Projet de BTS Maison des Ligues

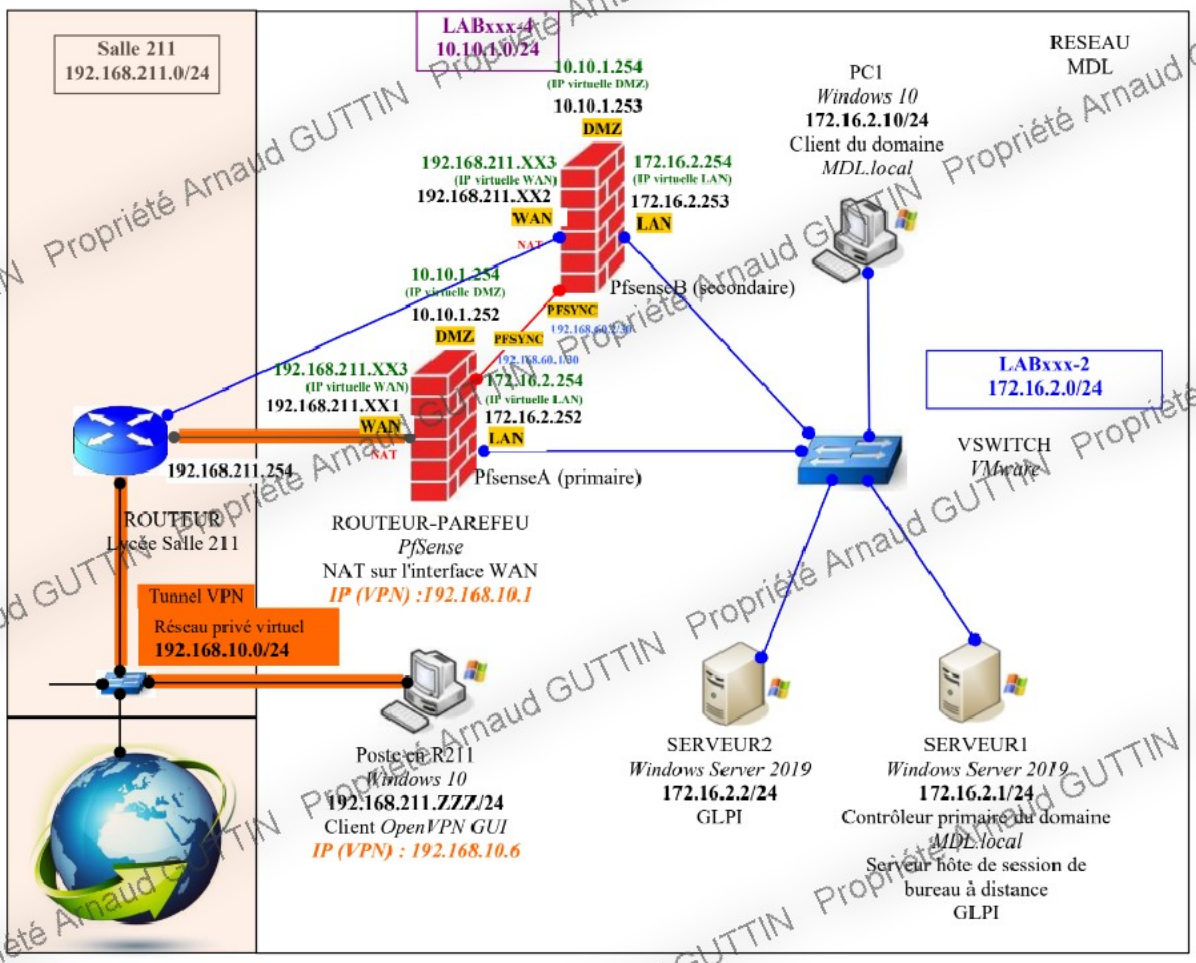
Présentation du projet MDL

Le projet MDL est une simulation de cas d'entreprise, il permet d'apprendre la mise en place d'une infrastructure d'entreprise.

Ce projet est constitué de différentes missions qui permettent d'apprendre la gestion d'un parc informatique, d'un Active directory et la mise en redondance de matériels.

Mission 1 : Installation du routeur-pare-feu PfSense
Mission 2 : Installation du serveur de domaine
Mission 3 : Inventaire du matériel avec GLPI/FusionInventory
Mission 4 : Installation d'un VPN-7
Mission 5 : Installation d'un serveur hôte de session Bureau à distance
Mission 6 : Configuration d'un cluster de deux Pfsense redondants (en Haute Disponibilité)

Schéma réseau du laboratoire de test



Mission 1 : Installation du routeur-pare-feu PfSense

Interfaces réseau de Pfsense

Interface physique	Interface Logique	MAC@	N°Adaptateur réseau	Etiquette réseau
vmx0	WAN	00:50:56:90:ec:7d	4	Salle 211
vmx1	LAN	00:50:56:90:4c:e5	1	LAB-SISR-5-2
vmx2	OPT1 (DMZ)	00:50:56:90:20:98	2	LAB-SISR-5-4
vmx3	OPT2 (pfsync)	00:50:56:90:66:31	3	LAB-SISR-5-3

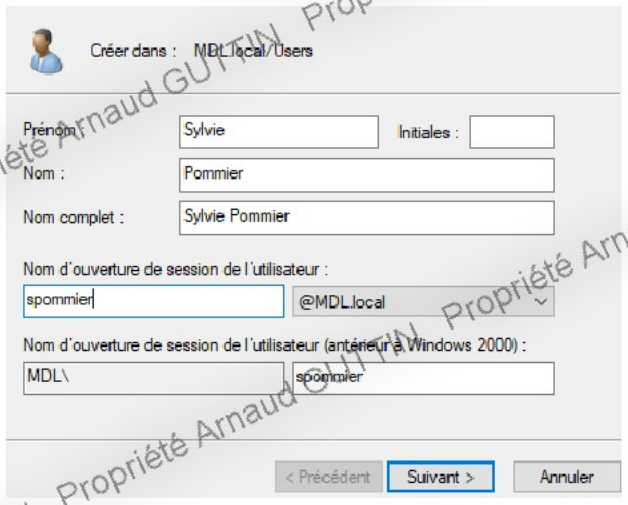
Mission 2 - Création du domaine et d'utilisateurs

Pour créer un domaine, il faudra ajouter le rôle Active Directory (ADDS).
On créera ensuite le domaine, ici MDL.local.

On ajoutera la liste des utilisateurs suivant:

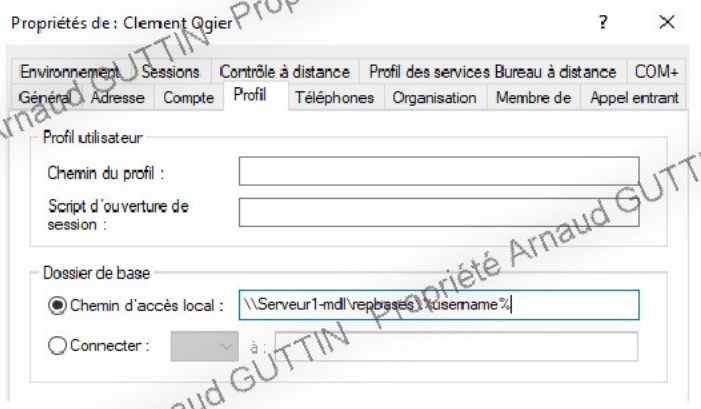
Nom et prénom	**Nom d'ouverture de session**	**Nom du dossier personnel**	**Mot de passe**
Clément Ogier	cogier	cogier	Windows2019
Laure Dubreuil	ldubreuil	ldubreuil	Windows2019
Sylvie Pommier	spommier	spommier	Windows2019
Kevin Dalle	kdalle	kdalle	Windows2019

Pour la création d'un utilisateur on ouvre Utilisateurs et Ordinateurs Active Directory. On clique sur ajouter un utilisateur puis on rentre ses informations.



Ajout d'un répertoire personnels pour les utilisateurs

Pour attribuer un répertoire personnel à un utilisateur, il faudra se rendre dans l'onglet profil, puis mettre le chemin de partage au dossier de base, (exemple ci-dessous).

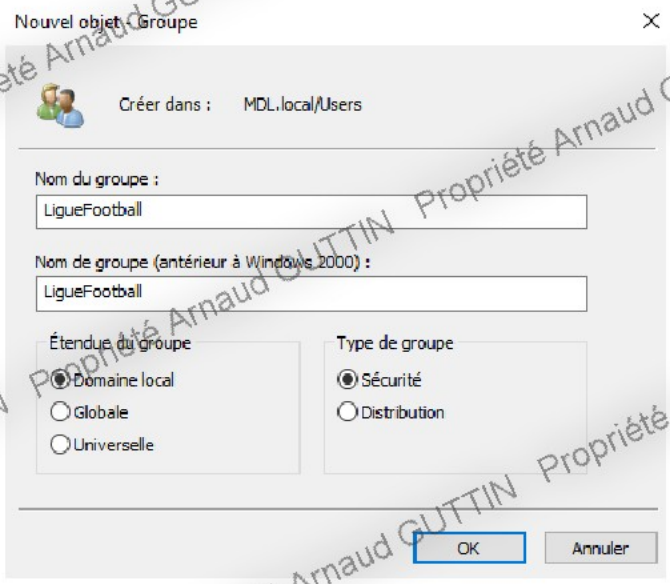


Ajout d'un utilisateur à un groupe

On ajoutera les utilisateurs aux groupes suivants:

Nom de groupe	**Membres du groupe**
LigueFootball	Clément Ogier Laure Dubreuil
LigueBasket	Sylvie Pommier Kevin Dalle

Pour ajouter un utilisateur à un groupe il faudra créer un groupe ou utiliser un groupe existant puis cliquer sur Ajouter des membres.

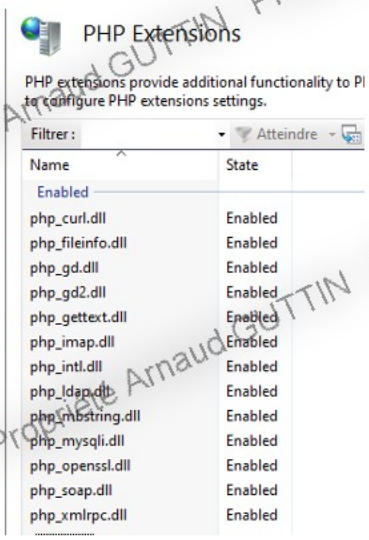


Mission 3 - GLPI

Installation PHP

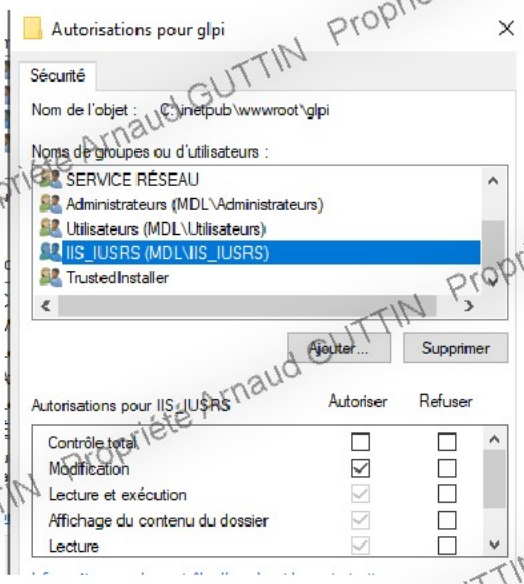
Pour mettre en place un serveur web avec PHP, il faudra installer le rôle IIS. Il faudra aussi installer PHP Manager de chez Microsoft. On mettra le répertoire PHP à la racine du disque.

On ajoutera les extensions nécessaires à GLPI, (voir exemple ci-dessous).



On placera le dossier GLPI dans le répertoire C:\inetpub\wwwroot\glpi.

