Projet Personnalisé Encadré 3 – PPE3

Mise en œuvre d'une infrastructure réseau

Réalisé par : ABDELBAKI Cédric – Formatrice : BARCHICHE Samira

BTS Services Informatiques aux Organisations option
Solutions d'Infrastructure, Systèmes et Réseaux.
Session 2022

TABLE DES MATIÈRES

TABLE DES ILLUSTRATIONS

NATURE DE L'ACTIVITÉ
Contexte : J'installerai, dans le cadre de la réalisation de ce PPE, trois machines virtuelles à l'aide de la solution de virtualisation Hyper-V de Microsoft. La première accueillera la distribution d'un pfSense et la seconde un serveur Microsoft Windows Server 2019 qui fera office de fournisseur de services. Enfin la troisième machine représentera un ordinateur appartenant à un technicien informatique. - Installer trois machines virtuelles - Mettre ces machines sur le même réseau local - Installer un pfSense et un serveur OpenVPN sur la première machine - Créer un serveur DHCP et un serveur d'impression sur la seconde machine - Accéder aux interfaces d'administration et tester la fonctionnalité des travaux réalisés à l'aide de la troisième machine. Le contexte est repris en détail dans la page **PARTIE 1 – CONTEXTE**.

CONDITIONS DE RÉALISATION	
Matériel : Un ordinateur fixe de marque Dell : - Processeur : Intel Core I5 ; - Mémoire vive 16 Go ; - Disque dur : 500 Go.	**Contraintes :** - Ordinateur physique limité par son matériel (Prévoir une bonne gestion des ressources).
Logiciels utilisés : - Microsoft Hyper-V ; - Client OpenVPN ; - Outil Capture d'écran ; - Paint ; - Microsoft Word 2019.	**Requis :** - Image disque du pfSense ; - Image disque Microsoft Windows 2019 ; - Image disque Microsoft Windows 10 ;
Difficultés rencontrées : - Fonctionnement des commutateurs et accès à internet pour le pfSense ; - Mauvais fonctionnement du VPN à la suite d'un mauvais paramétrage du serveur OpenVPN.	**Durée de réalisation :** - Activité : 20 heures - Rapport : 8 heures

Compétences mises en œuvre dans le cadre de cette activité	
Gérer le patrimoine informatique	• Recenser et identifier les ressources numériques ; • Vérifier le respect des règles d'utilisation des ressources informatiques.
Travailler en mode projet	• Analyser les objectifs et les modalités d'organisation d'un projet ; • Planifier les activités.
Mettre à disposition des utilisateurs un service informatique	• Réaliser les tests d'intégration et d'acceptation d'un service ; • Déployer un service.

INTRODUCTION

Le BTS Services Informatiques aux Organisations option Solutions d'Infrastructure, Systèmes et Réseaux forme des professionnels destinés à travailler ou poursuivre leurs études dans le domaine des réseaux informatiques. Il est donc nécessaire d'avoir de bonnes compétences en matière d'interconnexion des réseaux une fois le diplôme obtenu pour exercer efficacement son activité d'administrateur systèmes et réseaux.

Pour ces raisons, la mise en place d'un "lab" simulant une infrastructure complète m'a semblé être un excellent sujet d'étude pour la réalisation d'un projet personnalisé encadré. Devant l'ampleur des solutions à mettre en œuvre, j'ai décidé de fractionner ce projet en deux PPE qui traiteront chacun de divers aspects de la conception d'un réseau d'entreprise.

Je vais vous présenter, dans ce troisième projet, la mise en place d'un routeur / pare-feu avec pfSense, l'installation de services divers avec Microsoft Windows Server 2019 et le déploiement d'une solution VPN permettant aux salariés de travailler à distance avec OpenVPN.

Je remercie mes collègues, Jérôme MARSAN et Théo BOULLING ainsi que mon responsable Laurent BONABESSE pour la précieuse aide apportée lors de la réalisation de ce PPE. Je remercie également ma formatrice, Samira BARCHICHE pour les conseils donnés dans le cadre des cours d'informatique. Enfin, je remercie mon formateur Noureddine FIKRY pour son aide et ses idées quant aux solutions pouvant être employées pour réaliser ce projet.

Je vous souhaite une agréable lecture.

PARTIE I – CONTEXTE

1) PRÉSENTATION, SOLUTIONS ET IDENTIFIANTS

Dans ce PPE, je suis membre du service informatique d'un groupe immobilier disposant d'agences dans de nombreuses villes françaises. A l'occasion de l'ouverture d'une agence à Toulouse, je me vois confier le projet de concevoir une infrastructure et de la mettre en œuvre.

L'agence Occimmobilier compte 6 employés et nécessite la mise en place des solutions suivantes :

- Une solution de routage / pare-feu ;
- Une solution serveur permettant la fourniture de services divers ;
- Une solution VPN intégrale (Serveur et clients) ;
- Une solution serveur permettant l'hébergement et le partage de fichiers ; (VOIR PPE 4) ;
- Une solution serveur permettant la sauvegarde régulière des données (VOIR PPE 4) ;
- Une solution VOIP intégrale (Serveur et clients) (VOIR PPE 4).

Après analyse des besoins de l'agence, j'ai décidé d'utiliser les solutions reportées dans le tableau ci-dessous (Pour le PPE3) pour développer cette maquette de l'infrastructure, en tenant compte des contraintes matérielles et financières auxquelles je pourrais être confronté.

BESOIN	SOLUTION RETENUE
Virtualisation	Microsoft Hyper-V
Routeur / Pare-feu / VPN	PFSense/OpenVPN
Services	Microsoft Windows Server 2019

Les salariés de l'agence, leurs informations d'identification session AD/VPN et leurs besoins sont listés dans le tableau ci-dessous.

NOM	PRÉNOM	IDENTIFIANT	MDP	FONCTION	IMPRIMANTE
DELPECH	Marine	m.delpech	Oyt89!?7nK	Directrice	Direction
DELOITTE	Marc	m.deloitte	H4oU@r{56!	RH/Compta	Direction
BOUAZIZ	Jonathan	j.bouaziz	J7]74!rTy0	Gestion	Open-space
MARCHAL	Chloé	c.marchal	38uJk^5#rE	Location	Open-space
ALVAREZ	Florian	f.alvarez	mlU@0yXw!1	Achats	Open-space
DIOP	Constance	c.diop	A\87#hMc!9	Ventes	Open-space

Les noms et identifants utilisés pour chaque service sont répertoriés dans le tableau ci-dessous.

ÉQUIPEMENT	SERVICE	IDENTIFIANT	MOT DE PASSE
PFSENSE	Interface web	admin	Ih?4j^35Ty
SRV-SERVICE	Session	Administrateur	u8a^]AT6vC
	Annuaire DSRM	X	yU23-_7!5v

2) PLAN D'ADRESSAGE

Je décide, pour réaliser le plan d'adressage de cette infrastructure, d'utiliser une adresse de réseau privée de classe C. Etant donné le peu d'hôtes présents sur le réseau, il est même possible de réduire la quantité d'hôtes en adaptant le masque par défaut du sous-réseau.

Le tableau présenté ci-dessous expose le plan d'adressage choisi pour ce projet.

INFORMATIONS RELATIVES AU RESEAU	
Réseau	192.168.1.0/28 (255.255.255.240)
Nombre d'hôtes	14
Première adresse hôte	192.168.1.1
Dernière adresse hôte	192.168.1.14
Etendue DHCP	192.168.1.7 – 192.168.1.13
Passerelle par défaut	192.168.1.1
DNS principal	192.168.1.2
DNS secondaire	8.8.8.8
Domaine	occimmobilier.lan
INFORMATIONS RELATIVES AUX EQUIPEMENTS DU RESEAU	
NOM	ADRESSE IPv4
PFSENSE	192.168.1.1
SRV-SERVICES	192.168.1.2
SRV-DATA	192.168.1.3
NAS-BKP	192.168.1.4
FREEPBX	192.168.1.5
PC-DELPECH	DHCP
PC-DELOITTE	DHCP
PC-BOUAZIZ	DHCP
PC-MARCHAL	DHCP
PC-ALVAREZ	DHCP
PC-DIOP	DHCP
PC-TECHINFO	192.168.1.14

Six adresses sont réservées à la partie infrastructure tandis-que six adresses de l'étendue DHCP seront utilisées par les salariés. Cela laisse donc une possibilité d'extension d'une adresse supplémentaire pour l'ajout d'un équipement à l'infrastructure et d'une adresse supplémentaire pour le recrutement d'un éventuel salarié. S'agissant d'une agence immobilière de proximité, cela me convient pour valider le plan d'adressage.

L'image présentée dans la page suivante permet d'appréhender visuellement l'organisation de cette infrastructure (**Figure 01**). Ce schéma a été réalisé avec le logiciel Cisco Packet Tracer.

3) SCHÉMA RÉSEAU

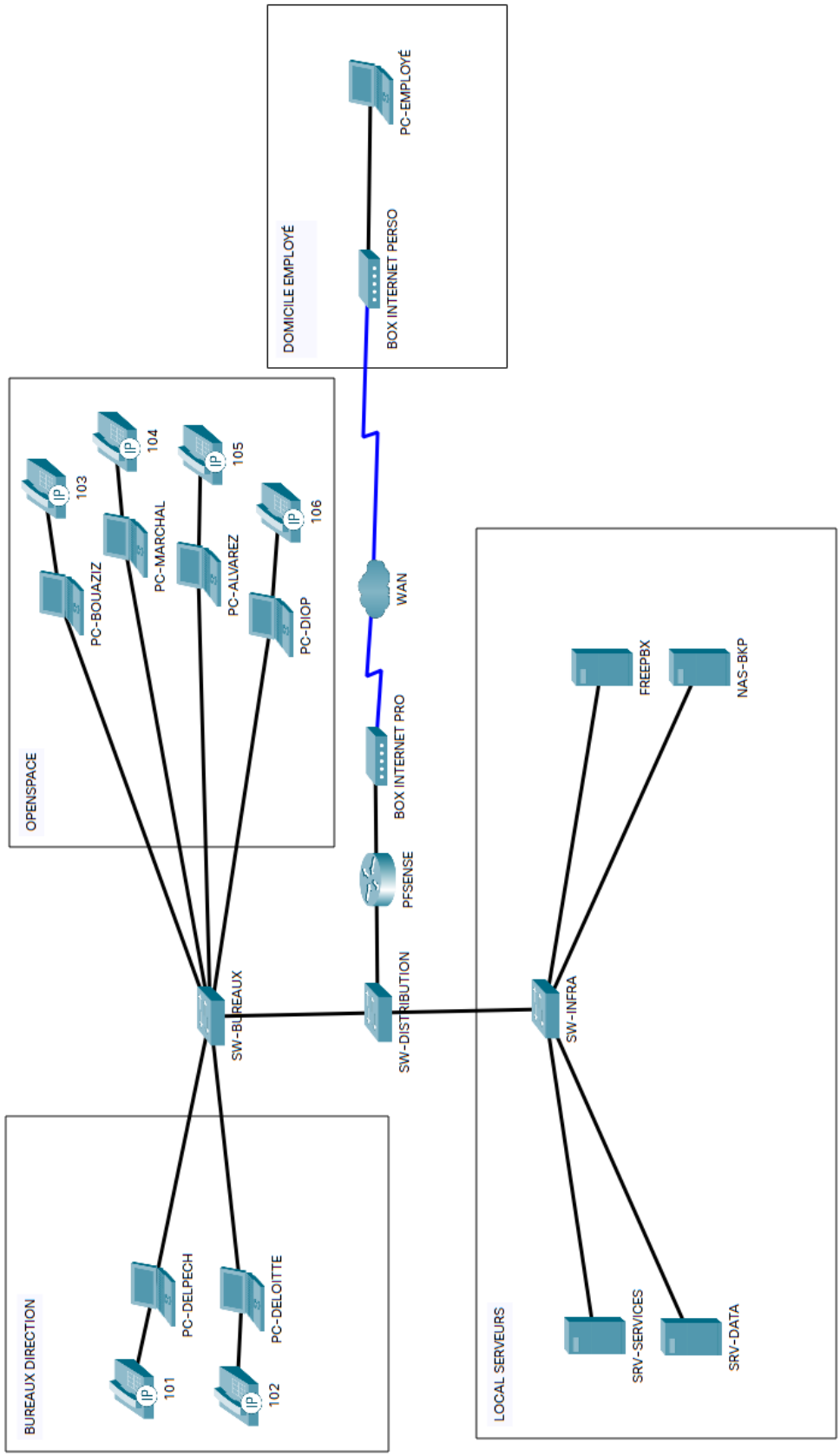

Figure 01 - Schéma réseau de l'infrastructure de l'agence.

PARTIE II – PARAMÉTRAGE DE MICROSOFT HYPER-V

1) ACTIVATION D'HYPER-V

Sur le PC préparé pour la réalisation de ce PPE, j'entre le mot clé **Activer** dans la barre de recherche de la barre des tâches et je sélectionne **Activer ou désactiver des fonctionnalités de Windows**. Dans la fenêtre nouvelle ouverte, je recherche et je sélectionne **Hyper-V** avant de de cliquer sur le bouton **OK** (**Figure 02**).

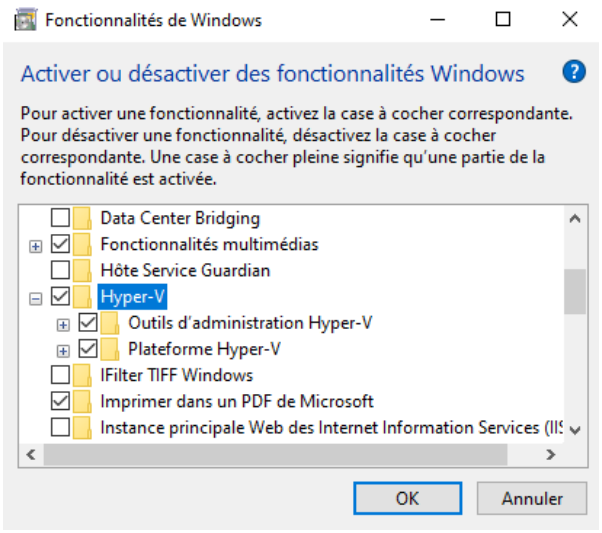

Figure 02 - Activation de la fonctionnalité Hyper-V.

L'installation de la fonctionnalité se poursuit et nécessite le redémarrage de l'ordinateur pour être terminée.

Après redémarrage, j'entre le mot clé **Hyper** dans la barre de recherche pour ouvrir le **Gestionnaire Hyper-V** (**Figure 03**).

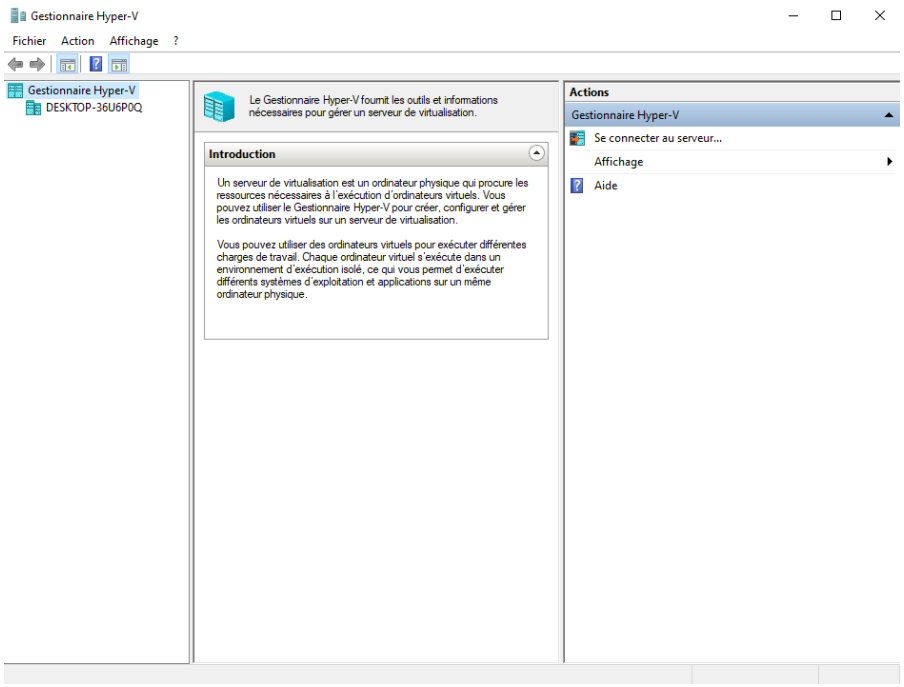

Figure 03 - Fenêtre du Gestionnaire Hyper-V.

Sur la droite de la fenêtre, dans l'onglet **Actions**, je clique sur **Se connecter au serveur…** et je sélectionne **Ordinateur local** avant de valider en cliquant sur le bouton **OK** (**Figure 04**).

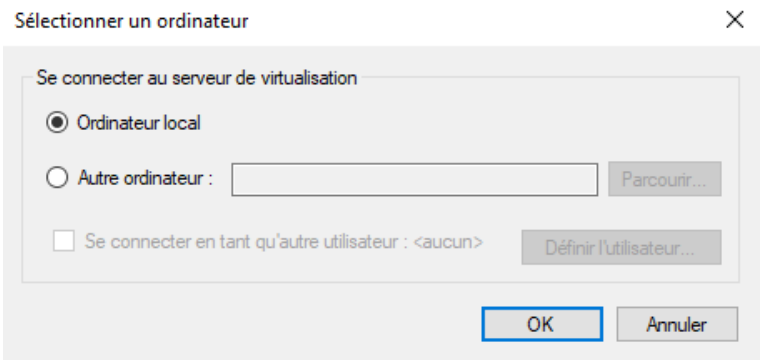

Figure 04 - Sélection du serveur de virtualisation.

La sélection d'**Ordinateur local** permet de définir ma propre machine physique comme serveur de virtualisation.

Après m'être rendu sur le site de pfSense pour télécharger la version **AMD64 (64-bit)** en version **DVD Image (ISO) Installer**, je retourne sur le **Gestionnaire Hyper-V**, dans l'onglet **Actions** pour sélectionner **Gestionnaire de commutateur virtuel…** afin de créer une interface **LAN** pour mon pfSense.

