République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira de Bejaia
Faculté des Sciences Exactes
Département Informatique

Mémoire de fin d'études

En vue de l'obtention du diplôme de Master professionnel en Informatique

Option : Administration et Sécurité des Réseaux

Thème

Virtualisation sécurisée et consolidation multi-sites via VPN sous PfSense
Cas : SPC GB -Groupe TOUDJA

Présenté par :

M^elle^ AIT DAHMANE Kamelia

M^elle^ ALLALI Lidia

Soutenu le 02 juillet 2024 devant les jurys composés de :

Président	M^me^ HOUHA Amel	MAA	U. A / Mira Béjaia
Examinateur	M^me^ BOUADEM Nassima	MCB	U. A / Mira Béjaia
Encadrant	M^me^ SAAD Narimane	MCB	U. A / Mira Béjaia
Co-encadrant	M^r^ BOURIHANE Mouloud	Ingénieur	Entreprise Toudja

Année universitaire : 2023/2024

Remerciements

***N**ous exprimons notre gratitude envers Dieu, notre créateur, pour nous avoir donné la force et le courage de tenir jusqu'à la fin de ce travail.*

***E**t nous adressons également nos vifs remerciements et notre sincère gratitude*

À :

***N**os familles, en particulier nos parents, ont été à nos côtés, nous ont apporté leur soutien et ont accompagné notre projet tout au long du chemin.*

***N**otre promotrice, Madame SAAD Narimane, pour nous avoir encadrés. Ses conseils éclairés, ses orientations précieuses et sa disponibilité tout au long de ce travail ont grandement contribué à sa réussite.*

***N**ous tenons à remercier également notre encadrant de stage Monsieur BOURIHANE Mouloud, qui nous a formé et accompagné tout au long de cette expérience professionnelle avec beaucoup de patience et de pédagogie. Ainsi nous remercions tout le personnel de Groupe Toudja pour leur orientation et accueil sympathique durant la période de stage.*

***N**ous tenons également à remercier les membres de jury qui nous font honneur en acceptant d'évaluer notre travail.*

***E**nfin, nous remercions tous ceux qui ont contribué de près ou de loin à la réalisation de notre projet.*

Dédicace

Je dédie ce modeste travail . . .

À mes chers parents, mes éternels supporters et mes confidents dans cette vie, auxquels je dois ma réussite et auxquels je ne rendrai jamais assez. Je vous remercie pour tout le soutien et l'amour que vous m'avez porté depuis mon enfance, et j'espère sincèrement que votre bénédiction m'accompagne toujours. Que Dieu, le Tout-Puissant, vous accorde santé, bonheur et longue vie, et que je puisse toujours vous rendre fier sans jamais vous décevoir.

À mes chers frères Massilas et Amine, pour leurs encouragements permanents et leur soutien indéfectible, et à qui je souhaite tout le meilleur dans ce monde.

À mon binôme et amie Lidia avec qui j'ai réalisé ce travail.

À mes amies pour leur soutien tout au long de mon parcours universitaire.

À toutes personnes que j'apprécie et que je n'ai pas cité.

Kamelia

Dédicace

Avec l'aide de Dieu tout puissant, qui trace le chemin de ma vie, j'ai pu arriver à réaliser ce petit travail que je dédie à :

Mes chers parents, pour lesquels aucune dédicace ne peut exprimer mes sentiments, pour leur patience sans limites, leurs encouragements continus, leur aide, en témoignage de mon profond amour et respect pour leurs grands sacrifices, j'espère qu'un jour j'aurai l'opportunité de vous rendre un peu de ce que vous avez fait pour moi. Que Dieu vous accorde le bonheur et une longue vie.

À chers frères et sœurs « Roumaissa, Mouna, Adam », vous êtes mes piliers, mes confidents et mes sources d'inspiration. Votre soutien indéfectible, vos encouragements sans faille et votre présence bienveillante ont joué un rôle essentiel dans mon cheminement. Ce dédicace est un témoignage de ma gratitude envers chacun de vous.

À mon amie kamelia avant d'être binôme. Je te remercie du fond du Cœur pour cette expérience.

À toutes nos familles sans exception, tous nos chers amis(e) pour leurs encouragements, et tous ceux qu'on aime.

Lidia

TABLE DES MATIÈRES

TABLE DES FIGURES

LISTE DES TABLEAUX

LISTE DES ACRONYMES

AD	**A**ctive **D**irectory
AD DS	**A**ctive **D**irectory **D**omain **S**ervices
AES	**A**dvanced **E**ncryption **S**tandard
CA	**C**ertificat **A**utorité
CN	**C**ommon **N**ame
DHCP	**D**ynamic **H**ost **C**onfiguration **P**rotocol
DNS	**D**omain **N**ame **S**ystem
ESXI	**E**lastic **S**ky **X** **I**ntegrated
GPO	**G**roup **P**olicy **O**bject
HTTP	**H**ypertext **T**ransfer **P**rotocol
IBM	**I**nternational **B**usiness **M**achines **C**orporation
ICMP	**I**nternet **C**ontrol **M**essage **P**rotocol
IP	**I**nternet **P**rotocol
ISO	**I**nternational **O**rganization for **S**tandardization
LAN	Un réseau local, en anglais **L**ocal **A**rea **N**etwork
LDAP	**L**ightweight **D**irectory **A**ccess **P**rotocol
NAS	**N**etwork **A**ttached **S**torage
NetBIOS	**N**etwork **B**asic **I**nput/**O**utput **S**ystem
OSI	**O**pen **S**ystems **I**nterconnection
OS	Système d'exploitation, en anglais **O**perating **S**ysteme
SE	**S**ystème d'**E**xploitation
SSH	**S**ecure **S**hell
SSL	**S**ecure **S**ocket **L**ayer
TCP	**T**ransmission **C**ontrol **P**rotocol
TLS	**T**ransport **L**ayer **S**ecurity
UDP	**U**ser **D**atagram **P**rotocol
VLAN	**V**irtual **L**ocal **A**rea **N**etwork
VM	**V**irtual **M**achine
VPN	**V**irtual **P**rivate **N**etwork

vSwitch **V**irtual **S**witch

WAN **W**ide **A**rea **N**etwork, ou réseau étendu

WINS **W**indows **I**nternet **N**ame **S**ervice

INTRODUCTION GÉNÉRALE

Dans un monde marqué par une nécessité accrue de sécurité des données et d'efficacité opérationnelle, les entreprises se tournent vers des solutions technologiques avancées pour rester compétitives. Parmi ces solutions, la virtualisation, PfSense et les VPN (Virtual Private Network) se distinguent comme un ensemble de technologies essentielles. Ensemble, ils forment un trio puissant qui non seulement optimise les infrastructures informatiques par une utilisation maximale des ressources, mais offre également une sécurité renforcée pour les communications d'entreprise.

La virtualisation se révèle être une solution d'entreprise de plus en plus incontournable, offrant une multitude de réponses aux défis actuels. Elle permet une réduction significative du nombre de serveurs physiques, favorisant ainsi une augmentation des serveurs virtuels par serveur physique. Cette stratégie d'optimisation des ressources conduit à une diminution notable des coûts matériels et de la consommation énergétique.

Cependant, l'internet est considéré comme un canal de communication principal entre les sites d'une entreprise ou entre différentes entreprises, la sécurité des données échangées sur ce réseau public est devenue extrêmement importante. L'utilisation d'Internet pour le transfert d'informations sensibles expose les entreprises à un risque accru de cyberattaques. Face à cette menace, l'adoption de solutions de sécurité réseau robustes et adaptables est indisponsable. PfSense, avec sa capacité à être configuré en tant que pare-feu avancé et système VPN, répond parfaitement à ce besoin. Il offre ainsi une protection renforcée contre les intrusions malveillantes, assurant la sécurité des données d'entreprise dans un environnement de plus en plus connecté et vulnérable.

Le stage que nous avons effectué au sein de l'entreprise de Groupe Toudja, nous a permis de découvrir son réseau et de comprendre la nécessité d'une architecture réseau sécurisée. L'intérêt

de notre travail est l'intégration d'une virtualisation et une communication sécurisée entre la direction GB Bejaïa avec les autres unités (GB El Kseur, Unilait et SET Toudja). Cette communication se fera à travers un VPN installé sur PfSense.

Et pour réaliser notre projet et atteindre nos objectifs fixés, nous avons subdivisé ce travail en quatre chapitres distincts :

- Le premier chapitre « **Généralité sur la sécurité informatique** » : aborde les principes fondamentaux de la sécurité informatique et ses mécanismes.
- Le deuxième chapitre « **Introduction à la virtualisation** » : présente quelques notions de base concernant la virtualisation.
- Le troisième chapitre « **Présentation de l'organisme d'accueil** » : aura pour objectif de mieux comprendre l'organisme et sa structure hiérarchique, nous allons donc évoquer la problématique rencontrés et la solution que nous considérons la plus appropriée.
- Le quatrième chapitre « **Réalisation et tests** », nous allons mettre en pratique toutes les connaissances et solutions proposées dans les chapitres précédents en proposant une architecture de réseau de l'entreprise « Groupe Toudja », puis nous expliquerons les différentes étapes d'installation et de configuration, ainsi que la vérification des résultats.
- Enfin, nous terminerons par une conclusion générale qui résume les éléments clés abordés dans notre mémoire afin de donner un aperçu global des éléments essentiels.

CHAPITRE 1

GÉNÉRALITÉS SUR LA SÉCURITÉ INFORMATIQUE

1.1 Introduction

Avant de s'approfondir dans l'essentiel de notre projet, il est recommandé de commencer par les notions de base de la sécurité informatique, son objectif et les mécanismes de sécurité.

1.2 Définition

La sécurité informatique recouvre l'ensemble de techniques informatiques permettant de réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles.

Elle consiste à plusieurs technologies, d'architectures permettant d'atteindre un certain niveau de protection.[1]

1.3 Les objectifs de la sécurité informatique

Elle vise généralement cinq (5) principaux objectifs [2] :

- **Intégrité :** c'est-à-dire garantir que les données sont bien celles que l'on croit être.
- **Confidentialité :** consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées.
- **Disponibilité :** les services (ordinateurs, réseaux périphériques, applications...) et les informations (données, fichiers...) doivent être accessibles aux personnes autorisées quand elles en ont besoin.

- **Authentification :** concerne la vérification de l'identité d'une entité afin d'assurer son authentification, garantissant ainsi que seules les personnes autorisées aient accès aux ressources.
- **La non répudiation :** permettant de garantir qu'une transaction ne peut être niée.

1.4 Terminologies de la sécurité informatique

- **Vulnérabilité :** il s'agit d'une faille dans un système informatique, permettant à un attaquant de porter atteinte à l'intégrité de ce système.[3]
- **Risque :** c'est la probabilité qu'un problème survienne lorsqu'une vulnérabilité est exposée à une population malveillante qui tentera de l'exploiter.[3]
- **Attaque :** elle représente le moyen d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas exploitables.[3]
- **Contre-mesure :** c'est la procédure ou technique permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique.[3]
- **Menace :** c'est un adversaire déterminé capable de monter une attaque exploitant une vulnérabilité.[3]

1.5 Les mécanismes de sécurité

Les mécanismes de sécurité consistent à déployer des moyens et des dispositifs visant à sécuriser le système d'information ainsi que de faire appliquer les règles définies dans une politique de sécurité. Parmi ces mécanismes, on peut citer :

1.5.1 Pare-feu (Firewall)

1.5.1.1 Définition

C'est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (internet).

Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante [4] :

- Une interface pour le réseau à protéger (réseau interne).
- Une interface pour le réseau externe.

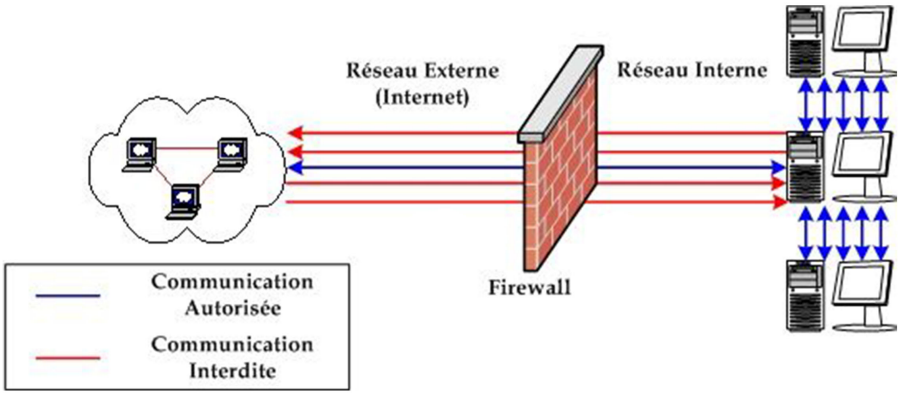

Figure 1.1 – Pare-feu.[5]

1.5.1.2 Le fonctionnement de pare-feu

Un système pare-feu contient un ensemble de règles permettant [4] :

- D'autoriser la connexion (allow).
- De bloquer la connexion (deny).
- De rejeter la demande de connexion sans avertir l'émetteur (drop).

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :

- Soit d'autoriser uniquement la communication ayant explicitement autorisées.
- Soit d'empêcher les échanges qui ont été explicitement interdites.

La première méthode est plus sure, mais elle impose toutes fois une définition précise et contraignante des besoins en communication.

1.5.1.3 Pourquoi utiliser un pare-feu ?

Les pare-feu sont utilisés principalement dans 4 buts[6] :

- **Maintenir des personnes dehors :**
  En effet ; pour se protéger des malveillances (externes), les firewalls permettent d'écarter divers intrus comme le problème de confidentialité de l'information.

- **Maintenir des personnes à l'intérieur :**
  Les pare-feux ont également pour objectif d'éviter la fuite d'information, non contrôlée vers l'extérieur.
- **Contrôler les flux :**
  Tous les flux du trafic entre le réseau interne et externe doivent être surveillés .cela permet par exemple d'avoir une vue de la consommation internet différents utilisateurs internes et de bloquer l'accès à certains sites contenant des informations illégales.Les garde-barrières effectuant un filtrage applicatif peuvent effectuer des vérifications sur les e-mails reçus.
- **Faciliter l'administration du réseau :**
  Sans firewall chaque machine du réseau est potentiellement exposée aux attaques d'autres machines d'internet. Les firewalls simplifient la gestion de la sécurité et donc l'administration du réseau car ils centralisent les attaques potentielles au niveau du firewall plutôt que sur le réseau tout entier.

1.5.2 VPN

1.5.2.1 Définition

Un réseau privé virtuel (VPN) désigne un service qui offre la possibilité d'établir une connexion sécurisée et chiffrée entre votre appareil (comme un ordinateur, un smartphone ou une tablette) et un serveur à distance.[7]

- Ce réseau est dit **virtuel** car il relie deux réseaux « physiques » (réseaux locaux) par une liaison non fiable (Internet), et **privé** car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent voir les données.[8]

1.5.2.2 Fonctionnement de VPN

Le VPN se base sur un protocole de tunneling, qui consiste à chiffrer les données à l'aide d'un algorithme cryptographique entre les deux réseaux. Le principe du tunneling est de créer un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel.[9]

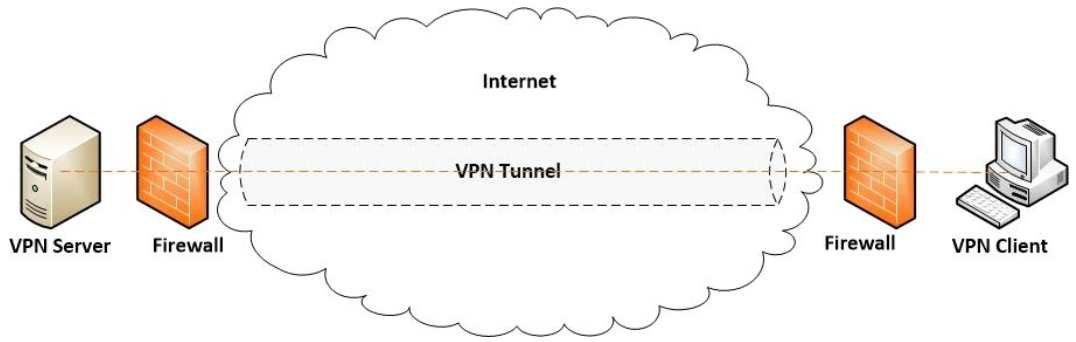

Figure 1.2 – Tunnel VPN.[10]

1.5.2.3 Les types des VPN

Il existe 3 types standard d'utilisation des VPN :

- **VPN Site à Site :** est utilisé pour relier au moins deux ou plusieurs sites entre eux. Ce type de réseau présente une utilité pour les entreprises possédant plusieurs sites distants. Le plus important dans ce type de réseau est d'assurer la sécurité et l'intégrité des données.[11]

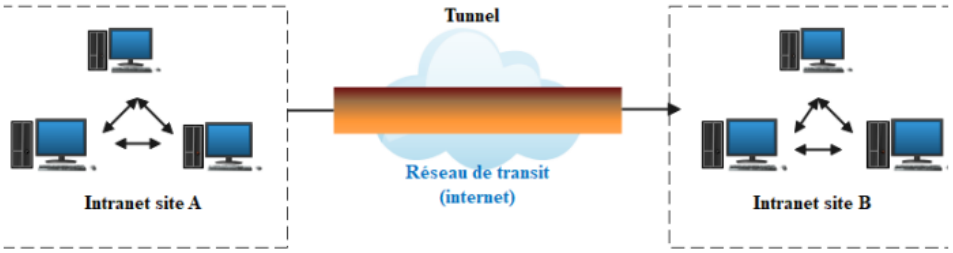

Figure 1.3 – VPN Site à Site.[12]

- **VPN Poste à Site :** Ce type de VPN est aussi fréquemment utilisé et permet aux utilisateurs distants (télétravailleurs ...) d'accéder aux ressources de l'entreprise via un VPN. Pour cela, un utilisateur distant a simplement besoin d'un client VPN installé sur son ordinateur pour se connecter au site de l'entreprise.[4]

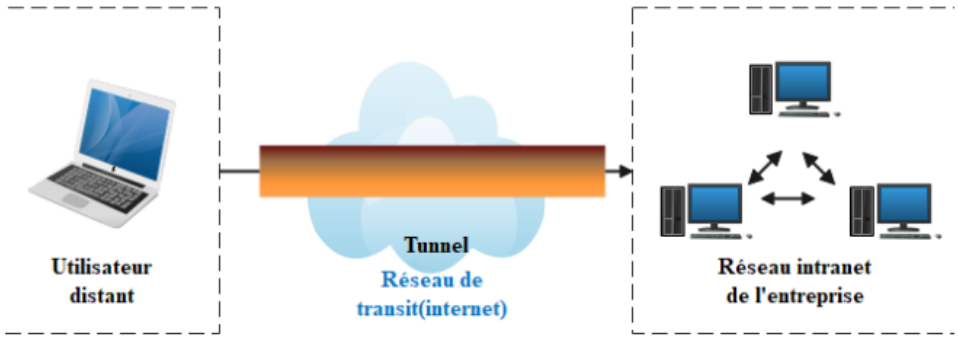

Figure 1.4 – VPN Poste à Site.[12]

- **VPN poste à poste :** l'objectif de ce type d'architecture est d'établir un canal sécurisé entre deux postes ou, plus couramment, entre un poste et un serveur. Le poste et le serveur peuvent être situés sur le même réseau ou sur deux réseaux différents reliés eux-mêmes par un VPN site à site.[9]

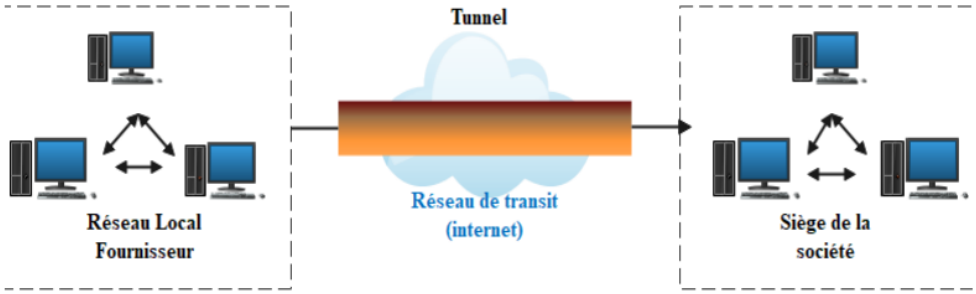

Figure 1.5 – VPN poste à poste.[12]

1.5.2.4 Avantages des VPN

Le VPN offre plusieurs avantages notables, on peut citer [13] :

- **Les économies sur les budgets alloués à la connectivité :** ces économies sont obtenues en remplaçant les connexions longues distances via des lignes louées privées par une connexion unique à Internet sur laquelle on implémente des tunnels VPN afin de réaliser un réseau privé à travers Internet.
- **La flexibilité :** dans le cas d'une entreprise ou d'une administration ayant plusieurs localisations, l'ajout d'un nouveau site se fait simplement en le connectant à Internet et en l'incluant sur le VPN d'entreprise. Il sera ainsi très facilement intégré sur l'intranet d'entreprise.
- La possibilité de communiquer entre vos partenaires ou vos clients en toute sécurité.

1.6 Les protocoles utilisés

1.6.1 Transmission Control Protocol (TCP)

TCP est un protocole de transport qui a pour objectif de fournir un service de communication fiable entre deux tâches exécutées[14], en mode connecté.

1.6.2 User Datagram Protocol (UDP)

UDP est un protocole non fiable et sans connexion. Il permet à une application d'envoyer un message à une autre avec un minimum de fonctionnalités.[14]

1.6.3 Internet Control Message Protocol (ICMP)

ICMP est un protocole de signalisation des problèmes utilisé par le protocole IP. Son but est de tester la connectivité réseau, mais aussi d'apporter une aide au diagnostic en cas de problèmes ou de défaillances.[15]

1.6.4 Transmission Control Protocol/Internet Protocol (TCP/IP)

TCP/IP signifie (Protocol de contrôle des transmissions/Protocole Internet). TCP/IP est un ensemble de règles normalisées permettant aux ordinateurs de communiquer sur un réseau tel qu'Internet.[16]

1.6.5 Secure Socket Layer (SSL)

SSL est un protocole de la couche transport du modèle OSI, utilisé par une application pour établir un canal de communication sécurisé avec une autre application. Pour cela, il assure l'authentification du serveur et du client à l'établissement de la connexion et il chiffre les données durant la connexion.[17]

1.7 Conclusion

Dans ce chapitre, nous avons présenté les notions fondamentales de la sécurité informatique, nous avons cité les objectifs, la terminologie et les mécanismes de sécurité à prendre pour remédier aux attaques, tels que les VPN et les pare-feu, ainsi que les protocoles utilisés.

Après avoir présenté les principaux points de ce chapitre, nous allons passer à une autre partie « Introduction à la virtualisation».

CHAPITRE 2

INTRODUCTION À LA VIRTUALISATION

2.1 Introduction

Dans les dernières années, l'informatique a connu un énorme développement, ce qui a incité les entreprises pour développer leur centre de données. Cela signifie augmenter le nombre de serveurs physiques, augmenter le budget de consommation d'énergie et recruter l'avantage de personnel de maintenance.

La virtualisation permet aux entreprises de ne pas avoir besoin d'un ordinateur supplémentaire à chaque fois qu'elles souhaitent installer un nouveau serveur. Elles ont la possibilité de répondre à des exigences supplémentaires en termes d'infrastructure en lançant simplement un nouveau système d'exploitation.

La virtualisation est utilisée par les entreprises pour réduire le nombre de serveur physique. Cependant, en revanche, cela implique une augmentation conséquente du nombre de serveurs virtuels sur chaque serveur physique, afin d'améliorer son utilisation et de diminuer les dépenses liées. En simplifiant l'administration du système informatique, le matériel serveur permet de réduire la consommation électrique et de libérer de l'espace dans la salle serveur grâce à son matériel.

Ce chapitre offre une base solide pour découvrir de plus près la virtualisation, son historique, ses types, ses nombreux avantages, son architecture et son impact sur les entreprises.

2.2 L'infrastructure informatique

L'infrastructure informatique regroupe l'ensemble des équipements matériels et logiciels d'une entreprise. Tous ces éléments, qui sont connectés entre eux, forment l'infrastructure informatique. On parle également de système informatique ou d'architecture informatique. Ces équipements supposent une installation et une maintenance bien gérées pour que l'entreprise puisse les exploiter au mieux.[18]

2.2.1 Les équipements de l'infrastructure informatique

Il existe plusieurs équipements, on cite quelques-uns :

1. **Les Datacenters**

   Un centre de données (ou Datacenter) est une installation composée d'ordinateurs en réseau et de périphériques de stockage que les entreprises et d'autres organisations utilisent pour organiser, traiter, stocker et diffuser de grandes quantités de données. Une entreprise dépend généralement des applications, des services, et des données contenues dans un datacenter, ce qui en fait est un élément central et essentiel pour ses activités quotidiennes.[2]

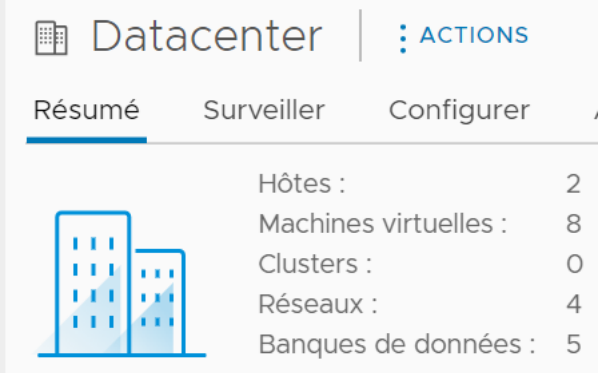

Figure 2.1 – Contenu de Datacenter.

2. **Les serveurs**

   Un serveur est un programme informatique qui « rend service » à plusieurs ordinateurs en réseau par : le stockage, le partage, l'échange de dossiers, de données ou des ressources comme des imprimantes ou fax par exemple.[19]

2.3 La virtualisation

2.3.1 Définition

La virtualisation est l'ensemble des techniques matérielles et logicielles qui permettent de faire fonctionner plusieurs systèmes d'exploitation et/ou plusieurs applications sur une même machine, avec avantages, de manière indépendante de la plateforme matérielle. Elle permet d'utiliser une ressource informatique virtuelle à partir d'une machine physique réelle. Nous pouvons avoir plusieurs systèmes virtuels, appelés machines virtuelles, fonctionnant sur un seul système physique. Ces systèmes virtuels partagent l'utilisation des ressources physiques tels qu'un processeur, une interface réseau ou un disque dur, ces derniers sont alloués à une machine virtuelle pour que celle-ci fonctionne comme une machine physique. La virtualisation est une couche d'abstraction qui découple le système d'exploitation du matériel afin de délivrer une meilleure utilisation et flexibilité des ressources de traitement (VMware) peut-être vu comme une surcouche permettant de créer sur mesure un environnement correspondant aux spéciations de traitements. On parle de [20] :
Machine hôte = machine exécutant les différents systèmes virtuels
Machine invitée = machine virtuelle s'exécutant dans l'environnement de virtualisation

Figure 2.2 – La virtualisation.[21]

2.3.2 Historique

Les années 60 ont marqué l'émergence du concept de virtualisation, lorsque des entreprises comme IBM ont cherché à répartir les ressources des mainframes. La figure ci-dessus illustre comment la virtualisation évolue au fil des années :

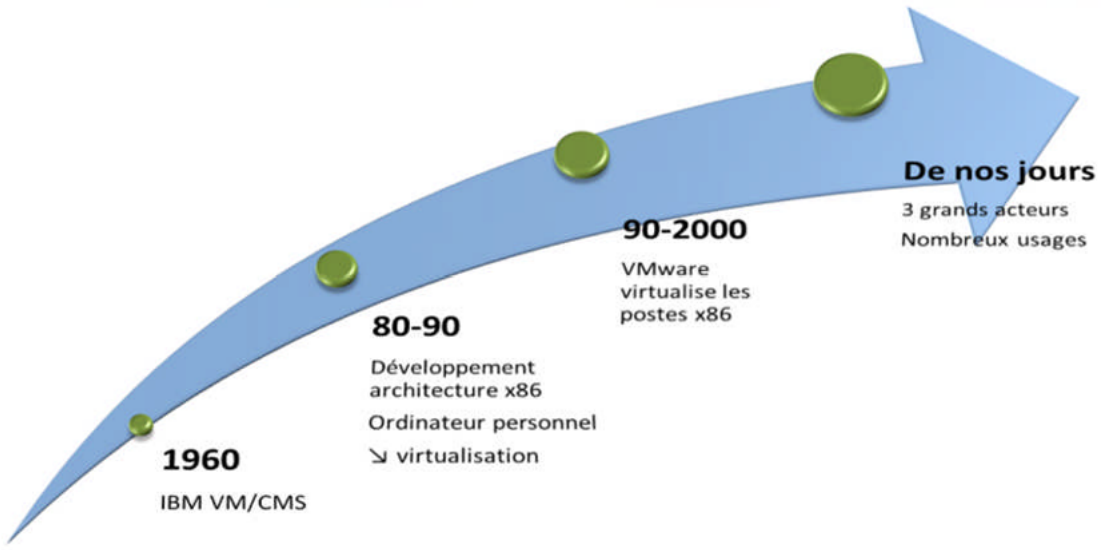

Figure 2.3 – Historique de la virtualisation.[22]

2.3.3 Fonctionnement

La virtualisation repose sur trois éléments principaux : le système hôte, l'hyperviseur et le système invité. La combinaison de toutes ces entités, permet la création d'une virtualisation.

Sur le serveur utilisé, un système d'exploitation, également désigné sous le nom de système hôte, est installé pour garantir le bon fonctionnement de la machine. Il joue le rôle d'OS principal, permettant d'accueillir d'autres systèmes d'exploitation.

Sur le système hôte, un logiciel de virtualisation appelé hyperviseur est installé. Son rôle consiste à créer des environnements dans lesquels d'autres systèmes d'exploitation peuvent être hébergés. Ces derniers sont appelés systèmes invités.

Chaque machine virtuelle, considérée comme un environnement indépendant, peut exploiter les ressources matérielles du serveur physique. Ainsi, chaque machine virtuelle a accès à la mémoire, au processeur et à l'espace disque.[20]

2.3.4 Avantages de la virtualisation

Faire le choix de la virtualisation pour son entreprise, c'est bénéficier de plusieurs avantages[23][24] :

- Utiliser un autre système d'exploitation sans redémarrer son ordinateur.
- Tester des logiciels dans des environnements isolées et sécurisés.
- Réduction du nombre de machines donc du coût de matériels et de sa maintenance.
- Possibilité d'installer plusieurs systèmes (Windows, Linux) sur une même machine.

- Portabilité des serveurs : une machine virtuelle peut être déplacée d'un serveur physique vers un autre.
- Une meilleure exploitation des ressources : jusqu'alors souvent sous-exploitées, les capacités matérielles de l'entreprise sont fortement optimisées grâce à la virtualisation.

2.3.5 Inconvénients de la virtualisation

Comme toutes solutions informatiques, la virtualisation présente des contraintes[24] :

- En cas de pannes d'une machine physique, plusieurs services deviennent indisponibles car c'est toutes les machines virtuelles qui vont s'arrêter.
- Vulnérabilité généralisée : si l'hyperviseur est exposé à une faille de sécurité, les machines virtuelles peuvent l'être également et ne sont plus protégées.

2.3.6 Architecture

2.3.6.1 Système Hôte

Le système hôte est la machine physique qui héberge les machines virtuelles.[25]

2.3.6.2 Hyperviseur

Un hyperviseur est une couche logicielle qui permet la création et la gestion des machines virtuelles (VM). Le système d'exploitation hôte et ses ressources sont séparés des machines virtuelles qui l'exécutent. Il existe deux types d'hyperviseurs :

1. **Hyperviseur type 1 (natif ou encore bare-metal)**
   Un hyperviseur de type 1 est un système qui s'installe directement sur la couche matérielle du serveur afin de se focaliser sur la gestion des SE invités. Ceci permet de libérer le plus de ressources possibles pour les machines virtuelles. Il est possible d'exécuter uniquement un hyperviseur à la fois sur un serveur. Lorsqu'un hyperviseur de type 1 est installé sur une machine, la machine ne peut pas servir à autre chose qu'à faire tourner l'hyperviseur, elle est dédiée à cet usage. Il faut considérer que l'hyperviseur devient le système d'exploitation de la machine. En fait, les ressources matérielles de votre machine, que ce soit un ordinateur ou un serveur, sont gérées directement par l'hyperviseur en lui-même. Voici quelques solutions : Hyper-V de chez Microsoft, ESXI de chez VMWare. VMWare occupe la première place sur le marché grâce à sa solution VMware ESXI.[26]

2. **Hyperviseur type 2 (hébergé, host-based)**

   Un hyperviseur de type 2 est un logiciel qui s'installe et s'exécute sur un système d'exploitation déjà en place. On parle d'hyperviseur hébergé. Par exemple, une machine sous Windows 10 sur lequel on va venir installer un hyperviseur (comme n'importe quel autre logiciel) dans le but de créer des VMs. On retrouve les solutions suivantes : Oracle VirtualBox, VMWare Workstation.[26]

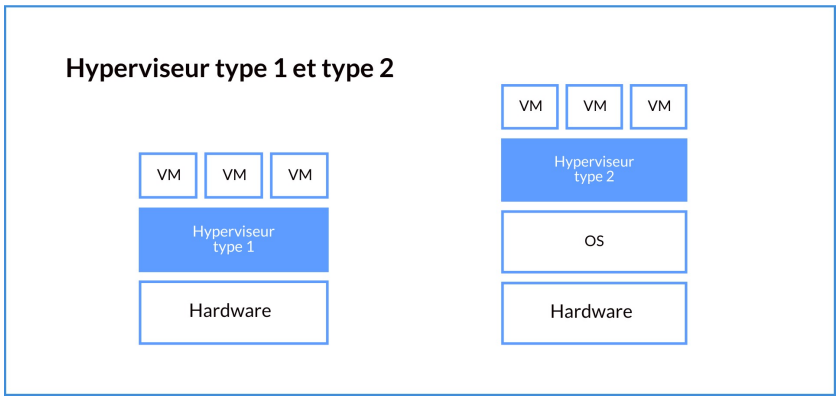

Figure 2.4 – Les types d'hyperviseurs.[27]

2.3.6.3 Virtual Machine (VM)

Les machines virtuelles sont des instances isolées qui fonctionnent comme des systèmes informatiques complets. Chaque machine virtuelle a son propre système d'exploitation, ses applications et ses ressources virtuelles attribuées. Elles sont exécutées sur l'hyperviseur et partagent les ressources physiques du serveur hôte. [28]

2.3.6.4 Système d'exploitation invité virtuel (OS)

Un système d'exploitation invité virtuel (Guest OS) est le système d'exploitation installé au sein d'une machine virtuelle (VM) dans un environnement de virtualisation. Chaque machine virtuelle peut exécuter son propre système d'exploitation invité, indépendamment des autres machines virtuelles et du système d'exploitation de l'hôte.[2]

2.3.6.5 Virtual Switch (vSwitch)

Commutateur virtuel ou vSwitch est une application logicielle, qui contrôle et dirige la communication entre le réseau physique existant et les parties virtuelles du réseau, comme les machines virtuelles.[29]

2.3.7 Les types de virtualisation

2.3.7.1 Virtualisation des serveurs

La virtualisation des serveurs est le premier type de virtualisation rencontré. Cette technique implique le regroupement de plusieurs serveurs virtuels en un seul serveur physique, et ce à l'aide d'une couche logicielle. Chacune des machines virtuelles crée agit ensuite de manière autonome et isolée, exécutant ses propres systèmes d'exploitation et applications. Ce type de virtualisation repose sur le rôle de l'hyperviseur, c'est-à-dire du logiciel, installé sur le serveur physique, qui assure la gestion des différents OS invités.[23]

1. **Les serveurs virtuels**

   Un serveur virtuel se situe sur un serveur physique qui accueille plusieurs serveurs virtualisés. Chaque serveur peut disposer de son propre système d'exploitation et applications. [30]

   Il est possible de consolider plusieurs serveurs en une seule machine qui exécute plusieurs machines virtuelles, ce qui permet d'économiser de l'espace dans le Datacenter. Ainsi, les entreprises peuvent effectuer la redondance sans avoir à acheter de matériel supplémentaire, ce qui permet de réduire au minimum les interruptions de service [31]. Parmi les serveurs virtuels les plus utilisés : Amazon EC2, Oracle VM VirtualBox et Apache Virtual Hosts.

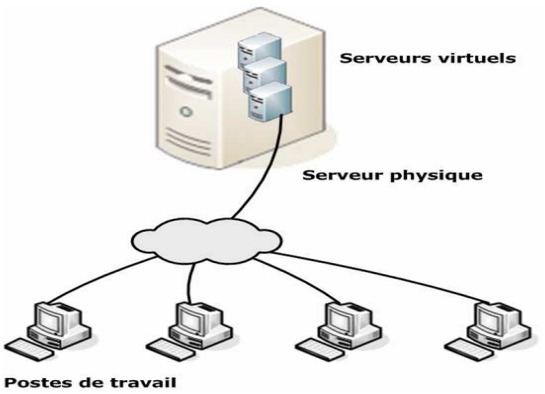

Figure 2.5 – Architecture virtualisée.[32]

2.3.7.2 Virtualisation de systèmes d'exploitation

La virtualisation des systèmes d'exploitation, utilisée parfois à l'échelle domestique, permet d'exécuter sur une seule et même machine plusieurs OS différents, n'interférant pas les uns avec les autres. Exemple : naviguer sur un même ordinateur d'un environnement Windows à un environnement Linux.[23]

2.3.7.3 Virtualisation de poste de travail

Permet l'utilisation et le stockage de fichiers à des endroits facilement accessibles par tous les membres d'une équipe. De cette manière, plusieurs individus peuvent avoir accès aux applications et aux systèmes d'exploitation d'un seul ordinateur une fois qu'ils ont été installés sur un serveur centralisant les données.[23]

2.3.7.4 Virtualisation de stockage

La virtualisation du stockage est la mise en commun de stockage physique de multiples périphériques de stockage réseau dans ce qui semble être un dispositif de stockage unique, qui est géré depuis une Console centrale. La virtualisation du stockage est couramment utilisée dans un réseau de stockage (NAS).[19]

2.3.7.5 Virtualisation de transmission

La virtualisation de transmission consiste à combiner des ressources de transmission matérielles et logicielles dans une seule unité administrative virtuelle. L'objectif de la virtualisation de transmission est de fournir aux systèmes et utilisateurs un partage efficace, contrôlé et sécurisé des ressources de transmission. Le résultat de la virtualisation de transmission est un système de transmission virtuel.

2.4 Conclusion

À travers ce chapitre nous concluons que la virtualisation semble à être imposé comme un élément essentiel au sein des entreprises et ce sont principalement les serveurs qui sont au cœur toutes les attentions, dans le chapitre suivant nous allons présenter l'organisme d'accueil, sa créations, sa situation géographique, son organigramme et ses activités.

CHAPITRE 3

PRÉSENTATION DE L'ORGANISME D'ACCUEIL

3.1 Introduction

Ce chapitre sera réservé à la présentation de l'entreprise Groupe Toudja dans laquelle nous avons effectué notre stage afin de réaliser notre projet de fin d'étude. Tout d'abord, nous commencerons par une brève présentation de l'entreprise, son historique, ses activités et son organigramme. Par la suite, nous ferons le point sur la problématique posée et la solution proposée.

3.2 Présentation de l'entreprise

SPC GB est une société de production de confiserie et des boissons gazeuses, boissons fruites, et Eaux minérales. Elle Fut créée en 1936 et vit une évolution remarquable du point de vue croissance de développement.[32]

FIGURE 3.1 – Logo de l'entreprise.[33]

3.3 Carte d'identité de SPC GB

- **Statut juridique :** Société à Responsabilité Limité SARL.
- **Création :** Depuis 1936.
- **Capital :** 400 000 000 DA.
- **Activité :** Production de confiserie et des boissons gazeuses boissons fruites, et Eaux minérales.
- **Siege sociale :** Route de concession, Quatre chemin BP N°252/253 TER Liberté, Bejaïa (06) Algérie.[33]

3.4 Historique

En 1936, le confiseur Gadouche Boualem a mis en place une fabrication de confiserie et de la limonade à El khmis dans la ville de Bejaia. Deux activités qui semblent complémentaire du point de vue de critère de la saisonnalité du marché local. Cette fabrication produit la limonade pendant la haute saison et se concentre sur la confiserie sur les périodes hivernales.

