BTS SIO - EPREUVE E5
PROJET N°2

Yanis Mingam

KEYCE ACADEMY OGEC D'ALZON

Table des matières

I. Mise en contexte

L'établissement scolaire Poudlard a ouvert ses portes. Devant accueillir un nombre assez élevé de personnel, administratif et pédagogique, mais aussi d'élèves / étudiants, il est nécessaire d'améliorer le parc informatique mis en place

C'est dans ce contexte que cet établissement fait appel à notre société « Mingam Corp. ». Avant toute chose, il faut considérer les moyens dont Poudlard dispose afin de le rapporter aux besoins évoqués et ainsi trouver des solutions adaptées.

Ne générant pas de revenus, l'école vit et se développe grâce aux subventions et à l'investissement de l'Education Nationale. En partant de se principe, on tentera au maximum de privilégier des solutions gratuites.

Voici le plan de l'infrastructure :

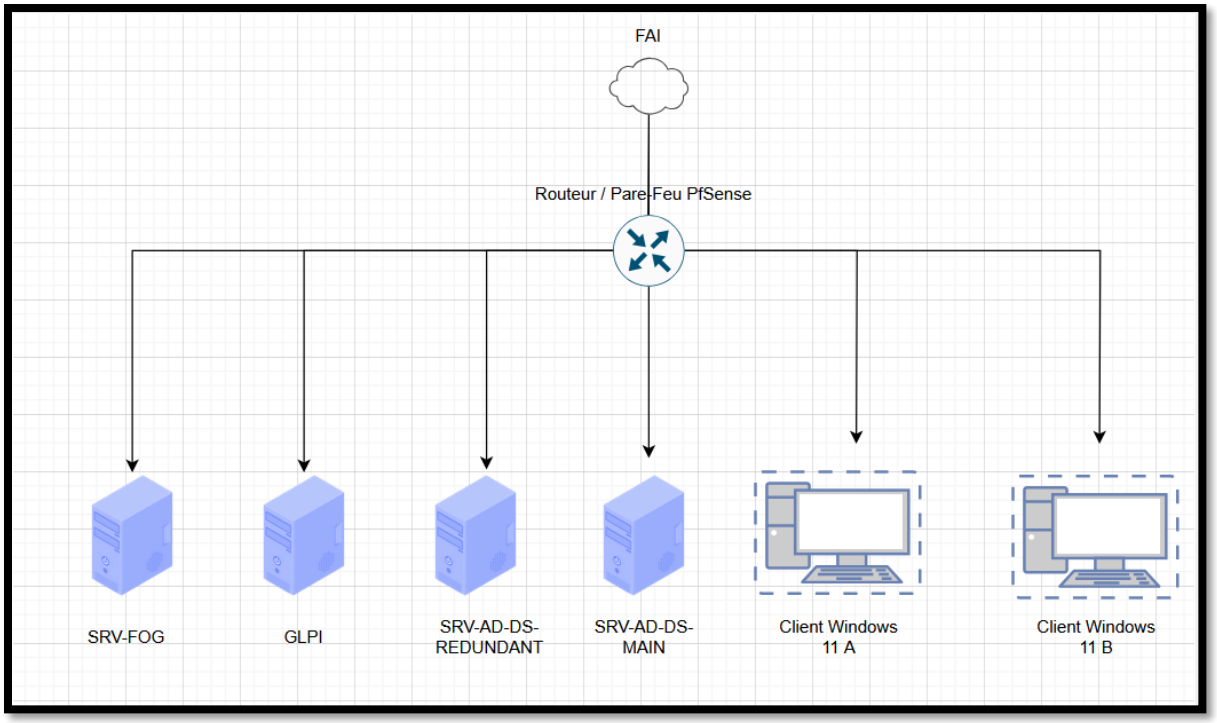

Figure 1 - Schéma de l'infrastructure

Le Schéma ci-dessus présente les composantes de l'infrastructure qui ont été mise en place et qui vont être mises en place au sein de l'établissement. On y retrouve les éléments suivants :

- Un routeur / Pare-Feu PfSense qui permet de fournir un accès à internet aux machines du réseau tout en filtrant le trafic, en distribuant par exemple des adresses IP.
- Un serveur Active Directory (AD) sous Windows Server 2022 permettant entre-autre de gérer efficacement un grand nombre d'utilisateurs ainsi que leurs spécificités.
- Un serveur redondant qui réplique en temps réel le serveur AD afin de pouvoir assurer une continuité des services en cas de panne du serveur dit « principal ».
- Un serveur GLPI, permettant de mettre en place un système de tickets, ainsi qu'un inventaire automatique du matériel (PC, écrans, vidéoprojecteurs, etc...).
- Une machine client Windows 11, faisant partie du domaine de l'AD.
- Un serveur VPN client-to-site afin de permettre aux techniciens IT d'accéder depuis un réseau distant au parc informatique (le poste technicien se trouve sur le réseau 172.16.0.0/24)

On a aussi le tableau d'adresses IP :

NOM	ADRESSE
Routeur / Pare-Feu (PfSense)	192.168.100.1
SRV-AD-DS-MAIN	192.168.100.2
SRV-AD-DS-REDUNDANT	192.168.100.3
GLPI	192.168.100.5
SRV-FOG	192.168.100.10
POSTE CLIENT A	DHCP
POSTE CLIENT B	DHCP
POSTE CLIENT TECH	DHCP

Figure 2 - Tableau d'adresses IP

Le routeur / pare-feu se situe entre le FAI et le réseau local de Poudlard. Les adresses des serveurs sont toujours fixes, car il faut pouvoir interagir en permanence avec eux. Quant aux postes clients, ils obtiendront une adresse via le DHCP.

II. Mise en place d'un serveur GLPI sur le réseau

Afin de permettre aux techniciens IT d'avoir un suivi en quasi-temps réel des machines du réseau, on déploie un serveur GLPI. Cela permettra d'assurer un suivi des incidents

Voici l'installation de GLPI depuis une machine Debian 12 sans interface graphique:

```
root@GLPI-POUDLARD:/home/glpi# cd /tmp
root@GLPI-POUDLARD:/tmp# wget https://github.com/glpi-project/glpi/releases/download/10.0.18/glpi-10.0.18.tgz
```

Figure 3 – Installation de GLPI10 dans le dossier tmp

```
root@GLPI-POUDLARD:/tmp# tar -xzvf glpi-10.0.18.tgz -C /var/www/
```

Figure 4 – Extraction de l'archive GLPI10

Il s'agit maintenant de créer la base de donnée à partir de laquelle les données de GLPI seront stockées.

```
root@GLPI-POUDLARD:/home/glpi# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 33
Server version: 10.11.6-MariaDB-0+deb12u1 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 DATABASE glpi CHARACTER SET utf8mb4 COLLATE utf8mb4_unicode_ci;
Query OK, 1 row affected (0,002 sec)

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

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

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

MariaDB [(none)]> EXIT;
```

Figure 5 : Création de la base de données GLPI

```
  GNU nano 7.2
<VirtualHost *:80>
    ServerName 192.168.100.5
    DocumentRoot /var/www/glpi

    <Directory /var/www/glpi>
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/glpi_error.log
    CustomLog ${APACHE_LOG_DIR}/glpi_access.log combined
</VirtualHost>
```

Figure 6 : Configuration PHP

Comme pour tout serveur web, lorsque l'on y monte un service, il est nécessaire d'activer ce service (pour pouvoir accéder à l'interface web de GLPI dans notre cas)

```
root@GLPI-POUDLARD:~# a2ensite glpi.conf
Enabling site glpi.
To activate the new configuration, you need to run:
  systemctl reload apache2
root@GLPI-POUDLARD:~# a2enmod rewrite
Enabling module rewrite.
To activate the new configuration, you need to run:
  systemctl restart apache2
root@GLPI-POUDLARD:~# systemctl restart apache2
```