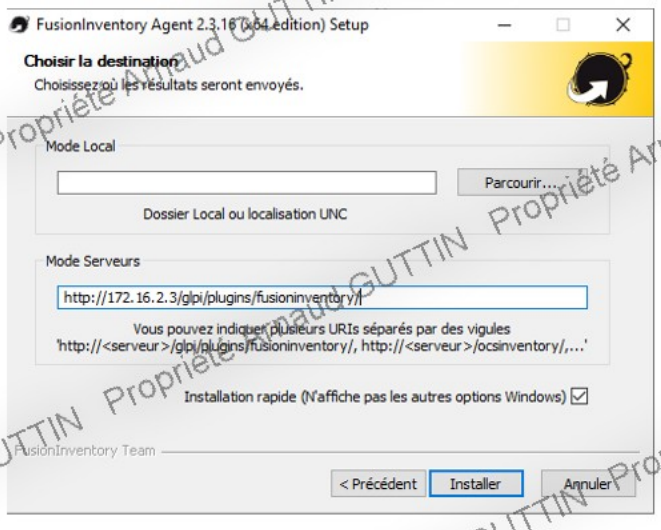
L'application GLPI à besoin d'autorisations pour fonctionner correctement, il faudra donc mettre les droits d'écriture sur le dossier dans C:\inetpub\wwwroot\glpi à l'utilisateur IIS_USERS.



Installation de Fusion Inventory

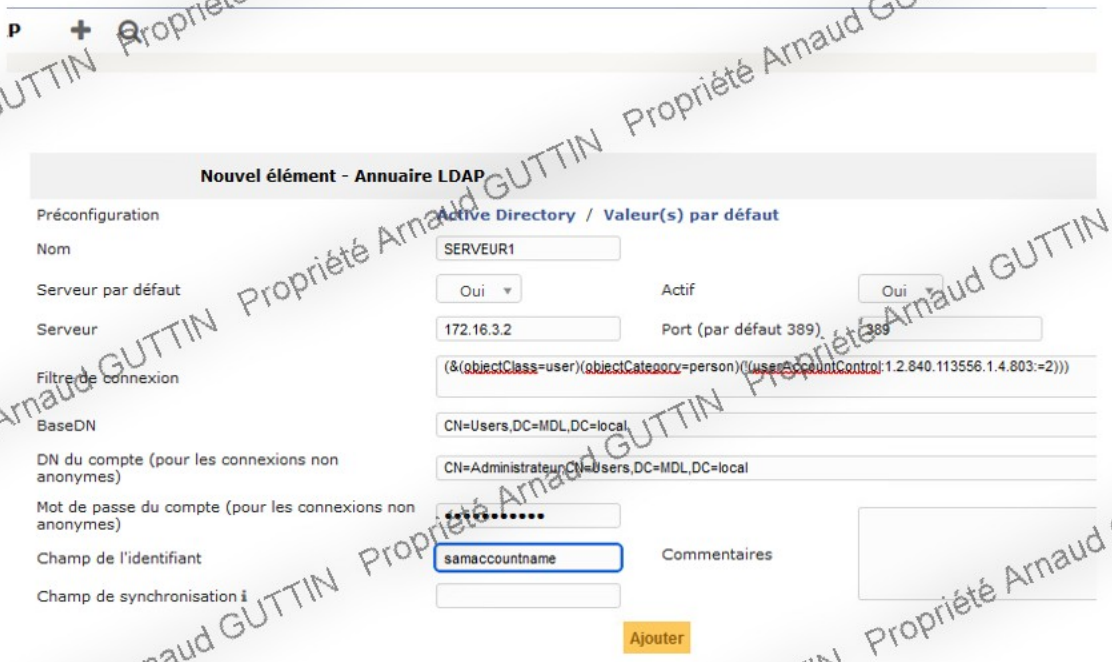
Fusion Inventory est agents permettant de transmettre les informations de statut d'une machine à un serveur (ici GLPI).

Il faudra exécuter Fusioninventory sur chaque machine, puis il faut indiquer le lien ci-dessous. Cela va indiquer à l'agent où il doit envoyer les données.



Connexion à l'annuaire LDAP

Sur l'interface web de GLPI il faudra se rendre sur l'onglet Authentification puis Annuaire LDAP. Cela va permettre de connecter GLPI à notre annuaire Active Directory.

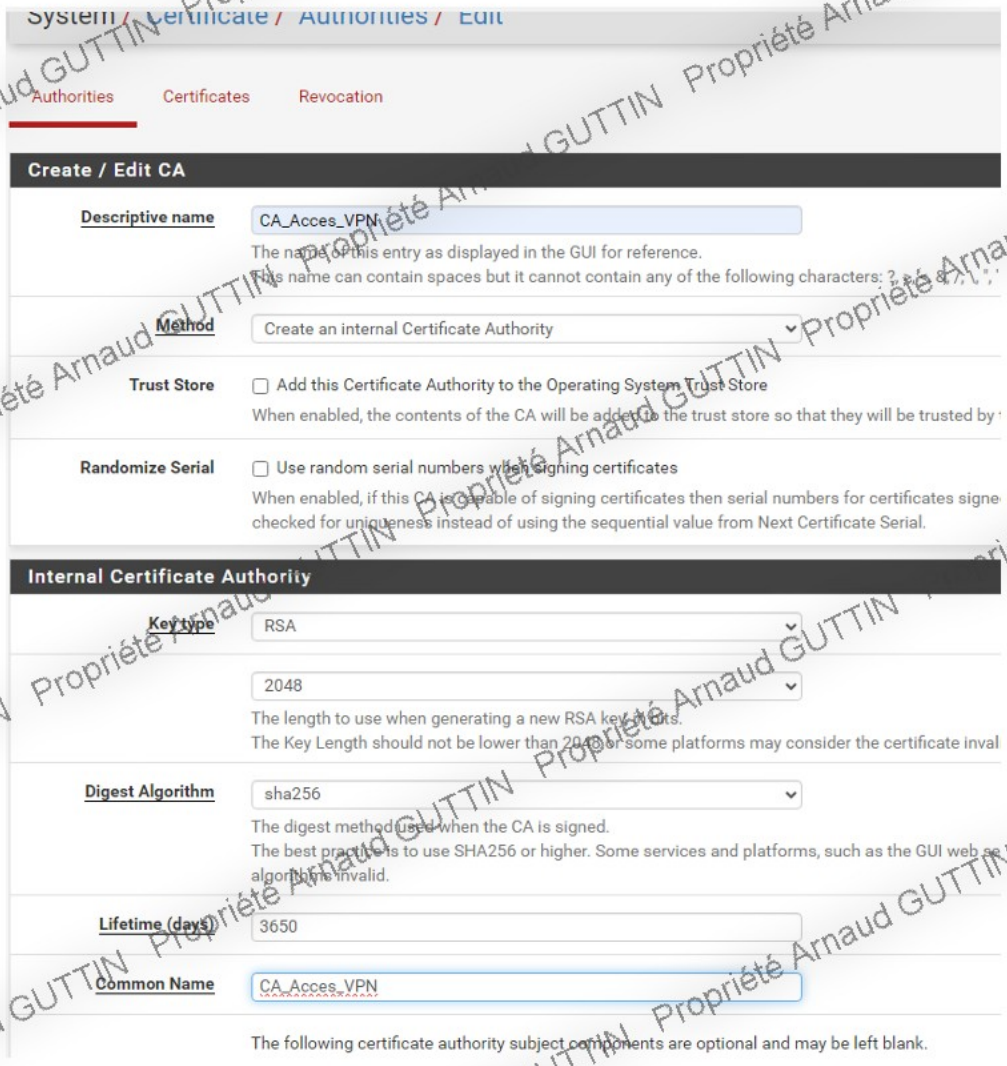


Mission 4 - Installation OpenVPN

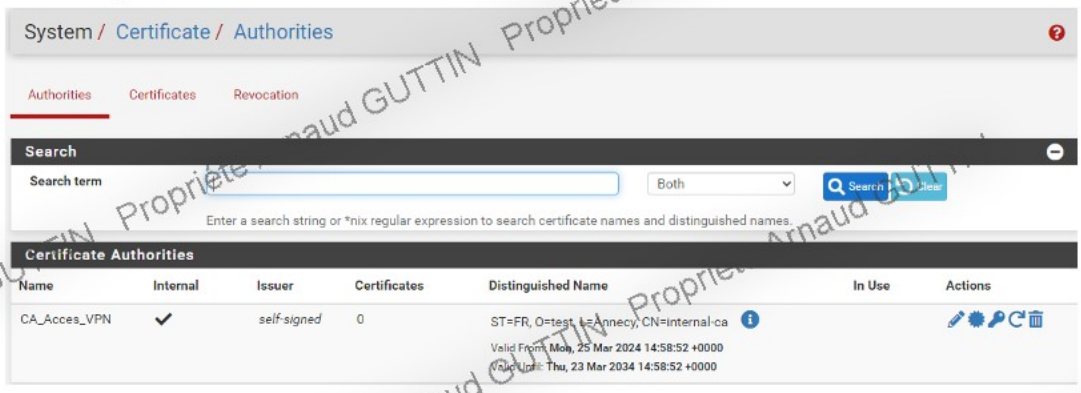
Création d'une entité de certificats

Sur Pfsense, il faudra créer une autorité de certification. Celle-ci va permettre de creer les certificats pour la connexion VPN.

Pour ce faire, il faudra aller dans System, puis Certificats et Autorité.
On remplira les informations ci-dessous.

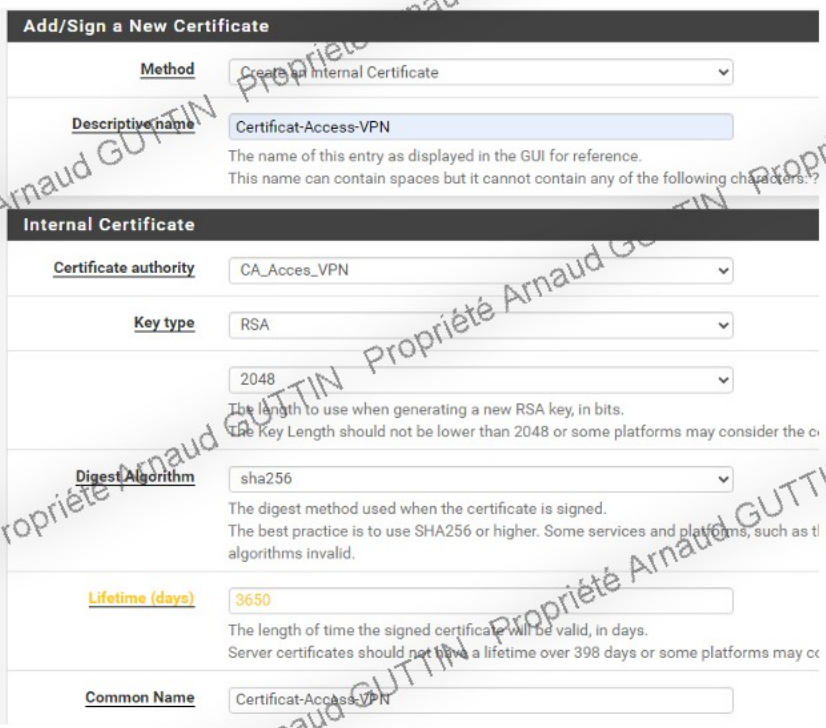


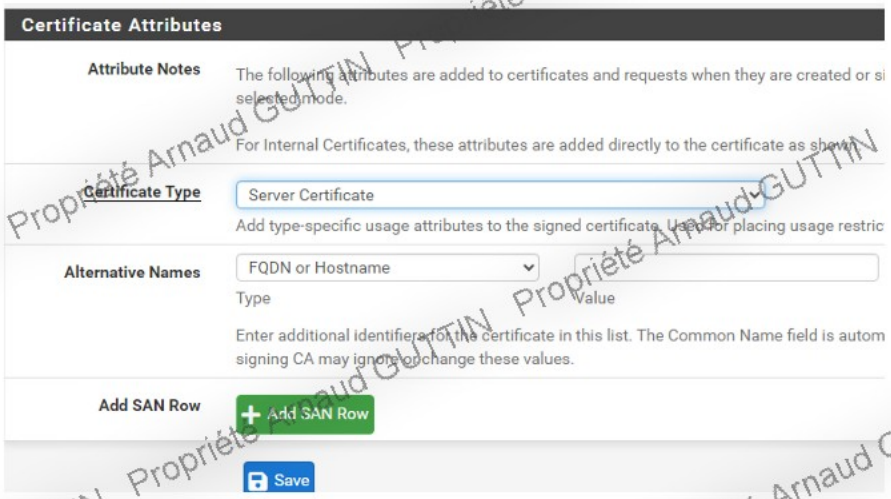
On peut voir que notre autorité de certifications est bien créée.