A l'ouverture de la zone industrielle de Bejaia, la fabrique place une extension a (Quatre chemines) ou elle redouble ses capacité productive. Cette unité existe à ce jour et considéré comme l'unité mère et abrite les locaux directionnels.

Au cours des années 80, l'entreprise délaisse l'activité de confiserie et se canalise sur la production de boisson gazeuse.

En 1992, elle s'engage dans un processus de structuration et de développement au cours du quelle elle érige son statut social en SARL. Des efforts notables coordonnés, dans cette initiative de développement ont permis de mettre en place des nouvelles unités pour l'exploitation. Sur ses fonds propres, elle décide d'investir et inaugure en 1996 une usine moderne de production et d'embouteillage des eaux minérales naturelles et gazéifiées à Toudja. Dénommée société des eaux de Toudja (SET). Cette nouvelle réalisation, située en plaine compagne emploie une centaine de salariés permanents avec une capacité de production frôlant 4000 litres/heure.

La société connait vite les succès escompté grâce aux qualités irréprochables de cette source qui date de l'époque romaine. Inspirée par la fascinante histoire de la source de Toudja.

L'entreprise s'approprie la marque « Toudja » sous la griffe GB (boissons gazeuses commuté au nom du créateur GADOUCHE Boualem).

En 2003, elle décide de suite d'installer une troisième unité dans la zone d'activité d'El Kseur pour la fabrication de jus et sirops avec une capacité de production et de commercialisation

de près de 200 000 bouteilles (25cl)/jour. Des extensions récentes concernant la production de nectar de jus en brique de 1 litre et 2 litres qui vivent à présent des renforcements en capacité productives. Sarl Unilait, une nouvelle unité qui localisée à El Kseur, spécialisée dans la production des jus et soda, comprenant un effectif de 100 employés. [33]

Figure 3.2 – Produit de l'entreprise.[33]

3.5 Situation géographique de la GB

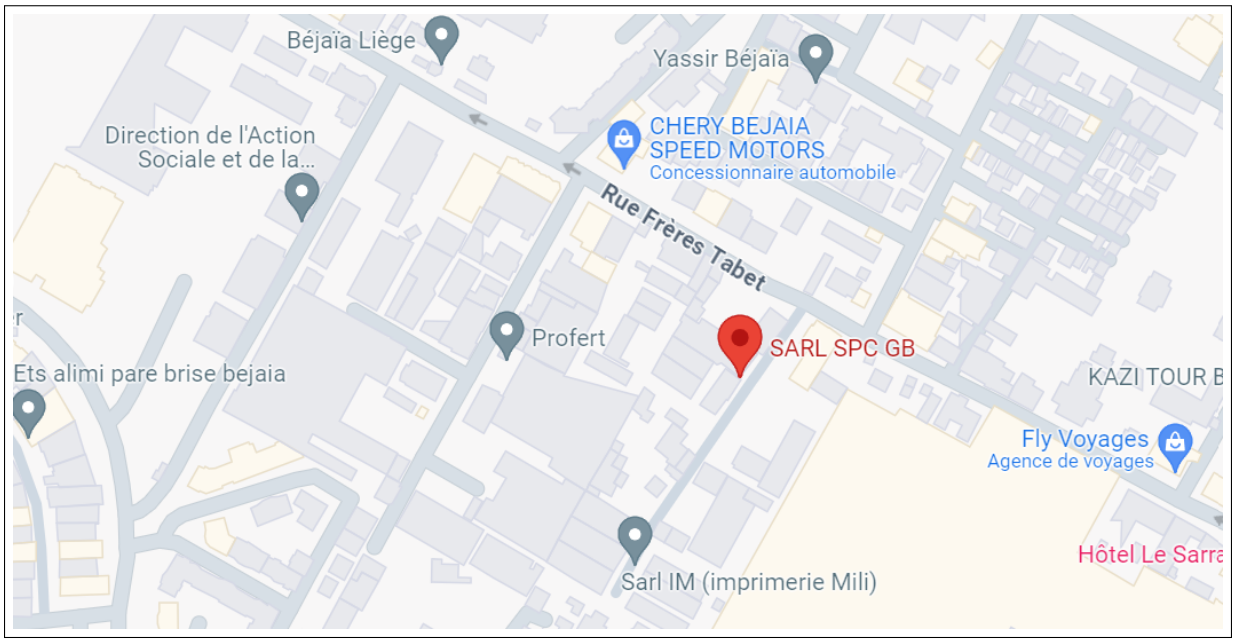

Figure 3.3 – Localisation de la direction générale de l'entreprise.[33]

3.6 Les activités et intervenants

Gardant toujours son activité première, la production des boissons gazeuses, SPC-GB s'est engagé récemment dans la production des nectars de jus. L'activité exploité fait intervenir différents acteurs dont principalement [33] :

- Les institutions étatiques et collectivités locales.
- Institutions financière (banque et postes).
- Des fournisseurs (locaux et étrangers) pour les équipements des matières premières et les services (transitaire, le port, bureaux d'analyse).
- Des distributeurs vus comme clients de l'entreprise.

3.7 Organisation et pilotages

Les activités de l'entreprise SPC GB sont coordonnées par la direction générale sise au site traditionnel de la limonade à Bejaia. Celle-ci est composée de responsable des différentes fonctions de l'entreprise dont on peut noter : l'administrative, commerciale, ressources humaine, achat, gestion de stock, maintenance et production.

L'organisation de l'entreprise GB est conçue à travers une hiérarchie présentable comme suit : le gérant, Directeur Finance et Comptable (DFC), GRH gérant des ressources humaines, les salariés.[33]

3.8 Organigramme de SPC GB

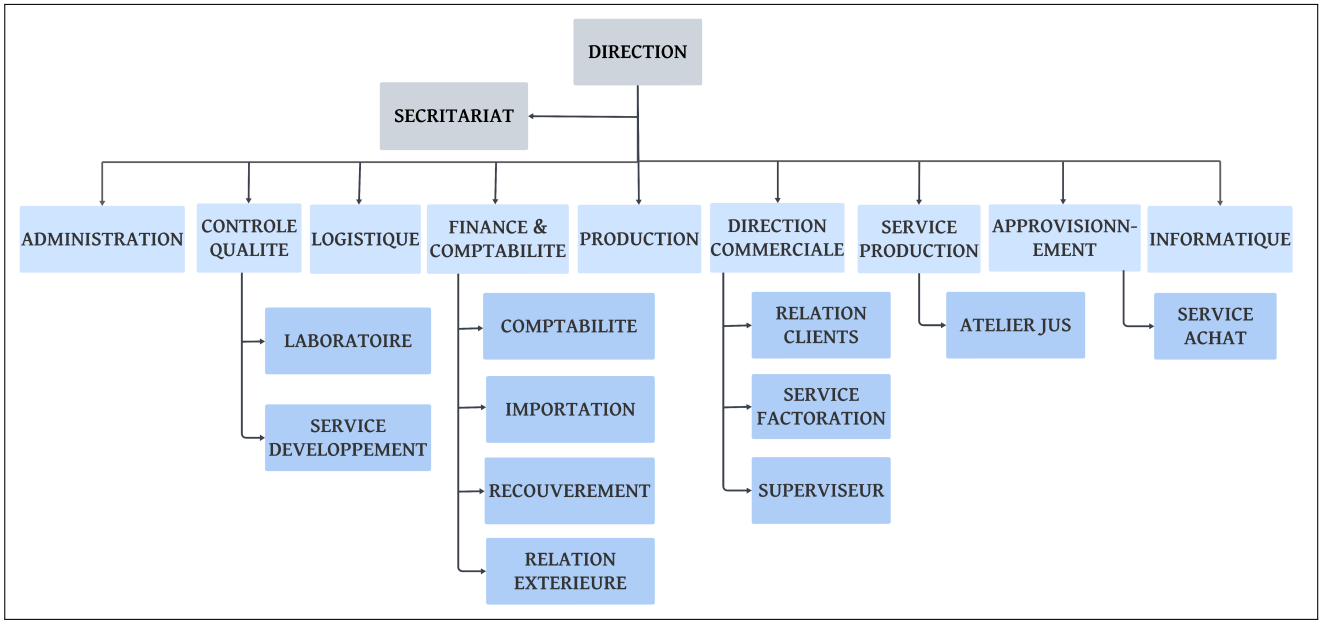

Figure 3.4 – Organigramme de l'entreprise.[33]

3.9 Présentation du département réseau et sécurité

Les tâches et les responsabilités du département réseaux et sécurité peuvent être résumées comme suit [33] :

- Administration réseau et serveurs
- Mise à jour des logiciels
- Maintenance et surveillance des systèmes de caméras de surveillance
- Maintenance PC et imprimantes (côté logiciel)
- Administration des comptes de messagerie
- Aide à l'achat de matériel informatique
- Établir des demandes d'achat de consommables et d'outils informatiques
- Surveillance et sécurité des données
- Analyse des performances du réseau
- Gestion des licences logicielles
- Veille technologique : rester informé des dernières tendances technologiques pour recommander des améliorations.

3.10 Architecture du réseau SPC GB

Le réseau de SPC GB est composé de quatre parties distinctes :

- Réseau de GB Bejaia
- Réseau de GB El Kseur
- Réseau de SET Toudja
- Réseau de Unilait El Kseur

La figure 3.5 illustre l'architecture du réseau de l'entreprise :

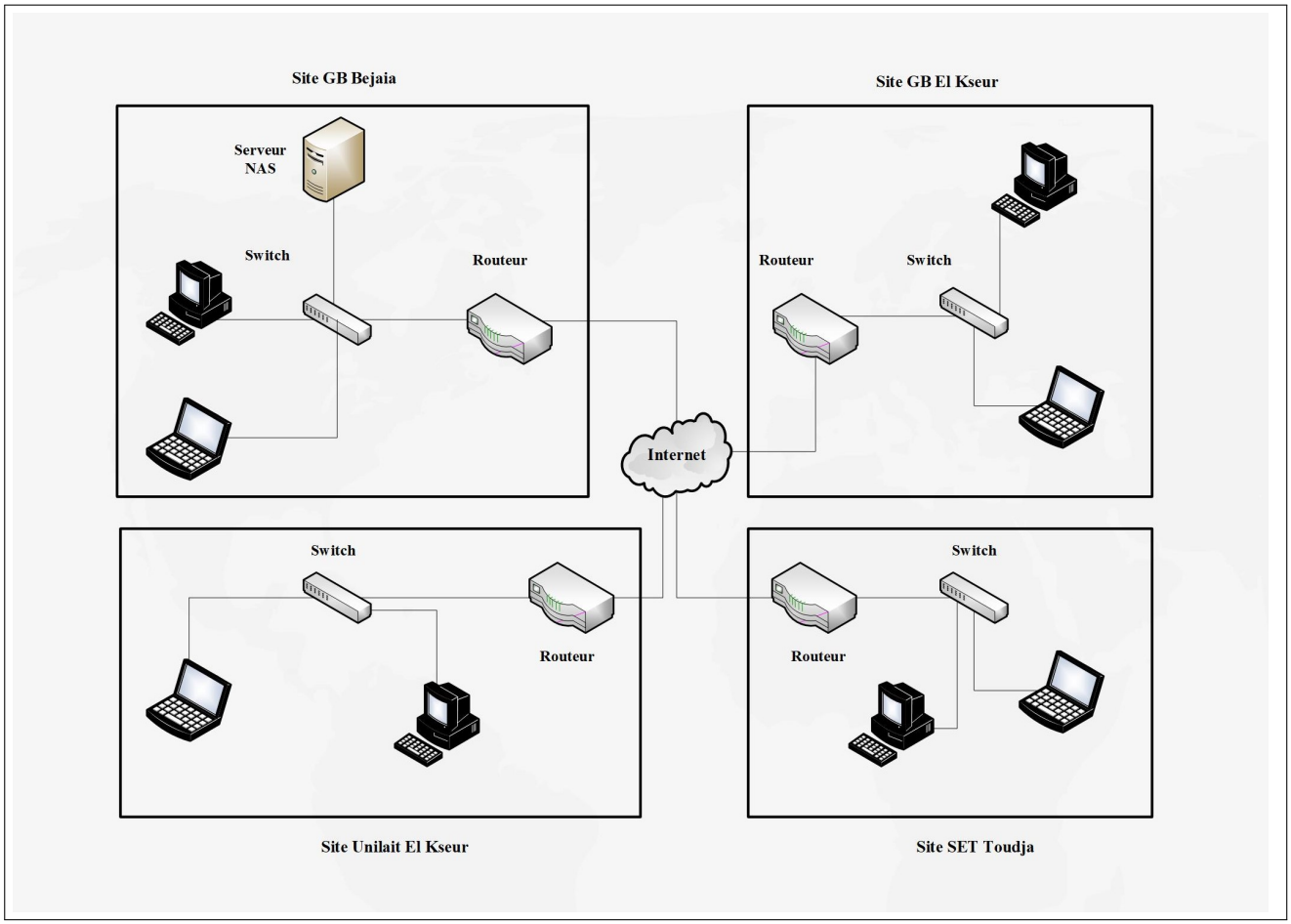

Figure 3.5 – Architecture réseau de « SPC GB ».

3.11 Problématique

Dans le cadre de notre étude de mémoire de fin d'étude, nous avons identifié plusieurs anomalies au sein du réseau de SPC GB -Groupe TOUDJA, susceptibles de compromettre sa sécurité et son efficacité opérationnelle :

- Une connectivité insuffisamment sécurisée entre les sites de l'entreprise, entravant ainsi l'administration à distance.
- La vulnérabilité des échanges de données entre les différentes unités de l'entreprise à travers Internet, exposant ces données à des risques de sécurité.
- Des coûts de maintenance élevés, impactant négativement le budget de l'entreprise.
- Des lacunes dans la procédure de restauration des données en cas de défaillance, mettant en péril la continuité des activités.

3.12 Solutions proposées

Dans le cadre de notre mémoire, nous proposons des ajustements et des solutions concrètes pour remédier à ces anomalies :

- Mise en place d'une stratégie de renforcement des mesures de sécurité, en utilisant des technologies telles que PfSense pour établir des VPN sécurisés entre les sites de l'entreprise.
- Développement et déploiement d'une architecture de virtualisation optimisée, permettant de consolider les ressources serveur tout en garantissant la confidentialité, l'intégrité et la disponibilité des données.
- L'installation et la configuration d'un système de gestion centralisée des utilisateurs et des adresses IP à travers Active Directory, DHCP et DNS.
- Mise en place d'un plan de sauvegarde et de restauration des données robuste, intégrant la réplication au niveau des serveurs pour assurer une disponibilité continue des données en cas de défaillance.

3.13 Conclusion

A travers ce chapitre, nous avons donné un aperçu général sur l'entreprise SPC GB, par la suite nous avons identifié une problématique et ainsi proposé des solutions. L'implémentation de la solution proposée sera abordée dans le chapitre suivant.

CHAPITRE 4

RÉALISATION ET TESTS

4.1 Introduction

Au cours de ce chapitre, nous décrirons la phase de mise en œuvre de ce projet. Cette section est le corps principal de ce mémoire, où nous montrons les étapes de l'installation, configuration et les différentes solutions choisies. Nous terminons en exposant les résultats des tests de vérification, qui confirment le bon fonctionnement de notre application.

4.2 Environnement de travail

4.2.1 Elastic Sky X Integrated (ESXI)

ESXI est un hyperviseur de type 1, qui permet de virtualiser des serveurs et des machines virtuelles sur des ressources matérielles dédiées. Il est développé par VMware et est une version gratuite et légère de VMWare vSphere. Il a son propre système d'exploitation qui assure l'interface avec les agents dont il soutient l'exécution.[34]

FIGURE 4.1 – Logo de l'ESXI.[35]

4.2.2 PfSense

PfSense est un routeur/pare-feu open source basée sur le système d'exploitation FreeBSD.[29]

Figure 4.2 – Logo de PfSense.

4.2.3 Windows server 2022

Windows server 2022 est une version du système d'exploitation serveur développé par Microsoft. Windows Server 2022 est une plate-forme conçue pour prendre en charge les besoins de gestion et de traitement des données des entreprises.[36]

Figure 4.3 – Logo de Windows Server 2022.[37]

4.2.4 OpenVPN

OpenVPN offre la possibilité de créer un réseau privé virtuel VPN. Dans PfSense, Ce logiciel permet à des paires de s'authentifier entre eux en utilisant des certificats ou une clé privée partagée à l'avance.

Figure 4.4 – Logo de l'OpenVPN.

4.3 Partie I : Réalisation

4.3.1 Architecture proposée

Dans notre projet nous allons emmener à faire la virtualisation des serveurs du site principal : le premier est le serveur AD-DNS-DHCP et le deuxième est le serveur de réplication pour assurer la sécurité et la redondance des données.
Notre infrastructure est répartie sur quatre sites à savoir SPC GB Béjaia, GB El Kseur, SET Toudja et Unilait El Kseur. Chaque site est doté d'un pare-feu PfSense, nous l'avons mis en place afin de simuler des tunnels VPN basé sur le protocole OpenVPN.
Pour intégrer ce protocole dans notre infrastructure, il est nécessaire de mettre en place sept connexions VPN, correspondant à la création de quatre tunnels VPN de la façon suivante :

- 4 VPN à SPC GB Béjaia.
- 1 VPN à GB El Kseur.
- 1 VPN à Unilait El Kseur.
- 1 VPN à SET Toudja.

En ce qui concerne la configuration des tunnels, on va créer quatre tunnels :

- 1 Tunnel entre le site de SPC GB Béjaia et celui de GB El Kseur.
- 1 Tunnel entre le site de SPC GB Béjaia et celui d'Unilait El Kseur.
- 1 Tunnel entre le site de SPC GB Béjaia et celui de SET Toudja.
- 1 Tunnel entre le site de SPC GB Béjaia et ces clients distants.

L'architecture du réseau que nous avons créé est illustrée dans la figure suivante :

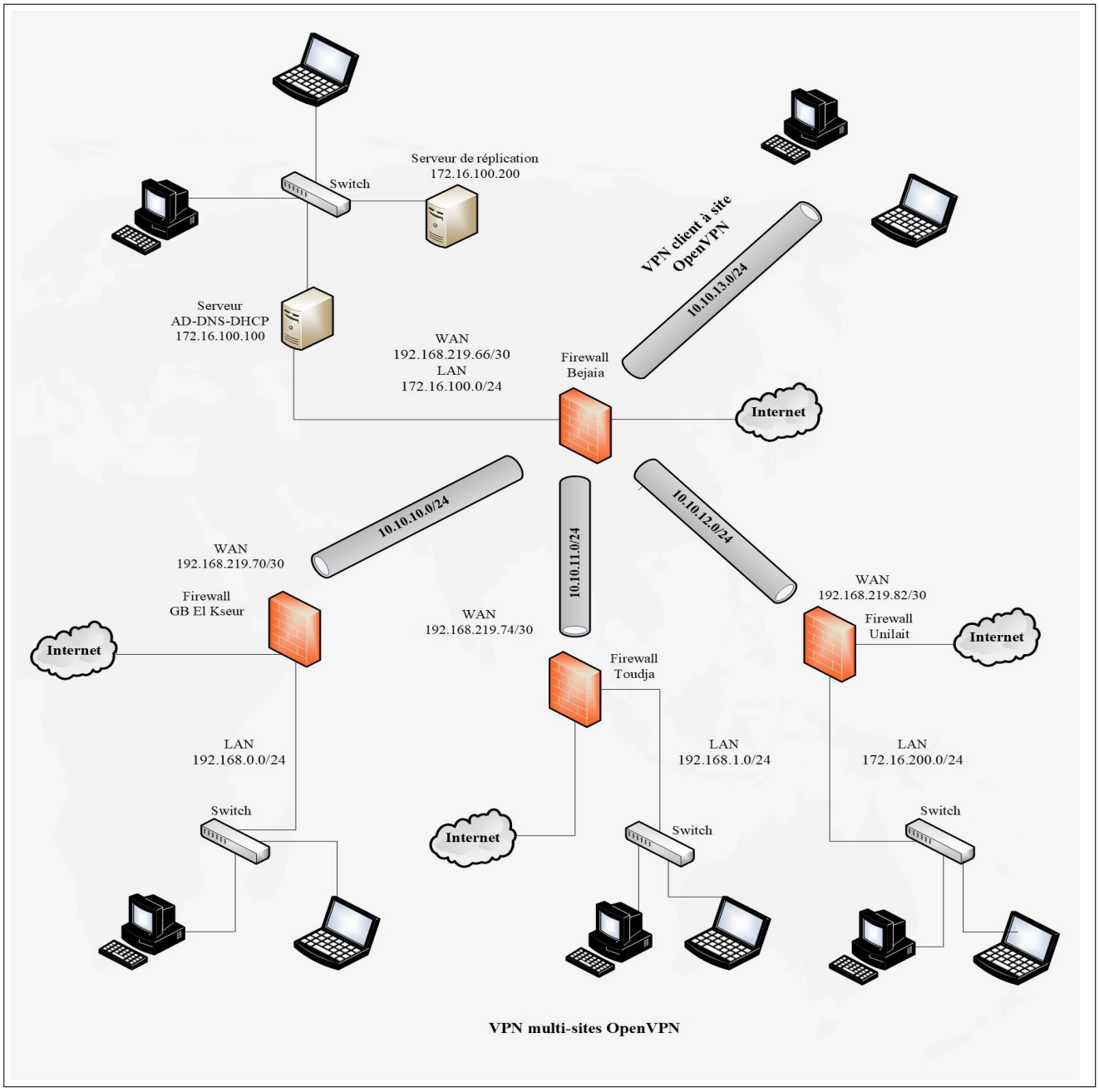

Figure 4.5 – Architecture réseau proposé.

Tableau d'adressage des équipements

Equipements	Interfaces réseau	Adresse IP
Serveur Béjaia	SRV1	172.16.100.100
	SRV2	172.16.100.200
Pare-feu Béjaia	WAN	192.168.219.66
	LAN	172.16.100.240
Pare-feu GB El Kseur	WAN	192.168.219.70
	LAN	192.168.0.10
Pare-feu SET Toudja	WAN	192.168.219.74
	LAN	192.168.1.10
Pare-feu Unilait El Kseur	WAN	192.168.219.82
	LAN	172.16.200.240

Table 4.1 – Tableau d'adressage des équipements.

4.3.2 Création des commutateurs virtuel vSwitch

Sur notre ESXI, on clique sur mise en réseau → commutateur virtuel, on clique sur ajouter un commutateur virtuel standard, sur la fenêtre qui va apparaitre on donne un nom à notre vSwitch et on clique sur ajouter. Comme illustré dans la figure :

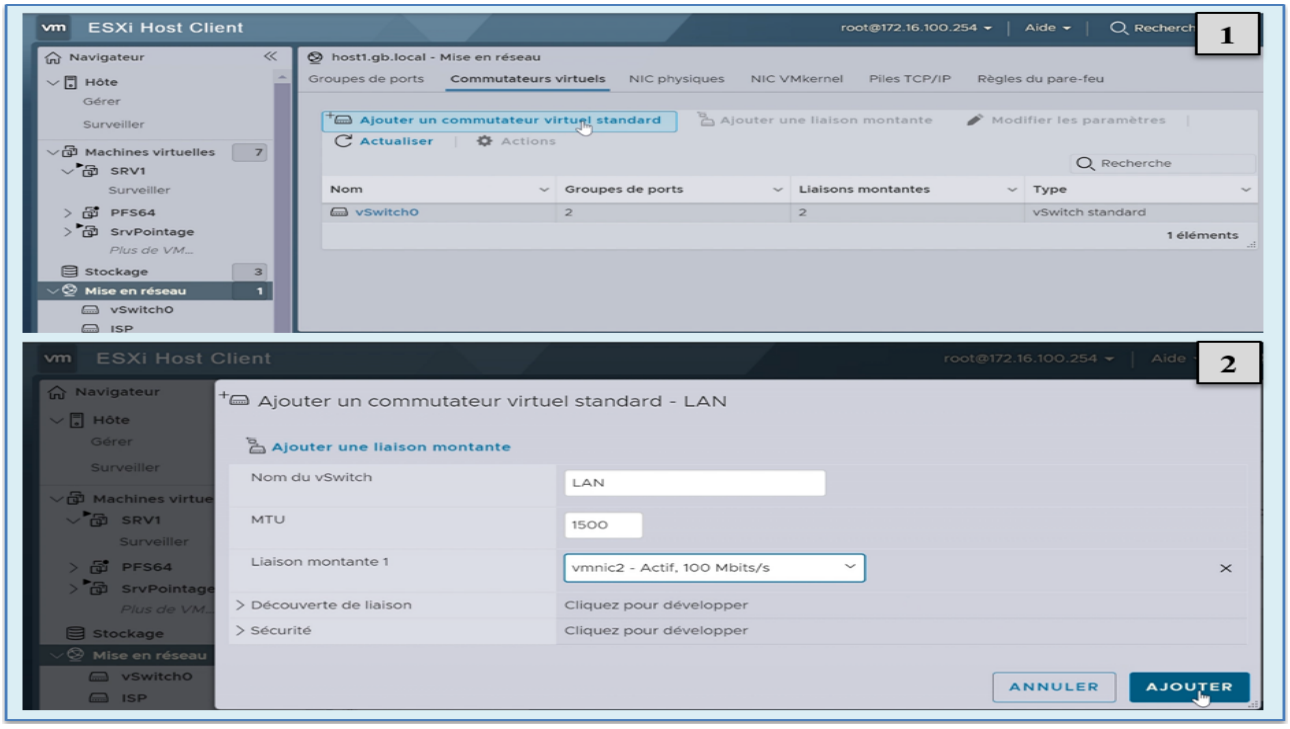

Figure 4.6 – Création d'un vSwitch.

La figure ci-dessous montre la liste des commutateurs virtuels qu'on a créé, le vSwitch0 c'est le commutateur par défaut de l'ESXI (pour le management de notre ESXI) :

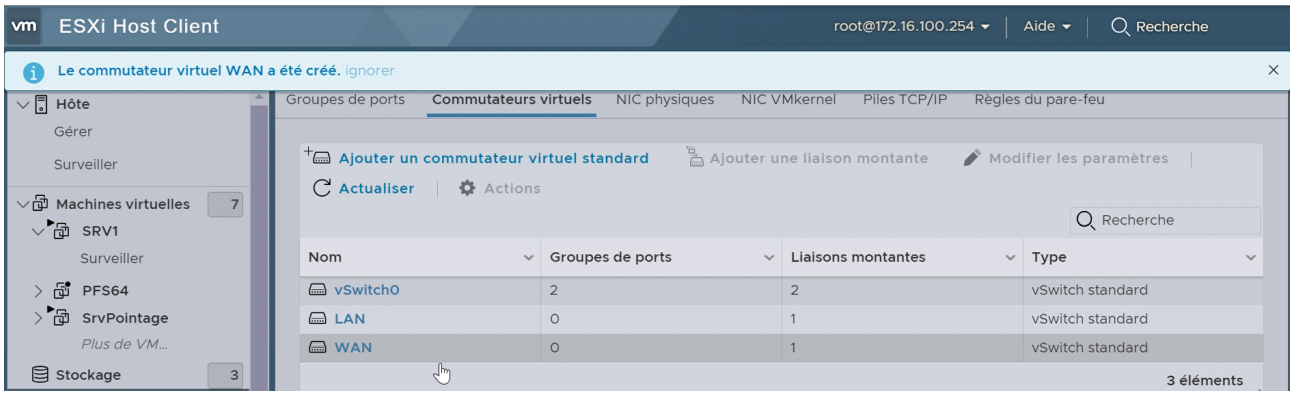

Figure 4.7 – La liste des vSwitch.

4.3.3 Création des groupes de ports

Les groupes de ports permettent de compartimenter une partie des ports du vSwitch. Un vSwitch peut avoir plusieurs groupes de ports, chacun est connecté à une interface réseau physique différente.

Pour créer un groupe de port, on clique sur ajouter un groupe de ports, sur la fenêtre qui va apparaitre on donne un nom à notre groupe de ports, puis on lui affecte le vSwitch adéquat, ici on n'utilise pas le vlan donc ID du VLAN est 0. Comme illustré dans la figure :

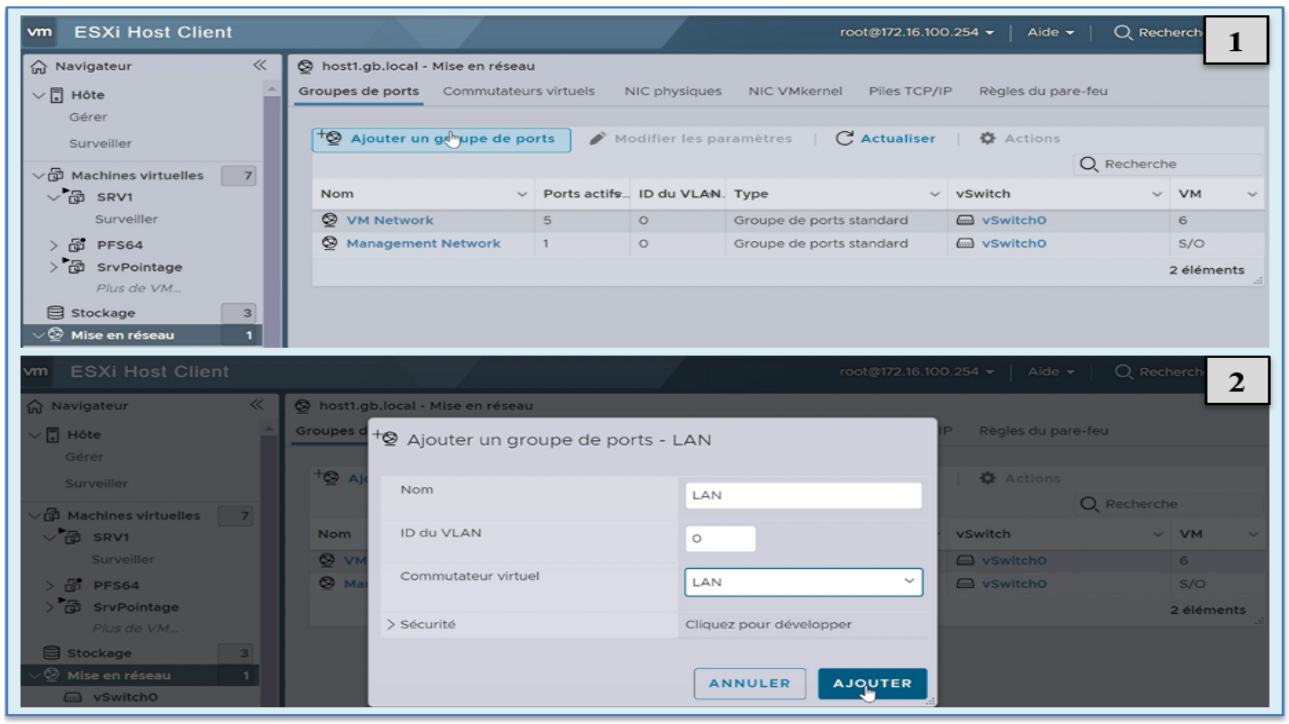

Figure 4.8 – Création des groupes de ports.

Les groupes de ports de notre ESXI sont comme suit :

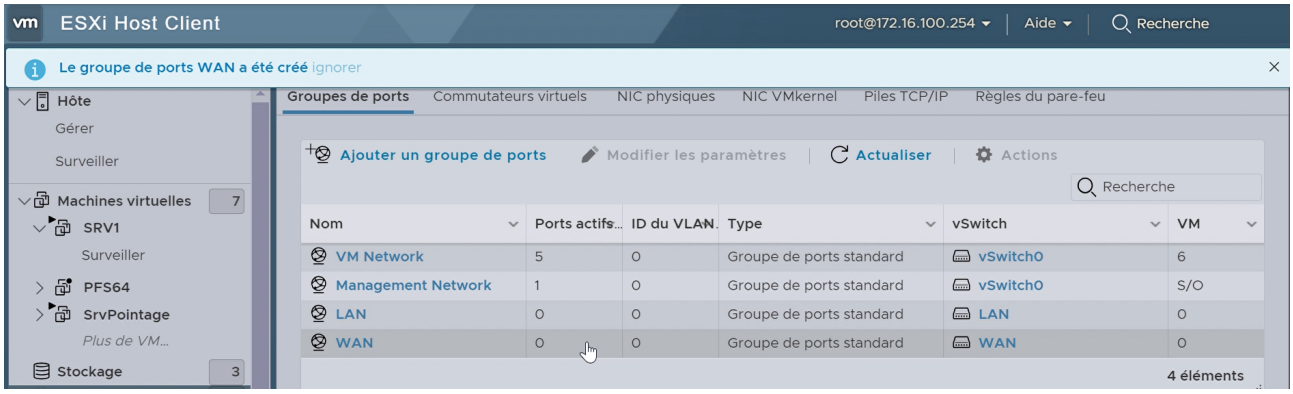

Figure 4.9 – Les groupes de ports crées.

4.3.4 Paramétrage du Firewall

❖ Configuration des interfaces de PfSense

Si l'installation s'est bien déroulée, la machine démarre sur le nouveau système, et après configuration des différentes interfaces, on obtient l'écran suivant :

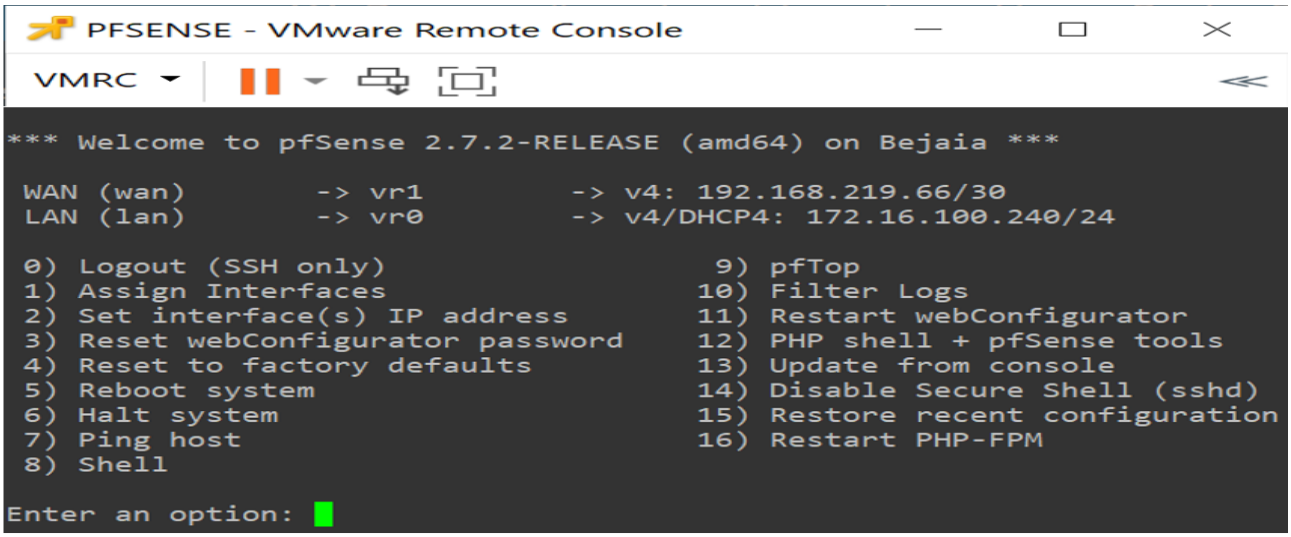

Figure 4.10 – Configuration des interfaces.

Ici on a l'interface graphique de notre firewall PfSense.

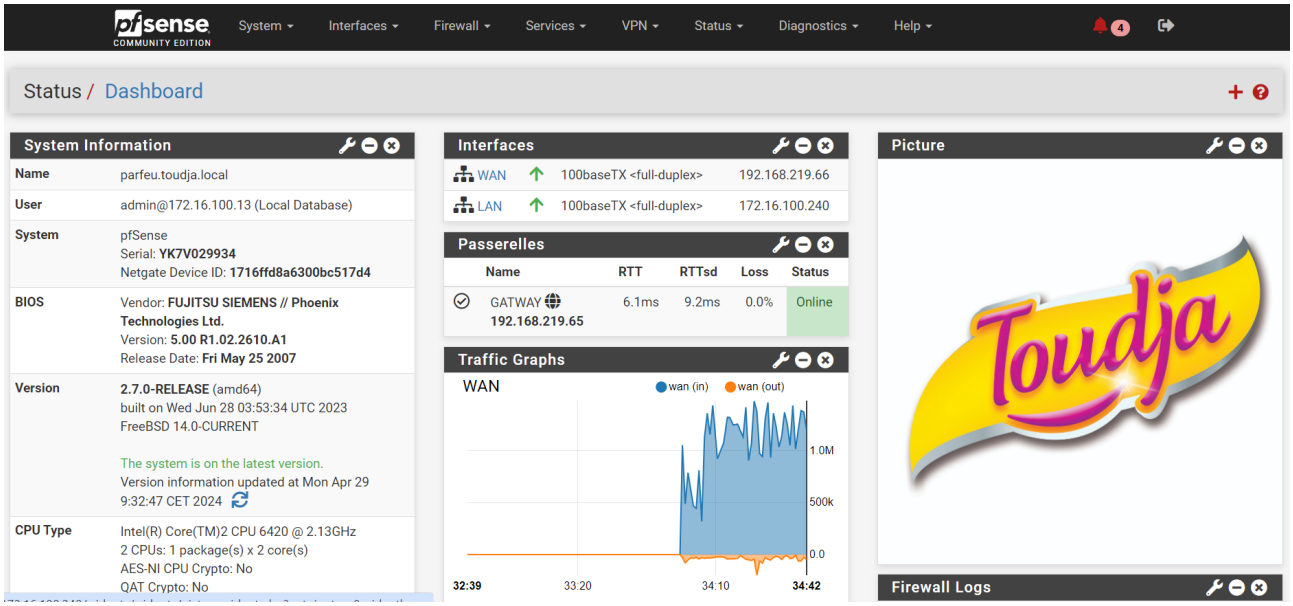

Figure 4.11 – Page d'accueil de PfSense.

De la même façon, nous avons configuré tous les pare-feu.

❖ Interface LAN

- La première règle permet de se connecter depuis n'importe quelle source à l'adresse IP de l'interface LAN, mais uniquement sur le port http (80) ou SSH (22). C'est ce qui nous autorisé de se connecter à l'interface web.
- La deuxième règle autorise tout trafic ICMP provenant de n'importe quelle source et de n'importe quelle destination, sans restriction de port.
- La troisième règle autorise le trafic des paquets IPv4.

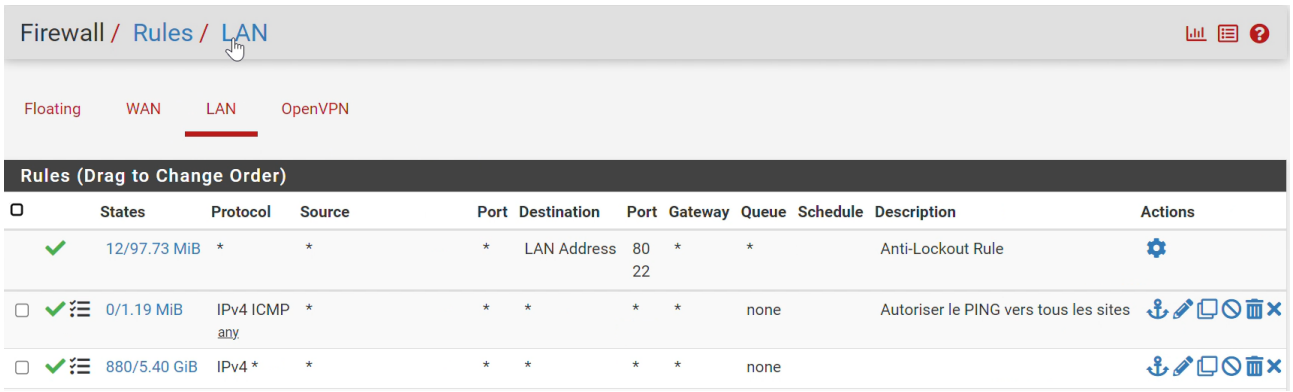

Figure 4.12 – La liste des règles associées à l'interface LAN.

Les mêmes règles sont appliquées pour tous les pare-feu.

4.3.5 Mise en œuvre de la configuration des serveurs

4.3.5.1 Installation des rôles pour le Serveur 1

Pour ajouter des rôles, dans le tableau de bord on va cliquer sur Ajouter des rôles et des fonctionnalités, on va sélectionner le type d'installation, puis on va cocher la case "Serveur AD DS", "Serveur DNS "et "serveur DHCP ", puis lancer l'installation.

De la même façon on va installer l'Active Directory et DHCP pour le **Serveur 2**.

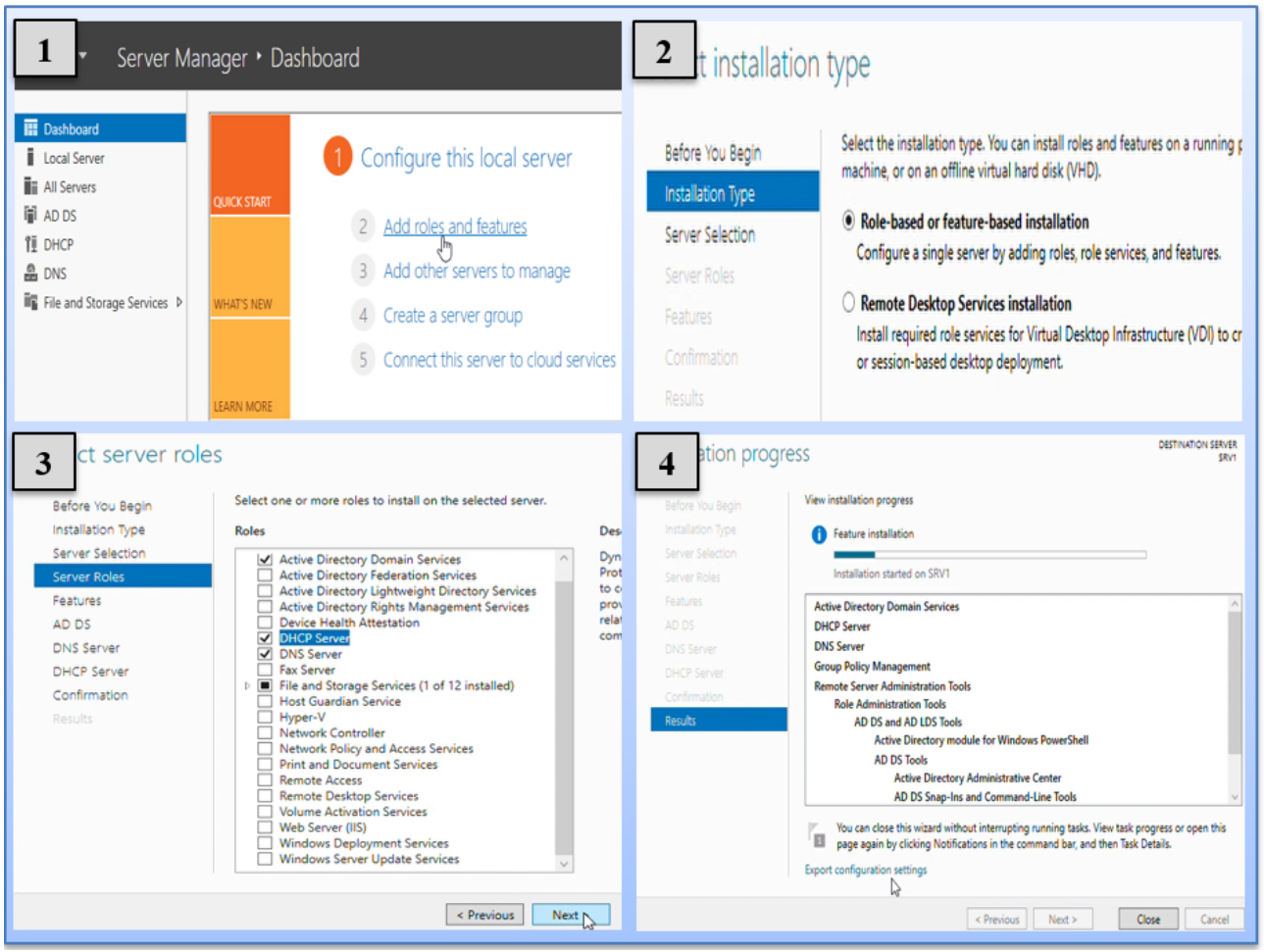

Figure 4.13 – Les étapes d'installation des rôles.

4.3.5.2 Serveur DNS

La fonction principale du serveur DNS (Domain Name System) est de traduire un nom de domaine en adresse IP. Pour simplifier, le serveur DNS fonctionne comme un annuaire.

Le serveur DNS offre la possibilité d'associer une adresse IP à un site web, un ordinateur connecté ou un serveur, tout comme un annuaire téléphonique permet d'associer un numéro de téléphone à un nom d'abonné.[30]

❖ Configuration du serveur DNS

Nous allons maintenant configurer le DNS sur la carte réseau. Pour commencer il faut définir l'adresse IP statique du serveur afin de configurer le serveur DNS.

Tout d'abord, nous cliquons sur le Panneau de configuration et suivons les étapes suivantes : On clique sur Réseau et Internet → Centre Réseau et partage → Modifier les paramètres de la carte.

Par la suite, on fait un clique droit sur la carte réseau → cliquer sur Propriétés → On double clic sur "Protocole Internet version 4 (TCP/IPv4)" → On coche « Utiliser l'adresse IP suivante : » → Notre DNS préféré 8.8.8.8 (c'est le DNS de Google).

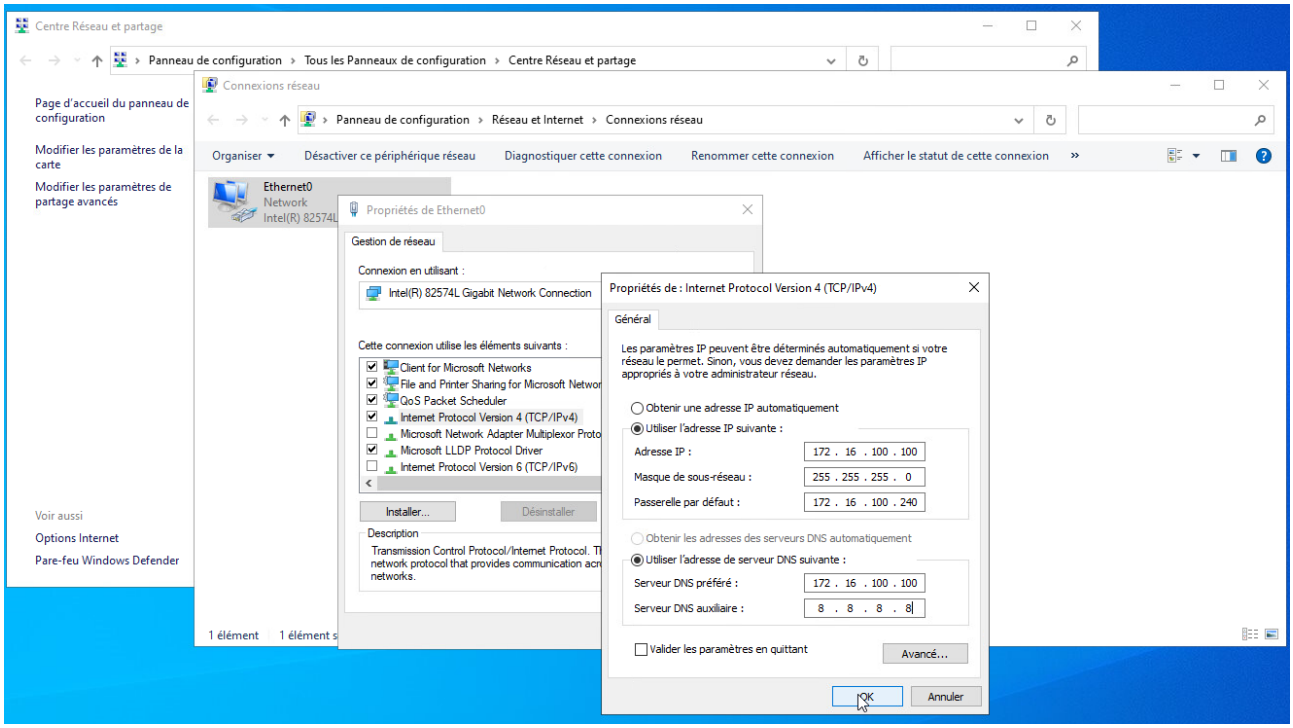

Figure 4.14 – Définir les paramètres IP.

❖ Création d'une nouvelle zone directe

Pour créer une nouvelle zone directe, on va suivre les étapes suivantes :

- On va ouvrir la console d'administration "Gestionnaire DNS" et on fait un clic droit sur "Zones de recherche directe" puis on clique sur "Nouvelle zone".
- On sélectionne le type de zone que nous souhaitons créer et on clique sur "Suivant".
- On va cocher la deuxième option pour que la zone soit répliquée dans l'environnement Active Directory et on va cliquer sur le bouton "Suivant".
- On va indiquer le nom de la zone et on clique sur "Suivant".

- La zone DNS qui va être créée s'affiche. On va cliquer sur le bouton "Terminer" pour confirmer l'ajout de la zone DNS sur le serveur.

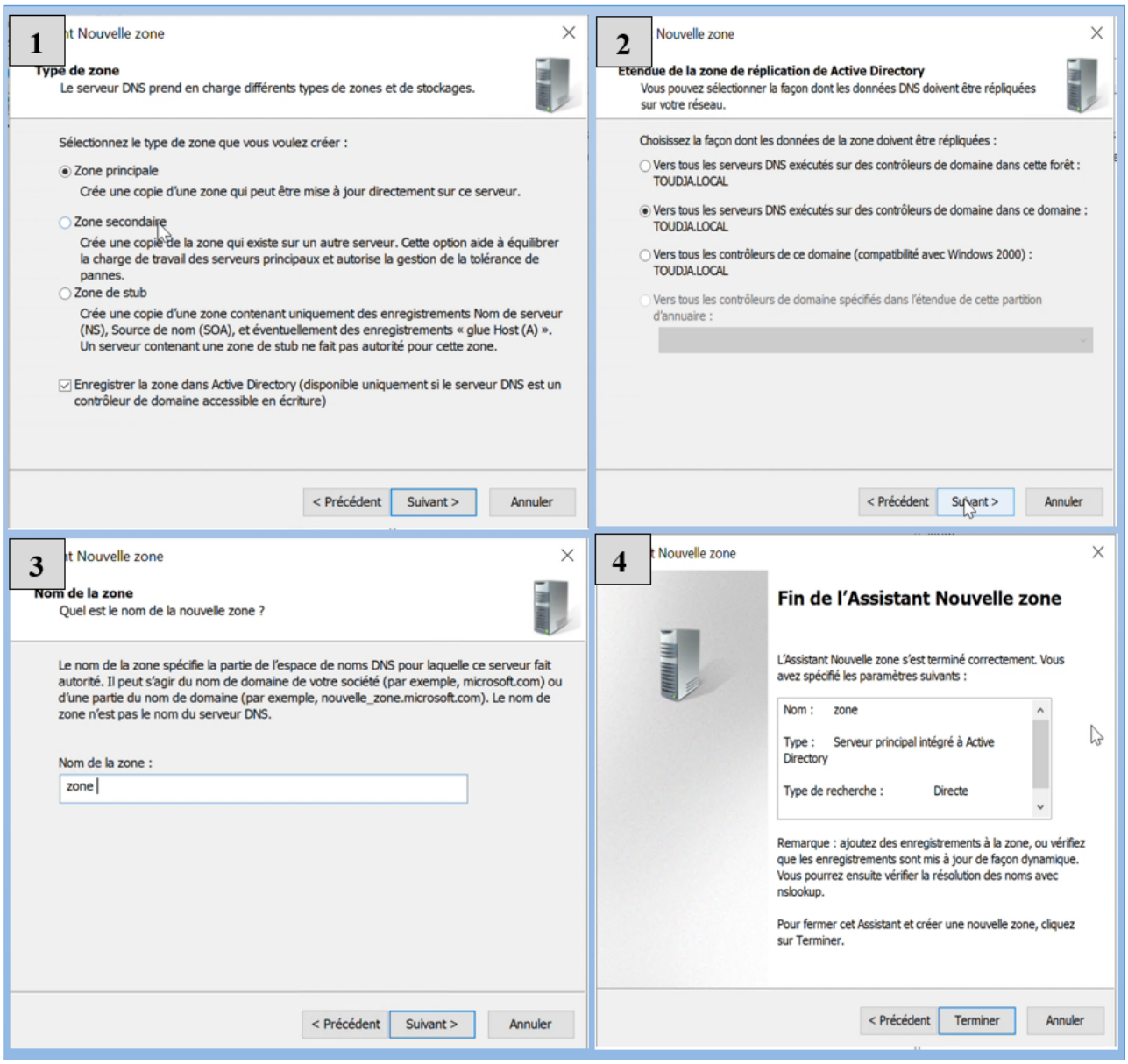

Figure 4.15 – Les étapes de création d'une nouvelle zone directe.

❖ Création d'une nouvelle zone inversée

Pour créer une nouvelle zone inversée, on va suivre les étapes suivantes :

- Sur la console DNS, on effectue un clic droit sur "Zones de recherche inversée", puis on clique sur "Nouvelle zone".
- L'assistant de création d'une nouvelle zone se lance. Tout d'abord, on va choisir "Zone principale" et on va cocher l'option en bas de page pour que la zone soit inscrite dans l'Active Directory.

- On va choisir la seconde option pour que cette zone soit répliquée vers l'ensemble des serveurs DNS associés à ce domaine, afin que la résolution DNS inversée fonctionne sur l'ensemble du réseau local.
- Dans l'étape suivante, on va sélectionner "Zone de recherche inversée". On clique sur "Suivant". Dans la fenêtre qui apparaît, on doit déclarer le sous-réseau concerné par la zone de recherche inversée.
- La dernière fenêtre qui s'affiche montre la fin de création de la zone. On clique sur "Terminer".

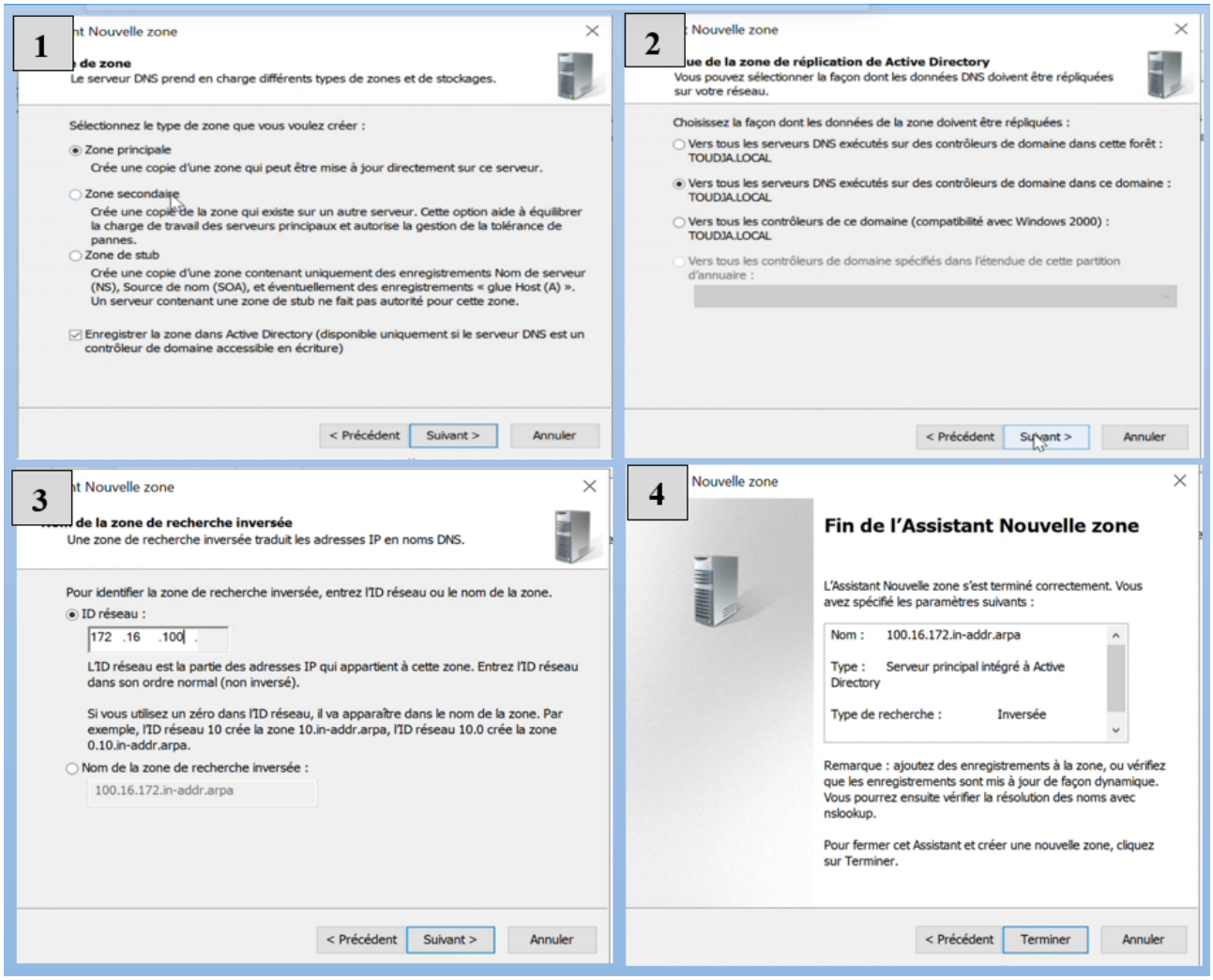

Figure 4.16 – Les étapes de création d'une nouvelle zone inversée.

4.3.5.3 Serveur Active Directory

Active Directory est la base d'un réseau Microsoft, il permet aux utilisateurs de localiser, gérer, nommer, décrire, et sécuriser de manière cohérente les informations concernant les ressources réseau.

❖ Configuration de l'Active Directory

Pour promouvoir ce serveur en contrôleur de domaine donc on va créer une nouvelle forêt, pour se faire, nous sélectionnons "Ajouter une nouvelle forêt" et indiquer un nom de domaine : TOUDJA. LOCAL → attribuer un mot de passe → Dans toutes les étapes suivantes on laisse les paramètres par défaut en cliquant sur suivant → Un dernier écran résume notre paramétrage, on clique sur installer et c'est terminer.

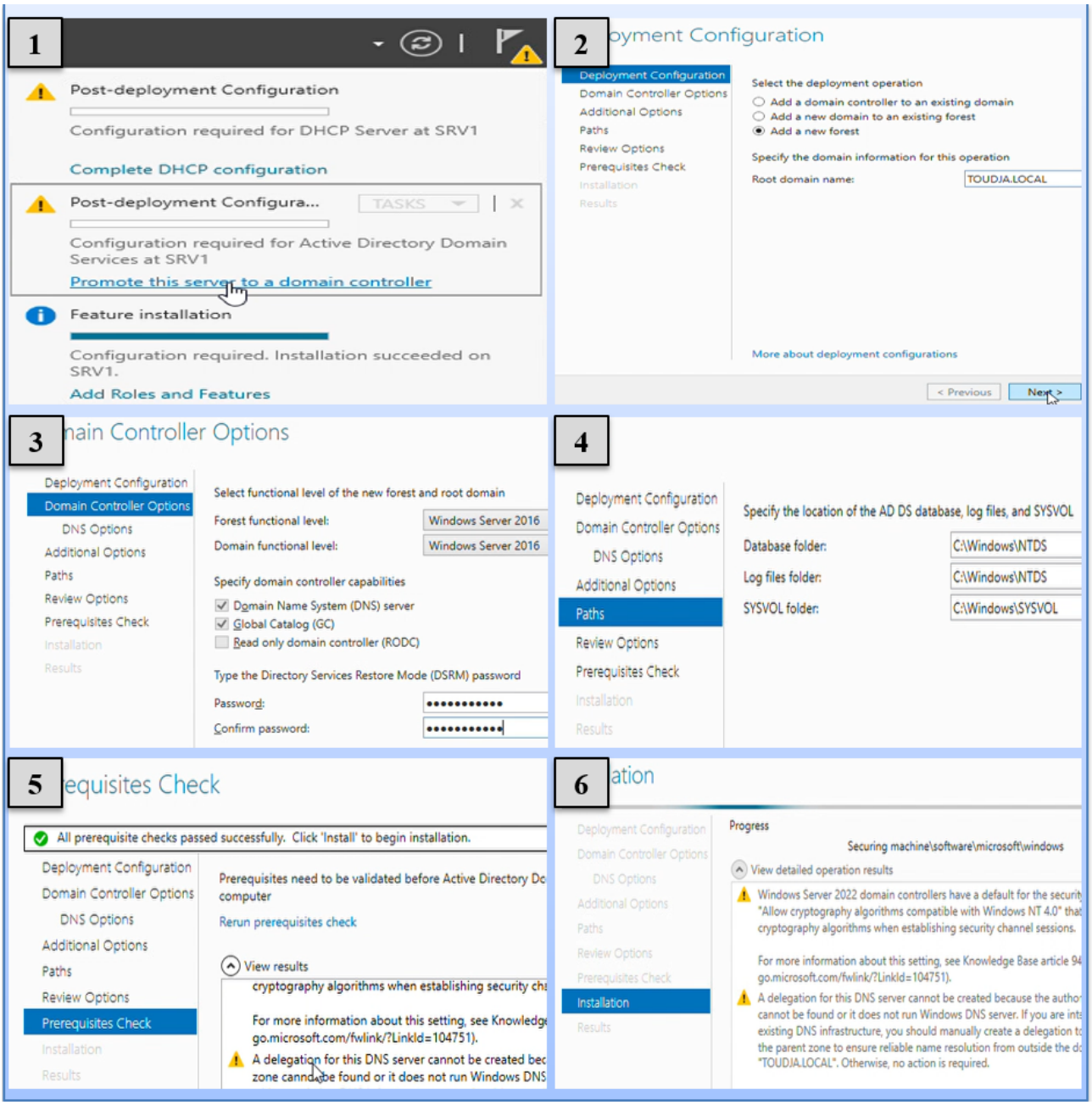

Figure 4.17 – Configuration de l'AD DS.

❖ Création d'unité organisation

Dans notre entreprise SPC GB, ils existent plusieurs utilisateurs, alors pour simplifier et centraliser la gestion de ces derniers, il faut leurs créer des comptes dans le serveur à travers

le service AD DS. D'abord, nous allons créer des unités d'organisations, pour organiser les utilisateurs et les ordinateurs afin de pouvoir leurs appliquer des procédures et des stratégies de groupes.

Pour créer l'unité d'organisation sous le nom (STAGIAIRE)

- Cliquant sur outils (Tools).
- On va choisir « Utilisateurs et ordinateurs Active Directory ».
- Un clic droit sur TOUDJA.LOCAL.
- On va cliquer sur Nouveau.
- On va selectionner Unité d'organisation et on va la nommée (STAGIAIRE).

La figure ci-dessous montre les étapes de la création de l'unité :

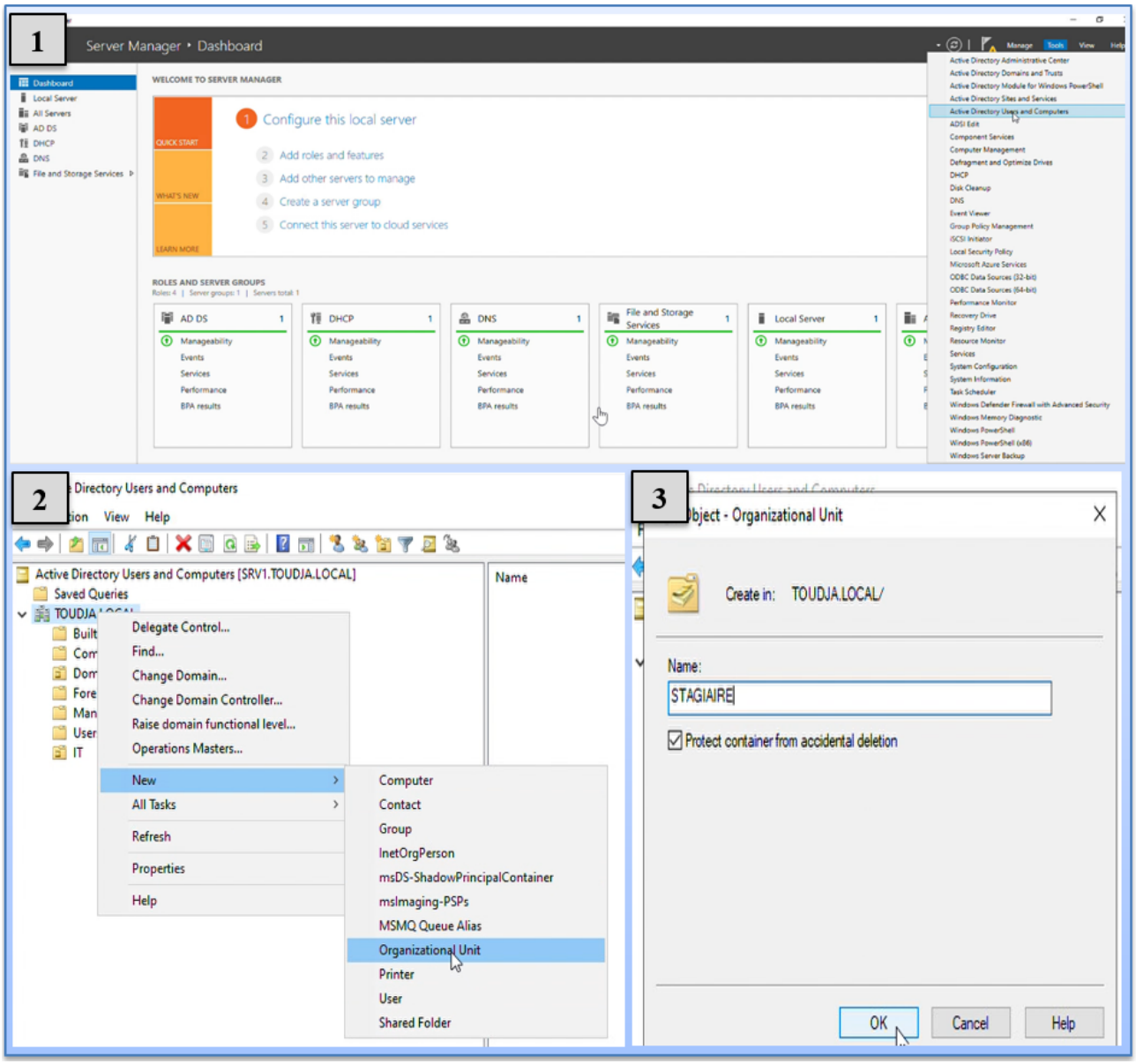

Figure 4.18 – Création d'une unité organisation.

❖ Création des utilisateurs dans l'Active Directory

Pour créer un utilisateur, il suffit de suivre les étapes suivantes :

Faisons un clic droit sur l'unité d'organisation → nouveau → utilisateur, on entre le nom, prénom et l'identifiant de l'utilisateur, puis on clique sur suivant, ensuite on doit introduire le mot de passe et le confirmer.

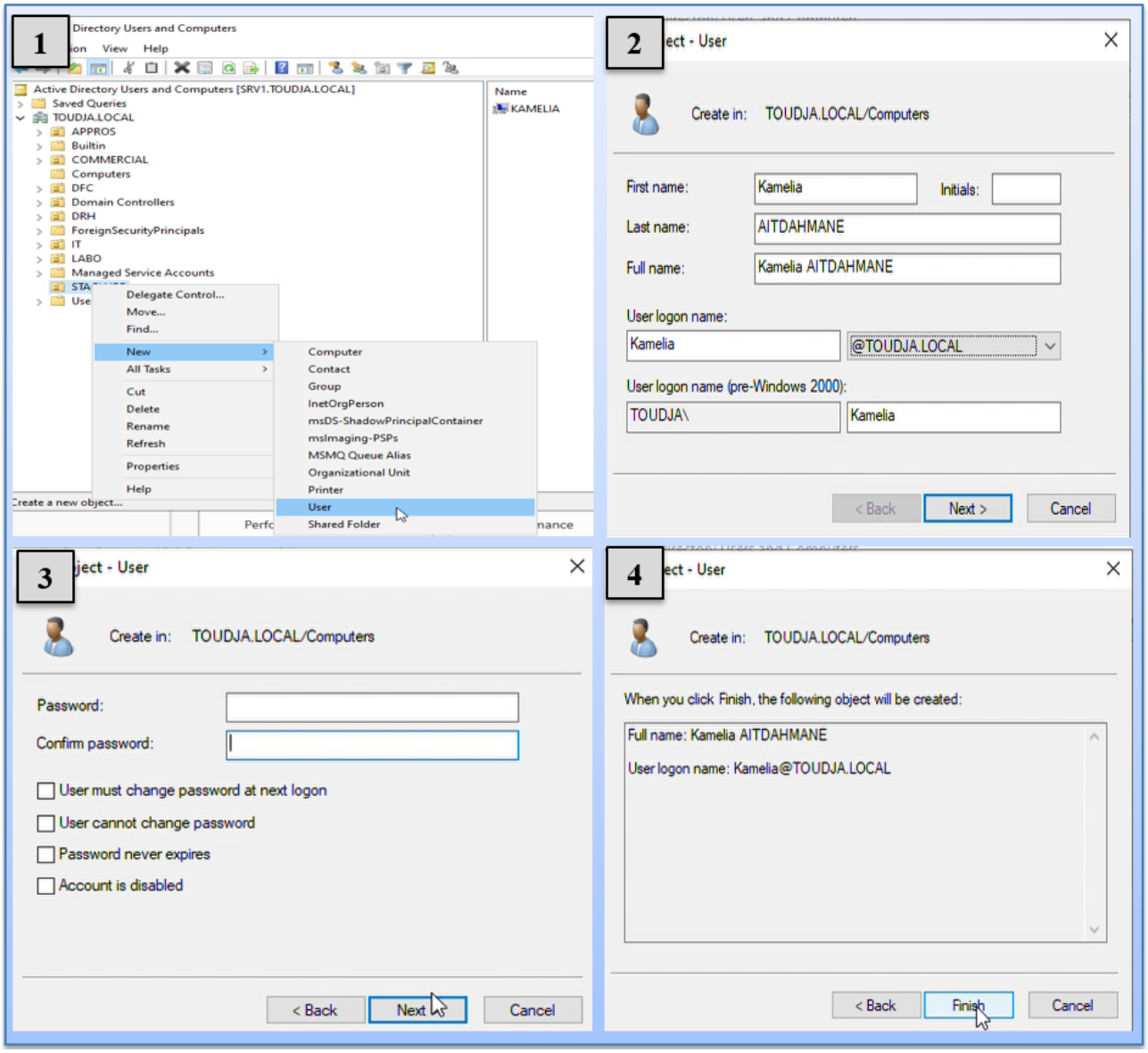

Figure 4.19 – Création d'un utilisateur Active Directory.

❖ Addition d'un membre a un groupe

Pour rendre un utilisateur administrateur du domaine, nous suivons les étapes ci-dessous :

- Préciser l'utilisateur que nous souhaitons rendre administrateur.
- Clique droit sur l'utilisateur en question et sélectionner "Ajouter à un groupe".

- Dans la fenêtre "Sélectionner les objets", taper "Administrators" dans le champ de recherche et cliquer sur "OK".

La figure présente les étapes à suivre pour rendre un utilisateur administrateur du domaine :

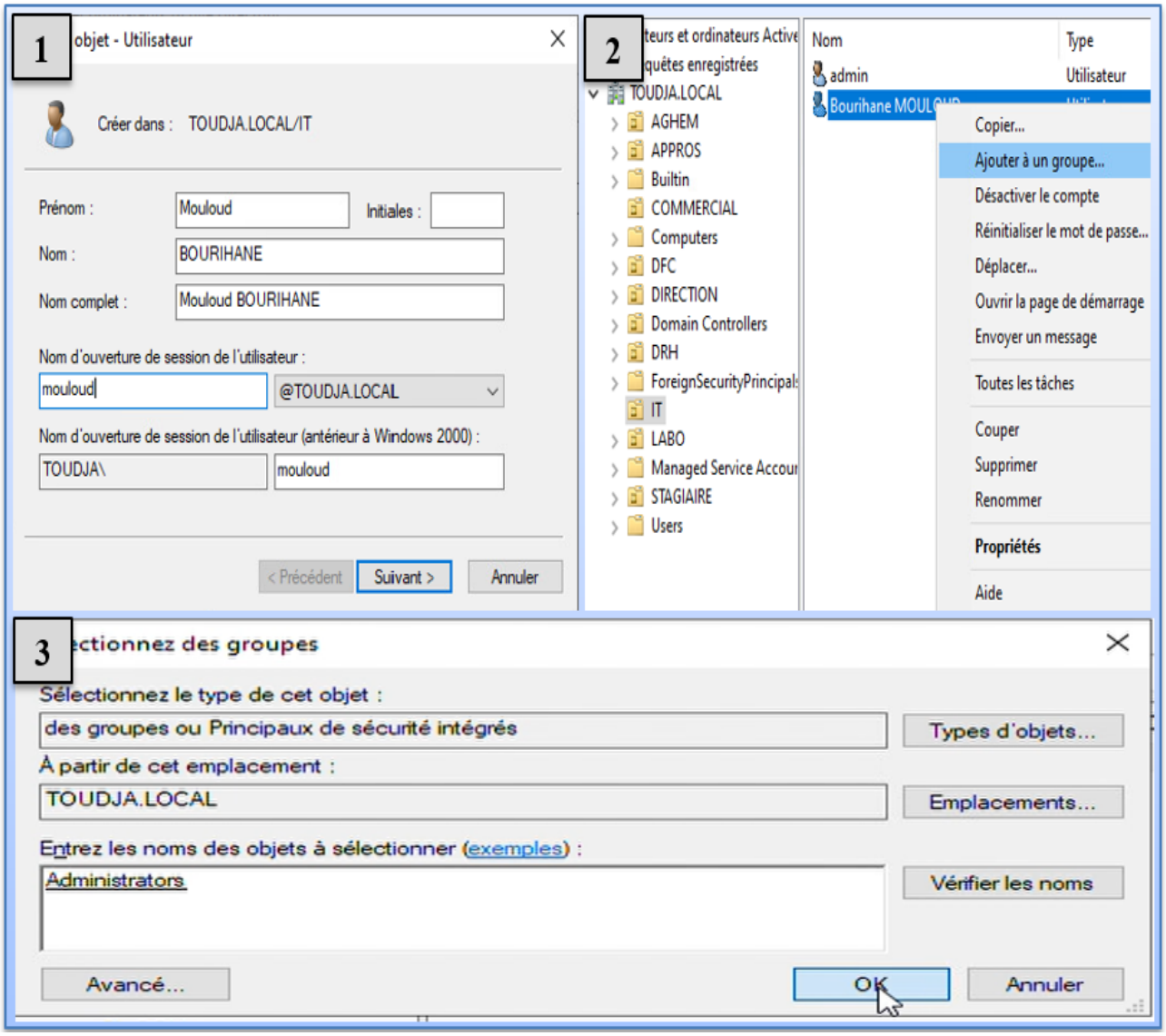

Figure 4.20 – Rendre un utilisateur administrateur du domaine.

4.3.5.4 Serveur DHCP

DHCP (Dynamic Host Configuration Protocol) est un protocole réseau qui permet de configurer automatiquement les paramètres IP d'une station ou d'une machine, en lui attribuant automatiquement une adresse IP et un masque de sous-réseaux.

❖ **Configuration de DHCP**

Pour créer les étendues :

On clique sur outils → on va choisir DHCP → on clique sur srv1.toudja.local → un clique droit sur IPv4 → on va choisir Nouvelle étendue → on lui donne un nom et une description, puis on

va définir la plage d'adressage IP → dans notre cas on va pas exclure les adresses → ajouter la passerelle → on va donner un nom et une adresse IP au serveur WINS pour convertir les noms NetBIOS en adresse IP.

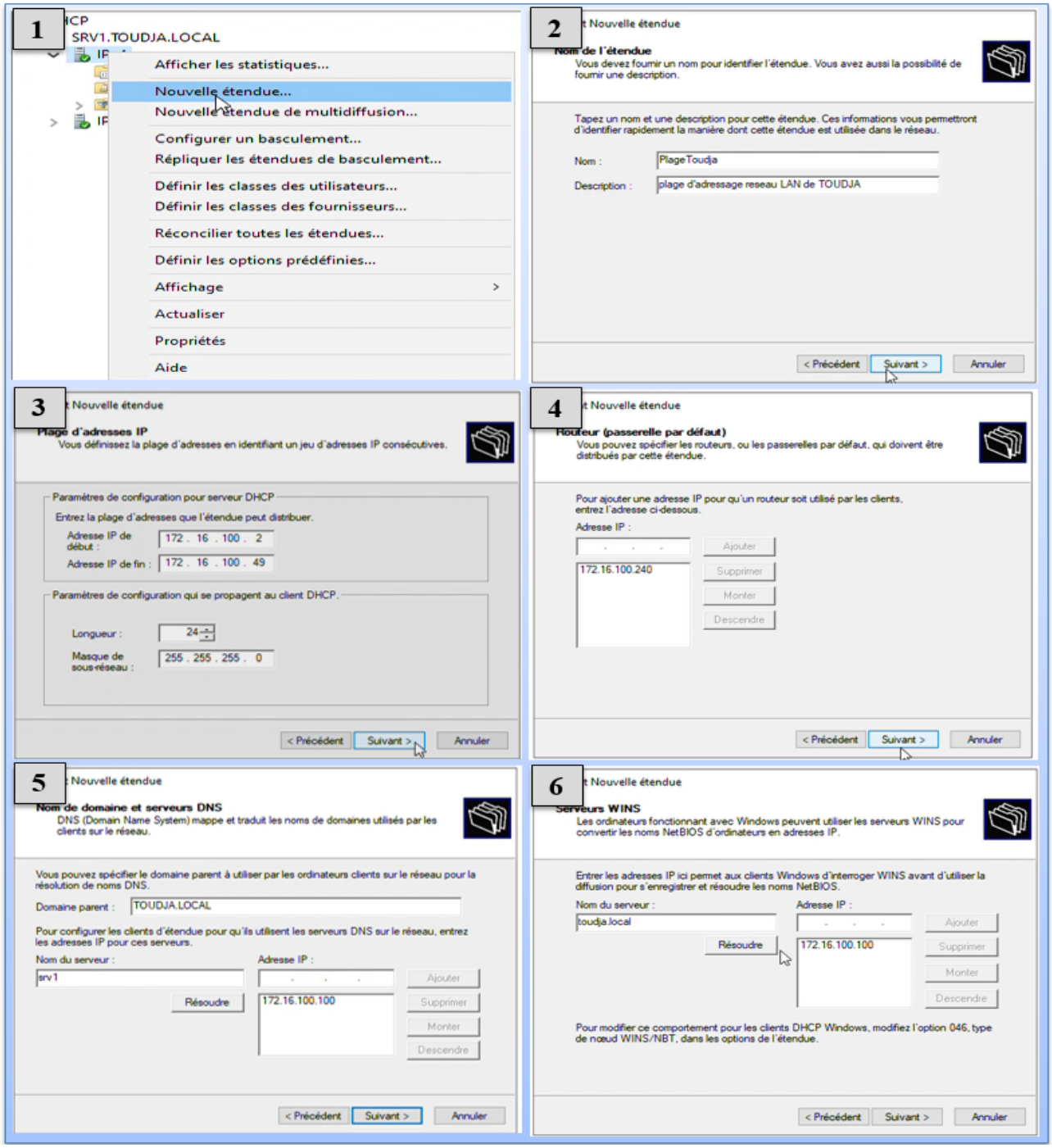

Figure 4.21 – Création de l'étendue.

❖ Création d'une réservation

Une réservation DHCP est une adresse IP, qui est écartée au sein d'une étendue afin d'être utilisée par un client DHCP spécifique.

Pour créer une réservation, il suffit suivre les étapes suivantes :

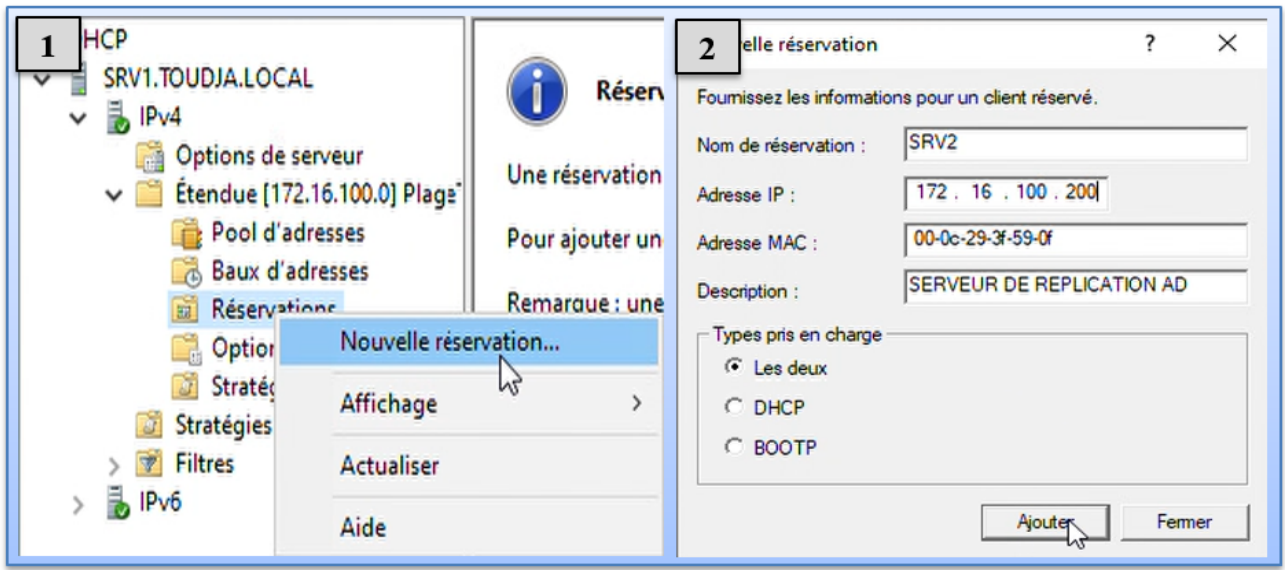

Figure 4.22 – Création d'une réservation.

❖ Connexion bureau à distance

La figure ci-dessous montre les étapes de connexion à distance :

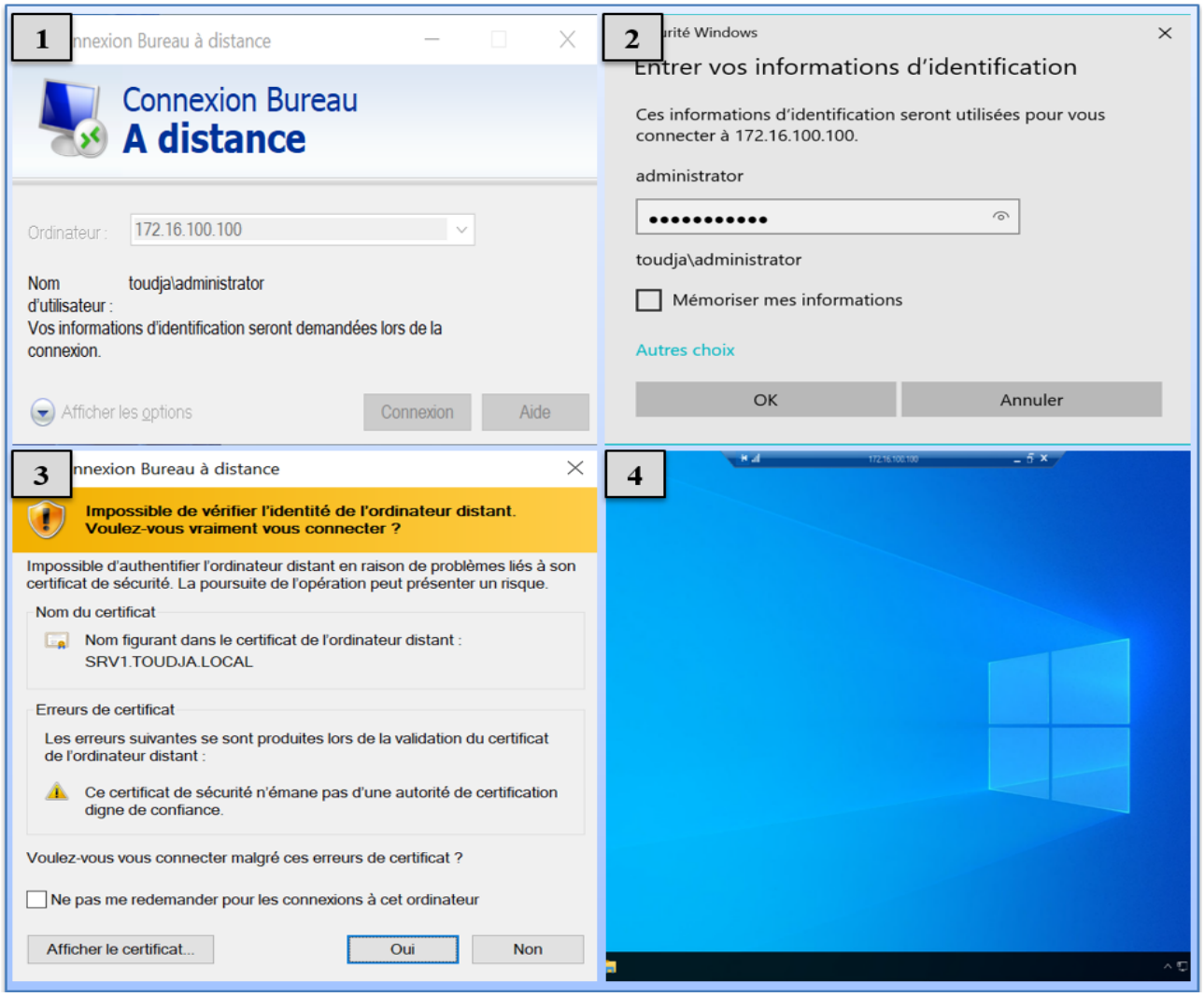

Figure 4.23 – Accéder au serveur à distance.

4.3.5.5 Réplication du Serveur 2

La réplication permet de synchroniser en toute sécurité les données sur plusieurs serveurs. Cette technologie est utilisée pour créer des sauvegardes et autoriser plusieurs versions du même fichier.

❖ **Réplication de l'Active Directory dans le serveur 2**

On va commencer par la configuration de l'adresse du deuxième serveur, ainsi dans la partie DNS nous attribuons l'adresse du premier serveur (SRV1), voir la figure au-dessous :

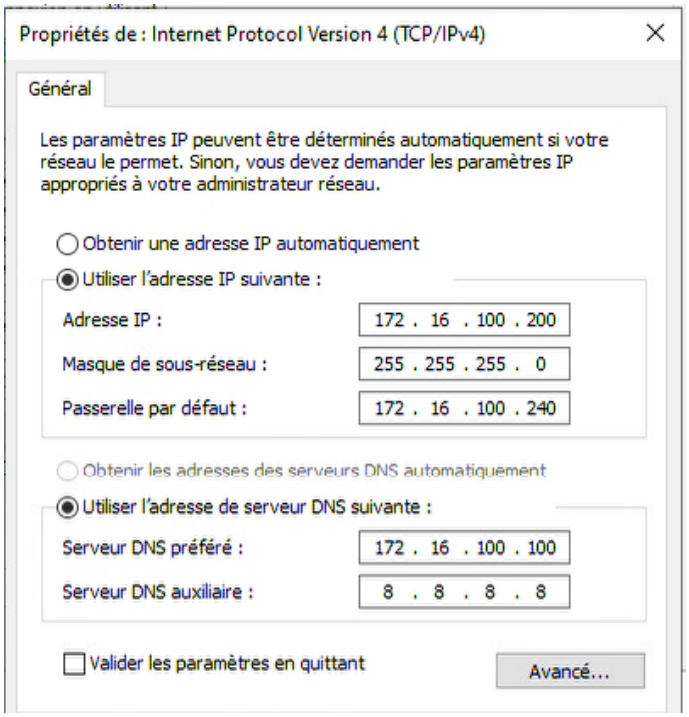

Figure 4.24 – Définir l'adresse IP statique du serveur 2.

Pour promouvoir ce serveur en contrôleur de domaine, Nous allons sélectionner : « Ajouter un contrôleur de domaine à un domaine existant » → spécifier le nom de domaine « TOUDJA » → attribuer un mot de passe → Nous allons indiquer que la réplication se fait depuis le premier serveur, puis lancer l'installation.

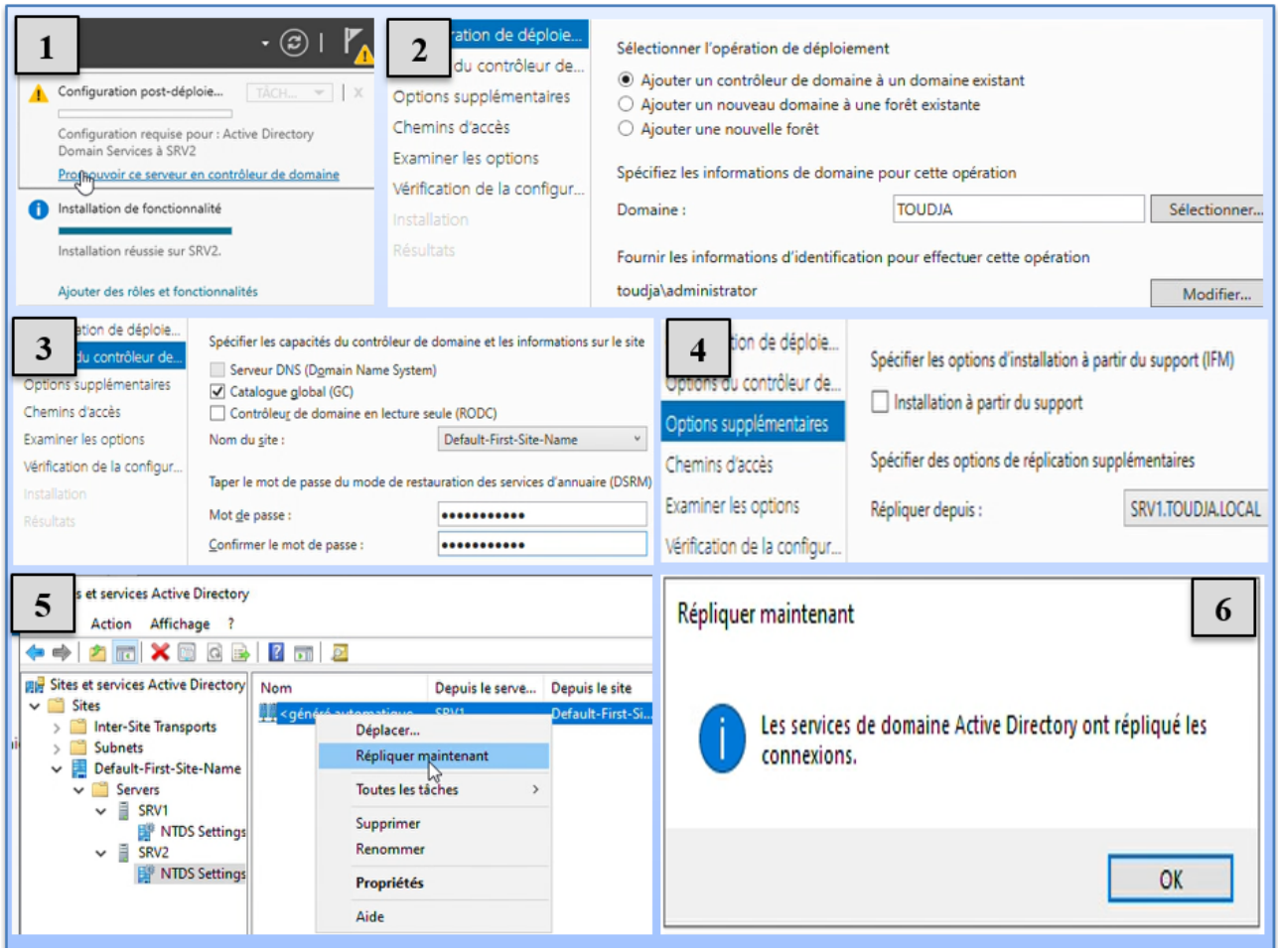

Figure 4.25 – Réplication de l'Active Directory dans le Serveur 2.

❖ Synchronisation

Une fois que le serveur 2 est ajouté au domaine «TOUDJA.LOCAL», on ajoute le serveur « SRV1 » a «SRV2» pour pouvoir l'administrer. Comme illustré dans la figure :

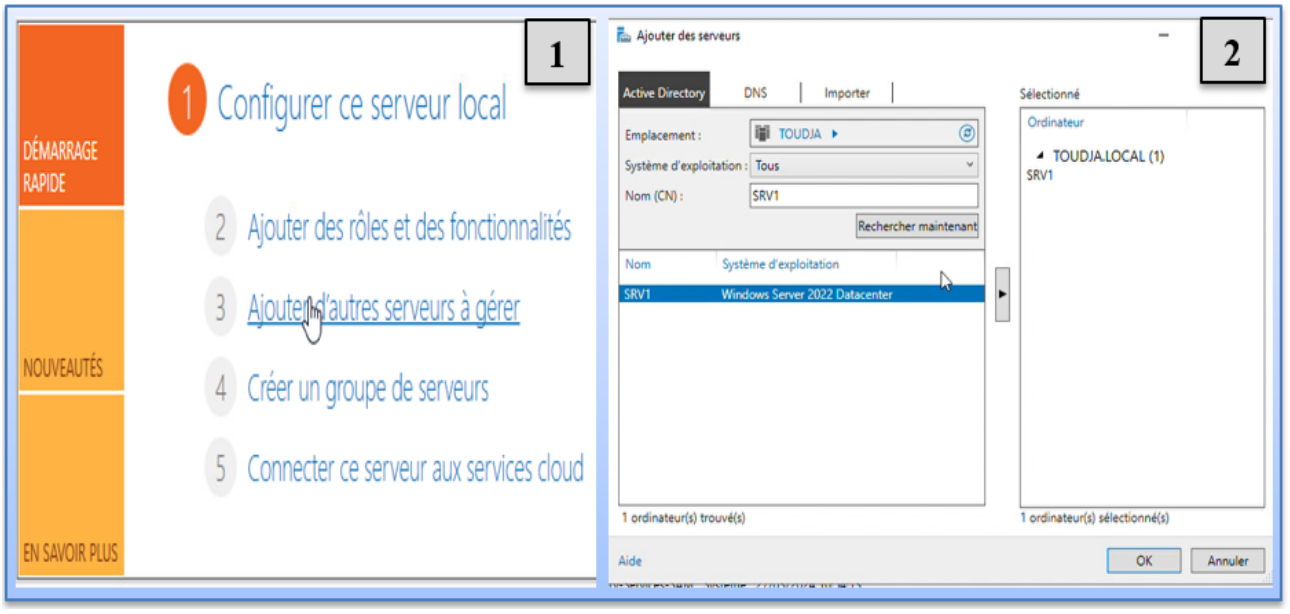

Figure 4.26 – Synchronisation de Serveur 2.

❖ Réplication du DHCP

Pour autoriser le Serveur 1 de gérer le Serveur 2, on doit passer par les étapes suivantes : Cliquant sur outils → DHCP → un clic droit sur IPv4 puis choisir configurer un basculement → spécifier le serveur partenaire à utiliser pour le basculement « srv2 » → créer une relation de basculement avec le serveur partenaire sous le nom : srv1.toudja.local-srv2, et on termine.

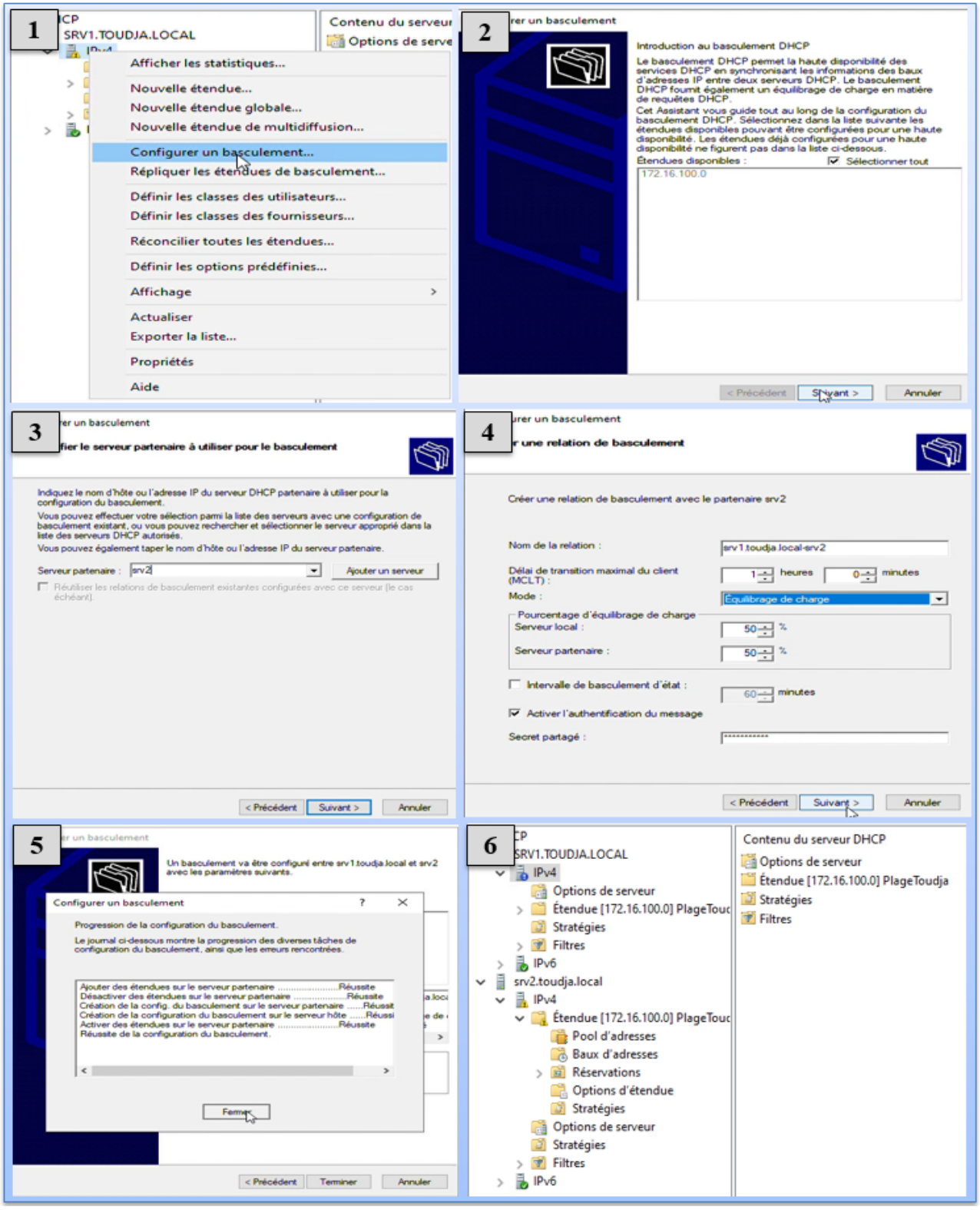

Figure 4.27 – Création de l'étendu dans le Serveur2.

4.3.5.6 Mise en œuvre des stratégies de groupe et des stratégies de sécurité

La stratégie de groupe et la sécurité sont essentielles pour maintenir la sûreté et l'intégrité des systèmes informatiques au sein d'une organisation. Elle permet de définir des règles et des paramètres pour les utilisateurs, les ordinateurs et les groupes d'utilisateurs au sein d'un réseau. Ces règles peuvent inclure des restrictions de sécurité, des politiques de mot de passe, des autorisations de fichiers, des restrictions logicielles et la configuration de l'écran de veille, entre autres.

Pour créer des GPO (Group Policy Object), nous devons d'abord créer des groupes. Ces groupes permettent d'appliquer des règles et des paramètres similaires à des types d'utilisateurs identiques, cela simplifie l'administration des comptes en nous permettant d'attribuer des autorisations et des droits à des groupes d'utilisateurs plutôt qu'à chaque utilisateur individuel.

❖ **Configuration d'une stratégie pour empêcher l'écriture d'USB**

Le but d'empêcher l'écriture sur les clés USB est de réduire le risque de propagation de logiciels malveillants tels que les virus et les malwares via ces périphériques. De plus, cela permet d'éviter que des données sensibles soient copiées sur des clés USB et emportées hors du réseau de l'entreprise.

Pour configurer cette stratégie, on va suivre les étapes ci-dessous :

- Dans le « Gestionnaire de serveur », on clique sur « Outils ». Dans la liste qui s'affiche, on sélectionne « Gestion de stratégie de groupe ».
- On fait un clic droit sur le domaine « TOUDJA.LOCAL » et on choisit de créer un objet GPO. On nomme cet objet « Empêcher l'écriture d'USB ».
- Ensuite, on va configurer les paramètres. Pour ce faire, on fait à nouveau un clic droit sur l'objet créé, puis on clique sur « Modifier ».
- Dans la fenêtre affichée, on suit le chemin suivant : « Stratégies » → « Directives » → « Modèles d'administration » → « Accès au stockage amovible ».
- On double-clique sur « Disques amovibles : refuser l'accès en écriture ». Il suffit de cocher la case « Activé » pour que la restriction soit effective. Ensuite, on clique sur « Appliquer », puis sur « OK » pour enregistrer les modifications.

La configuration de cette stratégie est illustrée dans la figure suivante :

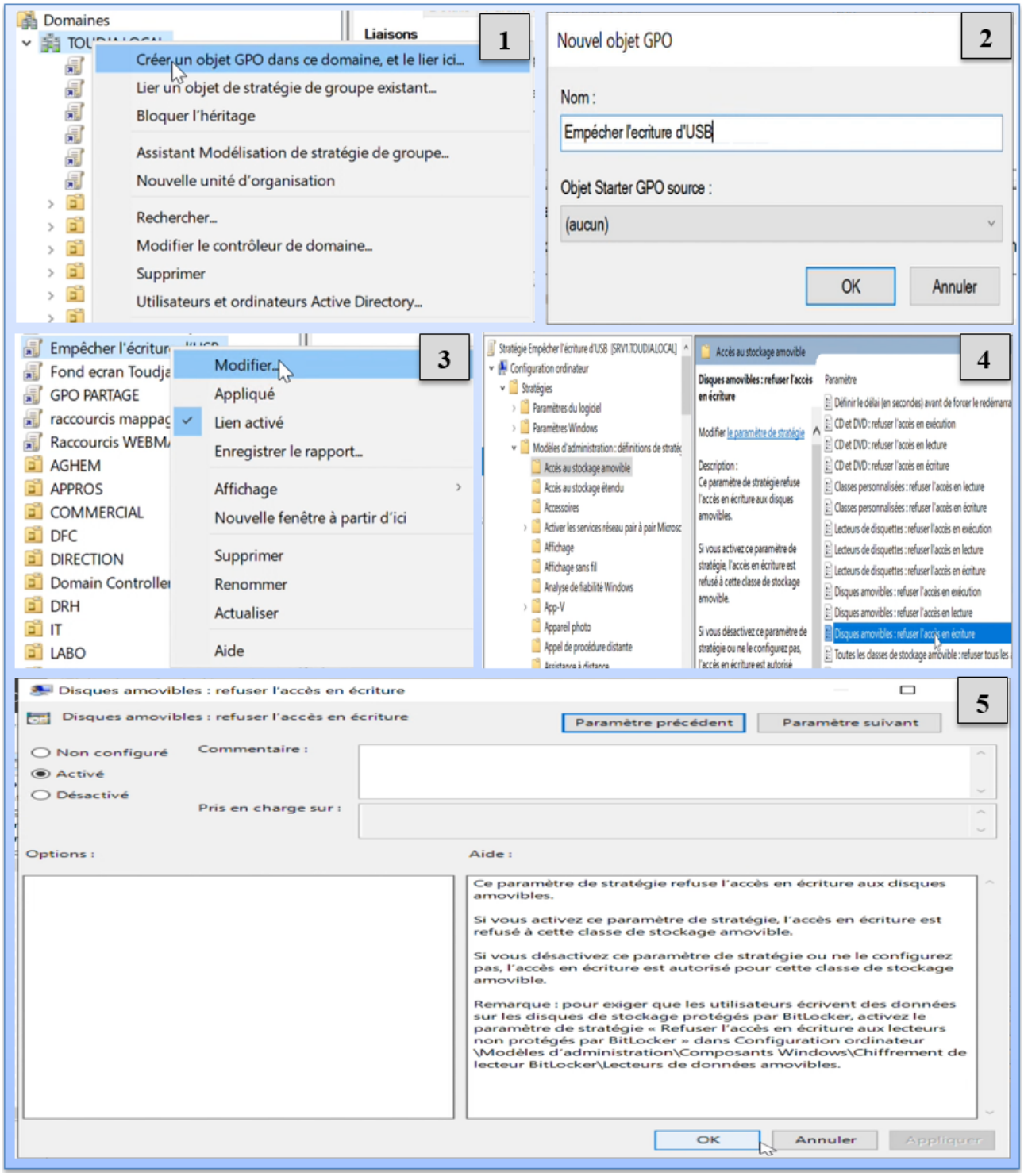

Figure 4.28 – Configuration d'une stratégie pour empêcher l'écriture d'USB.

Pour que le serveur prenne en compte plus rapidement cette stratégie, on va exécuter la commande gpupdate /force dans le terminal. Ensuite, on se connectera en tant qu'utilisateur pour tester le fonctionnement de la stratégie de groupe.

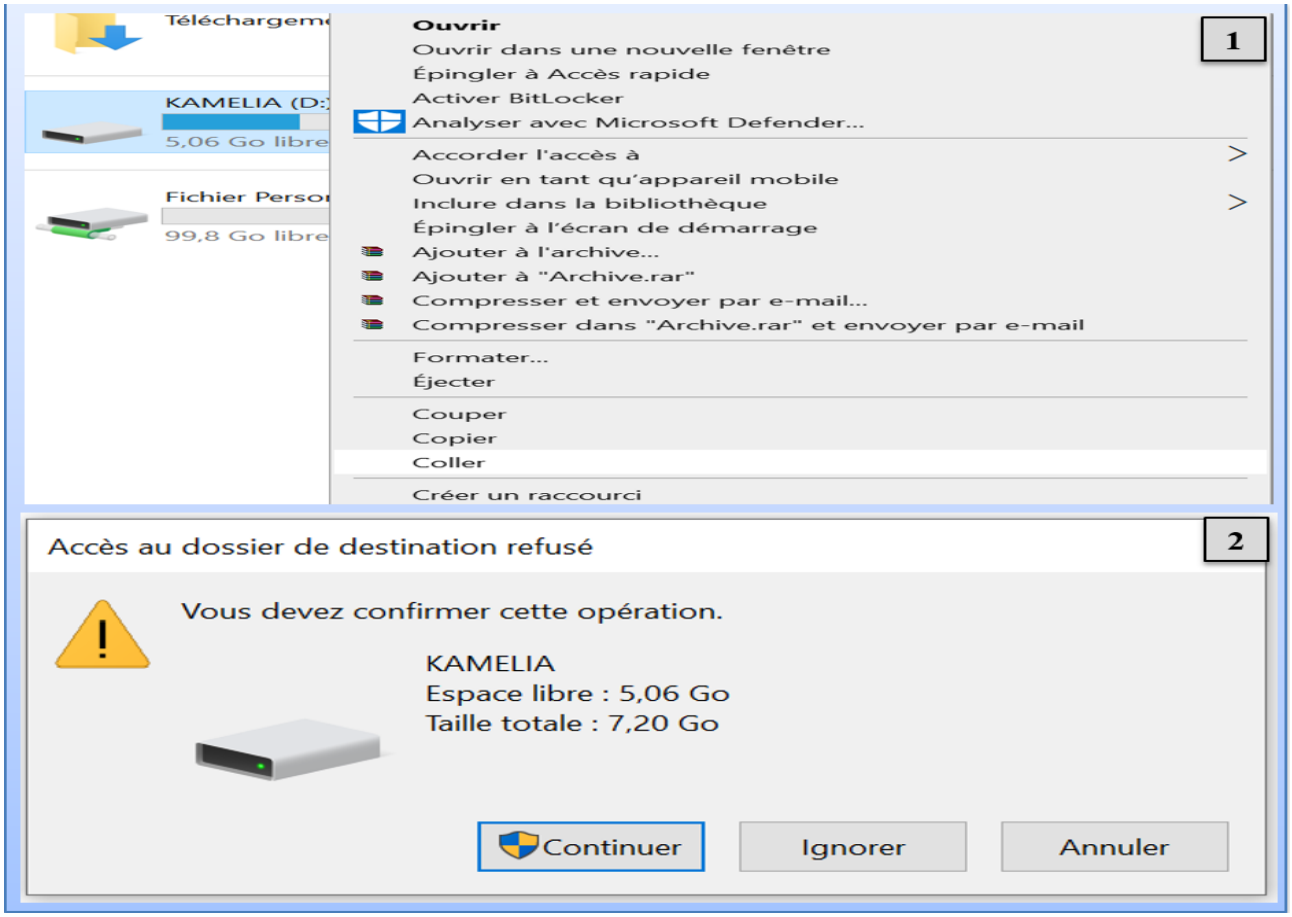

Figure 4.29 – Test de la restriction de l'écriture d'USB.

Nous voyons sur la figure que l'utilisateur ne peut pas copier les données sur la clé USB, car il ne dispose pas des droits d'écriture sur cette clé.

4.3.6 Configuration du VPN (OpenVPN)

4.3.6.1 Configuration du VPN multi-sites OpenVPN

Pour connecter plusieurs sites distants à un site principal, la première chose à faire est de définir le site principal comme « serveur » et les sites distants comme « clients ». Dans notre cas le serveur est le site de Bejaia, et les clients sont : site de « SET Toudja », site « GB d'El Kseur » et site « Unilait d'El Kseur ».

1. Configuration du serveur

Pour configurer le serveur, on va suivre les étapes suivantes :

D'abord, on va spécifier le mode site à site (peer to peer) avec une clé partagée et on va choisir UDP comme protocole et Tun pour spécifier que les données seront transmises via un tunnel par le port 1194. Une fois que la configuration aura été sauvegardée, une clé sera automatiquement créée et copiée sur l'interface du client. Par la suite, on va spécifier l'interface WAN qui doit

être utilisée pour accéder au serveur OpenVPN.

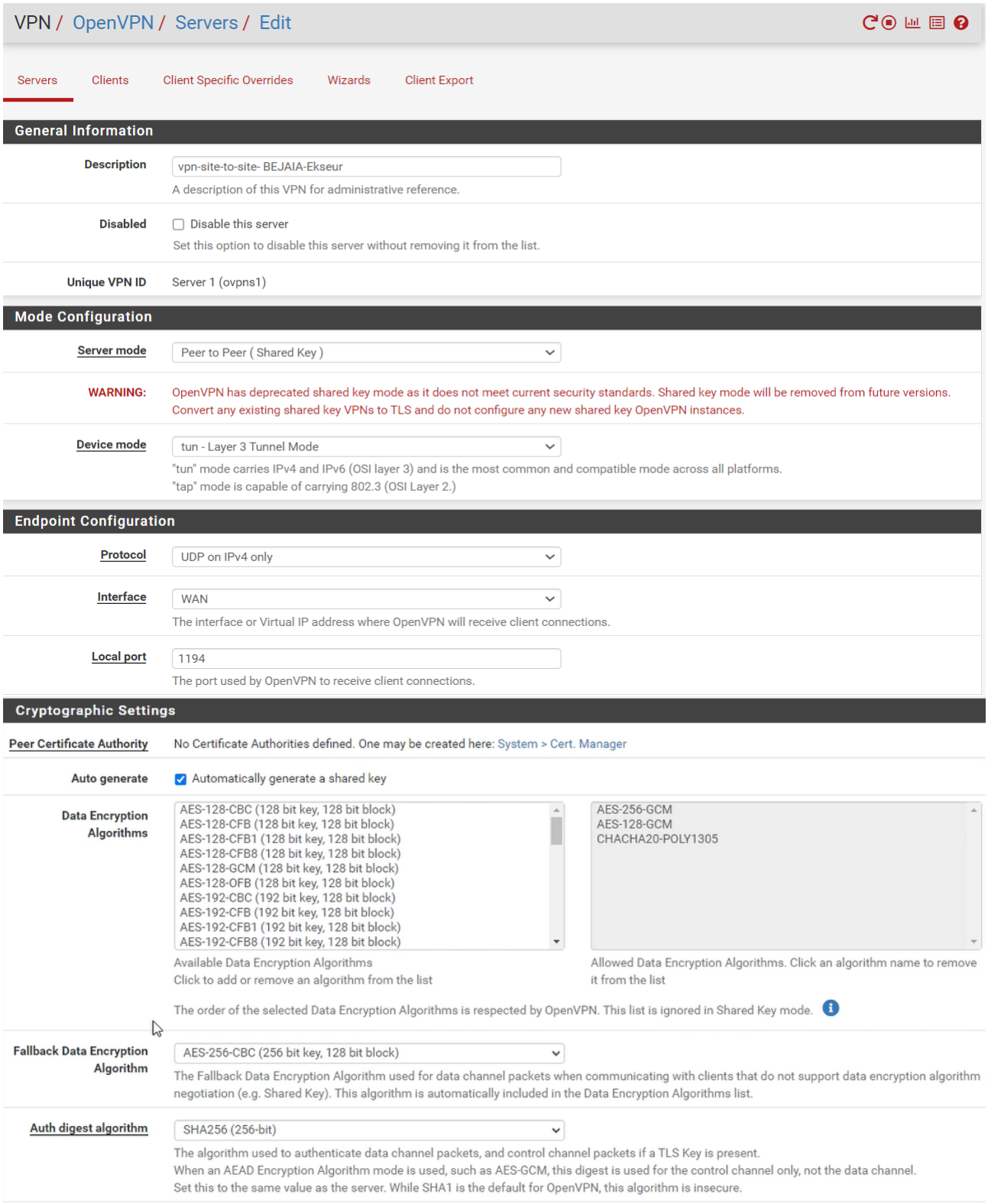

Figure 4.30 – Configuration du serveur et génération de la clé.

Pour créer une connexion entre les deux sites, nous allons attribuer les adresse suivantes sur notre serveur :

- 10.10.10.0/24 : un tunnel VPN, par lequel les données seront transmises entre les deux

sites.

- 192.168.0.0/24 : réseau LAN du site GB El Kseur.

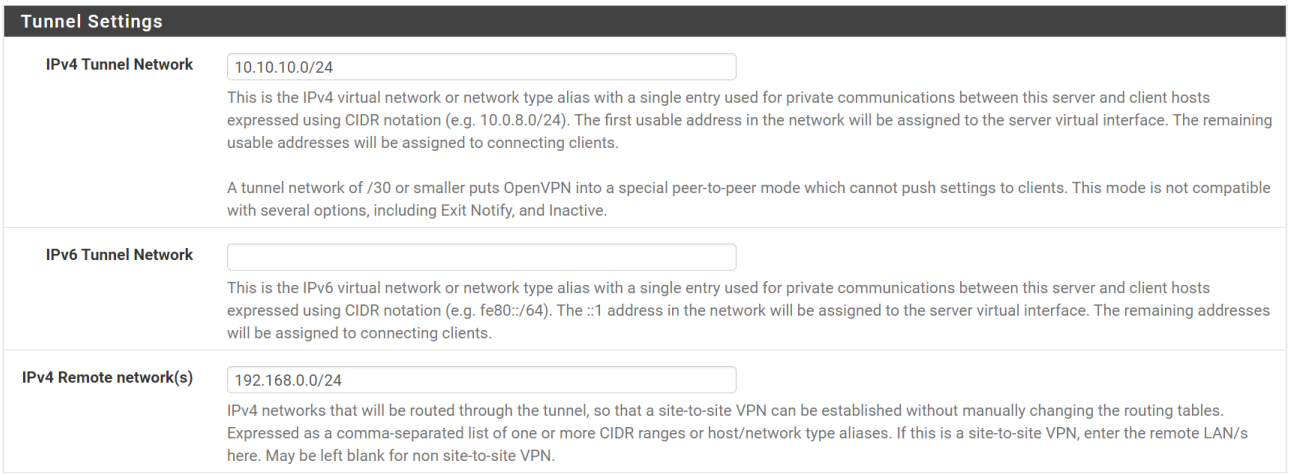

Figure 4.31 – Configuration du serveur.

Dans la zone “Custom options” on va indiquer l’option push "route". Cette directive permet de spécifier des routes pour les clients VPN.

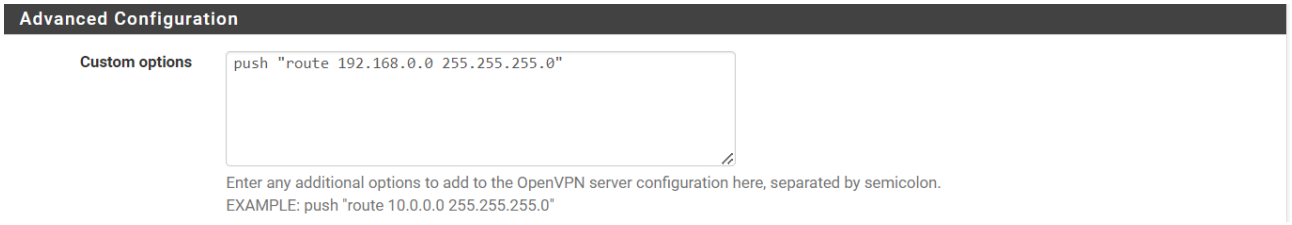

Figure 4.32 – Configuration avancée.

De la même façon on a créé les trois serveurs OpenVPN de Bejaia, Comme illustré dans la figure :

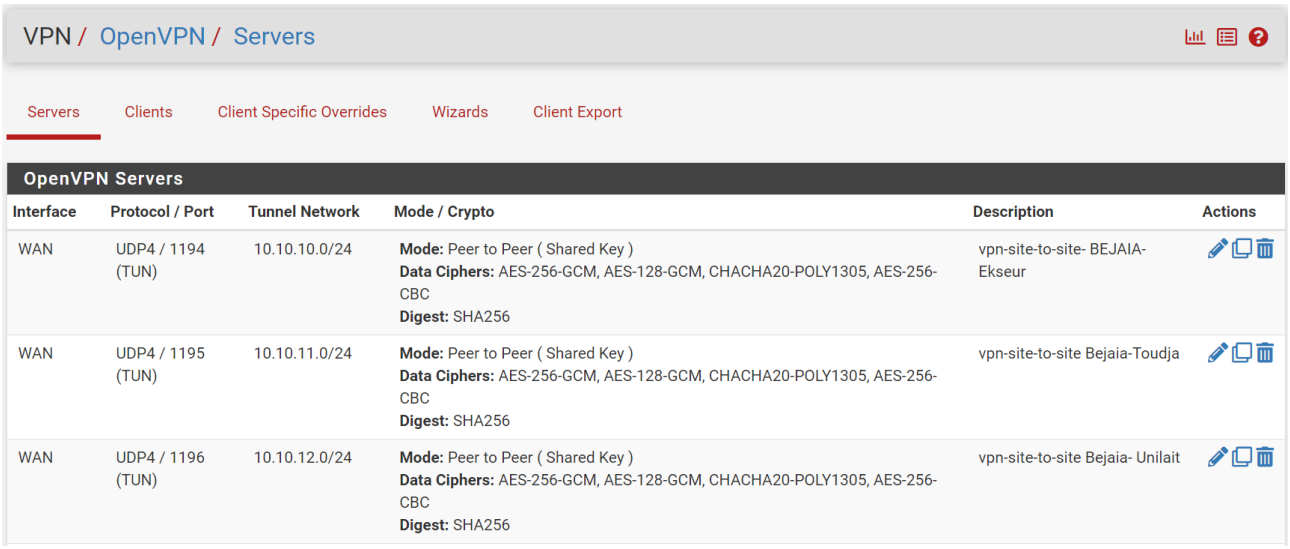

Figure 4.33 – Serveurs OpenVPN de Bejaia.

❖ Interface WAN

Pour créer la première règle nous allons remplir les champs de la manière suivante :

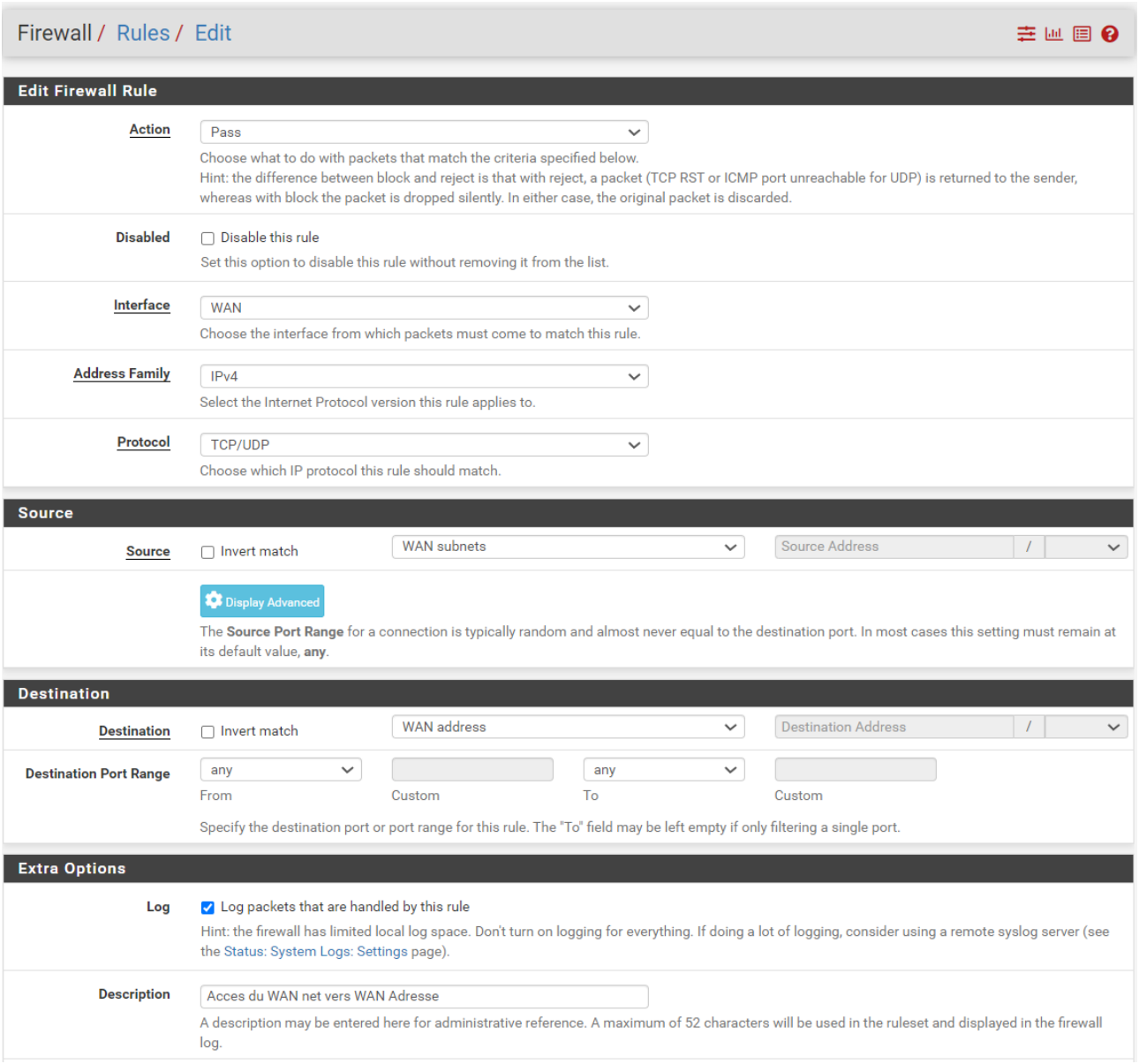

Figure 4.34 – Création des règles de filtrage.

De la même façon, nous avons créé toutes les règles comme illustrer dans la figure 4.35

- La première règle autorise le trafic provenant des sous-réseaux WAN, utilisant à la fois TCP et UDP, et destiné à l'adresse IP WAN de votre pare-feu, d'accéder depuis n'importe quel port.
- La deuxième règle autorise le trafic provenant de n'importe quelle source et n'importe quel port, utilisant UDP comme protocol et destiné à l'adresse IP WAN, mais uniquement sur les ports suivants :
  - Le port 1194 : pour le site GB El Kseur.

- Le port 1195 : pour le site SET Toudja.
- Le port 1196 : pour le site Unilait El Kseur.
- Le port 1197 : pour le VPN client à site.

- La troisième règle autorise tout trafic ICMP (ping, par exemple) provenant de n'importe quelle source et de n'importe quelle destination, sans restriction de port.

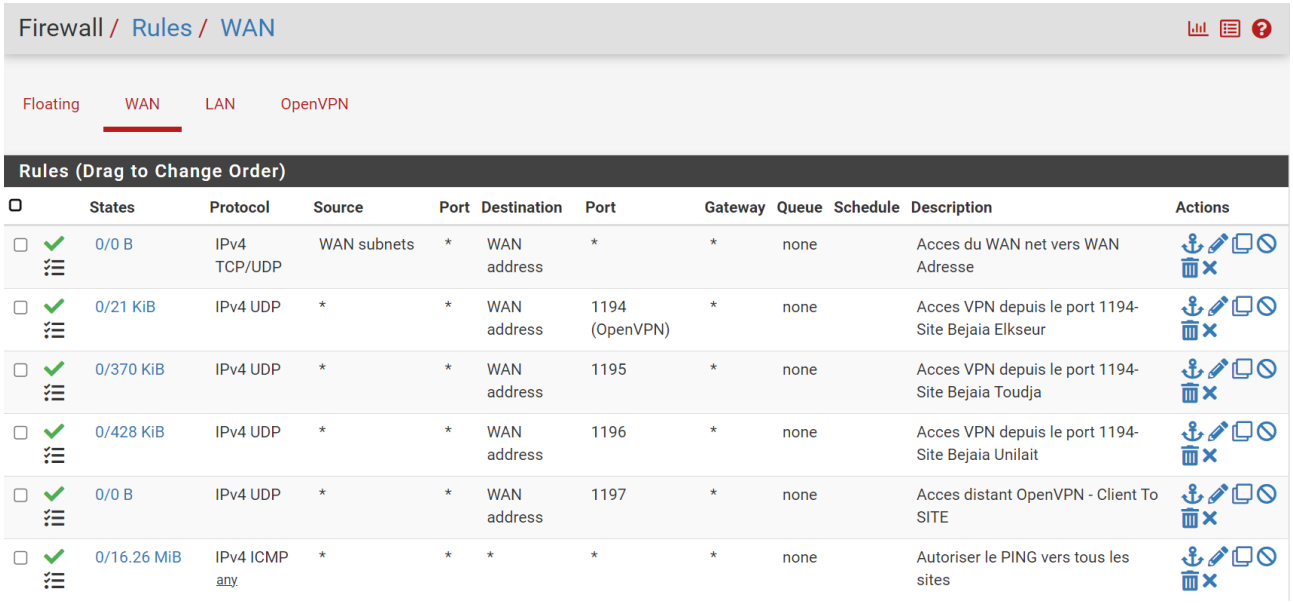

Figure 4.35 – Les règles crées.

❖ Tunnel OpenVPN

Cette règle autorise le trafic de tous les paquets IPv4.

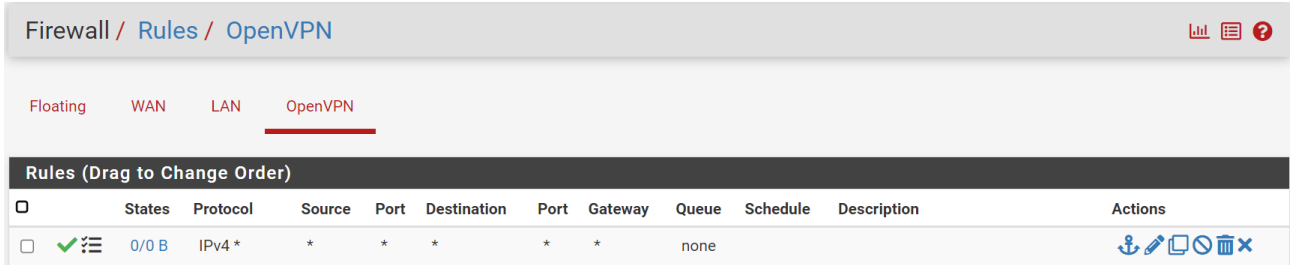

Figure 4.36 – Configuration des règles de filtrage du Tunnel.

2. Configuration des clients

De la même façon que le serveur, on va spécifier le mode site à site (peer to peer) en utilisant une clé partagée et on va opter pour UDP comme protocole et Tun pour spécifier que les données seront transmises via un tunnel par le port 1194 et on va sélectionner l'interface WAN pour permettre l'accès.

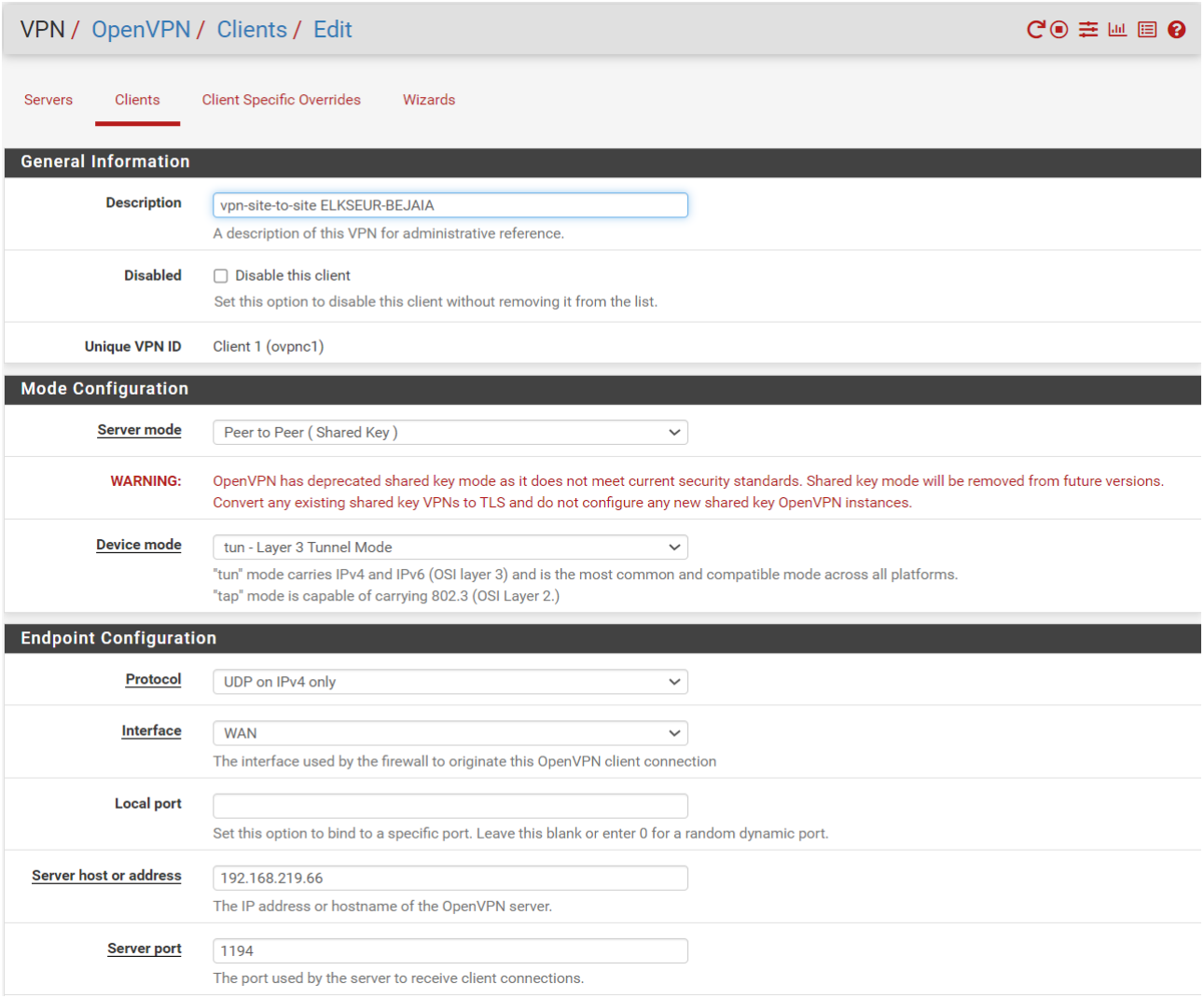

Figure 4.37 – Configuration du client.

Maintenant on va insérer la clé produite par le serveur dans le champ “clé partagée” du client.

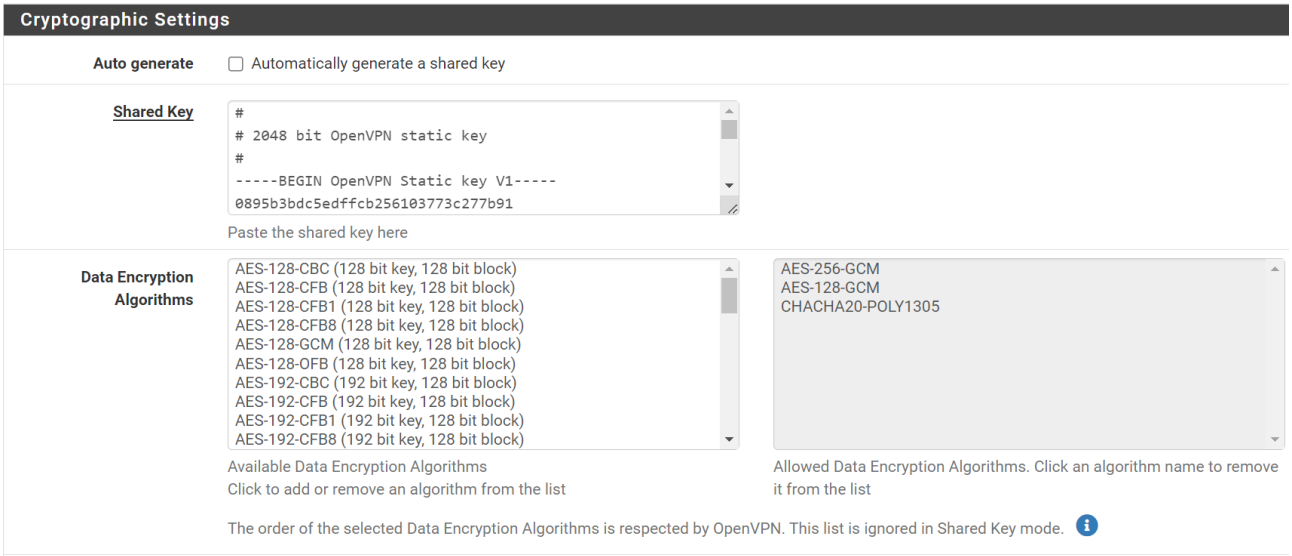

Figure 4.38 – Insertion de la clé partagée.

Pour terminer, on va définir les adresses suivantes :

- 10.10.10.0/24 : un tunnel VPN, par lequel les données seront transmises entre les deux sites.
- 172.16.100.0/24 : réseau LAN du site Bejaia.

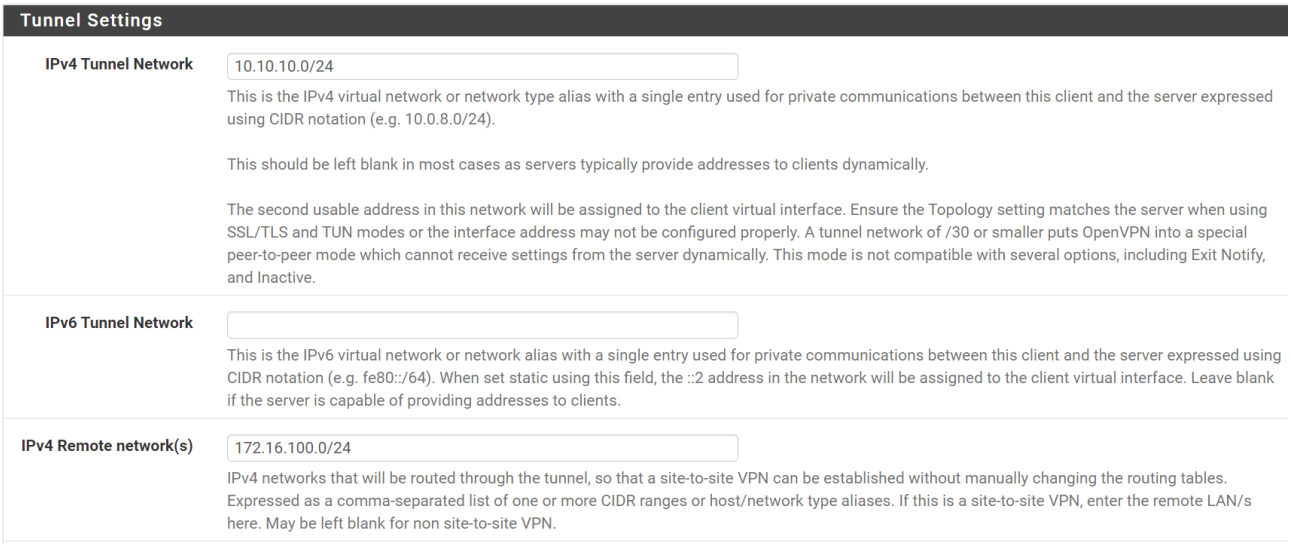

Figure 4.39 – Configuration du tunnel.

Le client a été bien créé, comme il est montré dans cette figure :

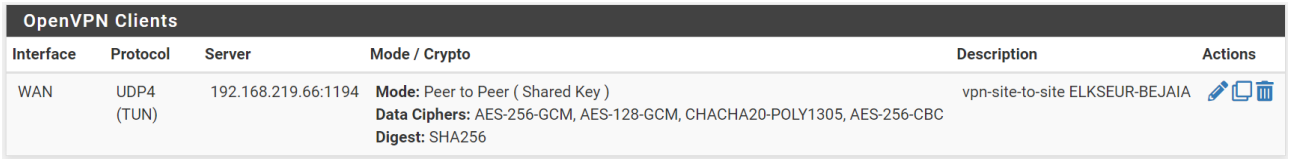

Figure 4.40 – Client de GB El Kseur.

De la même façon on a créé les trois clients OpenVPN, Comme illustré dans les figures :

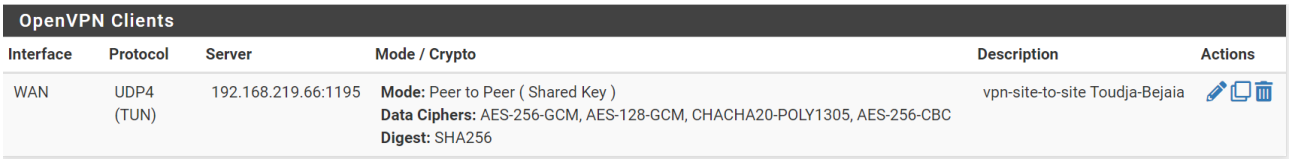

Figure 4.41 – Client de SET Toudja.

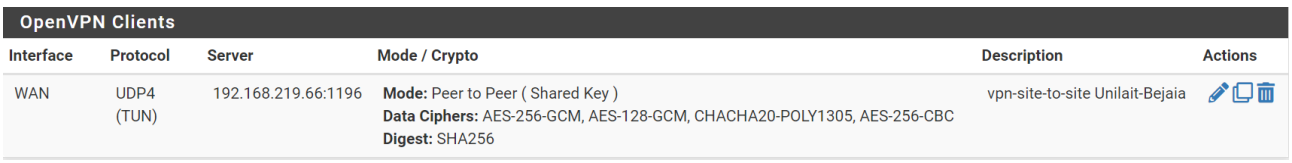

Figure 4.42 – Client de Unilait El Kseur.

❖ Interface WAN

Nous avons créé les mêmes règles que le serveur, sauf que nous avons associé les règles de chaque unité en fonction de leurs ports. Les règles sont illustrées dans les figures suivantes :

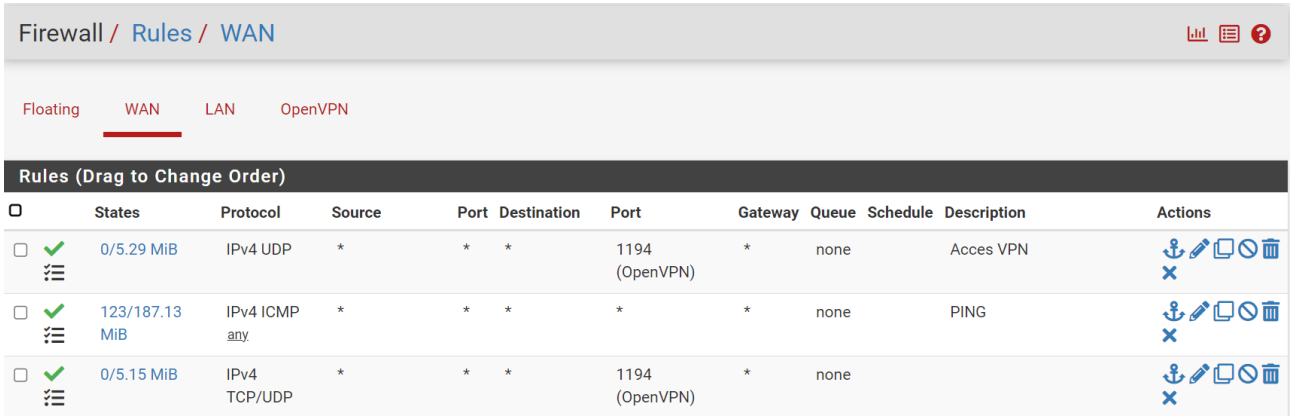

Figure 4.43 – Les règles de filtrage du site GB El Kseur.

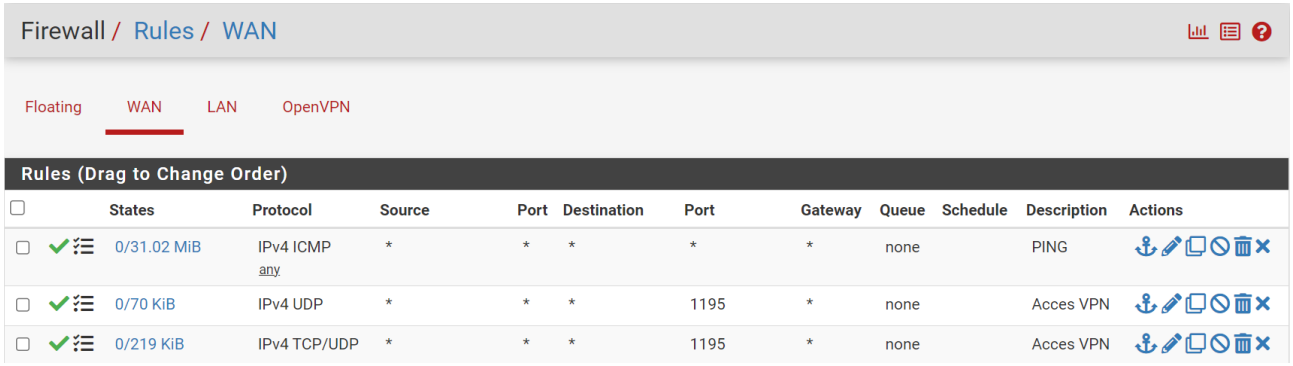

Figure 4.44 – Les règles de filtrage du site SET Toudja.

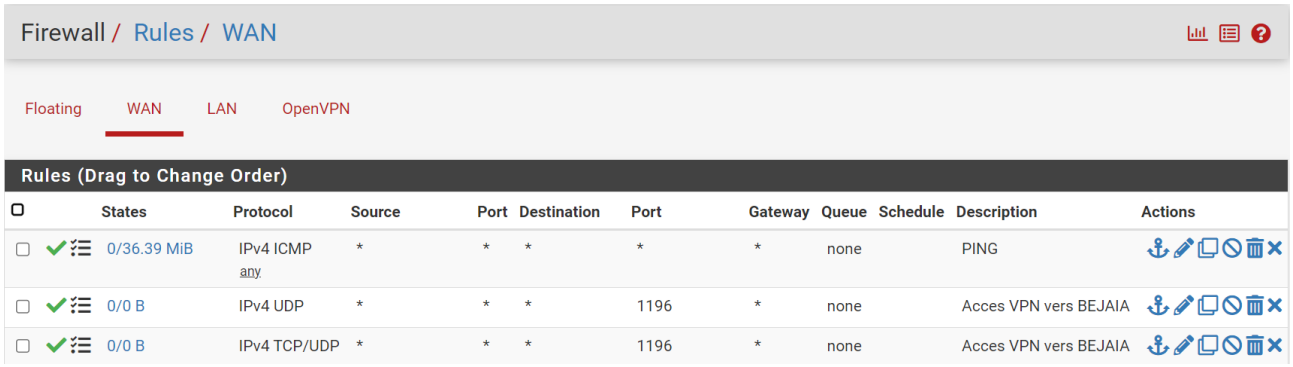

Figure 4.45 – Les règles de filtrage du site Unilait El Kseur.

❖ **Tunnel OpenVPN**

Cette règle autorise le trafic de tous les paquets IPv4.

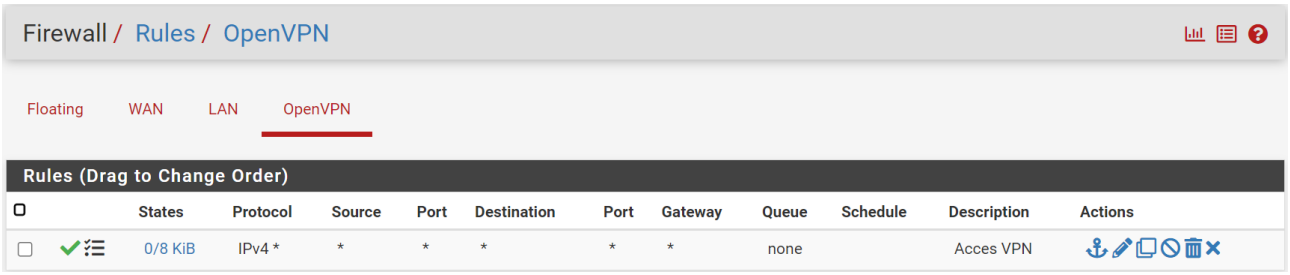

Figure 4.46 – Configuration des règles de filtrage du tunnel.

4.3.6.2 Configuration du VPN client à site OpenVPN

1. La gestion des certificats

Dans un premier temps, il est nécessaire de créer une autorité de certification interne pour le PfSense puis nous allons créer un certificat dédié au serveur. Notre tunnel VPN sera sécurisé grâce à l'utilisation de ce certificat.

❖ **Création de l'autorité de certification**

Dans l'onglet "Authorities", nous appuyons sur le bouton "Add" situé en bas à droite de la liste des certificats déjà existants.

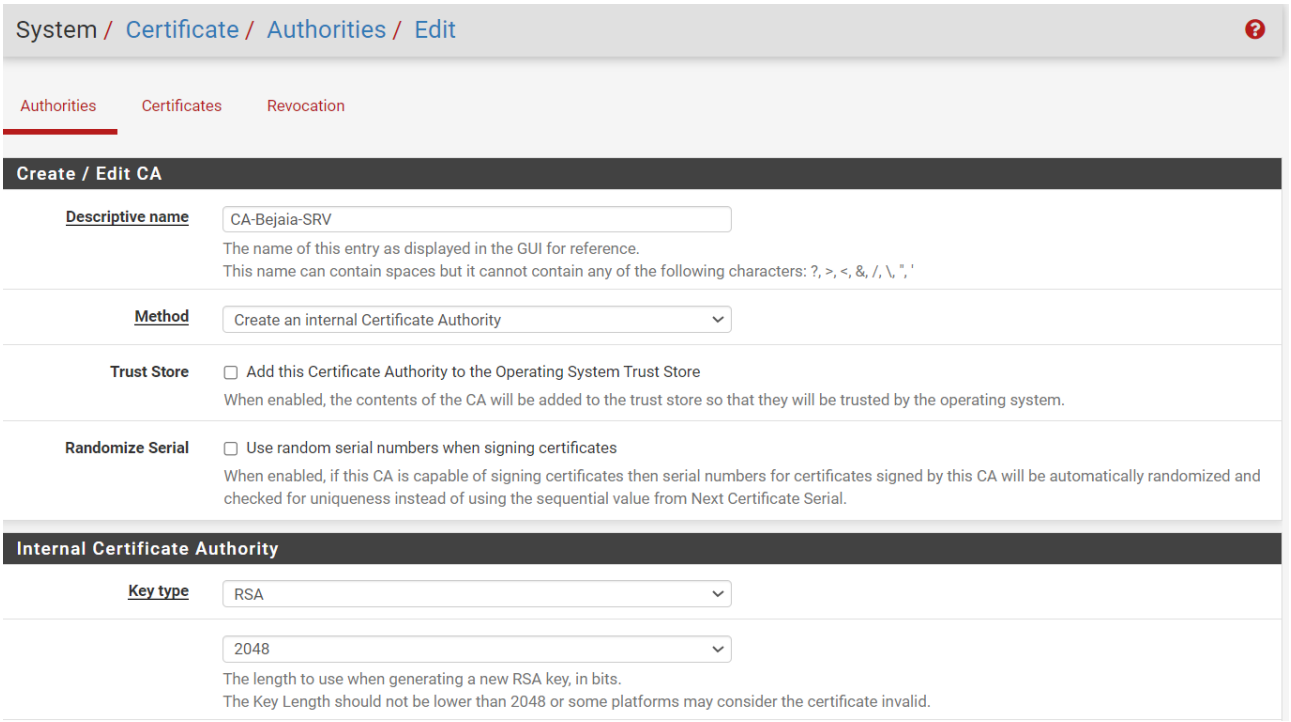

Figure 4.47 – Création d'un certificat autorité (CA).

Voilà, le certificat de l'autorité de certification :

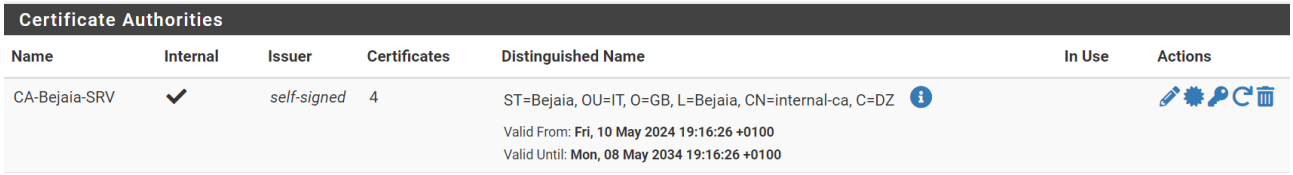

Figure 4.48 – Le certificat crée.

❖ Création du certificat du Serveur

Une fois le certificat d'autorité créé, on doit créer un autre pour le serveur VPN. On clique donc sur "certificates", ensuite "Add / Sign'.

Puis on va remplir les champs avec les informations qui correspondent à nos besoins comme nous l'avons vu lors de la création de certificat de l'autorité de certification. Et voilà, le certificat du serveur VPN est créé.

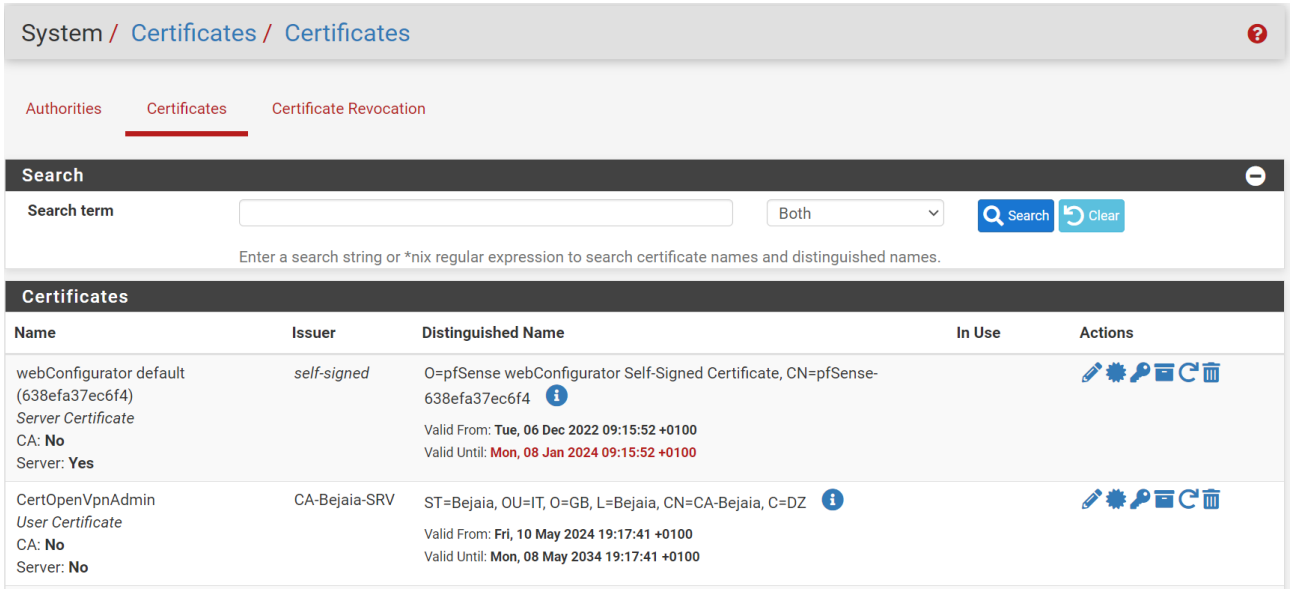

Figure 4.49 – Certificat du serveur VPN.

2. Configuration du serveur OpenVPN

Après avoir créé les certificats, nous pouvons commencer à configurer le VPN. Dans l'onglet "Servers", on clique sur "Add" afin de créer une nouvelle configuration.

D'abord, on va spécifier le mode Remote Access (SSL/TLS + User Auth), dans le champs "Backend for authentification" on va séléctionner l'authentification LDAP et la base locale, puis on va choisir UDP comme protocole et Tun pour spécifier que les données seront transmises via un tunnel par le port 1197. Pour l'interface, on va conserver "WAN" puisque c'est bien par cette interface que l'on va se connecter en accès distant.

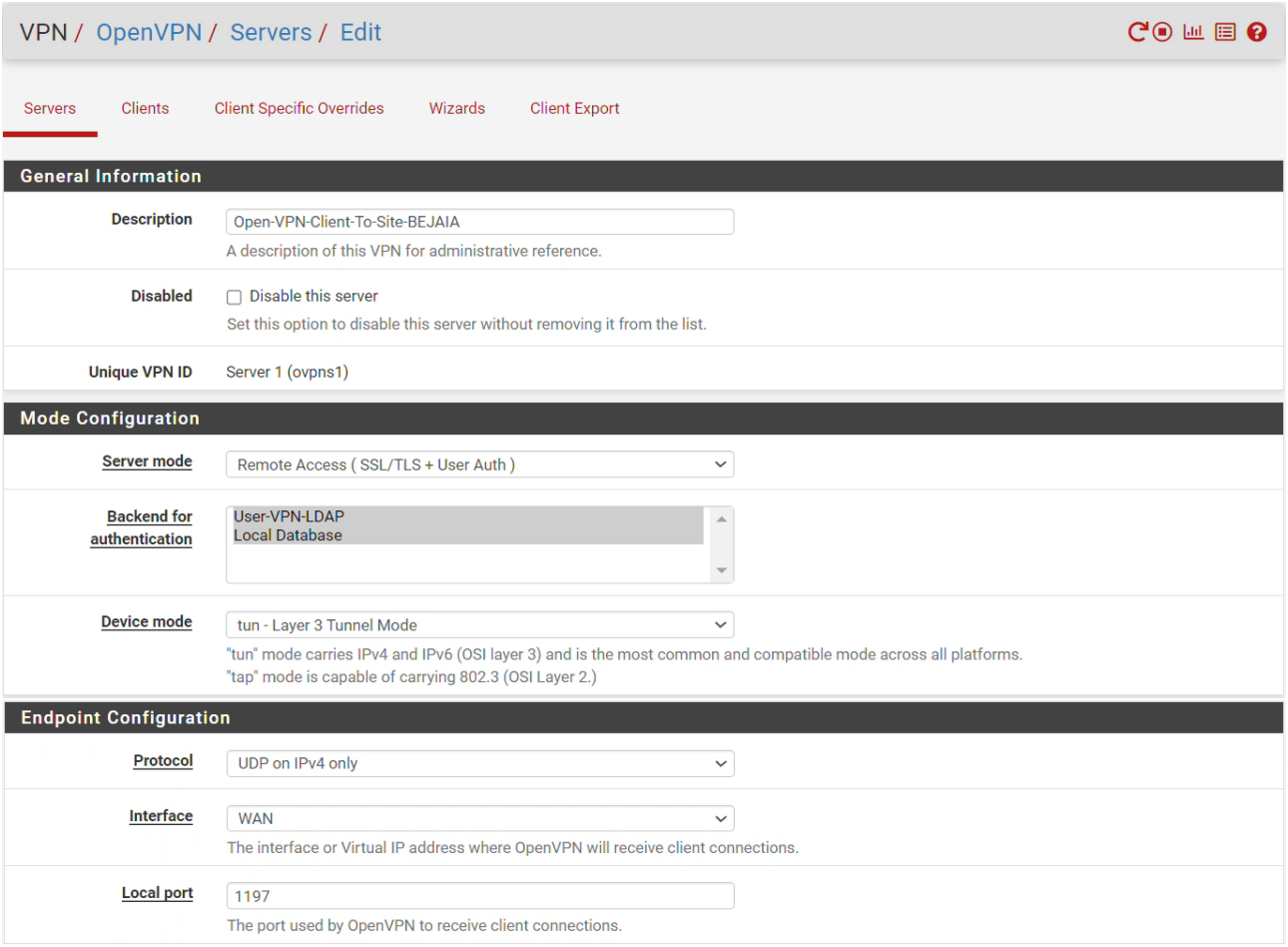

Figure 4.50 – Configuration du serveur.

Dans cette partie, on va sélectionner l'autorité de certification au niveau du champ "Peer Certificate Authority". Puis, on va sélectionner le certificat Server au niveau du champ "Server certificate".

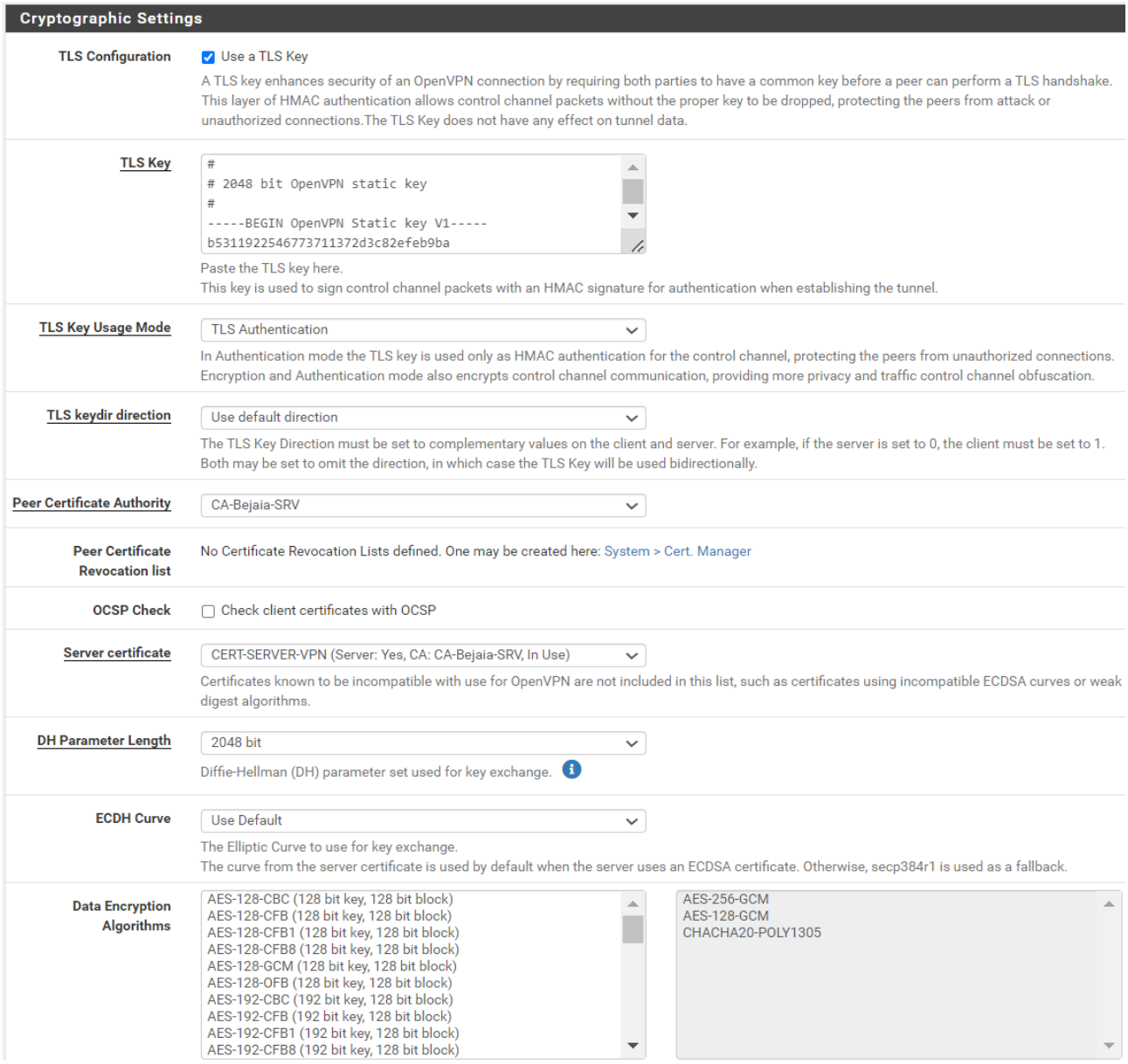

Figure 4.51 – Le choix de l'autorité de certification et certificat serveur.

Pour l'algorithme de chiffrement (Encryption Algorithm), nous pouvons passer sur de l'AES-256-CBC pour renforcé la sécurité.

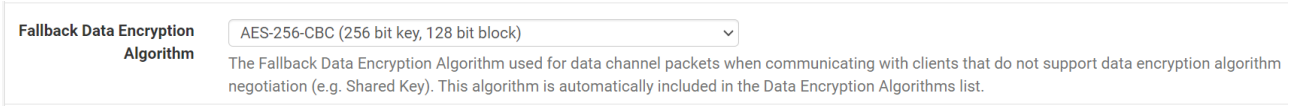

Figure 4.52 – Algorithme de chiffrement.

Maintenant on va passer à la configuration de notre tunnel VPN :
IPv4 Tunnel Network : adresse du réseau VPN, c'est-à-dire que lorsqu'un client va se connecter en VPN il va obtenir une adresse IP dans ce réseau au niveau de la carte réseau locale du PC. Par la suite, on va activer l'option Redirect IPv4 Gateway pour que tous les paquets de données générés par votre ordinateur client soient envoyés via le tunnel VPN.

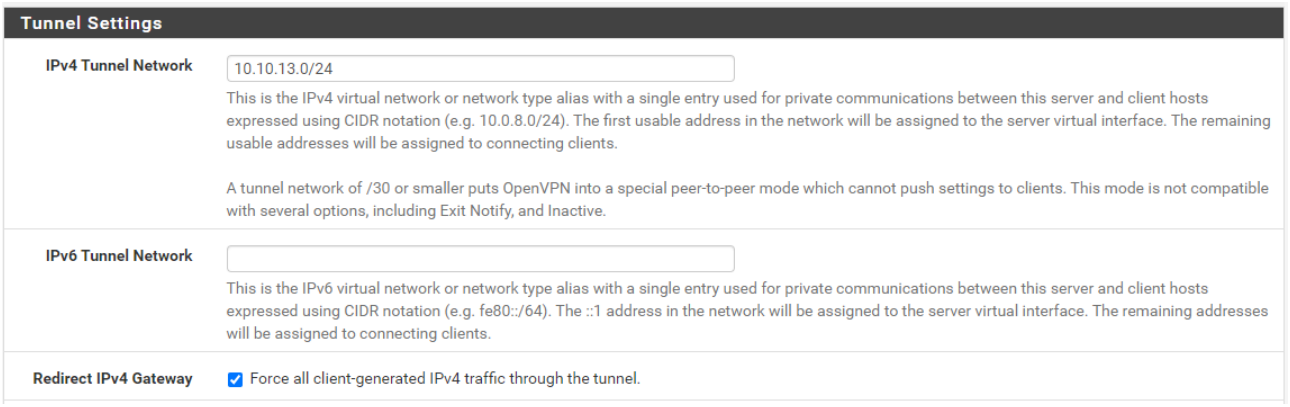

Figure 4.53 – Configuration du tunnel.

Pour les paramètres des clients on va activer l'option "Dynamic IP" : si l'adresse IP publique d'un client change, il pourra maintenir sa connexion VPN.

Au niveau de la topologie, on va utiliser la configuration net30 - isolated /30 network per client. Cette configuration permet à chaque client d'être isolé dans un sous-réseau de la plage réseau VPN, empêchant ainsi les clients de communiquer entre eux.

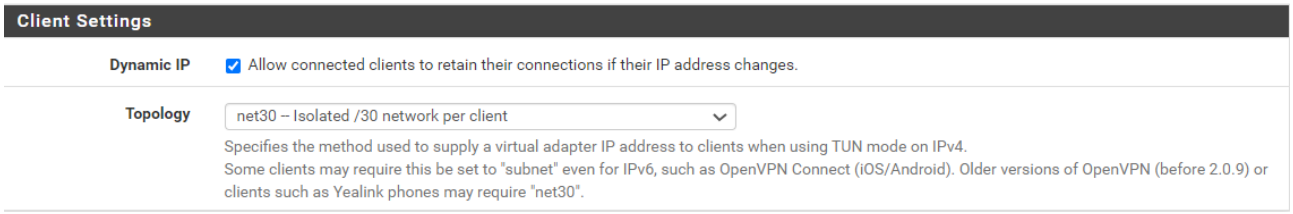

Figure 4.54 – Paramètres des clients.

On va cocher les options suivantes :

- "Provive a default domain name to clients" pour indiquer le nom de domaine local.
- "Provide a DNS server list to clients. Pour pouvoir utiliser la résolution DNS interne de notre entreprise puis on va indiquer en dessous les adresses IP de vos serveurs DNS.

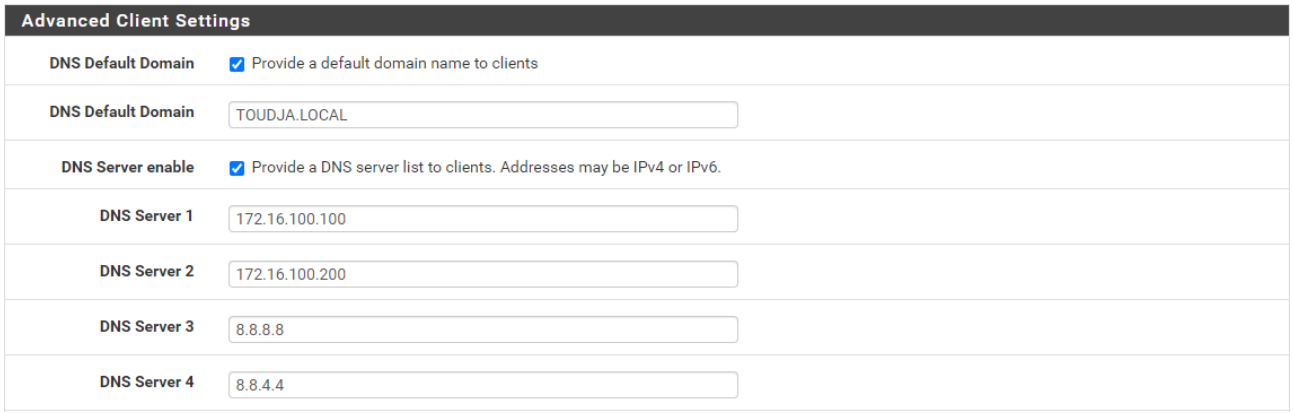

Figure 4.55 – Paramétres des clients avancés.

Dans la zone “Custom options” on va indiquer l’option push "route"n qui permet de spécifier des routes pour les clients VPN.

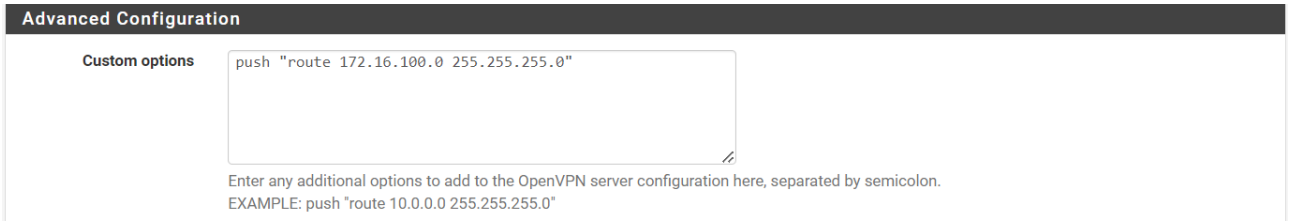

Figure 4.56 – Configuration avancé.

Le serveur crée est montrée dans la figure suivante :

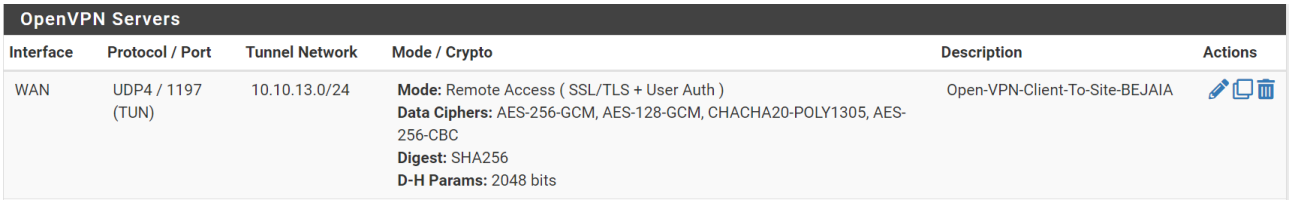

Figure 4.57 – Le serveur créé.

3. Création des utilisateurs

a.Création des utilisateurs de la base locale

Pour créer un nouvel utilisateur : dans l’onglet Users cliqué sur «Add », puis on va remplir les champs comme il est illustré dans la figure suivante :

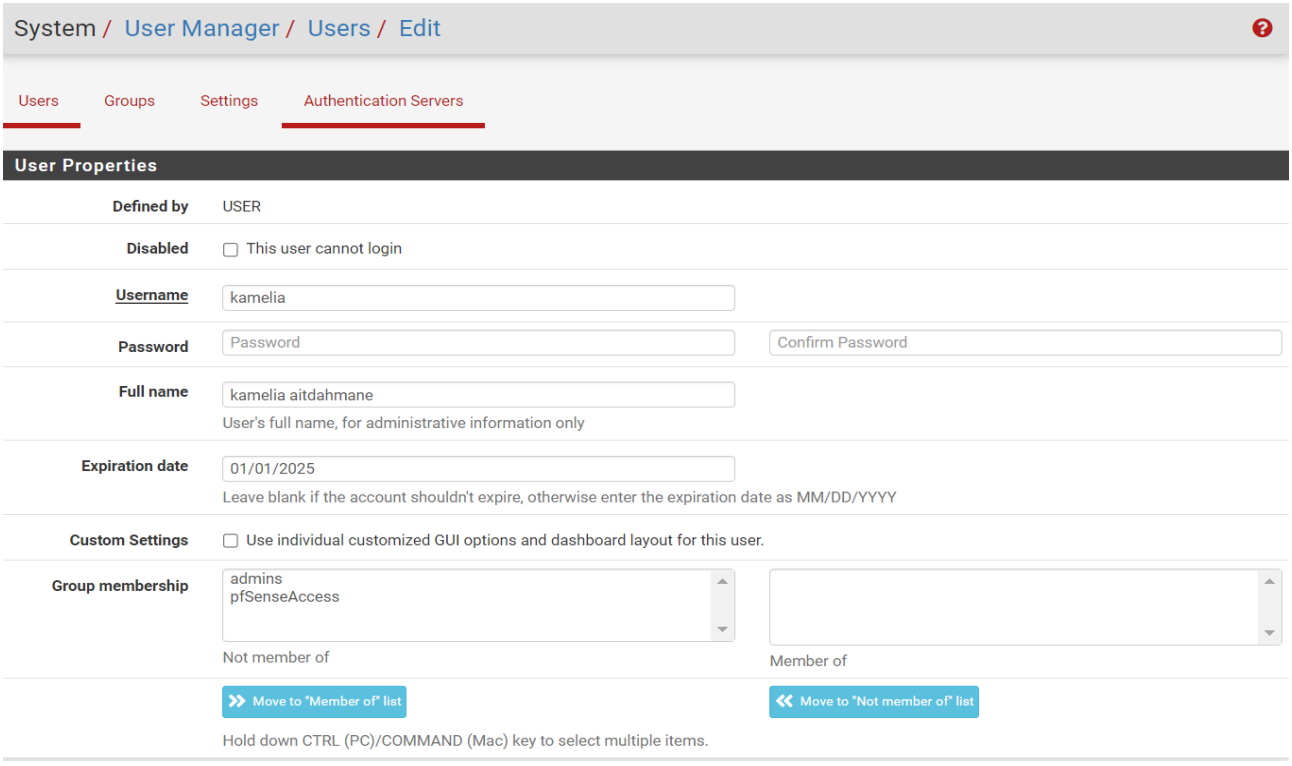

Figure 4.58 – Les informations de l’utilisateur.

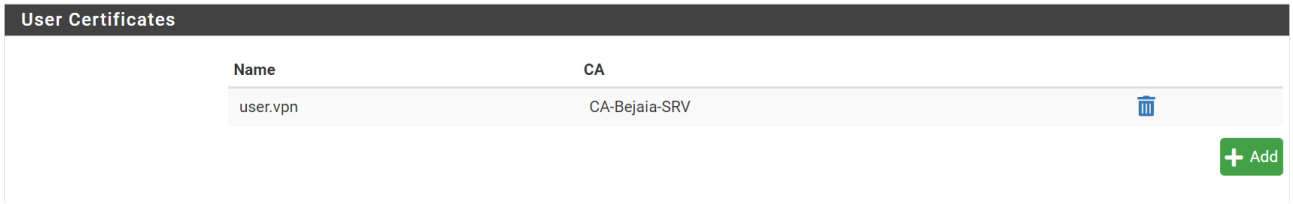

Figure 4.59 – Certificat utilisé pour l'utilisateur.

Lorsque l'utilisateur est créé, il apparaît dans la base locale :

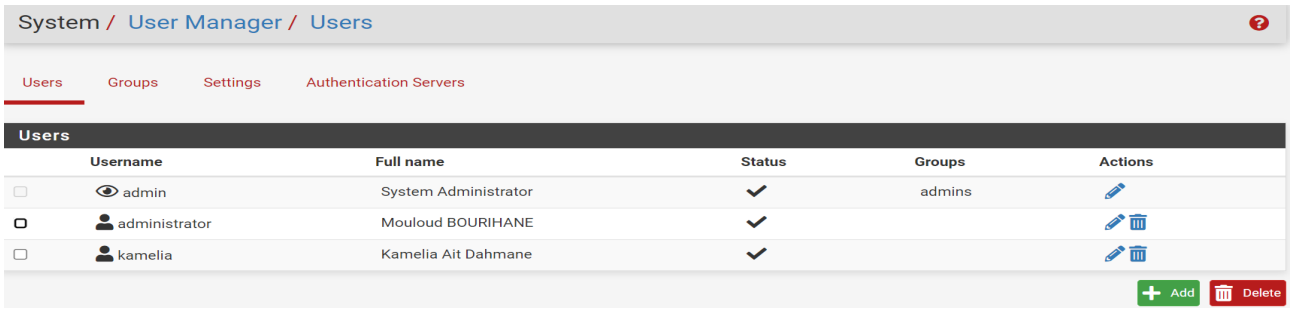

Figure 4.60 – Liste des utilisateurs.

b.Authentification LDAP (Active Directory)

En intégrant l'annuaire Active Directory sur PfSense, les utilisateurs peuvent être authentifiés à l'aide de leurs identifiants AD lorsqu'ils se connectent au VPN, pour assurer cette authentification en utilise le protocole LDAP.

❖ **Mise en place de l'annuaire LDAP**

LDAP (Lightweight Directory Access Protocol) est un protocole qui permet d'accéder à un annuaire centralisé contenant des informations essentielles pour une entreprise. Il est largement utilisé dans les entreprises pour faciliter l'accès et la communication des employés aux services internes. Ces communications LDAP s'effectuent sur le port 389, en TCP.

Pour mettre en place l'annuaire LDAP on va suivre les étapes suivantes :

- On va indiquer un nom pour ce serveur «User-VPN-LDAP».
- On va indiquer LDAP comme type.
- On va spécifier l'adresse du serveur
- Pour le certificat d'autorité on va utiliser le certificat déjà créer pour le serveur.
- Dans toutes les étapes suivantes on laisse les paramètres par défaut.

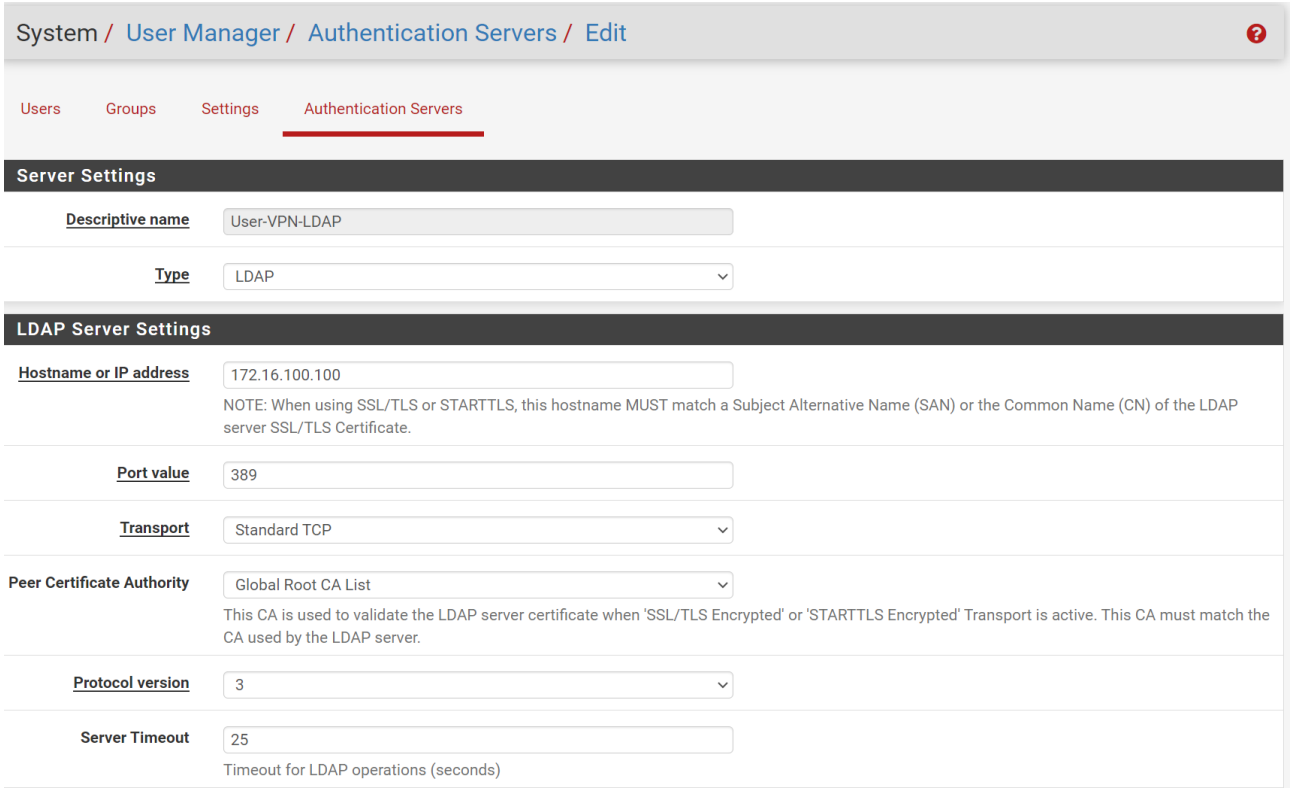

Figure 4.61 – Configuration d'un serveur d'authentification (1).

Search scope : on va laisser «Entire subtree »pour le scope de recherche. pour la «Base DN » : on va indiquer la racine de notre AD « toudja .local »

Authentification containers : on va indiquer les unités d'organisations OU dans lesquelles PfSense peut trouver les utilisateurs qui tentent de se connecter.

Ensuite, on va décocher « Bind anonyms » et on va passer à l'authentification pour interroger l'AD.

Bind credentials : ce champ vous demande d'associer les informations d'identification de l'utilisateur en utilisant le format "CN=nomUtilisateur" afin de vous authentifier auprès de l'annuaire LDAP.

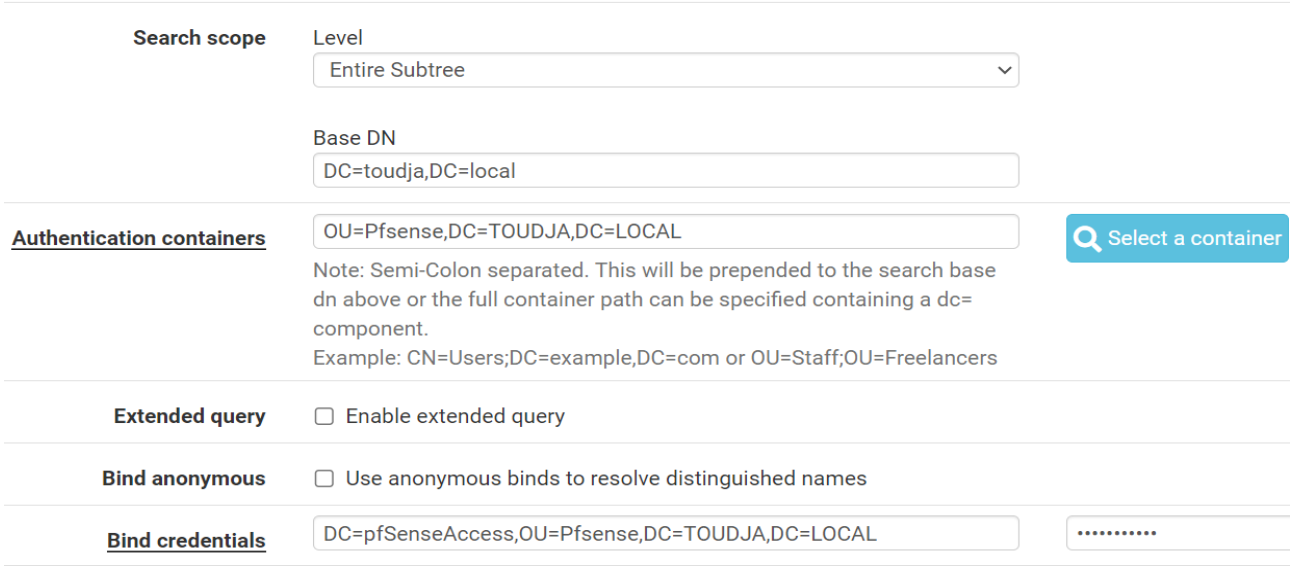

Figure 4.62 – Configuration d'un serveur d'authentification (2).

Dans cette partie on va laisser tous les paramètres par défaut

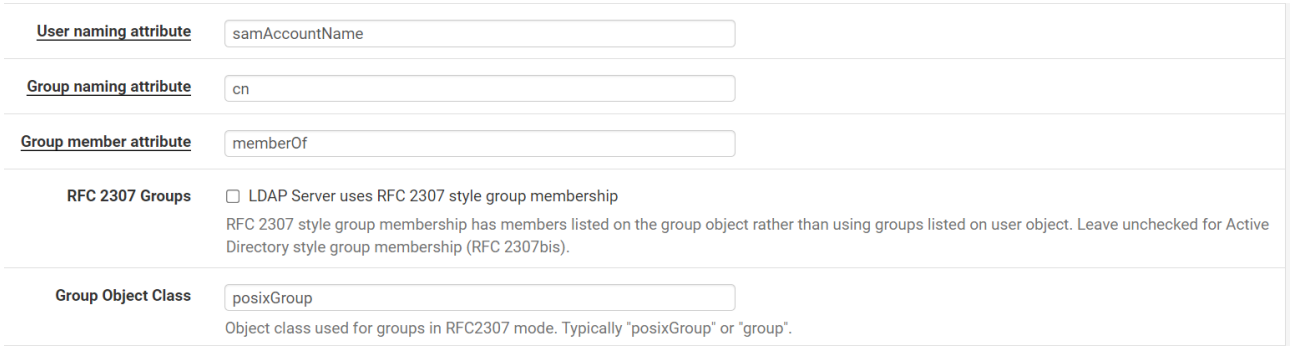

Figure 4.63 – Configuration d'un serveur d'authentification (3).

Le serveur d'authentification crée est montrée dans la figure suivante :

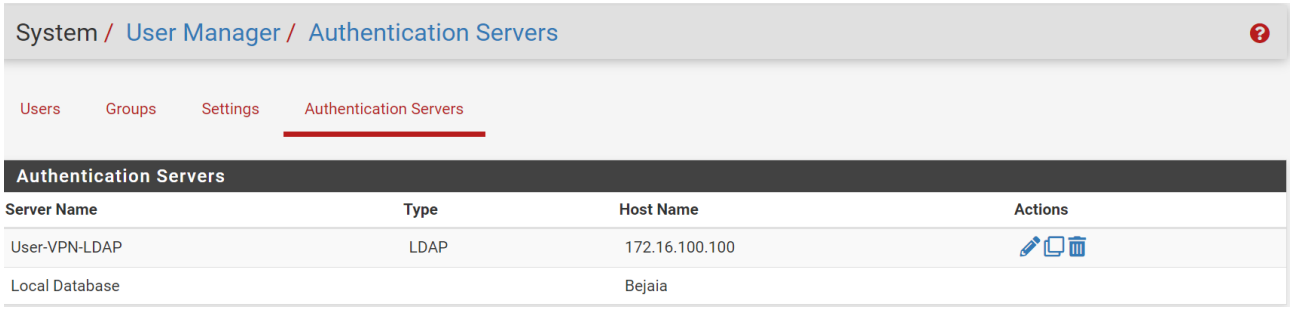

Figure 4.64 – Configuration d'un serveur d'authentification (3).

❖ Création d'un groupe Active Directory

Avant de tester l'authentification, il est nécessaire de créer un groupe sur l'Active Directory et d'y ajouter les utilisateurs déjà créés. Comme illustré dans la figure :

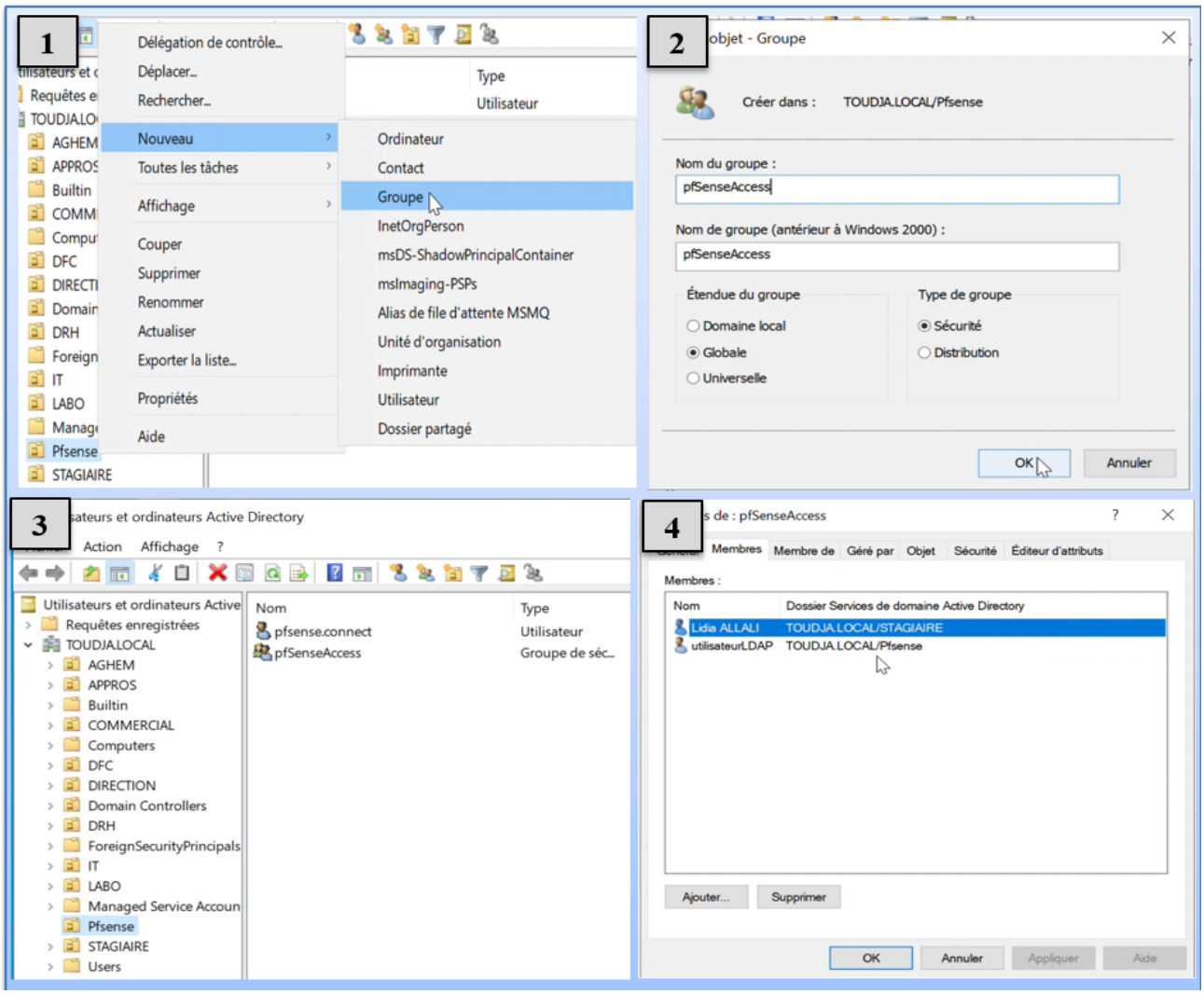

Figure 4.65 – Le groupe crée dans l'Active Directory.

❖ Déclaration du groupe local dans PfSense

Dans PfSense, il est nécessaire de créer un groupe local portant le même nom que le groupe Active Directory. Cela permettra à PfSense d'établir un lien entre les membres du groupe AD et les autorisations configurées pour le groupe PfSense.

On va nommer le groupe comme celui de l'Active Directory, et au niveau du scope, on va indiquer « Remote» à la place de « Local », car il s'agit d'un groupe AD.

Pour terminer, la liste des privilèges s'affiche, ce qui permet de gérer les droits avec une précision de délégation.

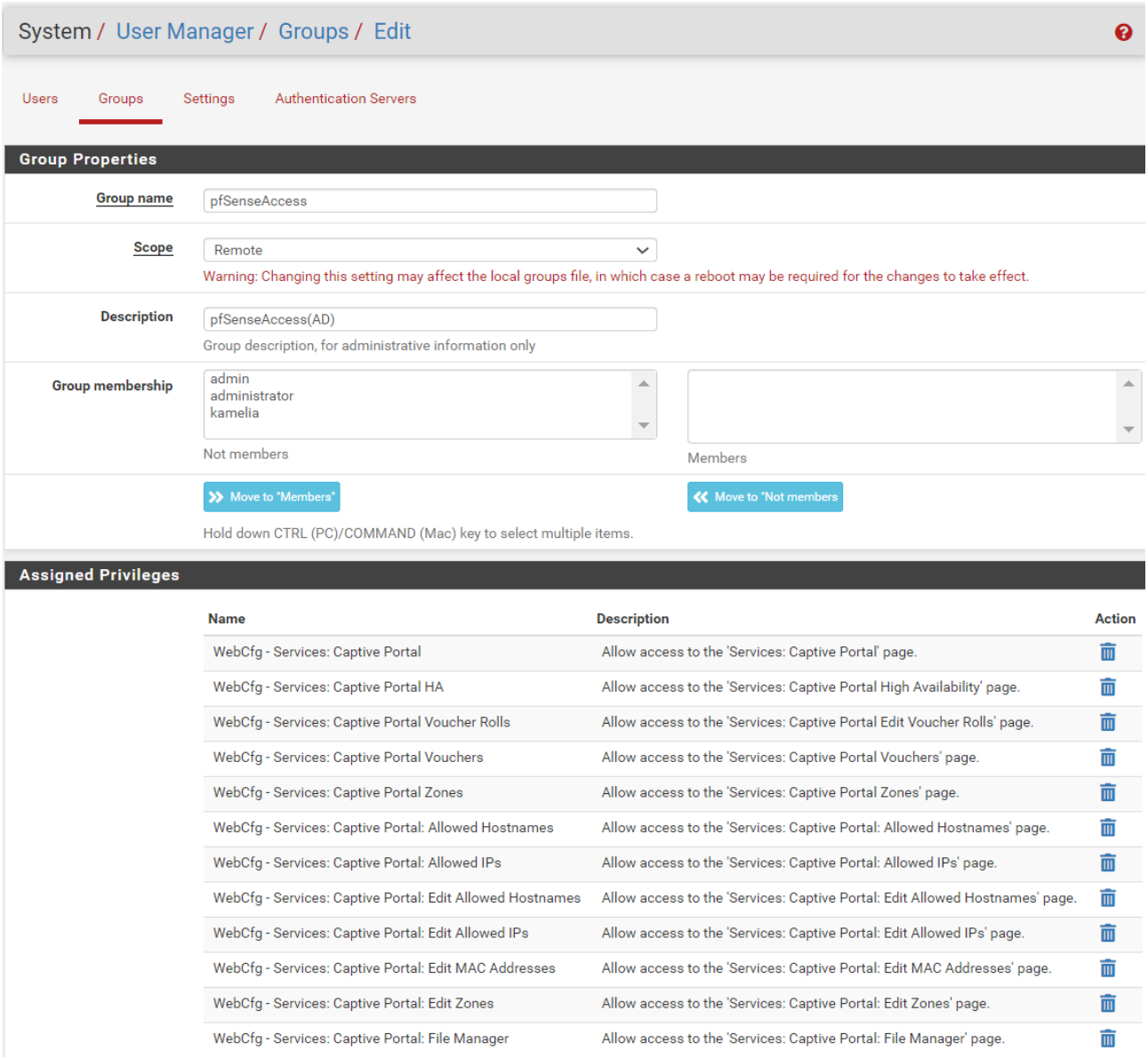

Figure 4.66 – Création d'un groupe sur PfSense.

Le groupe est bien crée, comme illustré dans la figure suivante :

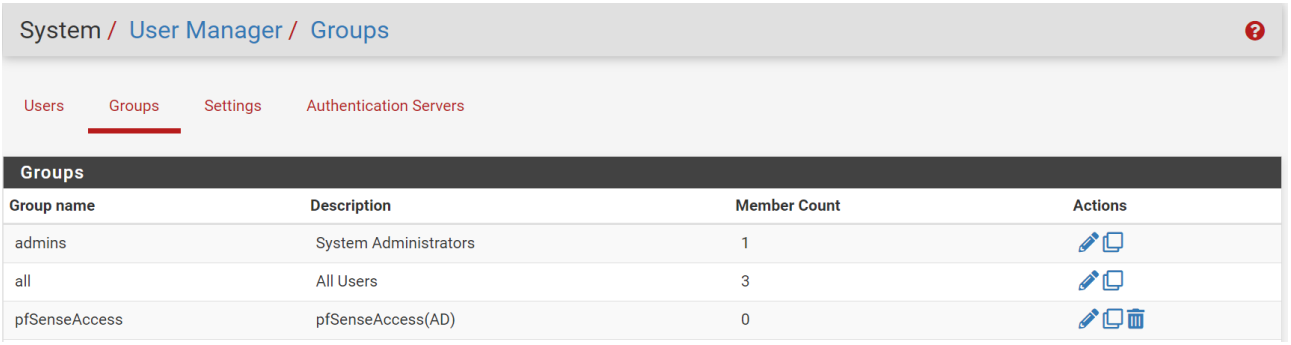

Figure 4.67 – Le groupe crée.

4.4 Partie II : Test

4.4.1 ESXI

On va effectuer des pings vers les adresses de nos hyperviseurs ESXI pour vérifier leur connectivité.

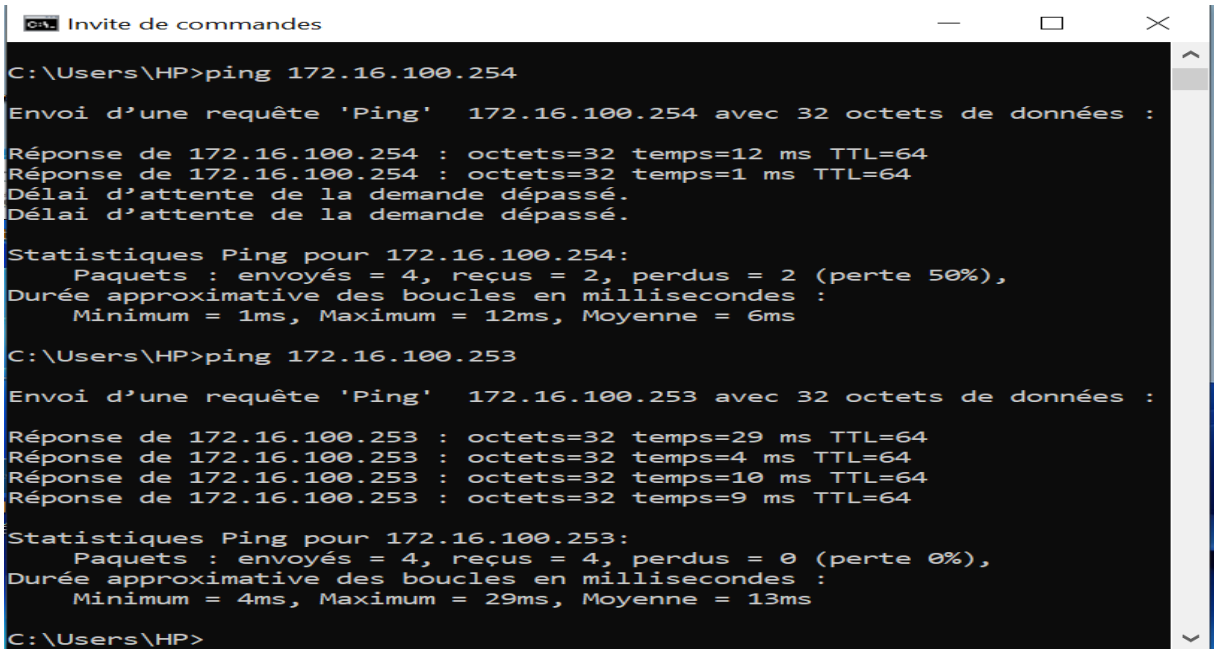

Figure 4.68 – Test de nos ESXI.

Linterface graphique de l'ESXI

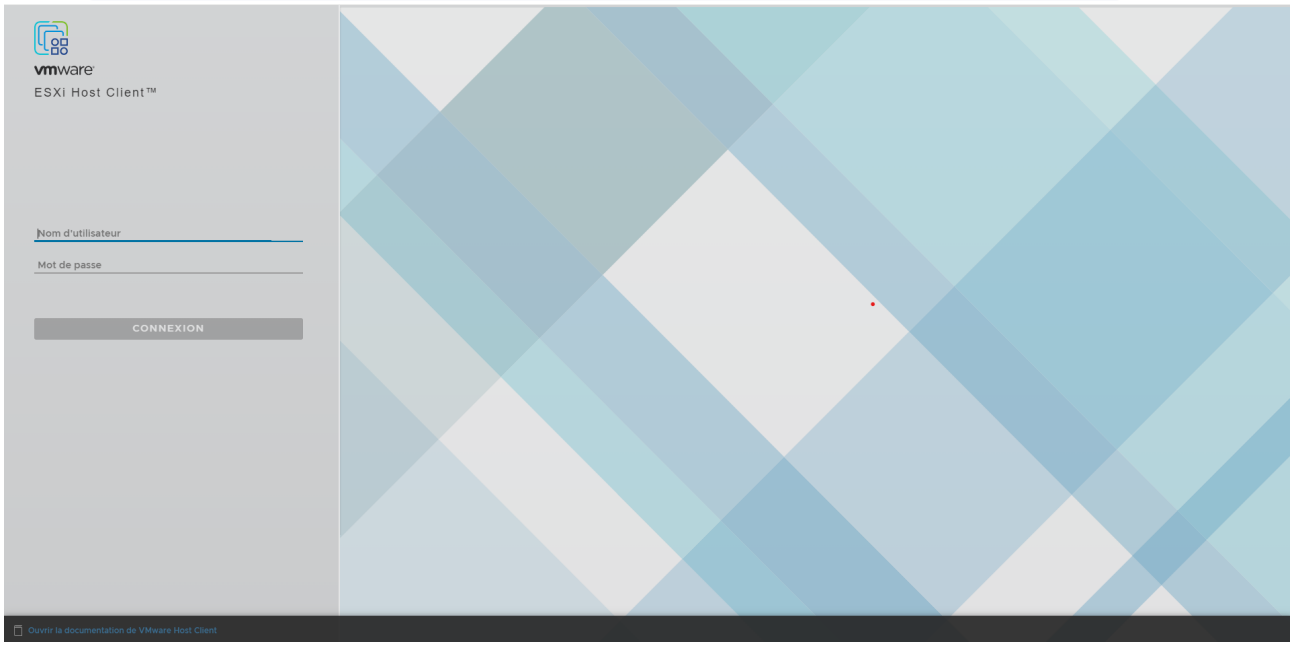

Figure 4.69 – VMware ESXI.

4.4.2 Firewall

On Ping de toutes les interfaces de nos pare-feu.

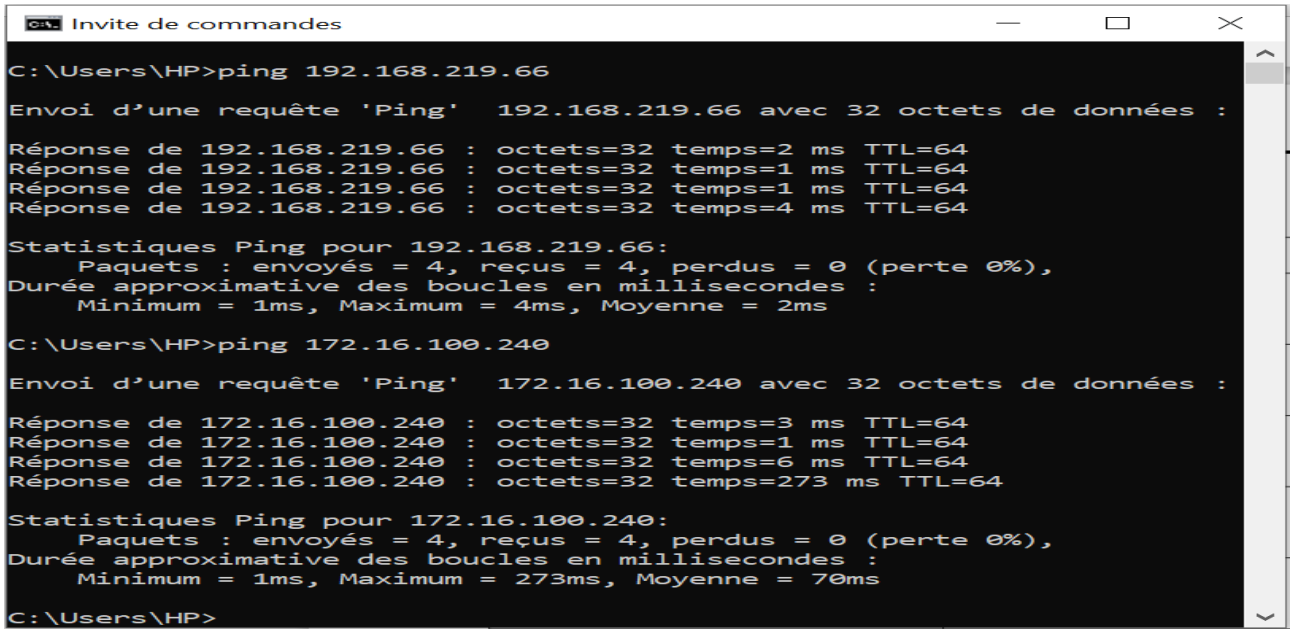

Figure 4.70 – Test du pare-feu Bejaia

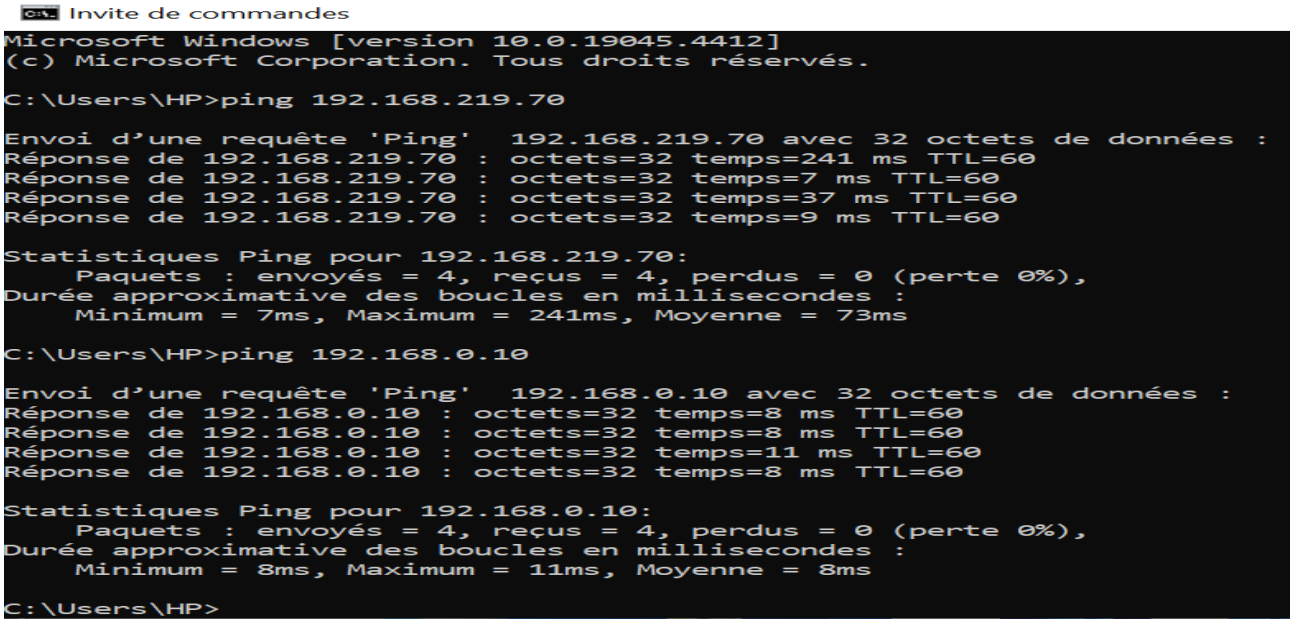

Figure 4.71 – Test du pare-feu GB EL Kseur.

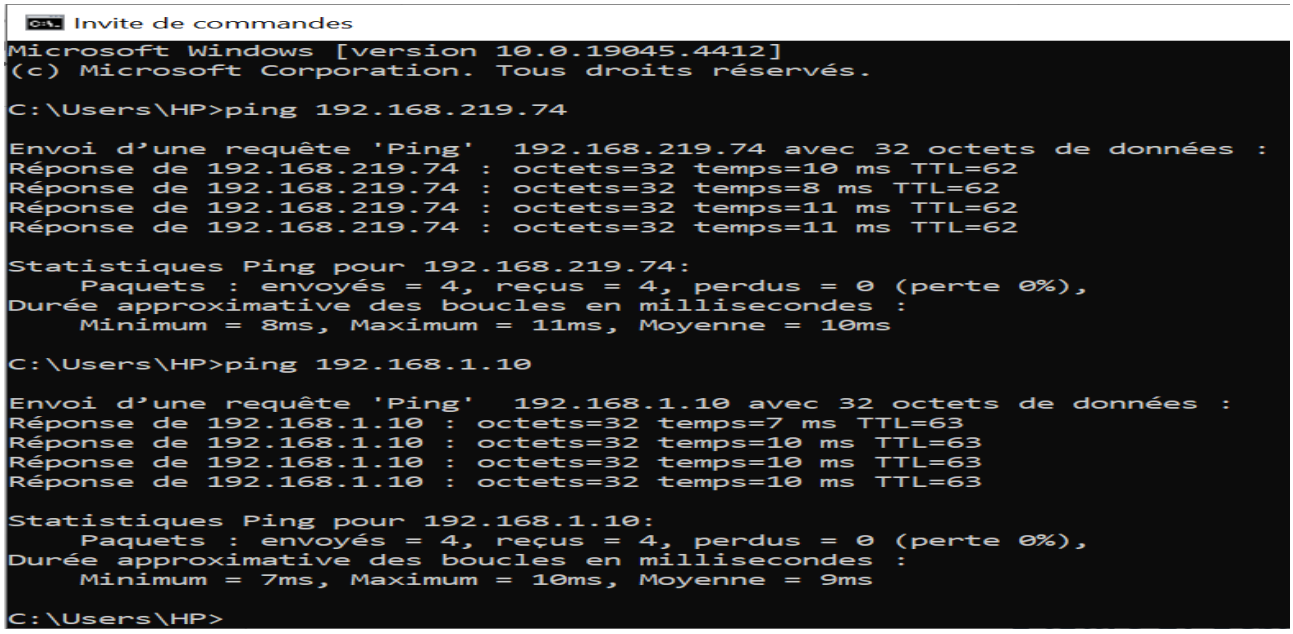

Figure 4.72 – Test du pare-feu de SET Toudja.

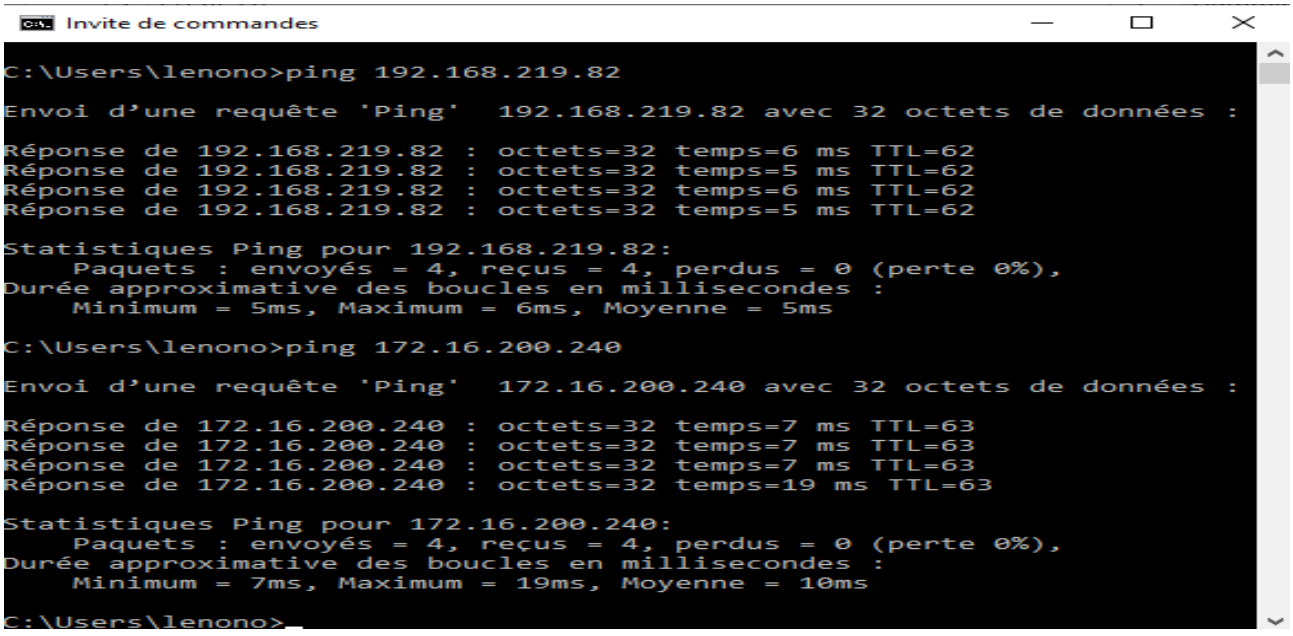

Figure 4.73 – Test du pare-feu de Unilait El Kseur.

4.4.3 Les serveurs

4.4.3.1 Serveur Active Directory

On va effectuer un ping vers le serveur AD-DNS-DHCP depuis la machine cliente avec l'adresse 172.16.100.100

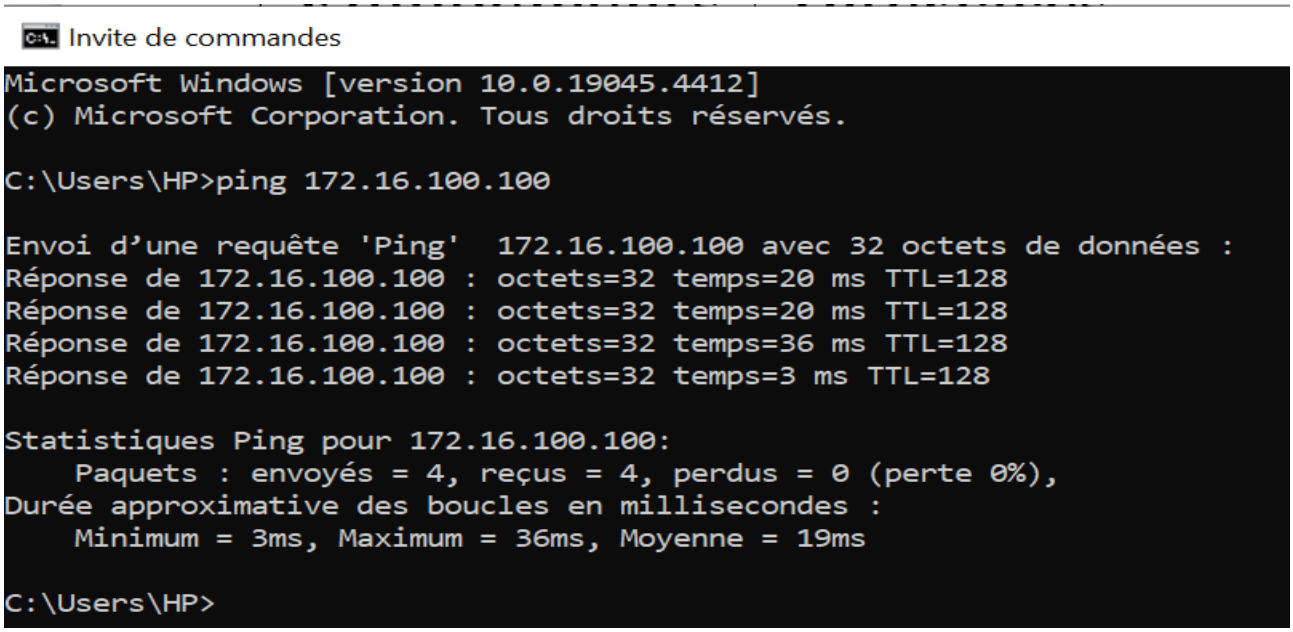

Figure 4.74 – Test du serveur AD-DNS-DHCP.

Authentification au tant qu'administrateur :

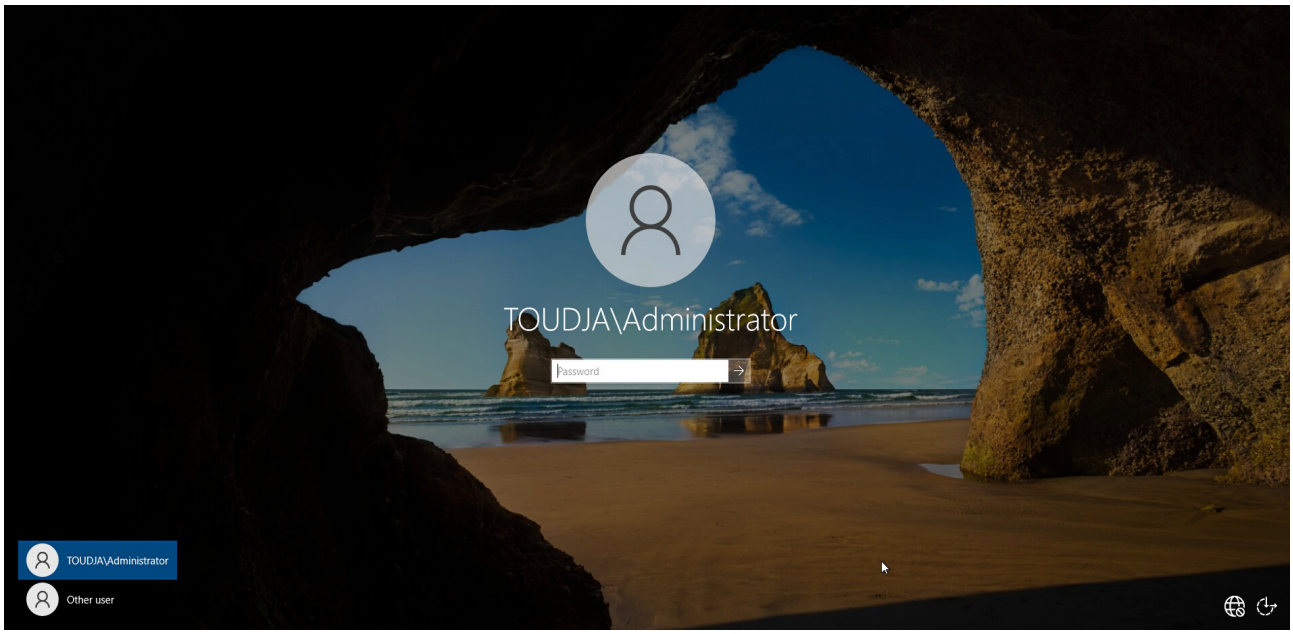

Figure 4.75 – Connexion réussie au domaine.

4.4.3.2 Serveur DHCP

Le serveur DHCP a donné à notre machine cliente une adresse IP dans la plage spécifiée : 172.16.100.13

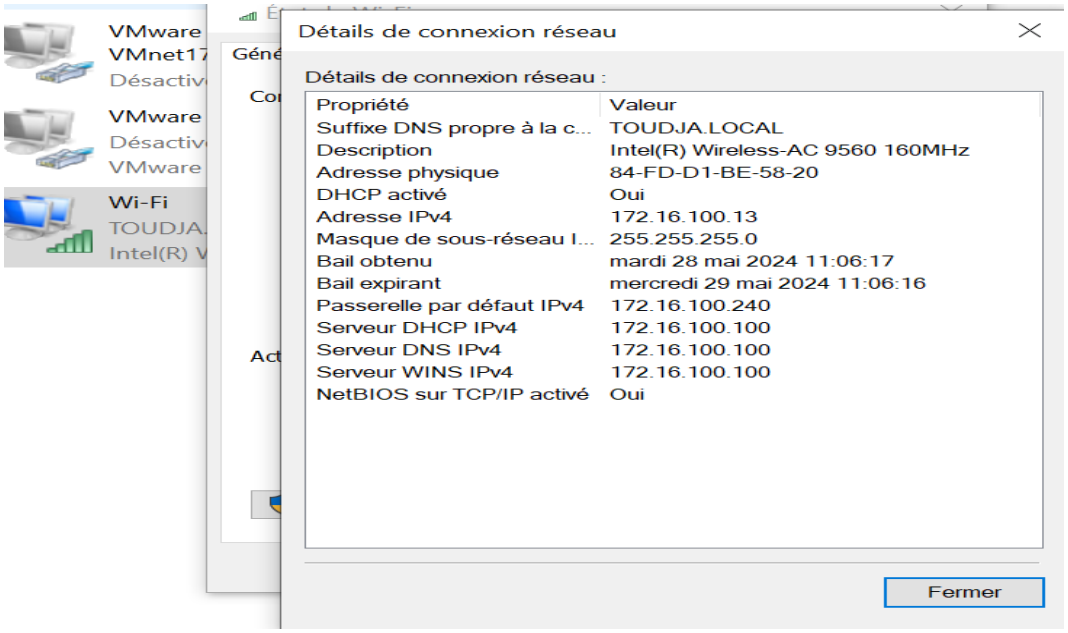

Figure 4.76 – Vérification de la mise en service de DHCP.

4.4.3.3 Serveur de réplication

On effectue un ping entre serveur1 et serveurs2 afin de vérifier si les deux serveurs peuvent se rejoindre sur réseau. La Figure suivante montre que la connectivité entre les deux serveurs est bien établie.

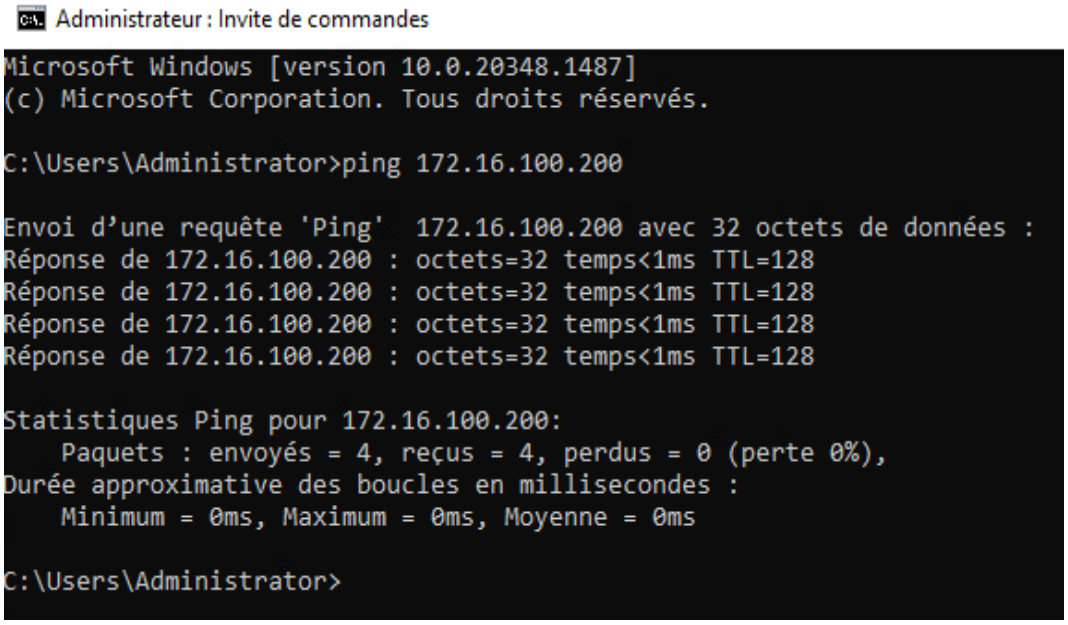

Figure 4.77 – Ping du serveur 1 vers serveur 2.

4.4.4 Test du VPN multi-sites

4.4.4.1 Tests des tunnels VPN

Pour vérifier si les tunnels ont été bien implémentés et que les données échangées entre les sites sont chiffrées, on va effectuer des ping sur chaque tunnel, comme illustré dans les figures ci-dessus :

```
C:\Users\HP>ping 10.10.10.1

Envoi d'une requête 'Ping'  10.10.10.1 avec 32 octets de données :
Réponse de 10.10.10.1 : octets=32 temps=5 ms TTL=64
Réponse de 10.10.10.1 : octets=32 temps=12 ms TTL=64
Réponse de 10.10.10.1 : octets=32 temps=6 ms TTL=64
Réponse de 10.10.10.1 : octets=32 temps=5 ms TTL=64

Statistiques Ping pour 10.10.10.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 5ms, Maximum = 12ms, Moyenne = 7ms
```

Figure 4.78 – Test du tunnel entre GB Béjaia et GB El Kseur.

```
C:\Users\HP>ping 10.10.11.1

Envoi d'une requête 'Ping'  10.10.11.1 avec 32 octets de données :
Réponse de 10.10.11.1 : octets=32 temps=31 ms TTL=64
Réponse de 10.10.11.1 : octets=32 temps=5 ms TTL=64
Réponse de 10.10.11.1 : octets=32 temps=19 ms TTL=64
Réponse de 10.10.11.1 : octets=32 temps=11 ms TTL=64

Statistiques Ping pour 10.10.11.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 5ms, Maximum = 31ms, Moyenne = 16ms
```

Figure 4.79 – Test du tunnel entre GB Béjaia et SET Toudja.

```
C:\Users\HP>ping 10.10.12.1

Envoi d'une requête 'Ping'  10.10.12.1 avec 32 octets de données :
Réponse de 10.10.12.1 : octets=32 temps=3 ms TTL=64
Réponse de 10.10.12.1 : octets=32 temps=3 ms TTL=64
Réponse de 10.10.12.1 : octets=32 temps=3 ms TTL=64
Réponse de 10.10.12.1 : octets=32 temps=4 ms TTL=64

Statistiques Ping pour 10.10.12.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 3ms, Maximum = 4ms, Moyenne = 3ms
```

Figure 4.80 – Test du tunnel entre GB Béjaia et Unilait El Kseur.

4.4.4.2 Tests d'interconnexion des sites

Pour vérifier la communication entre les sites de notre entreprise, nous allons d'abord effectuer un ping entre le site principal « GB Béjaia » et les autres sites (GB El Kseur, Set Toudja et Uniait El Kseur), puis inversement. La communication est bien établie, comme illustré dans les figures ci-dessus :

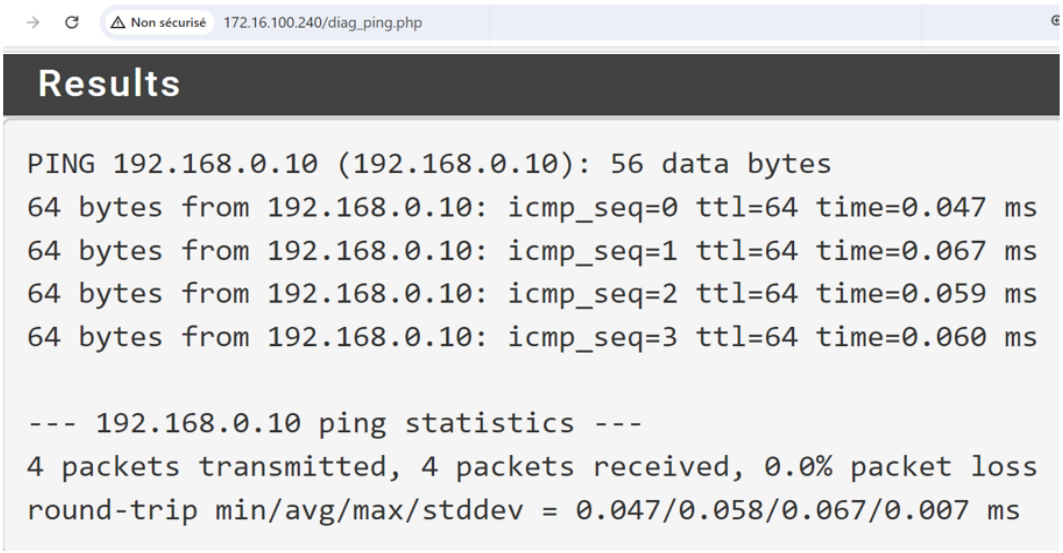

Figure 4.81 – Ping réussi de site SPC GB Béjaia vers GB El Kseur.

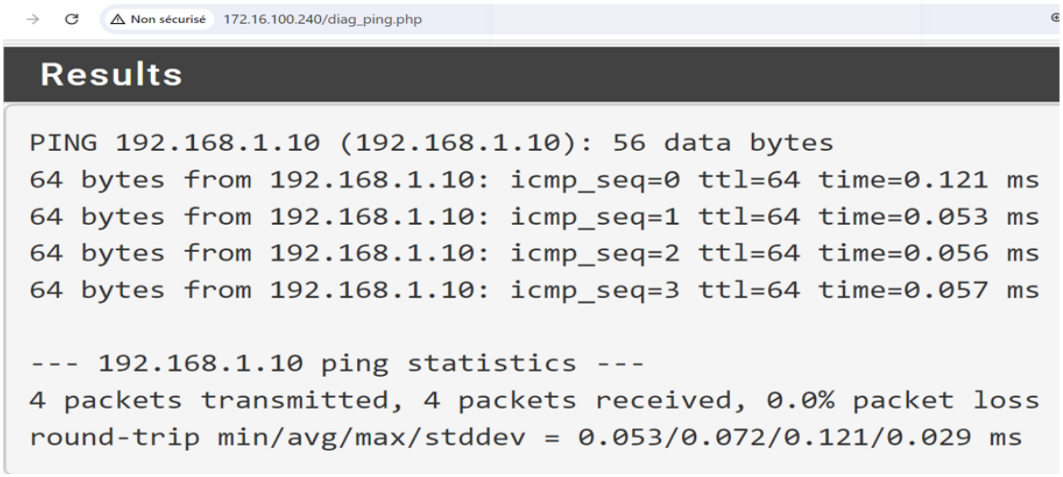

Figure 4.82 – Ping réussi de site SPC GB Béjaia vers SET Toudja.

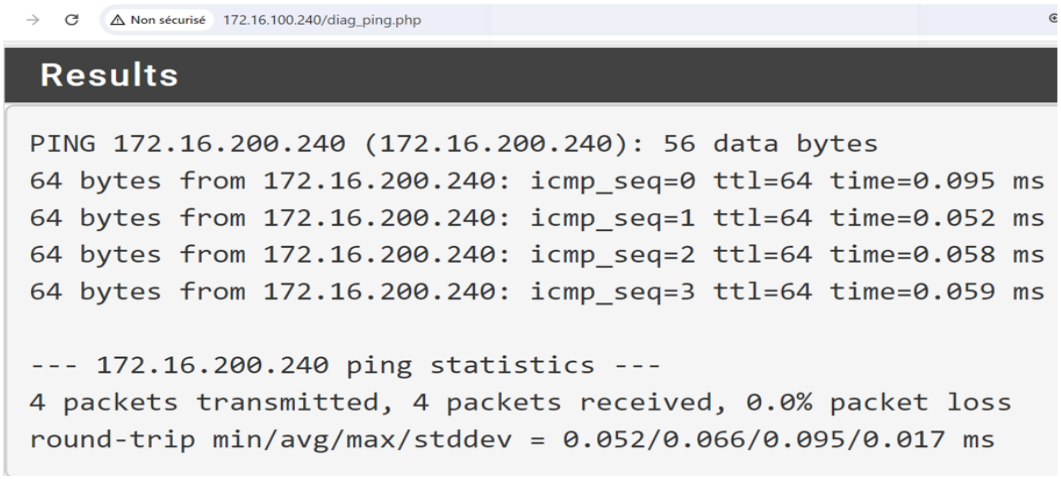

Figure 4.83 – Ping réussi de site SPC GB Béjaia vers Unilait El Kseur.

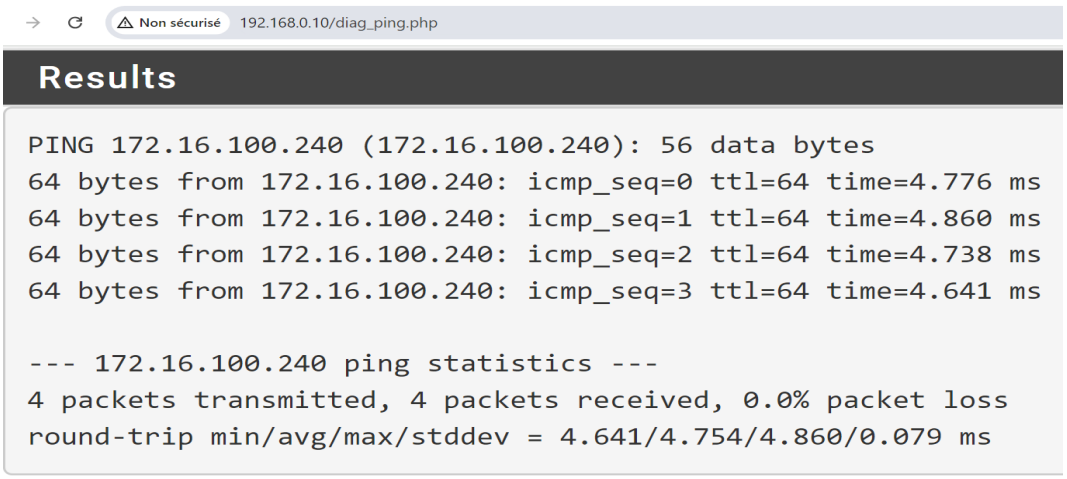

Figure 4.84 – Ping réussi de site GB El Kseur vers SPC GB Béjaia.

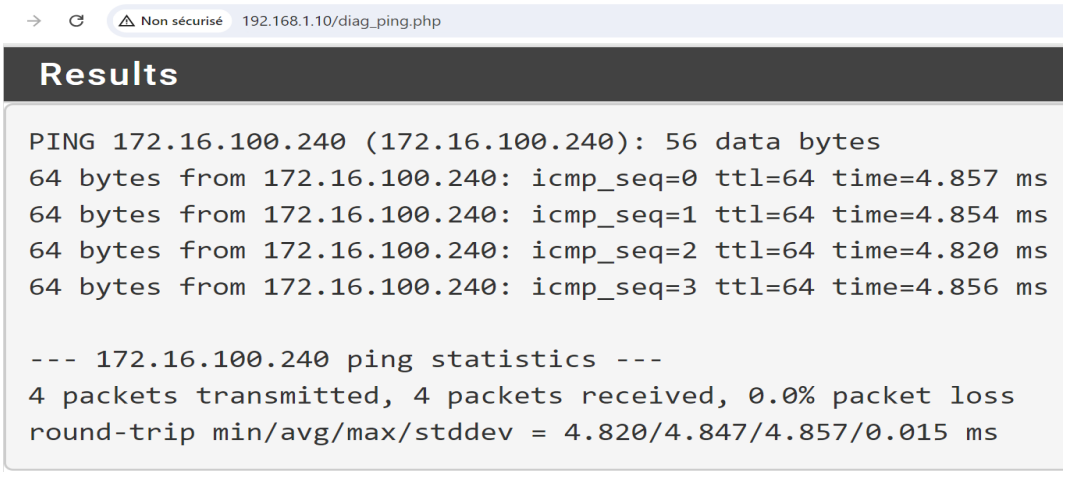

Figure 4.85 – Ping réussi de site SET Toudja vers SPC GB Béjaia.

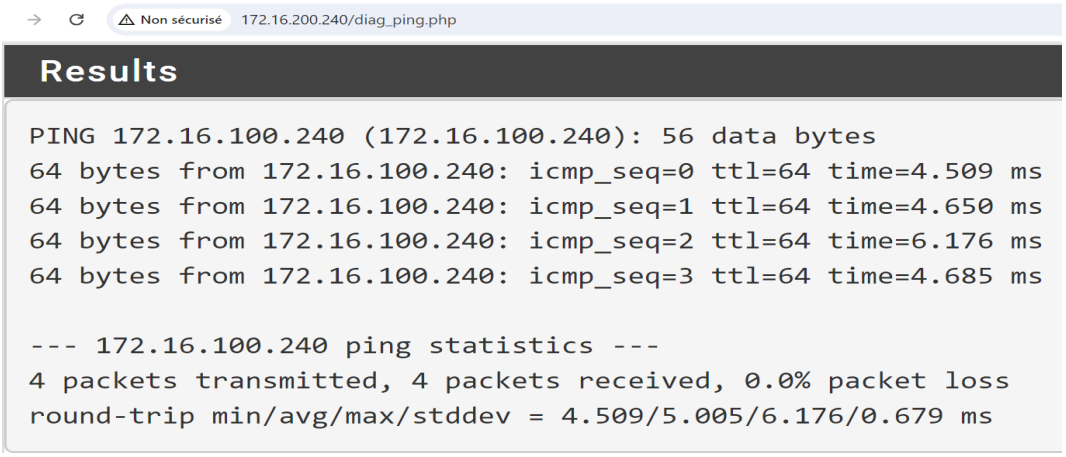

Figure 4.86 – Ping réussi de site Unilait El Kseur vers SPC GB Béjaia.

4.4.5 Test du VPN client à site

4.4.5.1 Test du tunnel VPN

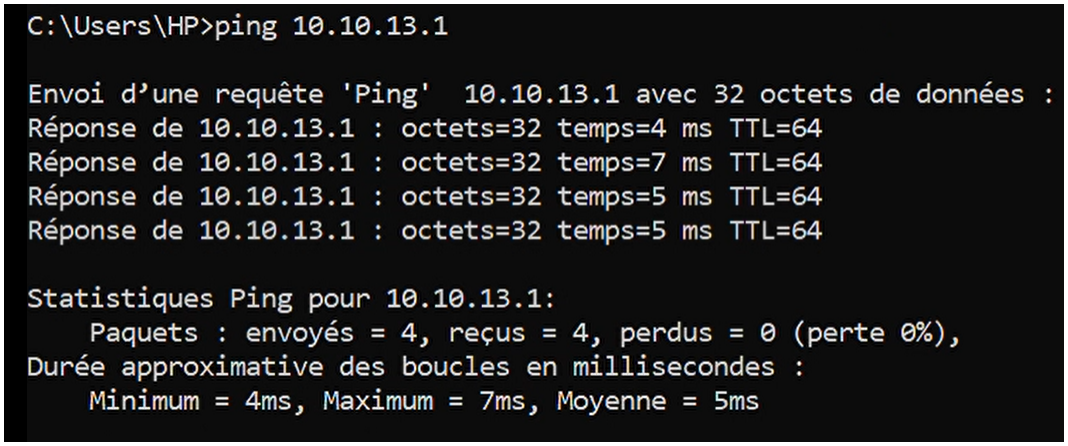

Figure 4.87 – Test du tunnel entre GB Béjaia et ces clients

4.4.5.2 Test d'authentification LDAP

Pour tester l'authentification : on va sélectionner le serveur d'authentification Active Directory, puis on va insérer le nom d'utilisateur, son mot de passe et on va cliquer sur « Test ».

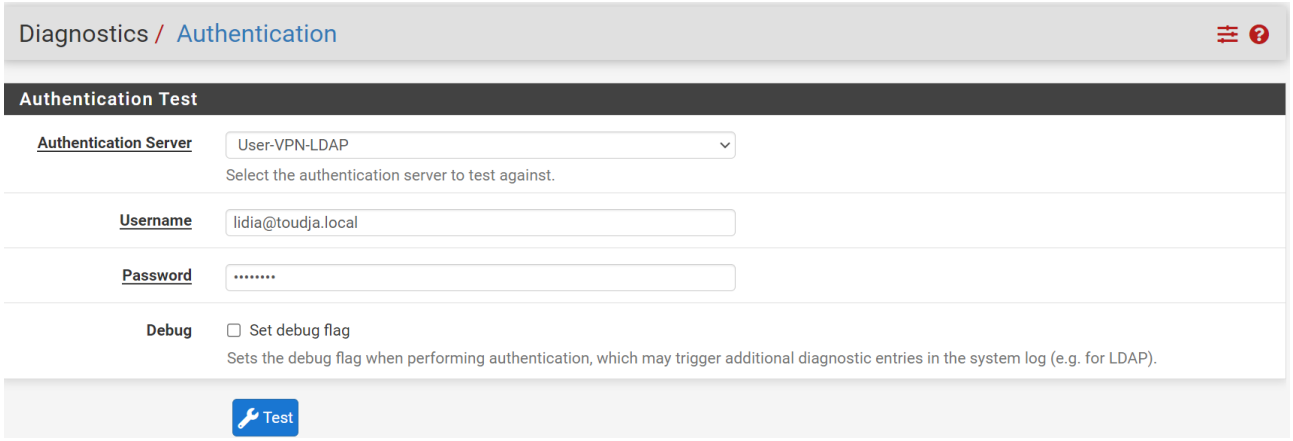

Figure 4.88 – Test d'authentification.

Si le test est bien réussi, le message suivant devrait s'afficher :

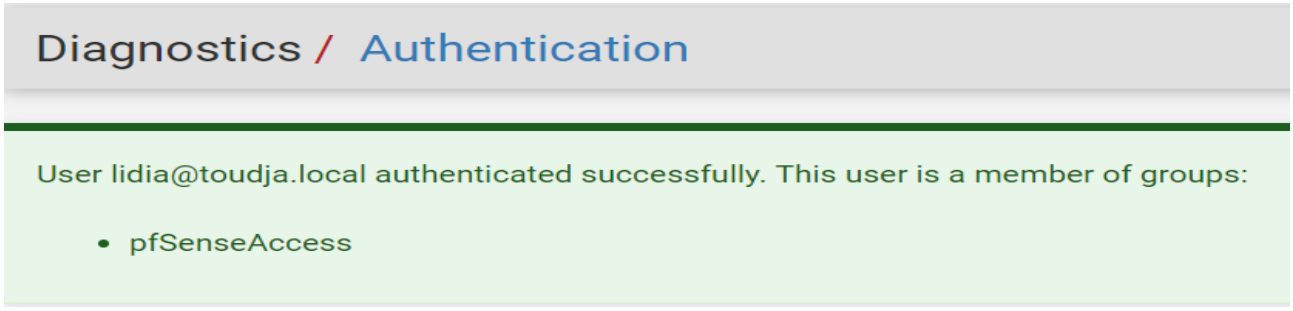

Figure 4.89 – Test réussi.

4.4.5.3 Tester l'accès distant depuis un poste client

Sur l'icône OpenVPN on va effectuer un clic droit et on va cliquer sur "Connecter".

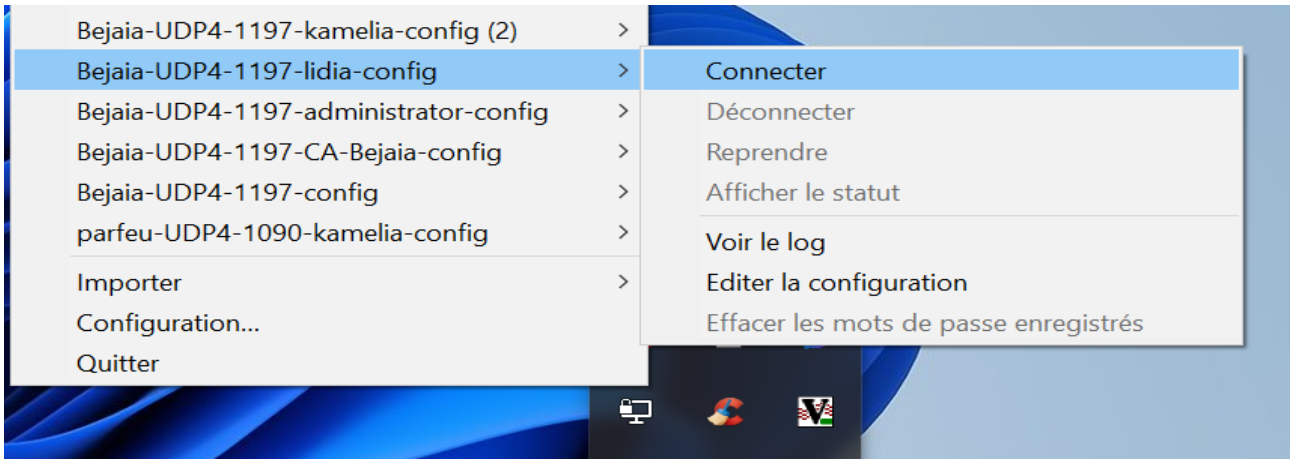

Figure 4.90 – Activation d'OpenVPN.

Pour s'authentifier, on va insérer le nom de l'utilisateur et son mot de passe, correspondant à un compte Active Directory ou un compte local du pare-feu.

❖ **Authentification de l'utilisateur AD**

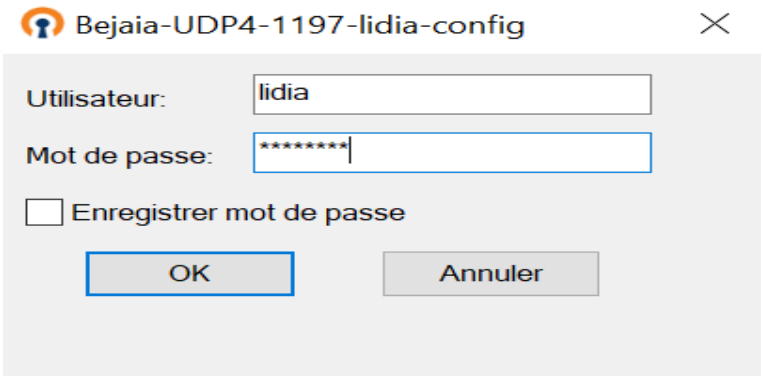

Figure 4.91 – Accès à l'OpenVPN.

Le client de l'Active Directory est bien connecté, Comme illustré dans la figure :

Figure 4.92 – Connexion VPN réussie pour le client LDAP.

❖ **Authentification de l'utilisateur de la base locale**

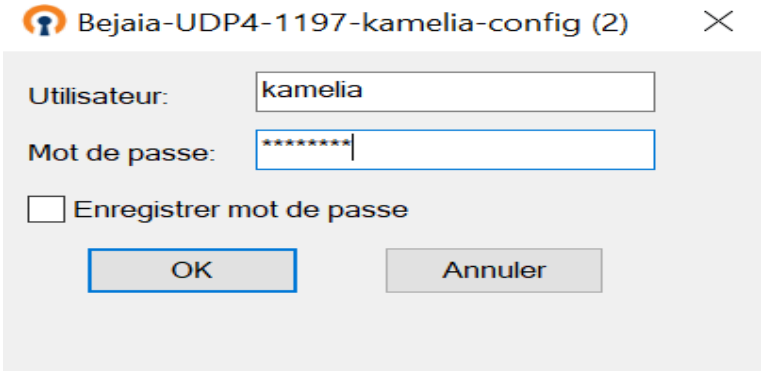

Figure 4.93 – Accès à l'OpenVPN.

Le client de la base locale est bien connecté, Comme illustré dans la figure :

Figure 4.94 – Le client est bien connecté.

La figure ci-dessous présente les clients connectés à l'OpenVPN.

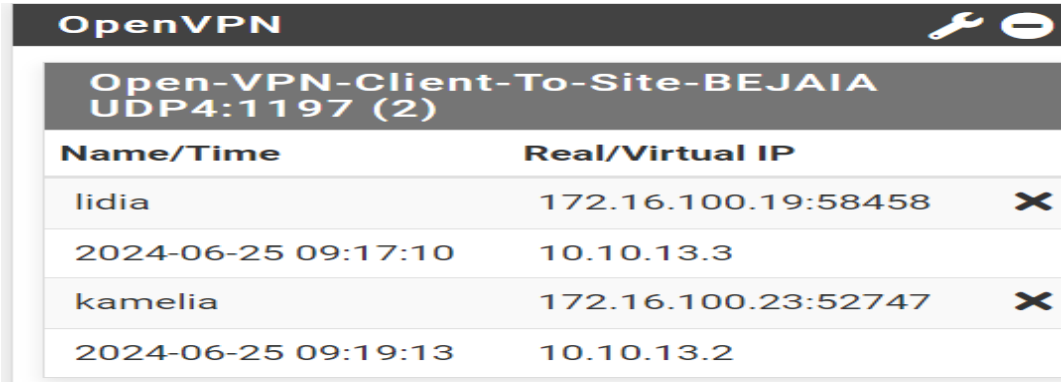

Figure 4.95 – Clients connectés à OpenVPN.

4.5 Conclusion

En conclusion, ce chapitre a été essentiel pour la mise en place réussie de notre application sur le réseau informatique de Groupe Toudja. Nous avons présenté les outils utilisés, configuré les solutions proposées, et effectué des tests pour valider nos configurations. Les résultats de ces tests confirment le bon fonctionnement de l'ensemble du système déployé. Nous sommes confiants que ce chapitre servira de base solide pour le déploiement futur de notre application et répondra efficacement aux besoins de l'entreprise.

CONCLUSION GÉNÉRALE

Il est indéniable que la sécurité informatique totale est difficile à atteindre, étant donné la multitude de menaces susceptibles de compromettre le bon fonctionnement d'un réseau informatique au sein d'une organisation. Par conséquent, il est essentiel d'élaborer une politique de sécurité adaptée aux risques réels auxquels le réseau est exposé. Il est crucial de mettre en place des mécanismes adéquats de prévention, de maintenance et de correction afin d'assurer une sécurité optimale du réseau informatique de l'entreprise.

Pendant notre stage au sein de l'entreprise Groupe Toudja, nous avons effectué une analyse approfondie du réseau informatique et identifié plusieurs anomalies en matière de sécurité. Suite à cela, nous avons abordé les différentes solutions adéquates en fonction des anomalies soulignées, permettant de rendre le réseau plus sécurisé tout en prenant en compte les besoins actuels de l'entreprise pour le bon fonctionnement de son réseau informatique et sa sécurité.

Afin d'améliorer son architecture réseau, nous avons mis en place un trio puissant qui permet d'optimiser l'utilisation des ressources matérielles, d'améliorer l'évolutivité et de réduire les coûts associés à la gestion des infrastructures.

Ce trio comprend la virtualisation, qui consiste à créer des versions virtuelles des ressources réseau. PfSense permet non seulement de centraliser l'administration de la sécurité aux points d'accès limités du réseau d'entreprise, mais aussi de créer un périmètre de sécurité. Enfin, le VPN poste à site entre le site de Béjaia et ses clients permet aux utilisateurs distants d'accéder aux ressources de l'entreprise. D'autre part, le VPN multi-sites consiste à mettre en place une liaison permanente distante et sécurisée entre les sites du groupe Toudja, à savoir Béjaia, GB El Kseur, SET Toudja et Unilait El Kseur. Ce VPN est basé sur le protocole OpenVPN. Enfin, la réplication des serveurs assure la redondance et la disponibilité des données, garantissant ainsi une continuité de service.

Ce travail a fait l'objet d'une expérience intéressante, et a eu énormément d'apport sur nos connaissances et nos compétences en termes de configuration dans un environnement ESXI, Pfsense. De plus nous avons enrichi nos connaissances déjà requise dans le domaine de la sécurité informatique notamment la sécurité d'un réseau d'entreprise grâce à l'implémentation d'une solution de Virtualisation, PfSense et d'un réseau privé virtuel (VPN).

Cependant, vu la taille importante du projet et la limitation du temps, plusieurs améliorations peuvent être encore envisagées. En perspective nous pouvons envisager quelques améliorations pour rendre ce projet plus performant. Parmi ces perspectives, nous citons en particulier :

- Une possibilité d'utilisation du cloud computing pour une meilleure prise en charge de la sécurité.
- Utiliser des VLAN pour segmenter le trafic réseau et limiter l'accès aux différents services et ressources.
- La mise en œuvre d'un système de supervision pour prévenir et détecter les intrus.

BIBLIOGRAPHIE

[1] N.BATTAT. *Systèmes de Sécurité*. Bejaia : Université de A.Mira de Bejaia, 2023/2024. Chap. Principes de sécurité informatique.

[2] M. Moustapha KABA. *Etude et mise en place s'une solution cloud computing sur une infrastructure de virtualisation,cas d'etude :AISAKAGROUP.Mémoire de Master en Informatique*. Senegal :Université Dakar Bourguiba. 2018/2019.

[3] L.Bloch et C.Wolfhugel. *Sécurité informatique principe et méthode*. EYROLLES 2eme Edition, 2005.

[4] P.Jean-François et B.Jean-Philippe. *Sécurité informatique*. 3ième édition, Dunod, Paris 2013.

[5] `https://wikimemoires.net/2012/08/quest-ce-quun-firewall-fonctionnement-et-types-de-firewall/`. consulté le 12 mai 2024.

[6] D. B Chapman et E D. Zwicky. *Building Internet Firewall*. o'railly, 1995.

[7] G. PUJOLLE. *Les réseaux*. 6ème édition. Eyrolles, 2008.

[8] N.BATTAT. *Systèmes de Sécurité*. Bejaia : Université de A.Mira de Bejaia, 2023/2024. Chap. La sécurité des infrastructures de télécommunication.

[9] J.ARCHIER. *LES VPN fonctionnement, mise en œuvre et maintenance des VPNs*. Edition ENI, juin 2010.

[10] `https://www.vpnmentor.com/blog/ultimate-guide-to-vpn-tunneling/`. consulté le 8 mai 2024.

[11] M.Carugi. "Virtual Private Network services". In : *Autrans-RHMD* (2Mai 2002).

[12] https://www.memoireonline.com/01/20/11531/Deploiement-d-un-coeur-de-reseau-IPMPLS.html. consulté le 8 mai 2024.

[13] J.AIT AMARA et L.AMEZZA. *Organisation du réseau en VLAN Cas d'´etude : Entreprise NAFTAL.Mémoire de Master en Informatique*. Bejaia : Université Abderrahmane Mira. 2016-2017.

[14] A.HOUHA A.SIDER. *TECHNOLOGIE INTERNET*. Bejaia : Université de A.Mira de Bejaia, 2020-2021. Chap. Le modèle TCP/IP, TCP et UDP.

[15] https://ram-0000.developpez.com/tutoriels/reseau/ICMP/. consulté le 4 mai 2024.

[16] https://www.avast.com/fr-fr/c-what-is-tcp-ip. consulté le 4 mai 2024.

[17] https://www.frameip.com/vpn/#36-8211-le-protocole-ssl. consulté le 4 mai 2024.

[18] https://www.appvizer.fr/magazine/services-informatiques/virtualisation/infrastructure-informatique/. consulté le 12 avril 2024.

[19] Thierry LONGEAU. *La Virtualisation des systèmes d'information*. 2012.

[20] E MAILLÉ. *VMware vSphere 4 ,4éme édition ,Editions ENI*. janvier 2010.

[21] https://mundopymes.net/definiciones/que-es-intranet/. consulté le 4 mai 2024.

[22] Mathieu Caizergues. *Point sur la virtualisation, OBJECTIF VIRTUALISATION*. 2013.

[23] https://www.appvizer.fr/magazine/services-informatiques/virtualisation/type-virtualisation. consulté le 13 avril 2024.

[24] K. Attil. *consolidation de serveurs avec la solution Xen Open Source.Mémoire de Master en Informatique*. Bejaia : Université Abderrahmane Mira. 2011.

[25] http://projet.eu.org/pedago/sin/ISN/8-securite_reseaux.pdf. consulté le 12 avril 2024.

[26] M.HEURTIN E.FOURN J.BERTON. *VMware vSphere 6, 6éme édition*. Editions ENI, janvier 2017.

[27] https://techtoday.lenovo.com/fr/fr/solutions/services/hyperviseur. consulté le 8 mai 2024.

[28] P.Alain A.Arnaud. *"Virtualisation & Partage de Charge"*. Edition AFNOG, 2014.

[29] F.TIGRINE A.MOUMENE. *Virtualisation de la couche infrastructure d'un systeme d'information,cas d'etreprise portuaire d'alger EPAL.Mémoire de Master en Informatique*. Bejaia : Université Abderrahmane Mira. 2020/2021.

[30] `https://www.oracle.com/fr/cloud/definition-it-virtual-server/`. consulté le 12 avril 2024.

[31] `https://community.fs.com/fr/article/Virtual-Server-vs-Physical-Server.html`. consulté le 12 avril 2024.

[32] `https://www-igm.univ-mlv.fr/~dr/XPOSE2008/virtualisation/architecture.html`. consulté le 4 mai 2024.

[33] Source : document interne de la SARL SPC GB.

[34] N.ZIANE. *Étude et mise en place d'une solution de virtualisation, Cas d'étude : Entreprise Cevital de Béjaïa.Mémoire de Master en Informatique*. Bejaia : Université Abderrahmane Mira. juin 2023.

[35] `https://sflanders.net/2014/04/08/changing-vmware-esxi-host-logging-level/`. consulté le 3 juillet 2024.

[36] G.TINOUILINE C.CHERAFT. *Configuration et sécurisation de réseau de l'entreprise Général Emballage à base des Liaisons Virtuelles.Mémoire de Master en Informatique*. Bejaia : Université Abderrahmane Mira. 2022/2023.

[37] `https://ar.inspiredpencil.com/pictures-2023/windows-server-2022-logo-png`. consulté le 3 juillet 2024.

Annexes

Annexe 1

Création d'une machine virtuelle

Sur notre interface ESXI, on clique sur le bouton machine virtuelle → Créer une machine virtuelle → On clique sur suivant dans la première fenêtre qui va afficher → on va saisir le nom de la machine (SRVW22) → Sélectionner OS qu'on voulait installer sur notre machine.

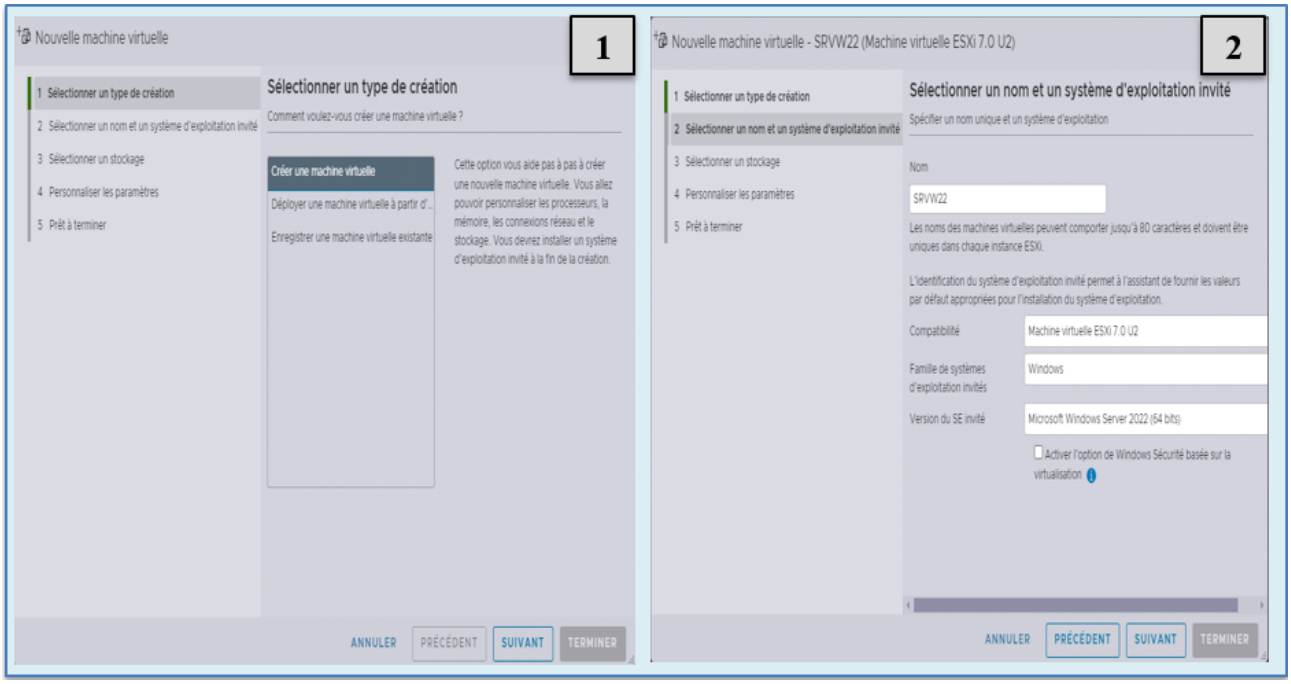

Figure 4.96 – Nommer et choisir l'OS de la machine.

Par la suite, sur la fenêtre qui va apparaitre on va sélectionner l'emplacement de stockage « DATA1 », ou on souhaite installer la VM, puis on arrive sur une fenêtre ou on configure le matériel virtuel et d'autres options selon nos besoins, et on termine. :

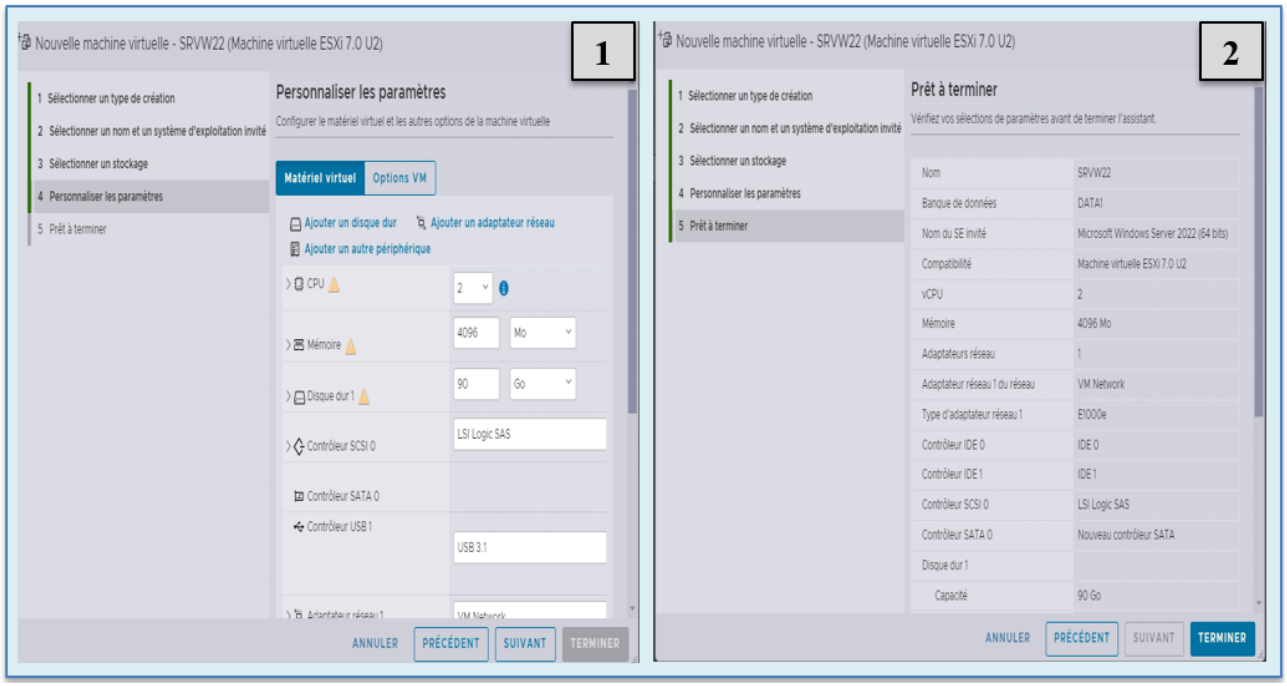

Figure 4.97 – Préciser l'emplacement de stockage.

On clique sur modifier les paramètres → On choisit le fichier ISO sur le lecteur CD/DVD 1 puis enregistrer. Après on clique sur la fenêtre de VMware pour démarrer notre machine.

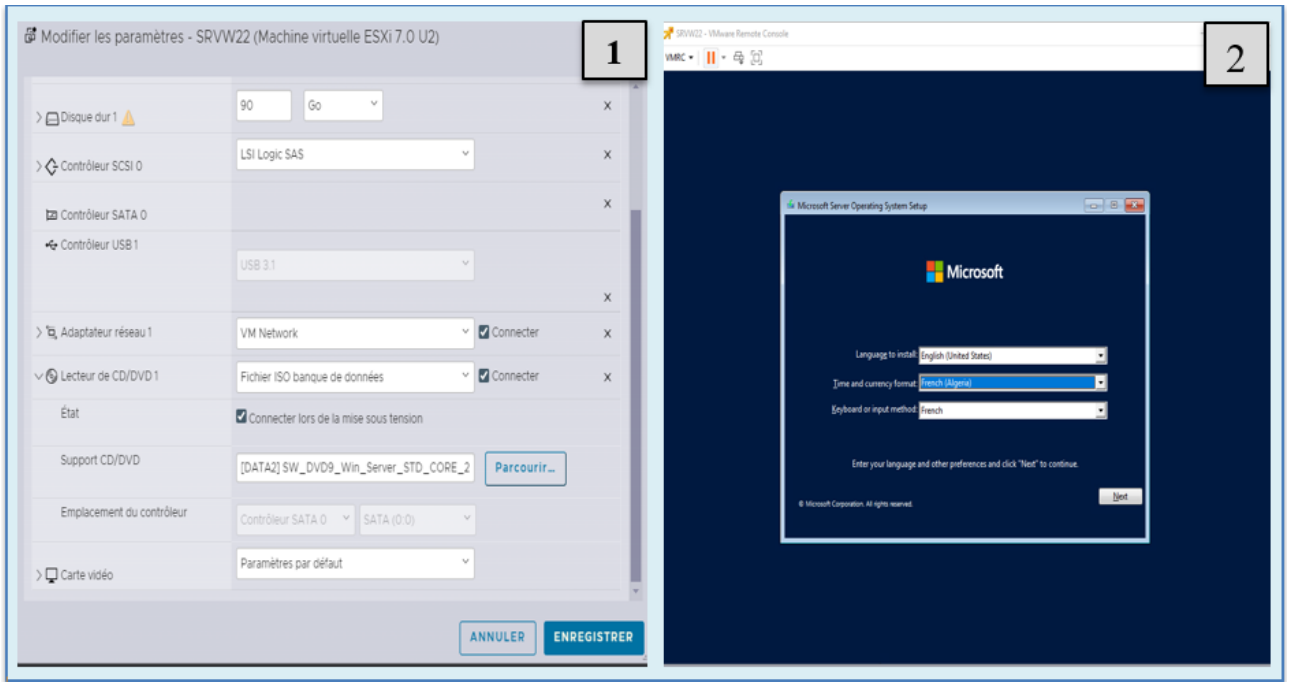

Figure 4.98 – Choisir le fichier ISO et lancer la VM.

Annexe 2

Installation de PfSense

❖ Création d'une machine virtuelle

Pour installer le firewall on va suivre la même procédure d'installation que la machine virtuelle .Avant de commencer l'installation de notre machine on doit lui attribuer au minimum deux cartes réseaux. Pour ce projet on va utiliser deux interfaces :

- **WAN :** pour qu'on puisse se connecter à l'internet.
- **LAN :** passerelle du réseau locale.

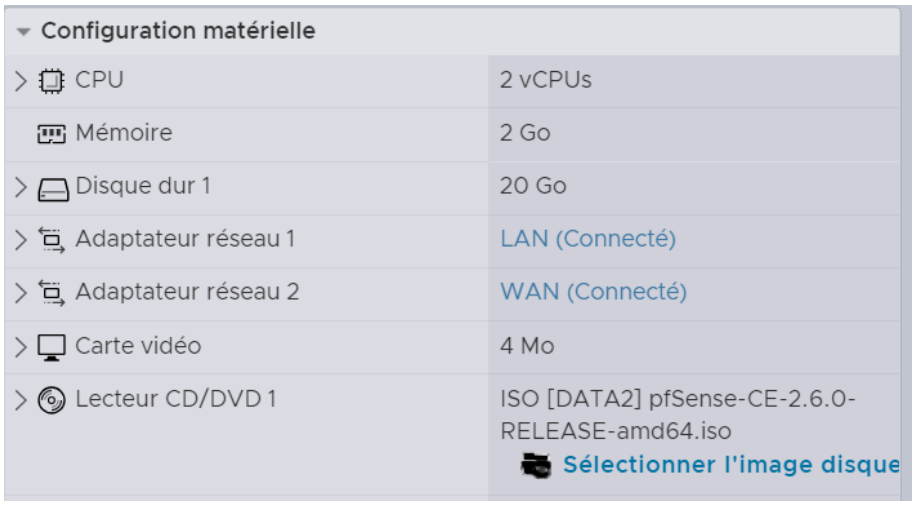

Figure 4.99 – Installation des cartes réseaux.

Pour commencer l'installation de PfSense, on clique sur mettre sous tension.

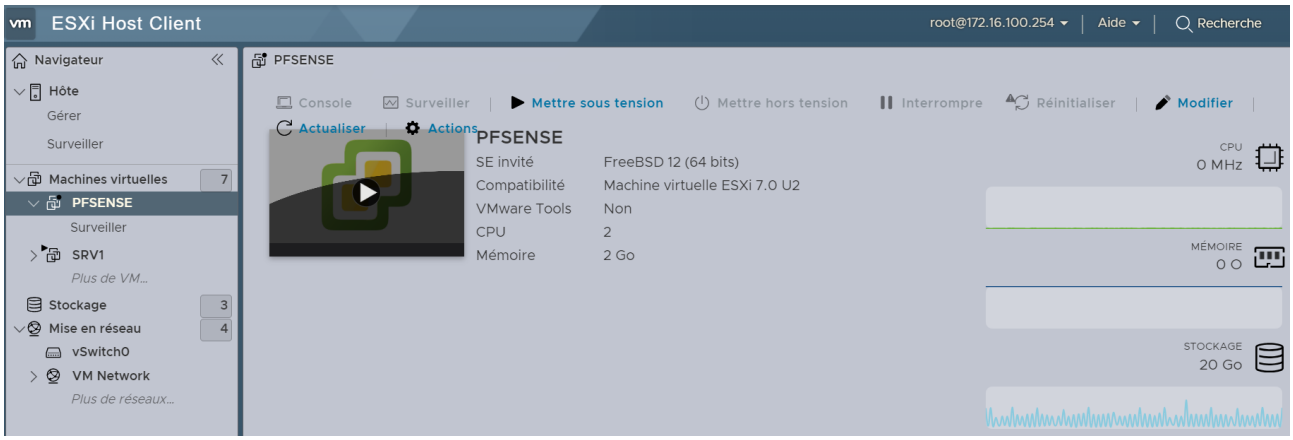

Figure 4.100 – La machine virtuelle de PfSense.

Après le démarrage de la machine virtuelle de PfSense, la fenêtre suivante s'affiche :

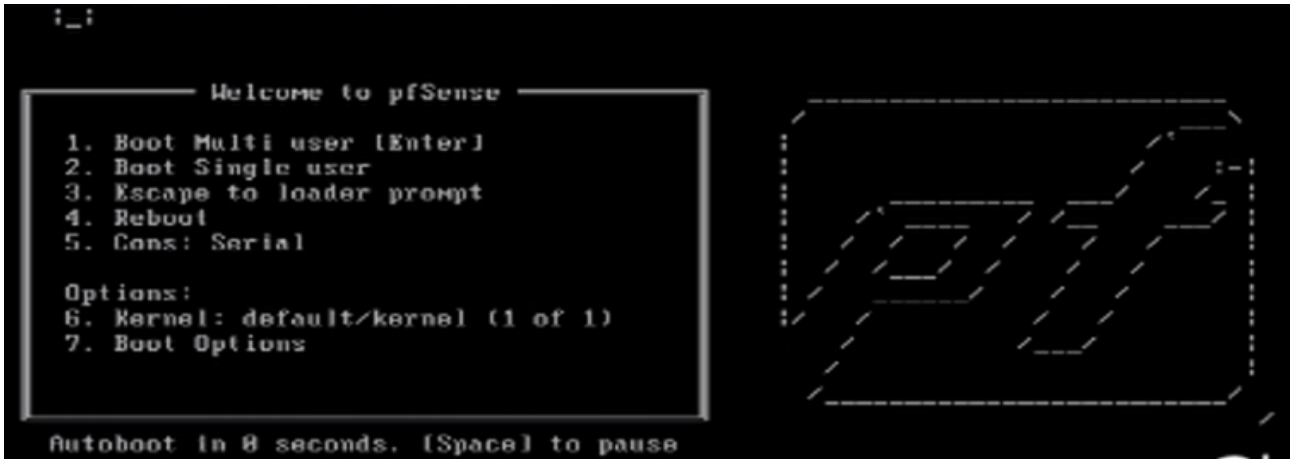

Figure 4.101 – Démarrage de PfSense.

À partir de là, on va suivre les étapes suivantes :

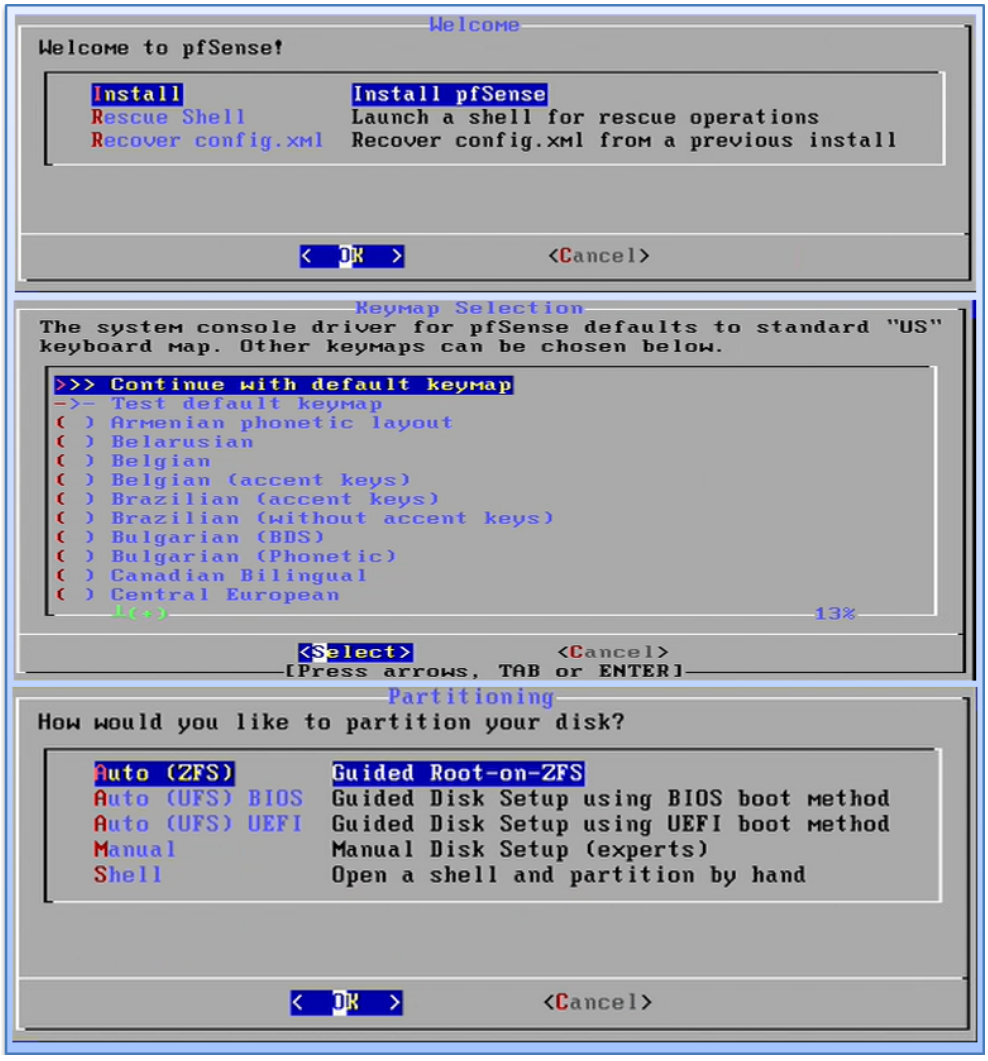

Figure 4.102 – Les étapes d'installation de PfSense.

Après quelques minutes, PfSense sera intégralement installé. De la même façon, nous avons installé tous les pare-feu.

Annexe 3

Installation d'OpenVPN

❖ Exporter la configuration OpenVPN

Afin d'exporter le protocol OpenVPN vers un poste client, on va suivre les étapes suivantes : on va accéder à la section OpenVPN / Client Export de l'interface, on va sélectionner l'option 'OpenVPN Clients', et pour finaliser l'opération on va cliquer sur 'Archive',pour récupérer tous les fichiers nécessaires.

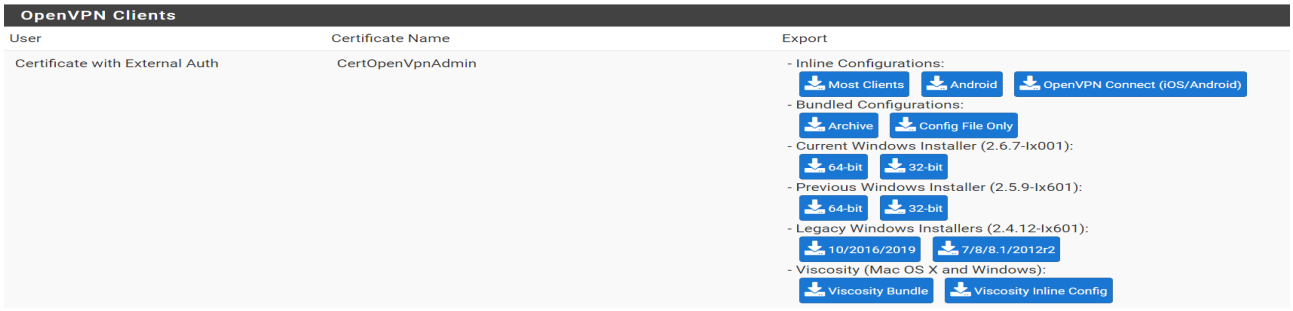

Figure 4.103 – Choix du client export.

On va lancer l'installation d'OpenVPN sur la machine.

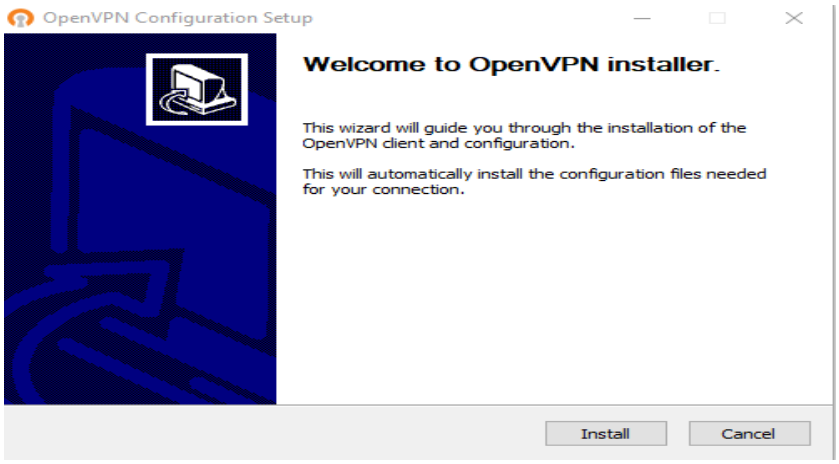

Figure 4.104 – Installation d'OpenVPN.

Une fois l'installation est terminée, on doit extraire le contenu de l'archive ZIP téléchargée depuis le Pfsense et qui contient la configuration.

Figure 4.105 – La configuration d'OpenVPN.

Résumé

L'objectif principal de notre projet est de virtualiser les serveurs du SPC GB et d'interconnecter les différents sites de l'entreprise de manière sécurisée. Pour réaliser cette interconnexion, nous avons décidé de mettre en place plusieurs pare-feux distants avec PfSense et d'implémenter une solution OpenVPN sur le pare-feu. Cette solution permettra d'interconnecter les sites à travers des tunnels sécurisés. Cette infrastructure combinée de virtualisation et de VPN via PfSense vise principalement à mieux gérer l'entreprise, à garantir la sécurité des données et réaliser les communications d'une manière transparente. Pour la mise en œuvre de notre projet, nous avons intégré divers environnements, notamment l'hyperviseur ESXI et le pare-feu PfSense, afin de réaliser notre architecture. Ainsi, nous avons configuré les serveurs nécessaires, tels que les serveurs AD, DNS et DHCP.

Mots clés : SPC GB, Pare-feu, VPN, PfSense, Tunnels, OpenVPN, ESXI, AD, DNS, DHCP.

Abstract

The main objective of our project is to virtualize the SPC GB servers and securely interconnect the company's various sites. To achieve this interconnection, we have decided to set up several remote firewalls using PfSense and implement an OpenVPN solution on the firewall. This solution will allow the sites to be interconnected through secure tunnels. This combined infrastructure of virtualization and VPN via PfSense primarily aims to better manage the company, ensure data security, and facilitate transparent communications. For the implementation of our project, we have integrated various environments, including the ESXI hypervisor and PfSense firewall, to create our architecture. We have configured the necessary servers, such as AD, DNS, and DHCP servers.

Keywords : SPC GB, Firewall, VPN, PfSense, Tunnels, OpenVPN, ESXI, AD, DNS, DHCP.