Figure 7 : Activation du site

Figure 8 : Installation de GLPI

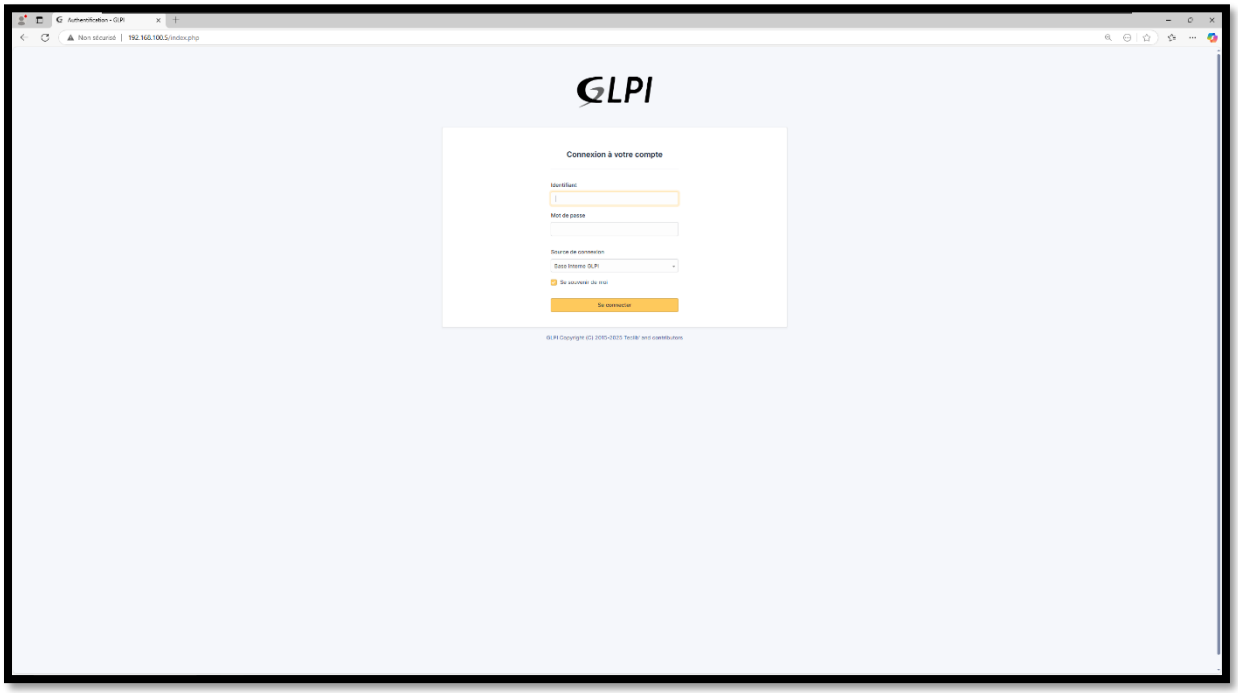

Figure 9 : Page de connexion GLPI

GLPI est maintenant accessible (il sera possible de faire l'inventaire des machines du réseau grâce à GLPI agent)

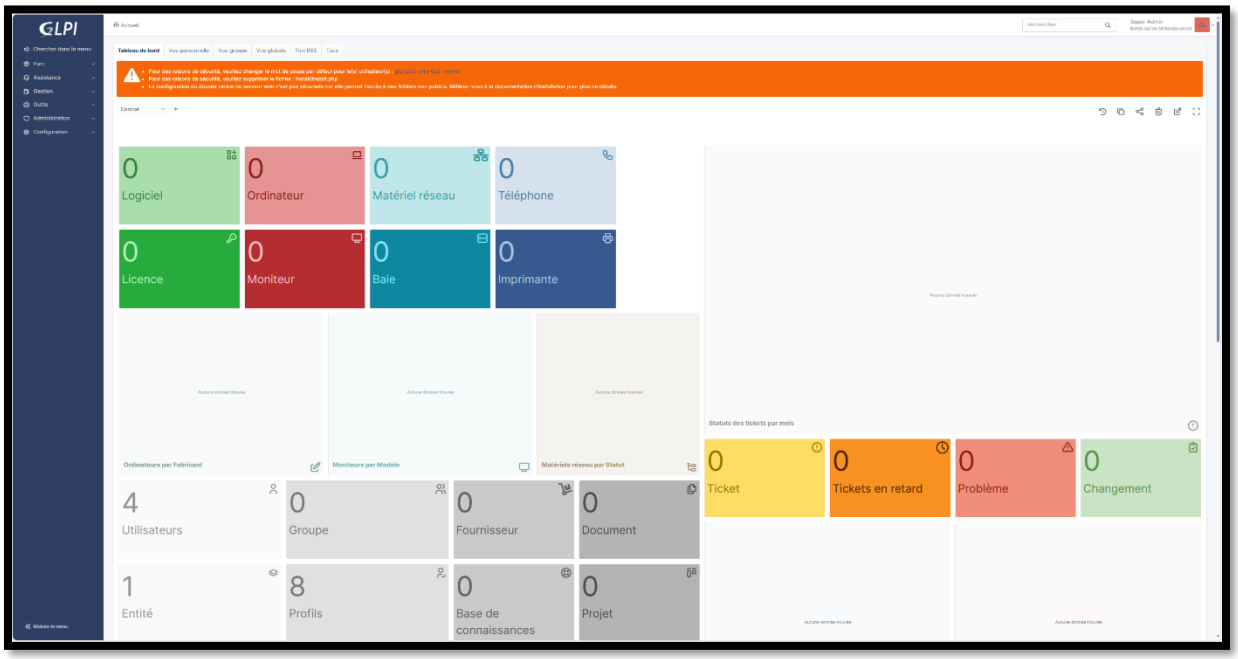

Figure 10 : Interface GLPI

III. Configuration d'un serveur de déploiement de client lourd par PXE (Fog Project)

FOG Project est un projet libre et open-source permettant de capturer et déployer des images à travers le protocole de démarrage PXE

Comme pour le serveur GLPI, on monte le serveur FOG sur une machine Debian 12 sans interface graphique :

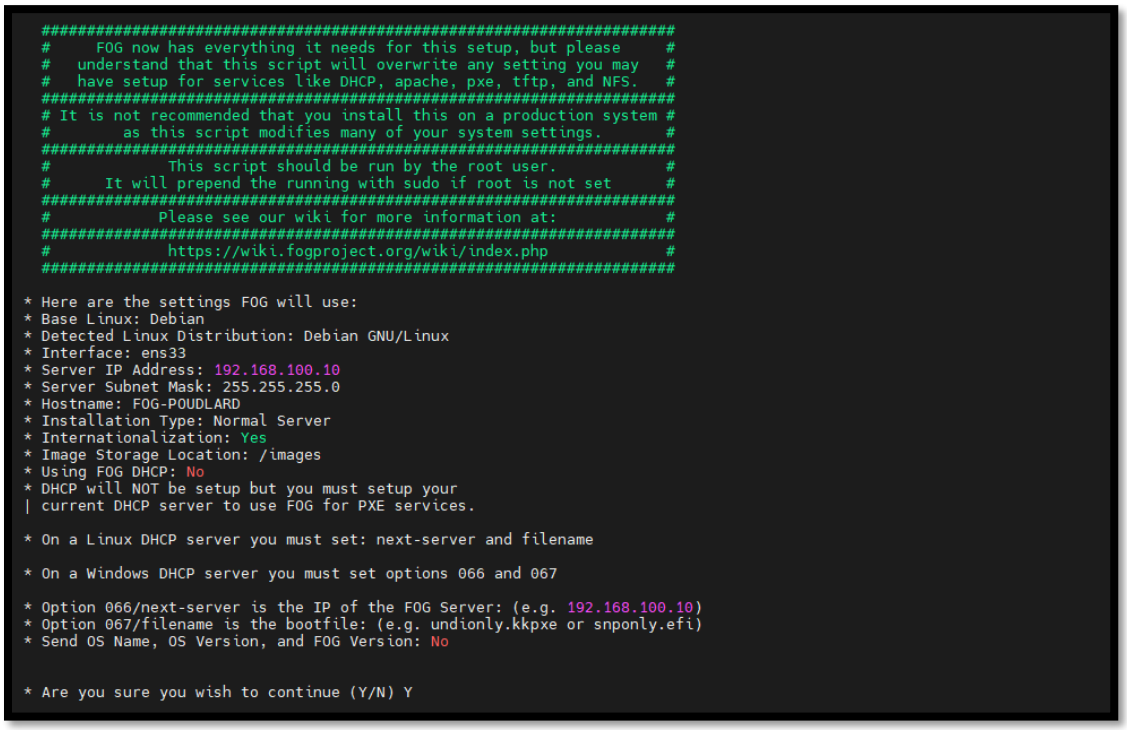

Figure 11 : Installation du serveur FOG

L’interface web de FOG est maintenant disponible à l’adresse 192.168.100.10 :