Création d'un certificat serveur

Pour la communication VPN, il faut créer un certificat serveur. Pour ce faire, on va cliquer sur Créer un certificat et entrer les informations ci-dessous.



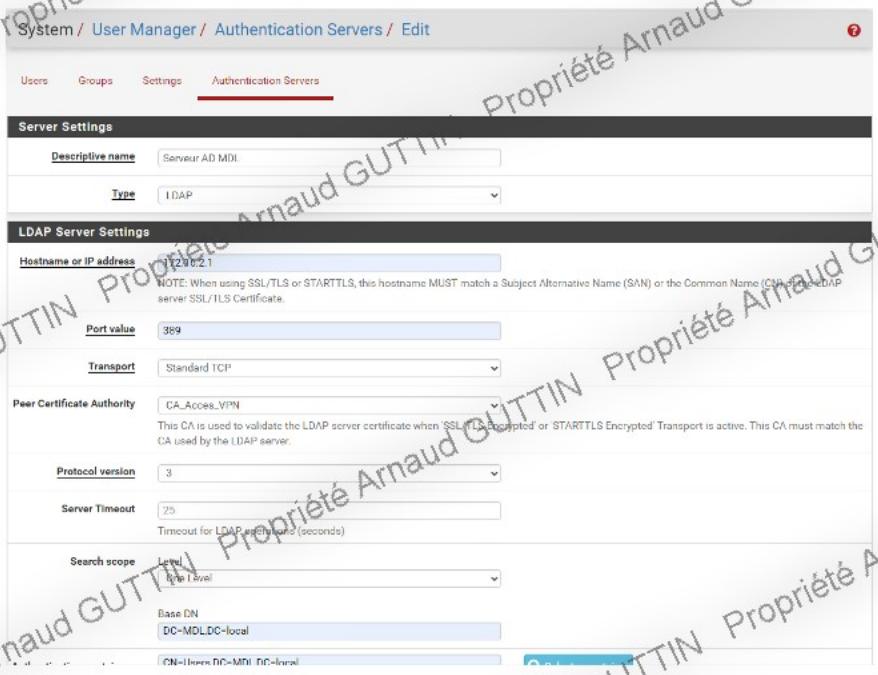


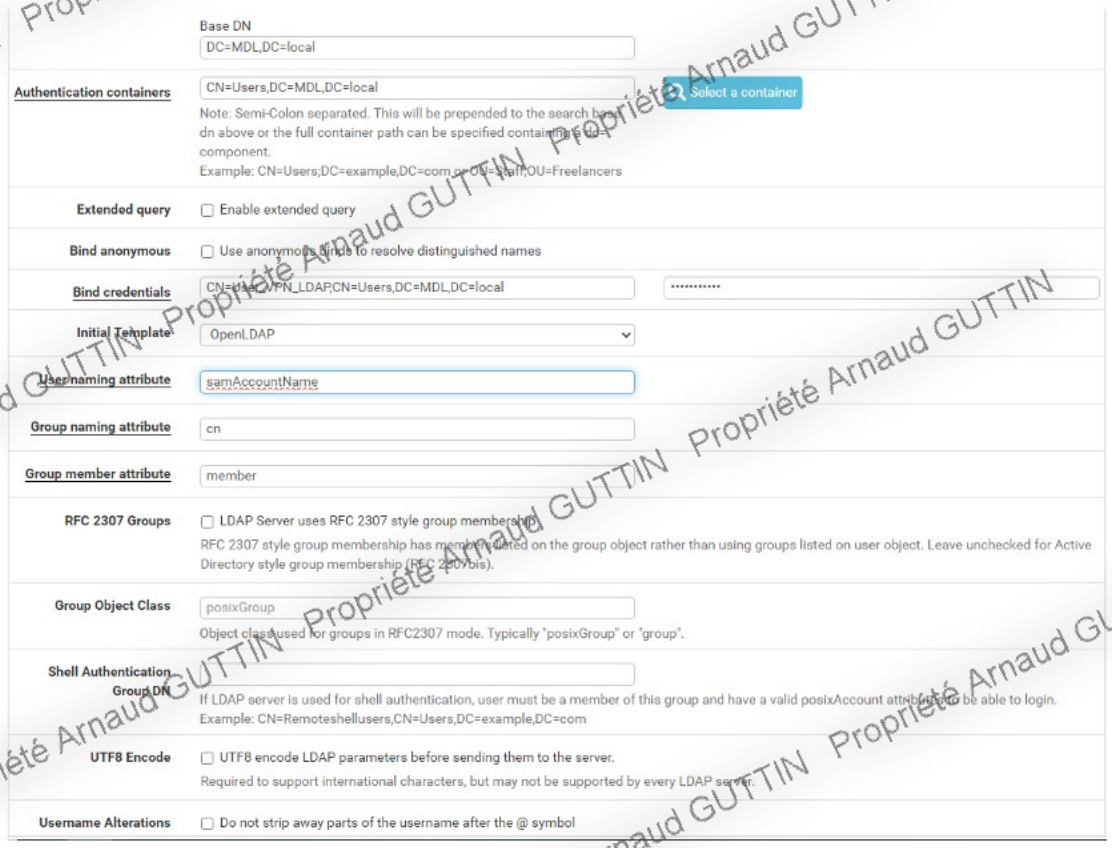
Création de l'utilisateur OpenVPN

Pour la connexion VPN, il faudra créer un utilisateur sur l'Active Directory, on appellera cet utilisateur, User_VPN_LDAP.

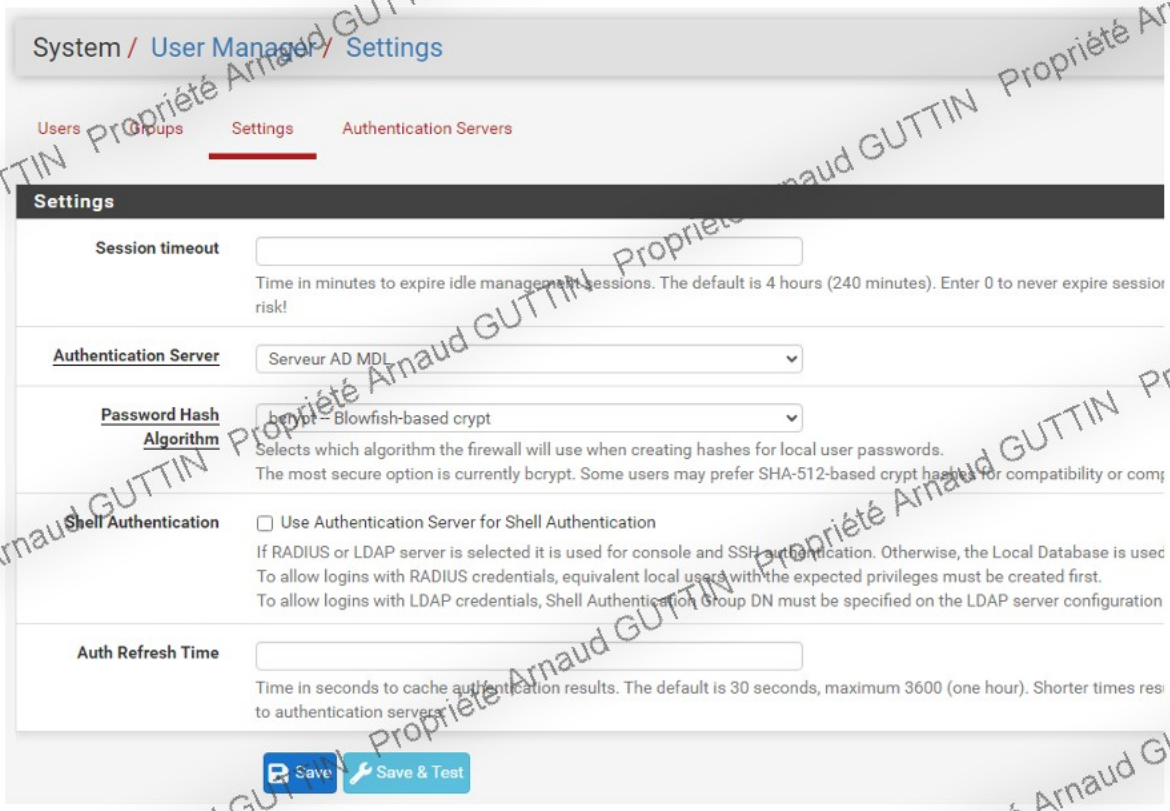
Création d'une autorisation d'authentification avec LDAP au SERVEUR1

Pour que les utilisateurs puissent se connecter avec leur identifiant de l'Active Directory, il faut créer une autorisation de connexion serveur avec l'annuaire LDAP. On va aller dans Gestion des utilisateurs, puis Authentification Serveurs, enfin on va entrer les informations ci-dessous.



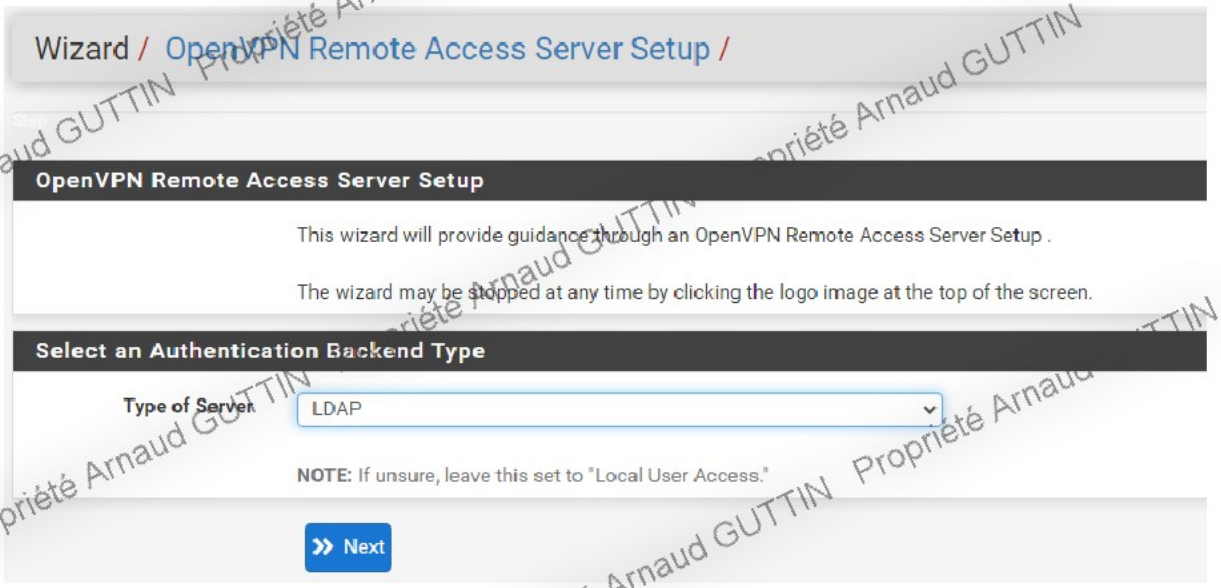


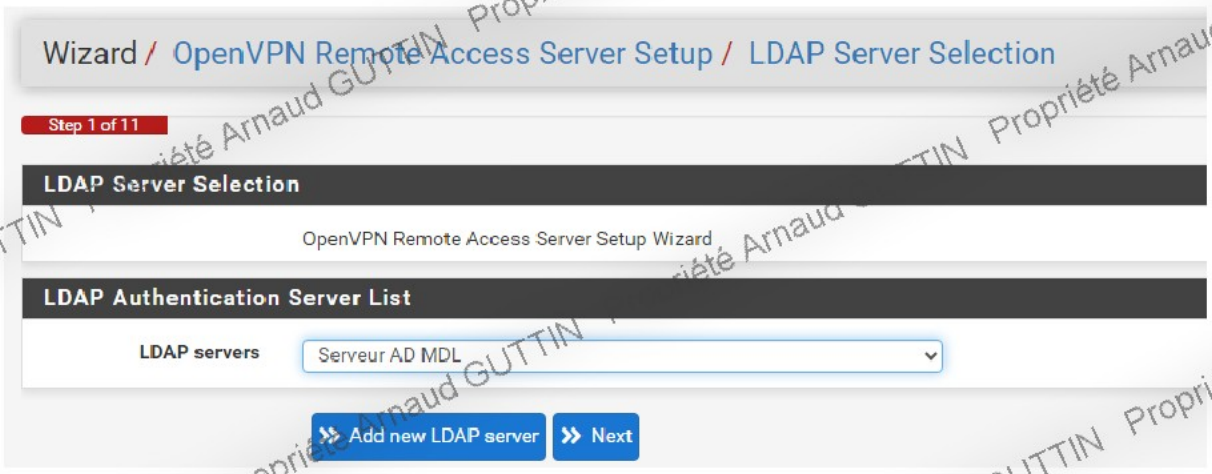
Dans Settings, on précisera Authentication Server comme Serveur AD MDL.

