

# BTS SIO - EPREUVE E5

## PROJET N°2

Yanis Mingam

KEYCE ACADEMY OGEC D'ALZON

## Table des matières

I.	Mise en contexte .....	2
II.	Configuration du Routeur / Pare-Feu (PfSense).....	<b>Erreur ! Signet non défini.</b>
III.	Configuration du serveur principal (AD-DS).....	8
IV.	Création d'Unités d'Organisation (UO) et création d'utilisateurs .....	<b>Erreur ! Signet non défini.</b>
V.	Configuration des machines clientes (Windows 11).....	<b>Erreur ! Signet non défini.</b>
VI.	Mise en place de dossiers partagés selon l'UO (secrétariat, RH, comptabilité, etc).....	<b>Erreur ! Signet non défini.</b>
VII.	Mise en place de GPO spécifiques .....	<b>Erreur ! Signet non défini.</b>
VIII.	Configuration du serveur de redondance .....	<b>Erreur ! Signet non défini.</b>
IX.	Configuration avancée du Routeur / Pare-Feu PfSense (DHCP, règles de filtrage, vlan).....	<b>Erreur ! Signet non défini.</b>

## 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 ce principe, on tentera au maximum de privilégier des solutions gratuites.

Voici le plan de l'infrastructure :

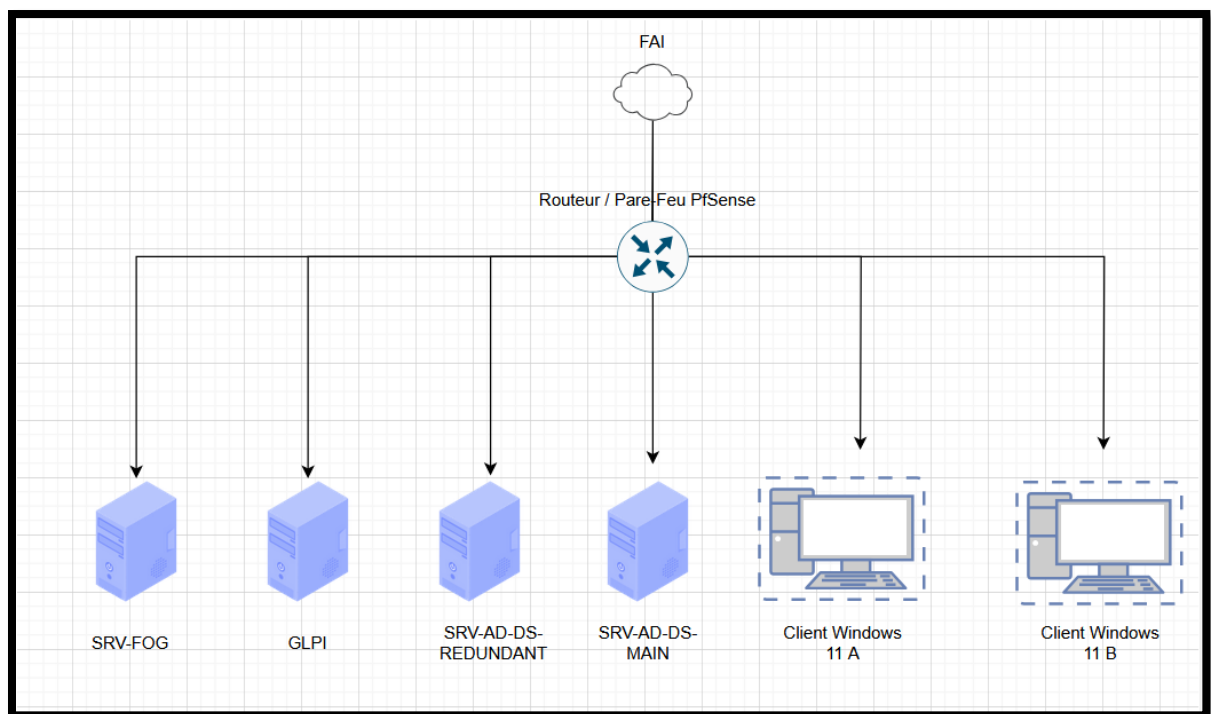


Figure 1 - Schéma de l'infrastructure

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 -xzf 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