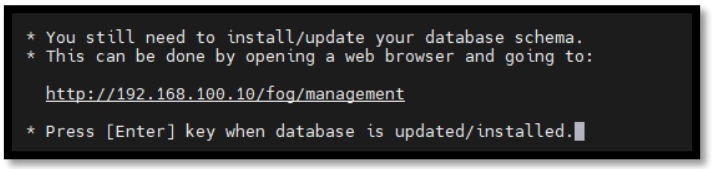

Figure 12 : L’interface web FOG est maintenant disponible

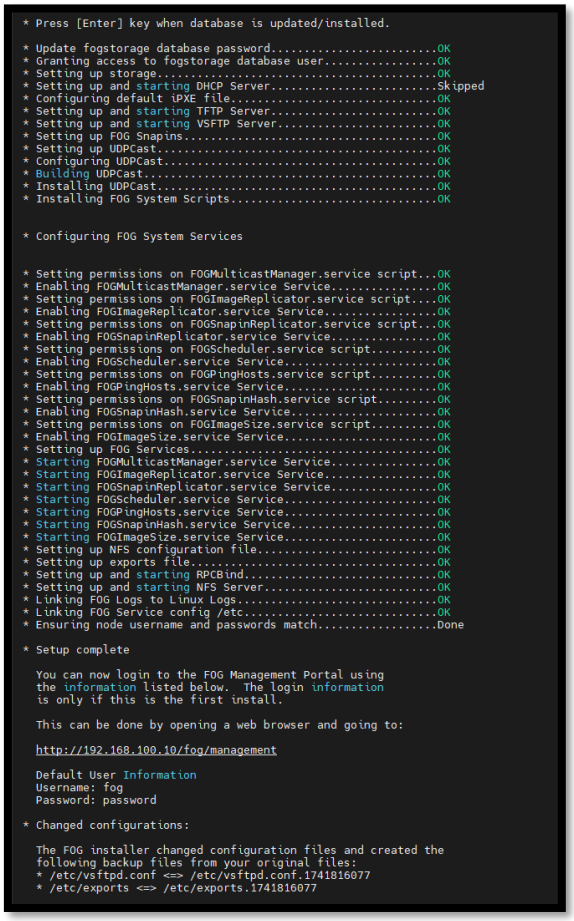

Figure 13 : La base de données est créée

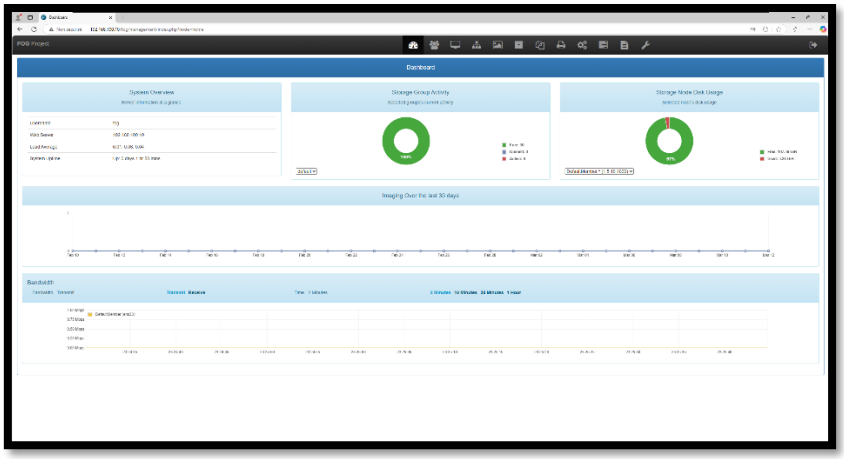

Figure 14 – Interface web FOG

Afin de permettre à FOG de fonctionner dans notre réseau (192.168.100.0/24) à travers le PXE, il faut préciser dans les options d'étendues DHCP l'adresse IP du serveur FOG (option 66) ainsi que le fichier de démarrage que les postes du pc devront charger sur le réseau lors du démarrage en PXE :

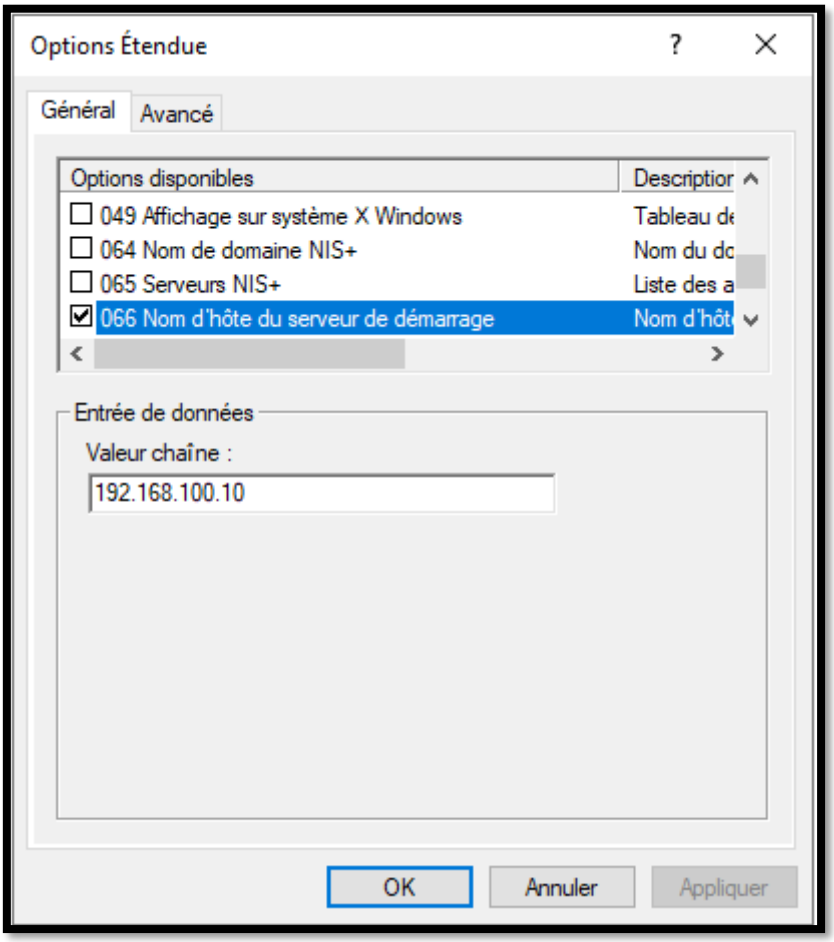

Figure 15 : Configuration des options d'étendues DHCP (1)

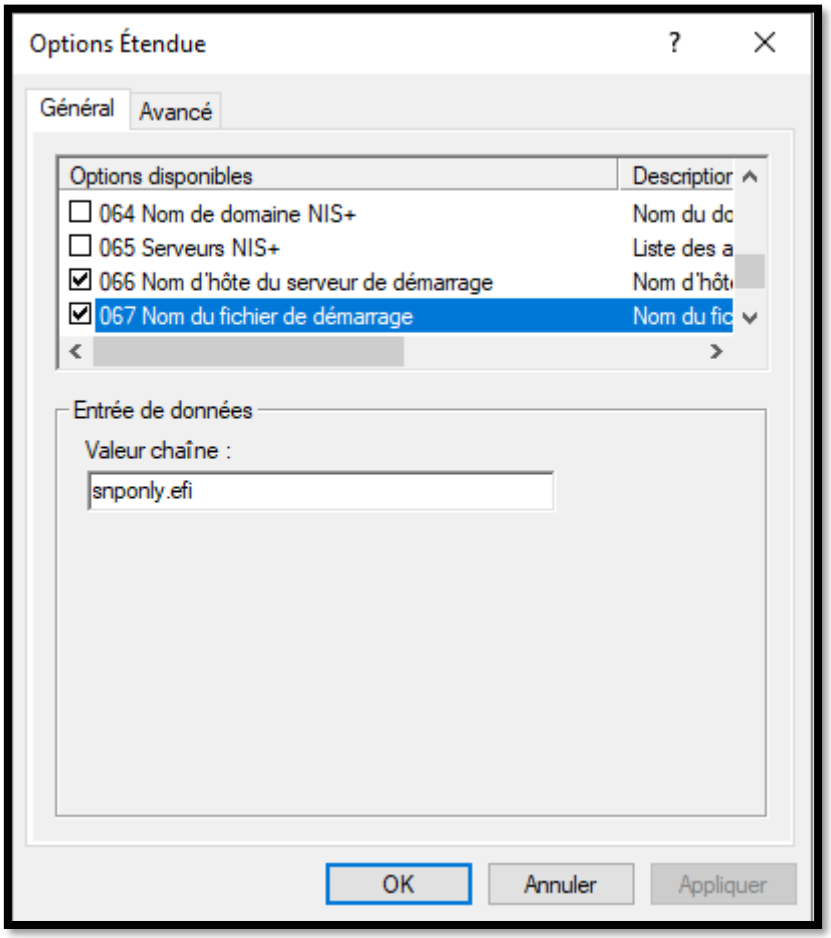

Figure 16 : Configuration des options d'étendues DHCP (2)

Lors du démarrage sur un poste client du réseau en PXE, on arrive sur l'interface FOG ce qui signifie que le déploiement a fonctionné. On peut maintenant capturer puis déployer une image. Pour cela, on lance l'option « Quick Registration and Inventory ». Une fois cela terminé, sur l'interface web, on lance une tâche de capture sur le poste client qui est maintenant reconnu par FOG :

