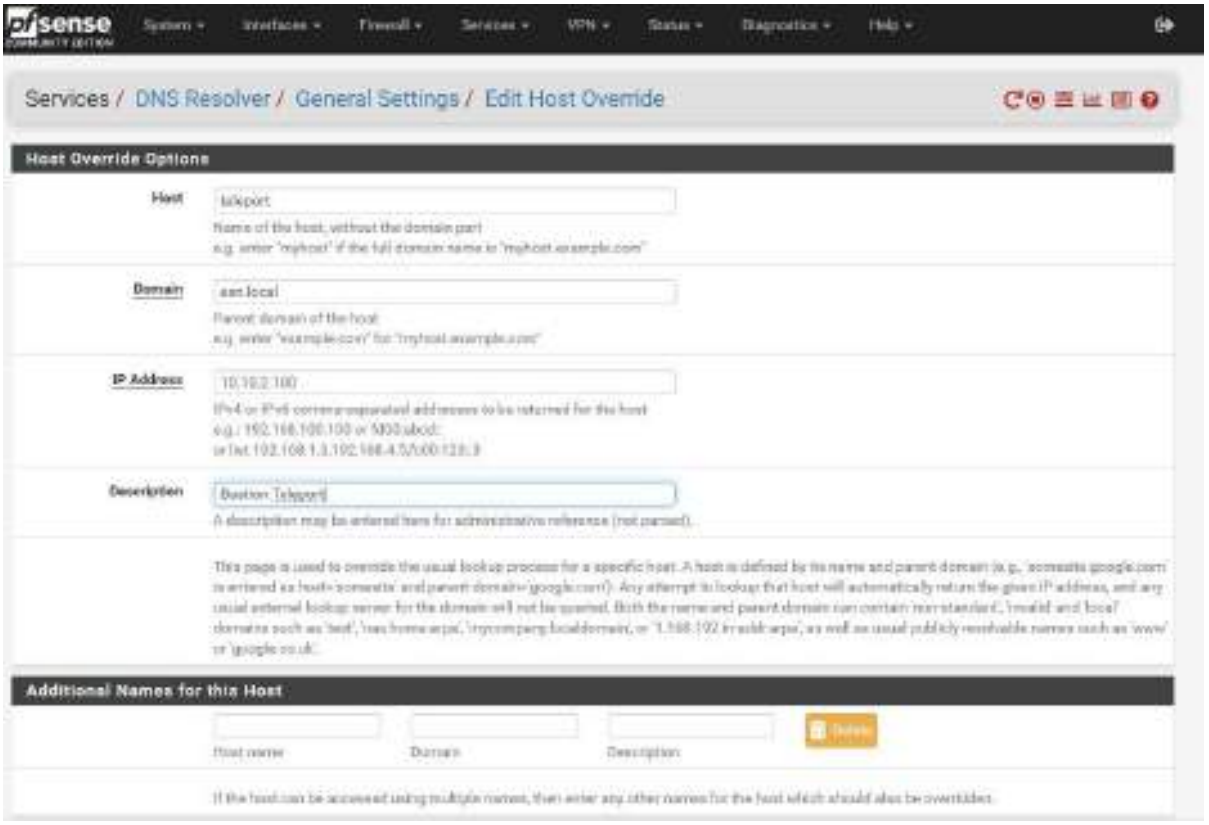


Puis démarrer le service teleport :

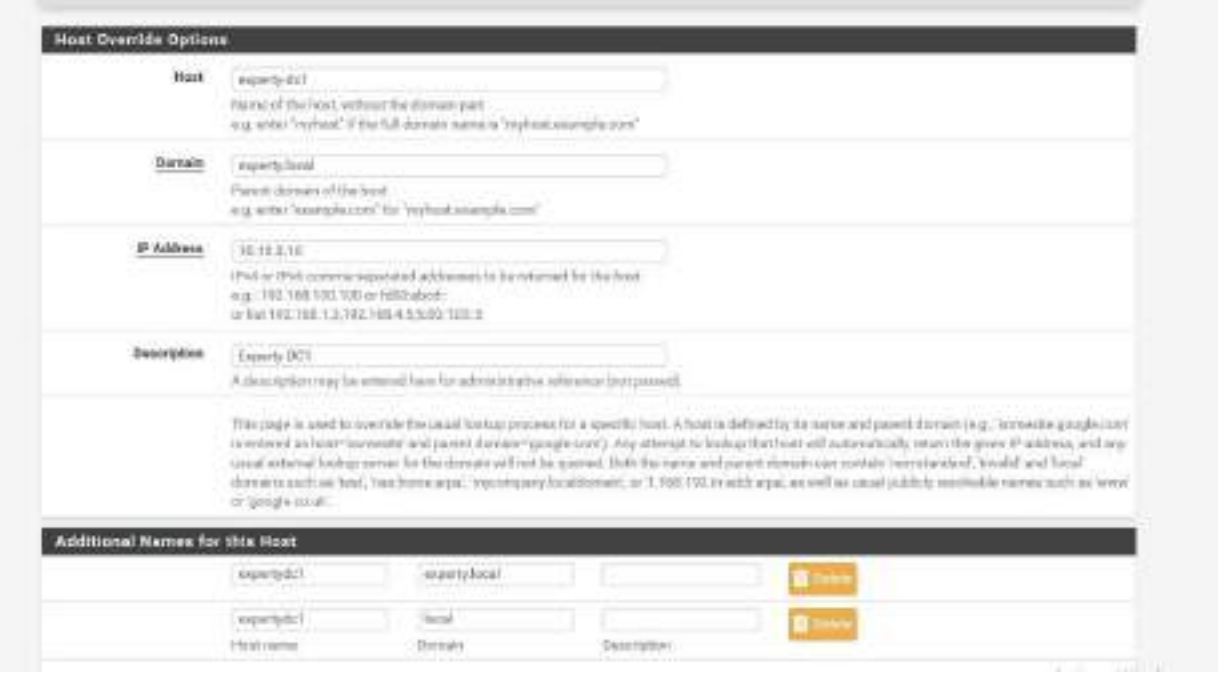
2. Ajout du nom de l'hôte dans le DNS

Sur PFSense, cliquer sur Services, DNS Resolver, défiler jusqu'à Host Override et cliquer sur Add :

Puis renseigner de la façon suivante :



Faire de même pour expertydc1.experty.local avec en alias expertydc1.local :



Vérifier que teleport fonctionne en allant sur teleport.esn.local :

Si une page blanche est la seule chose qui s'affiche, vérifier que Edge est à jour, minimum au-dessus de 110 pour la version.

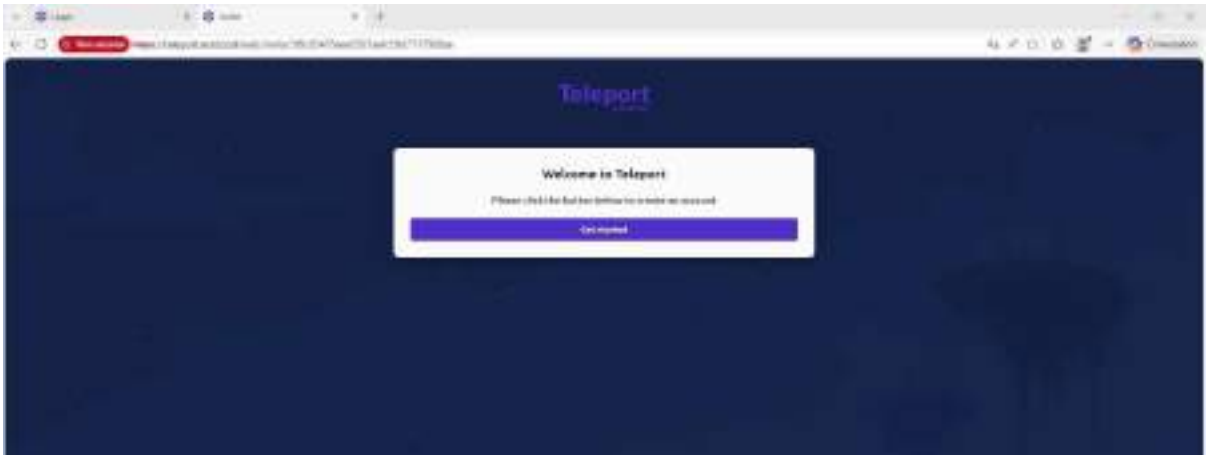
Vérifier que la debian teleport peut bien ping expertydc.experty.local.

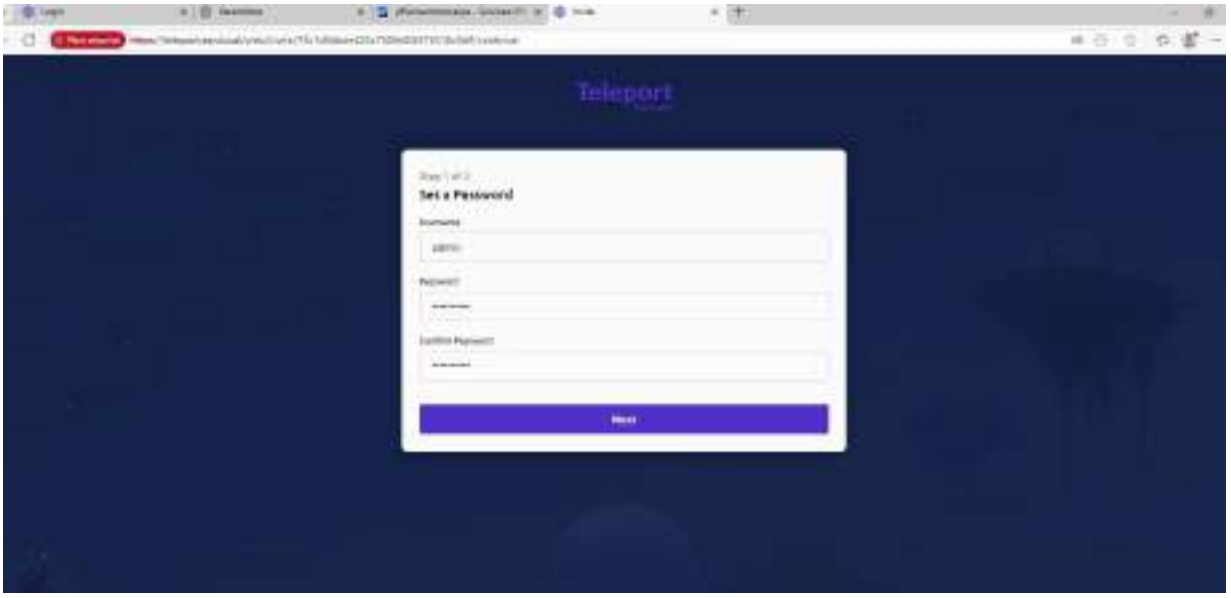
3. Création du compte administrateur Créer un utilisateur Teleport en faisant

```
tctl users add admin \
  --roles=editor,access \
  --logins=root,debian
```