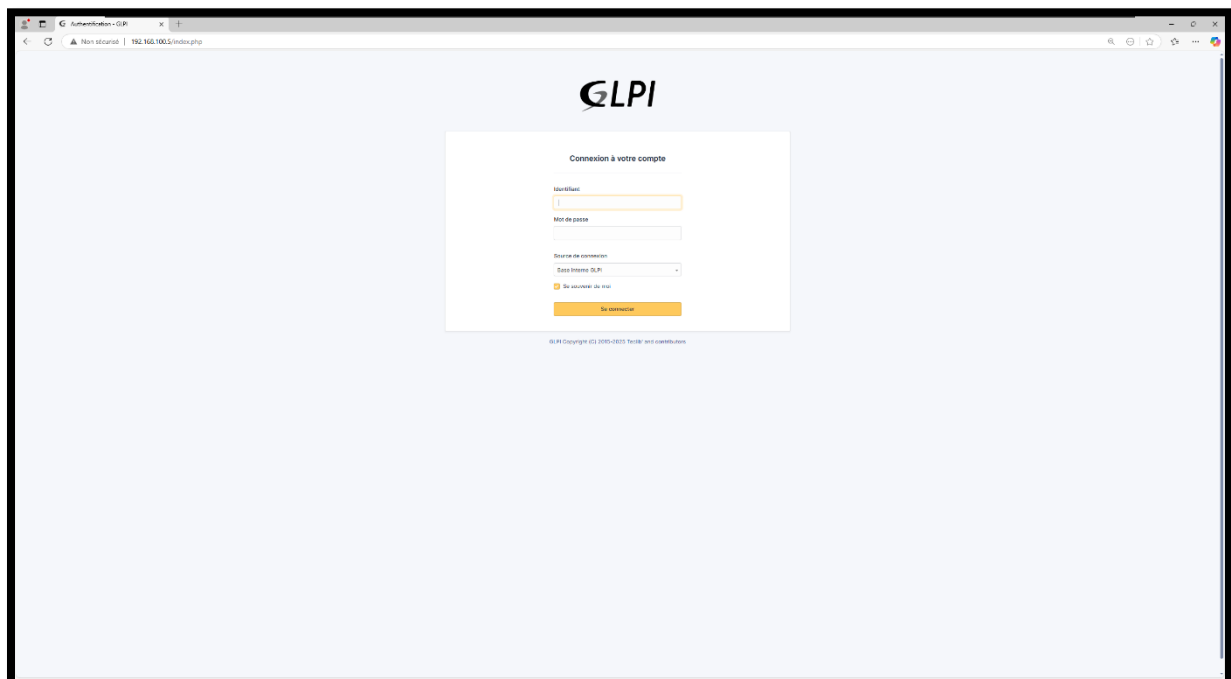


Figure 9 : Page de connexion GLPI

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

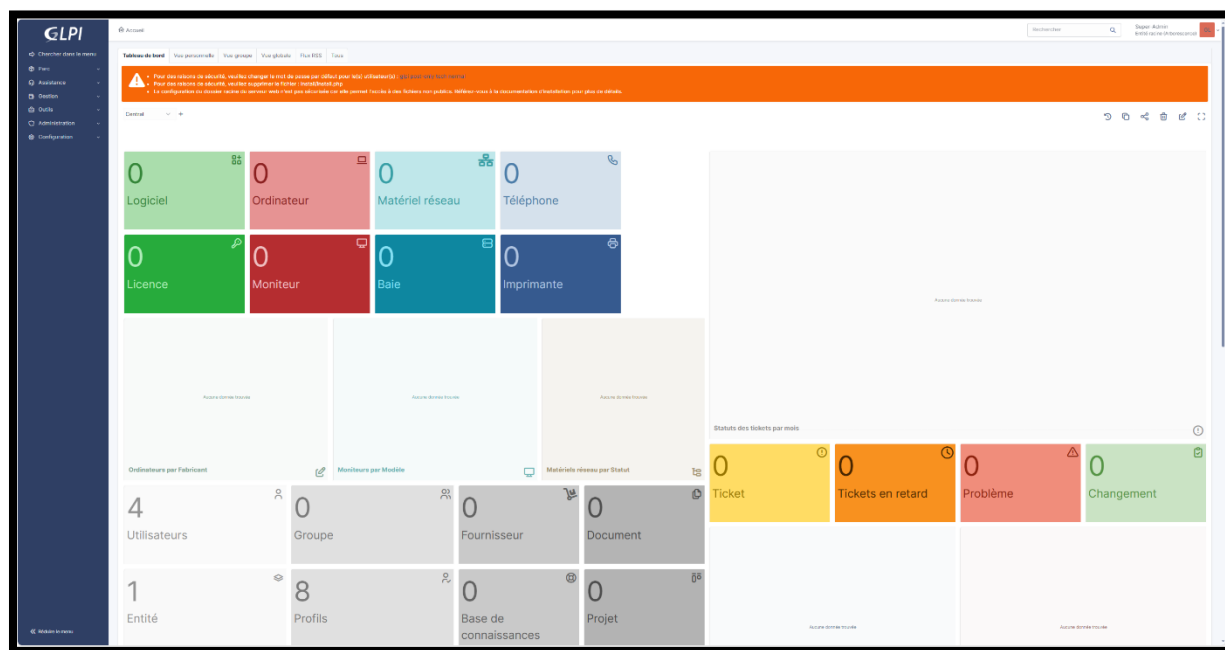


Figure 10 : Interface GLPI



### 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 :

```
#####
# FOG now has everything it needs for this setup, but please #
# understand that this script will overwrite any setting you may #
# have setup for services like DHCP, apache, pxe, tftp, and NFS. #
#####
# It is not recommended that you install this on a production system #
# as this script modifies many of your system settings. #
#####
# This script should be run by the root user. #
# It will prepend the running with sudo if root is not set #
#####
# Please see our wiki for more information at: #
# https://wiki.fogproject.org/wiki/index.php #
#####

* Here are the settings FOG will use:
* Base Linux: Debian
* Detected Linux Distribution: Debian GNU/Linux
* Interface: ens33
* Server IP Address: 192.168.100.10
* Server Subnet Mask: 255.255.255.0
* Hostname: FOG-POUDLARD
* Installation Type: Normal Server
* Internationalization: Yes
* Image Storage Location: /images
* Using FOG DHCP: No
* DHCP will NOT be setup but you must setup your
| current DHCP server to use FOG for PXE services.

* On a Linux DHCP server you must set: next-server and filename
* On a Windows DHCP server you must set options 066 and 067

* Option 066/next-server is the IP of the FOG Server: (e.g. 192.168.100.10)
* Option 067/filename is the bootfile: (e.g. undionly.kkpxe or snponly.efi)
* Send OS Name, OS Version, and FOG Version: No

* Are you sure you wish to continue (Y/N) Y
```

Figure 11 : Installation du serveur FOG

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

```
* You still need to install/update your database schema.
* This can be done by opening a web browser and going to:
http://192.168.100.10/fog/management
* Press [Enter] key when database is updated/installed.█
```