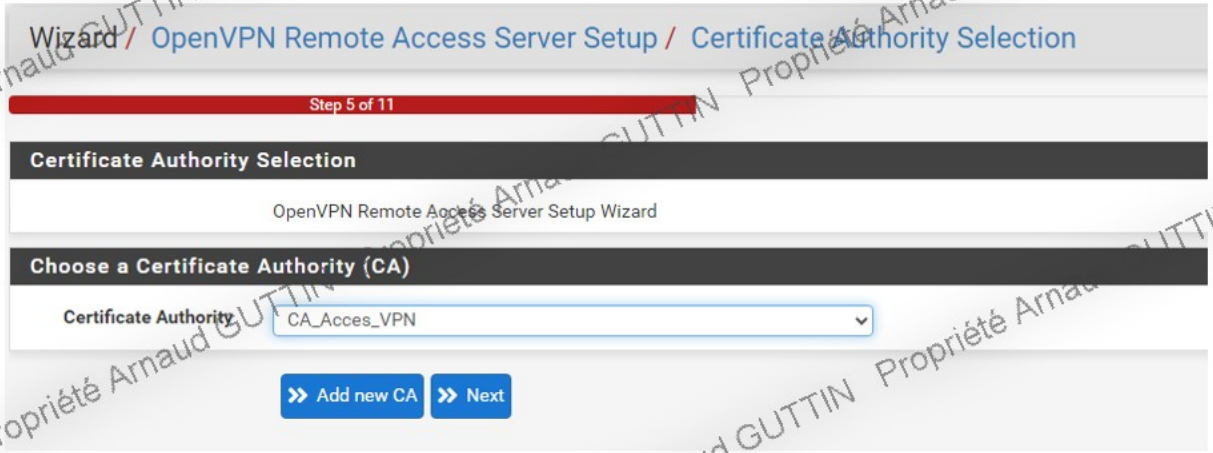


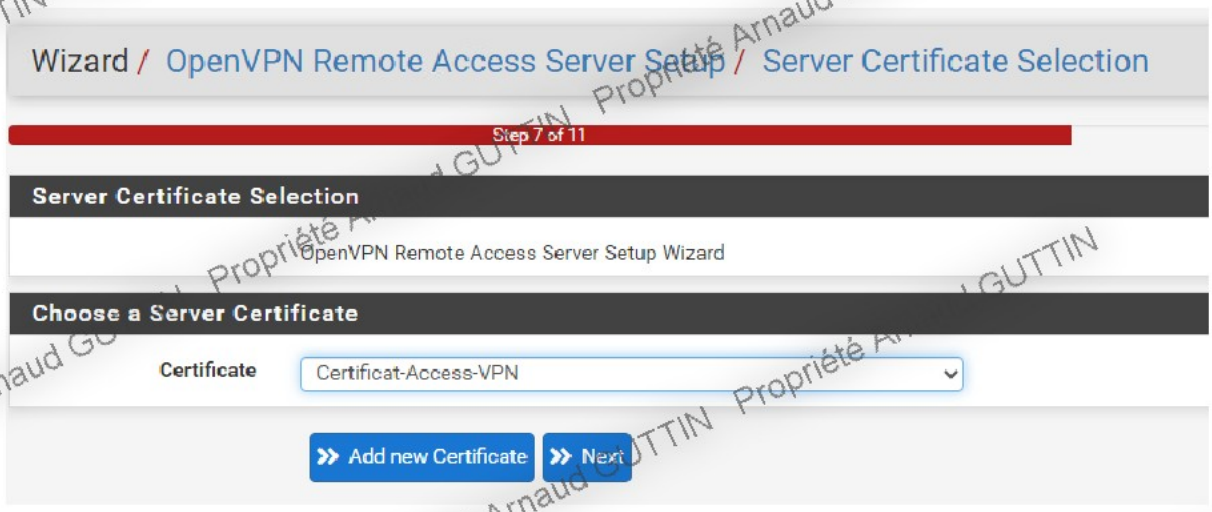
Création du service OPENVPN sur Pfsense

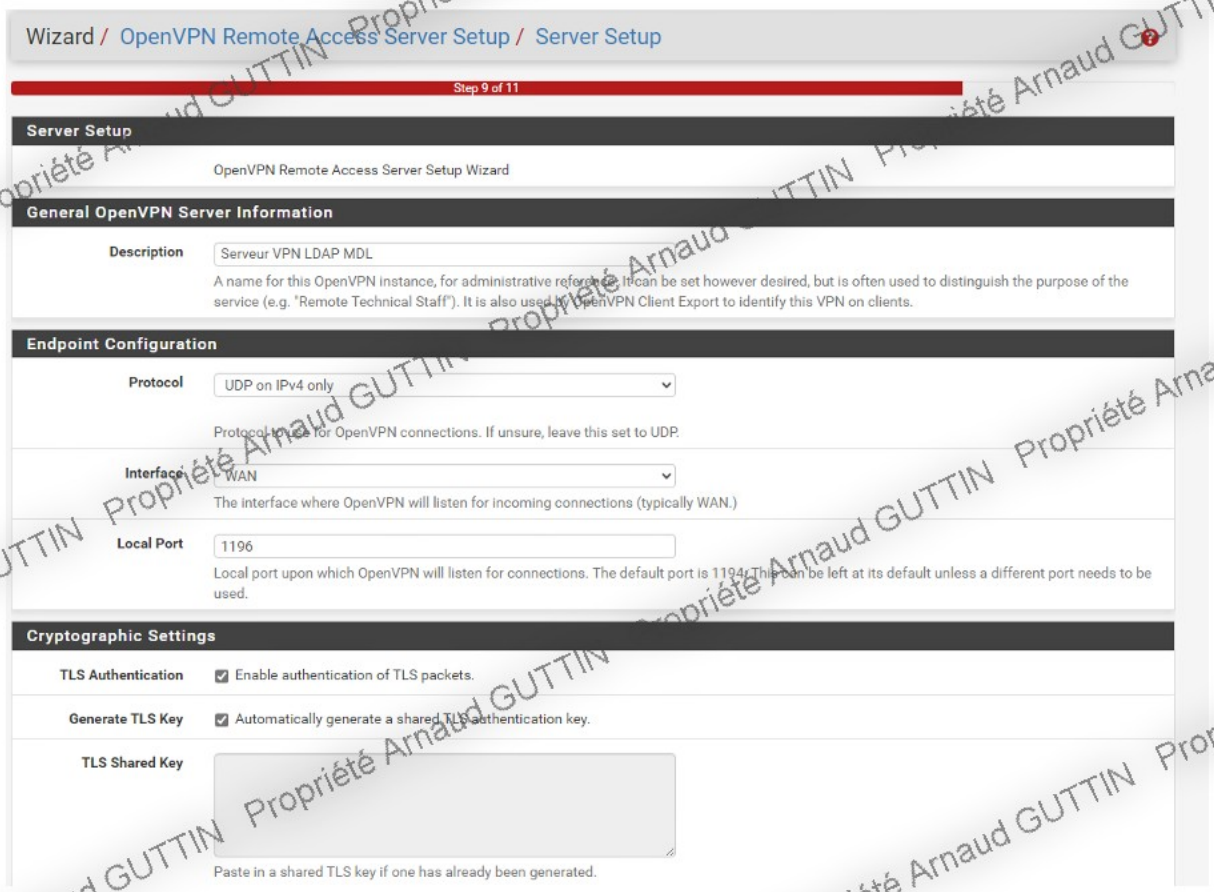
On va ensuite créer le service OpenVPN sur le routeur Pfsense.
Pour ce faire, on va ce rendre dans OpenVPN → Aller dans VPN→ OpenVPN→ Wizards, puis on entrera les valeurs ci-dessous.