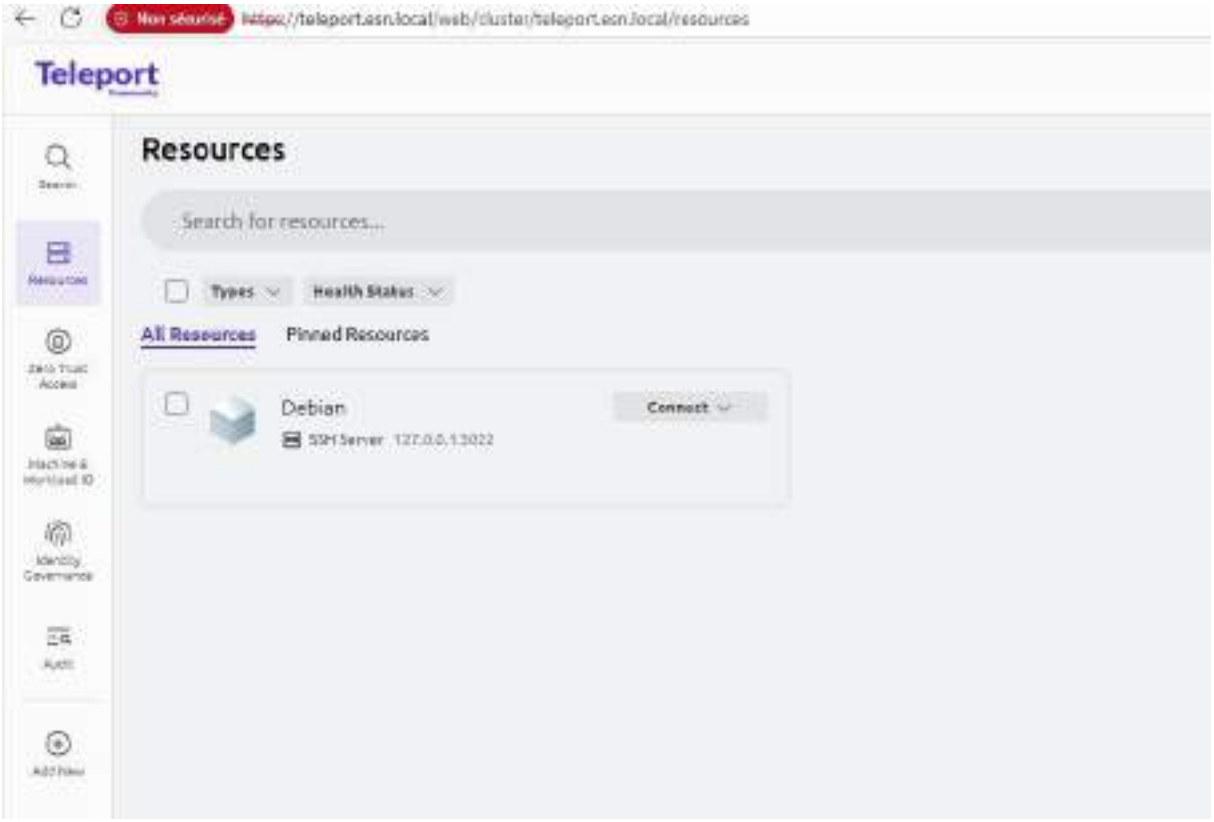
Cela fera un message comprenant un lien permettant de compléter la création du compte de l'utilisateur :

Le suivre et compléter :





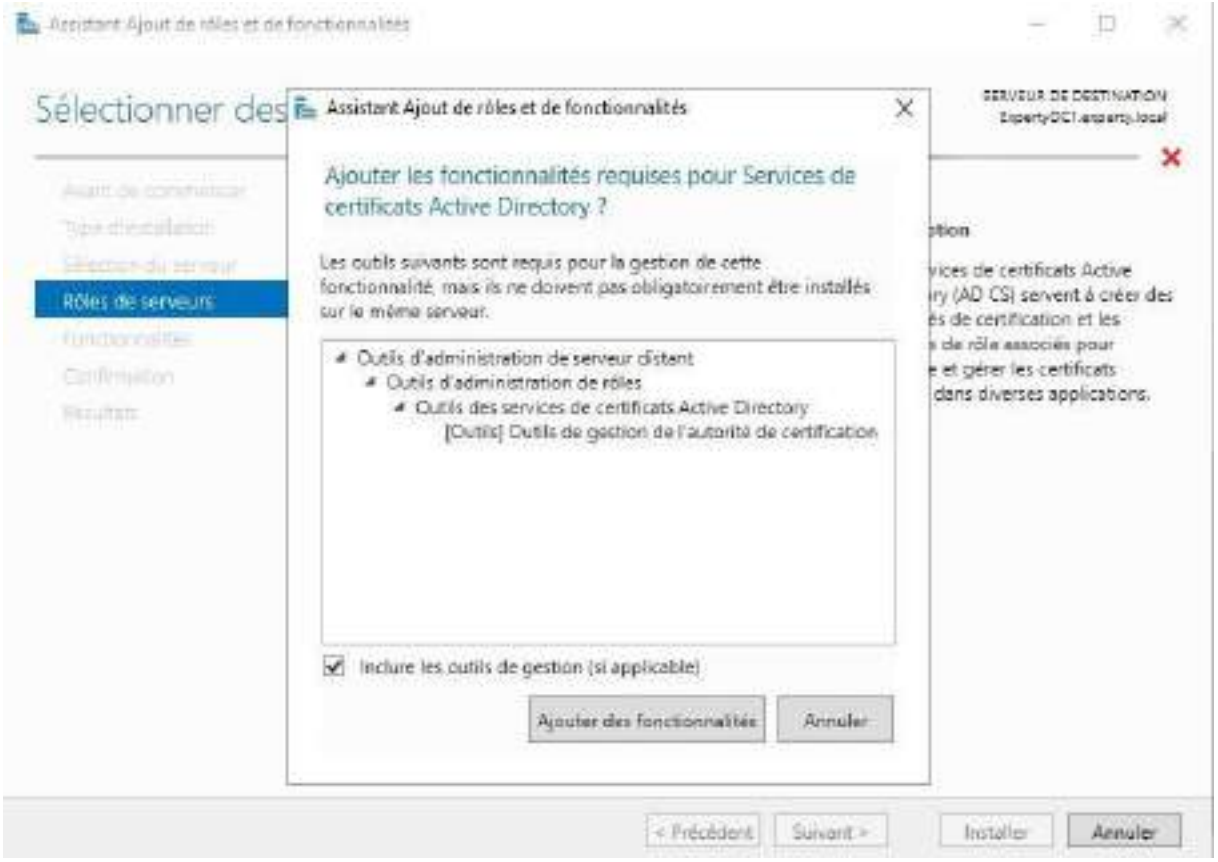
Ajouter un moyen de MFA puis accéder à la page d'accueil de Teleport :


Teleport
Resources
Search for resources...
Types
Health Status
All Resources
Pinned Resources
Debian
Connect

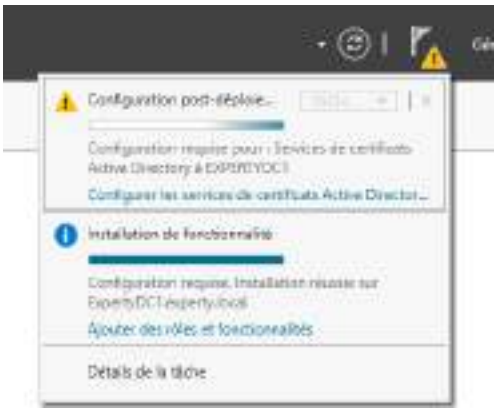
4. Ajouter le domaine experty

a. Configurations sur le DC

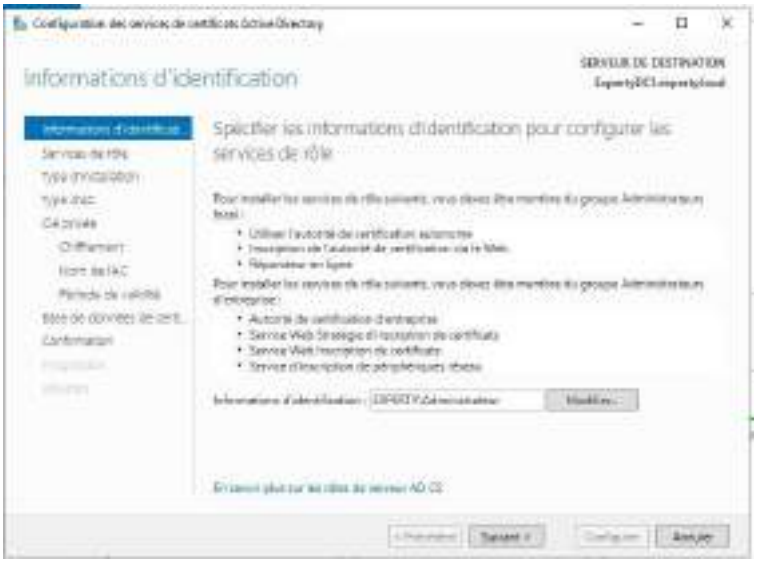
Aller sur le Domaine Controller, sur le gestionnaire de serveur, Gérer, Ajouter, et cliquer sur Services de certificats Active Directory :



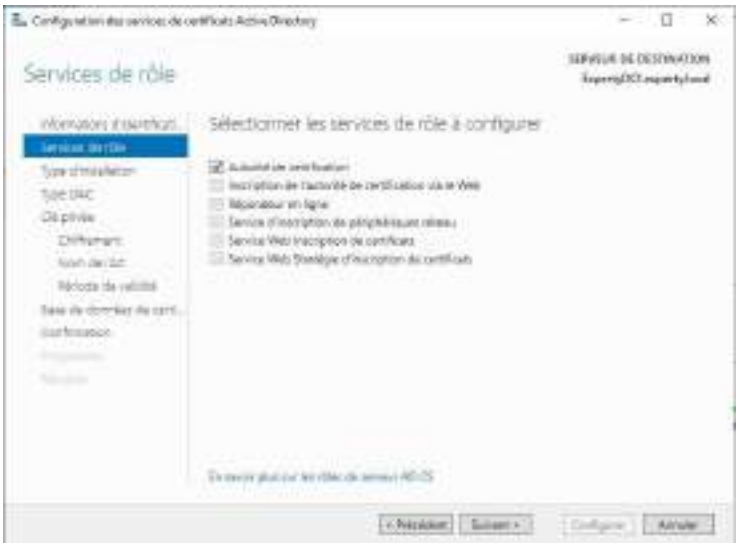
Terminer l'installateur, puis retourner sur le Gestionnaire de serveur, cliquer sur le drapeau puis Configurer les services de certificats Active Directory :