Figure 12 : L'interface web FOG est maintenant disponible

```
* Press [Enter] key when database is updated/installed.

* Update fogstorage database password.....OK
* Granting access to fogstorage database user.....OK
* Setting up storage.....OK
* Setting up and starting DHCP Server.....Skipped
* Configuring default PXE file.....OK
* Setting up and starting TFTP Server.....OK
* Setting up and starting VSFTP Server.....OK
* Setting up FOG Snapins.....OK
* Setting up UDPcast.....OK
* Configuring UDPcast.....OK
* Building UDPcast.....OK
* Installing UDPcast.....OK
* Installing FOG System Scripts.....OK

* Configuring FOG System Services

* Setting permissions on FOGMulticastManager.service script...OK
* Enabling FOGMulticastManager.service Service.....OK
* Setting permissions on FOGImageReplicator.service script...OK
* Enabling FOGImageReplicator.service Service.....OK
* Setting permissions on FOGSnapshotReplicator.service script...OK
* Enabling FOGSnapshotReplicator.service Service.....OK
* Setting permissions on FOGScheduler.service script.....OK
* Enabling FOGScheduler.service Service.....OK
* Setting permissions on FOGPingHosts.service script.....OK
* Enabling FOGPingHosts.service Service.....OK
* Setting permissions on FOGSnapshotHash.service script.....OK
* Enabling FOGSnapshotHash.service Service.....OK
* Setting permissions on FOGImageSize.service script.....OK
* Enabling FOGImageSize.service Service.....OK
* Setting up FOG Services.....OK
* Starting FOGMulticastManager.service Service.....OK
* Starting FOGImageReplicator.service Service.....OK
* Starting FOGSnapshotReplicator.service Service.....OK
* Starting FOGScheduler.service Service.....OK
* Starting FOGPingHosts.service Service.....OK
* Starting FOGSnapshotHash.service Service.....OK
* Starting FOGImageSize.service Service.....OK
* Setting up NFS configuration file.....OK
* Setting up exports file.....OK
* Setting up and starting RPCbind.....OK
* Setting up and starting NFS Server.....OK
* Linking FOG Logs to Linux Logs.....OK
* Linking FOG Service config /etc.....OK
* Ensuring node username and passwords match.....Done

* Setup complete

You can now login to the FOG Management Portal using
the information listed below. The login information
is only if this is the first install.

This can be done by opening a web browser and going to:
http://192.168.100.10/fog/management

Default User Information
Username: fog
Password: password

* Changed configurations:

The FOG installer changed configuration files and created the
following backup files from your original files:
* /etc/vsftpd.conf <=> /etc/vsftpd.conf.1741816077
* /etc/exports <=> /etc/exports.1741816077
```

Figure 13 : La base de données est créée

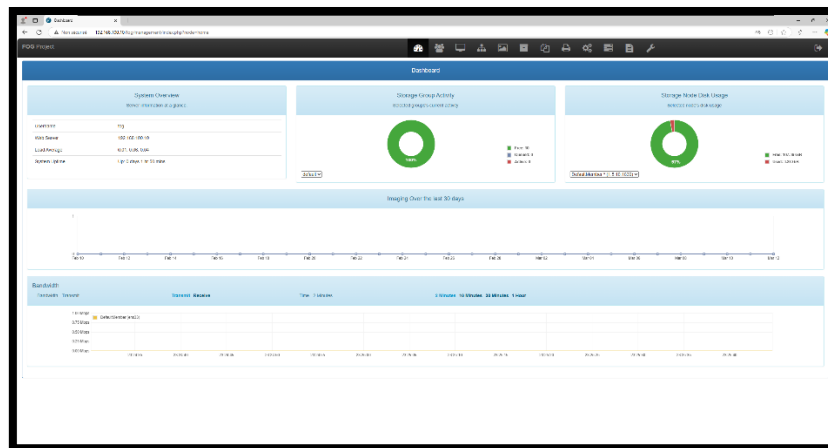


Figure 14 – Interface web FOG

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 :

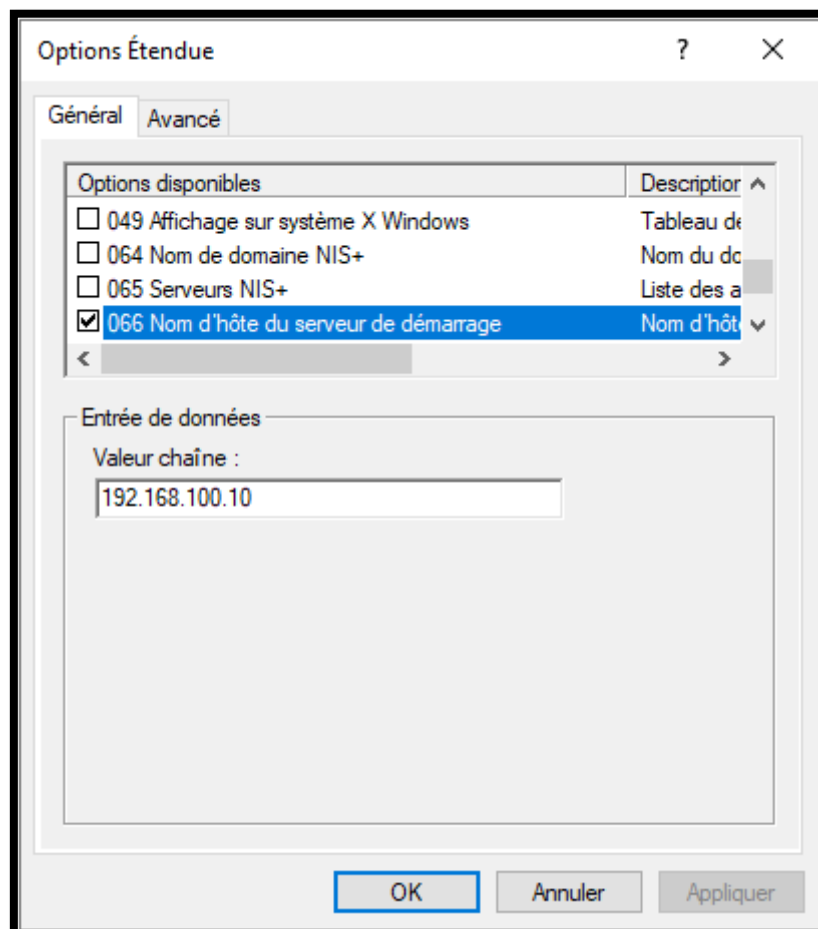


Figure 15 : Configuration des options d'étendues DHCP (1)