En cliquant sur **Nouveau commutateur réseau virtuel**, je sélectionne **Privé** et je clique sur le bouton **Créer le commutateur virtuel**. Je sélectionne alors le nouveau commutateur apparaissant dans la liste de gauche pour le renommer en **LAN** avant de valider en cliquant sur le bouton **OK** (**Figure 05**).

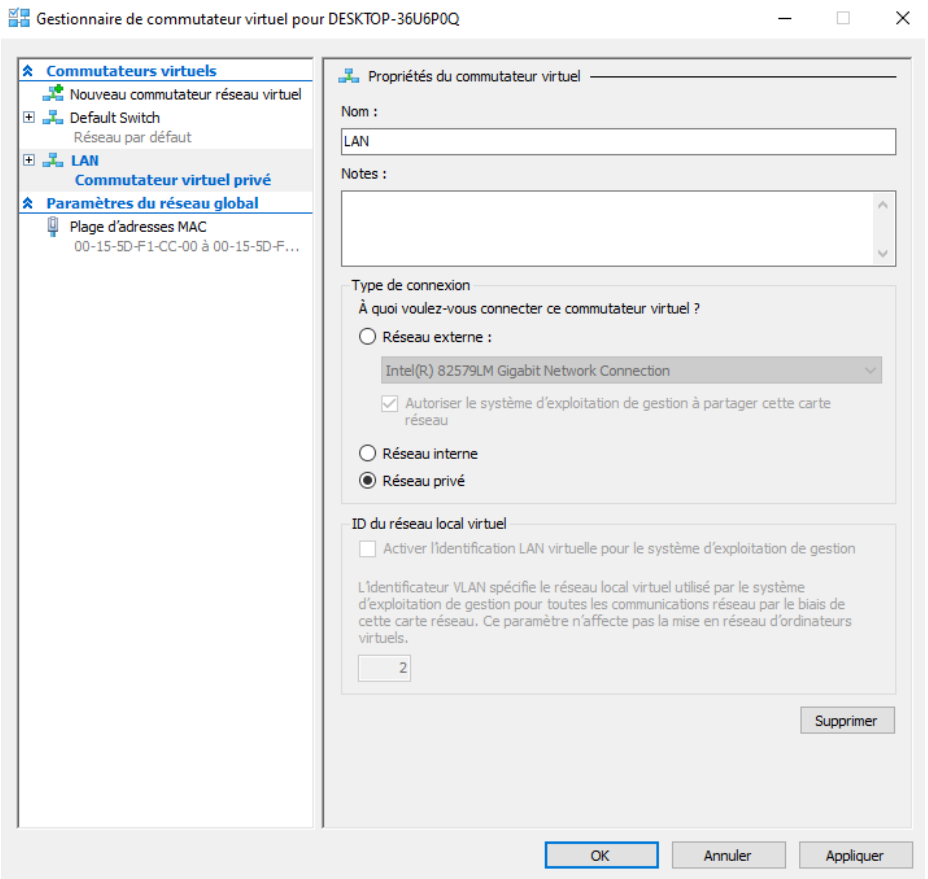

Figure 05 - Propriétés du nouveau commutateur virtuel.

2) PRÉPARATION DE LA MACHINE VIRTUELLE POUR LE PFSENSE

J'obtiens donc deux commutateurs, le **Default Switch** qui correspondra à l'interface WAN de mon routeur et le commutateur **LAN** qui représentera l'interface du même nom sur le pfSense.

De retour sur le **Gestionnaire Hyper-V**, dans l'onglet **Actions**, je sélectionne **Nouveau** puis **Ordinateur virtuel…** pour créer la machine virtuelle. Je nomme celle-ci **PFSENSE** (Figure 06).

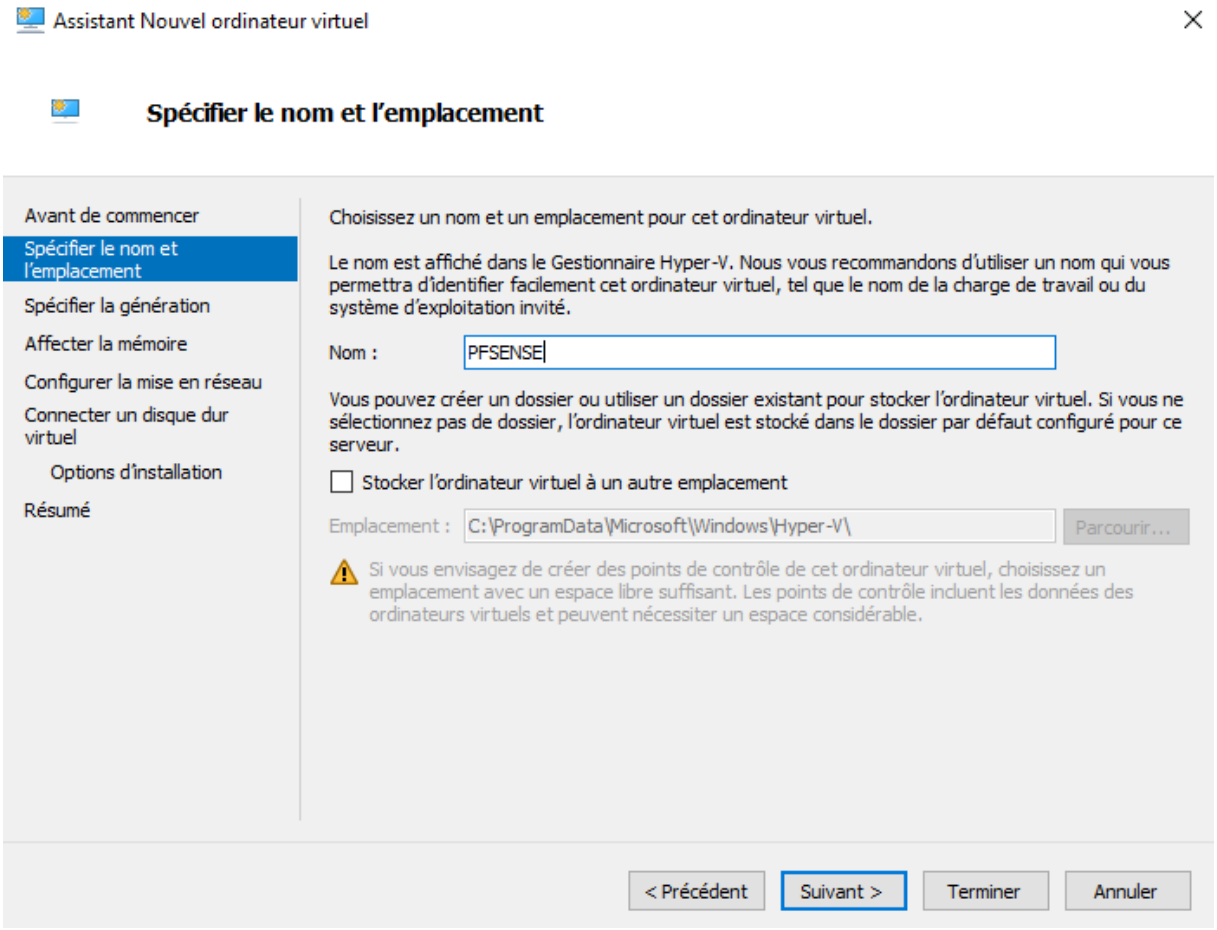

Figure 06 - Assistant nouvel ordinateur virtuel.

J'entre alors les paramètres reportés dans le tableau ci-dessous en cliquant sur le bouton **Suivant >** entre chaque étape. Je termine la configuration en appuyant sur le bouton **Terminer**.

ÉTAPE	PARAMÈTRES
Spécifier la génération	Génération 2
Affecter la mémoire	1024 Mo, utiliser la mémoire dynamique
Configurer la mise en réseau	Connexion Default Switch
Connecter un disque dur virtuel	Créer un disque dur virtuel, 20 Go
Option d'installation	A partir d'un fichier image de démarrage, monter l'ISO
Résumé	Contrôler et valider en cliquant sur Terminer

Ma machine virtuelle apparait désormais dans l'onglet du milieu du **Gestionnaire Hyper-V**. Dans l'onglet **Actions**, sous **PFSENSE**, je clique sur le menu **Paramètres…** pour sélectionner **Ajouter un matériel** dans l'onglet de gauche. Je sélectionne **Carte réseau** et je clique sur bouton **Ajouter**. Je choisis alors le Commutateur virtuel **LAN** pour celle-ci (**Figure 07**).

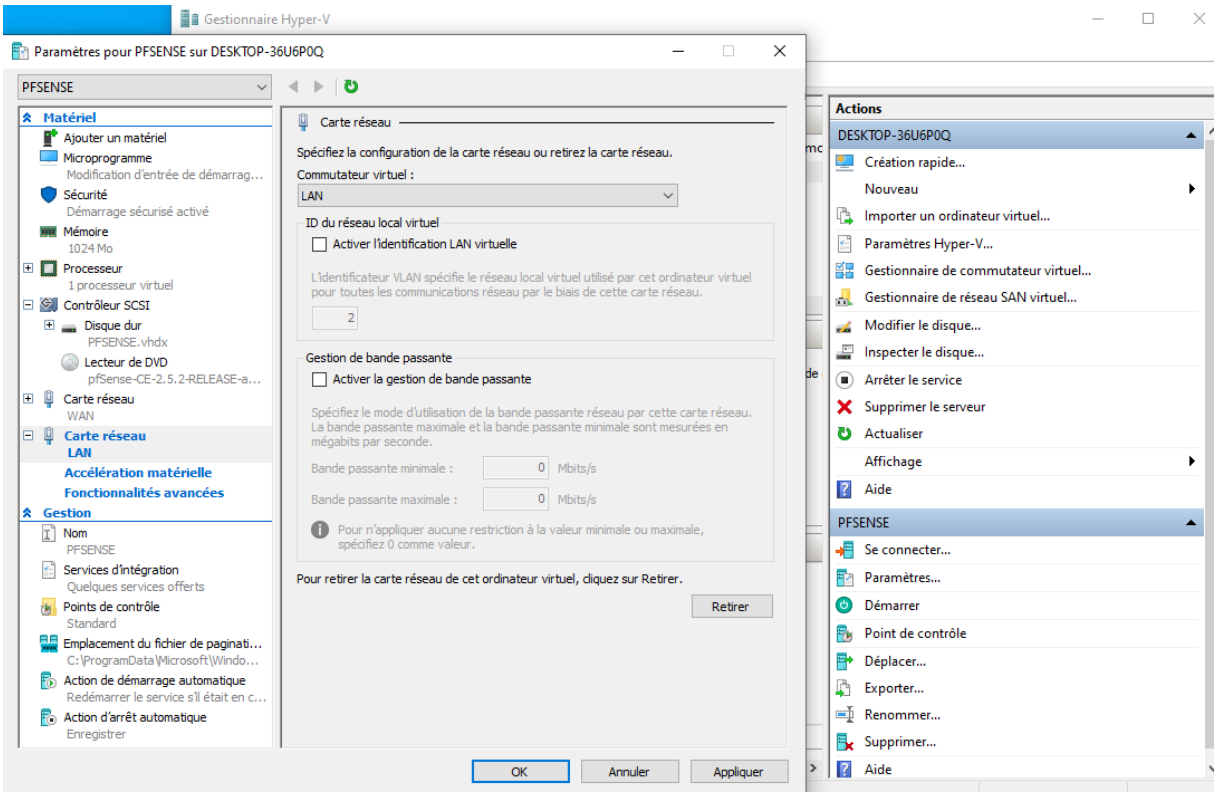

Figure 07 - Ajout d'une nouvelle carte réseau LAN.

NOTE : Lors d'essais précédent l'installation finale du pfSense, j'ai d'abord créé un commutateur nommé **WAN**. Certaines captures d'écran feront apparaitre ce nom en lieu et place de **Default Switch**. L'installation finale utilise bien le commutateur **Default Switch**.

Je peux maintenant lancer l'installation du pfSense en démarrant la machine virtuelle.

PARTIE III – MISE EN SERVICE DU PFSENSE

1) INSTALLATION DU PFSENSE

Dans le **Gestionnaire Hyper-V**, dans le menu **Actions**, sous **PFSENSE**, je sélectionne **Se connecter…** puis je clique sur le bouton **Démarrer**. Le menu d'installation du pfSense apparait alors et me demande d'accepter les termes d'un contrat de licence (**Figure 08**).

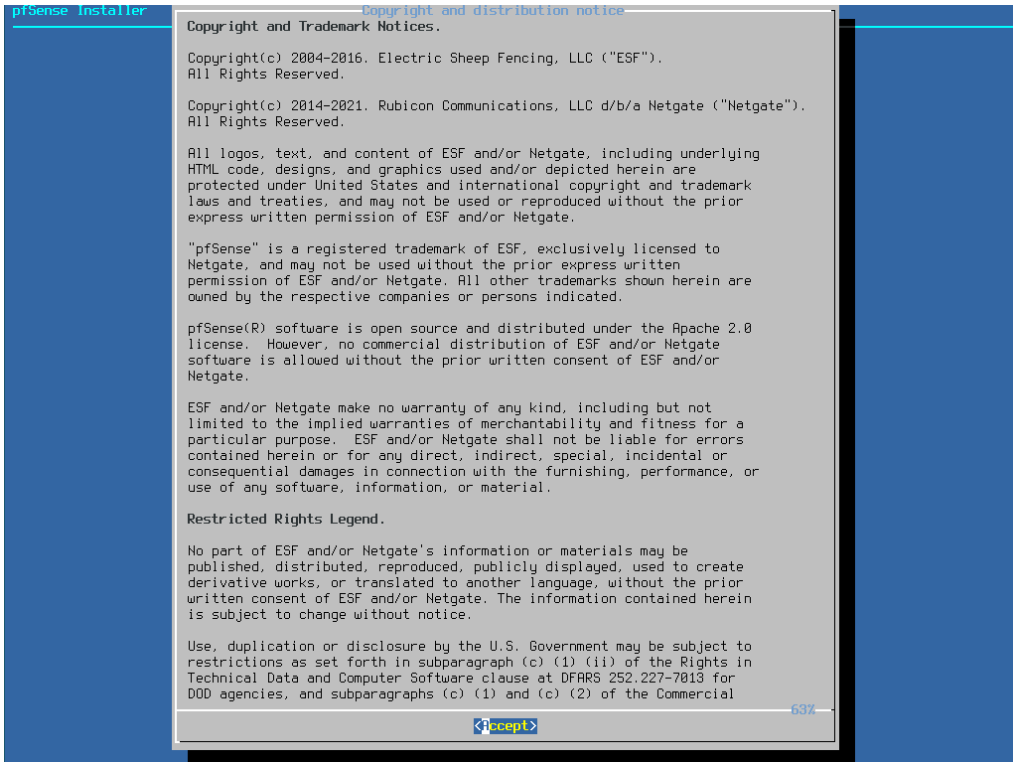

Figure 08 - Contrat de licence du pfSense.

L'acceptation de celui-ci me conduit sur la page d'accueil de l'installeur sur laquelle je sélectionne l'option **Install** (**Figure 09**).

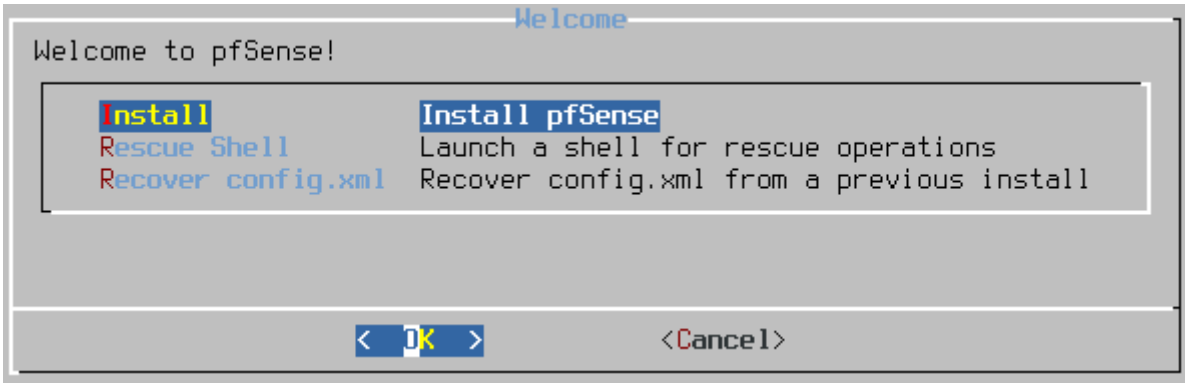

Figure 09 - Menu d'accueil du pfSense.

L'écran suivant me permet de sélectionner la langue du clavier. Je choisis **French (accent keys)** avant de poursuivre.

La page suivante me permet de choisir le partitionnement (Figure 10). Je sélectionne **Auto (ZFS)** ce qui m'envoie sur la page suivante me permettant de sélectionner le disque à utiliser (Figure 11).

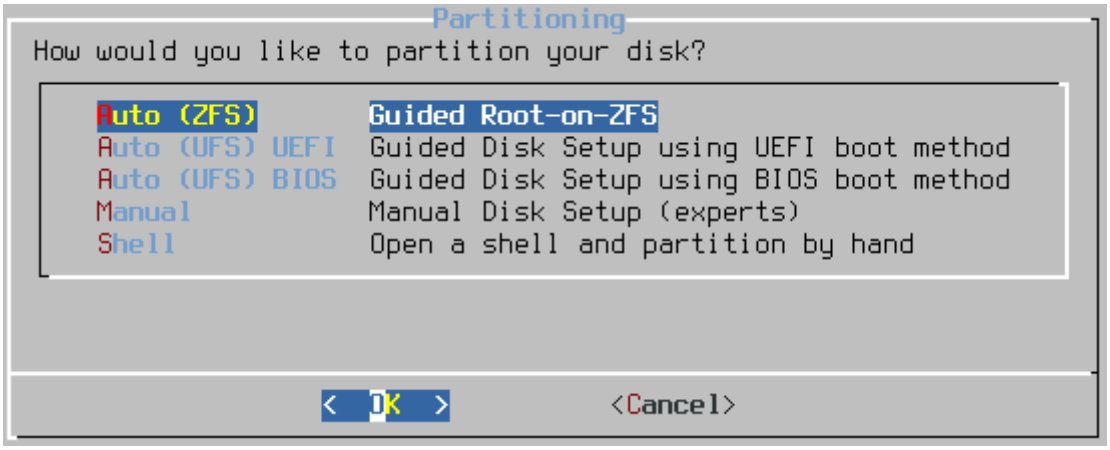

Figure 10 - Choix de la méthode de partitionnement.