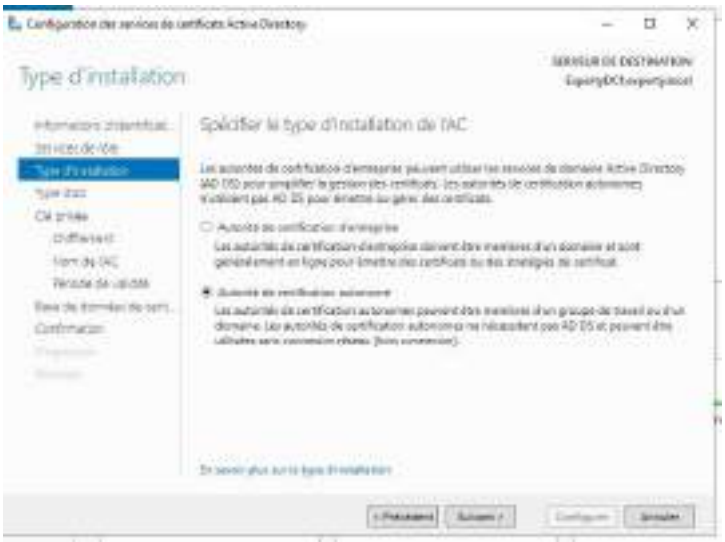
Le configurateur s'ouvre, valider la première page :



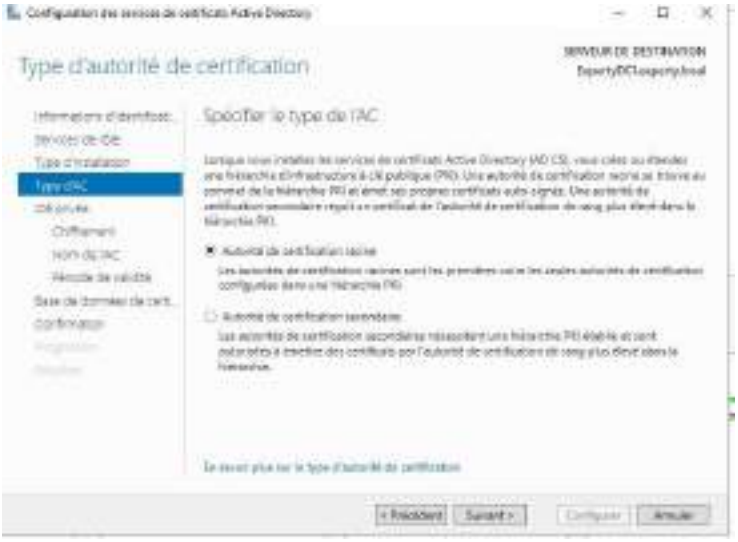
Cocher Autorité de certification :



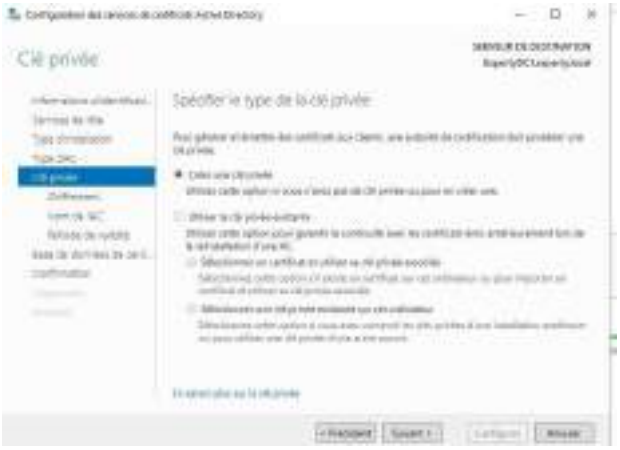
Puis Autorité de certification autonome :



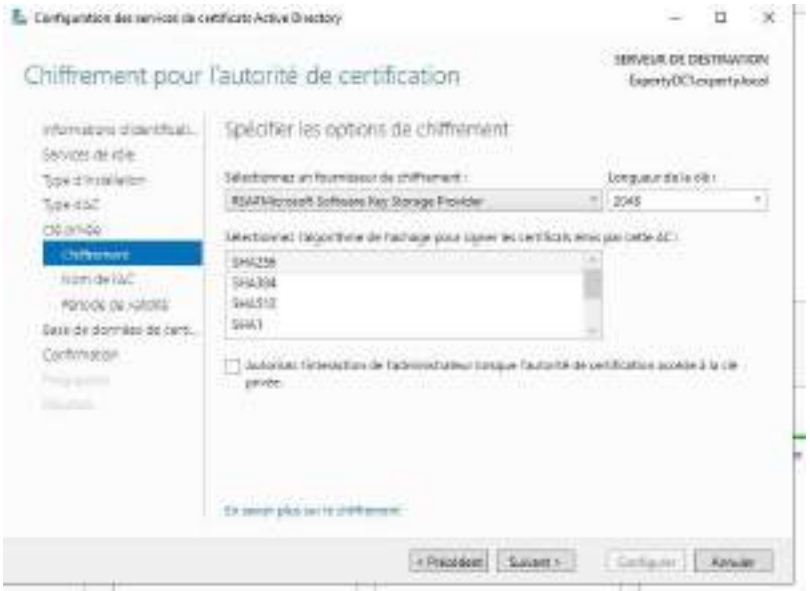
Ensuite autorité de certification racine :



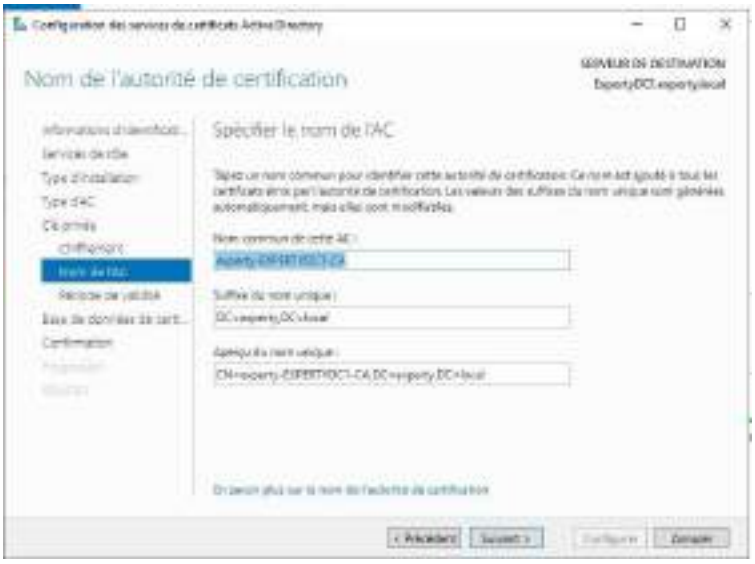
Laisser créer une clé privée :



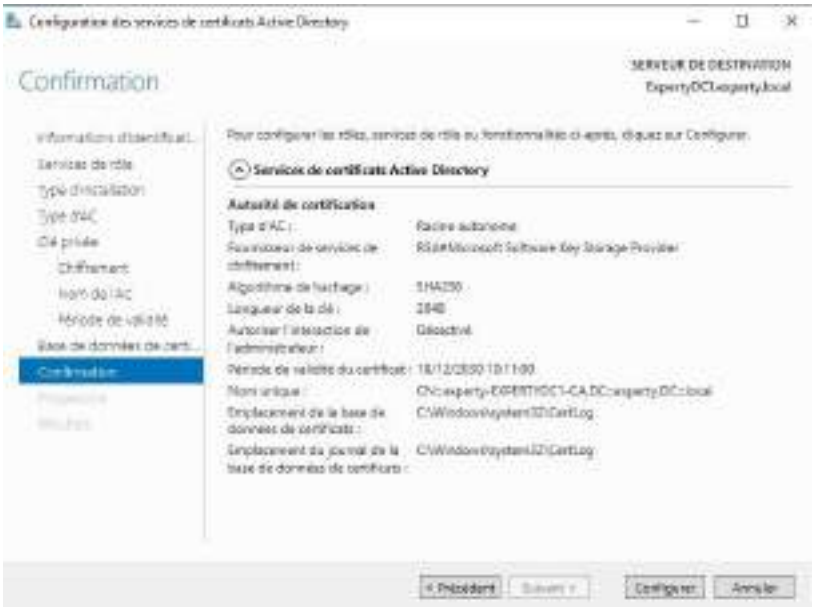
Laisser par défaut le chiffrement :



Donner un nom à l'autorité de certification (ou laisser celui par défaut) :

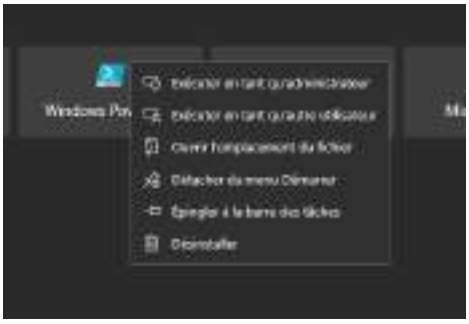


Laisser par défaut le reste puis valider la configuration en appuyant sur Configurer :

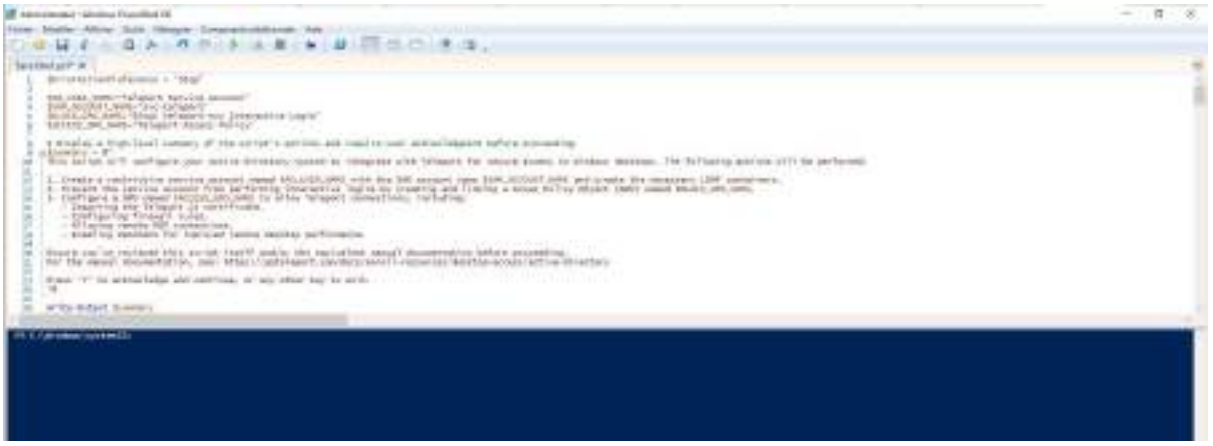


Puis retourner sur la debian hostant Teleport et faire cette commande : tctl desktop bootstrap > configure-ad.ps1. Cela va créer un script qui créé un compte de service pour Teleport sur l'AD et créé deux GPO pour sécuriser la connexion. Faire cat configure-ad.ps1 pour récupérer le script.