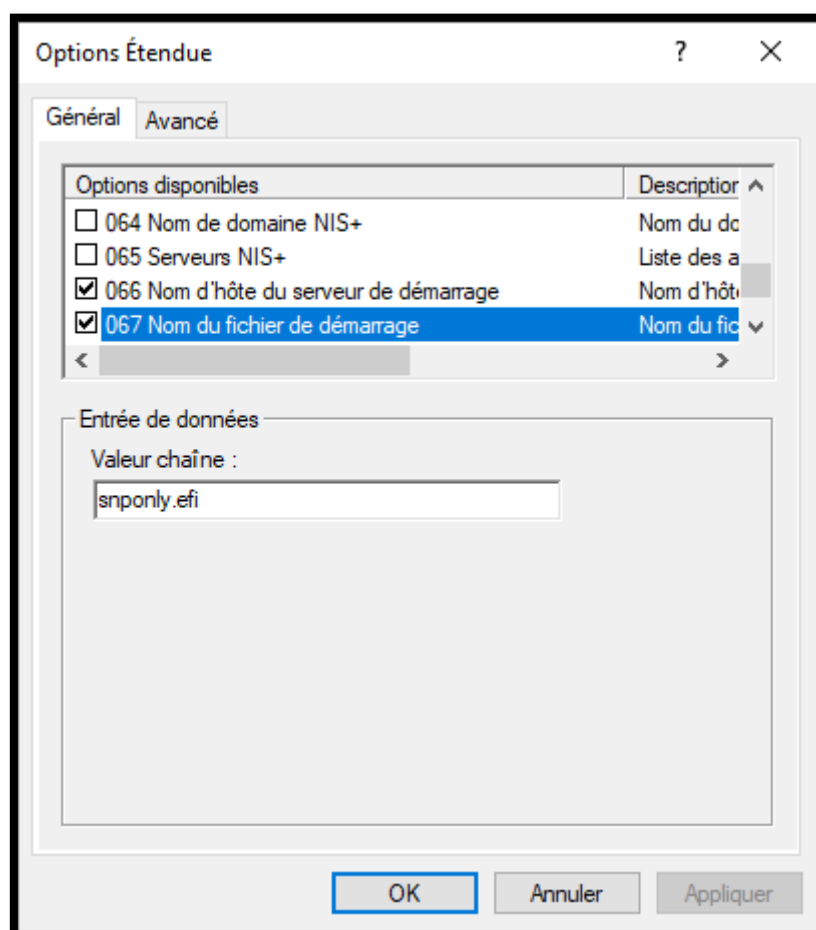


Figure 16 : Configuration des options d'étendues DHCP (2)

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 :