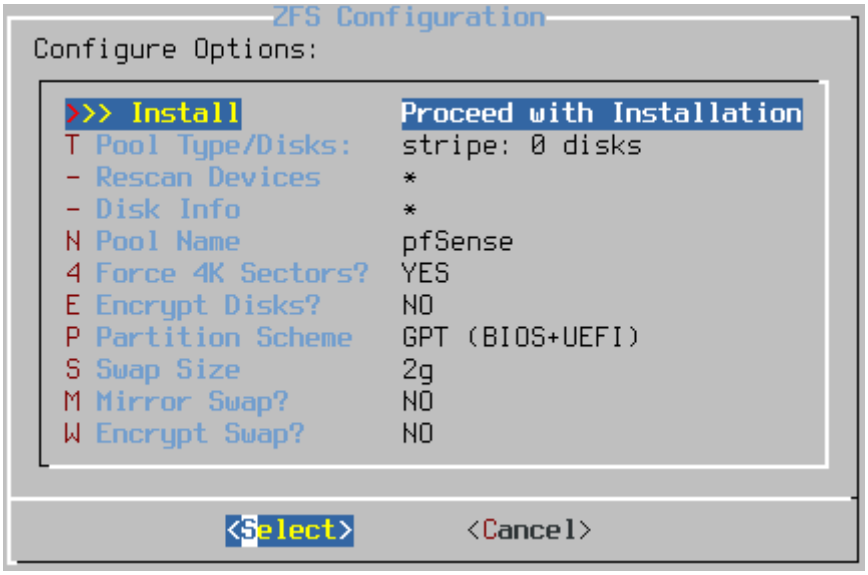

Figure 11 - Configuration du ZFS.

En choisissant l'option **Pool Type/Disks**, je peux sélectionner mon disque dur virtuel (Figure 12). De retour sur la page précédente, je choisis **Install**.

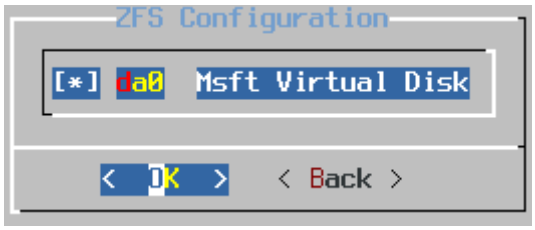

Figure 12 - Choix du disque dur virtuel.

Un message d'avertissement apparait alors pour me demander de confirmer le formatage de la partition du disque. Après avoir accepté, l'installation démarre et me demande si je souhaite ouvrir un terminal pour ajouter des paramètres supplémentaires. Je choisis **No** et l'installation se termine par un message me demandant de rebooter la machine virtuelle (**Figure 13**).

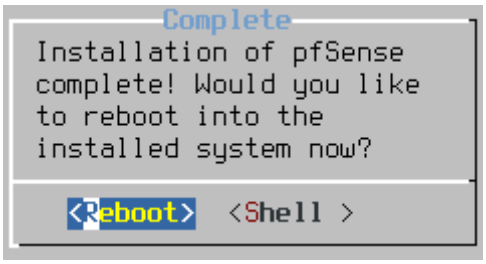

Figure 13 - Demande de redémarrage de la machine virtuelle.

Sachant qu'il est désormais nécessaire de démonter le fichier ISO du pfSense pour que celui-ci démarre sur le disque dur virtuel, j'éteins la machine virtuelle en utilisant le bouton **Éteindre** de la fenêtre **Hyper-V**.

Dans le **Gestionnaire Hyper-V**, dans l'onglet **Actions**, sous **PFSENSE**, je sélectionne **Paramètres…** et je clique sur **Lecteur de DVD** à gauche. Sous **Média**, je coche l'option **Aucun** avant de valider en cliquant sur le bouton **OK** (**Figure 14**). Je peux alors redémarrer le pfSense.

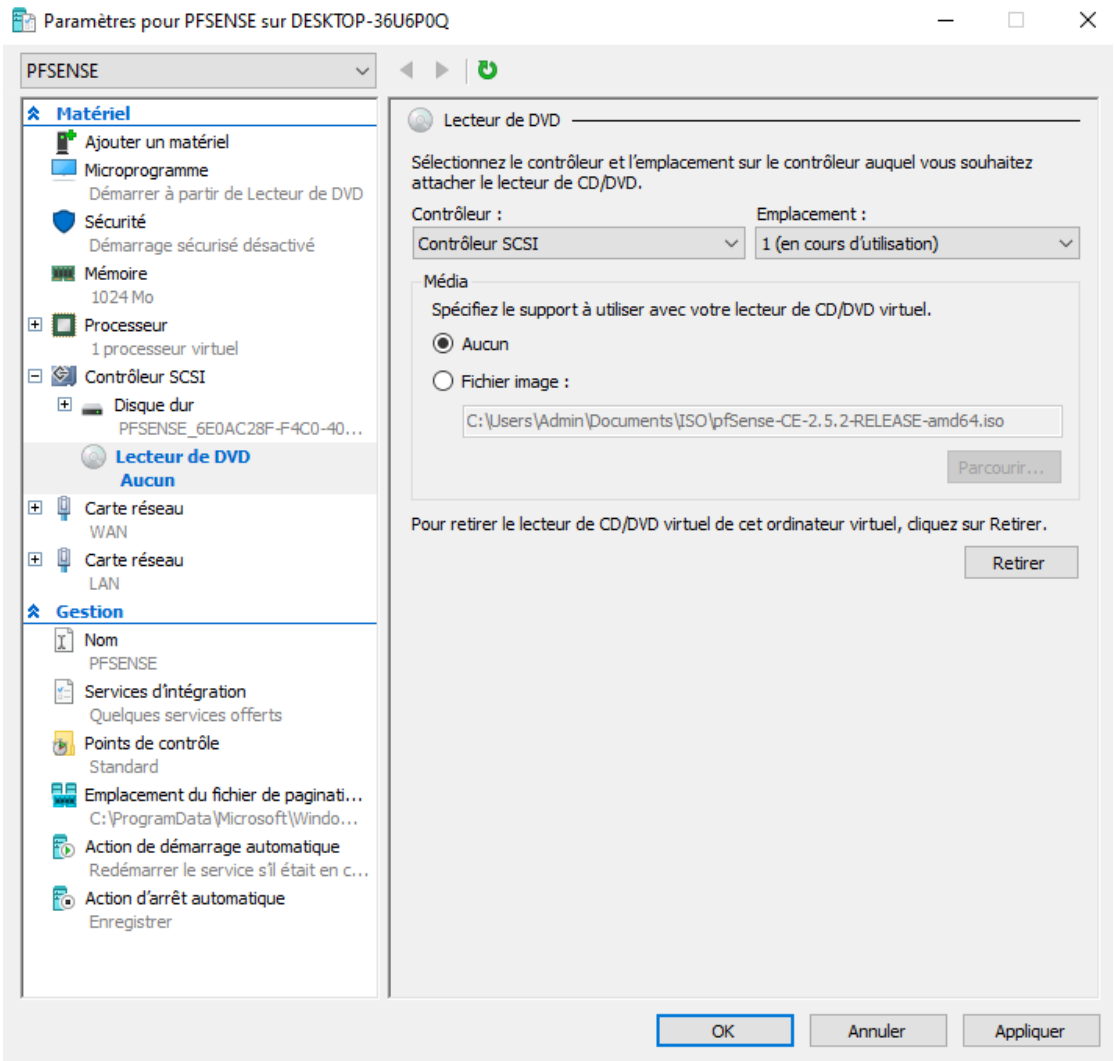

Figure 14 - Démontage du fichier ISO.

2) CONFIGURATION DU PFSENSE EN LIGNES DE COMMANDE

Après redémarrage de la machine virtuelle, une fenêtre en lignes de commandes apparait pour me demander de configurer les interfaces du pfSense. J'entre alors les paramètres reportés dans le tableau ci-dessous (**Figure 15**).

DEMANDE DE CONFIGURATION	RÉPONSE
Sould VLANs be set up now [y|n] ?	n
Enter the WAN interface name	hn0
Enter the LAN interface name	hn1
Do you want to proceed [y|n] ?	y

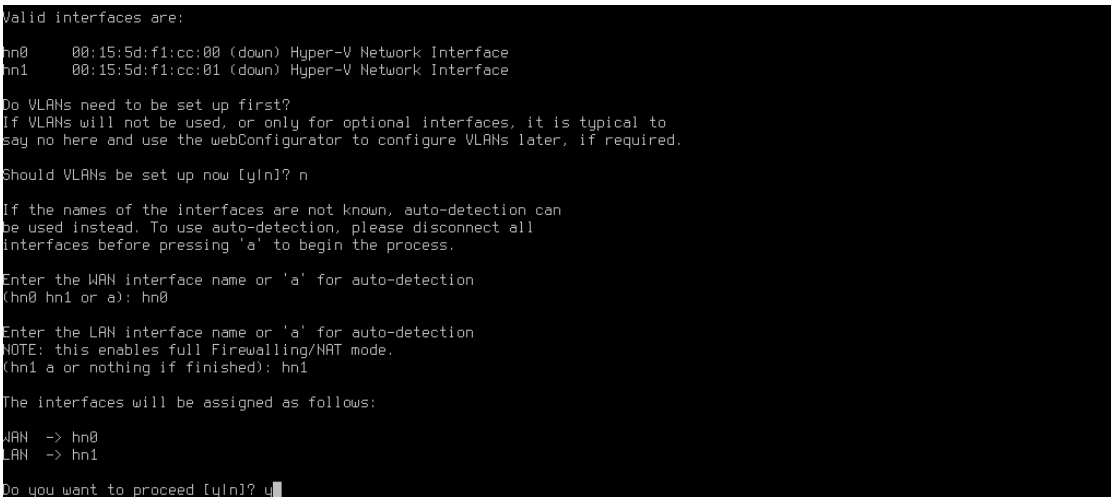

Figure 15 - Configuration des interfaces.

Pour poursuivre la configuration, j'ai besoin d'un ordinateur connecté au réseau de l'infrastructure pour pouvoir accéder à l'interface web du pfSense. J'installe alors un ordinateur fonctionnant avec Windows 10 sur une nouvelle machine virtuelle et je lui affecte les paramètres IP représentés dans la capture d'écran suivante (**Figure 16**). Cet ordinateur virtuel utilise le commutateur virtuel **LAN** et se trouve donc dans le même réseau que le pfSense.

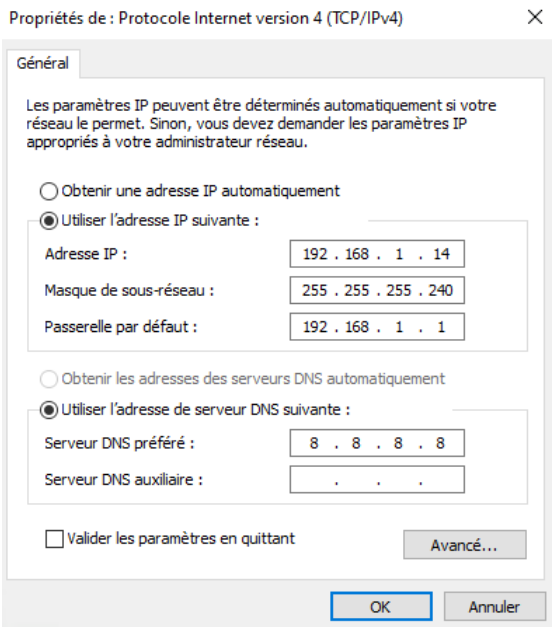

Figure 16 - Adressage IP de l'ordinateur du technicien informatique.

3) CONFIGURATION DU PFSENSE DANS L'INTERFACE WEB

L'adresse du pfSense étant par défaut paramétrée en **192.168.1.1**, il est possible de s'y connecter en entrant cette adresse dans la barre d'adresse du navigateur de mon ordinateur technicien informatique (**Figure 17**).

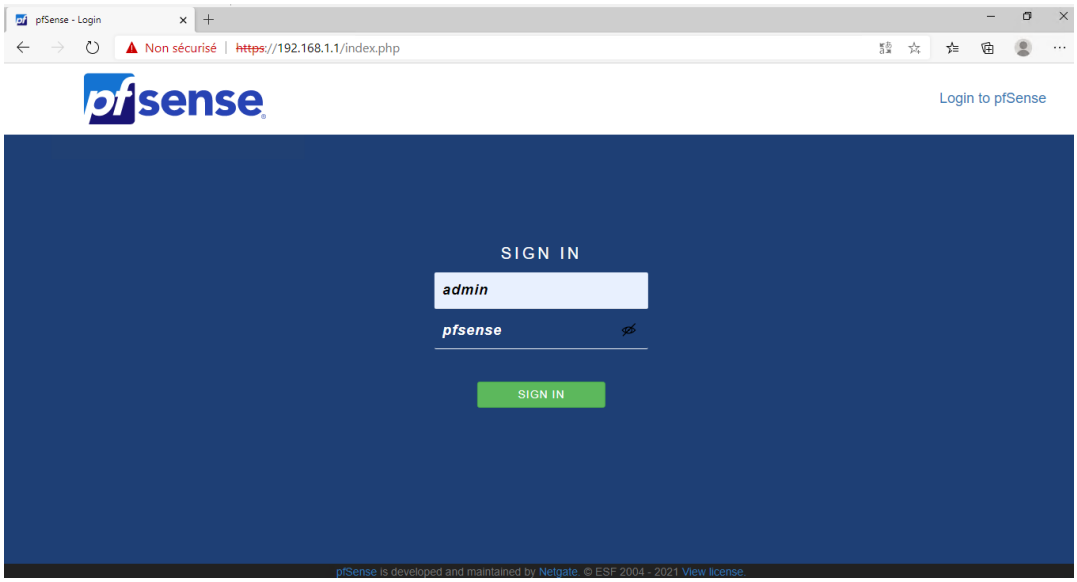

Figure 17 - Page d'authentification de l'interface web du pfSense.

En entrant les identifiants par défaut (**admin/pfsense**), je me connecte à la page d'accueil de l'interface web. Après avoir cliqué sur le bouton **>> Next**, j'accepte les conditions d'utilisation avant de voir apparaitre le dashboard du pfSense (**Figure 18**).

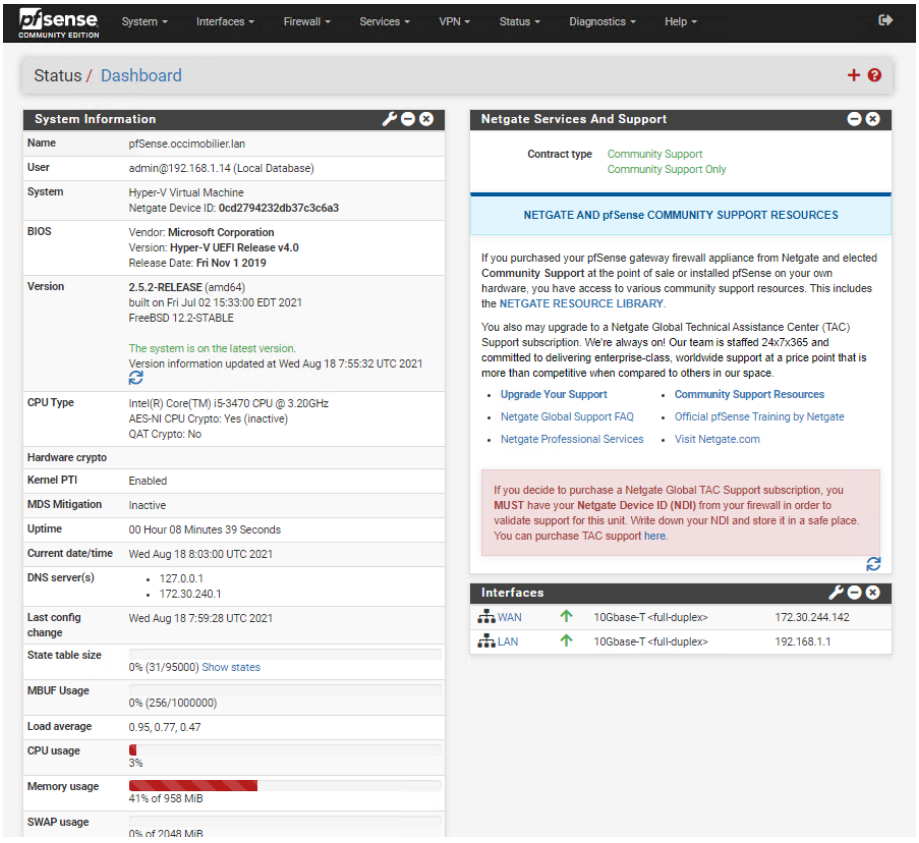

Figure 18 - Dashboard du pfSense.

J’entreprends tout d’abord de remplacer le mot de passe par défaut du pfSense par un mot de passe complexe et sécurisé. Dans le menu de l’interface, je sélectionne **System**, **User Manager** et j’édite l’utilisateur admin pour changer son mot de passe en **Ih?4j^35Ty** (Figure 19).