Aller sur le DC et exécuter le script en administrateur :



Coller le script et le lancer :



Une fois le script terminé, faire ceci :

```
$cert = New-SelfSignedCertificate `
 -DnsName "expertydc.experty.local", "experty.local", "10.10.3.10" `
 -CertStoreLocation "Cert:\LocalMachine\My" `
 -KeyUsage KeyEncipherment, DigitalSignature `
 -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.1") `
 -NotAfter (Get-Date).AddYears(5)
```

Vérifier avec la commande Get-ChildItem Cert:\LocalMachine\My qu'il y a bien deux certificats, par exemple :

```
6E73F4F4DAD7A0CC3A06EDB8C943525FF730CFCF
CN=experty-EXPERTYDC-
CA, DC=experty, DC=local
F1AFC8C11CE1E3C4700CFEABC4FE2BC9C016D3E9
CN=expertydc.experty.local
```

Puis faire :

```
$thumbprint  =  "F1AFC8C11CE1E3C4700CFEABC4FE2BC9C016D3E9"
$cert = Get-Item "Cert:\LocalMachine\My\$thumbprint"
$store = New-Object
System.Security.Cryptography.X509Certificates.X509Store("Root","Loc
alMachine ")
```

```
$store.Open("ReadWrite")
$store.Add($cert)
$store.Close()
```

Et relancer le service NDTS avec la commande Restart-Service "NTDS"

-Force. Ensuite exporter le script avec la commande :

```
Export-Certificate -Cert
"Cert:\LocalMachine\My\F1AFC8C11CE1E3C4700CFEABC4FE2BC9C016D3E9"
-FilePath "C:\teleport-dc.cer" -Type CERT
```

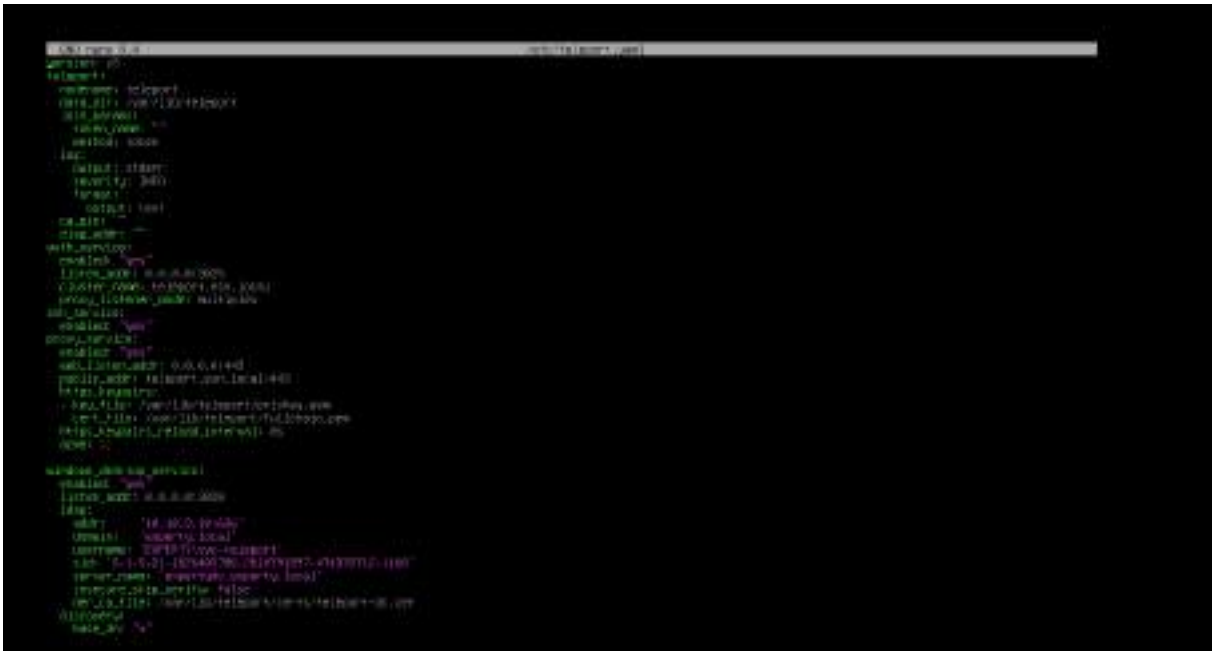
Récupérer ce certificat pour le transférer sur la debian.

b. Configuration sur le serveur Teleport

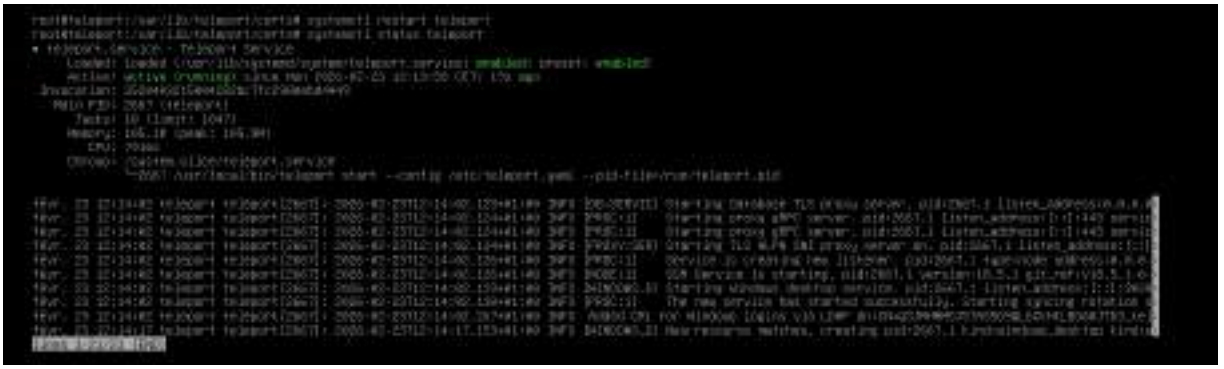
Aller sur la debian hostant Teleport et créer un dossier pour les certificats : mkdir -p
/var/lib/teleport/certs. Y mettre le certificat créé auparavant.

Rajouter une section sur Windows Desktop dans le fichier de configuration de teleport : nano /etc/teleport .yaml (se référer à la section LDAP du script) :

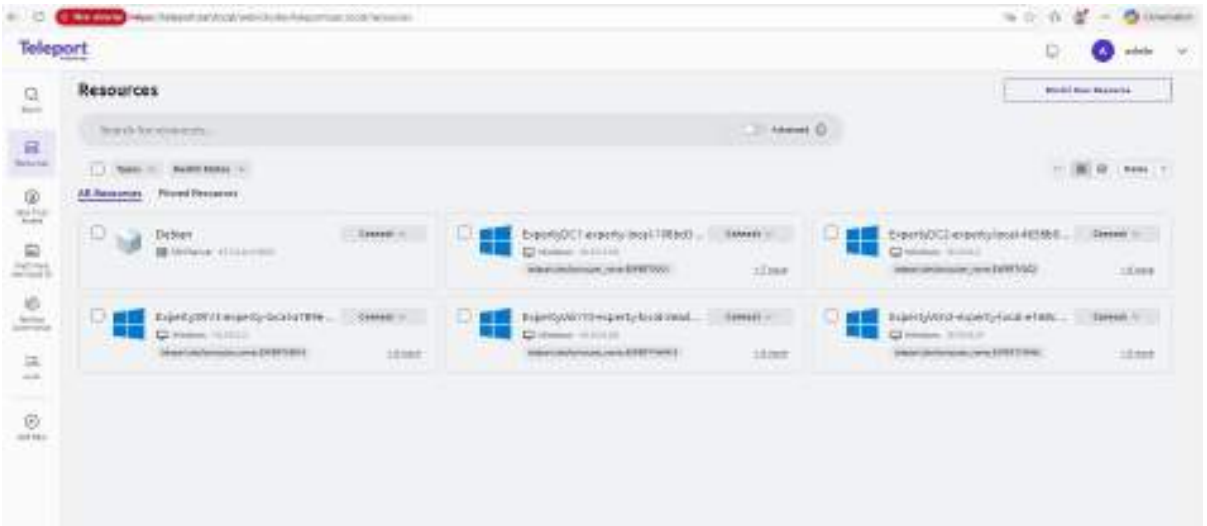
```
windows_desktop_service:
  enabled: "yes"
  listen_addr:
  0.0.0.0:3028 ldap:
    addr:    '10.10.3.10:636'
    domain:  'experty.local'
    username: 'EXPERTY\svc-teleport'
    sid: 'S-1-5-21-646546454-2773906599-3909544045-1604'
    server_name: 'ExpertyDC.experty.local'
    insecure_skip_verify: false
    der_ca_file: /var/lib/teleport/certs/teleport-ca.cer
```



Redémarrer le service Teleport : systemctl restart teleport. Faire systemctl status teleport pour vérifier que la connexion s'est bien établie et que les ressources sont bien ajoutées :



Les machines du domaine devraient s'afficher sur l'interface web.



c. Ajouter le rôle dédié à la connection aux windows du domaine Créer un fichier windows.yaml et y indiquer ceci :

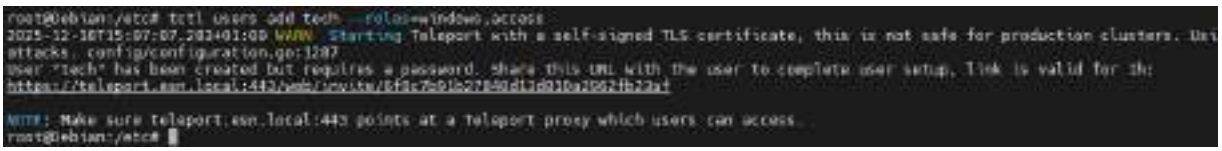
```
kind: role
version: v5
metadata:
  name: windows
spec:
  allow:
    windows_desktop_labels:
      "*": "*"
    windows_desktop_logins: ["administrateur", "tesn"]
```

La ligne windows_desktop_logins corresponds aux utilisateurs dans l'Active Directory.