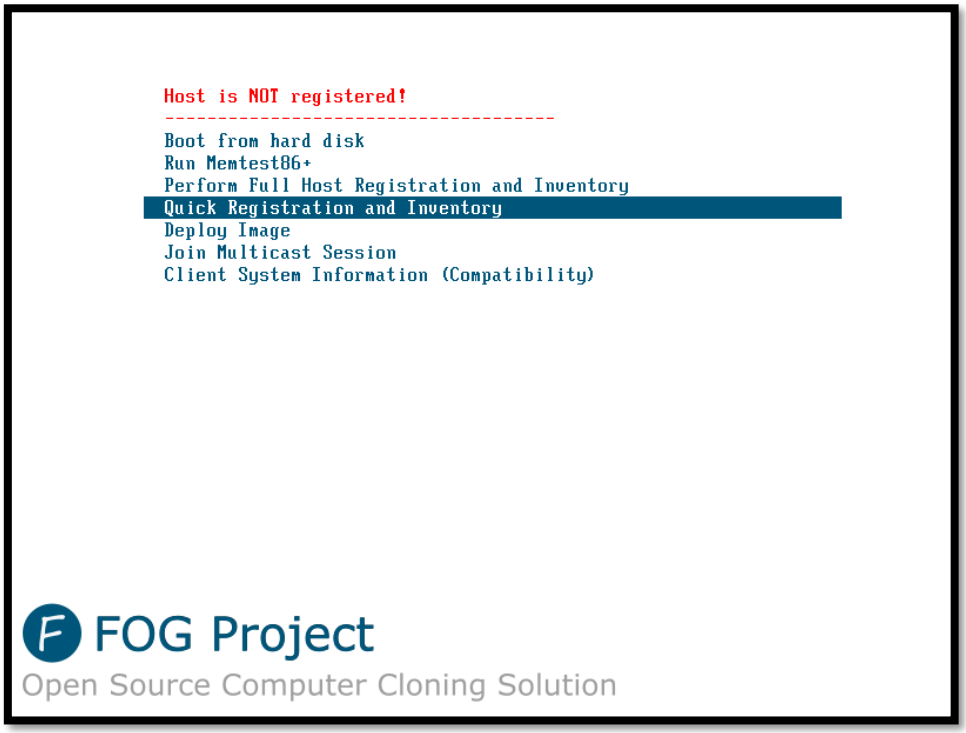

Figure 17 : Interface FOG lorsque l'on boot en PXE

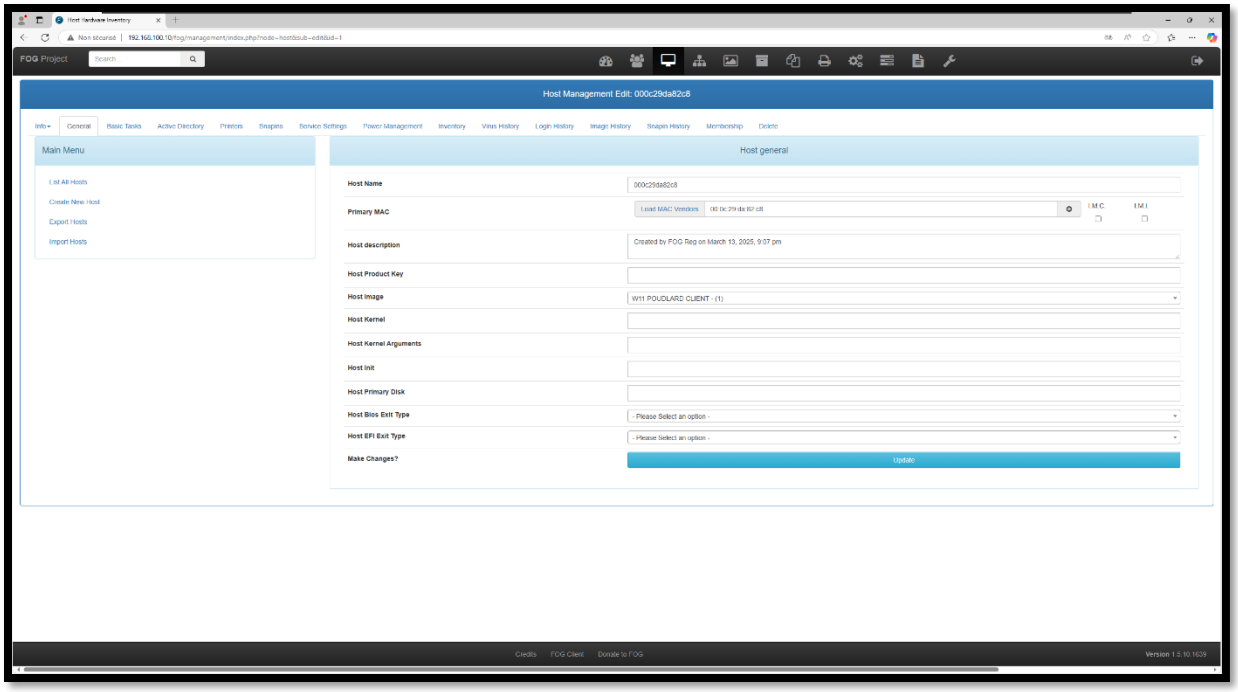

Figure 18 : Interface FOG lorsque l'on boot en PXE

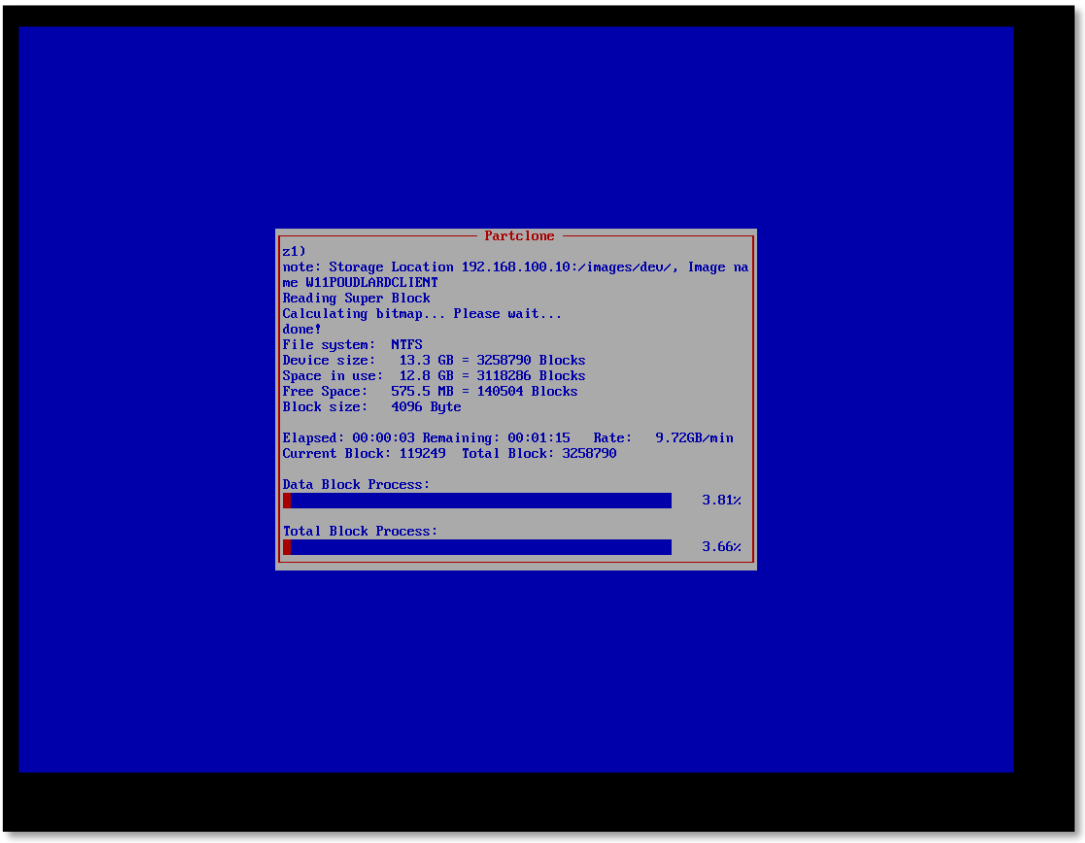

Figure 19 : Capture de l'image

Lorsque l’on redémarre FOG, l’image capturée est même prête à être déployée.