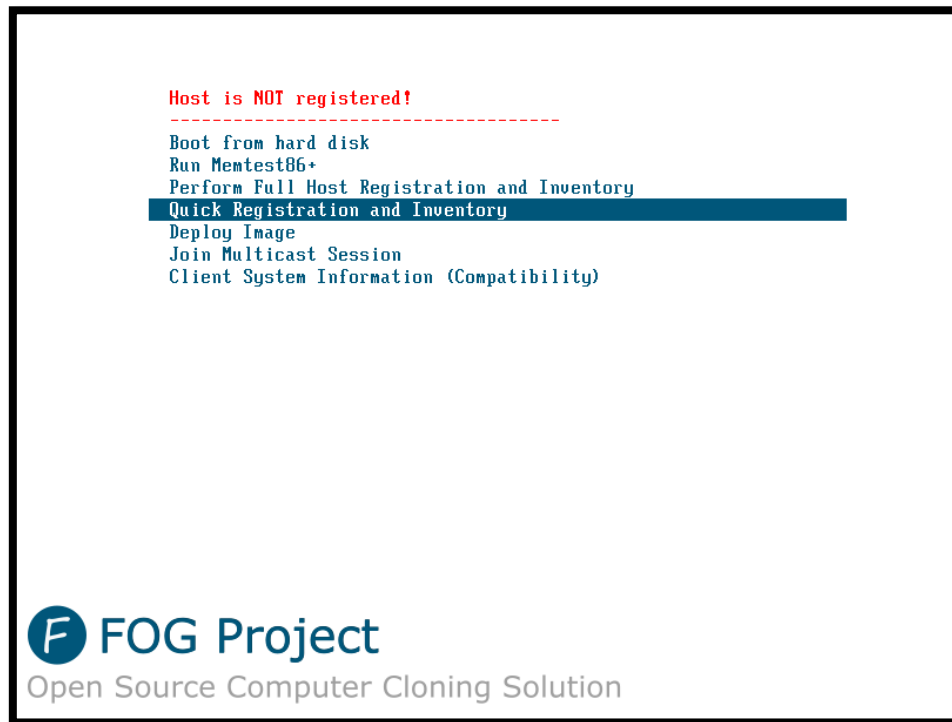
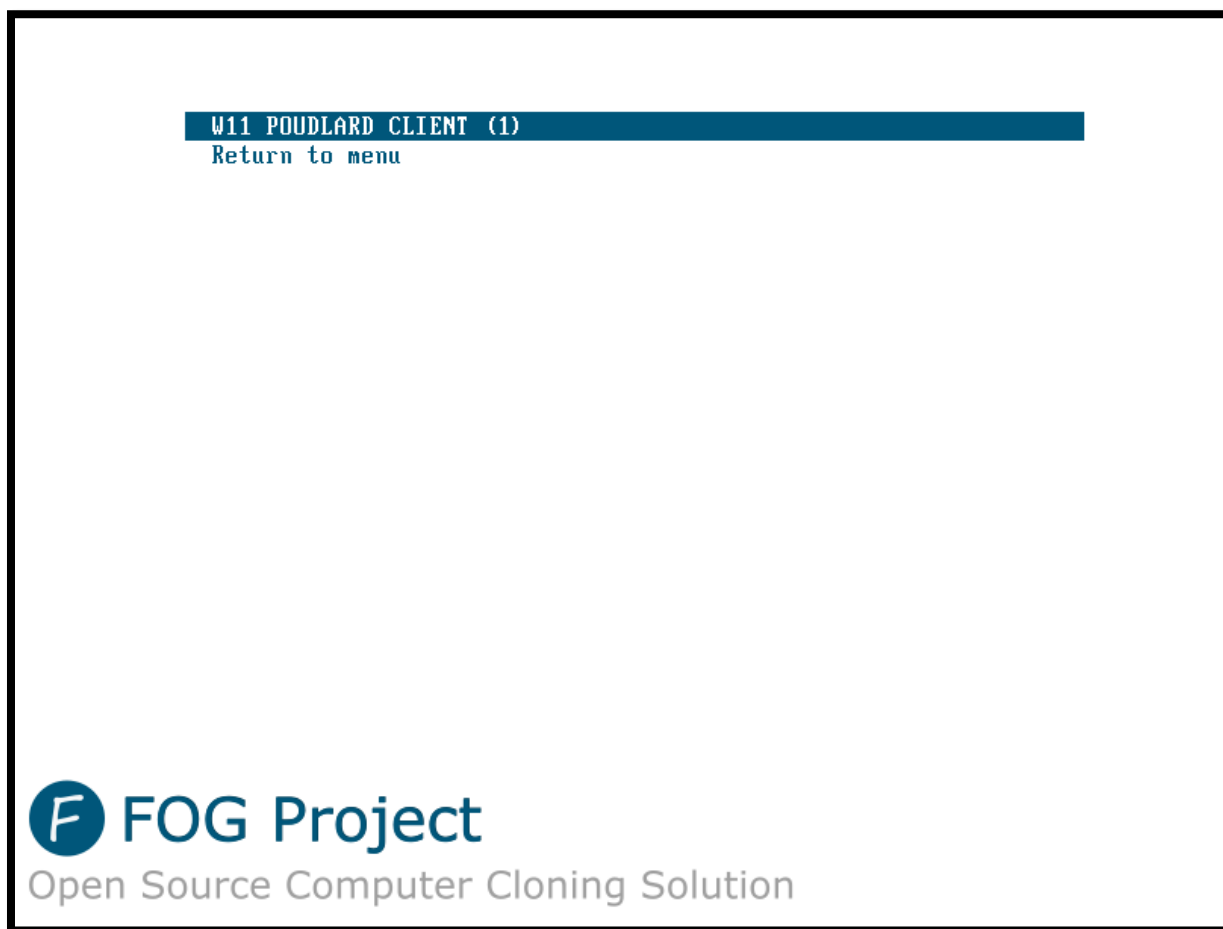


Figure 17 : Interface FOG lorsque l'on boot en PXE



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 crée un certificat qui permet de rendre le tunnel VPN plus sécurisé

Wizard / OpenVPN Remote Access Server Setup / Add Certificate Authority

Step 6 of 11

**Certificate Authority Selection**

OpenVPN Remote Access Server Setup Wizard

**Create a New Certificate Authority (CA) Certificate**

**Descriptive name** VPN POUJLARD  
A name for administrative reference, to identify this certificate.

**Randomize Serial** ☒ Use random serial numbers when signing certificates.  
When enabled, serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using sequential values.

**Key length** 2048 bit  
Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see [keylength.com](http://keylength.com)

**Lifetime** 3650  
Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)

**Common Name**  
The internal name of the CA, used as a part of the CA subject. If left blank, the descriptive name will be used instead.

**Country Code** FR  
Two-letter ISO country code (e.g. US, AU, CA)

**State or Province**  
Full State or Province name, not abbreviated (e.g. Texas, Indiana, Ontario).

**City**  
City or other Locality name (e.g. Austin, Indianapolis, Toronto).

**Organization** POUJLARD  
Organization name, often the company or group name.

**Organizational Unit**  
Organizational Unit name, often a department or team name.

[Add new CA](#)

Figure 21 : Création d'un certificat d'autorité

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



System / User Manager / Users / Edit

Users Groups Settings Authentication Servers

### User Properties

Defined by	USER
Disabled	<input type="checkbox"/> This user cannot login
Username	DUMBLEDORE
Password	*****
Full name	Albus DUMBLEDORE <small>User's full name, for administrative information only</small>
Expiration date	<input type="text"/> <small>Leave blank if the account shouldn't expire, otherwise enter the expiration date as MM/DD/YYYY</small>
Custom Settings	<input type="checkbox"/> Use individual customized GUI options and dashboard layout for this user.
Group membership	<div> <input type="text"/> <input type="button" value="Move to 'Member of' list"/> </div> <div> <input type="text"/> <input type="button" value="Move to 'Not member of' list"/> </div> <small>Hold down CTRL (PC)/COMMAND (Mac) key to select multiple items.</small>
Certificate	<input checked="" type="checkbox"/> Click to create a user certificate