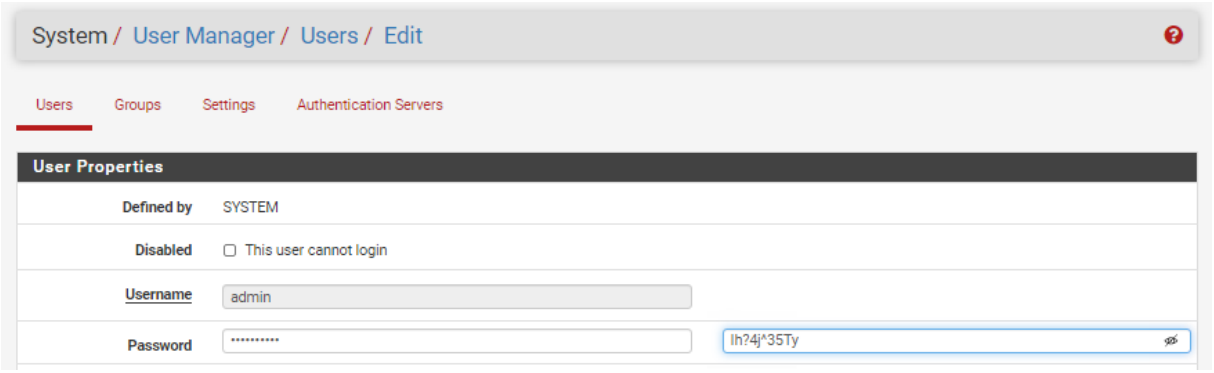

Figure 19 - Changement du mot de passe de l'utilisateur admin.

Je me rends ensuite dans **Interfaces**, **LAN** pour sélectionner **Static IPv4** pour le champ **IPv4 Configuration Type** et entrer l’adresse **192.168.1.1** avec le masque **/28** dans le but d’intégrer le sous-réseau de mon infrastructure (Figure 20).

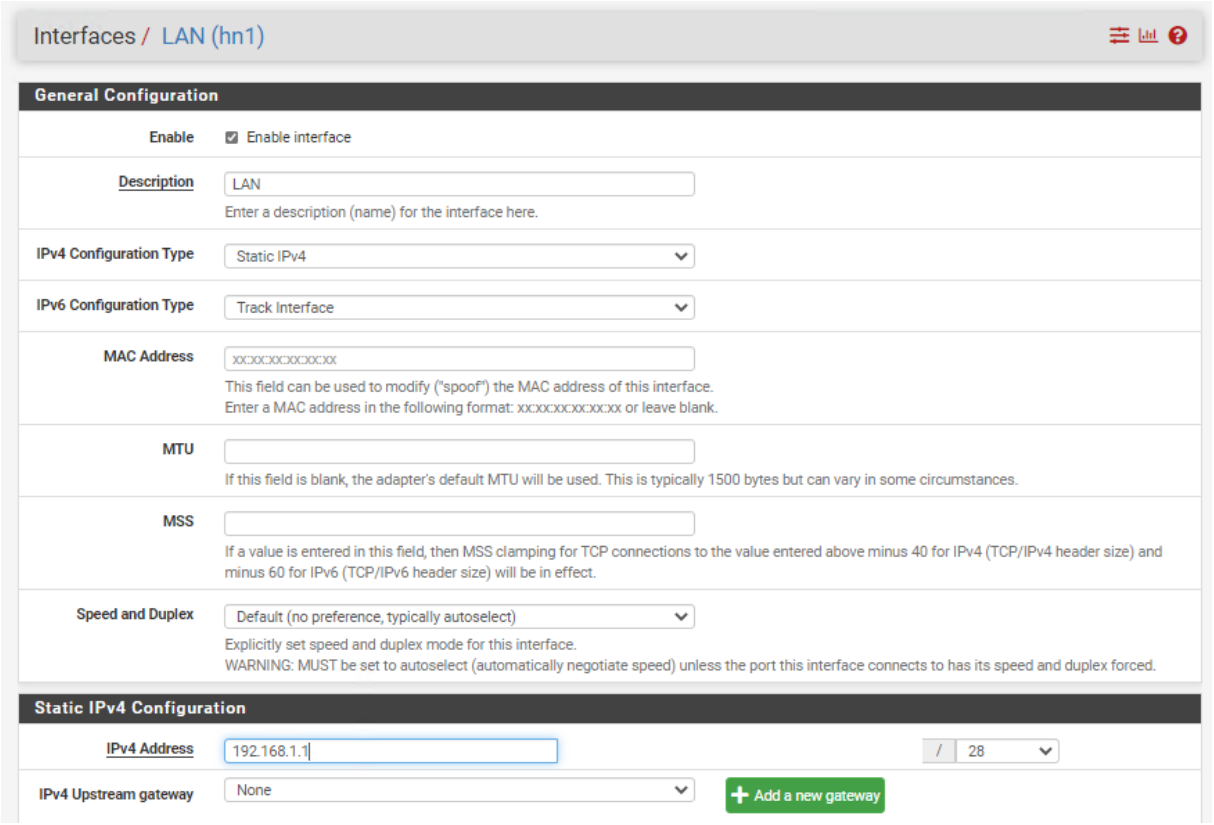

Figure 20 - Adressage IP de l'interface LAN du pfSense.

Je me rends ensuite dans **System**, **General Setup** pour modifier le champ **Domain** en **occimmobilier.lan** et entrer l'adresse **192.168.1.2** dans le champ **DNS Servers** (Figure 21).

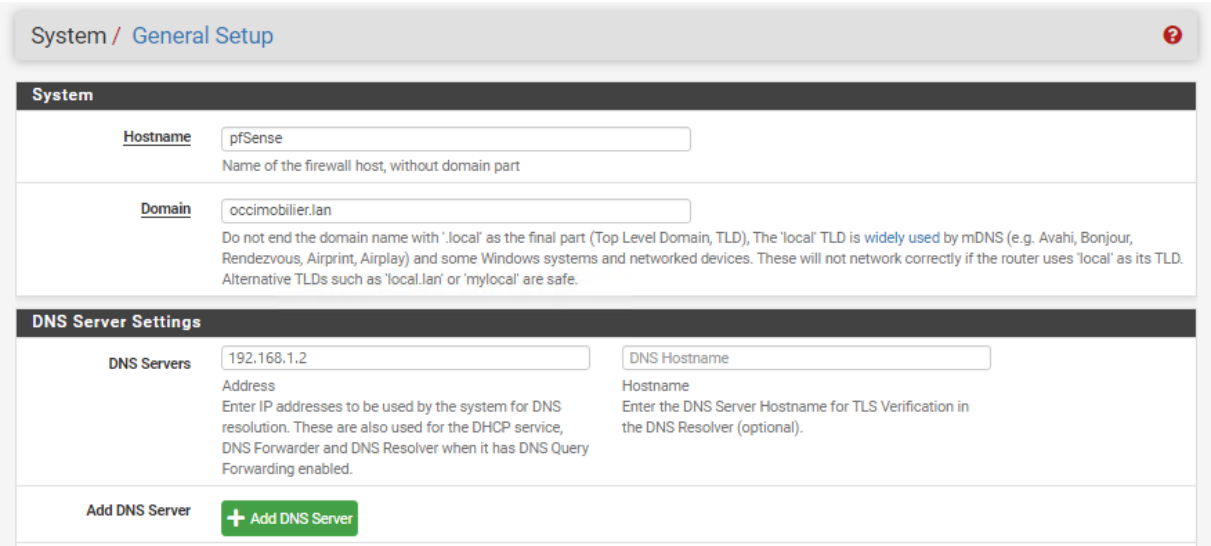

Figure 21 - Spécification du domaine et de l'adresse DNS.

Enfin, sur mon ordinateur technicien informatique, je teste la connectivité à internet (Figure 22). Celui-ci est en effet sur le commutateur virtuel **LAN**. Il ne dispose pas de connectivité à internet. En ayant indiqué l'adresse du pfSense comme adresse de passerelle, celui-ci devrait théoriquement pouvoir accéder à internet.

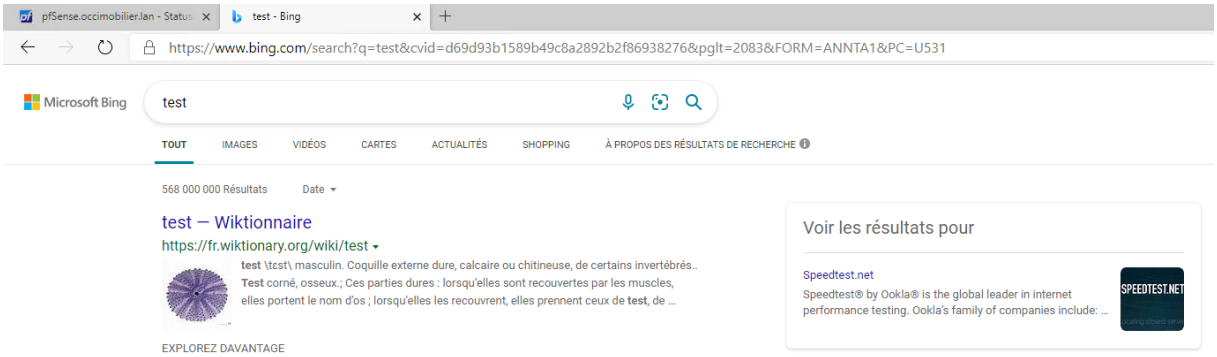

Figure 22 - Test de la connectivité à internet depuis l'ordinateur technicien informatique.

Le pfSense est désormais fonctionnel, configuré, et permet le trafic des paquets entre le WAN et mon réseau privé.

PARTIE IV – MISE EN PLACE DES SERVICES SUR SRV-SERVICES

1) NOMMAGE ET ADRESSAGE

Dans cette seconde partie, je créé une nouvelle machine virtuelle pour installer mon serveur de services, **SRV-SERVICES**.

J'entre les paramètres suivants dans les options de l'**Assistant Nouvel ordinateur virtuel**.

ÉTAPE	PARAMÈTRES
Spécifier le nom	SRV-SERVICES
Spécifier la génération	Génération 2
Affecter la mémoire	2048 Mo, utiliser la mémoire dynamique
Configurer la mise en réseau	Connexion LAN
Connecter un disque dur virtuel	Créer un disque dur virtuel, 40 Go
Option d'installation	A partir d'un fichier image de démarrage, monter l'ISO
Résumé	Contrôler et valider en cliquant sur Terminer

Dans les paramètres du système, je change le nom de l'ordinateur en **SRV-SERVICES** (**Figure 23**).

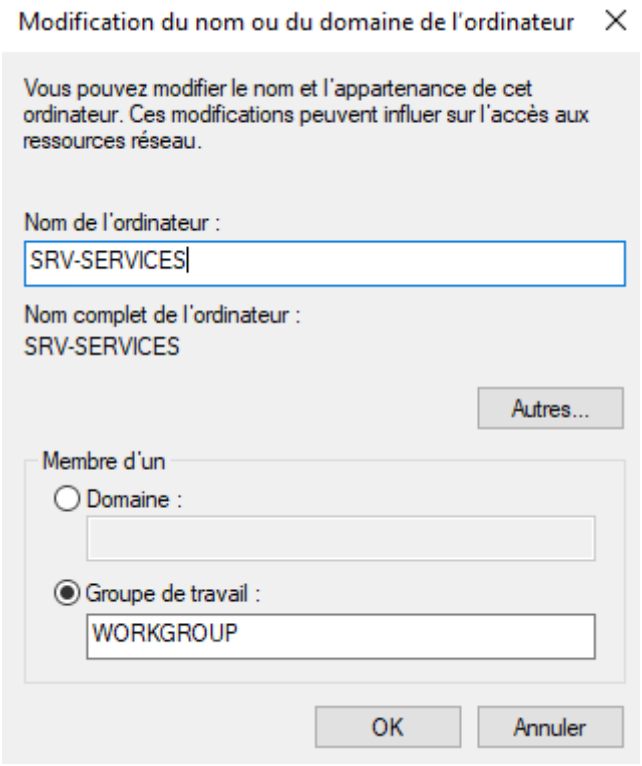

Figure 23 - Modification du nom du serveur.

Dans les paramètres de la carte réseau, j'effectue l'adressage présenté dans la capture d'écran ci-dessous (**Figure 24**).

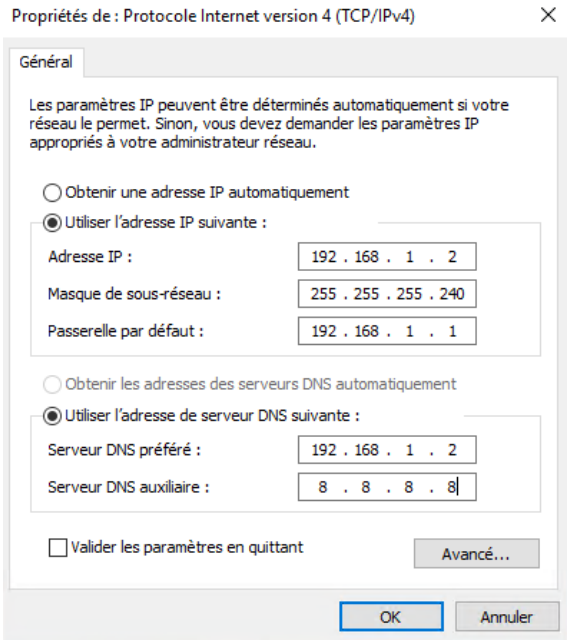

Figure 24 - Adressage IP du serveur.

2) INSTALLATION DU SERVICE DHCP

Après avoir installé et configuré les services **AD** et **DNS** sur le serveur, tel que vu dans mon second PPE, j'installe le service **DHCP** qui distribuera des adresses aux salariés de l'agence dans une étendue d'adresse définie par mes soins.

Une fois installé à l'aide de **l'Assistant Ajout de rôles et de fonctionnalités**, j'entre les informations d'identification dans l'**Assistant Configuration post-installation DHCP** (**Figure 25**). Je termine en cliquant sur **Valider**.

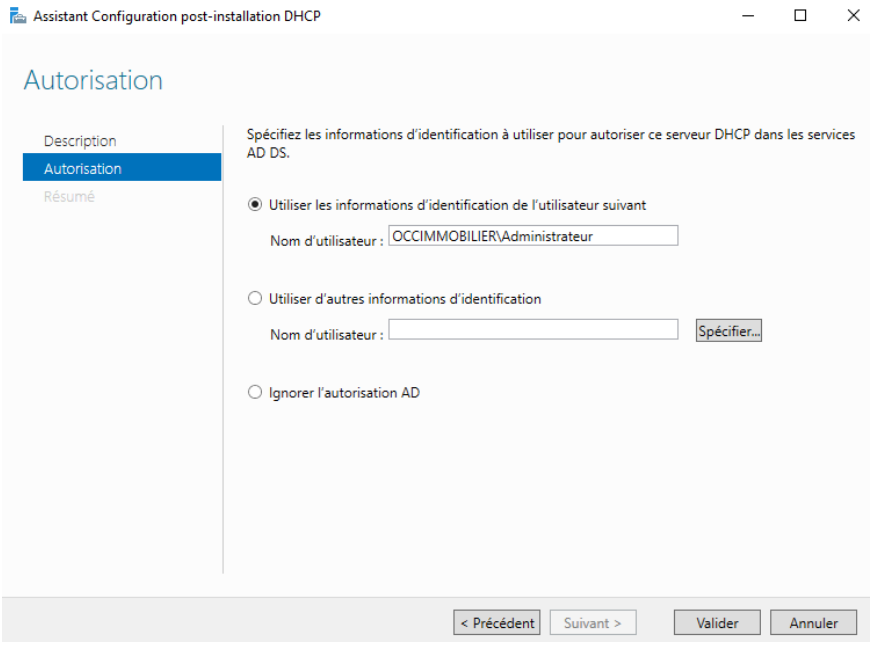

Figure 25 - Utilisation des informations d'identification de l'utilisateur Administrateur.

3) CRÉATION D'UNE NOUVELLE ÉTENDUE DHCP

J'ouvre ensuite l'application **DHCP**. Sur le côté gauche de la fenêtre, je déroule **srv-services.occimmobilier.lan** et je sélectionne **Nouvelle étendue…** après avoir fait un clic droit sur **IPv4** (**Figure 26**).

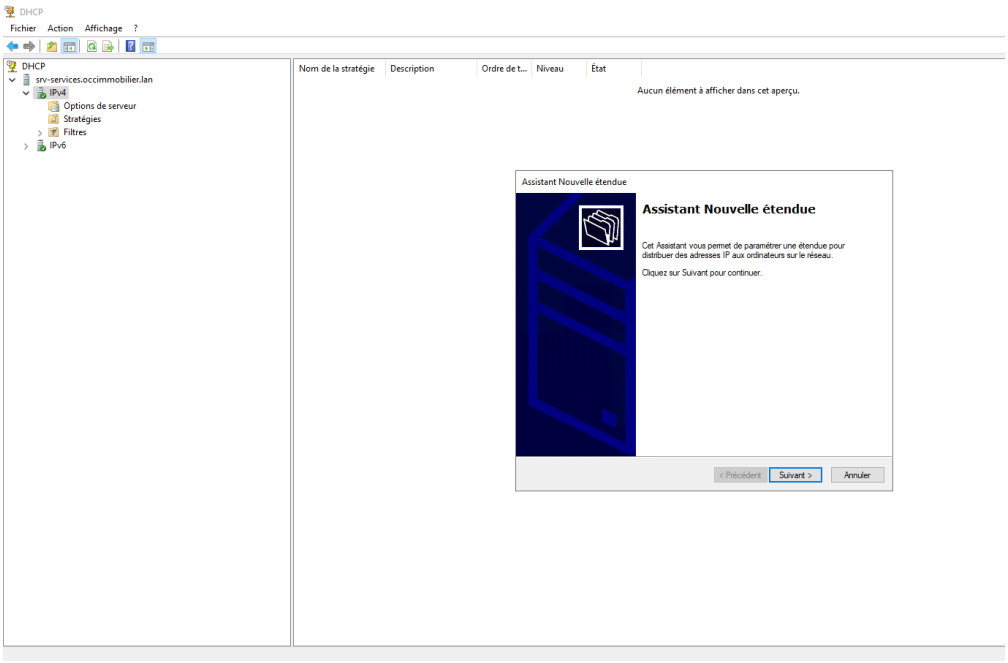

Figure 26 - Fenêtre de l'Assistant Nouvelle étendue.