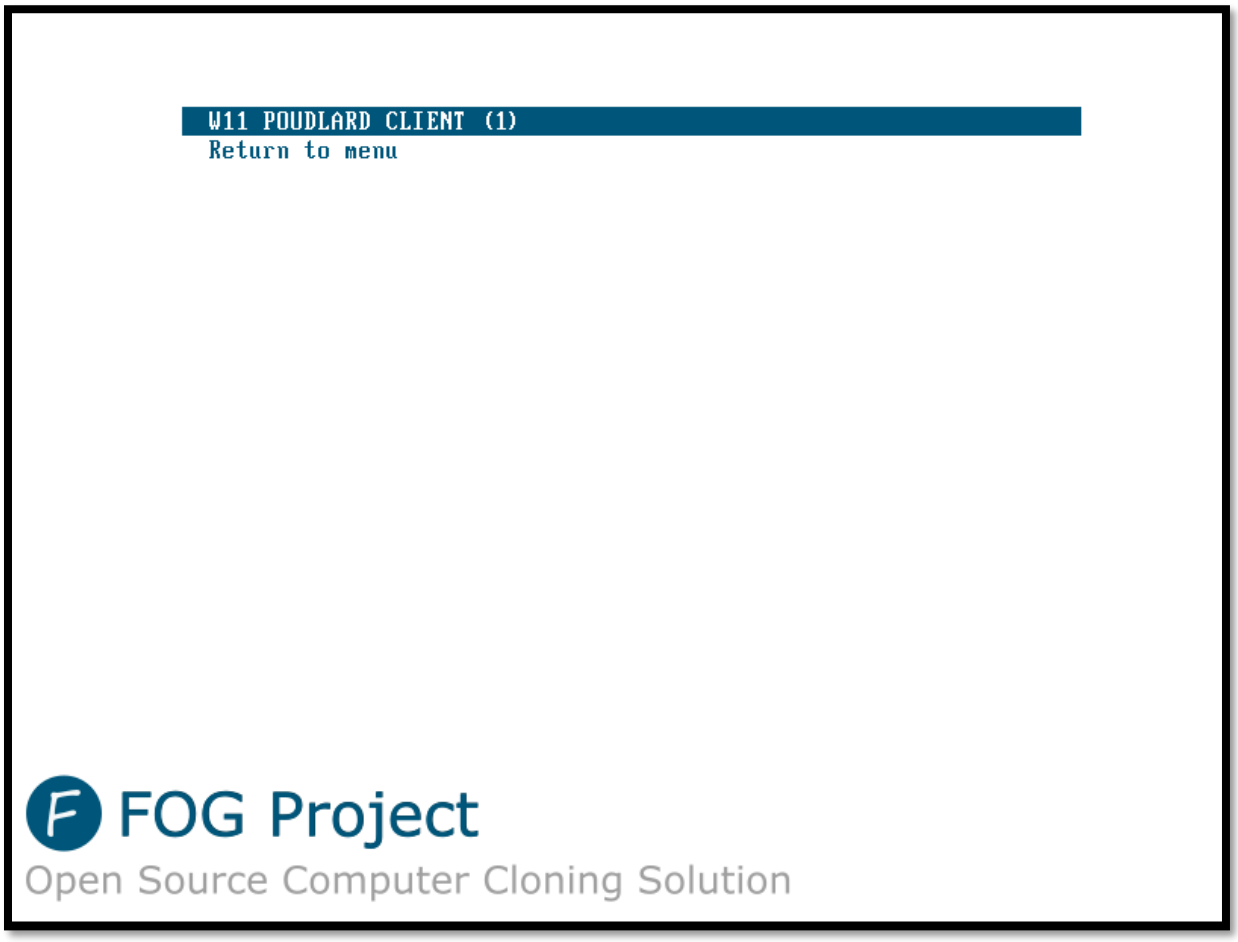

Figure 20 : L'image a été capturée et peut maintenant être déployée

IV. Déploiement d'un VPN (Open VPN) client to site

Afin de permettre aux techniciens informatiques d'accéder au réseau de l'école, on déploie un serveur VPN de type client-to-site (Open VPN). La connexion passera par un tunnel sur le réseau 10.10.10.0/24.

Tout d'abord, on créé un certificat qui permet de rendre le tunnel VPN plus sécurisé

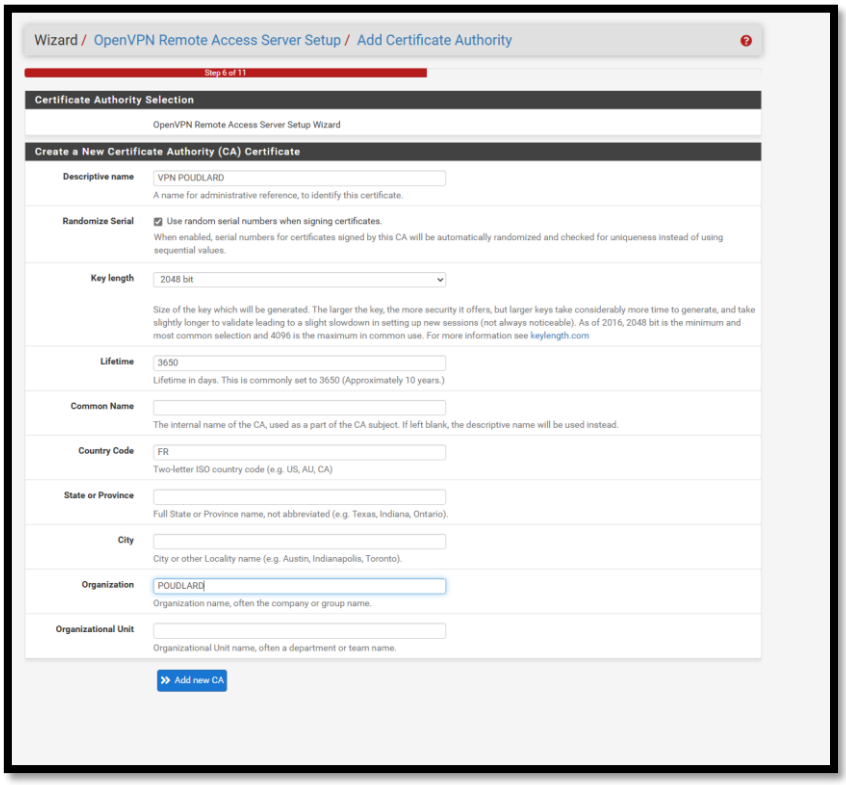

Figure 21 : Création d'un certificat d'autorité

On créé ensuite un utilisateur local pour lequel on attribue un certificat utilisateur qui permettra se connecter au VPN via cet utilisateur :

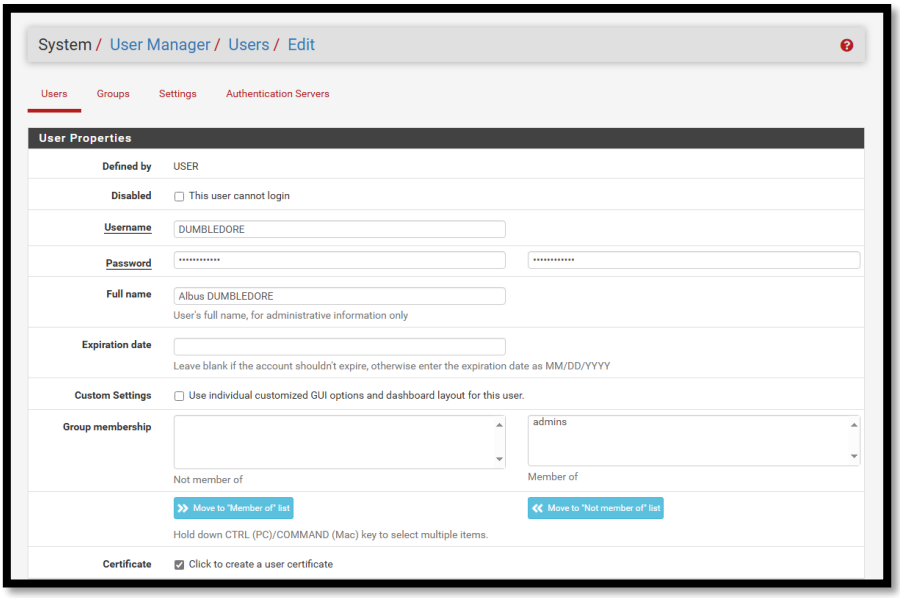

Figure 22 : Création d'un utilisateur pour l'accès VPN

On peut maintenant configurer le serveur OpenVPN (on change le port VPN qui par défaut est 1194 et on le passe à 1199

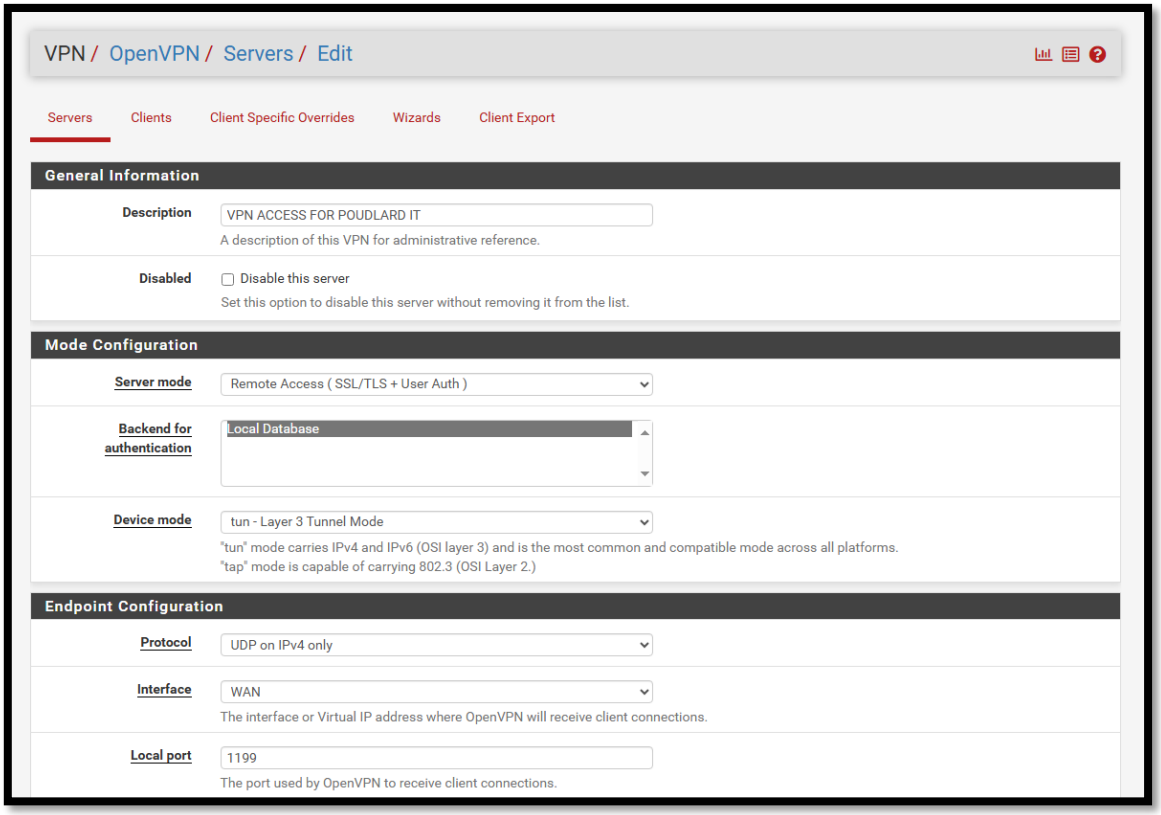

Figure 23 : Configuration du VPN

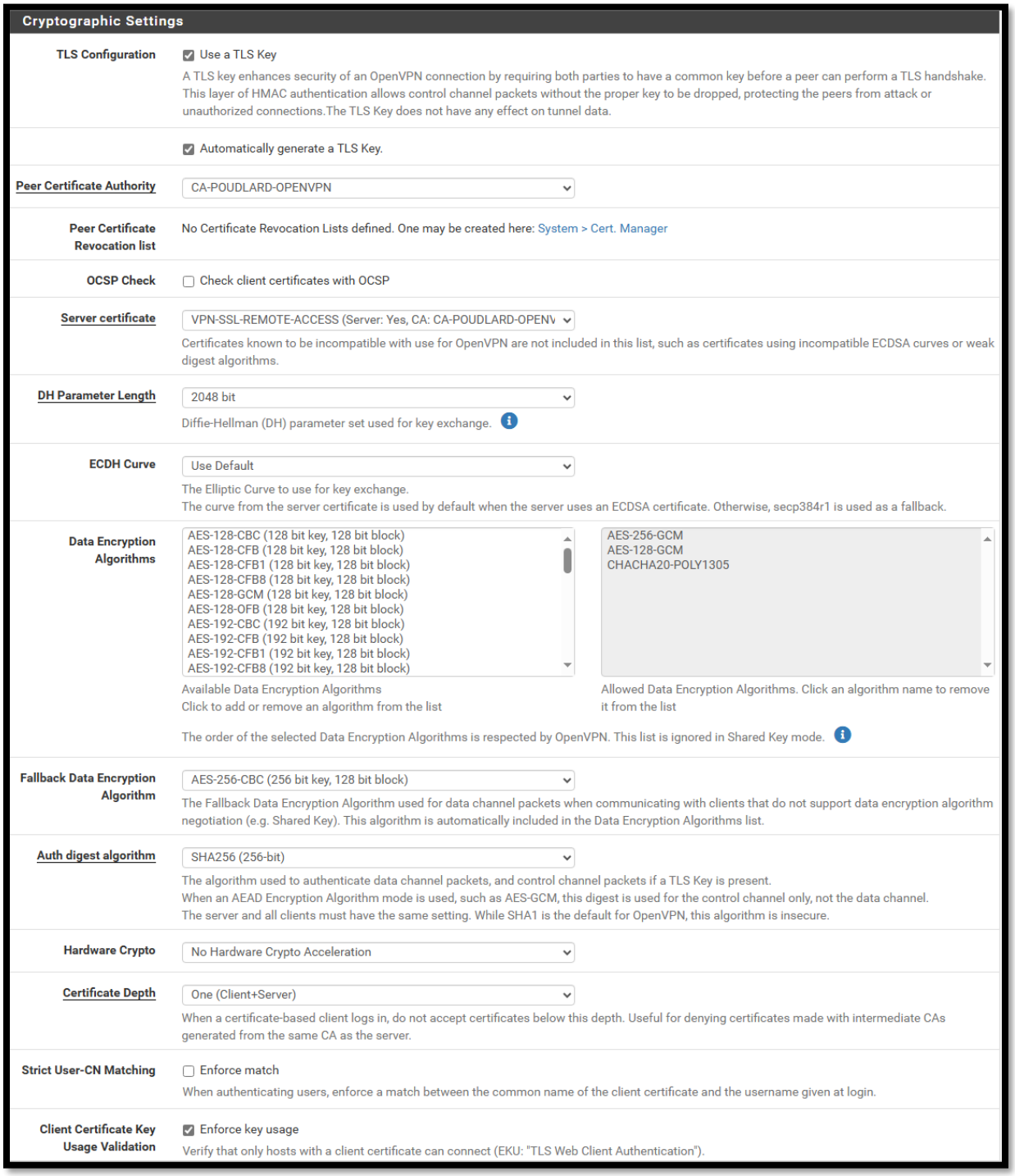

Figure 24 : Configuration du VPN (2)

On précise maintenant l'adresse du tunnel par lequel le VPN va passer (10.10.10.0/24) ainsi que l'adresse du réseau auquel on veut accéder (192.168.100.0/24) :