Créer le rôle: tctl create -f windows.yaml

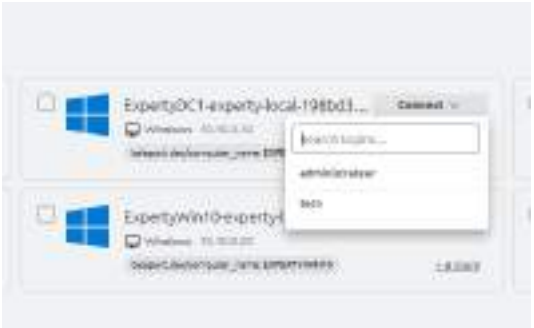
```
root@Debian:/etc# tctl create -f windows.yaml
2025-12-18T15:05:57.676+01:00 WARN  Starting Teleport with a self-signe
attacks. config/configuration.go:1287
role "windows" has been created
```

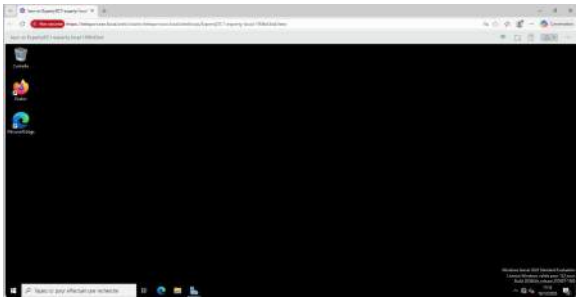
Créer le user pour le technicien et lui donner les bons rôles: tctl users add tesn --roles=windows,access



Comme pour l'administrateur, se connecter au lien et suivre l'assistant.

Puis se connecter sur teleport.esn.local avec les logins de tesn et vérifier qu'il est bien possible de se connecter à ExpertyDC1 :



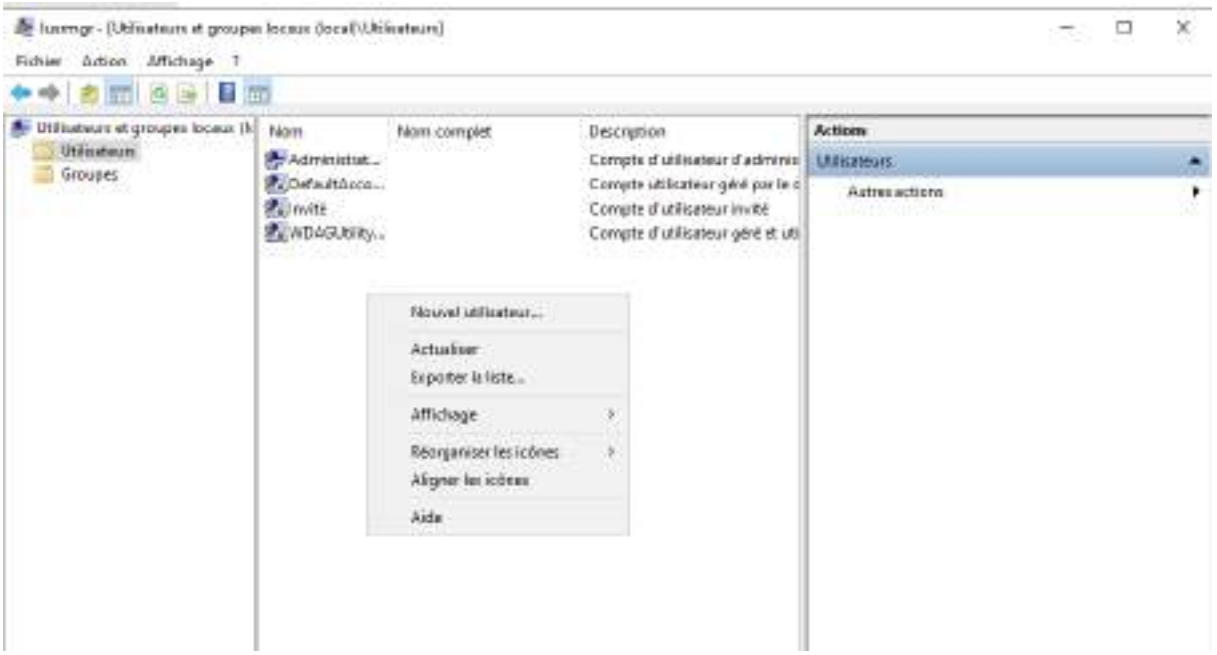


E. **Veeam**

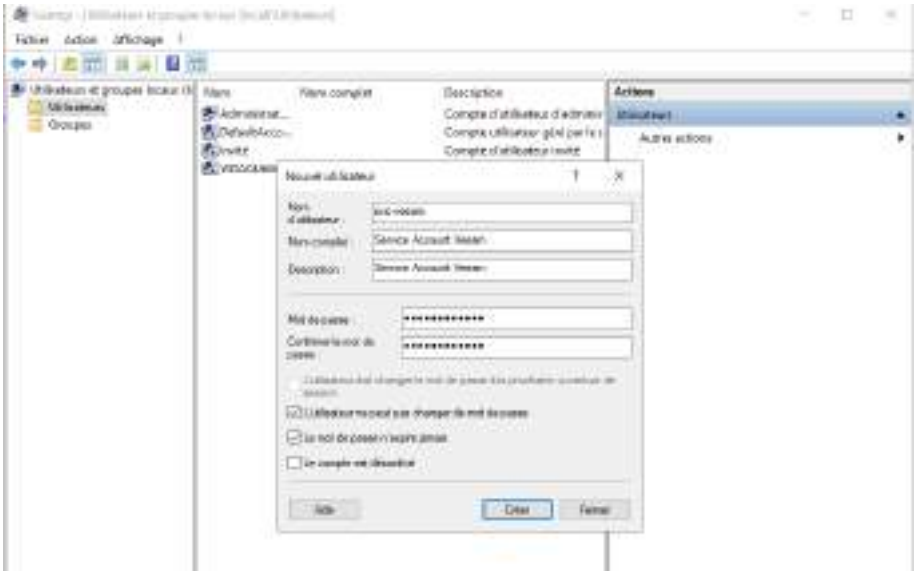
Avoir un windows server 2022 avec une adresse IP statique.

Si le serveur n'est pas membre d'un domaine, aller dans Paramètres, Comptes, Autres utilisateurs et cliquer sur Ajouter un autre utilisateur sur ce PC pour créer un utilisateur dédié à Veeam :

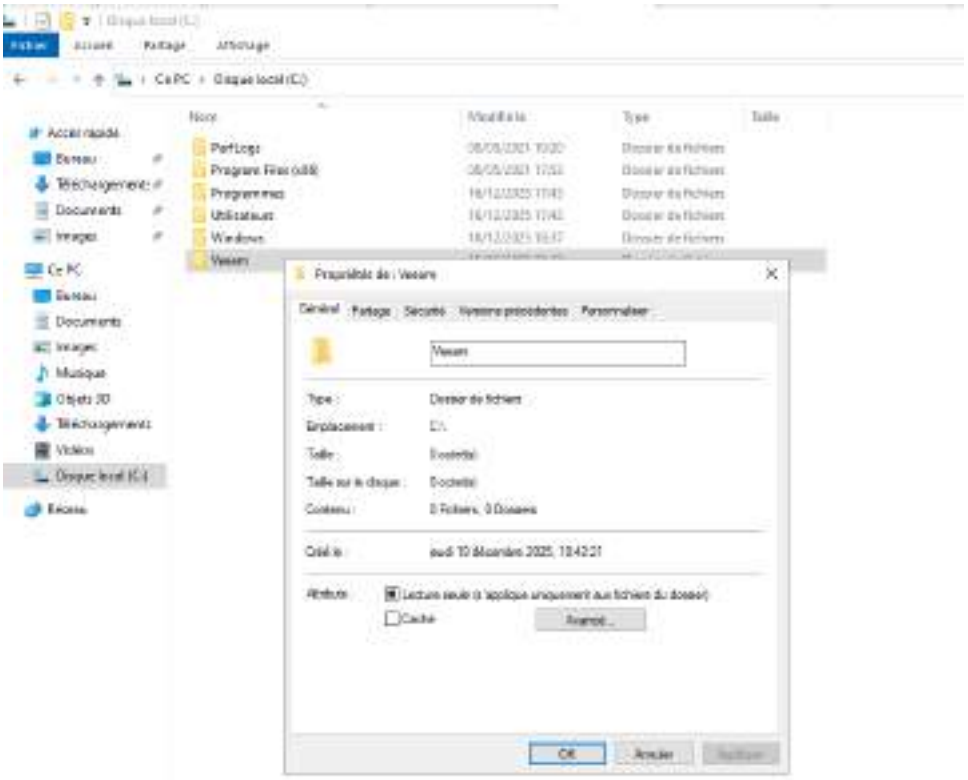
Faire un clic droit dans l'onglet du milieu, cliquer sur Nouvel utilisateur...



Renseigner les informations nécessaires puis décocher L'utilisateur doit changer le mot de passe et cocher L'utilisateur ne peut pas changer de mot de passe et Le mot de passe n'expire jamais. Cliquer sur Créer :

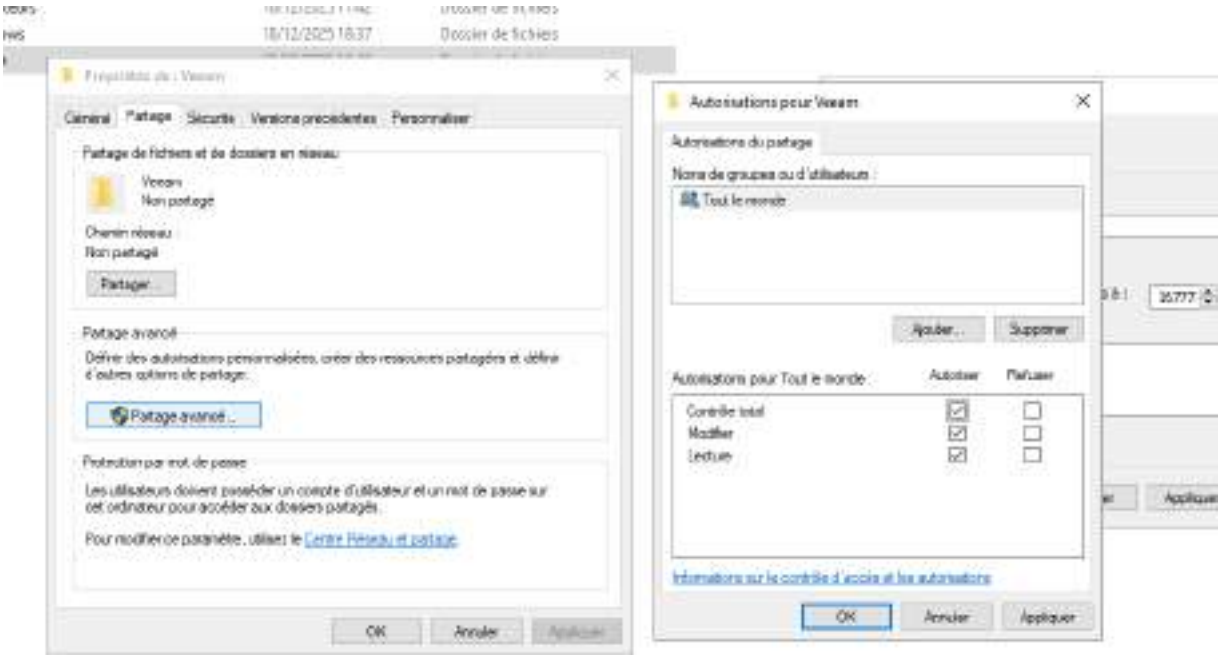


Créer un dossier pour les sauvegardes Veeam, puis faire un clic droit dessus et aller dans les propriétés :