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

VPN / OpenVPN / Servers / Edit

Servers Clients Client Specific Overrides Wizards Client Export

### General Information

Description	VPN ACCESS FOR POUDLARD IT <small>A description of this VPN for administrative reference.</small>
Disabled	<input type="checkbox"/> Disable this server <small>Set this option to disable this server without removing it from the list.</small>

### Mode Configuration

Server mode	Remote Access ( SSL/TLS + User Auth )
Backend for authentication	Local Database
Device mode	tun - Layer 3 Tunnel Mode <small>"tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms. "tap" mode is capable of carrying 802.3 (OSI Layer 2.)</small>

### Endpoint Configuration

Protocol	UDP on IPv4 only
Interface	WAN <small>The interface or Virtual IP address where OpenVPN will receive client connections.</small>
Local port	1199 <small>The port used by OpenVPN to receive client connections.</small>

Figure 23 : Configuration du VPN

Cryptographic Settings	
<b>TLS Configuration</b>	<input checked="" type="checkbox"/> Use a TLS Key A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.
	<input checked="" type="checkbox"/> Automatically generate a TLS Key.
<b>Peer Certificate Authority</b>	CA-POUDLARD-OPENVPN
<b>Peer Certificate Revocation list</b>	No Certificate Revocation Lists defined. One may be created here: <a href="#">System &gt; Cert. Manager</a>
<b>OCSP Check</b>	<input type="checkbox"/> Check client certificates with OCSP
<b>Server certificate</b>	VPN-SSL-REMOTE-ACCESS (Server: Yes, CA: CA-POUDLARD-OPENV Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.
<b>DH Parameter Length</b>	2048 bit Diffie-Hellman (DH) parameter set used for key exchange.
<b>ECDH Curve</b>	Use Default The Elliptic Curve to use for key exchange. The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.
<b>Data Encryption Algorithms</b>	<div> <div>           AES-128-CBC (128 bit key, 128 bit block)            AES-128-CFB (128 bit key, 128 bit block)            AES-128-CFB1 (128 bit key, 128 bit block)            AES-128-CFB8 (128 bit key, 128 bit block)            AES-128-GCM (128 bit key, 128 bit block)            AES-128-OFB (128 bit key, 128 bit block)            AES-192-CBC (192 bit key, 128 bit block)            AES-192-CFB (192 bit key, 128 bit block)            AES-192-CFB1 (192 bit key, 128 bit block)            AES-192-CFB8 (192 bit key, 128 bit block)         </div> <div>           AES-256-GCM            AES-128-GCM            CHACHA20-POLY1305         </div> </div> <p>Available Data Encryption Algorithms Click to add or remove an algorithm from the list</p> <p>Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list</p> <p>The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode.</p>
<b>Fallback Data Encryption Algorithm</b>	AES-256-CBC (256 bit key, 128 bit block) The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.
<b>Auth digest algorithm</b>	SHA256 (256-bit) The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present. When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel. The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.
<b>Hardware Crypto</b>	No Hardware Crypto Acceleration
<b>Certificate Depth</b>	One (Client+Server) When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.
<b>Strict User-CN Matching</b>	<input type="checkbox"/> Enforce match When authenticating users, enforce a match between the common name of the client certificate and the username given at login.
<b>Client Certificate Key Usage Validation</b>	<input checked="" type="checkbox"/> Enforce key usage Verify that only hosts with a client certificate can connect (EKU: "TLS Web Client Authentication").

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) :

Tunnel Settings	
<b>IPv4 Tunnel Network</b>	<input type="text" value="10.10.10.0/24"/> <p>This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.</p> <p>A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible with several options, including Exit Notify, and Inactive.</p>
<b>IPv6 Tunnel Network</b>	<input type="text"/> <p>This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.</p>
<b>Redirect IPv4 Gateway</b>	<input type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.
<b>Redirect IPv6 Gateway</b>	<input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel.
<b>IPv4 Local network(s)</b>	<input type="text" value="192.168.100.0/24"/> <p>IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. 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.</p>
<b>IPv6 Local network(s)</b>	<input type="text"/> <p>IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. 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.</p>
<b>Concurrent connections</b>	<input type="text" value="10"/> <p>Specify the maximum number of clients allowed to concurrently connect to this server.</p>
<b>Allow Compression</b>	<input type="text" value="Refuse any non-stub compression (Most secure)"/> <p>Allow compression to be used with this VPN instance.          Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack.</p> <p>Asymmetric compression allows an easier transition when connecting with older peers.</p>
<b>Push Compression</b>	<input type="checkbox"/> Push the selected Compression setting to connecting clients.
<b>Type-of-Service</b>	<input type="checkbox"/> Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
<b>Inter-client communication</b>	<input type="checkbox"/> Allow communication between clients connected to this server
<b>Duplicate Connection</b>	<input type="checkbox"/> Allow multiple concurrent connections from the same user <p>When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session.</p> <p>Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is discouraged security reasons, but may be necessary in some environments.</p>

Figure 25 : Configuration du VPN (3)

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

### Ping settings

Inactive

300

Causes OpenVPN to close a client connection after n seconds of inactivity on the TUN/TAP device. Activity is based on the last incoming or outgoing tunnel packet.

A value of 0 disables this feature.

This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.