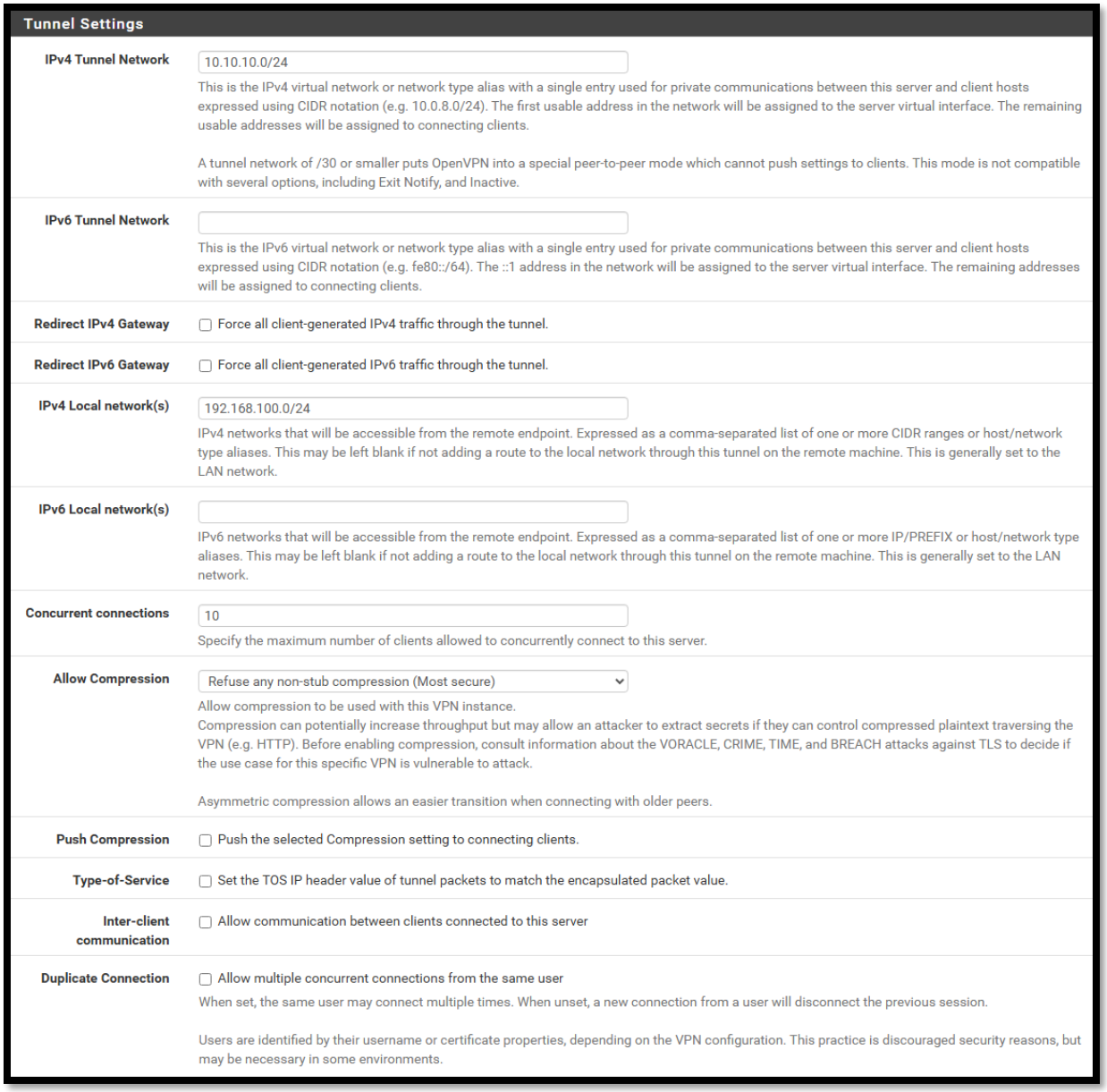

Figure 25 : Configuration du VPN (3)

Ici, on précise l'adresse du ou des serveurs DNS du réseau cible :

Figure 26 : Configuration du VPN (4)

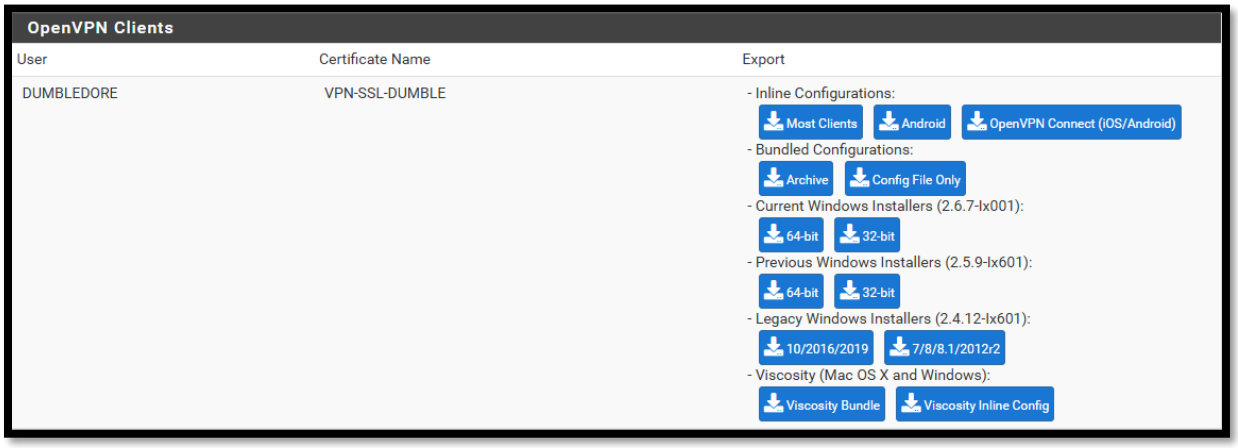

Figure 27 : Exportation de la configuration VPN

On créé une règle de filtrage qui permet au service RDP de fonctionner via la connexion VPN.

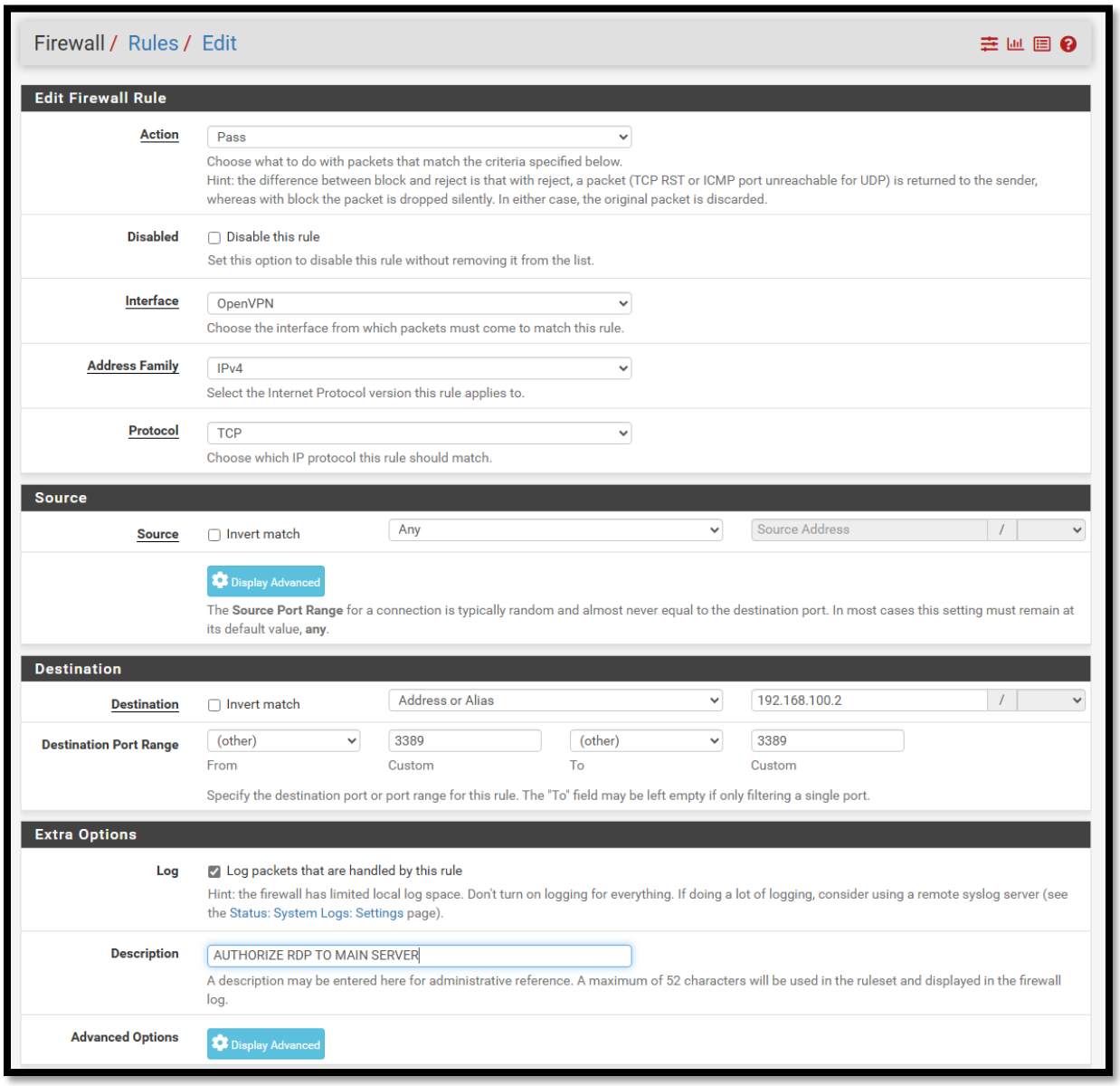

Figure 28 : Création d'une règle de filtrage pour permettre au service RDP de fonctionner