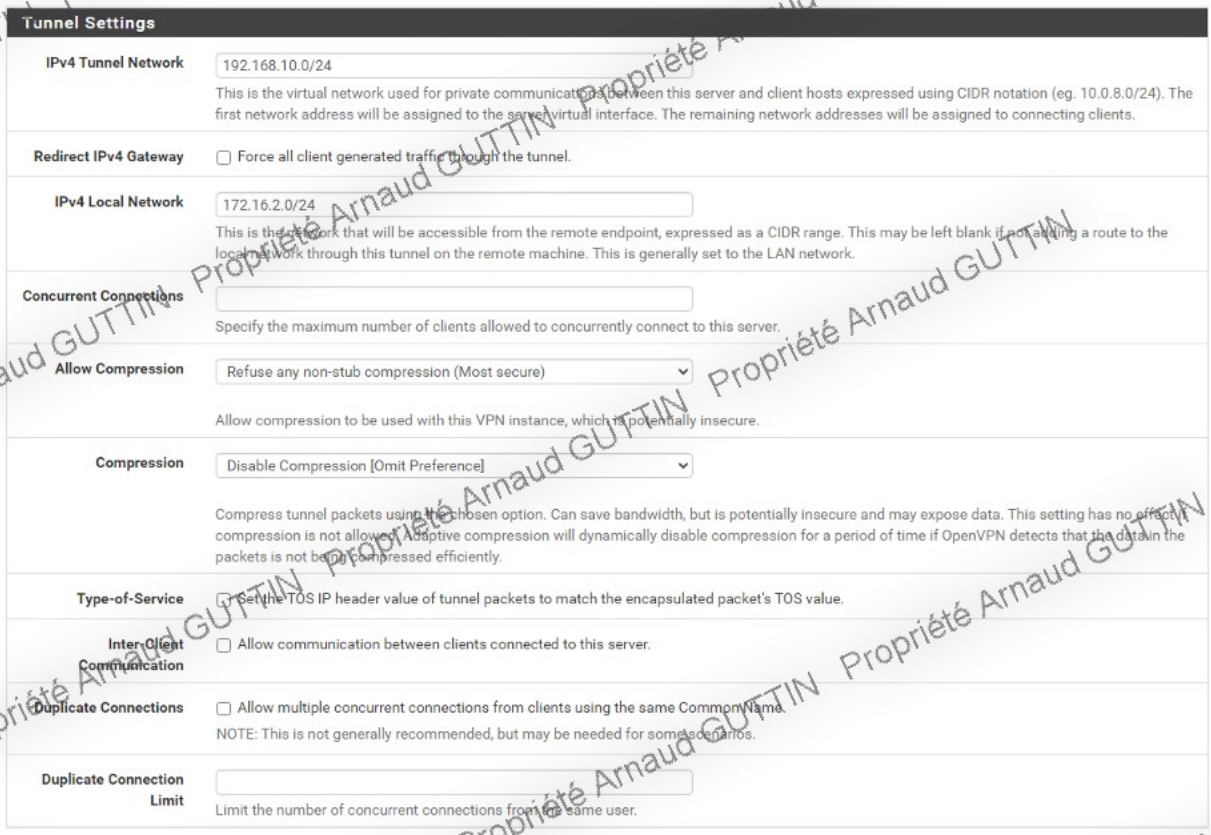


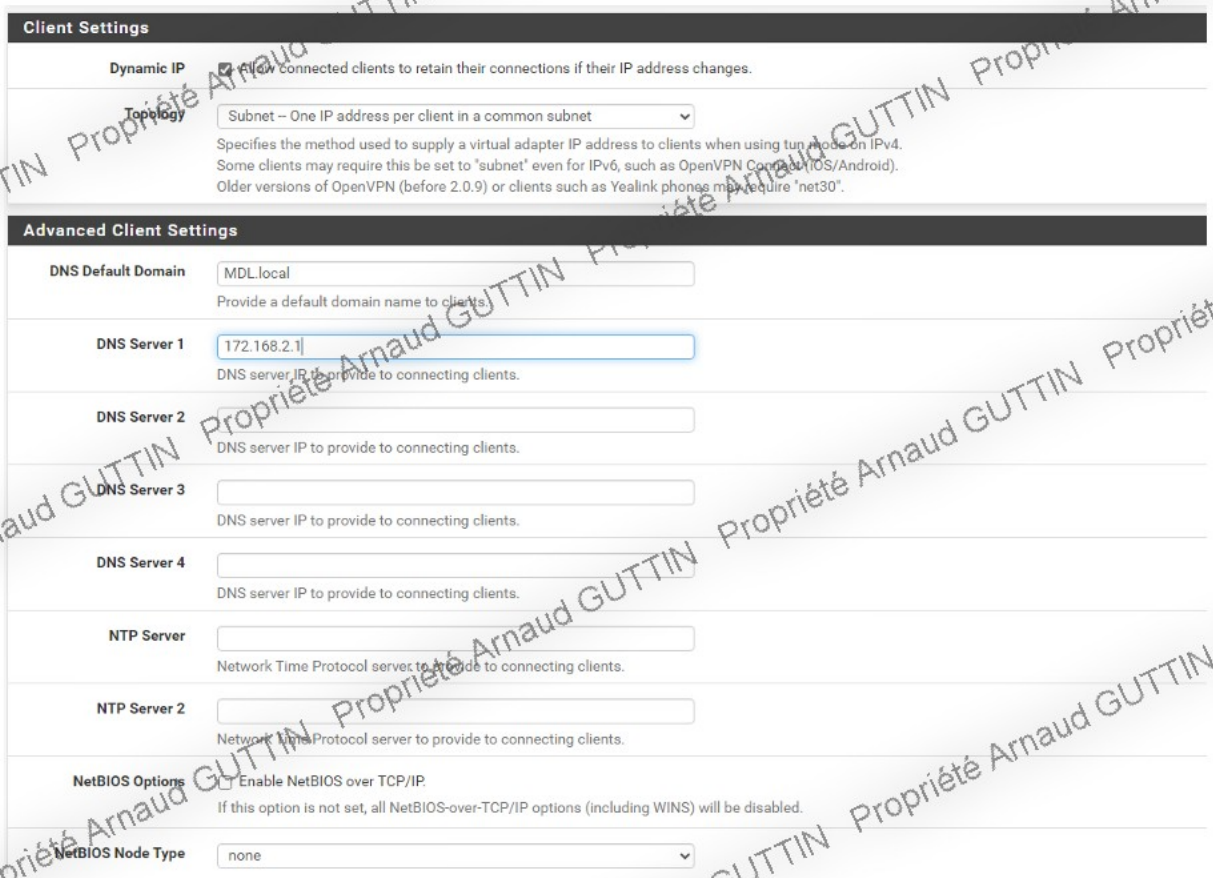


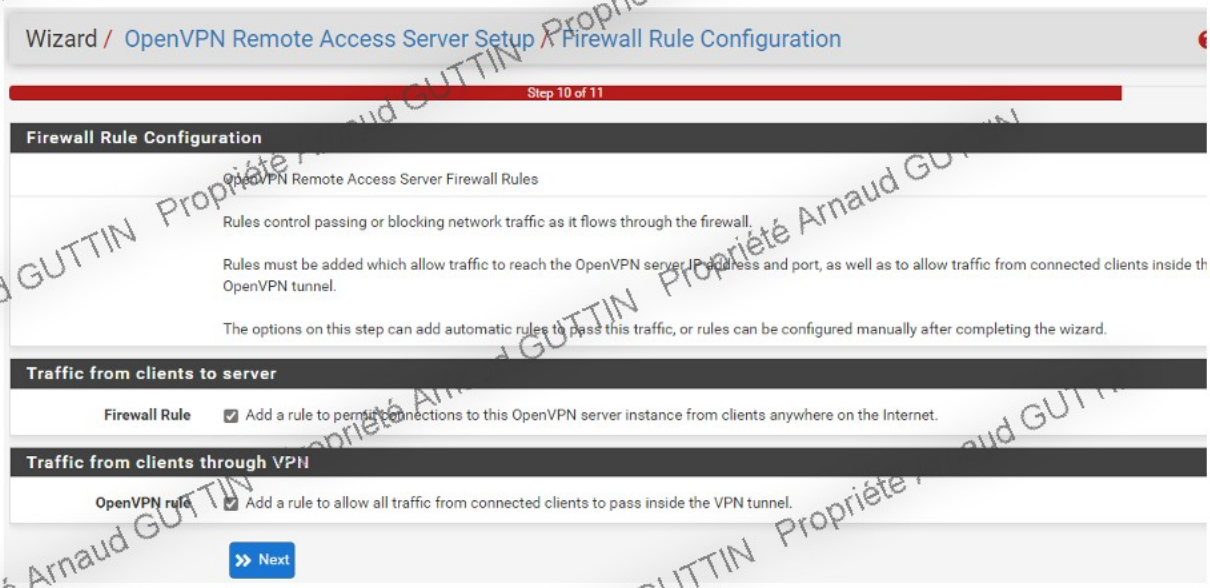






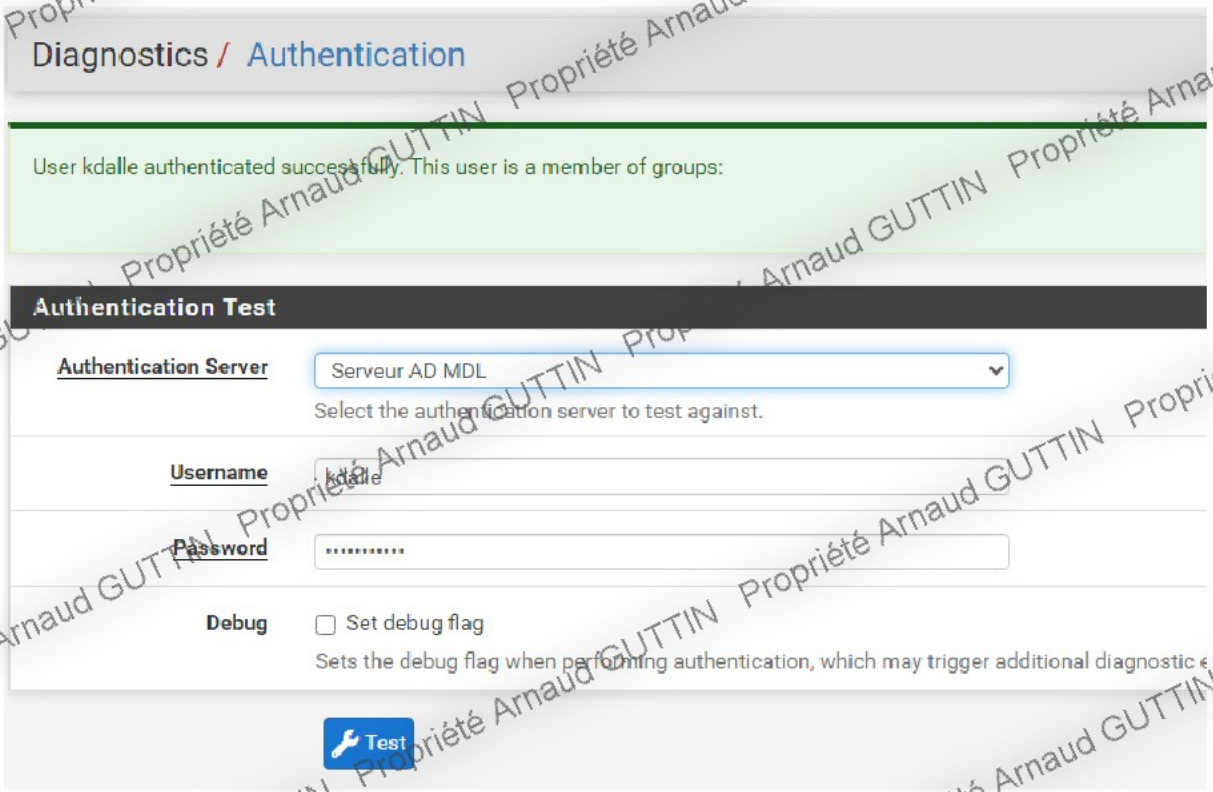






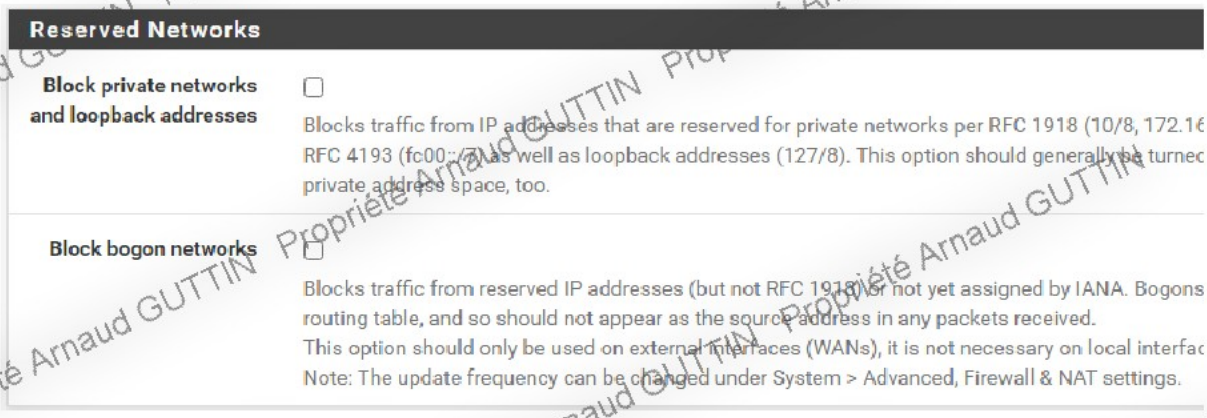
Test de connection

Pour tester le bon fonctionnement du serveur OpenVPN, il est possible de se rendre dans Diagnostics puis Authentification, puis entrer un utilisateur de l'Active Directory.



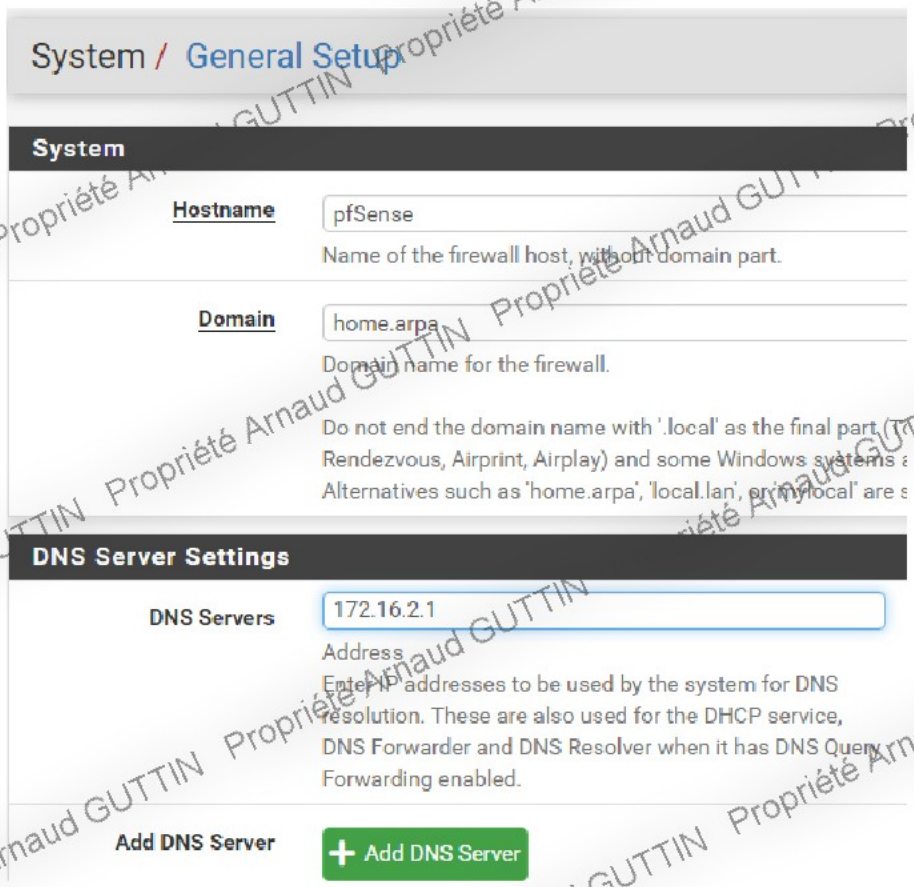
Modification de l'interface WAN

Sur l'interface WAN, il faudra désactiver les deux cases, elles permettront de laisser la connexion entrante depuis l'extérieur.



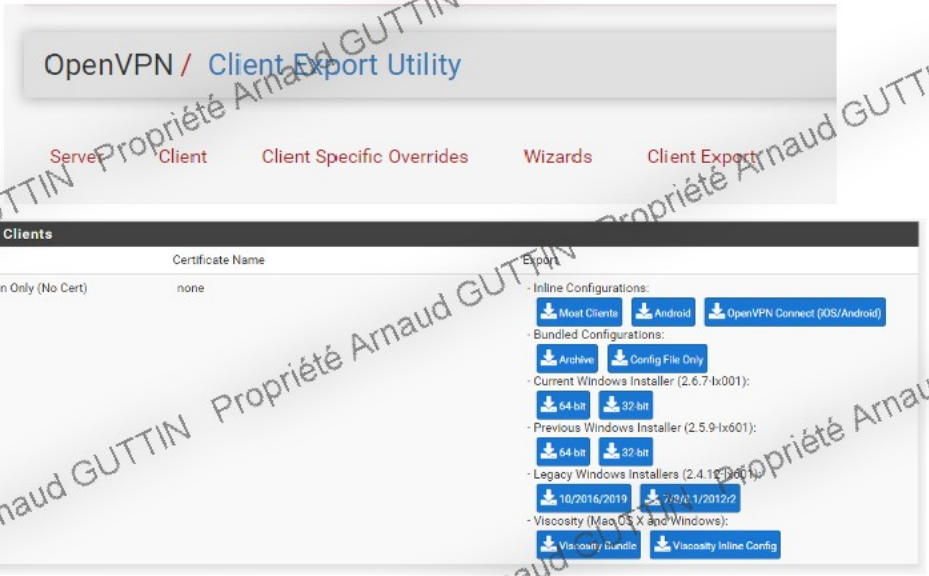
Modification du serveur DNS de Pfsense

Il faudra modifier le serveur DNS de Pfsense et mettre l'adresse IP du Serveur1.

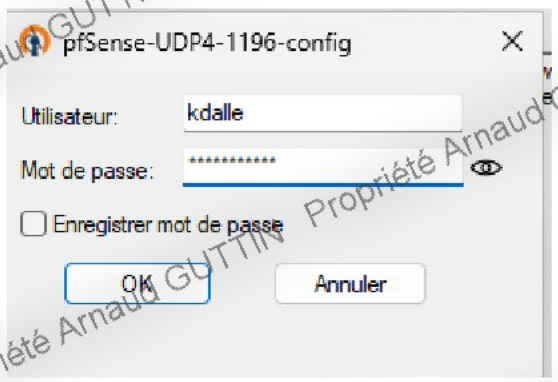


Téléchargement du client OPENVPN et configuration

Pour télécharger le client OpenVPN qu'il faudra exécuter sur les postes informatiques voulant se connecter en VPN, il faut se rendre dans OpenVPN, puis Client export. Il faudra télécharger la version correspondant à votre système d'exploitation (ici Windows Installer 64 bits).



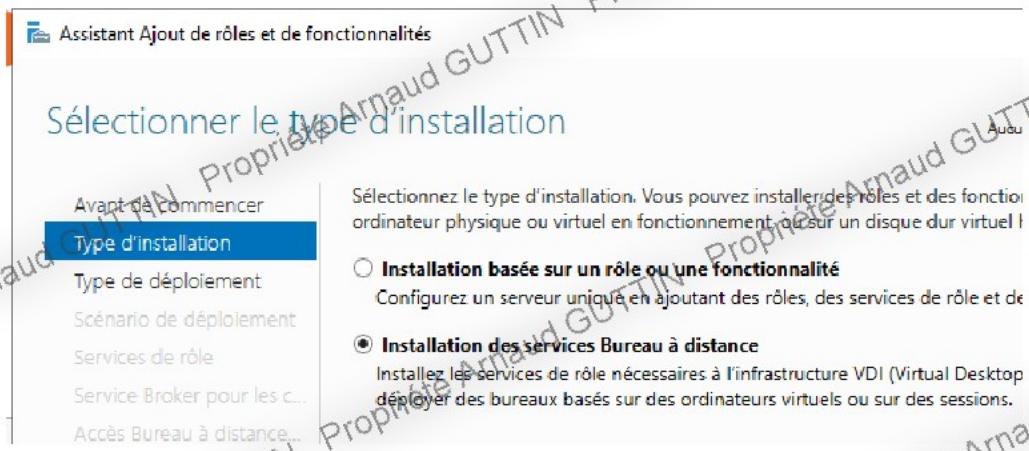
Vous pouvez ensuite tester la connexion VPN à distance.



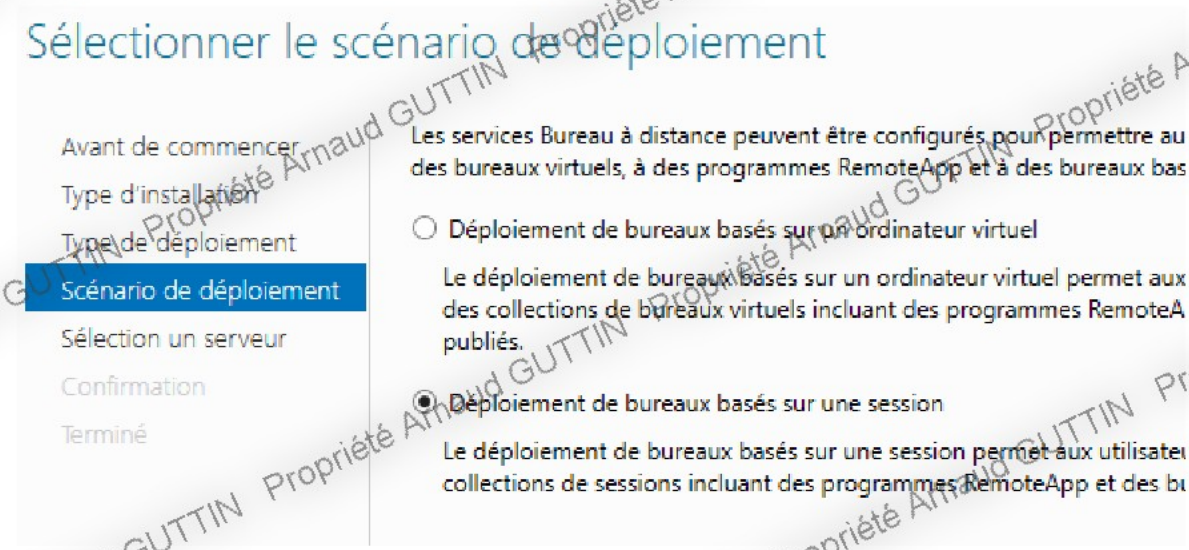
Mission 5 : Bureau à distance

Installation des rôles Bureau à distance

Pour utiliser le service Bureau à distance, il faudra installer le rôle, dans type d'installation, il faudra cliquer sur Installation des Services Bureau à distance, (voir ci-dessous).

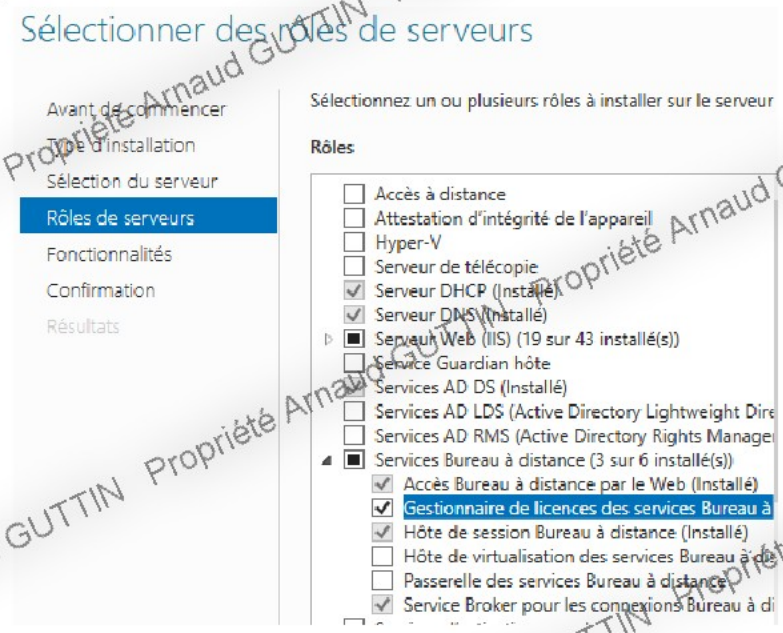


On choisit ensuite, Déploiement de bureaux sur une session.



Le redémarrage se fera automatiquement.

Il faudra aussi installer le rôles Gestionnaire de licences des services bureaux à distance, (voir ci-dessous).



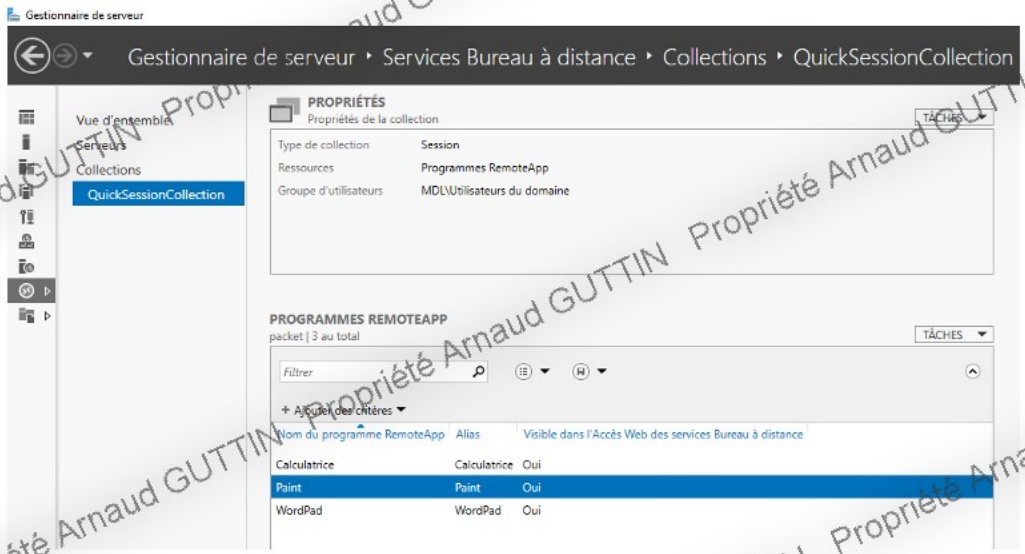
Installation Packet Tracer sur SERVEUR1

Pour installer Packet Tracer sur le Serveur1, il faudra exécuter le fichier .exe.

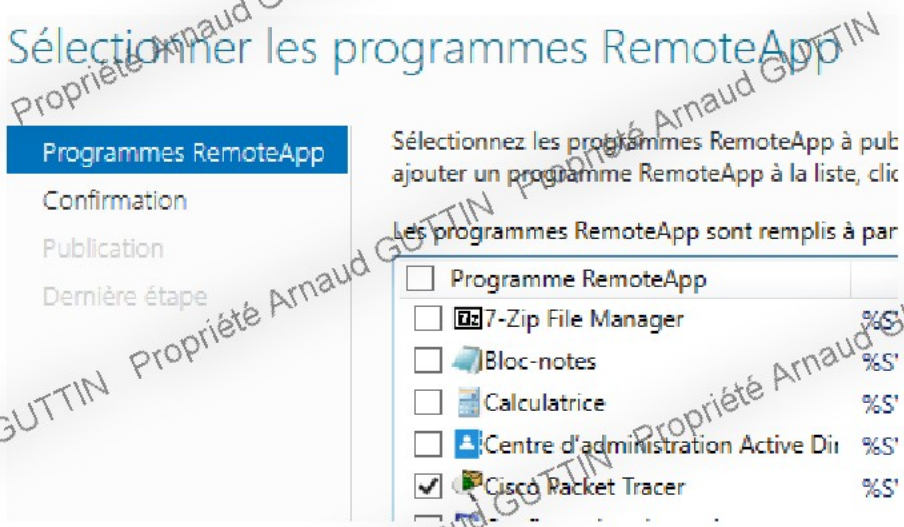
Deployment Application RemoteApp

Pour déployer le logiciel Packet Tracer, il faudra se rendre sur le Gestionnaire de Serveur dans Services de bureaux à distance.

Dans Quick Session Collection vous pouvez apercevoir les outils déployés dans Bureaux à distance.

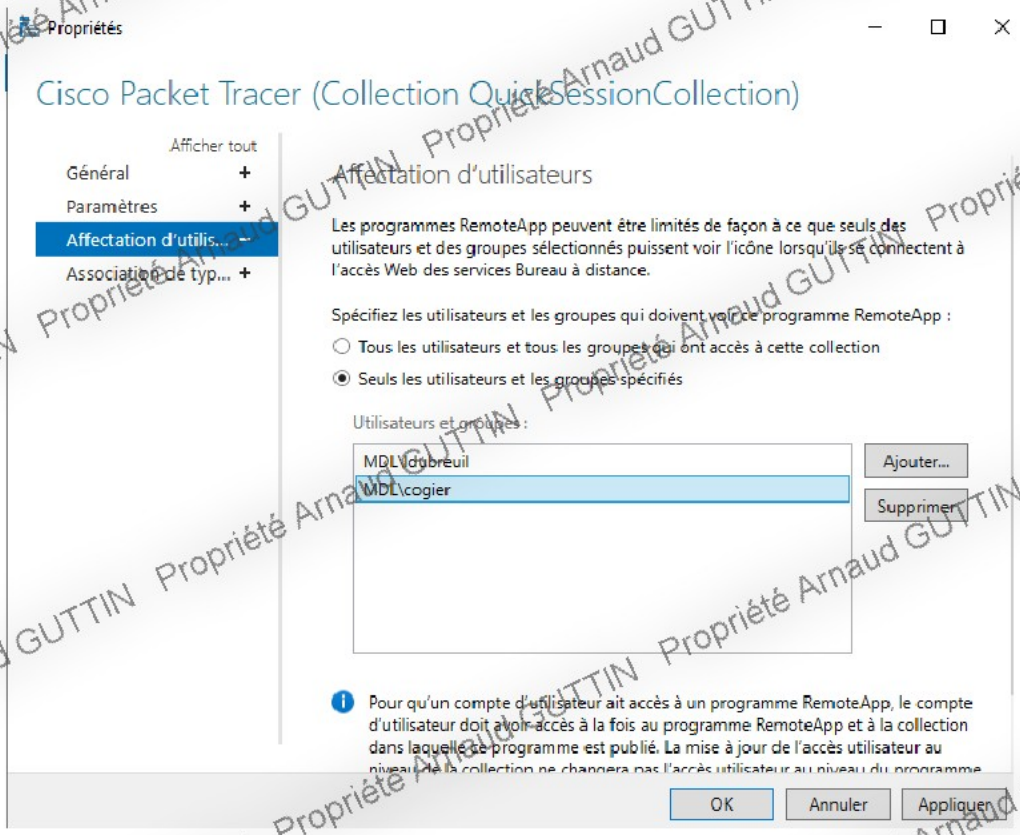


Pour publier de nouveaux logiciels tels que Packet Tracer, il faut cliquer sur le bouton Tache puis Publier des programmes RemoteApp, enfin, on sélectionne le programme souhaité.

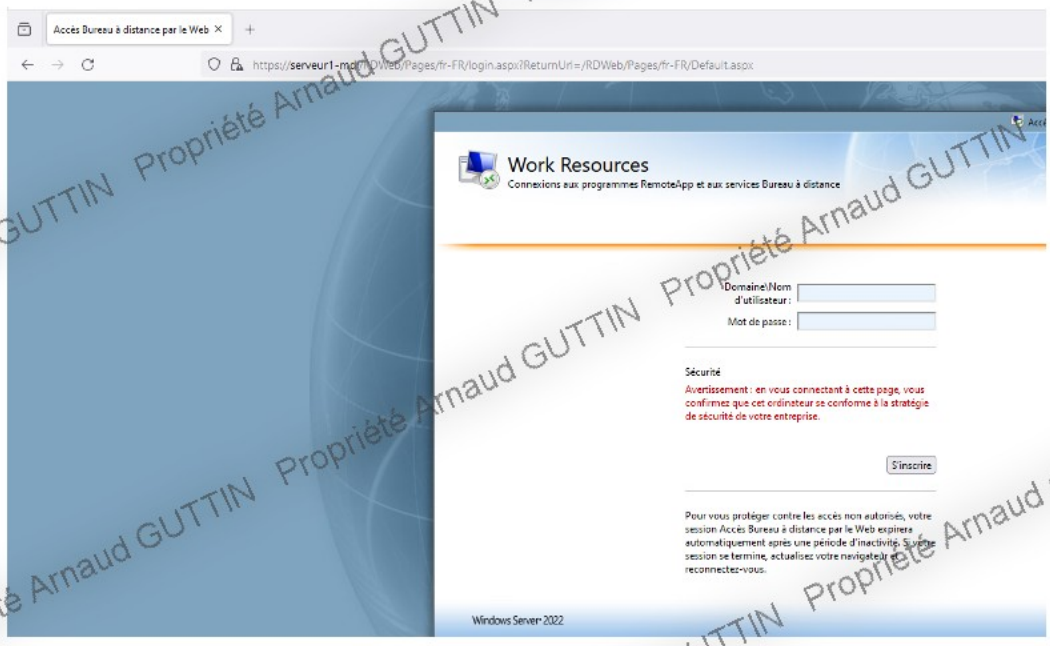


Modification des paramètres d'affectations utilisateurs

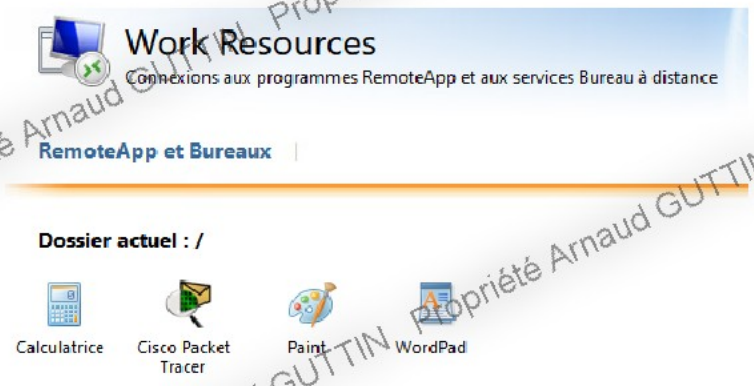
Il est possible de choisir à quels utilisateurs est affecté un déploiement.



Pour vous connecter au service de bureaux à distance, il faudra se rendre sur le navigateur et entrer l'adresse, serveur1-mdl/rdweb.
Attention il y a uniquement le navigateur Firefox qui fonctionne.



Puis ce connecter avec un utilisateur comme Laure Dubreuil



Mission 6 : Cluster PFsense

Le cluster de Pfsense a pour objectif de mettre en redondance les routeurs/pare-feux pour prévenir d'une panne d'un des deux.

Modification IP des interfaces

Il faudra modifier les adresses IP des interfaces et se référer au IP du schéma.

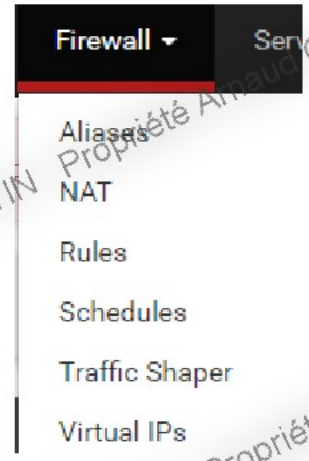
Les deux routeurs Pfsense prendront pour adresse IP virtuelle 172.16.2.254.

Sur PFsense Esclave, pour l'interface WAN il aura l'IP 192.168.211.230.

Sur PFsense Maitre, pour l'interface WAN il aura l'IP 192.168.211.229.

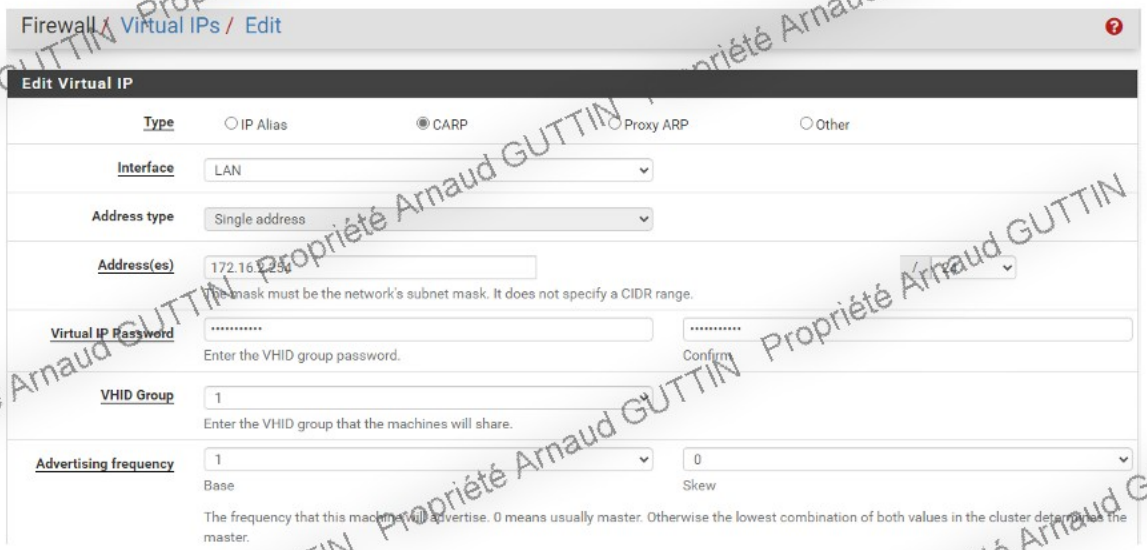
Paramétrage du cluster

Pour paramétrer le cluster Pfsense, il faudra se rendre sur Firewall puis Virtual IPS.



Création de l'IP virtuelle pour l'interface LAN

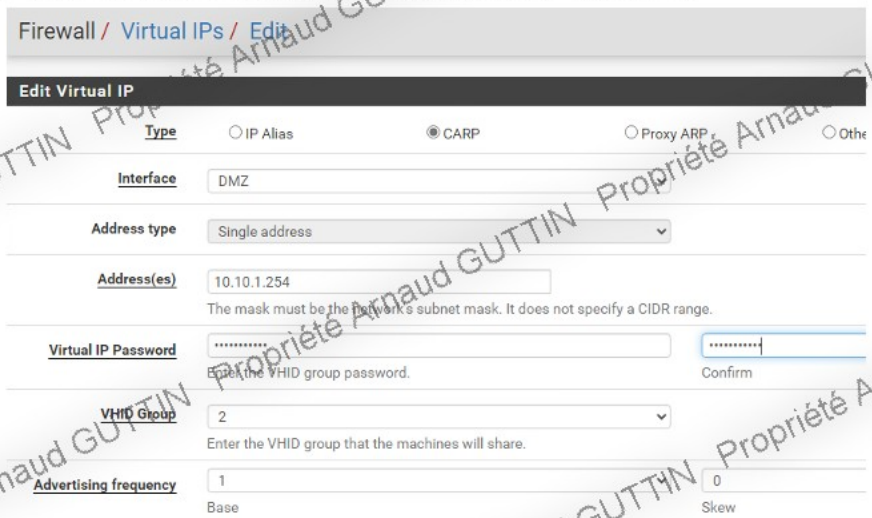
Il faudra ajouter la configuration ci-dessous au deux Pfsense.
Le protocole CARP, permet le transfert des informations de statut entre les routeurs.



Attention, sur le Pfsense Esclave il faudra mettre le Skew à 1, cela permet de définir la priorité (il sera donc esclave car il est à 1 et le Pfsense Maître est à 0).

Création de l'IP virtuelle pour l'interface DMZ

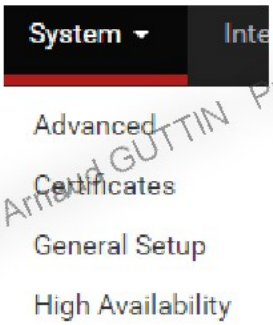
Il faudra effectuer la même pratique pour l'interface DMZ. Cependant, il faudra changer le VHID (chaque VHID permet un canal de communication différent).



Configuration de la haute disponibilité

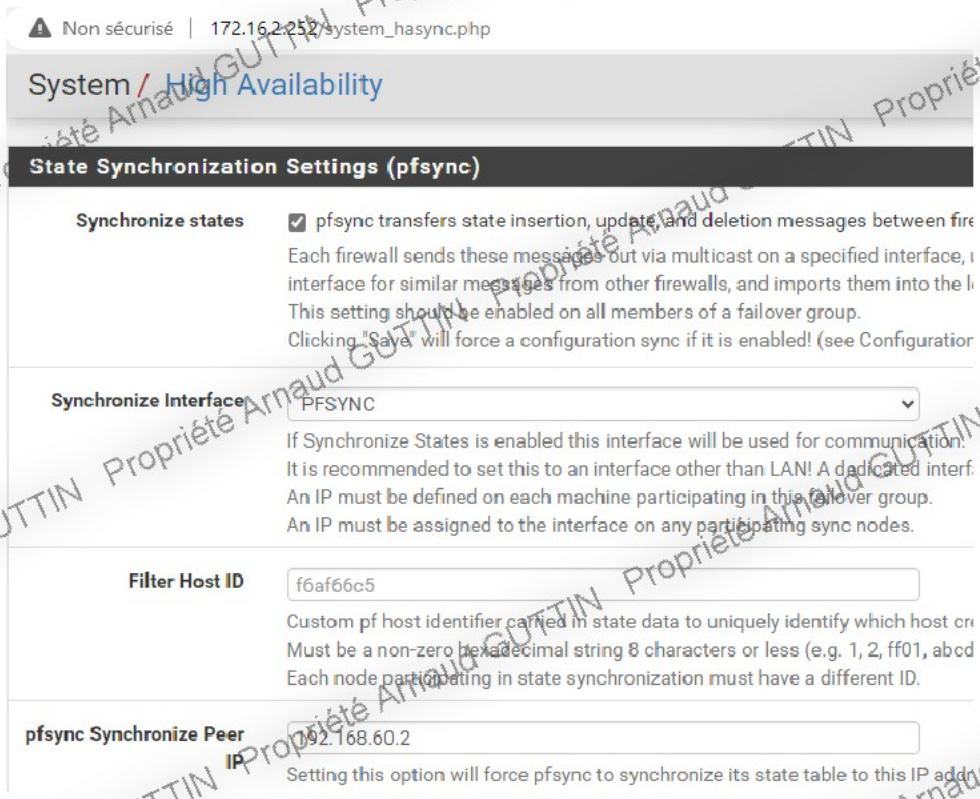
Il faudra ensuite configurer la haute disponibilité, c'est le service qui va permettre de surveiller si le routeur voisin est toujours actif ou non. On utilisera l'interface PFSYNC des routeurs PFsense pour la haute disponibilité.

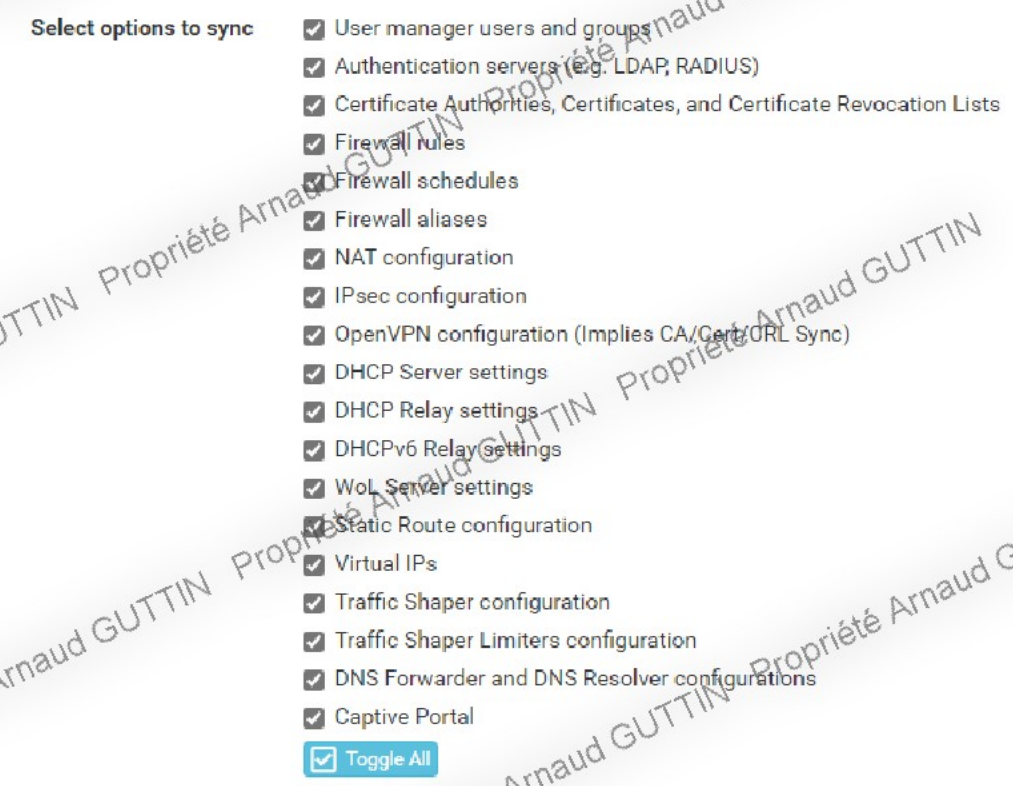
Pour ce faire, il faut aller dans High Availability.



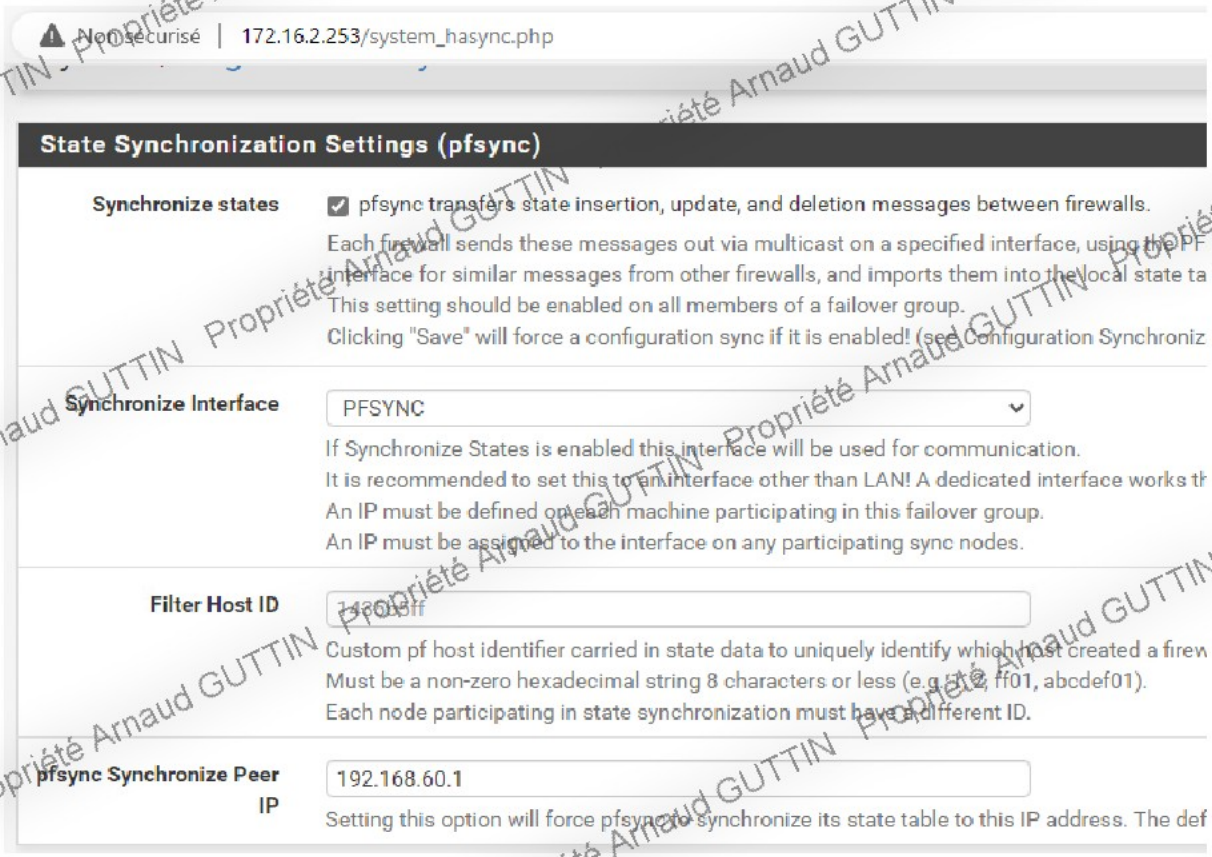
High Availability sur Pfsense Maître

Il faudra cocher la case Syncronize states, puis remplir les informations ci-dessous.





High Availability sur Pfsense Esclave



Attention, pour le Pfsense Esclave il ne faut cocher que l'option Virtual IPS.

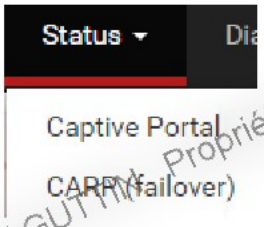
Modification des règles de pare feu pour l'interface PFSYNC

Il faudra ensuite configurer les règles pour l'interface PFSYNC.

La configuration est à réaliser sur les deux PFsense. Il faudra créer une règle qui autorise la communication entre les deux serveurs sur PFSYNC, (ici on autorise tout le trafic mais il est possible de rendre cette règle plus sélective en utilisant les adresses IP respective des routeurs PFsense).

Vérification du statut de la synchronisation

Pour vérifier le statut de la synchronisation entre les routeurs, il faut aller dans CARP failover.



On peut voir les deux Pfsense sur le statut de la synchronisation.