Ping method

keepalive – Use keepalive helper to define ping configuration

keepalive helper uses interval and timeout parameters to define ping and ping-restart values as follows:

ping = interval

ping-restart = timeout\*2

push ping = interval

push ping-restart = timeout

Interval

10

Timeout

60

### Advanced Client Settings

DNS Default Domain

☒ Provide a default domain name to clients

DNS Default Domain

poudlard.local

DNS Server enable

☒ Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.

DNS Server 1

192.168.100.1

DNS Server 2

192.168.100.2

DNS Server 3

DNS Server 4

Block Outside DNS

☐ Make Windows 10 Clients Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.

Force DNS cache update

☐ Run "net stop dnscache", "net start dnscache", "ipconfig /flushdns" and "ipconfig /registerdns" on connection initiation. This is known to kick Windows into recognizing pushed DNS servers.

NTP Server enable

☐ Provide an NTP server list to clients

NetBIOS enable

☐ Enable NetBIOS over TCP/IP  
If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.

Figure 26 : Configuration du VPN (4)

### OpenVPN Clients

User	Certificate Name	Export
DUMBLEDORE	VPN-SSL-DUMBLE	<div> <div>Inline Configurations:</div> <div> <div>Most Clients</div> <div>Android</div> <div>OpenVPN Connect (iOS/Android)</div> </div> </div> <div> <div>Bundled Configurations:</div> <div> <div>Archive</div> <div>Config File Only</div> </div> </div> <div> <div>Current Windows Installers (2.6.7-1x001):</div> <div> <div>64-bit</div> <div>32-bit</div> </div> </div> <div> <div>Previous Windows Installers (2.5.9-1x601):</div> <div> <div>64-bit</div> <div>32-bit</div> </div> </div> <div> <div>Legacy Windows Installers (2.4.12-1x601):</div> <div> <div>10/2016/2019</div> <div>7/8/8.1/2012r2</div> </div> </div> <div> <div>Viscosity (Mac OS X and Windows):</div> <div> <div>Viscosity Bundle</div> <div>Viscosity Inline Config</div> </div> </div>

Figure 27 : Exportation de la configuration VPN

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

Firewall / Rules / Edit

### Edit Firewall Rule

**Action** Pass  
Choose what to do with packets that match the criteria specified below.  
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled** ☐ Disable this rule  
Set this option to disable this rule without removing it from the list.

**Interface** OpenVPN  
Choose the interface from which packets must come to match this rule.

**Address Family** IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol** TCP  
Choose which IP protocol this rule should match.

### Source

**Source** ☐ Invert match Any Source Address /   
[Display Advanced](#)  
The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

### Destination

**Destination** ☐ Invert match Address or Alias 192.168.100.2 /   
**Destination Port Range** (other) 3389 (other) 3389  
From Custom To Custom  
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

### Extra Options

**Log** ☒ Log packets that are handled by this rule  
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description** AUTHORIZE RDP TO MAIN SERVER  
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

**Advanced Options** [Display Advanced](#)

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

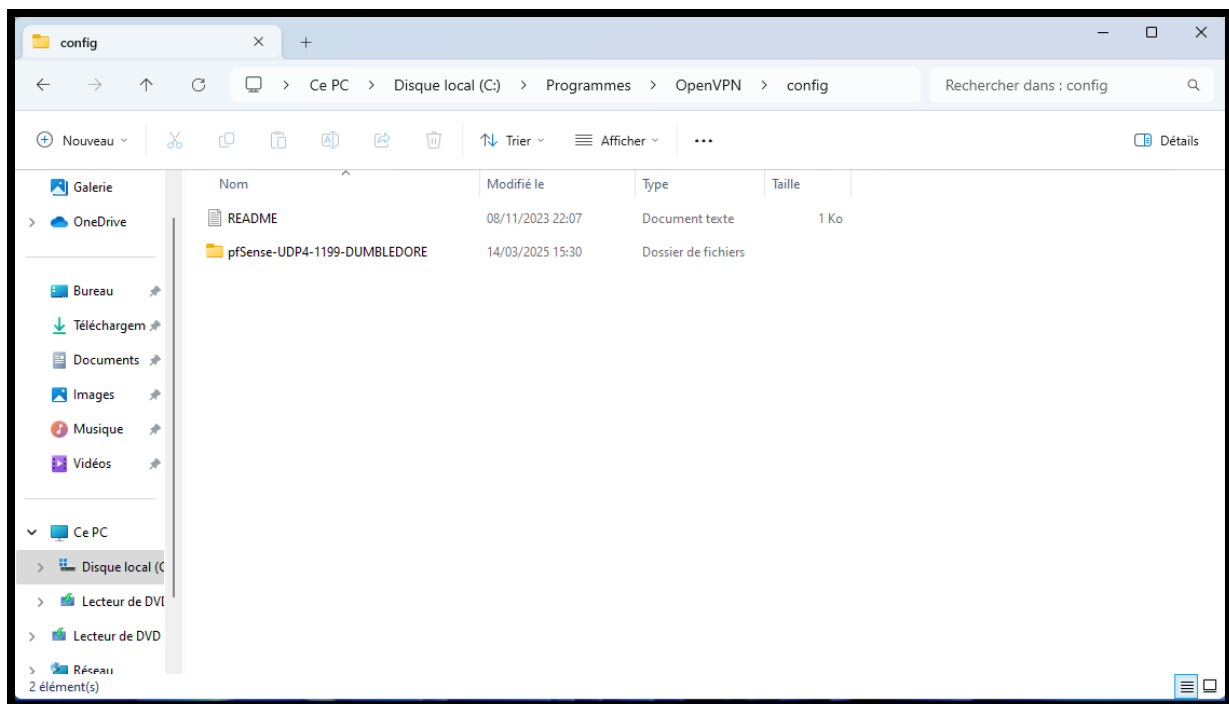


Figure 29 : Importation de la configuration VPN

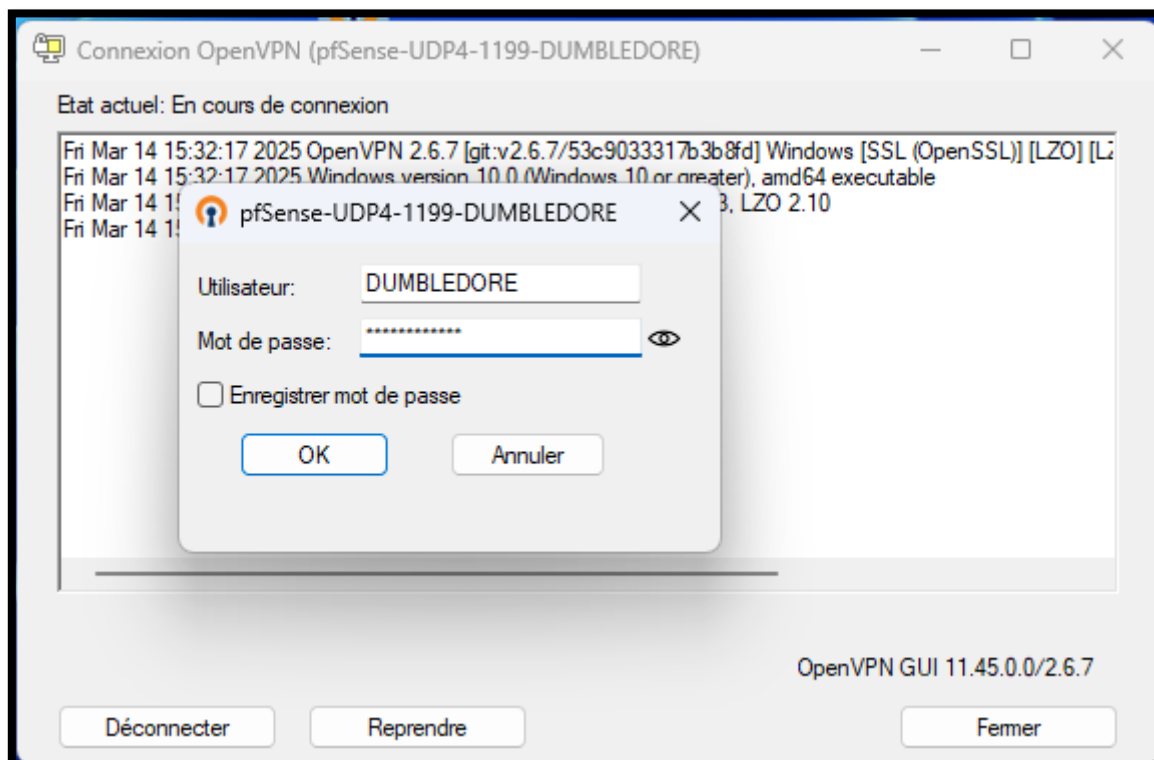


Figure 30 : Connexion VPN

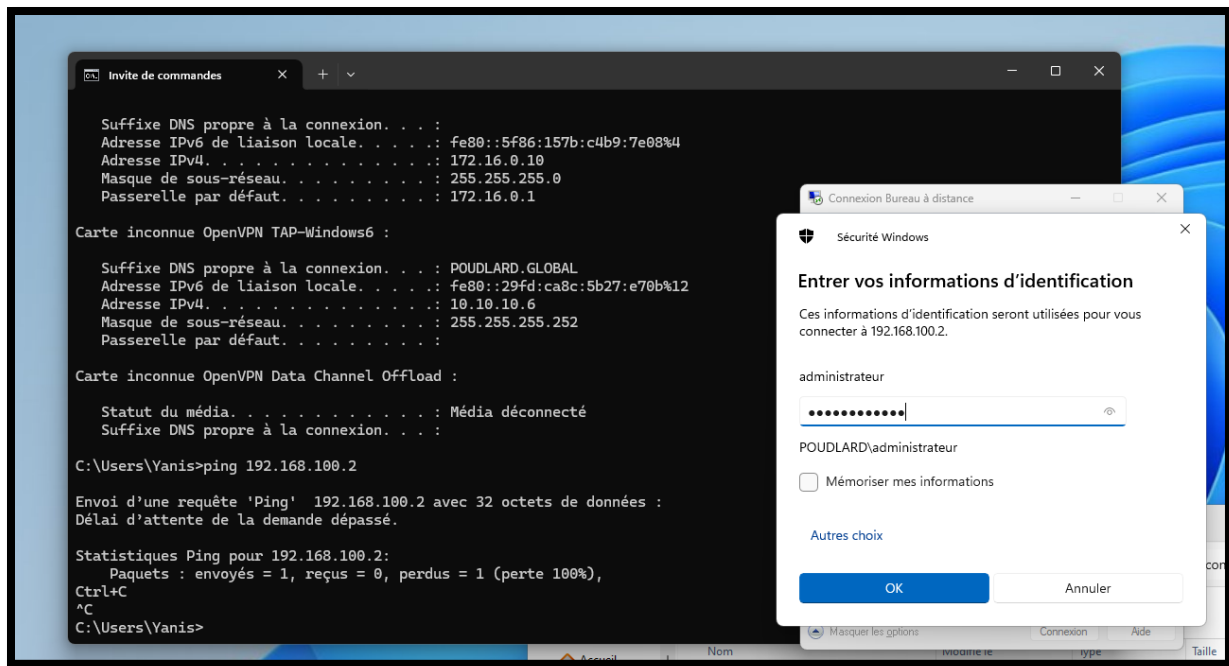


Figure 31 : La connexion RDS s'initie

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)