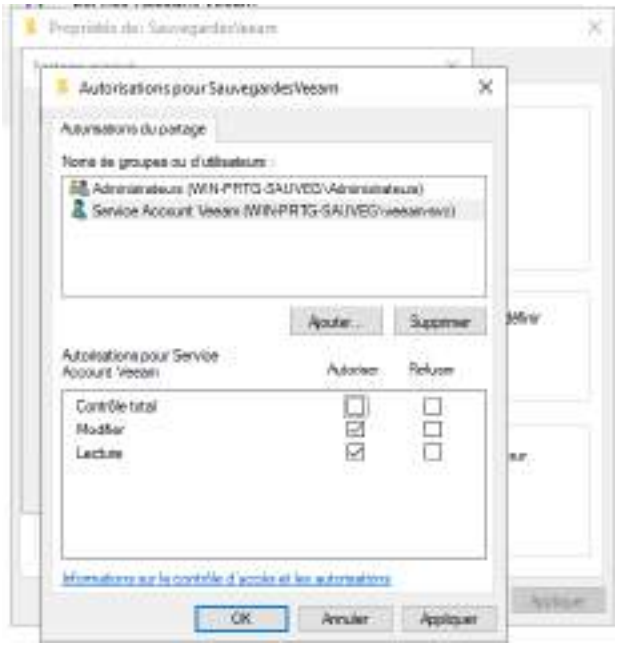


.

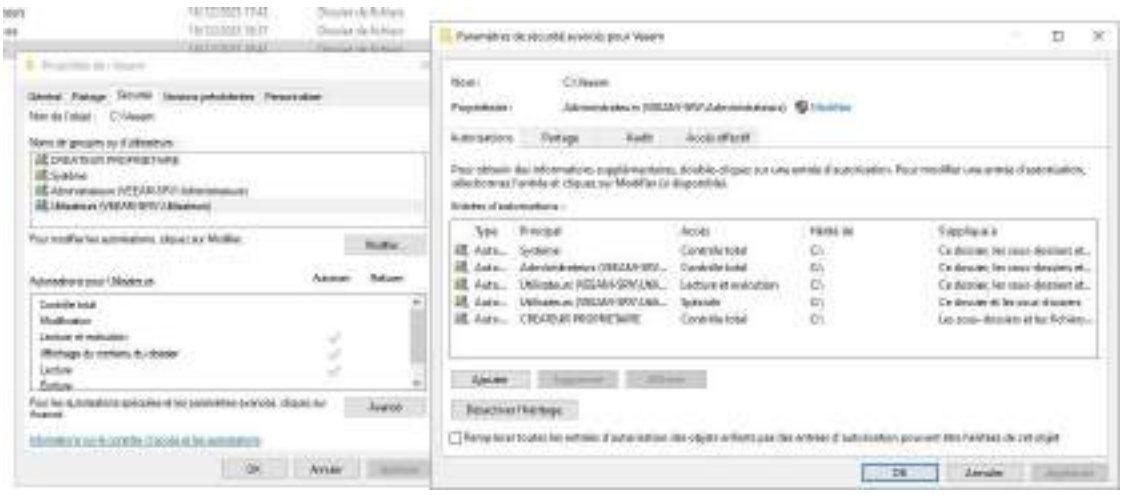
Aller dans Partage et cliquer sur Partage Avancé, supprimer Tout le monde :



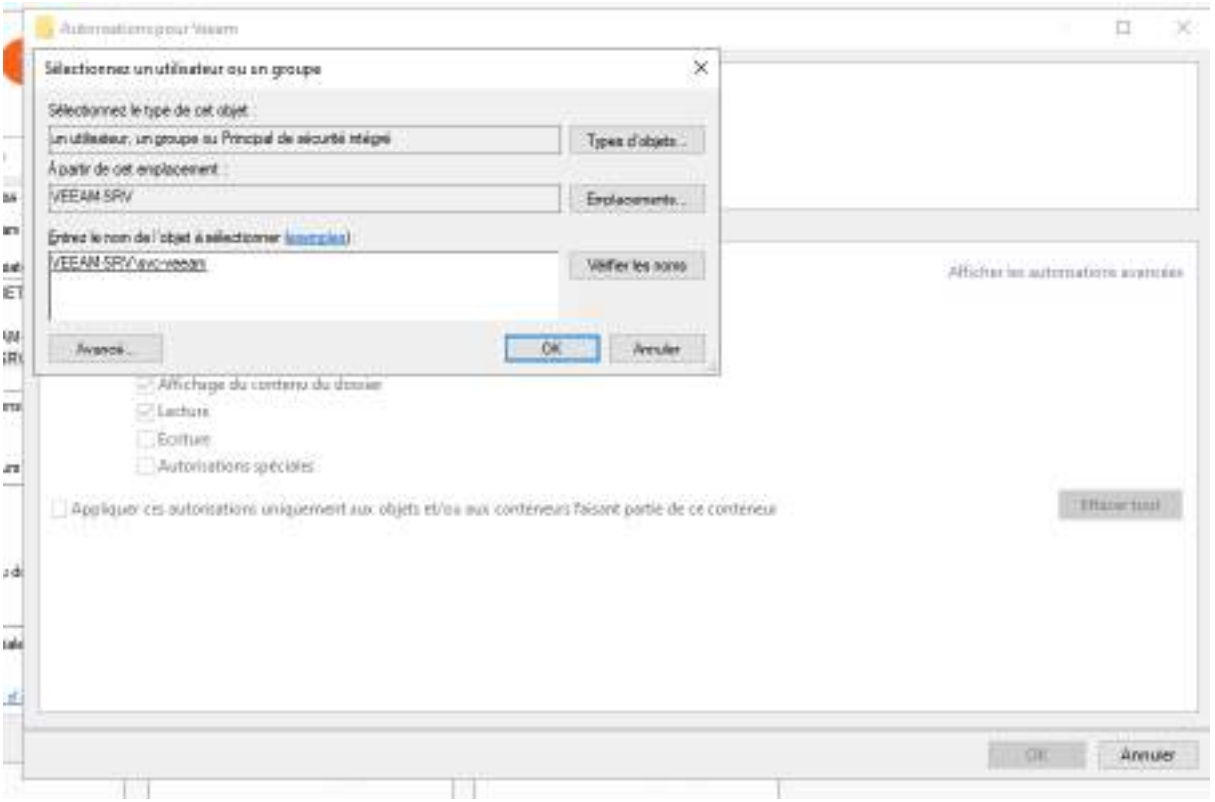
Cliquer sur Ajouter et ajouter le groupe Administrateurs et l'utilisateur dédié :



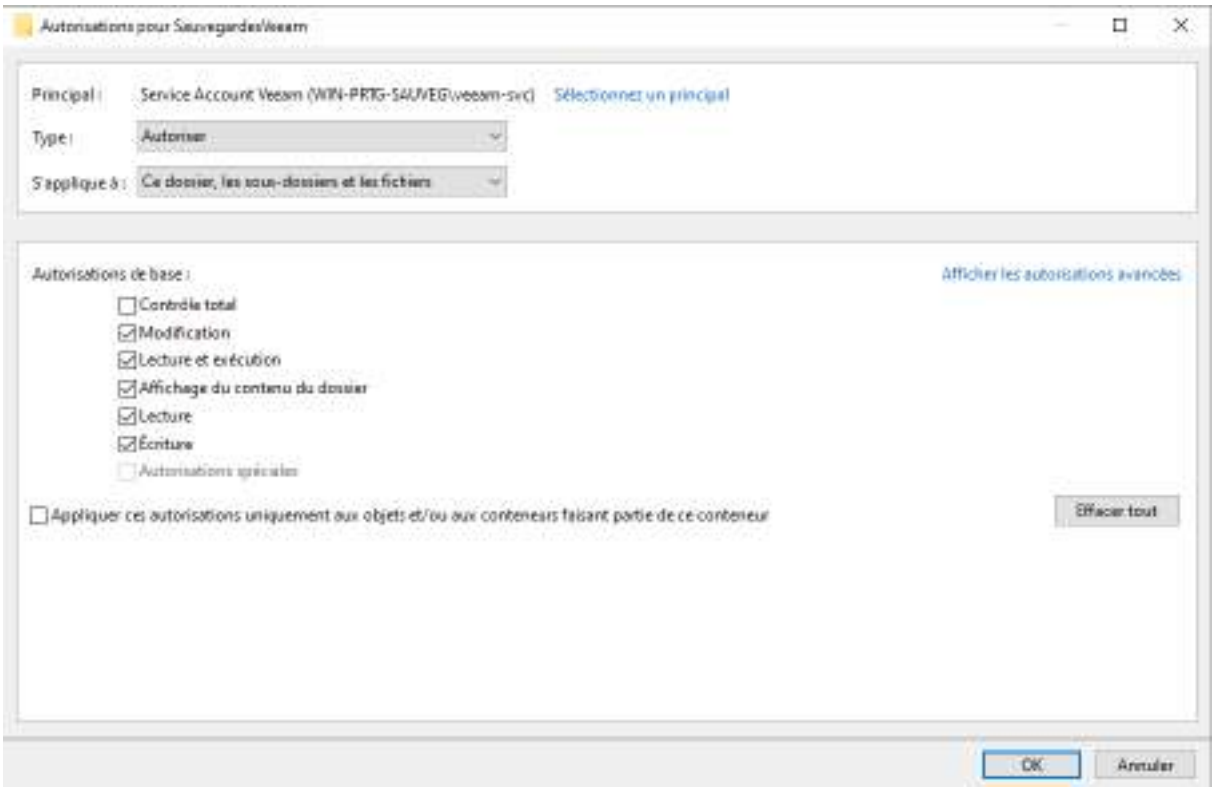
Aller dans l'onglet Sécurité et cliquer sur Avancé, cliquer sur Désactiver l'héritage, supprimer Utilisateurs puis sur cliquer sur Ajouter :