Après avoir cliqué sur **Suivant >**, j'entre **postes_occimmobilier** dans le champ **Nom** avant de cliquer à nouveau sur **Suivant >**. Sur la nouvelle page, j'entre la plage d'adresse IP désirée et les réglages relatifs au masque de sous-réseau (**Figure 27**). Je valide enfin en cliquant sur **Suivant >**.

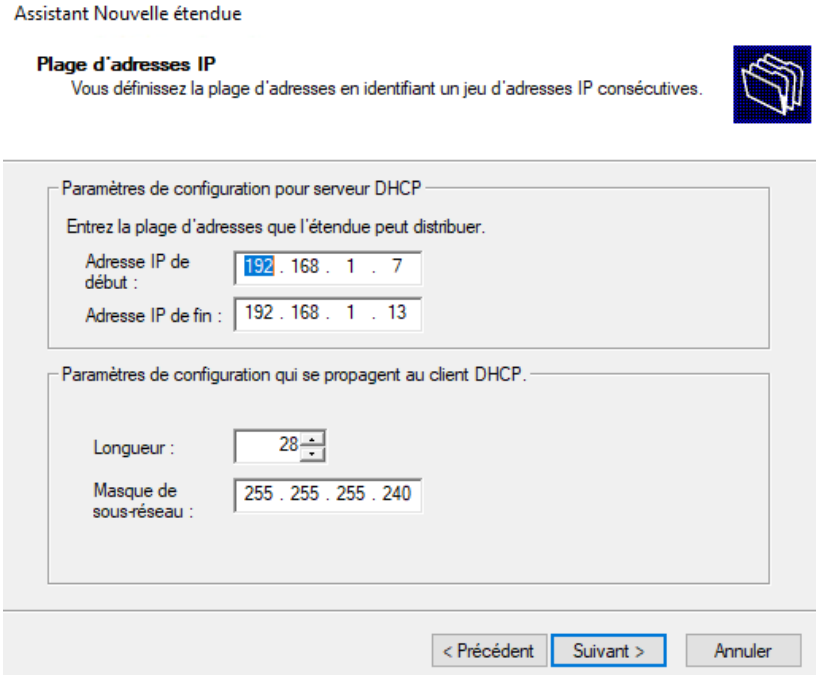

Figure 27 - Paramétrage de la plage d'adresses IP.

L'assistant me propose ensuite d'ajouter une plage d'adresses IP à exclure. N'en ayant pas l'utilité dans le cadre de ce projet, je passe à la page d'après sur laquelle j'entre les réglages de **Durée du bail** (**8 jours**, **00 heures**, **00 Minutes**). J'entre ensuite dans la **Configuration des paramètres DHCP** pour entrer les réglages du **Routeur (passerelle par défaut)** (Figure 28) et du **Nom de domaine et serveurs DNS** (Figure 29).

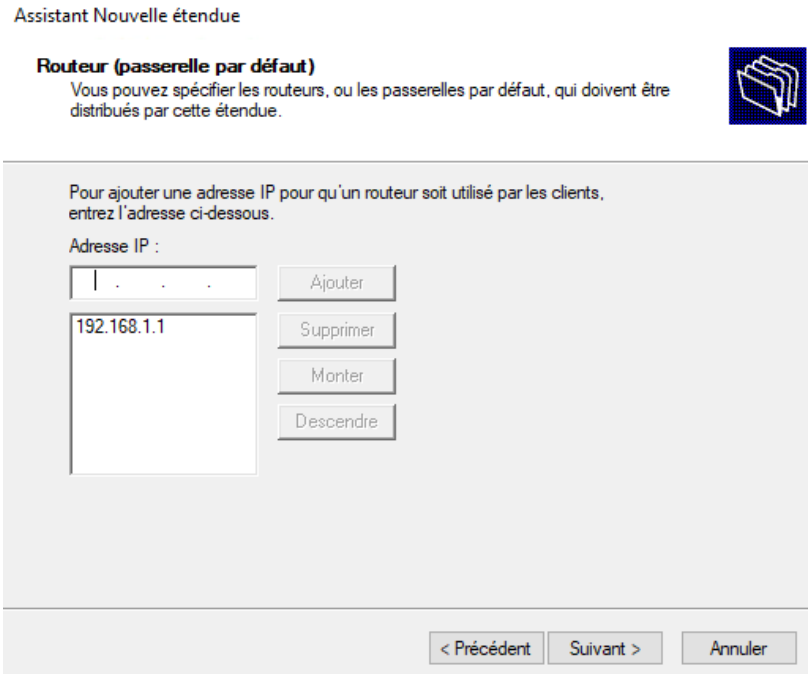

Figure 28 - Ajout de l'adresse de passerelle par défaut.

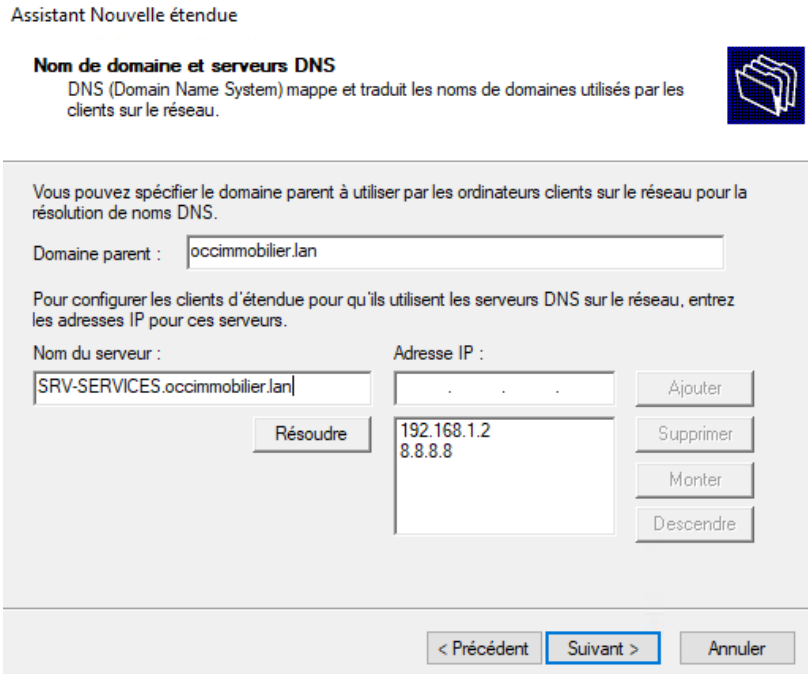

Figure 29 - Ajout du domaine, du nom du serveur DNS et des adresses DNS.

J'arrive ensuite sur la page de configuration des serveurs WINS. N'en utilisant pas, je laisse les réglages par défaut avant de sélectionner le bouton **Suivant >**. J'arrive enfin sur la page **Activer l'étendue** ou je sélectionne l'option **Oui, je veux activer cette étendue maintenant** avant de cliquer sur le bouton **Suivant >**.

L'entendue nouvellement créée apparait désormais dans l'application **DHCP** (**Figure 30**).

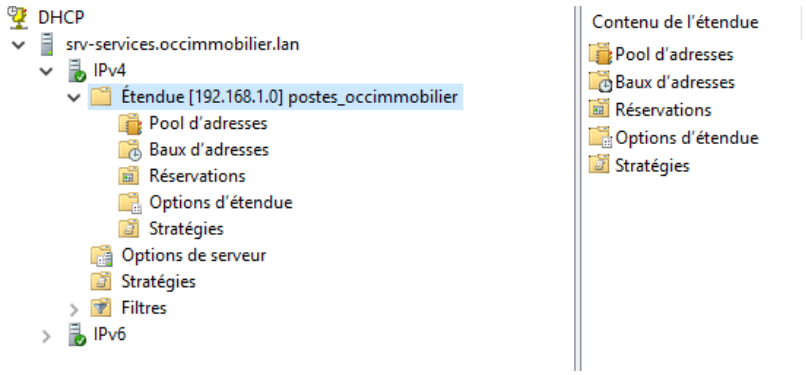

Figure 30 - Nouvelle étendue dans l'application DHCP.

Je retourne ensuite sur la machine virtuelle accueillant l'ordinateur technicien informatique. Dans les paramètres de la carte réseau, je bascule temporairement les réglages sur **DHCP** pour vérifier le fonctionnement du service en entrant la commande **ipconfig /all** dans l'**invite de commande** du système d'exploitation (**Figure 31**).

```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : occimmobilier.lan
   Description. . . . . . . . . . . . . . : Microsoft Hyper-V Network Adapter
   Adresse physique . . . . . . . . . . . : 00-15-5D-F1-CC-02
   DHCP activé. . . . . . . . . . . . . . : Oui
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::f974:ff4d:f94d:b72a%8(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 192.168.1.10(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.240
   Bail obtenu. . . . . . . . . . . . . . : mercredi 25 août 2021 17:26:11
   Bail expirant. . . . . . . . . . . . . : mardi 21 mai 2024 17:25:11
   Passerelle par défaut. . . . . . . . . : 192.168.1.1
   Serveur DHCP . . . . . . . . . . . . . : 192.168.1.2
   IAID DHCPv6 . . . . . . . . . . . : 100668765
   DUID de client DHCPv6. . . . . . . . : 00-01-00-01-28-AB-E5-16-00-15-5D-F1-CC-02
   Serveurs DNS. . .  . . . . . . . . . . : 192.168.1.2
                                    8.8.8.8
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé

C:\Users\SI>
```

Figure 31 - Vérification du fonctionnement du serveur DHCP.

4) INSTALLATION DU SERVICE D'IMPRESSION

Les salariés de l'agence auront besoin d'une imprimante pour imprimer les documents relatifs à leur activité professionnelle. J'ai donc fait le choix d'utiliser un serveur d'impression sur lequel seront installées deux imprimantes en réseau. L'une sera destinée aux bureaux de la direction et l'autre à l'Open-Space.

A l'aide de l'**Assistant Ajout de rôles et de fonctionnalités**, j'ajoute le rôle **Services d'impression et de numérisation de documents**.

Sur la page **Sélectionner des services de rôle**, je coche la case **Serveur d'impression** avant de cliquer sur **Suivant >** (**Figure 32**).

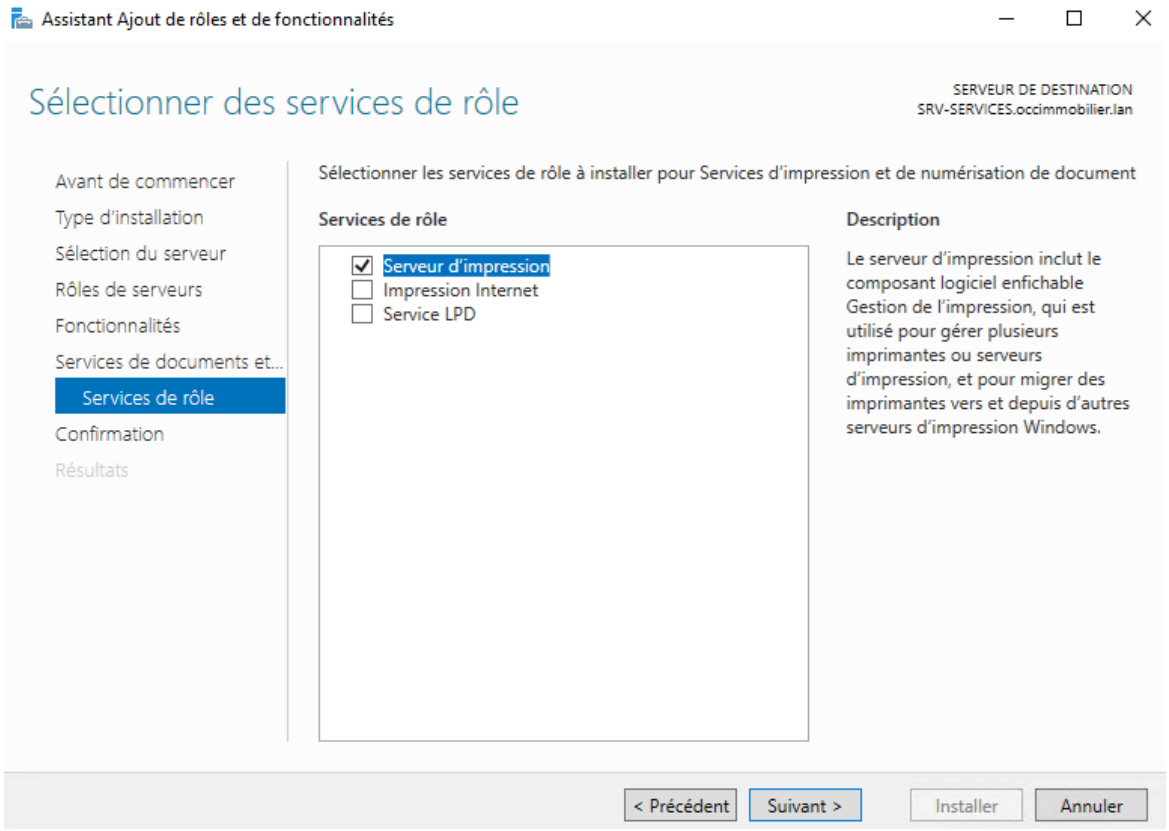

Figure 32 - Sélection du service de rôle Serveur d'impression.

Je poursuis ensuite la configuration de l'assistant pour terminer l'installation du rôle de services d'impression.

5) INSTALLATION D'UNE NOUVELLE IMPRIMANTE SUR LE SERVEUR

J'ouvre maintenant l'application **Gestion de l'impression** et je déroule dans la liste déroulante de gauche **Serveurs d'impression**, **SRV-SERVICES (local)** pour sélectionner **Ajouter une imprimante** après avoir fait un clic droit sur **Imprimantes**.

L'**Assistant Installation d'imprimante réseau** s'ouvre alors. Je sélectionne **Ajouter une nouvelle imprimante via un port existant**. Je choisis alors **FILE: (Impression dans un fichier)** dans la liste déroulante de droite, pour simuler une imprimante physique qui se trouverait dans les locaux (**Figure 33**).

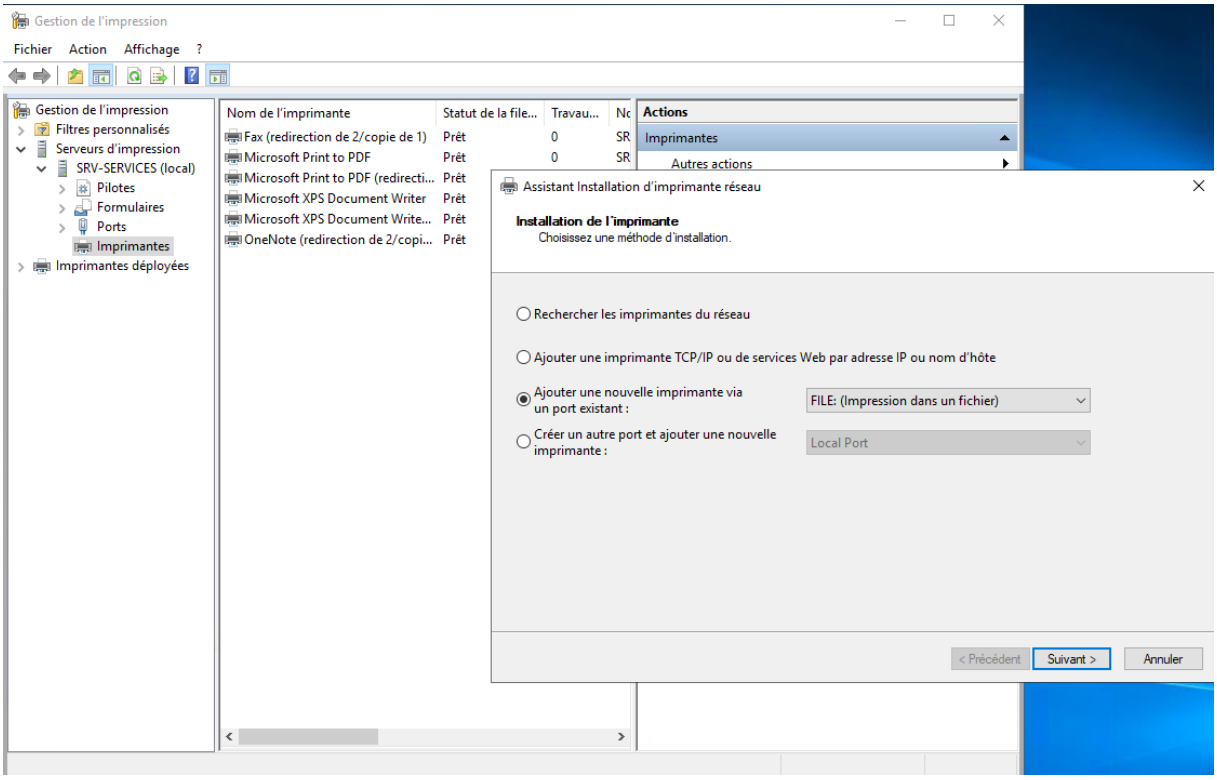

Figure 33 - Assistant Installation d'imprimante réseau.

J'appuie ensuite sur le bouton **Suivant >** pour sélectionner l'option **Installer un nouveau pilote** avant de cliquer à nouveau sur le bouton **Suivant >**.

Je peux alors sélectionner le pilote **Microsoft PCL6 Class Driver** du fabricant **Microsoft** avant de poursuivre (**Figure 34**).

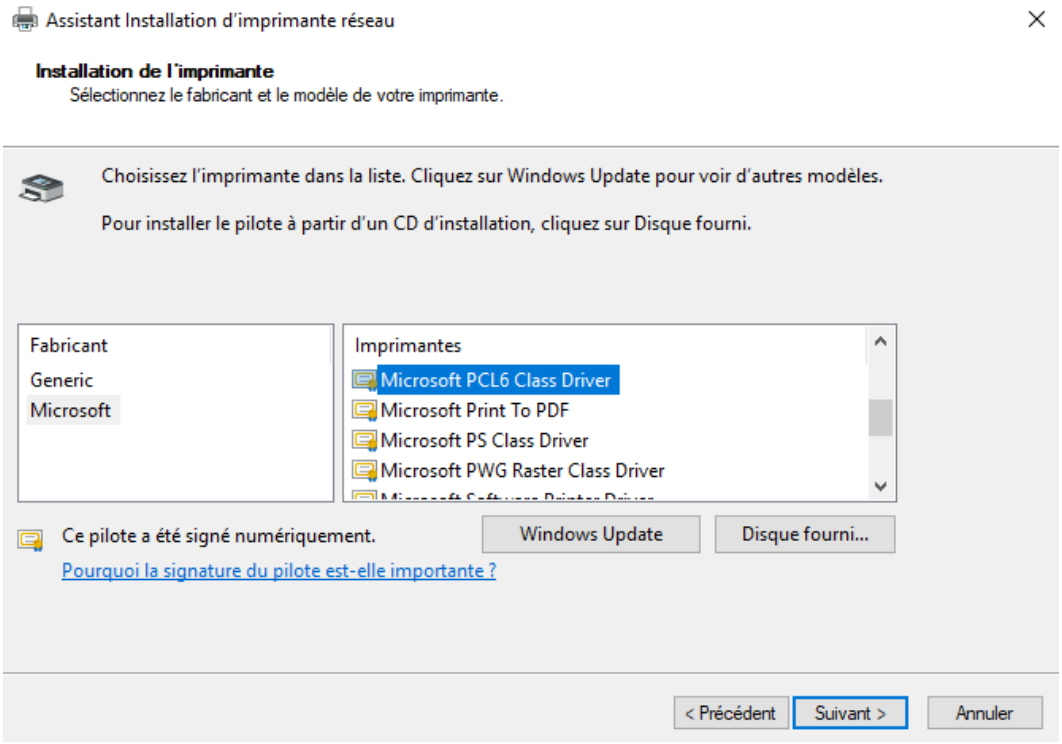

Figure 34 - Sélection du pilote de l'imprimante.

Enfin, la page suivante me permet de nommer l'imprimante **Imprimante open space** dans le champ **Nom de l'imprimante** et de partager celle-ci (**Figure 35**). Le champ **Nom du partage** est complété par les mêmes informations.

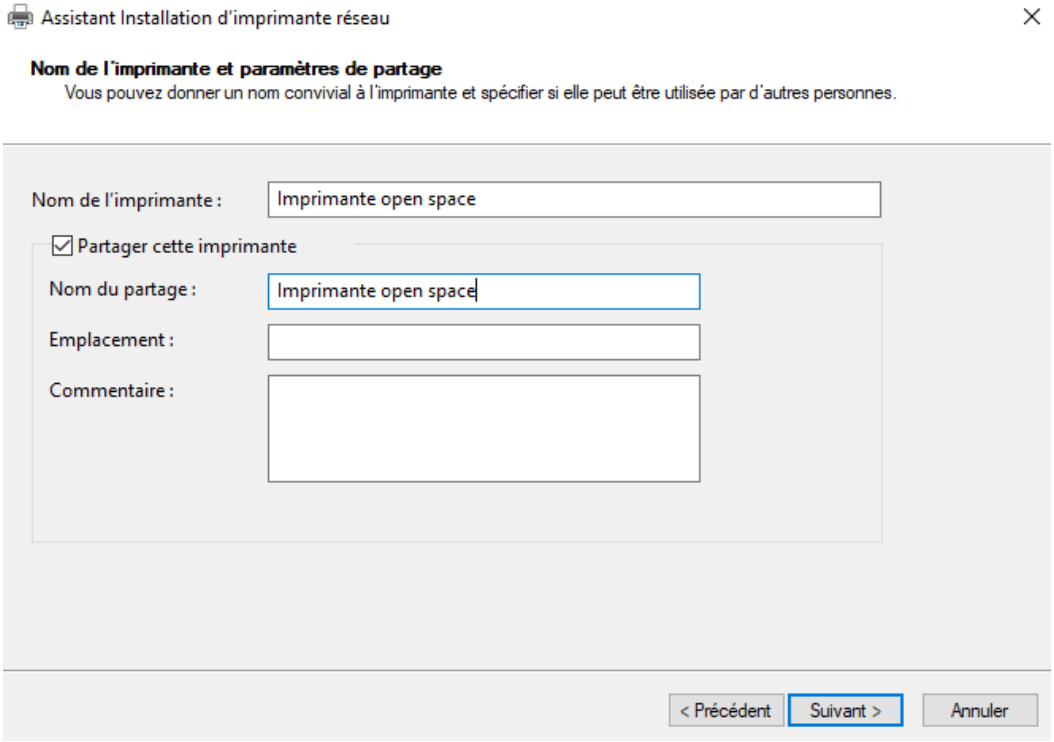

Figure 35 - Nommage de l'imprimante et partage.

Après avoir validé, j'accède à la fin de l'installation qui me propose d'ajouter une nouvelle imprimante. J'ajoute alors une imprimante nommée **Imprimante direction** en utilisant les mêmes paramètres.

De retour sur l'application **Gestion de l'Impression**, j'effectue un clic droit sur les deux imprimantes créées pour sélectionner **Répertorier dans l'annuaire**.

A l'aide de l'ordinateur technicien informatique, j'accède au serveur d'impression en entrant **\\SRV-SERVICES** dans l'explorateur de fichier. Connecté en session locale, j'entre les informations d'identification de la directrice, Marine Delpech, pour simuler sa connexion au serveur d'impression (**Figure 36**).

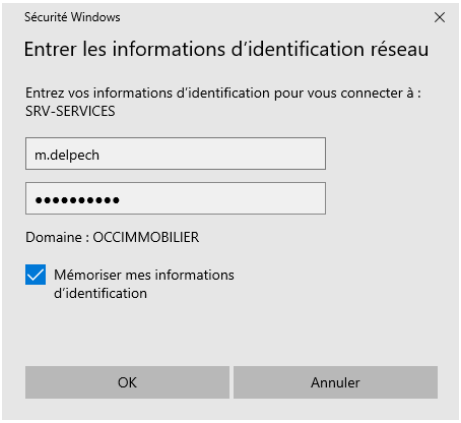

Figure 36 - Connexion au serveur d'impression avec les identifiants de l'utilisateur.

Je vois alors les imprimantes apparaitre à l'écran. Il suffit de cliquer sur l'une d'entre-elles pour l'installer sur l'ordinateur (**Figure 37**).

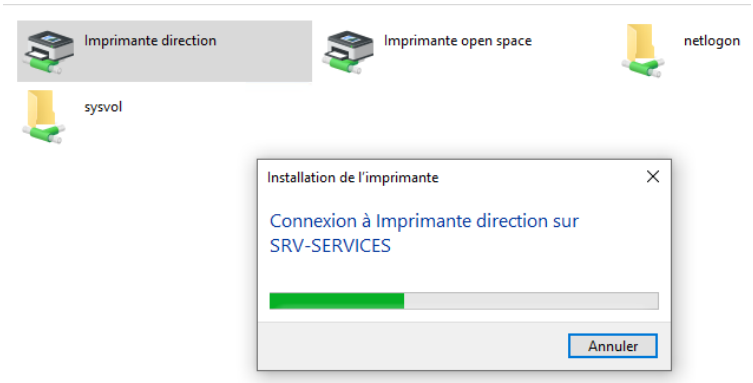

Figure 37 - Installation de l'imprimante sur l'ordinateur.

Une rapide vérification dans les **Paramètres**, **Périphériques**, **Imprimantes et scanners** permet également de vérifier la bonne installation des imprimantes (**Figure 38**).

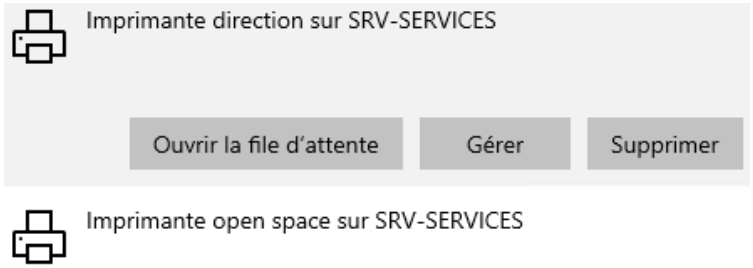

Figure 38 - Vérification de l'installation des imprimantes.

PARTIE V – MISE EN PLACE D'UNE SOLUTION VPN

1) INSTALLATION ET CONFIGURATION DU SERVEUR VPN

En ces temps de pandémie, les salariés du groupe immobilier sont invités à télétravailler lorsque leurs missions ne leur imposent pas de visites de biens. Pour accéder aux ressources de l'entreprise à distance, il faut donc mettre en place une connexion VPN entre les domiciles des salariés et l'infrastructure de l'agence.

pfSense intègre nativement la solution OpenVPN (Autrement téléchargeable séparément) qui permet la création d'un VPN-SSL. SSL est un protocole de sécurité permettant la sécurisation des échanges entre appareils distants.

La première étape d'une telle mise en place consiste en la création d'une autorité de certificat. A l'aide de l'ordinateur technicien informatique, j'accède à l'interface web du pfSense avant de sélectionner le menu **System** puis **Certificate Manager**. J'entre le nom **CA-OCCIMMOBILIER-VPN** dans le champ **Descriptive name** et je sélectionne **Create an internal Certificate Authority** dans la liste déroulante du champ **Method**. Enfin j'entre **occimmobilier** dans le champ **Common Name** avant de cliquer sur le bouton **Save** au bas de la page (**Figure 39**).

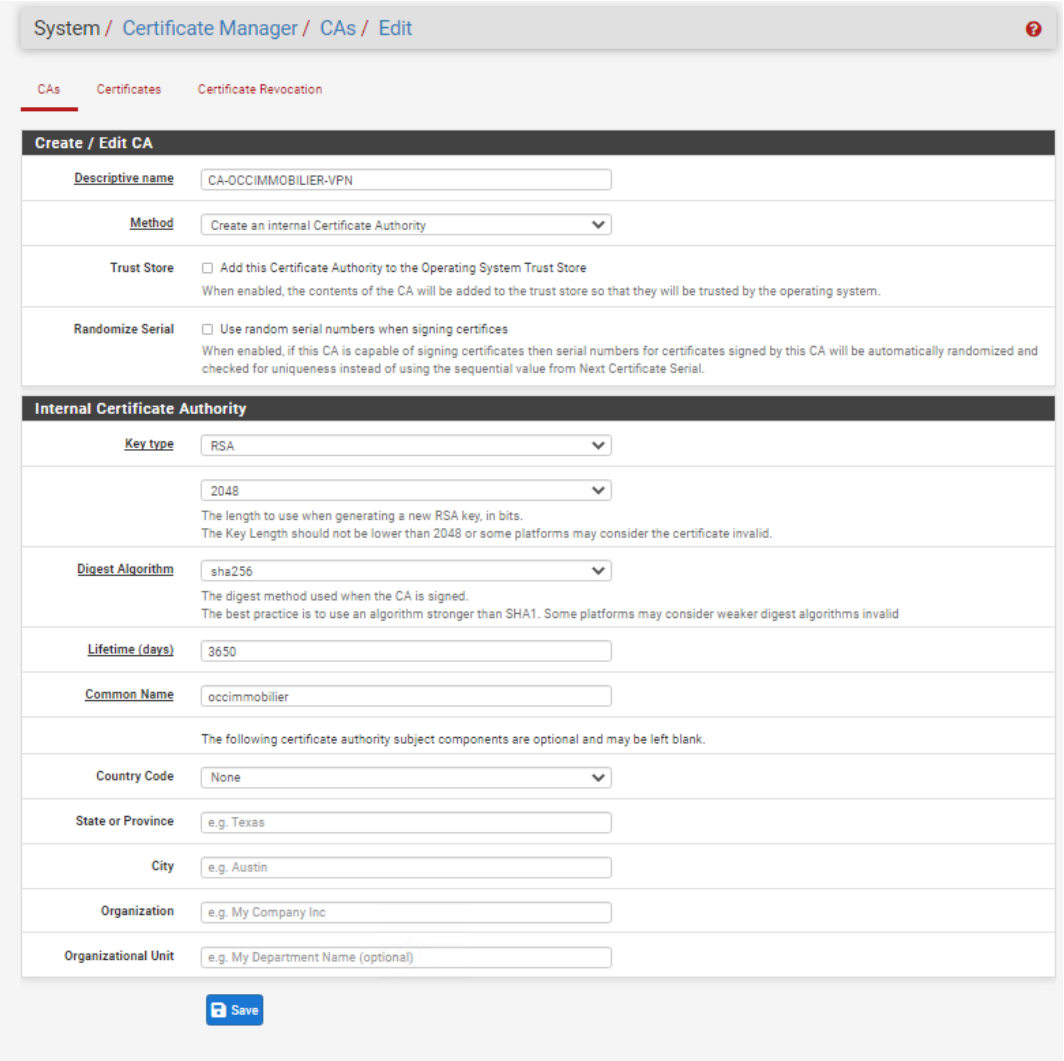

Figure 39 - Création d'une autorité de certificat.

En cliquant sur l'onglet **Certificates** situé sur le côté droit de **CAs**, je peux créer un nouveau certificat pour mon serveur VPN (**Figure 40**). J'entre les paramètres reportés dans le tableau ci-dessous tout en laissant les autres paramètres par défaut.

CHAMP	PARAMÈTRE
Method	Create an internal Certificate
VPN-SSL-ACCES-DISTANCE	VPN-SSL-ACCES-DISTANCE
Certificate Authority	CA-OCCIMMOBILIER-VPN
Common Name	vpn.occimmobilier.lan
Certificate Type	Server Certificate

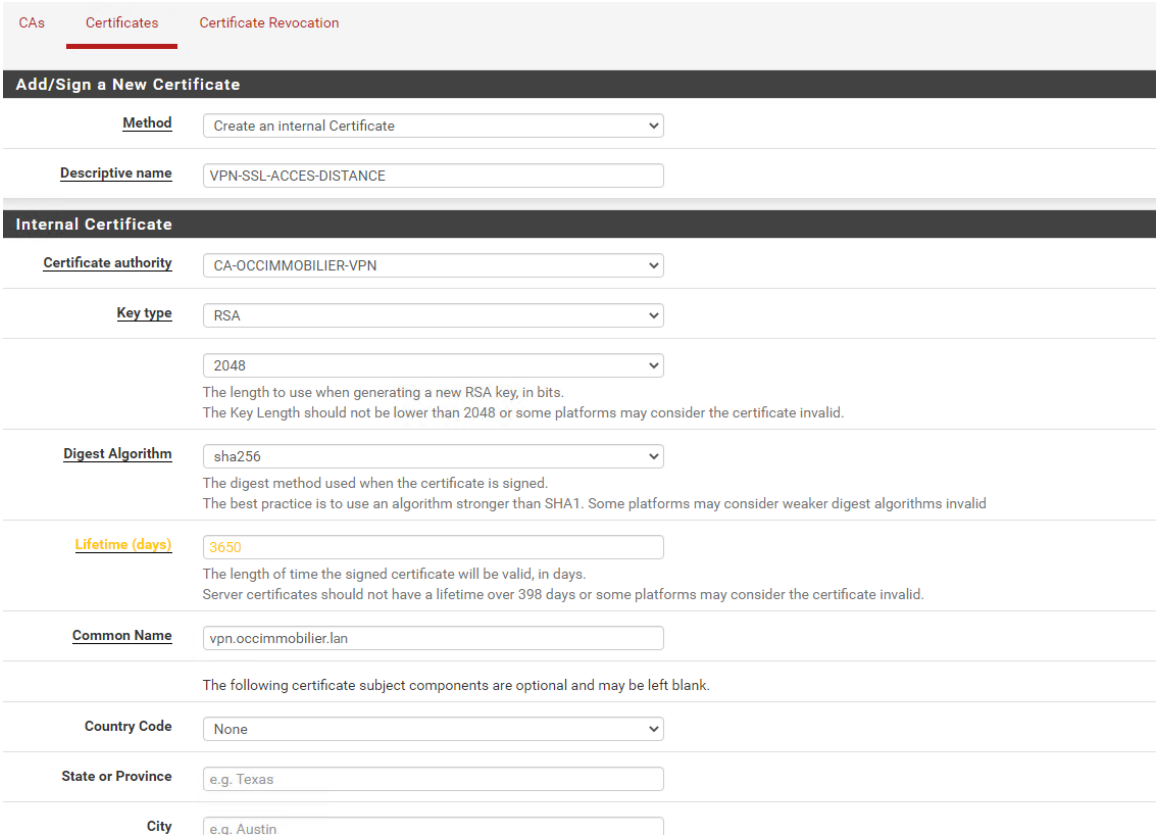

Figure 40 - Création d'un certificat serveur.

Il est très important de bien sélectionner **Server Certificate** dans le champ **Certificate Type** avant de cliquer sur le bouton **Save**, au bas de la page (**Figure 41**).

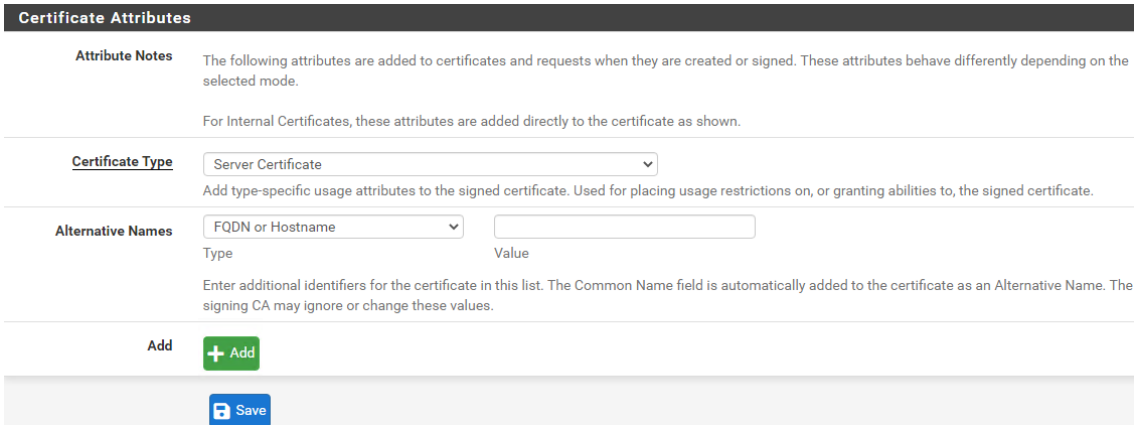

Figure 41 - Sélection du type de certificat.

J'entreprends maintenant de créer des utilisateurs dans le pfSense qui pourront, à l'aide de leurs identifiants, se connecter au client VPN. Dans le menu **System** puis **User Manager**, je crée un utilisateur pour la directrice, Marine Delpech et je spécifie les mêmes informations de connexion que dans l'Active Directory (**Figure 42**).

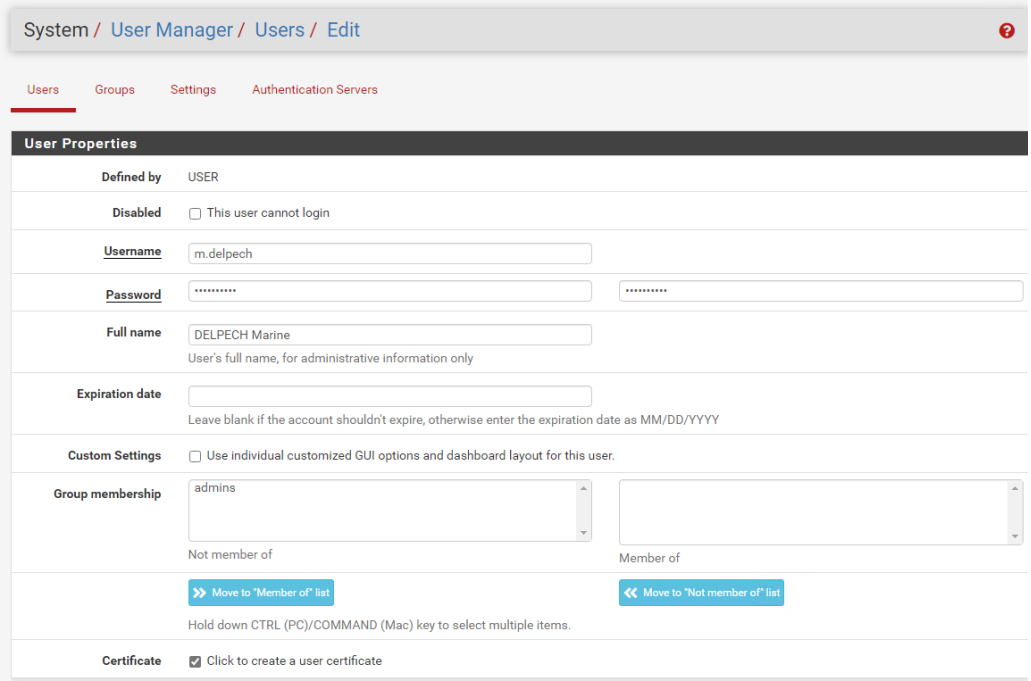

Figure 42 - Création de l'utilisateur m.delpech.

Je sélectionne également l'option **Click to create a user certificate** ce qui a pour effet d'ouvrir une nouvelle liste de champs à paramétrer. J'entre **VPN-SSL-DELPECH** dans le champ **Descriptive name** et je sélectionne **CA-OCCIMMOBILIER-VPN** dans le champ **Certificate authority** avant de valider en cliquant sur le bouton **Save**, au bas de la page (**Figure 43**).

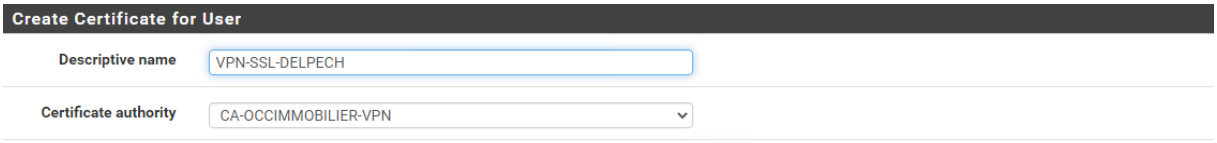

Figure 43 - Création d'un certificat pour l'utilisateur.

J'ajoute également des comptes pour l'ensemble des salariés de l'agence en utilisant la méthode précédente (**Figure 44**).

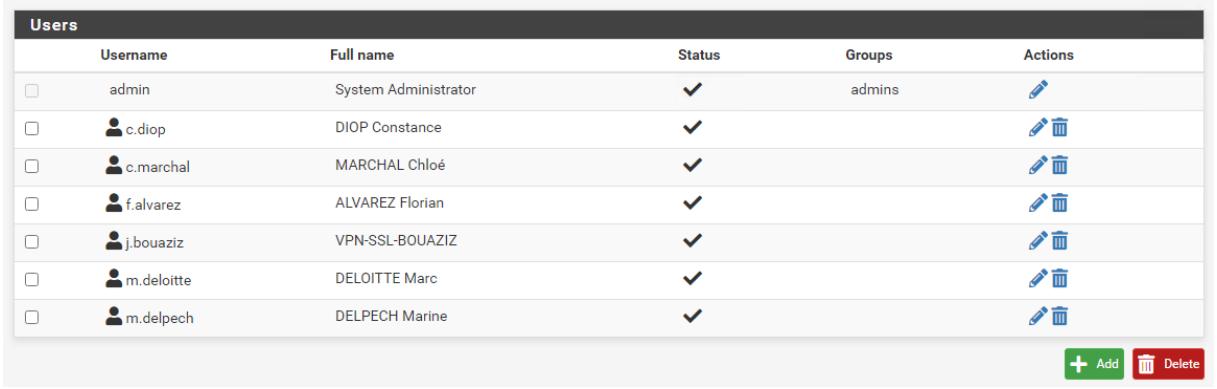

Figure 44 - Comptes pfSense des salariés pour la connexion au client VPN.

Je me rends maintenant dans le menu **VPN** puis **OpenVPN**. Sous l'onglet **Servers** je configure les options du serveur (**Figure 45**) en utilisant les paramètres reportés dans le tableau suivant. Les autres paramètres sont laissés par défaut.

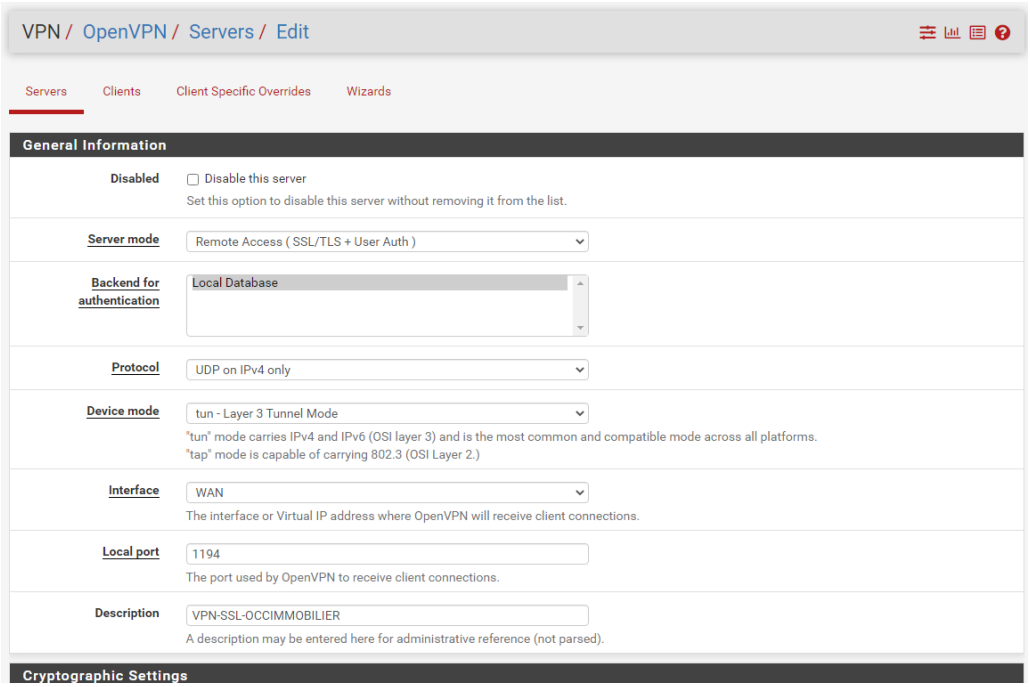

Figure 45 - Menu de configuration du serveur VPN.

CHAMP	PARAMÈTRE
Server mode	Remote Access (SSL/TLS + User Auth)
Protocol	UDP on IPv4 only
Device mode	Tun – Layer 3 Tunnel Mode
Interface	WAN
Local port	1194
Description	VPN-SSL-OCCIMMOBILIER
Peer Certificate Authority	CA-OCCIMMOBILIER-VPN
Server certificate	VPN-SSL-ACCES-DISTANCE
IPv4 Tunnel Network	10.10.10.0/24
IPv4 Local network(s)	192.168.1.0/28
Concurrent connections	6
Topology	net30 – Isolated /30 network per client
DNS Default Domain	Provide a default domain name to clients
DNS Default Domain	occimmobilier.lan
DNS Server enable	Provide a DNS server list to clients
DNS Server 1	192.168.1.2
DNS Server 2	8.8.8.8
Custome options	Ajouter auth-nocache

IPv4 Tunnel Network peut être n'importe quelle adresse privée n'étant pas dans le réseau de destination (le masque doit admettre au moins autant d'hôtes que de connexions souhaitées). **IPv4 Local network(s)** doit être complété par l'adresse du réseau de destination (le réseau privé de l'agence). La topologie **net30** permet d'isoler chaque client dans un sous-réseau différent pour éviter les communications non désirées. Le paramètre **auth-nocache** permet quant à lui de refuser la mise en cache.

Je souhaite maintenant générer des fichiers de configuration nécessaires au paramétrage des clients VPN. Chaque utilisateur dispose d'un fichier de configuration différent qui doit être exporté depuis le pfSense puis importé dans le client OpenVPN.

Dans le menu **System** puis **Package Manager**, je sélectionne l'onglet **Available Packages** et j'entre le terme **openvpn** dans la barre de recherche. Je choisis alors **openvpn-client-export** que j'installe en sélectionnant le bouton **Install** (Figure 46).

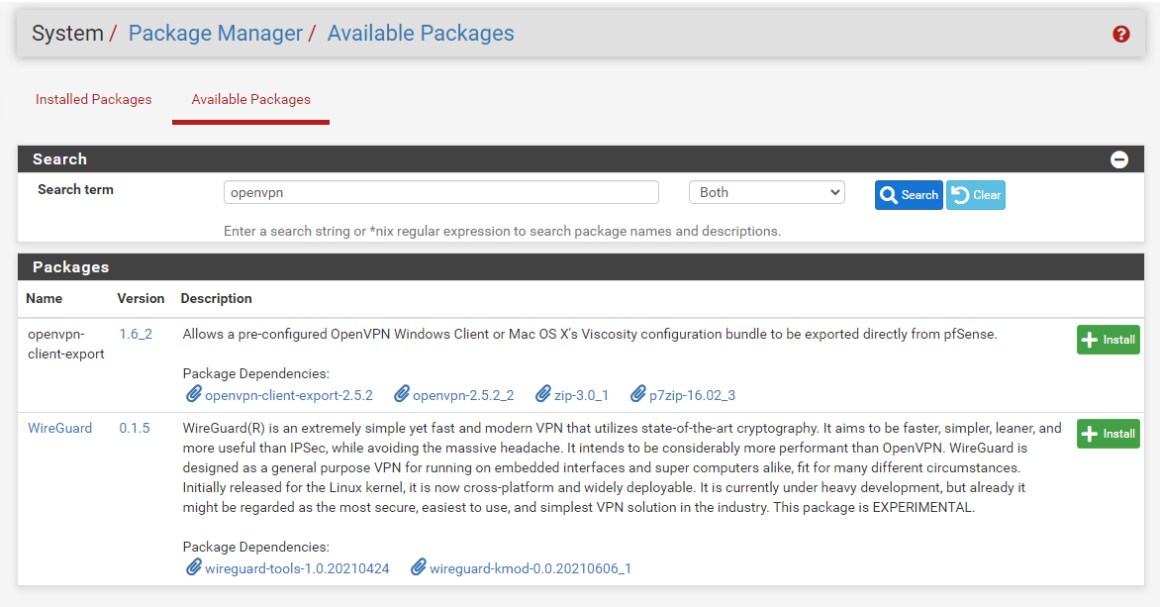

Figure 46 - Installation de la fonctionnalité permettant l'export des configurations clients.

Une fois installé, je peux me rendre dans le menu **VPN** puis **OpenVPN** pour accéder à l'onglet **Client Export Utility**. Je sélectionne alors **VPN-SSL-OCCIMMOBILIER UDP4:1194** dans le champ **Remote Access Server** et je reporte le paramètre **auth-nocache** dans le champ **Additional configuration options** avant de valider en cliquant sur le bouton **Save as default** (Figure 47).

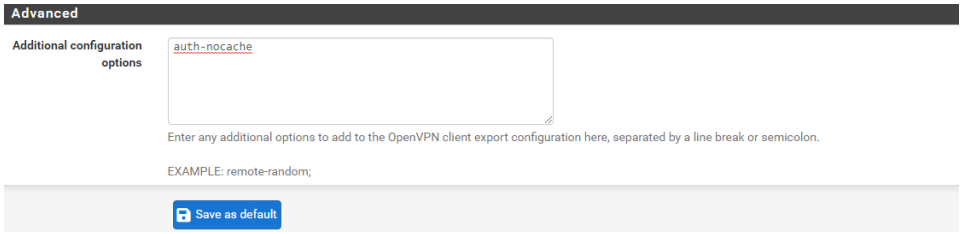

Figure 47 - Report du paramètre auth-nocache.

S'affichent alors une liste de liens de téléchargement au bas de la page qui permettent le téléchargement et l'export des fichiers de configuration de chaque utilisateur. Je sélectionne alors la version **Archive** en **Bundled Configurations** pour l'utilisateur **m.delpech** (Figure 48).

Figure 48 - Téléchargement du fichier de configuration utilisateur.

La page précédente permet également le téléchargement du fichier d'installation du **client OpenVPN**.

Je me rends désormais dans le menu **Firewall** puis **Rules**. L'idée est ici de créer deux règles qui permettront la communication et le passage des paquets par le pare-feu, entre le domicile du salarié et les ressources de l'agence. Dans l'onglet **WAN**, je créé une règle permettant d'autoriser le traffic en UDP vers les adresses WAN. J'utilise les paramètres listés dans le tableau ci-dessous et je laisse les autres options par défaut.

CHAMP	PARAMÈTRE
Address Family	IPv4
Protocol	UDP
Destination	WAN address
Destination Port Range	From OpenVPN (1194) to OpenVPN(1194)
Log	Log packets that are handled by this rule

Je valide alors en sélectionnant le bouton Save (**Figure 49**).

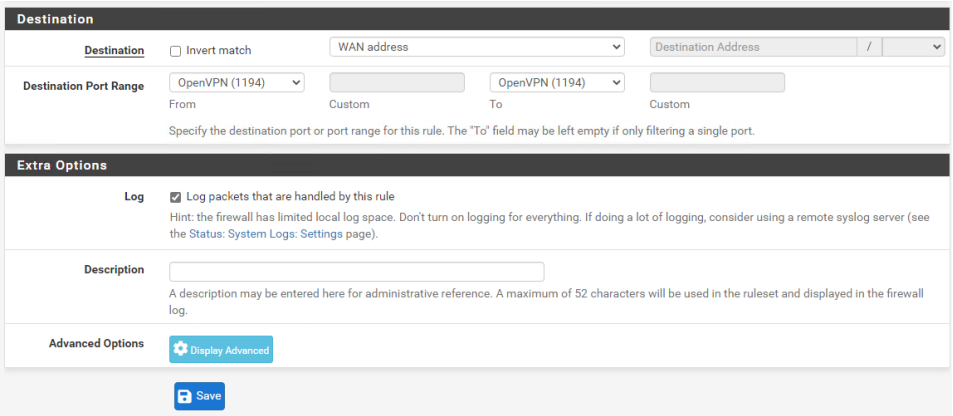

Figure 49 - Paramétrage d'une règle WAN pour le pare-feu.

Je créé ensuite une règle pour l'interface **OpenVPN**. J'utilise les paramètres décrits dans le tableau suivant en laissant les autres options par défaut.

CHAMP	PARAMÈTRE
Address Family	IPv4
Protocol	Any
Log	Log packets that are handled by this rule

Les réglages sont ici très permissifs car cette règle a pour but d'autoriser l'accès aux ressources une fois la connexion effectuée. Des restrictions pourraient évidemment être appliquée en étudiant précisément les besoins d'accès aux ressources des utilisateurs.

Je valide en cliquant sur le bouton **Save**.

2) INSTALLATION DU CLIENT OPENVPN

Afin de simuler une connexion distante, je choisis d'utiliser mon ordinateur physique pour tester la validité de la connexion VPN (Celui-ci est en effet hors du réseau LAN de l'agence). J'installe le client après transfert vers cette machine du fichier d'installation et de l'archive contenant les fichiers de configuration. Ces fichiers doivent être extraits dans le dossier **C:\Programmes\OpenVPN\Config**. J'exécute le fichier d'installation du client (**Figure 50**).

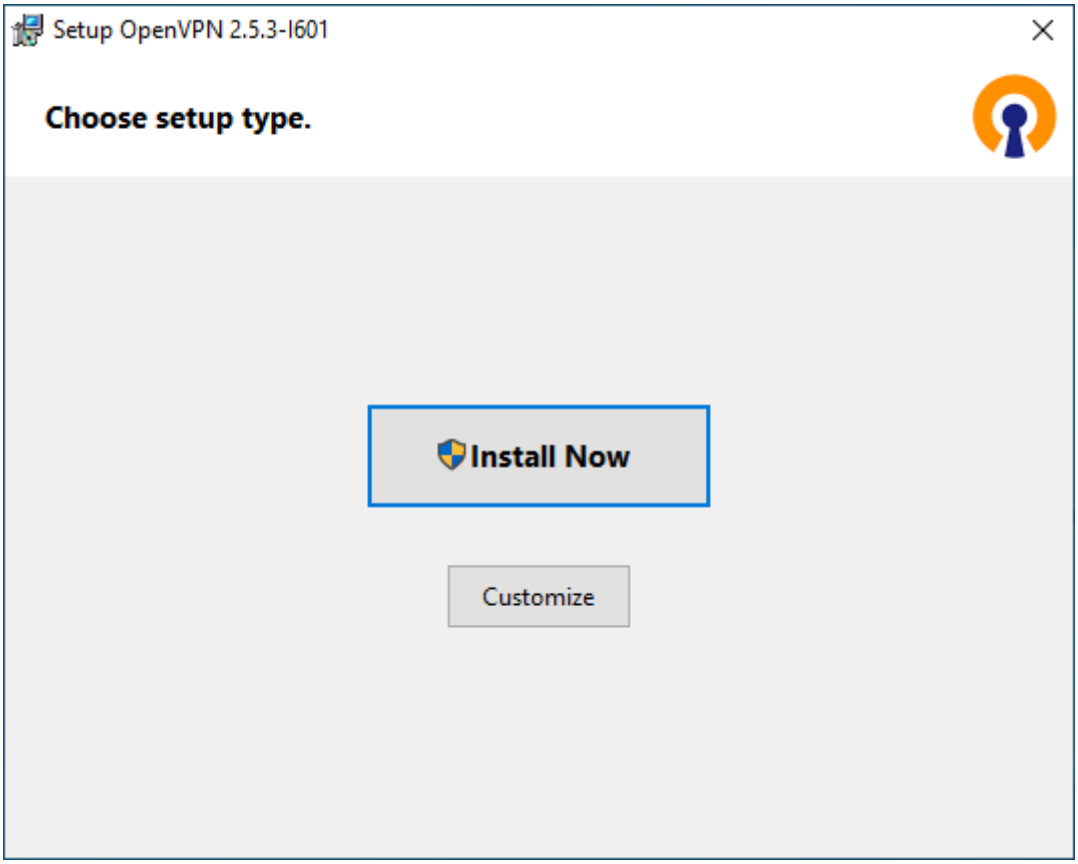

Figure 50 - Programme d'installation du client OpenVPN.

L'appui sur le bouton **Install Now** lance l'installation du programme qui se termine par l'apparition d'une fenêtre nécessitant de cliquer sur le bouton **Close**.

Je lance enfin le client et celui-ci m'avertit alors qu'aucun profil de connexion n'a été détecté (**Figure 51**). Il faut donc importer la configuration.

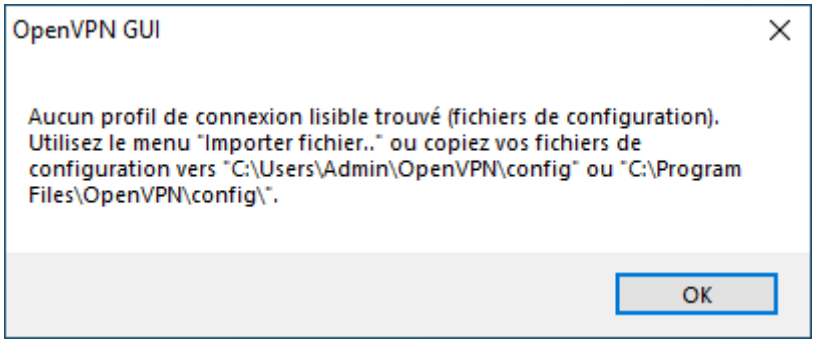

Figure 51 - Avertissement profil de connexion manquant.

Dans la barre des tâches, je sélectionne la petite flèche vers le haut situé à côté de l'icône réseau et je constate l'apparition d'un logo correspondant au **client OpenVPN**. Un clic droit sur ce logo me permet de choisir l'option **Importer fichier…** pour aller chercher ma configuration dans le dossier **Config** (Figure 52).

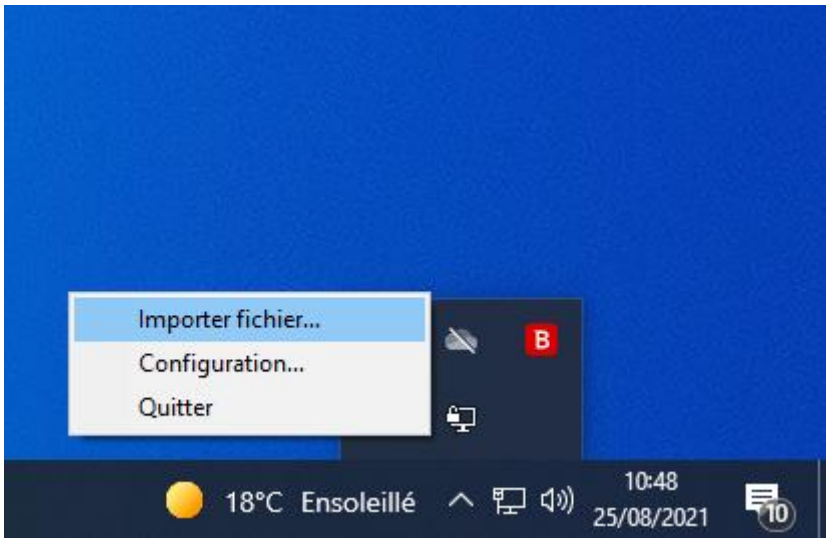

Figure 52 - Importation du fichier de configuration.

Un nouveau clic droit sur l'icône me permet maintenant de sélectionner l'option **Connecter**. La sélection de ce paramètre ouvre une fenêtre de connexion me demandant les informations de connexion nécessaires à l'authentification. J'entre alors les identifiants de l'utilisateur **m.delpech** (Figure 53).

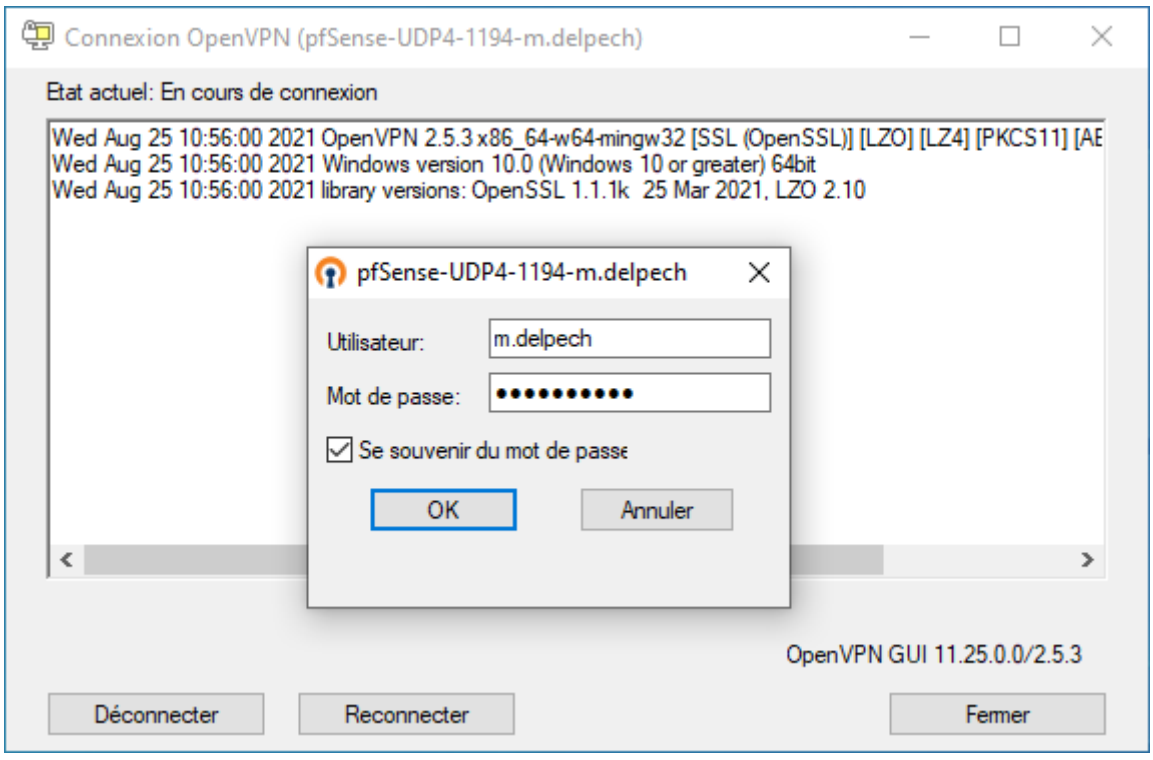

Figure 53 - Connexion au client OpenVPN.

Une alerte de sécurité Windows apparait alors pour demander l'autorisation de l'accès à l'application OpenVPN. Après avoir coché les cases **Réseaux privés** et **Réseaux publics**, je clique sur le bouton **Autoriser l'accès** (Figure 54).

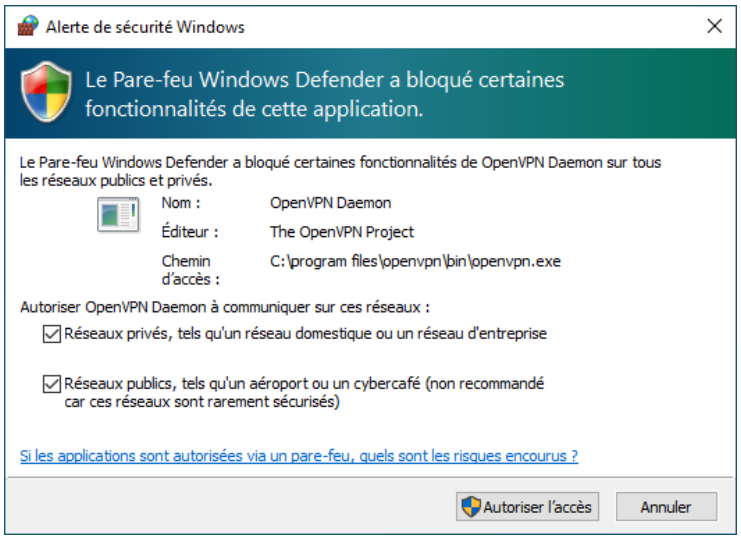

Figure 54 - Alerte de sécurité Windows.

La connexion au pfSense, puis au réseau de l'agence s'effectue alors comme l'indique la fenêtre du client OpenVPN (Figure 55).

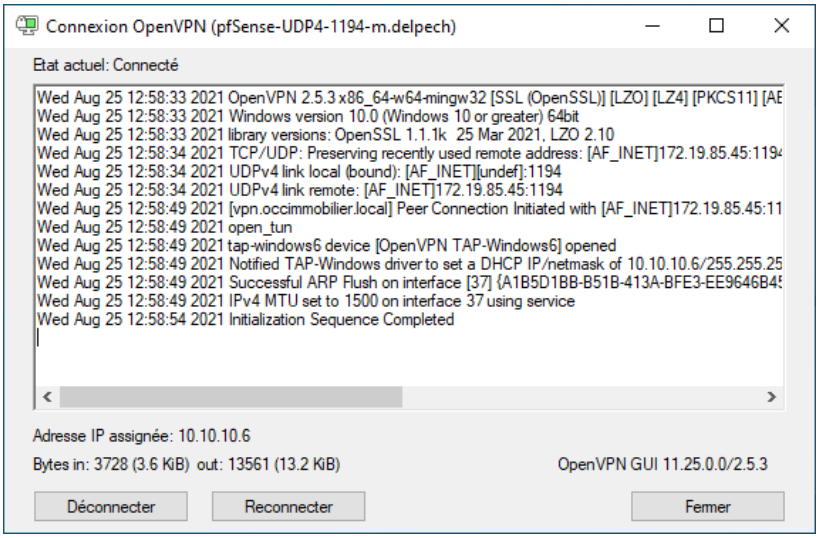

Figure 55 - Connexion du client au serveur VPN.

Afin de pousser la vérification du fonctionnement, j'ouvre l'**invite de commandes** et entre la commande **ipconfig /all** pour constater l'attribution d'une adresse IPv4 dans la plage d'adresses définie pour le tunnel VPN (**Figure 56**).

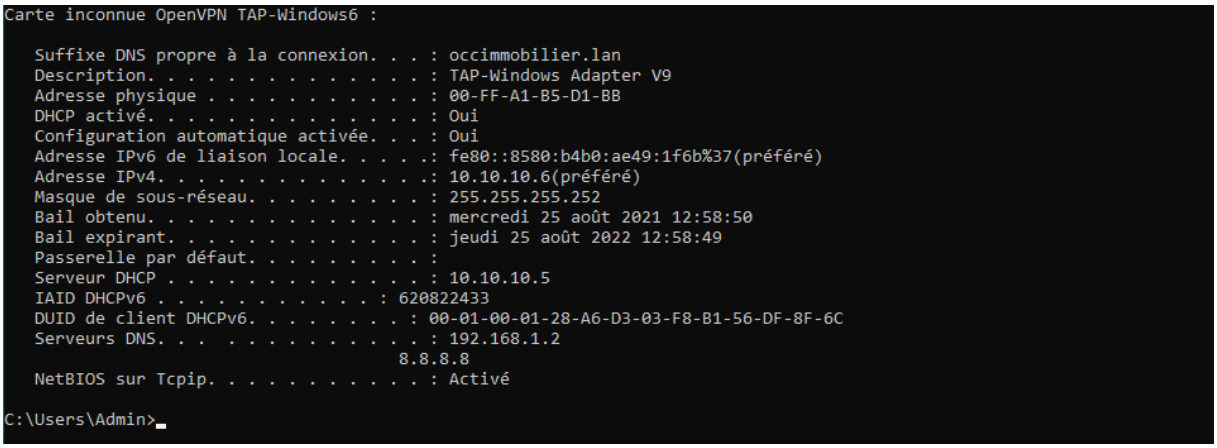

Figure 56 - Vérification de l'attribution d'une adresse valide.

Enfin, je tente d'envoyer un **ping** vers l'ordinateur technicien informatique. Celui-ci parvient à la machine et me montre le bon fonctionnement de ma connexion VPN (**Figure 57**).

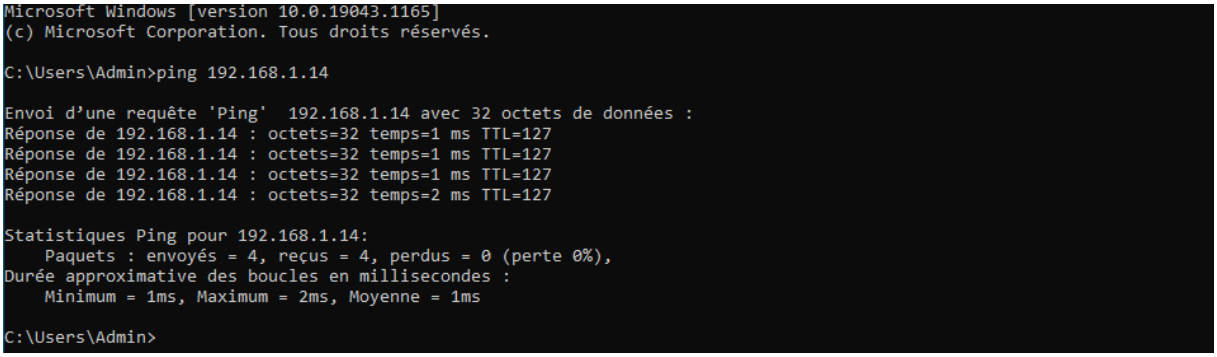

Figure 57 - Test de connectivité entre les machines.

CONCLUSION

1) PISTES D'AMÉLIORATION

J'ai eu de nombreuses idées relatives à ce que je souhaitais mettre en œuvre dans le cadre de la réalisation de ce projet. Réalisant l'ampleur du travail à fournir pour mettre en place une telle infrastructure, j'ai simplifié certaines étapes de l'installation des équipements par manque de temps, de matériel ou de finances. Ces failles dans la conception de cette infrastructure pourraient bénéficier d'un travail de recherche d'améliorations et de solutions pouvant permettre de contourner ces contraintes. Je prends ainsi la liberté dans ce paragraphe de vous lister certaines pistes d'amélioration sur lesquelles je pourrais travailler pour concevoir une infrastructure plus optimisée, et plus sécurisée :

- Création d'un raid sur le pfSense pour plus de sécurité dans la gestion des disques ;
- Création d'une sauvegarde régulière de la configuration du pfSense ;
- Création de règles plus poussées et plus strictes concernant le trafic du pfSense (notamment en ce qui concerne l'usage des ressources en connexion VPN) ;
- Mise en place d'une liaison LDAP entre le pfSense et l'Active Directory pour éviter les doublons de créations de comptes utilisateurs ;
- Séparation du réseau de l'agence en sous-réseaux différenciants les équipements de l'infrastructure des postes des salariés ;
- Utilisation d'une imprimante réseau physique et test d'impression.

D'autres idées sont bien évidemment à étudier et feront l'objet d'une analyse plus poussée de ma part dans les prochaines semaines.

2) EXPÉRIENCE PERSONNELLE

Ce troisième PPE est un projet m'ayant passionné tant il couvrait divers aspects de la mise en œuvre d'une infrastructure réseau. Ce fut également un exercice très chronophage m'ayant poussé à améliorer mes capacités en termes de gestion du temps. Bien que n'ayant pas utilisé d'outil de planification comme c'était originellement prévu, j'ai utilisé des compétences de gestion de projet acquise lors de mes cours et en entreprise pour réaliser ce travail.

Celui-ci m'a également permis d'en apprendre plus sur le fonctionnement d'un pare-feu et d'une connexion VPN, me forçant parfois à étudier des documentations techniques pour comprendre l'utilité et l'effet de mes actions. J'espère avoir, lors de la réalisation de mon quatrième PPE, l'opportunité de mettre en œuvre ces compétences et de pouvoir en développer de nouvelles.

Je vous remercie pour l'attention que vous avez porté à ce rapport.