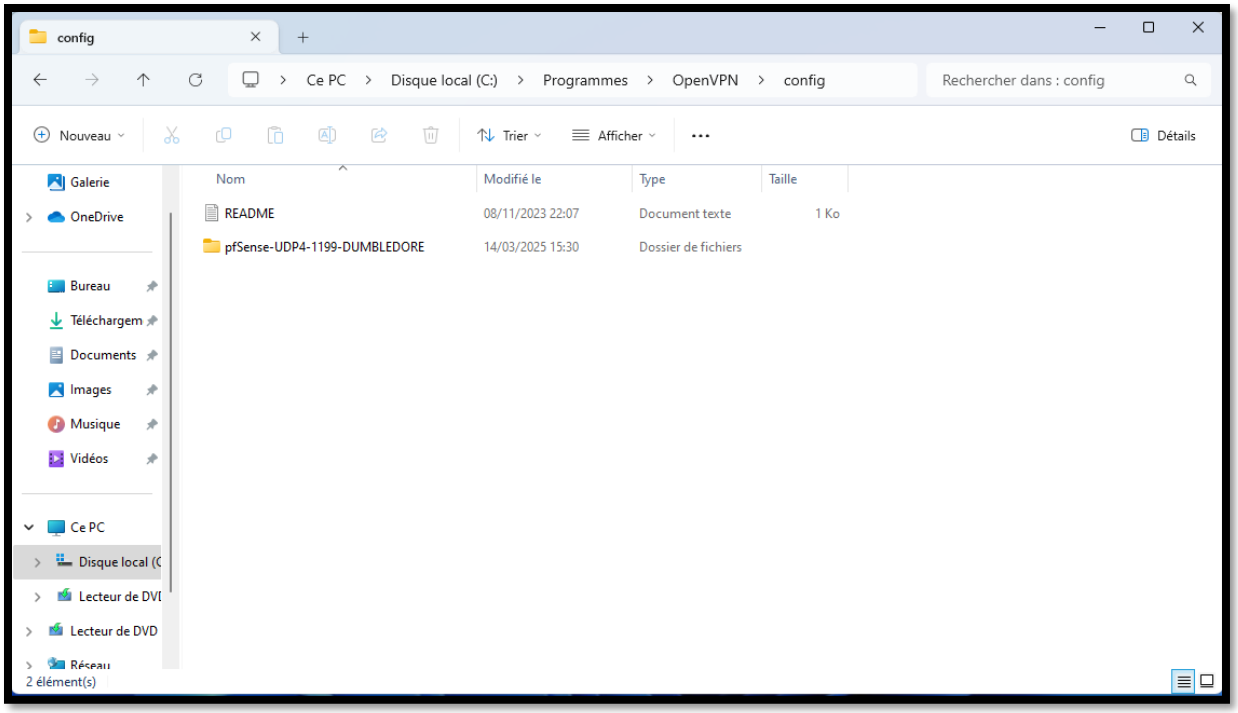

Figure 29 : Importation de la configuration VPN

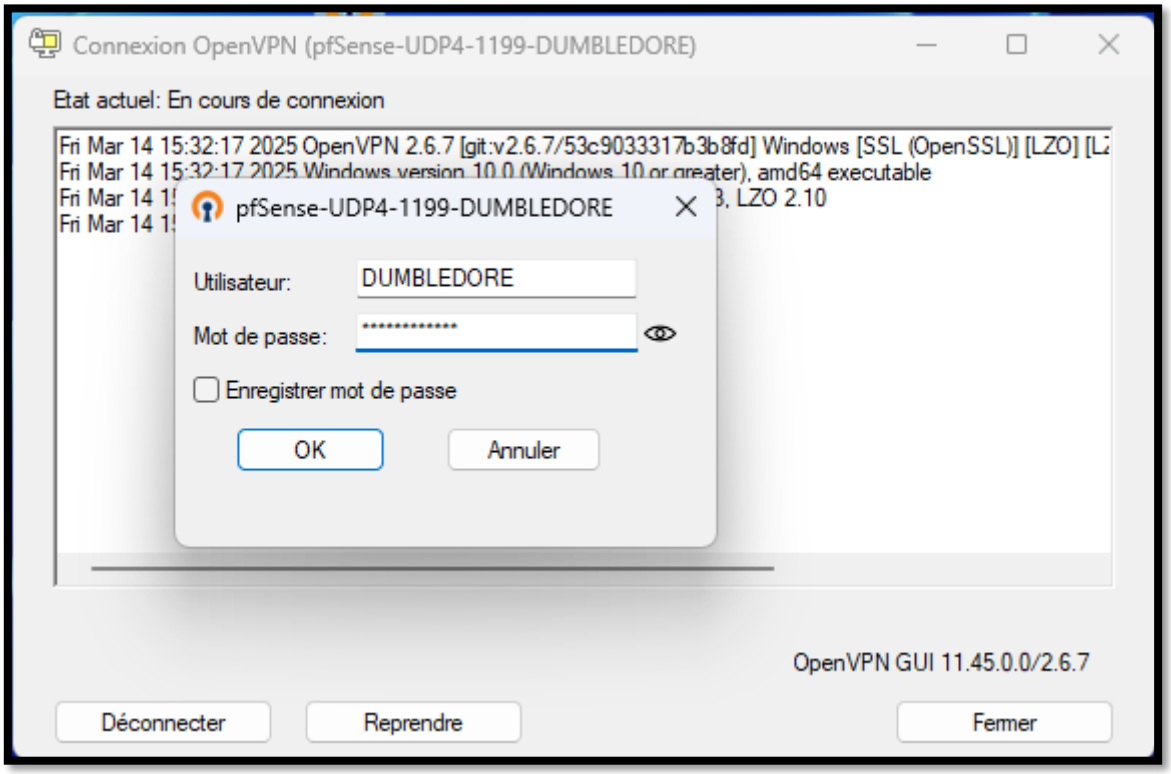

Figure 30 : Connexion VPN

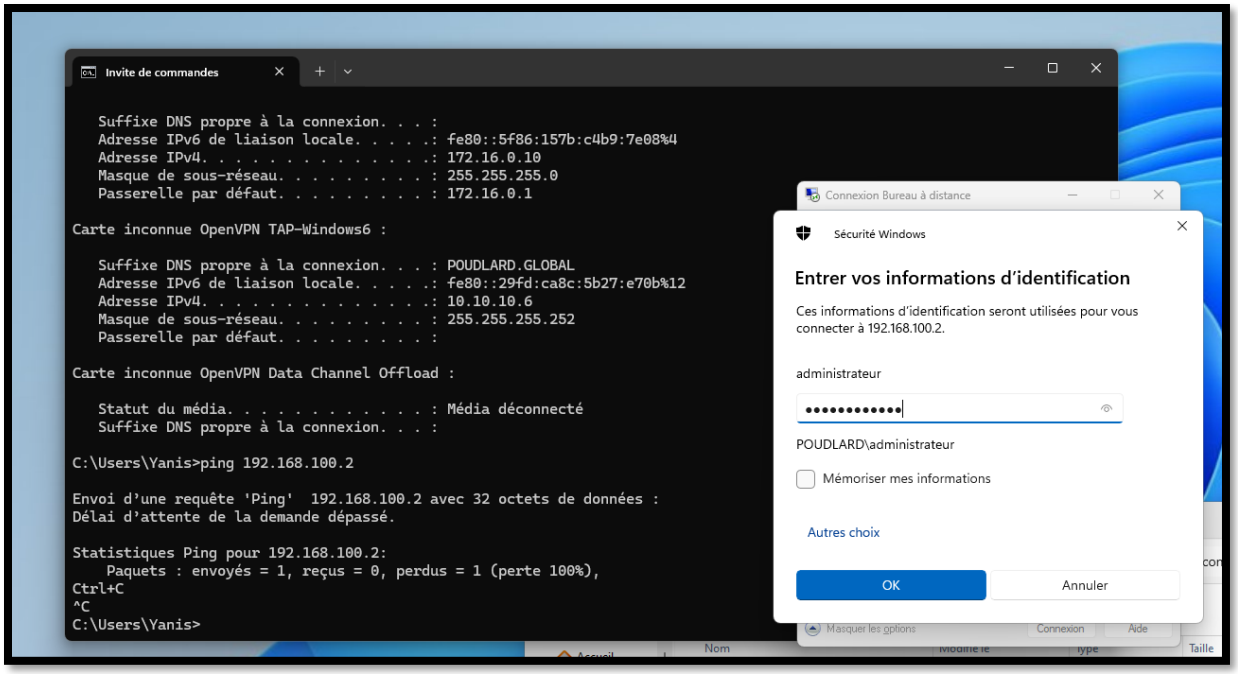

Figure 31 : La connexion RDS s'initie

On constate bien qu'après exportation de la configuration VPN sur le poste technicien en dehors du réseau, la connexion VPN s'établit correctement via le tunnel à l'adresse 10.10.10.6. On peut se connecter via le service RDP sur le serveur AD principal.

V. Mise en place de sauvegarde de postes (Veeam Backup)