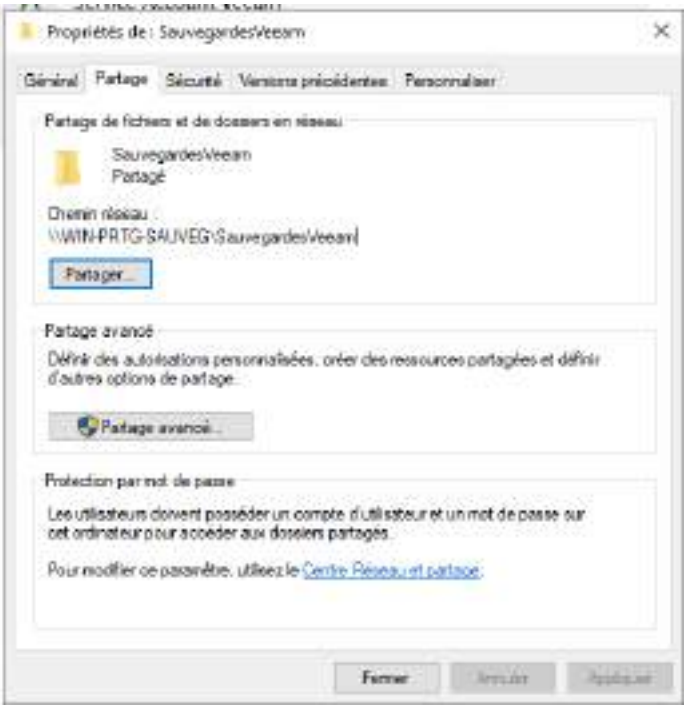
Cliquer sur Sélectionner un principal, renseigner le nom de l'utilisateur veeam :



Puis lui donner les autorisations suivantes :



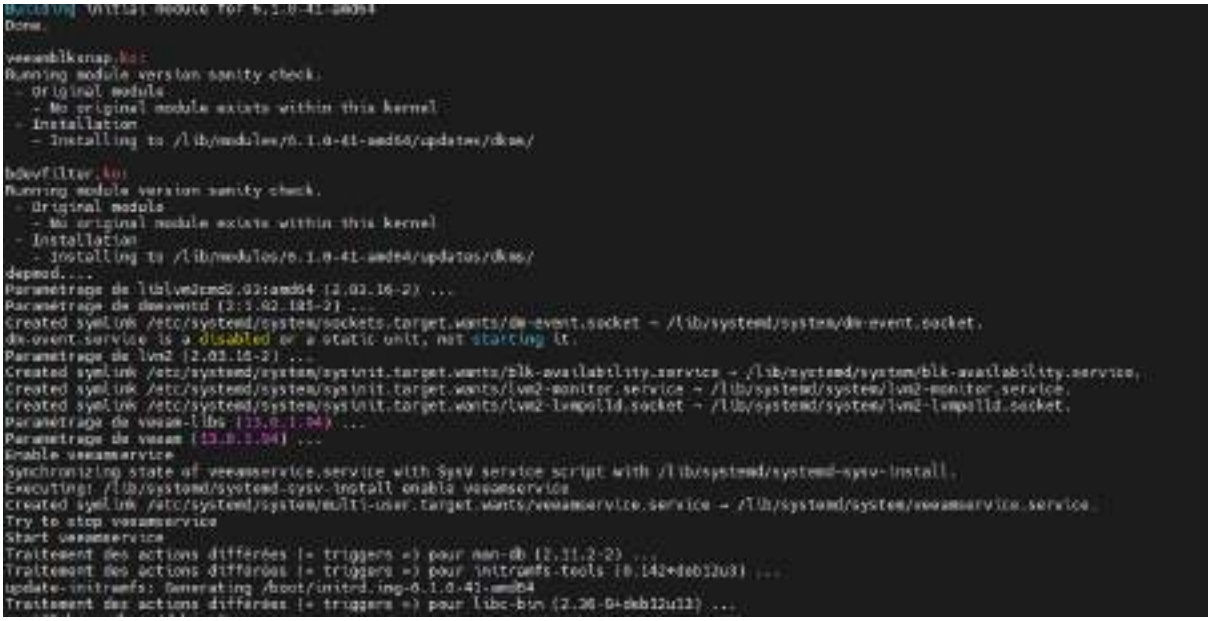
Valider le tout et retourner dans l'onglet Partage pour noter le chemin réseau :



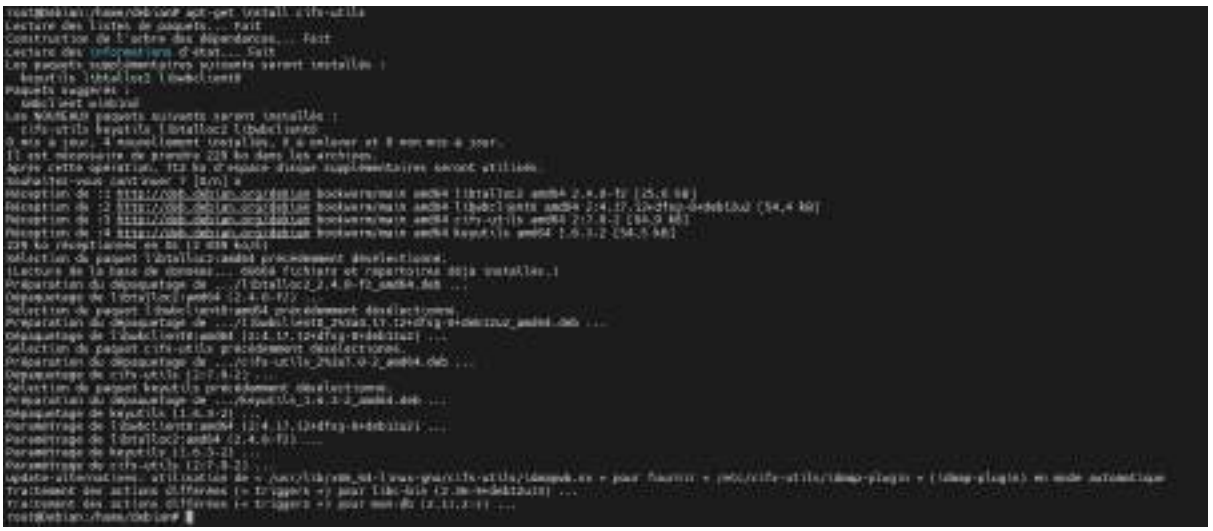
Aller sur le site de Veeam et télécharger le paquet pour debian : https://www.veeam.com/products/physical/linux-backup-recovery-download.html

Le mettre sur la vm linux que l'on souhaite sauvegarder, ici la debian GestSup. Puis aller dans le répertoire où se trouve le paquet et faire dpkg -i ./veeam-release* && apt-get update

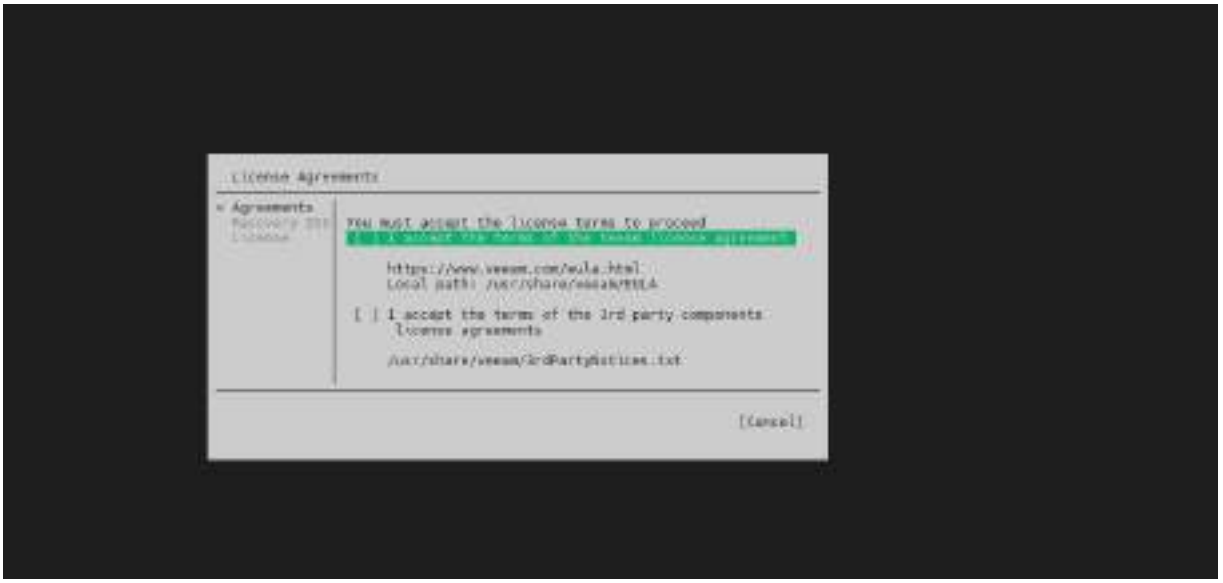
Ensuite faire apt-get install blksnap veeam :



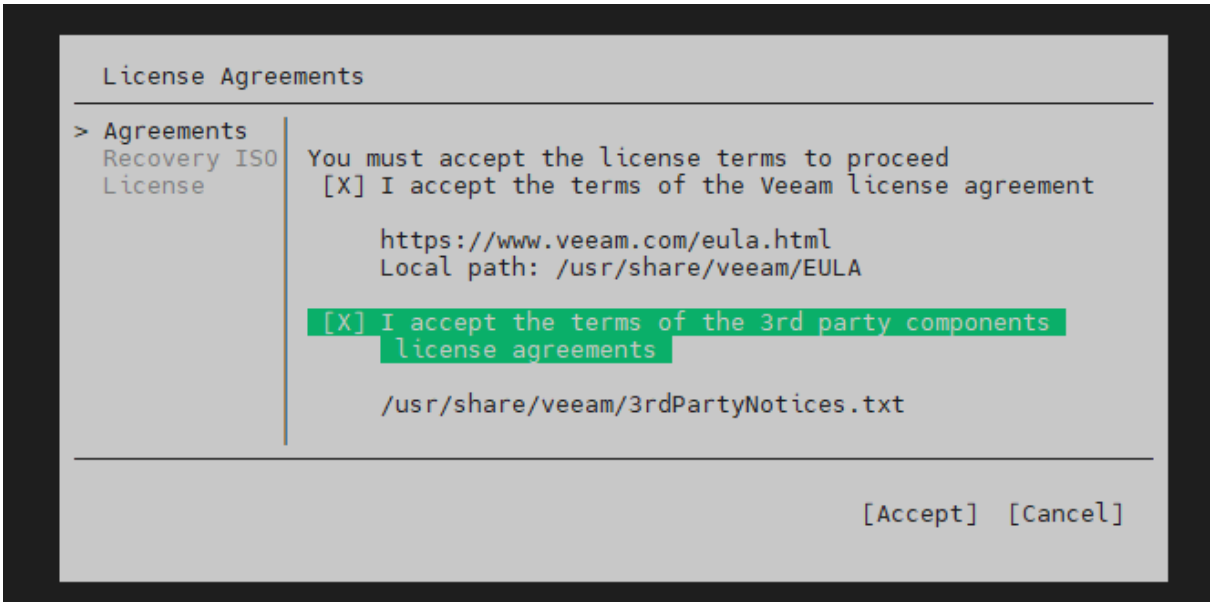
Faire apt-get install cifs-utils:



Et lancer Veeam en faisant simplement la commande veeam :

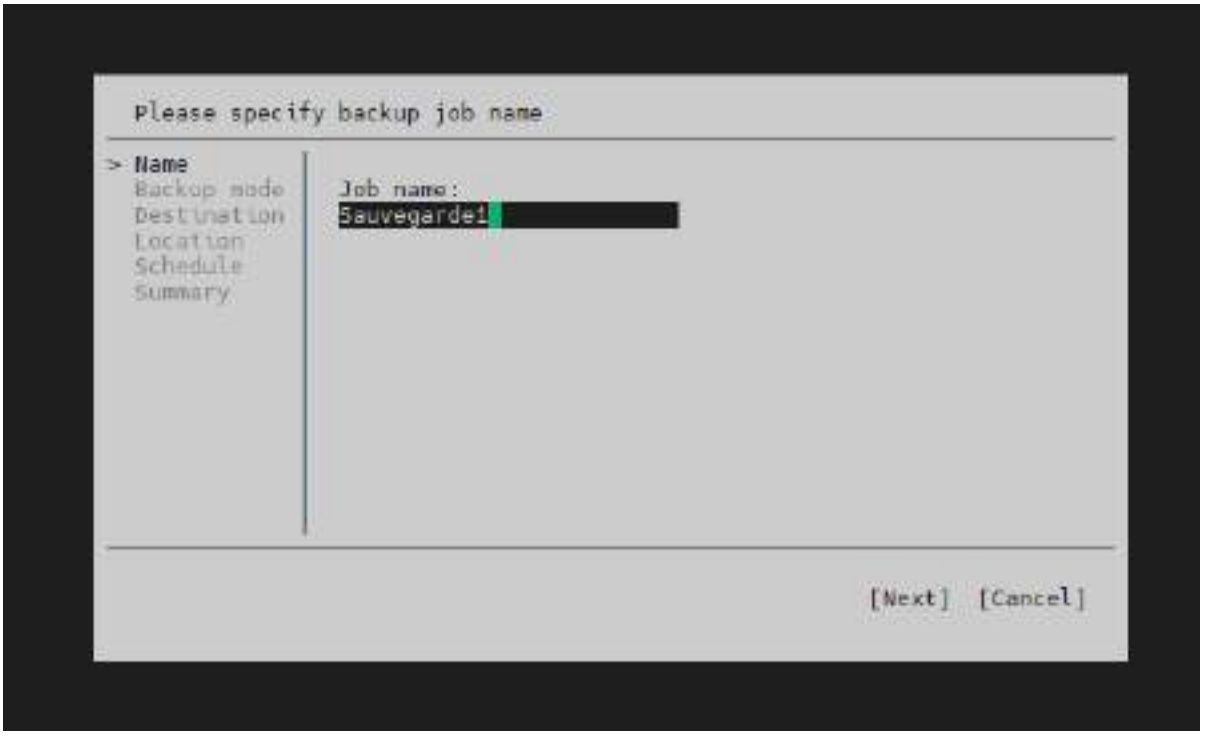


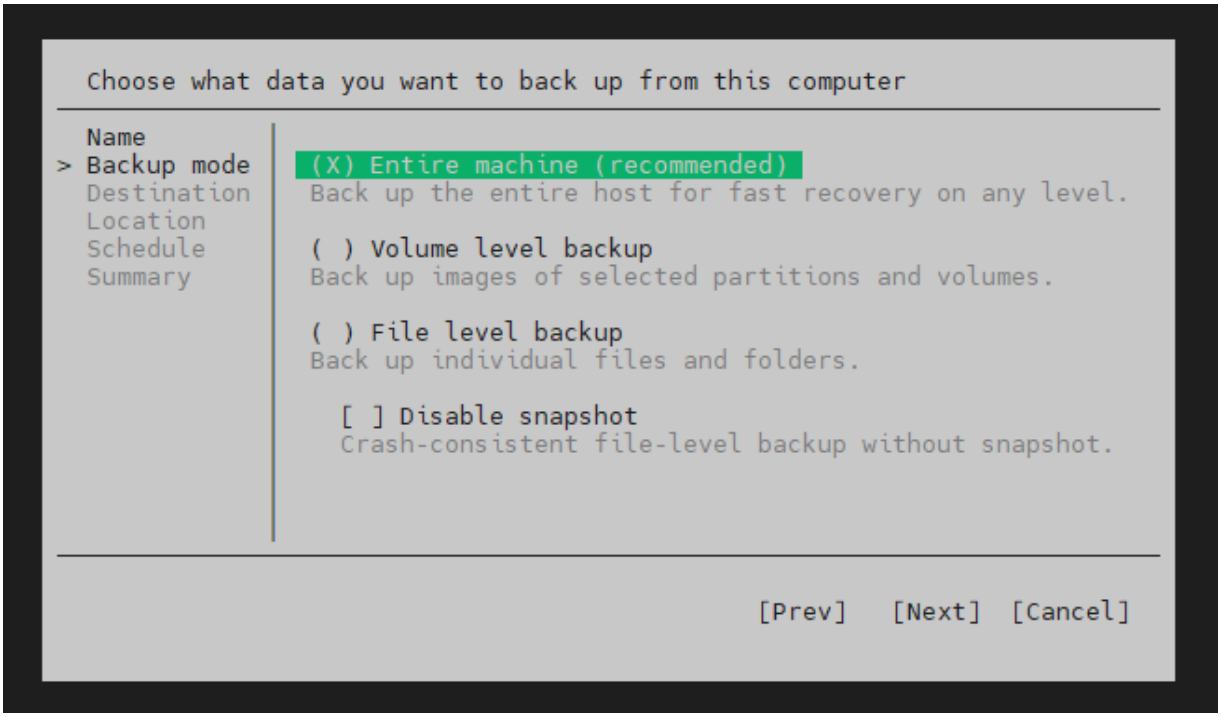
Faire espace pour cocher puis aller sur Accept



Suivre l'installateur puis faire C pour configurer la sauvegarde :

La nommer :

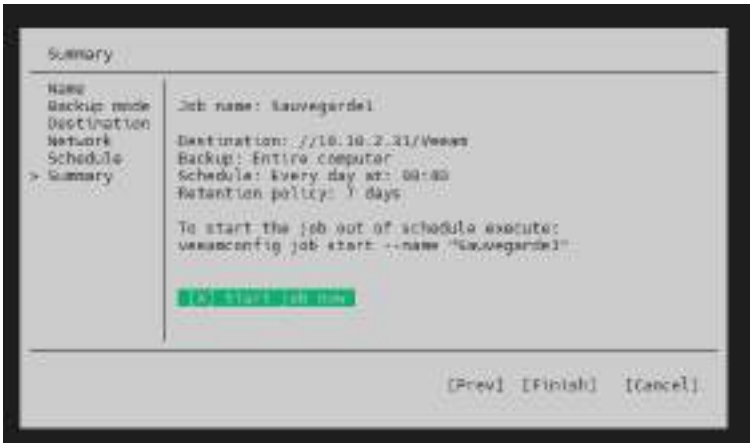

Please specify backup job name
> Name
Backup mode
Destination
Location
Schedule
Summary
Job name:
Sauvegarde1
[Next] [Cancel]



En destination choisir Shared folder puis sélectionner SMB et remplir avec les informations du serveur :

Choisir l'heure et les jours où la sauvegarde est faite :

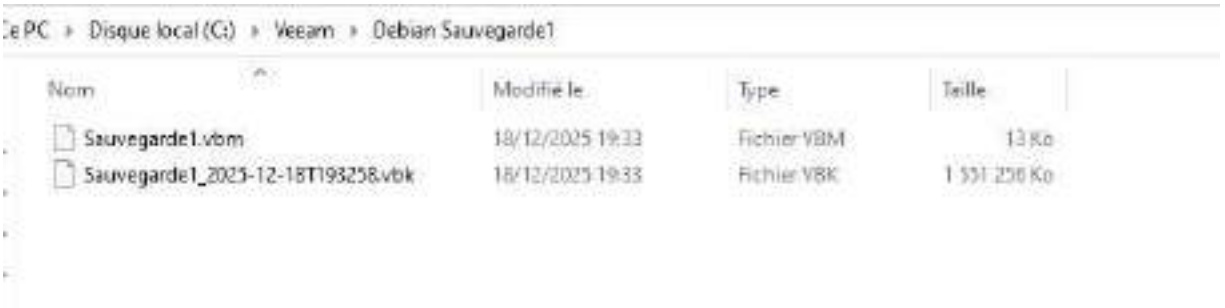
Cocher Start job now et valider:



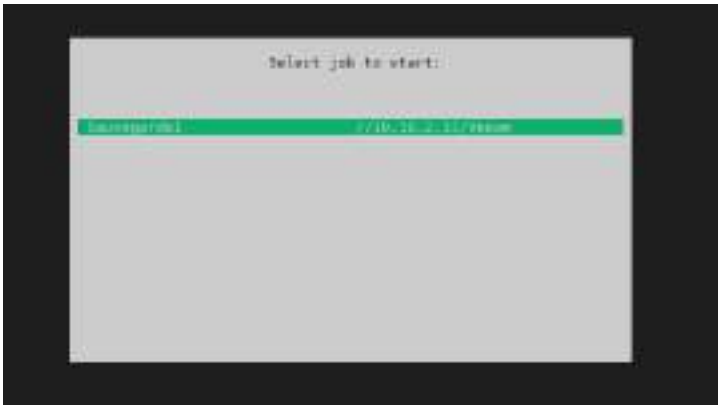
La sauvegarde commence alors:

Attendre qu'elle soit complétée:

Un dossier comprenant la sauvegarde apparaît alors sur le serveur windows :



Il est possible de lancer une sauvegarde manuellement en allant sur Veeam, faire S et sélectionner la sauvegarde à réaliser :


Select job to start: