République Algérienne Démocratique et Populaire
Ministère de l'enseignement Supérieur et de la Recherche Scientifique

Université A/Mira de Béjaia
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de Master professionnel

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

Option
Administration et sécurité des réseaux

Thème

Installation et configuration d'un pare-feu *Pfsense*. Cas d'étude : Société de Gestion des Services et Infrastructures Aeroportuaires (SGSIA)

Présente par :
M. AMZAL Massinissa
M^{lle} BENYAHIA Cylia

Soutenu le 04 juillet 2024 devant le jury composé de :

Présidente	**Dr SAAD Narimane**	**U. A/Mira Béjaia.**
Examinatrice	**Dr ZAMOUCHE Djamila**	**U. A/Mira Béjaia.**
Examinatrice	**M^{lle} BOUAFIA Khadoudja**	**U. A/Mira Béjaia.**
Encadrante	**Dr CHERIFI Feriel**	**U. A/Mira Béjaia.**

Béjaia, Juillet 2024.

⁕ *Remerciements* ⁕

Nous souhaitons adresser nos remerciements les plus chaleureux aux membres du jury pour avoir acceptées de consacrer leur temps et leur expertise pour évaluer notre travail en profondeur.

Nous tenons également à exprimer notre gratitude envers nos encadrants à l'entreprise SGSIA aéroport d'Alger Monsieur Mohamed ABDELAZIZE CHOUKRI et Madame Sara FERRAH pour leur accueil chaleureux lors de notre stage pratique, qui nous a permis d'acquérir une expérience concrète et de mettre en pratique les connaissances acquises au cours de notre parcours universitaire.

Nous tenons à exprimer notre sincère gratitude envers notre encadrante madame CHERIFI Feriel, pour ses précieux conseils, son orientation éclairerai et son assistance précieuse.

Nous aimerions également exprimer notre profonde reconnaissance envers l'ensemble des enseignants et professeurs qui nous ont prodigue leur aide, sans oublier de remercier sincèrement tous ceux qui ont contribué, de prés ou de loin, à la réalisation de notre mémoire.

Et enfin, que nos chers parents et familles, trouvent ici l'expression de nos remerciements les plus sincères et les plus profonds en reconnaissance de leurs sacrifices, aides, soutien et encouragement afin de nous assurer cette formation dans les meilleures conditions.

⁂ *Ddédicaces* ⁂

Je souhaite exprimer ma gratitude envers mes parents et mes amis pour leur soutien et leur encouragement durant cette période de travail et de recherche.

MASSI

⁂ *Ddédicaces* ⁂

À mes parents,
votre amour inconditionnel et votre soutien sans faille ont été les piliers sur lesquels j'ai construit ce mémoire. Chaque étape de ce parcours académique a été éclairerai par votre encouragement constant et votre conviction en mes capacités. Merci pour votre sacrifice et votre dévouement qui ont fait de ce rêve une réalité.

À mes amis et collègues,
Ma deuxième famille AAI (Amazday Adelsan Inelmaden) et toutes la famille théâtrale, votre amitié et votre camaraderie ont rendu ce parcours enrichissant et joyeux. Vos encouragements et discussions stimulantes ont été essentiels pour maintenir ma motivation. Merci d'avoir partagé ce voyage avec moi et d'avoir rendu chaque étape mémorable.

Enfin, à moi-même,
pour avoir persévérer malgré les obstacles, pour avoir cru en mes capacités et pour avoir travaillé avec acharnement pour atteindre cet objectif. Ce mémoire est le fruit de mon engagement, de ma passion et de ma détermination à aller au-delà de mes limites. Chaque personne mentionnée ici a joué un rôle crucial dans la réalisation de ce mémoire. Leur soutien et leur inspiration ont façonne ce travail académique et je leur suis profondément reconnaissant.

CYLIA

Table des matières

Table des figures

Liste des tableaux

Notations et symboles

ARP	Address Resolution Protocol
$DHCP$	Dynamic Host Configuration Protocol
DIT	Direction des Infrastructures et des Travaux
DNS	Domain Name System
DSI	Département Systémes Informatique
$EGSA$	Etablissement de Gestion de Services Aéroportuaires
EPE	Entreprise Eublique Economique
$ETUSA$	Entreprise de Transport Urbain et Suburbain d'Alger
$HTTP$	HyperText Transfer Protocol
IP	Internet Protocol
LAN	Local Area Network
MAN	Metropolitan Area Network
OSI	Open Systems Interconnection
PAN	Personal Area Network
$RJ-45$	Registered Jack-45
$SGSIA$	Société de Gestion des Services et Infrastructures Aeroportuaires
SSH	Secure Shell
STP	Shielded Twisted Pair
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
USB	Universal Serial Bus
URL	Uniform Resource Locator
UTP	Unshielded Twisted Pair
$VLAN$	Virtual Local Area Network
WAN	Wide Area Network

Introduction générale

L'évolution du réseau Internet et de ses extensions sous la forme d'Intranet et d'extranet pose des problèmes majeurs de sécurité informatique. Toutes les entreprises, possédant un réseau local disposent aussi d'un accès à Internet, dans le but d'avoir accès à la quantité d'informations disponibles sur le réseau et avoir la possibilité de communiquer avec l'extérieur. Cependant, cette ouverture est à la fois nécessaire et risquée. En connectant l'entreprise vers un monde, elle s'expose au risque d'intrusions potentielles par des tiers, susceptibles de causer des dommages tels que la destruction de données, le vol d'informations sensibles, et la vulnérabilité accrue des appareils mobiles.

La société de la gestion des services et des infrastructures de l'aéroport d'Alger (SGSIA) est une entreprise spécialisée dans la gestion des services et d'exploiter l'infrastructure de l'aéroport, qui donne une grande importance à la sécurité en fonction de plusieurs mécanismes et une architecture sécurisée. Nous avons eu l'occasion d'effectuer notre stage au sein du département des systèmes informatiques (DSI) de la SGSIA et nous avons analysé leur réseau, ce qui nous a permis de soulever quelques faiblesses. Cette entreprise est vulnérable à des attaques malveillantes, des fuites de données et un risque d'accès non autorises aux systèmes et aux informations sensibles. De plus, les utilisateurs sont exposés à des publicités intrusives et à des sites web inappropriés.

Afin de garantir une sécurité du réseau local de l'entreprise, il est essentiel que le cœur de l'architecture doit être basé sur un pare-feu qui offre un véritable contrôle sur le trafic réseau de l'entreprise. C'est pour cela que nous avons installé et configuré un pare-feu *Pfsense* et dans ses services on a utilisé le portail captif, OpenVPN et AdGuard. Cela a permet d'analyser, de sécuriser, de gérer le trafic et ainsi d'utiliser le réseau de la façon pour laquelle il a été prévu et sans l'encombrer avec des activités inutiles et d'empêcher une personne sans autorisation d'accéder à ce réseau. C'est dans le but d'authentifier, de contrôler les activités des utilisateurs et d'identifier les sources de menaces et ses dégâts informationnels.

Notre mémoire est organisé de la façon suivante :

Dans le premier chapitre, nous traiterons des généralités sur les réseaux informatiques, en exa-

minant les catégories de réseaux, les équipements requis, les méthodes de transmission ainsi que les diverses architectures réseau. Ensuite, nous nous concentrerons sur les systèmes de sécurité, en abordant les principes de base, les vulnérabilités fréquentes, les politiques de sécurité et les outils disponibles pour sécuriser les infrastructures informatiques.
Le second chapitre sera consacré à la présentation de l'organisme d'accueil, la SGSIA, en détaillant son organigramme et les missions du Département Systèmes Informatiques (DSI). Nous y analyserons également la problématique rencontrée et la solution proposée pour renforcer la sécurité des réseaux de l'organisme.
Enfin, le troisième chapitre détaillera la mise en œuvre des solutions de sécurité, incluant l'installation et la configuration de pare-feu (*Pfsense*), la mise en place d'un portail captif, le filtrage via AdGuard, ainsi que l'accès distant sécurisé via VPN. Ce chapitre fournira une vue d'ensemble pratique sur les étapes et les outils utilisés pour réalisé notre solution.

Chapitre 1

Généralités sur les réseaux et les systèmes de sécurité

1.1 Introduction

Les réseaux informatiques ont pris une place centrale dans notre vie quotidienne, mais cela expose également nos vies à des risques d'attaques et à une surveillance constante, la sécurité des communications et des données est devenue une priorité essentielle à la fois pour les utilisateurs et les entreprises.

Pour construire un réseau et le sécuriser, il faut comprendre la signification de réseau ainsi d'avoir une connaissance sur ses catégories, les matériels physiques, les protocoles nécessaires pour la transmission d'informations et son système de sécurité. Nous aborderons l'ensemble de ces points tout au long de ce chapitre.

1.2 Les réseaux informatiques

Les réseaux informatiques sont nés du besoin de faire communiquer des terminaux distants, avec un site central, puis des ordinateurs entre eux, et enfin de connecter des machines terminales, telles que des stations de travail avec leurs serveurs. Dans un premier temps, ces communications étaient destinées au transport des données informatiques. Aujourd'hui, on se dirige vers des réseaux qui intègrent en plus des données, la parole et la vidéo [30]. Donc un réseau est un moyen de communication qui permet à des utilisateurs d'échanger des information et des services [12].
D'une autre manière, le réseau est un système qui permettant de relier deux à plusieurs machines entre elles. Un réseau est caractérisé par un aspect physique qui est constitué d'un ensemble de câble véhiculant des signaux électriques, et d'un aspect logique qui définit des règles de communication (des protocoles) [27].

1.2.1 Catégories des réseaux

Les réseaux informatiques peut être classifié en fonction de leur étendue géographique et de leur topologie, chacune présentant des avantages spécifiques pour satisfaire aux différentes exigences de connectivité et de performance.

1. **Selon leur étendu géographique**
   Comme illustré sur la figure 1.1, un réseau peut être classé selon son étendue [31].

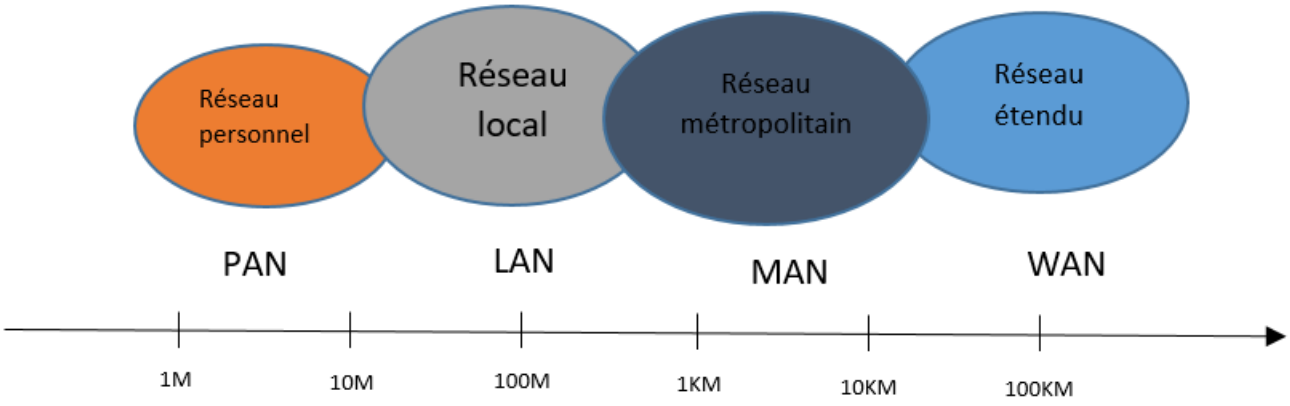

FIGURE 1.1 – Schéma de l'étendu d'un réseau informatique [12]

— **Le réseau personnel**(PAN : Personal Area Network) : il interconnecte sur quelque mètre des équipements personnels tel que smart-phone, clé USB, etc. De la façon indiquée dans la figure 1.2 [30]. C'est un réseau centré sur l'utilisateur, on le surnom aussi un réseau individuel ou un réseau domestique [12].

FIGURE 1.2 – Schéma réseau PAN [8]

— **Le réseau local** (LAN : Local Area Network) : il couvre une région géographique limitée qui s'étent sur quelques dizaines à quelques centaines de mètres [12]. Il serre au transport de toutes informations numériques, il relie physiquement les unités adjacentes, comme indiqué sur la figure 1.3 [30].

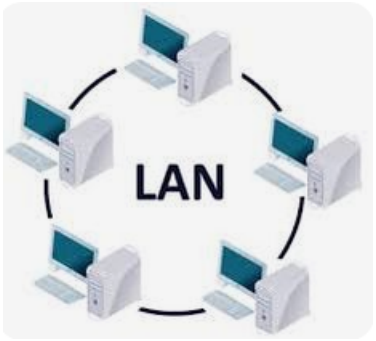

FIGURE 1.3 – Schéma de réseau LAN [8]

— **Le réseau métropolitain**(MAN : Metropolitan Area Network) : est également nommé réseau fédérateur, il assure des communications sur des distances de quelques dizaines de kilomètres, interconnecte plusieurs réseaux locaux LAN, tel que montré sur la figure 1.4 [12].

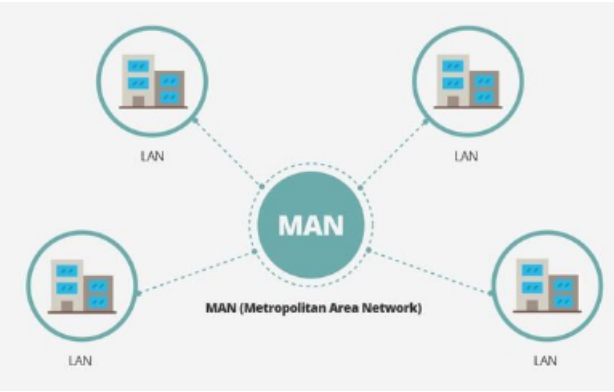

FIGURE 1.4 – Schéma de réseau MAN [8]

— **Le réseau étendu**(WAN : Wide Area Network) : relie des unités sur des distances à l'échelle d'un pays, continent ou plusieurs continents, comme décrit la figure 1.5 [30]. Le réseau étendu est constitué des réseaux de type LAN et MAN [12].

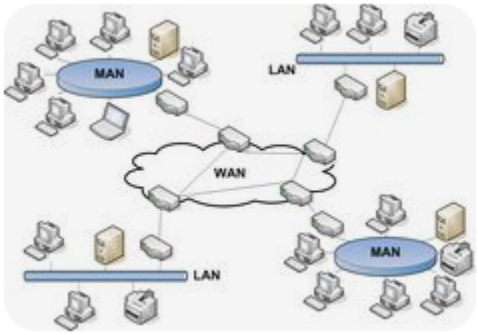

FIGURE 1.5 – Schéma de réseau WAN [8]

2. **Selon la topologie**

Il faut distinguer deux type de topologie, la topologie physique et la topologie logique. La première décrit et définit la manière dont les équipements échangent leurs données sur les réseaux locaux, la deuxième topologie logiques sont considérés, le bus et l'anneau. On peut utiliser différentes topologies physiques pour réaliser une topologie logique [17]. La seconde topologie représente la structure et la forme physique du réseau. Il existe plusieurs topologies physiques [36] :

— **Topologie en bus :** elle consiste à utiliser un long câble, sur lequel les équipements sont connectés en série de la manière illustré dans la figure 1.6, il existe qu'un seul chemin sans boucle entre les équipements du réseau local [17]. L'avantage de connexion sur une topologie en bus, c'est une connexion sécurisée, ces connexions passives sont simples et faciles à réaliser sur un câble coaxial ou paire de fils métalliques [28]. La topologie en bus n'a pas que des avantages, il existe aussi des inconvénients, étant donné que le câble de transmission est commun, il peut avoir des collisions quand deux machines communiquent simultanément, en plus la vitesse de transmission est très faible [36].

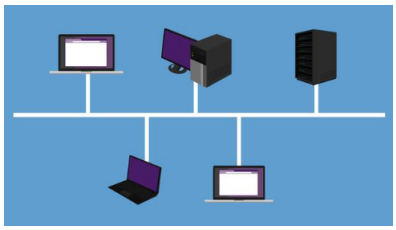

FIGURE 1.6 – Schéma de topologie en bus [7]

— **Topologie en anneau :** dans cette topologie, le support relie tous les équipements sur une forme d'un circuit en boucle conformément à ce qui est illustré dans la figure 1.7, l'information circule dans une seule direction [28]. On peut dire que le réseau en anneau c'est comme un réseau en bus avec les équipements disposées en cercle, sauf que la topologie en anneau ne possède pas le problème de collision de données [36]. Cependant la connexion en anneau manque de fiabilité en cas de rupture du support, il existe une solution qui consiste à réaliser un double anneau qui peuvent transmettre soit dans le même sens ou en sens inverse, il est préférable en sens inverse [17].

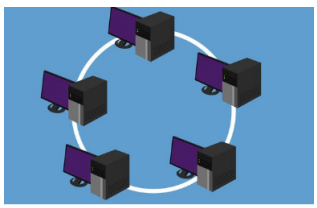

FIGURE 1.7 – Schéma de topologie en anneau [7]

— **Topologie en étoile :** dans un réseau en étoile, la forme physique du réseau ressemble à une étoile tel que montré dans la figure 1.8, dans le quelle chaque équipements d'un réseau est connecté à un central (routeur, commutateur, ...). Le principal défaut de cette topologie, c'est que si l'élément central ne fonctionne plus, toute communication est impossible [36].

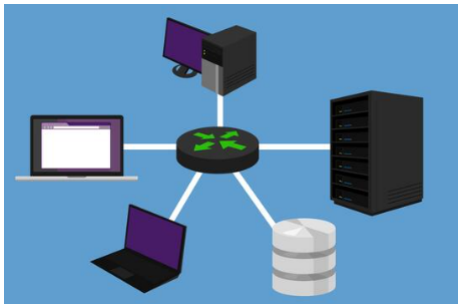

FIGURE 1.8 – Schéma de topologie en étoile [7]

1.2.2 Les équipements réseau

Dans le but de faciliter la communication, différents types d'équipement ont été développés [39].

— **Ordinateur** Un ordinateur est une machine dotée d'une unité de traitement lui permettant d'exécuter des programmes enregistrés. C'est un ensemble de circuits électroniques permettant de manipuler des données sous forme binaire. Cette machine permet de traiter automatiquement les données, ou informations, selon des séquences d'instructions prédéfinies appelées aussi programmes. Elle interagit avec l'environnement grâce à des périphériques comme le moniteur, le clavier, la souris, le lecteur de CD. Les ordinateurs peuvent être classés selon plusieurs critères comme le domaine d'application, taille ou architecture [5].

— **Carte réseau**

Elle se trouve dans un ordinateur connecté au réseau ; c'est une carte électronique qui porte le nom de carte réseau mais elle est aussi appelée NIC (Network Interface Card). Bien que la carte réseau soit en général intégrée à la carte mère de votre ordinateur, sur les ordinateurs récents, vous avez la possibilité d'utiliser une interface réseau externe reliée à l'ordinateur par le port USB de ce dernier [26].

— **Concentrateur (Hub)** Il permet de concentrer le trafic provenant de différents équipements terminaux, cela peut se réaliser par une concentration du câblage en un point donné ou par une concentration des données qui arrivent simultanément par plusieurs lignes de communication [29].

Généralement le câble de raccordement entre les équipements et le concentrateur est une

paire torsadée [17]. Le concentrateur c'est un équipement qu'agit au niveau de la couche 1(couche physique) de modèle OSI [39].
Avec le développement des réseaux, le concentrateur en tant que organe spécifique tend à disparaitre. Il a été remplacé par un micro-ordinateur, comme une passerelle ou un commutateur (la figure 1.9)[33].

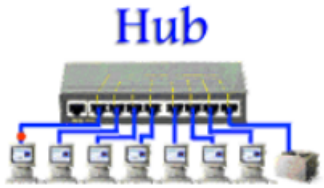

FIGURE 1.9 – Concentrateur(hub) [38]

— **Commutateur (Switch)** C'est un élément actif agissant au niveau de la couche 2 (couche liaison) du modèle OSI [39].
Un commutateur (la figure 1.10) fonctionne à peu prés comme un hub, sauf qu'il est plus discret et intelligent, Il n'envoie pas tout ce qu'il reçoit à tout le monde, mais il l'envoie uniquement au destinataire. Afin de déterminer l'équipement à qui il faut renvoyer les données, le switch se base sur les adresses physiques (adresses MAC) des cartes réseau [36].
On peut dire que le commutateur est l'un des atouts majeurs des systèmes de communication. Il prend en charge les paquets et il les Transférer vers le récepteur en utilisant des identificateurs. Un identificateur est une suite de chiffres accompagnant un bloc (trame, paquet) pour lui permettre de choisir une porte de sortie au sein d'une table de commutation [29].
Le commutateur se comporte donc comme une mémoire vive. Comme il gère simultanément plusieurs échanges, la taille de la mémoire nécessaire à la gestion des messages est importante [17].
L'installation d'un commutateur est généralement très simple, il suffit de brancher le cordon d'alimentation puis de connecter les câbles de raccordement du réseau. Chaque port est une prise RJ-45 à laquelle est associée un électroluminescente qui s'allume lorsqu'une connexion est établie sur ce port [26].

FIGURE 1.10 – Commutateur [38]

— **Passerelle (Gateway)** une passerelle est un autre ordinateur qui a plusieurs cartes réseau, elle peut communiquer avec plusieurs sous-réseaux [36].
La passerelle assure une compatibilité au niveau des protocoles de couches hautes entre les réseaux qui sont composées des différents types d'équipements, de technologies ou de protocoles [17].
Si on se tient à cette définition de la passerelle, on peut réaliser une interconnexion des réseaux à n'importe quel niveau de couche du modèle OSI ou TCP/IP. Il y a plusieurs différentes catégories de passerelles, un répéteur est une passerelle de niveau 1, qu'agit au niveau de la couche 1 (couche physique), un pont est une passerelle de niveau 2, qu'agit au niveau de la couche 2 (couche liaison), un relais ou un routeur est une passerelle de niveau 3, qu'agit au niveau de la couche 3 (couche réseau), un relais de transport est une passerelle de niveau 4, qu'agit au niveau de la couche 4 (couche transport) [29].

— **Routeur (Router)** C'est un dispositif d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter [39].
Le routeur (la figure 1.11) possède au moins deux interfaces, et il agit au niveau 3 (couche réseau). Il est constitué de deux éléments, une composante matérielle comme des ports qui reçoivent des trames. Cette partie elle raccorde n'importe quel type de réseau. Le second élément est une composante logicielle, il s'agit d'un système d'exploitation, cette partie a en charge de déterminer vers quelle interface envoyer un paquet reçu [19].
Lorsqu'un routeur reçoit sur l'une de ses interfaces une trame qu'il a reçu, il la décapsule et extrait le data-gramme IP qu'elle contenait. Le rôle du routeur est de chercher dans sa table de routage la route qui permet d'atteindre le réseau destiné. Le routeur contient la liste des réseaux connus et l'adresse du routeur suivant ainsi peut en déduire le chemin à suivre à partir des informations de sa table de routage [17].
Les routeurs sont notre première ligne de défense et doivent être configurés de manière à ne transmettre que le trafic autorisé par les administrateurs réseau. Les routages peuvent être configurés comme statiques ou dynamiques. S'ils sont statiques, ils ne peuvent être configurés que manuellement et restent ainsi jusqu'à ce qu'ils soient modifiés. S'ils sont dynamiques, les routeurs apprennent l'existence des autres routeurs de leur environnement et utilisent les informations sur ceux-ci pour élaborer leurs tables de routage [6].

FIGURE 1.11 – Routeur [38]

— **Serveur** Un serveur est un dispositif informatique qui fournit des services à un client ou plusieurs sur un réseau. Il peut être un ordinateur ou un système qui offre des ressources, des données, des services ou des logiciels à d'autres ordinateurs. parmi les différents types des serveurs nous distinguons [1] :
  — Serveur web : c'est un serveur qui est conçu pour stocker, traiter et distribuer des ressources telles que des pages web et d'autre contenus sur Internet, et il répondre aux requêtes des clients via le protocole HTTP ou HTTPs.
  — Serveur de fichiers : ce serveur enregistre et distribue les documents et fichiers partagés par les utilisateurs.
  — Serveur d'application : il permet d'utiliser un programme sur un serveur à partir de tous les postes clients simultanément, principalement des applications qui utilisent des bases de données (gestion de fabrication, commerciale, comptabilité, stock, ...). Ces applications doivent être programmées pour gérer les partages.

1.2.3 Moyen de transmission

En informatique les moyens de transmission sont les moyens utilisés pour rendre possible la communication et l'échange des données entre les équipements du réseau. Nous verrons donc quels sont les moyens de connexion et comment ils sont reliés entre eux [36].

1.2.3.1 Moyens physique

Deux familles sont à distinguer comme indiqué dans le tableau 1.1, les supports métalliques et non métalliques. Les supports métalliques comme les paires torsadées et les câble coaxiaux, sont les plus anciens et les plus utilisées. Les non métalliques comme les fibres optiques [17]. Nous présenterons dans ce qui suit une brève description.

— **Paires torsadées** C'est l'un des supports de transmission les plus anciens et il est toujours d'actualité. Comme l'indique la figure 1.12, une paire torsadée est constituée de deux fils de cuivre isolés. Ces fils sont enroulés les uns autour des autres de manière hélicoïdale, tout comme une molécule d'ADN. Cela permet de réduire les rayonnements électromagnétiques parasites [18].
— **Câble coaxial** : il est composé d'un fil, entouré d'une couche d'isolant, elle-même entourée d'une couche de blindage, et le tout est enroulé par une couche de protection isolante. Ces câbles réseau sont très puissants. Leurs débits vont de 56 kilobits à plusieurs gigabits. Ils sont utilisés aussi bien dans les réseaux locaux que dans les liaisons longues distance. Ces câbles transportent à la fois des signaux analogiques et numériques. Le câble coaxial est largement utilisé pour connecter une antenne parabolique à un décodeur ou un téléviseur [18].
  Il existe deux catégories de câble coaxial, dans le première la gaine isolante est fabriquée

Type de câble	Protection électromagnétique	Débit courant	Distance	Utilisation
Coaxial	Bonne	10 Mbits/s	2500 m par segment de 500 m	Ethernet, en environnement perturbé ou confidentiel
Paire torsadée UTP	Faible	10 à 100 Mbits/s	100 m	Ethernet sur paire torsadée
Paire torsadée STP	Moyenne	10 à 100 Mbits/s	100 m	Ethernet sur paire torsadée
Fibre optique	Excellente	100 à 1000 Mbits/s	de quelques km à une centaine de km	réseaux haut débit

TABLEAU 1.1 – Les différents câbles[33]

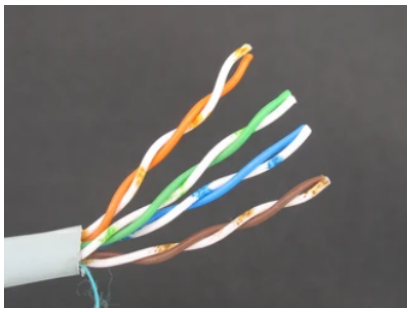

FIGURE 1.12 – Câble paire torsadée [10]

en PVC. Il est le plus répandus et le moins cher, en cas d'incendie il dégage des fumées toxiques. La seconde catégorie le câble est fabrique en téflon, il est résistant au feu en cas d'incendie [12]. La figure 1.13 montre un modèle de câble coaxial.

FIGURE 1.13 – Câble coaxial [10]

— **La fibre optique** : une fibre optique est un fil de verre extrêmement fin, puisqu'il mesure environ un dixième d'un cheveu humain. Il a la capacité de conduire la lumière et est utilisé pour transmettre des données numériques ou pour des explorations visuelles dans le milieu

médical. [18]
La fibre optique offre un débit nettement supérieur à celui des câbles coaxiaux, pour cette raison la fibre est considéré comme la forme la plus rapide, la plus faible et la plus coûteuse de la connexion Internet [26]. Un exemple est illustré dans la figure 1.14.

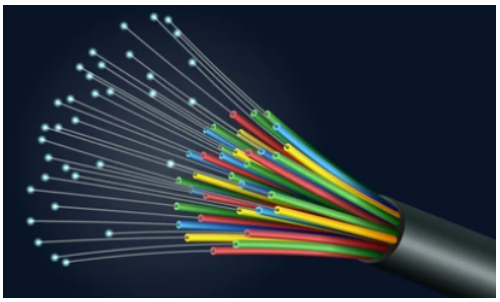

FIGURE 1.14 – Câble fibre optique [10]

1.2.3.2 Accès sans fils

Un réseau sans fils est un réseau qui n'utilise pas des câbles mais des signaux radio pour échanger des informations. Quelques exemples sur le réseau sans fils, le Bluetooth, infrarouge, Wi-Fi, etc. [26].

1.2.4 Architecture des réseaux

Un réseau permet de connecter des ordinateurs de tous types pour partager des ressources (la figure 1.15). Deux types d'ordinateurs sont utilisés sur un réseau : les ordinateurs du réseau et les clients. Les serveurs partagent leurs ressources, les clients utilisent ces ressources [26].

1.2.4.1 Client/Serveur

L'ordinateur du réseau qui possède les disques, l'imprimante et autres ressources partagées avec d'autres ordinateurs est un serveur. Tout ordinateur qui n'est pas un serveur est un client. Un ordinateur est un serveur ou un client, mais pas les deux à la fois. Un serveur ne peut pas devenir client et un client ne peut pas devenir serveur [26].
Le serveur assure la mise à disposition et la gestion des ressources partagées entre les clients. Chaque serveur dispose en principe d'une mémoire de masse importante, qui contient tout ou partie des fichiers et programmes communs. Il est souvent équipé d'une ou plusieurs. Ce doit donc être une machine rapide et relativement puissante [22].

1.2.4.2 Poste à poste

Ce type de réseau est nommé aussi pair à pair ou point à point, et peer to peer en anglais. Dans les réseaux modernes, chaque ordinateur a la capacité de jouer le rôle à la fois de client et de serveur. Par conséquent, tout ordinateur peut partager ses périphériques tels que l'imprimante ou les disques avec les autres ordinateurs du réseau [26].

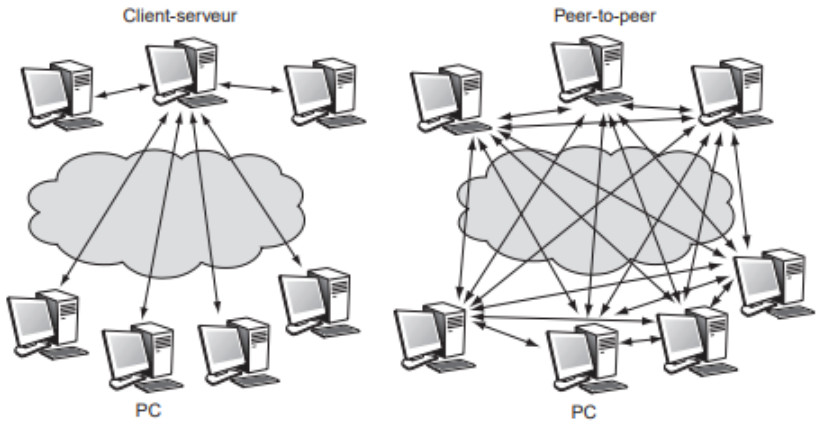

FIGURE 1.15 – Comparaison point à point et serveur client [29]

1.2.5 Architecture protocolaire

L'architecture réseau assure à l'utilisateur un accès fluide et transparent aux ressources informatiques, offrant un service identique que ces ressources soient locales ou distantes. Pour réaliser une interconnexion transparente entre des équipements provenant de constructeurs différents, pour qu'ils s'échangent des informations nécessite que ceux-ci utilisent non seulement des techniques de connexion, mais aussi des protocoles d'échange identiques et une sémantique de l'information compréhensible par les partenaires de la communication. Aussi, pour éviter une description trop complexe, le système a été découpé en entités fonctionnelles appelées couches. Une couche est donc un ensemble homogène destiné à accomplir une tâche ou à rendre un service. La prise en compte d'une nouvelle technologie ne remet en cause que la couche concernée. Le modèle de référence est une architecture en couches [26].

1.2.5.1 Modèle OSI

Le modèle OSI (Open Systems Interconnection) est une façon standardisée de segmenter en plusieurs blocs le processus de communication entre deux entités. Chaque bloc résultant de cette segmentation est appelé couche. Une couche est un ensemble de services accomplissant un but

précis, chaque couche du modèle OSI communique avec la couche au-dessus. Ainsi le modèle OSI permet de comprendre de façon détaillée comment s'effectue la communication entre les équipements. Le modèle OSI est constitué de 7 couches : Physique, liaison de donnée, réseau, transport, session, présentation, application [36].
Les trois premières couches constituent les couches basses où les contraintes du réseau sont perceptibles. Les trois dernières couches constituent les couches hautes où les contraintes de l'application sont perceptibles [34].

- **Niveau application (couche 7)** : elle constitue la dernière couche du modèle OSI. Il fournit aux processus applicatifs le moyen d'accéder à l'environnement réseau. Ces processus échangent leurs informations par l'intermédiaire des entités d'application. La couche 7 contient toutes les fonctions impliquant des communications entre systèmes, en particulier si elles ne sont pas réalisées par les niveaux inférieurs. Il s'occupe essentiellement de la sémantique [29].
- **Niveau présentation (couche 6)** : consiste à garantir la signification des données transférées. Elle garantit à la couche application l'accès aux services de la couche session [33]. Elle effectue le formatage des données, le transcodage des caractères et le cryptage des informations si nécessaire [32].
- **Niveau session (couche 5)** : elle permet l'ouverture et la fermeture d'une session de travail entre deux systèmes distants et assure la synchronisation du dialogue. Elle décide du mode de transmission, et ajoute au paquet de données des informations de contrôle déterminant entre autre le type de trame, le numéro de la trame dans le message à transmettre [22].
- **Niveau transport (couche 4)** : assure un service de transport de bout en bout, même à travers plusieurs réseaux. Elle est également chargée de fournir des services qui ne sont pas pris en charge par les couches inférieures, tels que la détection et la correction d'erreurs et le routage. En tant que dernier niveau impliqué dans le cheminement des données, la couche transport effectue la segmentation des messages de données en paquets au niveau de l'émetteur, puis les réassemblé dans le bon ordre au niveau du récepteur. Cette couche permet le multiplexage de plusieurs flux d'informations sur un même support, ainsi que leur démultiplexage inverse [22].
- **Niveau réseau (couche 3)** : est responsable de l'acheminement des données à travers l'ensemble du réseau en utilisant des informations d'adressage. Elle gère le choix des chemins (adressage et routage des paquets de données entre les nœuds du réseau), ainsi que les éventuels multiplexages et le contrôle de flux. En cas de surcharge ou de panne d'un nœud, le contrôle de flux doit éviter les congestions en redirigeant les données vers un autre nœud disponible. En plus de cela, la couche réseau s'occupe également de convertir les adresses logiques en adresses physiques [22].
- **Niveau liaison (couche 2)** : elle est chargée de garantir le bon acheminement des blocs d'informations. Cette couche établit des règles pour l'émission et la réception des données à travers la connexion physique de deux systèmes, assurant ainsi la transmission sans erreur

et déterminant la méthode d'accès au support. Les données circulant sur le réseau sont généralement structurées en trames. La couche liaison gère ces trames et assure la détection et la correction des erreurs [22].

— **Niveau physique (couche 1)** : elle correspond aux règles et procédures nécessaires pour acheminer les éléments binaires sur le support physique. On trouve dans le niveau physique les équipements réseau qui manipulent directement les éléments binaires, tels que les modems, les concentrateurs, les ponts... [29].

1.2.5.2 Modèle TCP/IP

Le modèle TCP/IP a été conçu comme un cadre opérationnel pour soutenir les protocoles fonctionnant sur des réseaux locaux (LAN) et étendus (WAN). Le modèle TCP/IP comprend 4 couches : application, transport, Internet et accès réseau. La fonctionnalité de ces couches est équivalente à celle du modèle OSI. Cependant il faut remarquer que la couche accès réseau regroupe deux couches liaison et physique du modèle OSI, de même la couche application regroupe trois couches, application, présentation et session [32].

— **Niveau application (couche 4)** : elle correspond aux 3 couches 5, 6 et 7 du modèle OSI. En réalité il apparaît que les couches 5 (session) et 6 (présentation) sont très peu utilisées voir inutiles. Leur rôle est souvent effectué par le logiciel. Le principal choix que fait cette couche est le protocole de transport qui doit être utilisé [24].

— **Niveau transport (couche 3)** : elle est identique dans son rôle à celle du modèle OSI. Son rôle est de fragmenter et réassembler les messages lors d'une communication entre 2 entités. Il existe 2 implémentations principales de cette couche, TCP (Transport Control Protocol) et UDP (User Datagram Protocol) [24].

— **Niveau Internet (couche 2)** : autrement dit la couche IP, correspond à la couche 3 du modèle OSI. En effet, cette couche doit gérer l'envoi des paquets et leur réception. Le paquet doit donc pouvoir trouver seul son chemin à travers le réseau. De plus, les paquets pouvant arriver en désordre, cette couche se doit de pouvoir les remettre en ordre et fournir des éléments qui permettent de les remettre dans le bon ordre [24].

— **Niveau accès réseau (couche 1)** : assure le formatage des données en trames et leur acheminement sans erreur à travers un réseau physique. C'est à ce niveau que se déroule la transmission de bits sur un support physique de communication [32].

La figure 1.16 présente une comparaison entre le deux modèle OSI et TCP/IP.

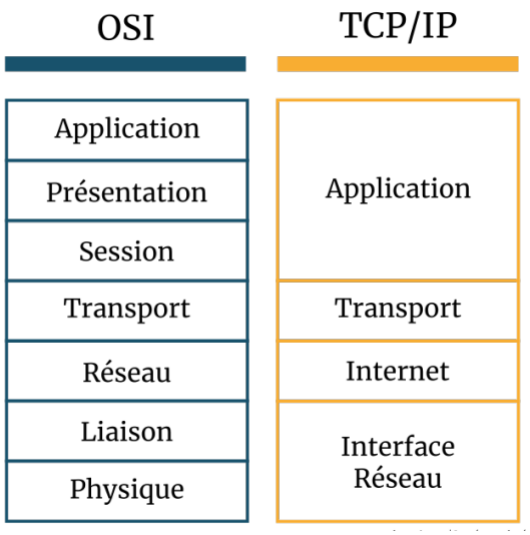

FIGURE 1.16 – Les modèles OSI, TCP/IP et leur différence [36]

1.2.5.3 Différents protocoles

Un protocole réseau est un ensemble de règles qui définit comment les équipements communiquent entre eux. Il permet également de garantir la sécurité et la confidentialité des données. Il existe différents types de protocoles, chacun a ces propres caractéristique et fonctionnalités [11].Dans ce qui suit nous allons présenté quelques protocoles :

- **Protocole DHCP (Dynamic Host Configuration Protocol)** : est un protocole de la couche application. Il permet d'obtenir dynamiquement une adresse à un client DHCP lorsqu'il doit être connecté à un réseau pour une durée limitée. Cette durée de vie est appelée un bail. Le client renvoit l'adresse au serveur à n'importe quel moment, le serveur réclame automatiquement l'adresse après l'expiration de bail. Le DHCP est utile dans les réseaux de grand taille où un grand nombre de machines [15].
- **Protocole TCP (Transmission Control Protocol)** : il regroupe les fonctionnalités de la couche transport. Il offre un service de transport fiable, le transfert des données ne peut commencer qu'après l'établissement d'une connexion entre deux machines [28].
  Pour pouvoir assurer ce service, les fonctionnalités suivantes sont nécessaires : 1. transfert de données de base, en découpant le flux transférer, TCP décide de lui-même là où le flux de données doit être coupé. 2. correction d'erreur, TCP est sensé récupérer les erreurs de la transmission Internet. 3. contrôle de flux, contrôler le débit de données envoyé par l'émetteur. 4. multiplexage, permet à plusieurs tâches d'une même machine de communiquer simultanément via TCP, le protocole définit un ensemble d'adresses et de ports pour la machine [34].
- **Protocole UDP (User Datagram Protocol)** : est un protocole non fiable et sans connexion, de la couche transport. Il permet à une application d'envoyer un message à

une autre avec un minimum de fonctionnalités, pas de garantie d'arrivée, pas de contrôle de flux, ou de congestion. Il est parfait pour les applications telles que les requêtes de configuration dynamique DHCP, ou dans les applications audio et vidéo [34].
Il utilise la notion de port, qui permet de distinguer les différentes applications qui s'exécutent sur une machine. Il offre la possibilité d'une exécution rapide, en prenant en considération les contraintes de temps réel ou les limitations d'espace sur un processeur [28].

— **Protocole IP (Internet Protocol)** : c'est un protocole de la couche Internet du modèle TCP/IP, et la couche réseau du modèle OSI. Le protocole IP transfère les données à travers une interconnexion de réseaux. Il cherche un chemin pour transférer les données d'un équipement émetteur, identifié par son adresse IP, à un équipement destinataire, identifié lui aussi par son adresse IP. Chaque datagramme est géré indépendamment des autres [17].
— **Protocole HTTP (HyperText Transfer Protocol)** : c'est un protocole de la couche application qui permet d'envoyer une page web d'un serveur web vers un ordinateur équipé d'un navigateur [27].
— **Protocole ARP (Address Resolution Protocol)** : il convertit l'adresse IP en adresse physique et il permet aux machines de résoudre les adresses sans utiliser la table statique. Une machine détermine l'adresse physique du destinataire en utilisant le protocole ARP [28].
— **Protocole DNS (Domain Name System)** : est un système mettant une correspondance entre un nom logique et un identifiant (numérique). Il consiste en deux parties : une hiérarchie de noms logique et un système d'adresses IP. Le DNS est essentiel pour la navigation sur Internet, car il simplifie le processus d'accès aux sites web en remplaçant les adresse IP difficiles a retenir par des noms de domaine facilement reconnaissables [34].
— **Protocole RDP (Remote Desktop Protocol)** : est une norme technique permettant l'utilisation d'un poste de travail à distance. Initialement publié par Microsoft, RDP est disponible pour la majorité des systèmes d'exploitation Windows, et peut également être utilisé sur des systèmes d'exploitation Mac [4].

1.3 Systéme de sécurité

La sécurité informatique recouvre l'ensemble de techniques informatiques permettant de réduire au maximum les chances de fuites d'informations, de modification de données ou de détérioration des services. C'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles et des techniques qui assurent que les ressources du système d'information d'une organisation sont utilisées uniquement dans le cadre où il est prévu qu'elles le soient [13].

1.3.1 Principes de sécurité

Pour mettre en place une politique de sécurité, il faut d'abord commencer par identifier la menace et le risque potentiel. Il faut connaître les motivations des attaquants et prévoir la façon dont ils procèdent pour s'en protéger et limiter les risques d'intrusion [20].
La notion de sécurité fait référence à la propriété d'un système, qui s'exprime généralement en termes d'intégrité, de disponibilité et de confidentialité. Des fonctions additionnelles peuvent offrir des services complémentaires pour confirmer l'authentification, et pour prouver l'existence d'une action à des fins de non-répudiation. Ce sont des approches complémentaires d'ingénierie et de gestion de la sécurité informatique qui permettent d'offrir un niveau de sécurité cohérent au regard de besoins de sécurité clairement exprimés [21].
Les cinq concepts de base de la sécurité sont :

- **L'intégrité** : il faut garantir à chaque instant que les données qui circulent sont bien celles que l'on suppose, et qu'elles n'ont pas été modifiées intentionnellement ou accidentellement pendant la transmission. Ceci implique la vérification de l'intégralité, de la précision, de l'authenticité et de la validité des données à tout moment [20].
- **La confidentialité** : seules les personnes habilitées doivent avoir accès aux données. Toute interception ne doit pas être en mesure d'aboutir, les données doivent être cryptées, seuls les acteurs de la transaction possédant la clé de compréhension [20].
- **La disponibilité** : est relative à la période de temps pendant laquelle le service qu'elle offre est opérationnel. Il ne suffit pas qu'une ressource soit disponible, elle doit pouvoir être utilisable avec des temps de réponse acceptables [21].
- **L'authentification** : cette procédure implique de prouver son identité. Par exemple, cela peut se faire en utilisant un mot de passe ou une méthode de défi basée sur une fonction cryptographique et un secret partagé [35].
- **non-répudiation** : elle consiste à prouver l'origine des données. Généralement cette opération utilise une signature asymétrique en chiffrant l'empreinte du message avec la clé privée de son auteur [35].

1.3.2 Vulnérabilité et menaces

Les systèmes informatiques sont exposés à des risques lié de manière étroite à la menace et à la vulnérabilité.

1.3.2.1 La vulnérabilité

La vulnérabilité représente les failles, les brèches dans le système, et tout ce qu'expose le système à la menace [20].
Trois facteurs de vulnérabilité amplifient les failles des systèmes informatiques modernes : Complexité, Extensibilité, Connectivité.

- **La complexité :** les logiciels sont devenus de plus en plus complexes, ce qui rend difficile pour les développeurs de maîtriser tous les bugs et comportements non désirés.
- **L'extensibilité :** au fil de sa durée de vie, la configuration d'une plateforme informatique subit des modifications constantes.
- **La connectivité :** les vulnérabilités des logiciels peuvent être exploitées à distance en raison de l'interconnexion croissante des systèmes [35].

1.3.2.2 La menace

La menace contre un système se traduit par une variété d'actions malveillantes, telles que les attaques, l'espionnage, le vol d'informations, et ainsi de suite [20]. Le système est exposé à des risques de perte de confidentialité et l'indisponibilité des données. Les risques peuvent se réaliser si les systèmes menacés présentent des vulnérabilités [25].
Les types de menaces sont nombreux et variés. Voici quelques exemples :

— **Attaque de l'homme du milieu :** un pirate crée un point d'accès factice à partir duquel il peut lire l'ensemble de votre trafic et insérer des communications factices, mais d'apparence réelle.
— **Attaque par saturation :** un cybercriminel empêche les utilisateurs légitimes d'accéder au réseau sans fil.
— **Cheval de Troie :** programme apparemment inoffensif, mais dont l'intention cachée est malveillante.
— **Logiciel espion (spyware) :** logiciel indésirable qui surveille secrètement l'activité d'un utilisateur et enregistre en général des informations personnelles pour les transmettre.
— **Virus :** code écrit afin de se répliquer. Un virus tente de se répandre d'un ordinateur à l'autre en infectant d'autres fichiers.
— **Ver :** type de virus qui peut répandre des copies de lui-même ou de ses segments sur les réseaux [37].

1.3.3 Politique de sécurité

Une politique de sécurité contribue à la maîtrise de risque, en réduisant la probabilité d'incidents intentionnels ou non-intentionnels, et leurs impacts sur l'organisation. Une politique de sécurité est élaborée en analysant les risques et en répondant aux besoins de sécurité, dans un contexte donné. Elle se traduit par la mise en place de mesures, de fonctions et de procédures appropriées :

- Des règles pour classer l'information et utiliser les ressources de manière appropriée et réaliser un plan d'actions, ou un tableau de bord de la sécurité d'un système d'information.
- Employés des outils pour sécuriser et protéger les systèmes informatiques.

- Les contrats de service établissent clairement qui doit faire quoi et quelles sont les responsabilités et les engagements de chaque partie [21].

1.3.4 Outils de sécurité

Pour sécuriser un réseau nous avons besoins de plusieurs systèmes, logiciels et matériels qu'on présente dans ce qui suit :

— **Pare-feu** : également connu sous le terme Firewall en anglais, c'est un dispositif informatique qui peut être matériel (*Cisco ASA*, *FortiGate*, *SonicWall*, ...) ou logiciel (*Pfsense*, *comodo*, *GlassWire*, ...). Dans le cas où le pare-feu est un logiciel, ses fonctions sont implémentées à l'aide d'un logiciel adapté qui filtre les entrées et sorties sur une carte réseau à partir de règles prédéfinies et configurables. Un pare-feu a pour rôle d'interconnecter deux réseaux ayant des niveaux de sécurité différents et d'éviter la propagation d'attaques entre les réseaux reliés [13].

Les principales fonctions d'un pare-feu incluent l'analyse du trafic au niveau des paquets, l'évaluation du trafic dans son contexte, la restriction des accès non autorisés, l'analyse et la manipulation du contenu à travers des filtres applicatifs, ainsi que la sécurisation des serveurs exposés au réseau externe [14].

— **Anti-virus** : est un logiciel disposé sur la passerelle d'accès à Internet, qui consiste à détecter la présence d'infections lors de l'analyse complète des fichiers d'un serveur ou d'un poste de travail puis le supprimer complètement de la machine sur laquelle ils peuvent résider et être actifs [14].

— **Réseau Privé Virtuel (VPN : Virtual Private Network)** : c'est un environnement de communication, dans lequel l'accès est contrôlé, afin de permettre des connexions entre une communauté d'intérêt seulement. Ce réseau est dit virtuel car il relie deux réseaux locaux par une liaison privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent voir les données. Un réseau privé virtuel repose sur un protocole, appelé protocole de tunneling qui permet aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie entre l'entrée et la sortie du VPN, les données sont chiffrées et donc incompréhensibles pour toute personne située entre les deux extrémités du VPN [13].

— **Réseau local virtuel (VLAN : Virtual Local Area Network)** : ils suivent les mêmes concepts que le VPN, mais appliqués aux réseaux locaux. Un VLAN est un domaine de diffusion, qui se comporte comme un réseau local. La différence avec un vrai réseau local provient de l'emplacement géographique des clients, qui peut être quelconque. L'idée est de simuler un réseau local et donc de permettre à des clients parfois fortement éloignés géographiquement d'agir comme s'ils étaient sur le même réseau local [29].

Les VLAN ne peuvent être déployés qu'au sein d'un même réseau local. L'objectif des VLAN est d'améliorer la sécurité d'un réseau local en segmentant le trafic réseau, attribuant

à chaque équipe ou entité fonctionnelle un réseau privé virtuel dédié, afin de limiter la circulation non autorisée des données [25].

— **Proxy** : est placé entre la connexion Internet et le réseau interne de l'entreprise. Lorsqu'une page web est demandée, le proxy vérifie d'abord si cette page est déjà enregistrée sur son disque. Si c'est le cas, il récupère la page directement depuis son cache et l'envoie au navigateur de l'utilisateur. Si la page n'est pas enregistrée, le proxy effectue une requête vers le serveur web pour obtenir la page, puis il la stocke sur son disque avant de l'envoyer au navigateur. Cela permet d'améliorer les performances en réduisant le temps de chargement des pages fréquemment consultées et en réduisant la bande passante nécessaire pour accéder à Internet. De plus, le proxy peut également être configuré pour filtrer le contenu et renforcer la sécurité du réseau en bloquant l'accès à des sites web malveillants ou inappropriés [27]. Le proxy permet de surveiller le flux de paquets pour détecter toute tentative d'attaque. Il analyse les différents champs des paquets pour s'assurer qu'aucun d'entre eux ne contient des données malveillantes ou ne constitue une menace potentielle [29].

1.4 Conclusion

Dans ce chapitre, nous avons abordé les réseaux informatiques et les systèmes de sécurité de manière générale. Nous avons exploré les bases de la communication et de la connectivité dans les réseaux, ainsi que leur rôle crucial dans notre monde interconnecté. De plus, nous avons analysé l'impact de la sécurité sur les réseaux et souligné l'importance cruciale de sécuriser ces infrastructures pour assurer leur fiabilité et leur intégrité.

Chapitre 2

Présentation de l'organisme d'accueil

2.1 Introduction

L'entreprise SGSIA assure la gestion et la sécurité de l'aéroport d'Alger Houari Boumediene, l'un des principaux aéroports d'Algérie. L'objectif de ce chapitre est consacré pour la présentation de l'organisme d'accueil, plus exactement au Département Systèmes Informatique (DSI), au sein duquel nous avons effectué le stage pratique, qui nous a permet d'effectuer une analyse sur leur réseau, d'identifier les problèmes et de repérer les difficultés actuelles. et de suggérer des solutions appropriées. Afin de mettre en place une solution efficace et répondre à nos besoins.

2.2 Présentation de la SGSIA et son organigramme

L'aéroport d'Alger Houari Boumediene, est situé à environ 20 km d'Alger. Il s'agit du plus important de tous les aéroports Algériens. Sa capacité actuelle est d'environ 12 millions de passagers par an pour un flux réel de plus ou moins 4 millions. Il est composé d'une aérogare pour les vols intérieurs, et d'une nouvelle aérogare inaugurée le 5 juillet 2006 pour les vols internationaux. L'aéroport d'Alger a été classé meilleur aéroport Africain en 2011, c'est un aéroport civil international desservant la capitale Algérienne et sa région (Alger, Tipaza, Blida, Médea, Boumerdès et Tizi Ouzou). L'aéroport est géré depuis novembre 2006 par la société de gestion des services et infrastructures aéroportuaires (SGSIA), filiale de l'Établissement de Gestion de Services Aéroportuaires (EGSA) [1].

2.2.1 Historique et description de la SGSIA

La SGSIA, appelée plus communément *aéroport d'Alger*, et une entreprise publique économique (EPE) sous la forme d'une société par action, filial de l'entreprise de gestion des services aéroportuaire d'Alger (EGSA), et par conséquent a des capitaux publics.
Elle a été constituée le 1er novembre 2006 ayant pour objet de gérer et d'exploiter les infrastructures de l'aéroport d'Alger, avec un niveau de qualité et de performance élevé [3].

La SGSIA bénéficie d'un transfert de savoir-faire et de compétence d'aéroport de Paris au terme d'un contrat de gestion d'une durée de 4ans. Elle emploie 1200 salariés. Plus d'une année après l'ouverture de la nouvelle aérogare internationale d'Alger, la SGSIA poursuivent son effort de modernisation des structures d'accueils des passagers. D'après la revue Aéroports éditée par l'EGSA l'ex- aérogare international d'Alger est en plein rénovation pour abriter une nouvelle infrastructure dédiée aux lignes domestique dénommé terminal 2 [3].
L'objectif de cette réhabilitions vise l'optique d'une qualité de services rendus aux usagers, selon les normes internationales en vigueur. Par ailleurs le développement du tourisme passe inévitablement par le développement des infrastructures de transport, en premier lieu le transport aérien [3].
La société SGSIA gère actuellement 3 terminaux :

Terminal 1 : le terminal offre une surface d'exploitation de 82.000 m2, il est doté de deux halls symétriques. Le terminal est dédié aux vols domestiques et aux vols omra. Capacité d'accueil : 6 millions de passagers par an.

Terminal 2 : exploité sur une surface d'exploitation de 20.886,40 m2, le terminal 2 est dédié aux vols spéciaux (charters) et aux vols de pèlerinage. Capacité d'accueil :2,5 millions de passagers par an.

Terminal ouest : la nouvelle aérogare Ouest a été conçue afin de devenir le plus important point de connexion entre l'Afrique et l'Europe. La forme et l'aspect extérieur du nouveau terminal sont conçus pour lui donner un profil dynamique ainsi qu'une image à forte présence immédiatement reconnaissable. Il est construit selon des critères bioclimatiques afin de garantir l'efficacité énergétique. Il dispose d'une enveloppe lumineuse grâce aux murs vitrés tamisés par des plateaux en aluminium pour le contrôle solaire, ainsi, indispose d'un éclairage naturel grâce aux façades vitrées, aux lanterneaux de la toiture et aux écocells.
Le terminal offre une surface de plus de 192 000 m2 construit sur trois niveaux et deux mezzanines. Il est divisé en deux composants différents (le bâtiment principal et la jetée), dont la capacité d'accueil étant de 10 millions de passagers de classe "A" [3].

2.2.2 L'organisme de la SGSIA

L'organisation de la SGSIA est structurée en différents départements et services pour assurer la gestion efficace de ses activités. Voici un aperçu de l'organisation de la SGSIA [3] :

- Direction Générale : Responsable de la supervision générale de la société et de la prise de décisions stratégiques.
- Direction des Infrastructures et des Travaux (DIT) : responsable de l'élaboration du plan directeur de l'aéroport, des programmes d'aménagement, de la gestion du domaine, de l'inventaire immobilier et foncier, et de la coordination des travaux d'infrastructures et de superstructures.
- Département Études : Chargé de l'élaboration du plan directeur de l'aéroport en coordi-

nation avec les tiers concernés, et de la participation à l'élaboration des plans SMC et des manuels.

- Département Travaux et Équipements : Responsable de l'exécution du budget d'investissement de la SGSIA en termes d'acquisition d'équipements et de travaux neufs, de l'élaboration des fiches techniques, et de la coordination des travaux d'infrastructures et de superstructures.
- Service Contrat : Impliqué dans la gestion des contrats liés aux activités de la SGSIA.
- Département Systèmes Informatique : Responsable de la gestion des systèmes informatiques de la société.

Cette structure organisationnelle permet à la SGSIA de coordonner efficacement ses activités, de gérer ses ressources et ses infrastructures aéroportuaires, et de fournir des services de qualité aux passagers et aux compagnies aériennes, tout en assurant le développement et la valorisation de ses actifs. Le diagramme de la figure 2.1 illustre la structure organisasionelle de la SGSIA, mettant en evidence son hierarchie et ses differents departements.

2.2.3 Les missions de SGSIA

La SGSIA gère l'aéroport d'Alger Houari Boumediene en assurant plusieurs missions clés [3] :

- Acquisition, construction, aménagement, gestion, exploitation, maintenance et développement d'installations et infrastructures aéroportuaires. La SGSIA est responsable de la construction, de l'aménagement et de l'exploitation des installations et des infrastructures aéroportuaires, ainsi que de leur entretien et de leur développement.
- Fourniture de prestations de services dans le domaine aéroportuaire. La SGSIA offre des services aéroportuaires tels que la gestion des services et des infrastructures, la valorisation et l'exploitation des actifs, ainsi que des services de systèmes informatiques, sureté et sécurité, qualité et environnement, et communication.
- Valorisation et exploitation d'actifs. La SGSIA est chargée de valoriser et d'exploiter les actifs de l'aéroport, ce qui comprend la gestion des ressources humaines, financières et matérielles.
- Liaisons et accès. L'aéroport est connecté au réseau ferroviaire algérois, avec la ligne qui relie l'aéroport à la gare d'Agha au centre d'Alger (via Bab Ezzouar).
- De plus, l'extension de la ligne 1 du métro d'Alger, actuellement en construction, reliera l'aéroport à Alger Centre à l'horizon 2026.
- En outre, les lignes de bus ETUSA 39, 100 et 178 relient le centre-ville d'Alger à l'aéroport, et la Rocade Sud relie l'aéroport à Zéralda via le sud d'Alger, tandis que la Rocade Nord via Bab Ezzouar relie l'est à Alger.

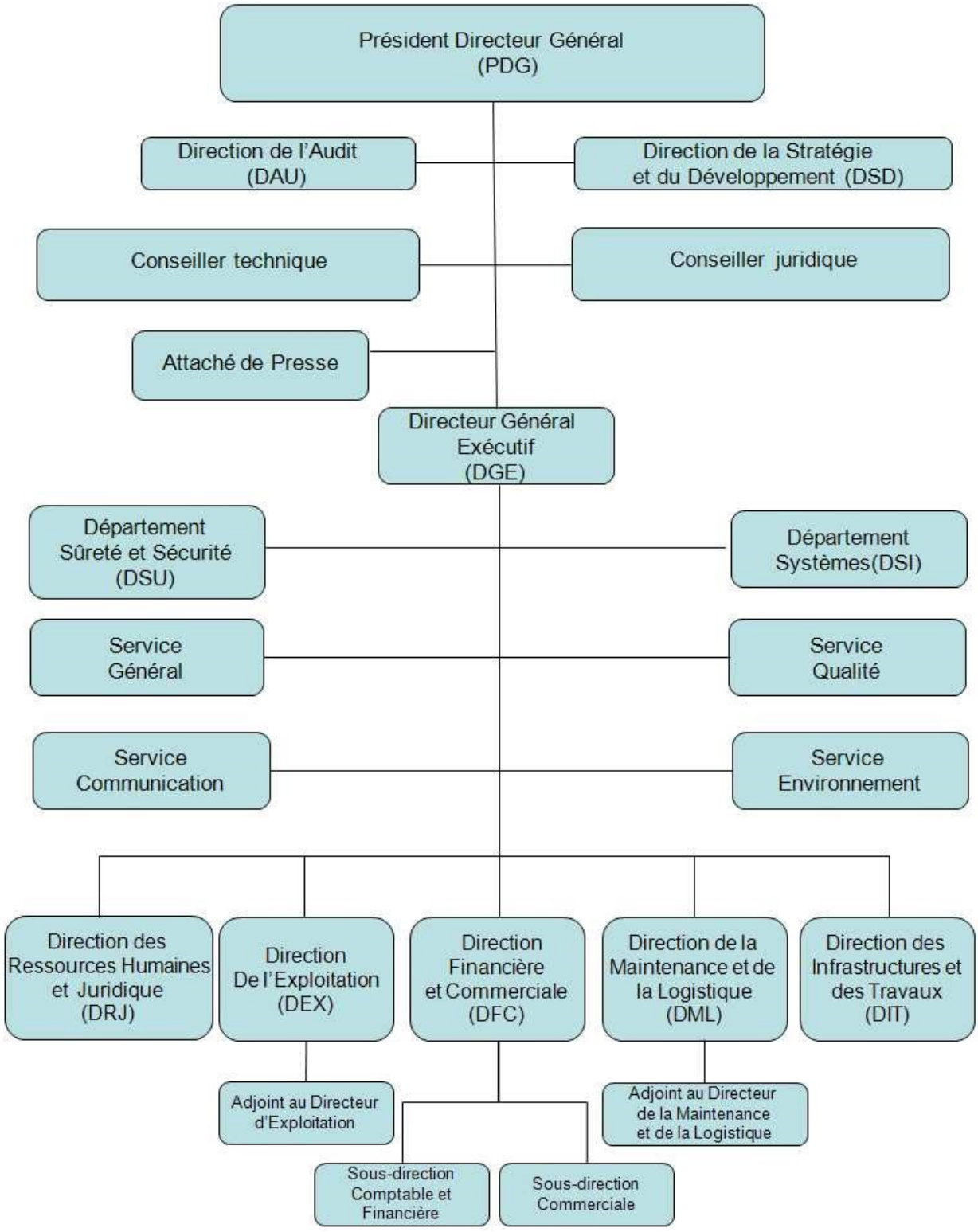

FIGURE 2.1 – L'organigramme de la SGSIA [2]

2.3 Département Systèmes Informatique (DSI)

La SGSIA est composé de plusieurs département, dont figure le département système informatique (DSI) où nous avons effectué notre stage. Ce département recouvre trois domaines d'applica-

tions à savoir, l'informatique aéroportuaire, l'informatique de gestion, l'informatique industrielle. Il est composé d'un service d'étude qui est chargé de développer et/ou adapter de nouveaux systèmes ou de nouvelles applications. Des administrateurs réseaux sont chargés de superviser l'utilisation des différents systèmes, de garantir leur cohérence, d'assurer leur maintenance, et d'apporter une assistance aux utilisateurs. Les administrateurs réseaux sont secondés par des coordinateurs réseaux et ils disposent de techniciens d'assistance et de maintenance. Ce département a pour missions :

— De développer et/ou d'adapter des systèmes et des programmes informatiques nécessaires à la gestion et à l'exploitation de l'aéroport.

— De maintenir en état les différents systèmes et outils informatiques de l'aéroport.

La figure 2.2 démontre la répartition et l'hiérarchie au sein du département.

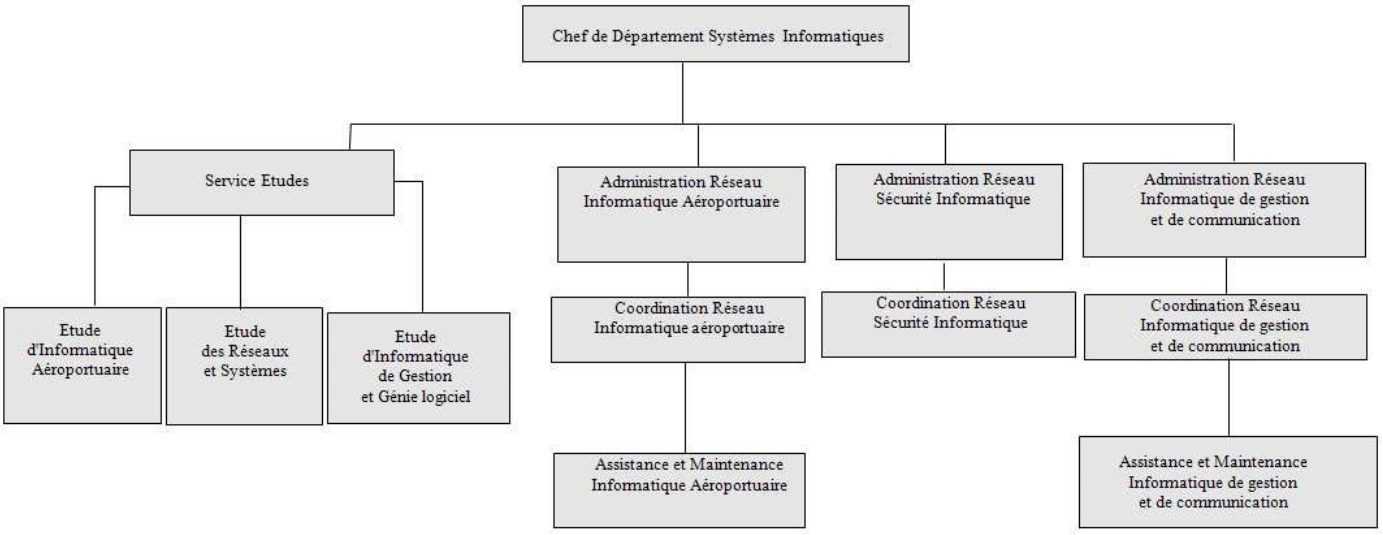

FIGURE 2.2 – L'organigramme de DSI [2]

2.4 L'analyse du réseau SGSIA et les solutions proposées

Il est essentiel de garantir la sécurité informatique afin de préserver la confidentialité des données sensibles, comme les informations personnelles, les secrets industriels et les informations financières, et de prévenir toute utilisation malveillante des systèmes informatiques. Cela s'applique notamment à l'entreprise SGSIA, qui accorde une grande importance à la sécurité informatique. Plusieurs mécanismes et stratégies de sécurité sont mis en place par cette entreprise, en appliquant soigneusement des équipements, des logiciels et surtout un savoir-faire précis.

En premier lieu on a effectué une analyse approfondie du réseau de l'aéroport, plusieurs informations ont été découvertes,ce qui nous a également permis de déterminer un nombre considérable de faiblesses potentielles.

Cette approche nous a démontré que SGSIA est vulnérable à des attaques malveillantes, des fuites

de données, des perturbations de performance et des problèmes de conformité réglementaire. Cela est dû à une surveillance insuffisante du trafic entrant et sortant, ce qui constitue un risque important pour la sécurité et la conformité d'un réseau informatique. Grâce aux suggestions des membres du personnel qui nous ont accompagnés pendant le stage, nous avons réussi à trouver une solution qui implique la mise en place d'un pare-feu *Pfsense* pour protéger le réseau et surveiller le trafic entrant et sortant.
En plus de ça il existe un risque d'accès non autorisés aux systèmes et aux informations sensibles, ce qui peut mettre en péril la sécurité et la protection des données. Il est donc primordial de mettre en place un système robuste de contrôle d'accès qui inclut l'authentification pour renforcer la sécurité des comptes utilisateurs, et de limiter l'accès à Internet. Afin de relever ce défi, nous avons choisi d'utiliser l'un des services de notre pare-feu, le portail captif, comme solution idéale.
On aperçoit également que l'utilisateur est expose à des publicités intrusives, à des logiciels malveillants et à l'accès à des sites web inappropriés ou dangereux. Cela peut être évité par l'utilisation d'un filtrage Web spécialisés tels qu'AdGuard pour filtré la navigation sur Internet afin de bloquer les publicités indésirables, des pages web et empêcher les logiciels malveillants d'atteindre les utilisateurs.
Afin de garantir le bon déroulement de l'entreprise, il est essentiel de fournir aux employés la possibilité de se connecter à distance de manière sécurisée aux réseaux de l'entreprise. Cette exigence résulte de l'évolution vers un environnement de travail flexible où les employés peuvent travailler à partir de différents endroits, tout en nécessitant un accès sécurisé aux ressources et aux données de l'entreprise. Pour résoudre ce problème, il est nécessaire de mettre en œuvre un système de connexion sécurisée à distance pour les employés, en exploitant des technologies comme les VPN. OpenVPN est un service de *Pfsense* qui permet un accès à distance à l'infrastructure de l'entreprise en toute sécurité.

En adoptant ces mesures, la SGSIA peut renforcer la sécurité de son réseau, garantir la confidentialité de ses données sensibles et garantir une expérience en ligne sécurisée et fiable pour leurs employés.

2.5 Conclusion

En conclusion, ce chapitre a permis de mieux comprendre le rôle et l'organisation de la SGSIA où nous avons réalisé notre stage pratique, ainsi nous avons mis en évidence une analyse du réseau qui nous a permis de repérer ses principaux problèmes, cela nous a amené à suggérer un ensemble de solutions afin de relever ce défi et d'améliorer le réseau SGSIA.

Chapitre 3

Mise en œuvre

3.1 Introduction

Après avoir analysé le réseau SGSIA, une partie de celui-ci nous a été mise à disposition pour accéder à Internet, cette section étant considérée comme un réseau externe par rapport à notre réseau local. De plus, nous avons obtenu les équipements nécessaires pour réaliser et mettre en place notre solution à la problématique soulignée dans le deuxième chapitre.
Ce chapitre sera dédié à présenter les différentes parties de notre réalisation pratique, l'environnement de travail, ainsi que l'installation et les diverses configurations effectuées durant notre stage chez SGSIA.

3.2 Présentation des outils utilisés

Pour la réalisation de notre solution, nous avons mis en place une infrastructure qui comporte plusieurs composants essentiels. Parmi ces composants nous avons trois machines clientes, chacune équipée de systèmes d'exploitation différents, Windows 10, Windows 11, et un Windows serveur installé sur un serveur *HP ProLiant DL380 Gen7*. En plus des machines clientes, nous utilisons un serveur *HP ProLiant DL380 Gen7*, il est dédié à la configuration et à la gestion du pare-feu *Pfsense*, qui joue un rôle crucial dans la sécurité et le contrôle du trafic réseau. Pour l'administration à distance de notre pare-feu, nous employons le logiciel Putty. Ce logiciel, installé sur l'une de nos machines clientes, permet d'accéder et de gérer les serveurs, routeurs, et switches de manière sécurisée via SSH et autres protocoles de réseau.
Pour assurer l'interconnexion de tous nos équipements dans le réseau local, nous utilisons un switch hub de la marque *Link*. Ce switch est essentiel pour la communication fluide entre les différents dispositifs du réseau, permettant une transmission rapide et efficace des données entre les machines clientes et le pare-feu, pour connecter physiquement chaque équipement avec le hub, nous utilisons des câbles *RJ45*. Ces câbles garantissent des connexions stables et fiables au sein de notre réseau local.

3.3 L'architecture déployée pour notre solution

En utilisant les équipements préalablement présentés, nous avons mis en œuvre notre solution. Pour mieux appréhender l'organisation de notre infrastructure, nous exposons à présent la topologie complète de notre réseau. Cette section vise à détailler l'agencement de notre infrastructure en mettant en lumière la connectivité des éléments, comme illustré dans la figure 3.1. Les lignes continues représentent les connexions physiques entre les équipements et les câbles, tandis que les lignes discontinues décrivent la topologie logique, spécifiant comment les données sont acheminées entre les différents dispositifs du réseau. Les connexions VPN sont signalées par des lignes bleues pour souligner leur rôle crucial dans notre architecture sécurisée, tandis que les lignes jaunes est une connexion sans VPN, montrent les accès directs et le portail captif pour les utilisateurs locaux. Cette configuration nous permet de gérer efficacement la sécurité, les accès et les ressources réseau pour notre projet. Voici une explication détaillée des composants illustré dans la figure 3.1 et de leurs interconnexions :

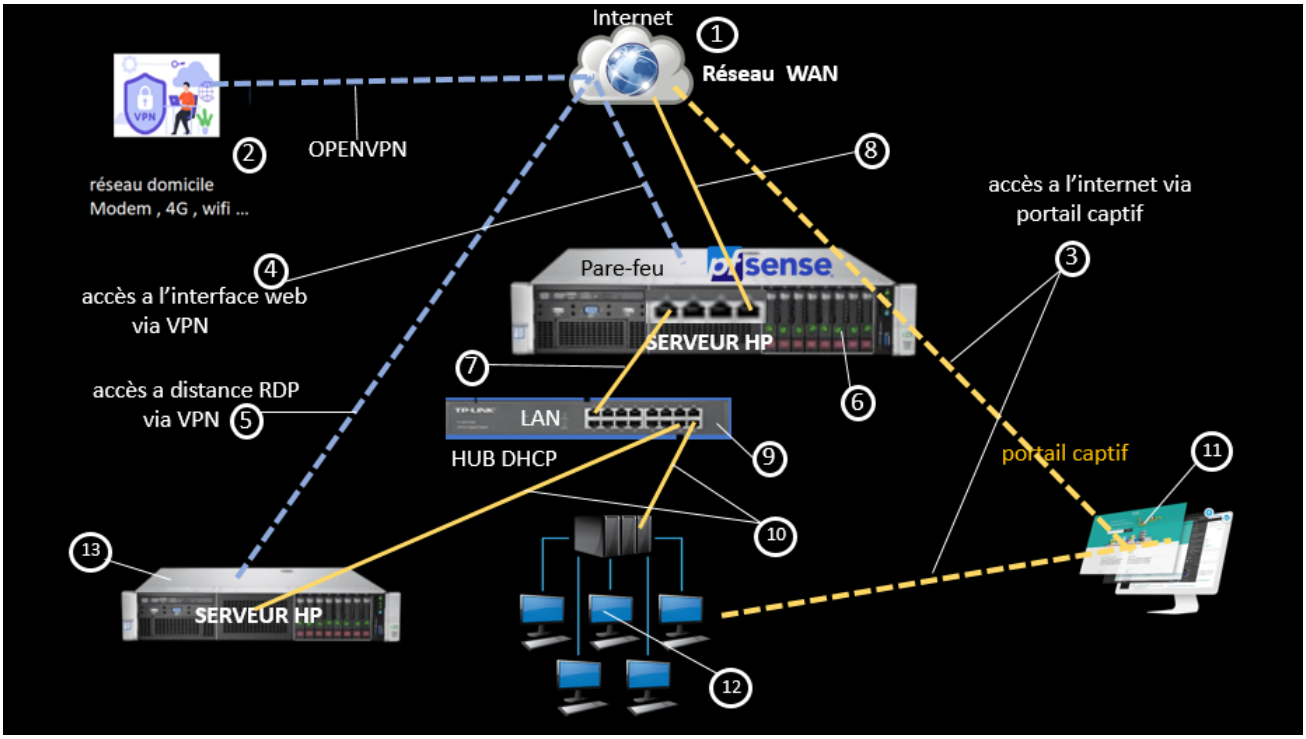

FIGURE 3.1 – Architecture déployée pour notre solution

1 Réseau WAN : connexion Internet via le pare-feu SGSIA, avec une liaison câble RJ45 (ligne jaune continue).

2 Accès VPN externe via client OpenVPN : permet aux utilisateurs de se connecter à distance de manière sécurisée (Ligne bleue discontinue).

3 Lien logique pour accéder à Internet via le portail captif : utilisé pour gérer l'accès des utilisateurs locaux à Internet via une authentification (Ligne jaune discontinue).
4 Lien logique pour accéder à l'interface web via VPN : permet une gestion sécurisée de l'interface web depuis une connexion externe (Ligne bleue discontinue).
5 Lien logique pour accéder à distance RDP via VPN : permet aux utilisateurs de se connecter à distance aux machines via Remote Desktop Protocol (RDP) en utilisant une connexion VPN (Ligne bleue discontinue).
6 Pare-feu *Pfsense* : installé sur un serveur HP, il gère la sécurité du réseau, filtre le trafic, et assure la gestion des connexions VPN.
7 Lien physique LAN entre HUB et *Pfsense* : permet la communication interne et la distribution des adresses IP via DHCP, une liaison câble RJ45 (Ligne jaune continue).
8 Lien physique WAN entre le pare-feu SGSIA et notre pare-feu *Pfsense* : gère le trafic entrant et sortant d'Internet avec le pare-feu *Pfsense* avec une liaison câble RJ45 (Ligne jaune continue).
9 Switch hub : utilisé pour diffuser les adresses IP à travers le réseau local via DHCP.
10 Lien physique entre le HUB et le réseau LAN : connecte les différents équipements sur le réseau local avec un câble RJ45 et assure la distribution des adresses IP via DHCP (Ligne jaune continue).
11 Service Portail Captif : gère l'accès à Internet pour les utilisateurs locaux via une authentification.
12 Réseau LAN : comprend toutes les machines clientes (Windows 10, Windows 11 et un serveur Windows), interconnectées et gérées via le switch hub et des adresses IP via DHCP.
13 Serveur HP : utilisé pour effectuer des tests de configuration et de sécurité pour les connexions VPN et le portail captif.

3.4 Mise en place de *Pfsense*

Le logiciel *Pfsense* est une distribution personnalisée gratuite et open source, spécialement conçue pour être utilisée comme pare-feu et routeur entièrement gérée via une interface Web, un point d'accès sans fil ou une passerelle VPN. Il date de 2004 et hébergé et développé par Rubicon Communications (Netgate). Il est réputé pour sa fiabilité. Après une installation en mode console, il s'administre ensuite simplement depuis une interface web. *Pfsense* offre une plateforme stable, sécurisée et hautement personnalisable pour répondre aux besoins spécifiques des utilisateurs. Il est largement utilisé dans les environnements professionnels et domestiques en raison de sa fiabilité, de sa souplesse et de sa robustesse. En plus de ses capacités de pare-feu avancées, il fournit des fonctionnalités telles que le filtrage de contenu d'URL et le blocage de domaines [23].

3.4.1 Installation de distribution *Pfsense*

Pour faire fonctionner *Pfsense* nous avons besoin de télécharge une image iso de 64 bits (PfSense-CE-2.7.2-RELEASE-amd64.iso) et l'installer sur une machine physique Serveur HP Pro-Lint dl380 gen7.
Lors du démarrage de serveur avec l'image ISO monté, un menu de boot apparaît. On peut choisir de démarrer *Pfsense* avec certaines options activées. Si aucune touche n'est appuyée, *Pfsense* bootera avec les options par défauts (choix 1) au bout de 8 secondes, de la manière présenté dans la figure 3.2

FIGURE 3.2 – Boot *Pfsense*

- On appui sur "Entrée" pour lancer l'installation avec les options par défaut.

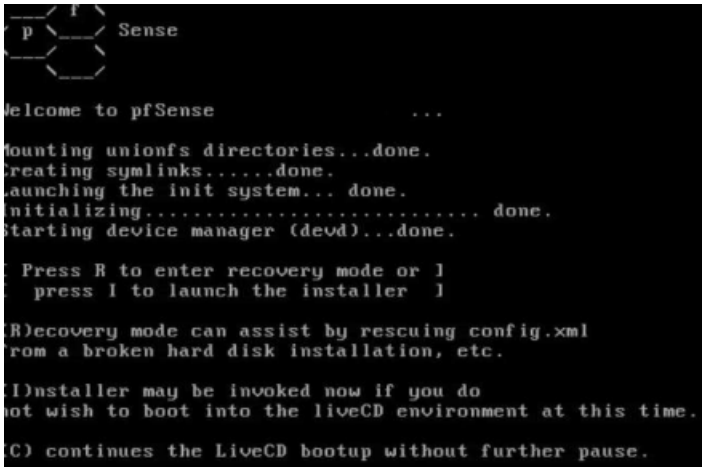

FIGURE 3.3 – Les options par défaut de *Pfsense*

- On appui sur la touche "I" afin de démarrer l'installation et on choisit " Install" pour procéder à l'installation comme l'indique la figure 3.4).

FIGURE 3.4 – Démarrage d'installations *Pfsense*

- L'installation débute et copie les fichiers nécessaires sur le disque dur, nous devons par la suite choisir quel type d'installation voulons. On Clique sur "OK " pour sélectionner le type d'installation (figure 3.5).

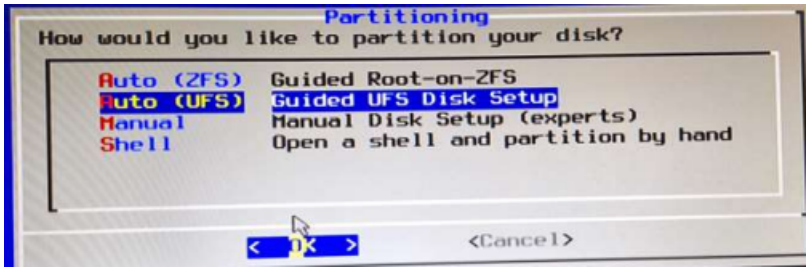

FIGURE 3.5 – Le type d'installation *Pfsense*

- On choisi le disque pour l'installation et en cliquant sur "Ok" (figure 3.6).

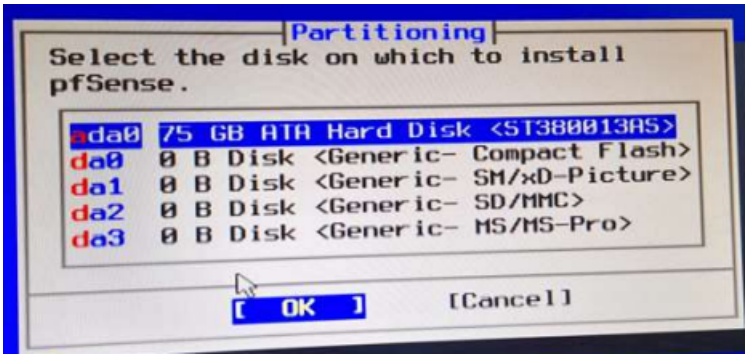

FIGURE 3.6 – La sélection du disque sur le serveur

- On Clique sur "Entire Disk" pour entrer dans le disque (figure 3.7).
- On confirmer notre choix en cliquant sur "Yes" (figure 3.8).

- On sélection la partition puis on clique sur "ok" (figure 3.9).
- On clique sur "Finish" pour terminer la sélection de la partition (figure 3.10).

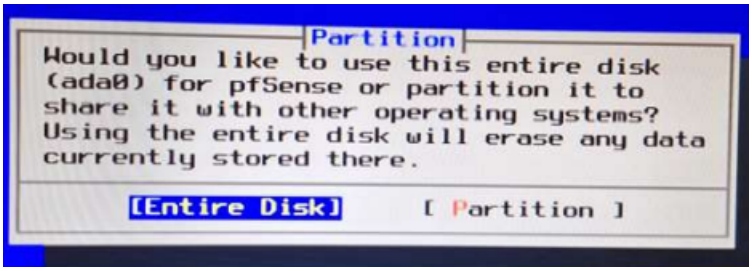

FIGURE 3.7 – Sélection de l'entire Disque de serveur

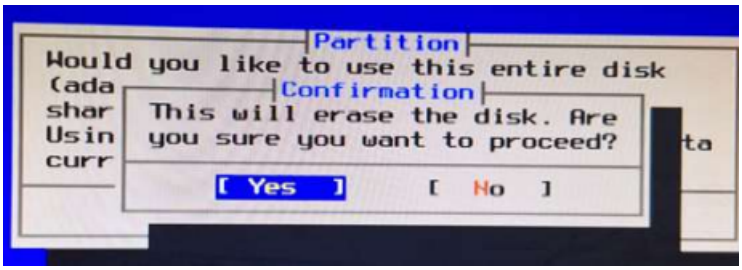

FIGURE 3.8 – Confirmation de la sélection de disque

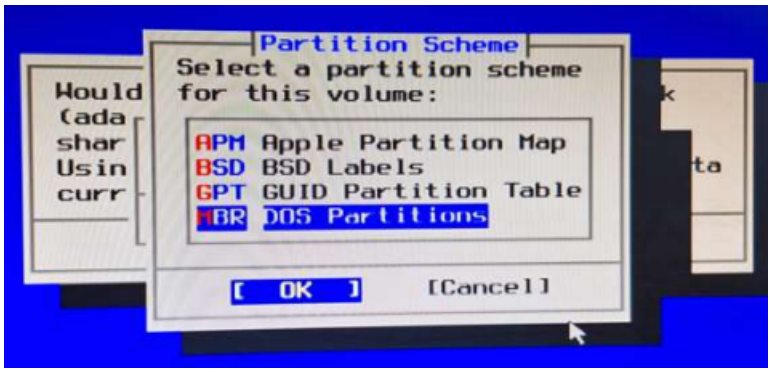

FIGURE 3.9 – Sélection de partition

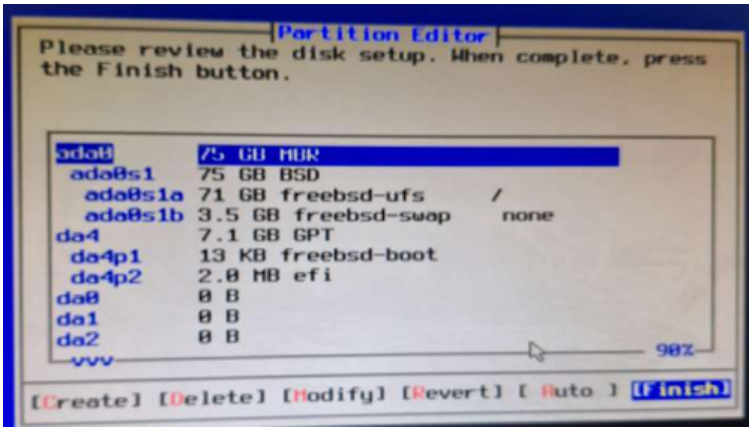

FIGURE 3.10 – Finition la sélection de Partition

- On Sélectionne "Commit" et on Clique sur "Finish" pour confirmer la partition. (figure 3.11).

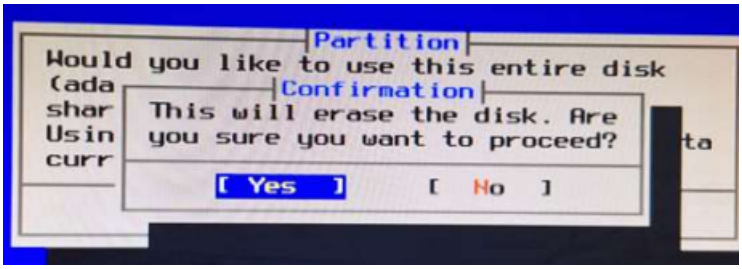

FIGURE 3.11 – Confirmation de partition

- L'installation est effectuée (figure 3.12).

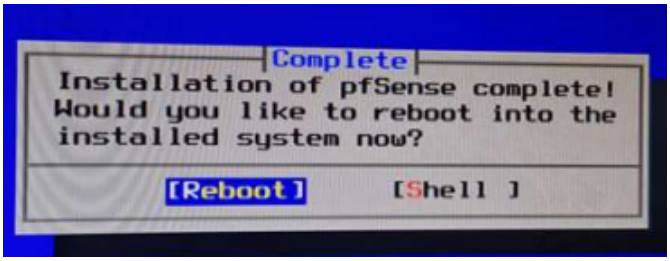

FIGURE 3.12 – Fin d'installation *pfsense*

- Une fois l'installation finie, on choisit "Reboot" et nous redémarrons sur notre nouvelle installation, comme sur la figure 3.13.

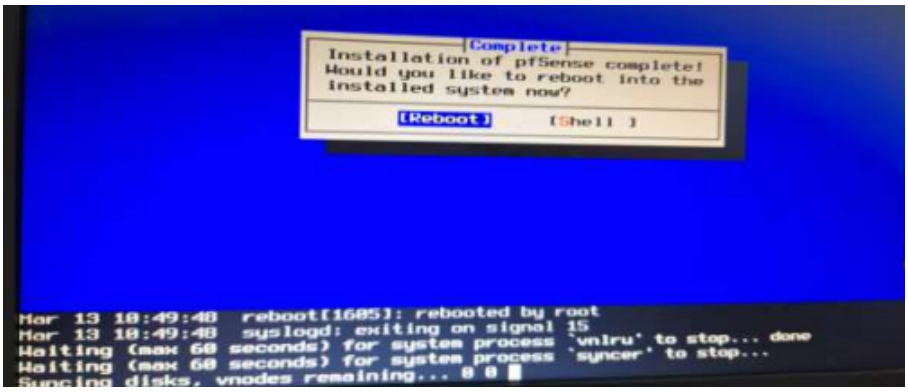

FIGURE 3.13 – Redémarrage du *Pfsense*

3.4.2 Configuration de *Pfsense*

Lors du premier démarrage de *Pfsense* il faut configurer les différents interfaces (WAN et LAN). Il nécessite deux cartes réseaux minimum, une pour le WAN et une pour le LAN.

- Pour procéder à la configuration de base de *Pfsense*, nous appuyons donc sur la touche "N", comme c'est illustrée sur la figure3.14.

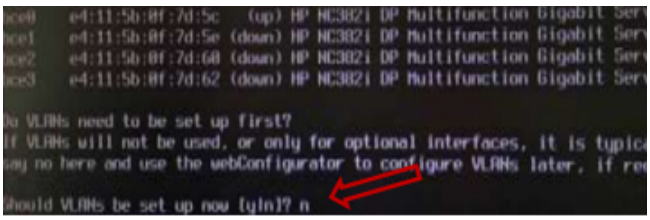

FIGURE 3.14 – Configuration de base de *Pfsense*

- Nous devons ensuite déterminer quelle interface est sur le côté WAN, pour cela on peut saisir manuellement le nom de l'interface "bce0" (figure 3.15).

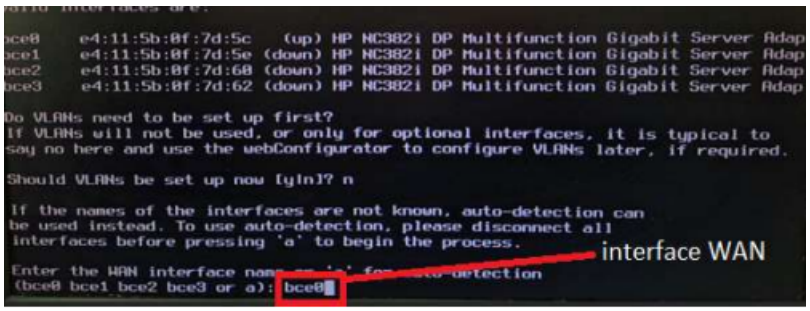

FIGURE 3.15 – Configuration de réseau WAN

- Nous devons déterminer aussi quelle interface est sur le côté LAN, on saisir le nom de l'interface "bce1" figure 3.16.

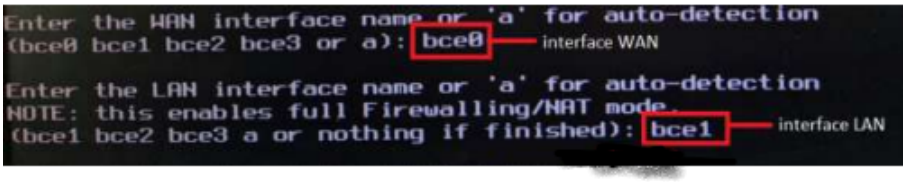

FIGURE 3.16 – Configuration de l'interface LAN

- On valide avec "Y" notre configuration des deux interfaces (fiqure 3.17).

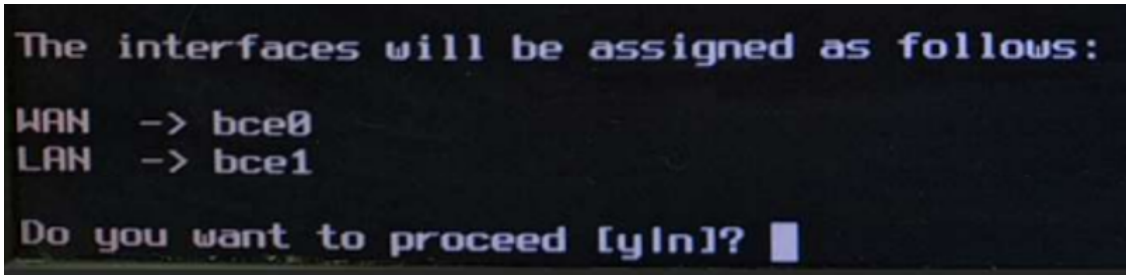

FIGURE 3.17 – Validation des interfaces WAN et LAN

- A la fin de la configuration sa nous affiche la figure 3.18.

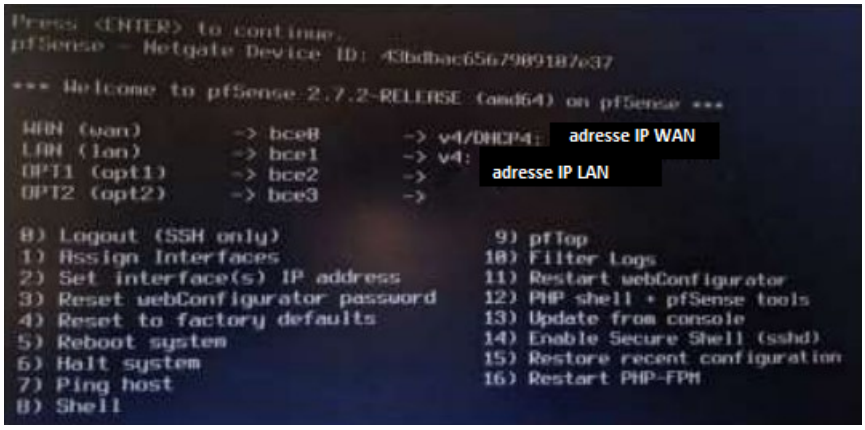

FIGURE 3.18 – Fin de configuration *Pfsense*

- Une fois la configuration terminée, dans un navigateur on accède avec notre adresse IP du LAN à l'interface web de *Pfsense*. Une fois que cette interface s'afficher on se connecte avec un utilisateur "admin" défini par défaut et avec son mot de passe "*Pfsense*" (figure 3.19).

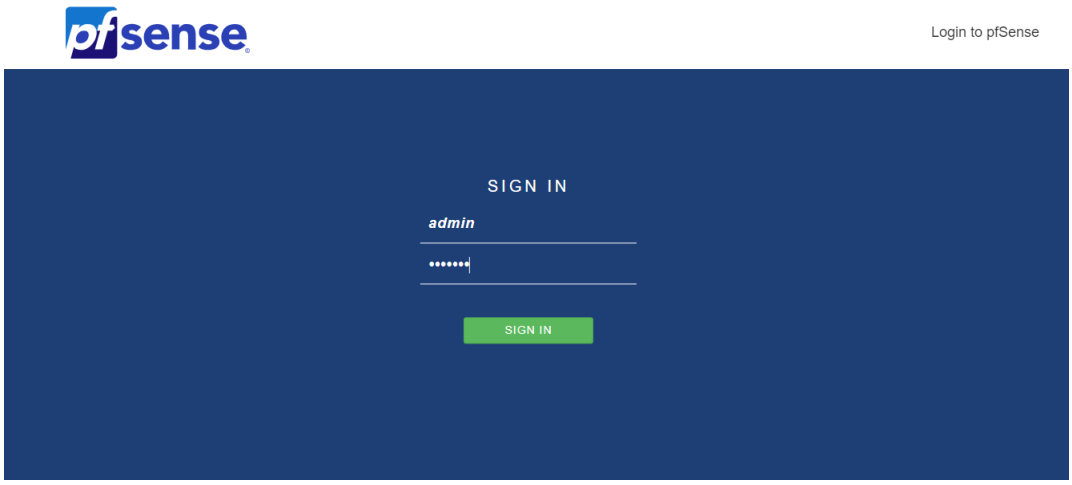

FIGURE 3.19 – Page d'identification de *Pfsense*

- Après s'être connecté, le tableau de bord de *Pfsense* s'affichera pour le premier accès, l'assistant de configuration *Pfsense* s'affiche, on clique sur next dans les deux fenêtres qui se suit (figure 3.20).
- Ensuite on donne le nom d'hôte et on fait la configuration DNS (primary DNS et secondary DNS), on coche "Override DNS" et on poursui avec "next" (figure 3.21).
- Comme l'illustre la figure 3.22, après la configuration et l'installation de *Pfsense*, nous aurons deux interfaces : l'une pour le réseau WAN qui a accès à Internet et l'autre pour le réseau LAN.
- On peut modifier la configuration et changer le thème de l'interface de *Pfsense*, dans le menu System>General Setup.

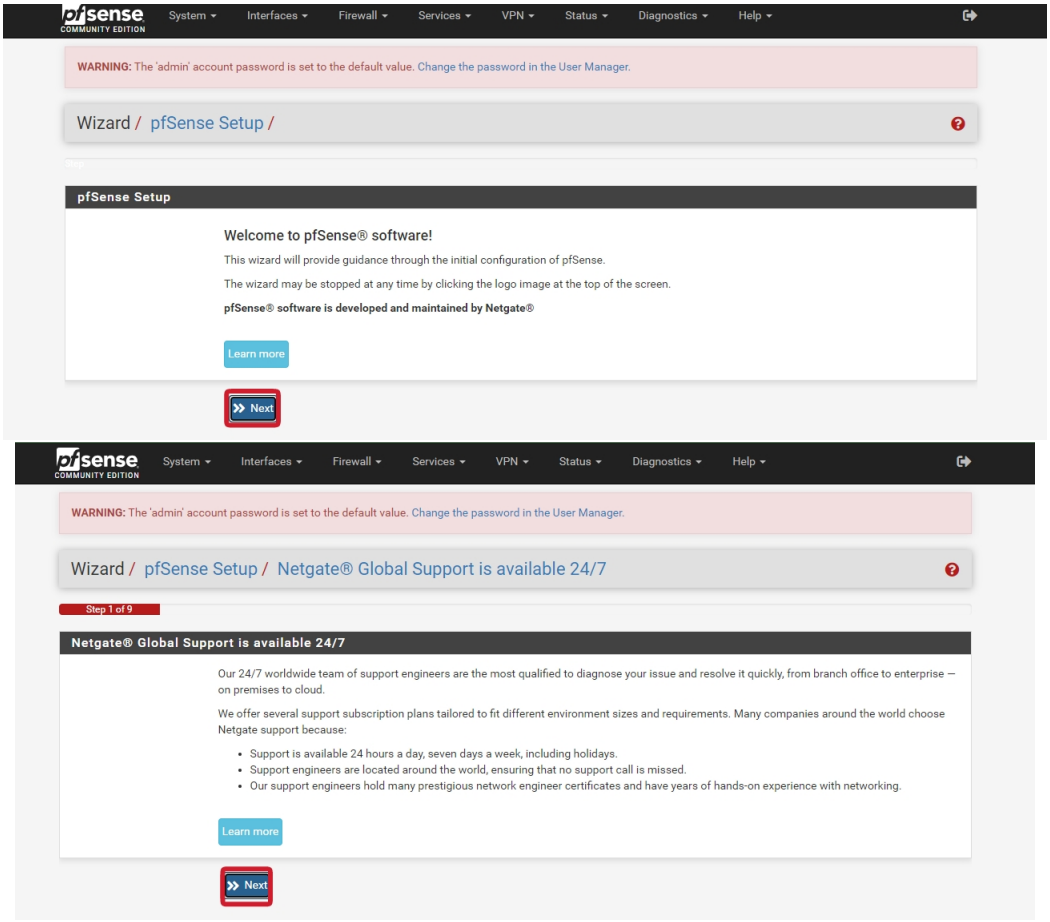

FIGURE 3.20 – Premier Accès où *Pfsense*

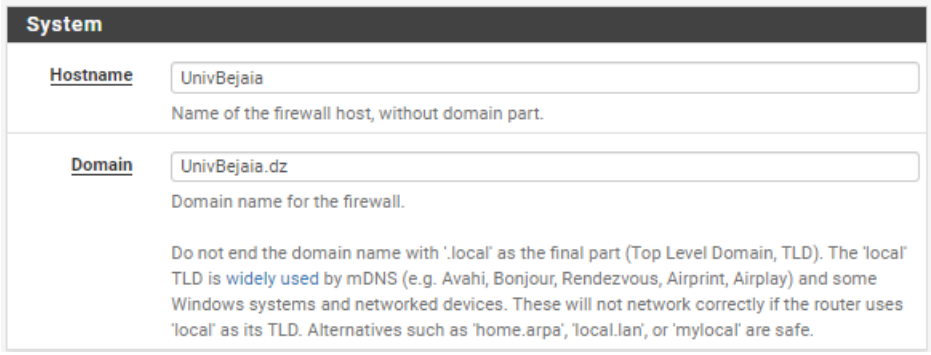

FIGURE 3.21 – Saisir le nom d'hôte

- Maintenant on va créer des règles pour autoriser l'accès Internet sur réseau LAN. On clique sur "firewall" après sur "rules".
- On sélectionne l'interface LAN et on clique sur "Add". Après cela l'accès Internet est autorisé dans le réseau LAN.

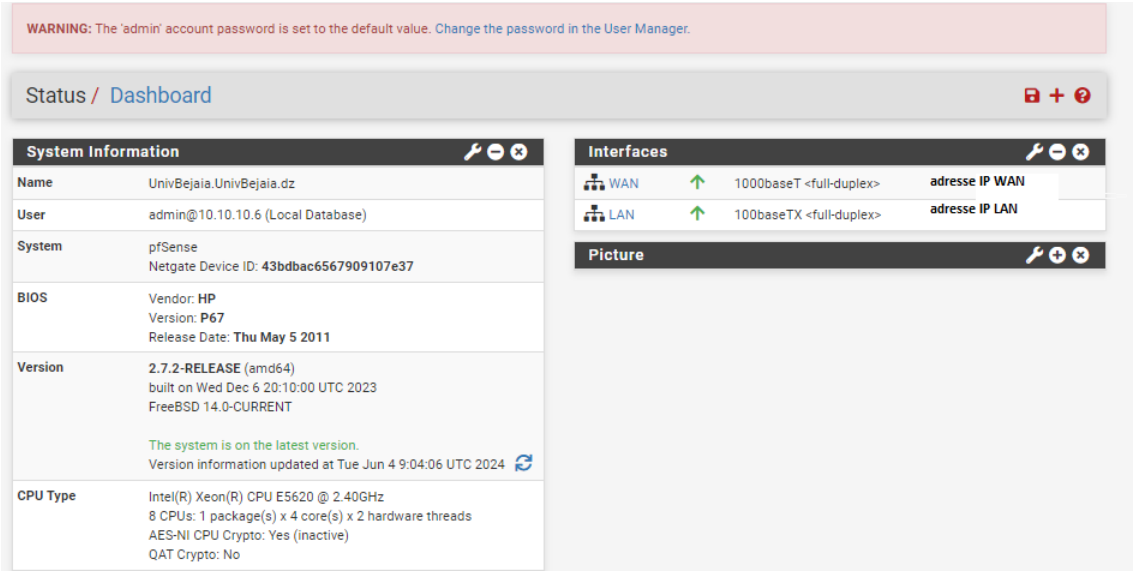

FIGURE 3.22 – Tableau de bord de *Pfsense*

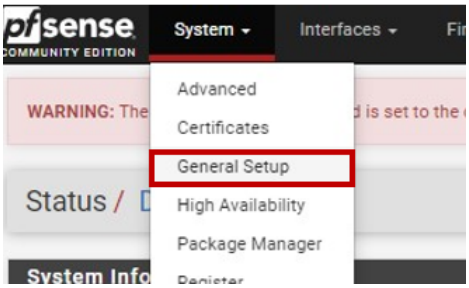

FIGURE 3.23 – Menu de configuration *Pfsense*

3.5 Mise en place d'un portail captif

Les portails captifs (Captive Portal) demandent généralement une authentification afin d'accéder à Internet, ils sont utilisés dans des environnements de diffusion d'un réseau publique. Les clients sont alors obligés de demander les identifiants au propriétaire de la connexion. Le portail captif offre donc un contrôle de l'accès à l'Internet.

3.5.1 Création des utilisateurs et des groupes

Les utilisateurs et les groupes jouent un rôle crucial dans la gestion des accès au réseau. Chaque utilisateur qui souhaite accéder au réseau externe doit être authentifié. Cela signifie qu'ils doivent fournir des identifiants valides, tels qu'un nom d'utilisateur et un mot de passe.
En revanche les groupes facilitent la gestion des autorisations d'accès. En regroupant les utilisateurs selon leurs besoins, nous pouvons appliquer des règles d'accès uniformes à chaque groupe. Cette approche simplifie la gestion des autorisations en évitant d'avoir à définir des règles pour chaque

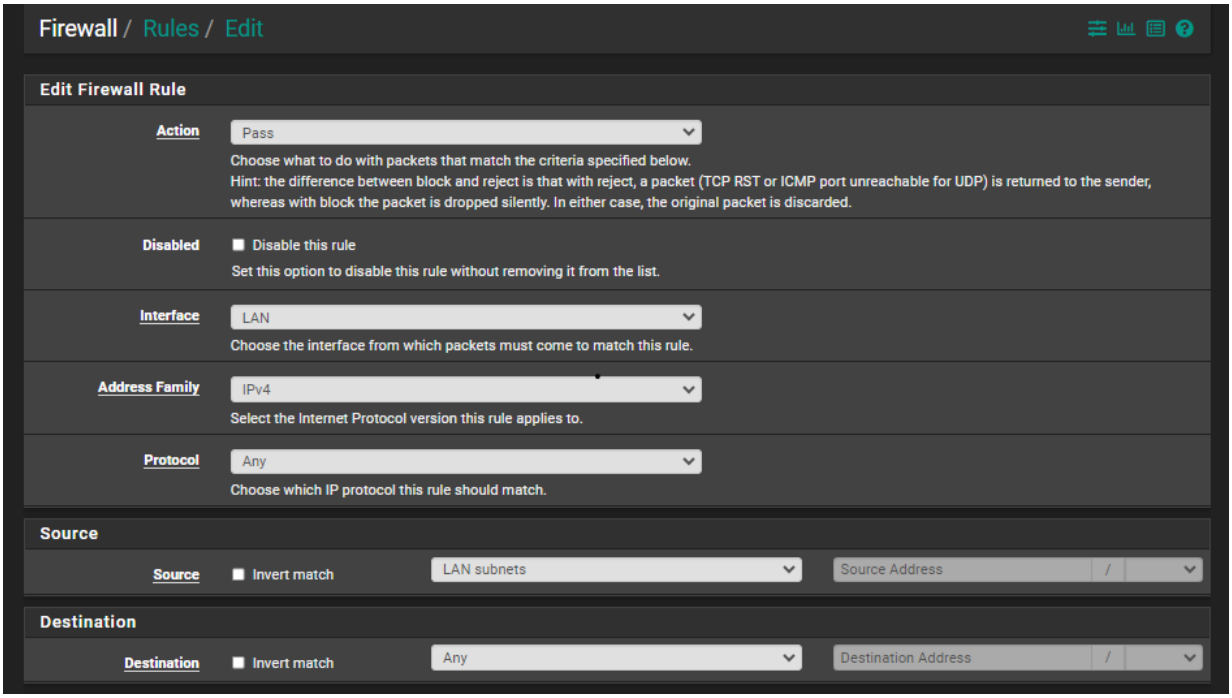

FIGURE 3.24 – L'ajout d'une règles LAN

utilisateur individuellement.
pour cela, nous suivant ces étapes :

- Dans notre interface Web de pare-feu *Pfsense*, on accède au menu system>User Manager.
- Sur l'onglet *User* on clique sur "Add" comme sur la figure 3.25 pour créer un nouveau compte.

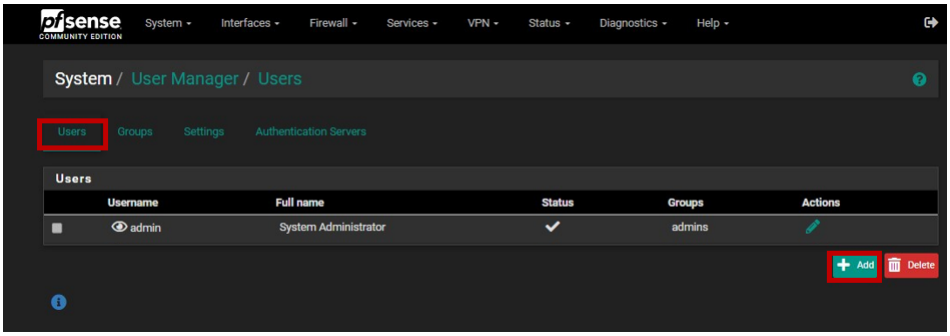

FIGURE 3.25 – L'ajout d'un utilisateur portail captif

- Sur l'écran de création des utilisateurs, on a effectué la configuration comme c'est illustré dans la figure 3.26. On clique sur "save" pour enregistrer.
- On passe à la création de groupe, toujours dans menu system> User Manager, sur l'onglet *groups* on clique sur "Add" pour créer un groupe (figure 3.27).
- Sur l'écran de création de groupe, on saisit le nom de groupe dans l'onglet *Group name*, sur l'onglet *Group membership* on sélection les utilisateurs qu'on veut ajouter à ce groupe et

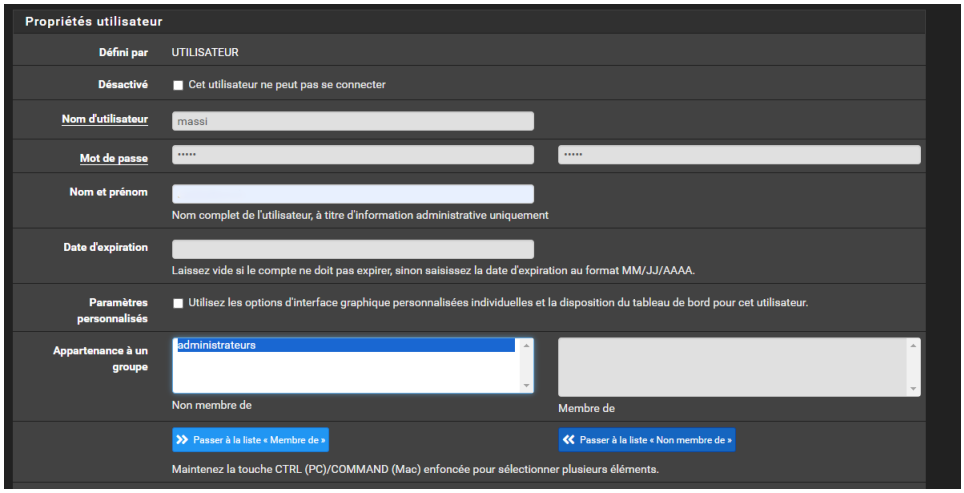

FIGURE 3.26 – Création du utilisateur

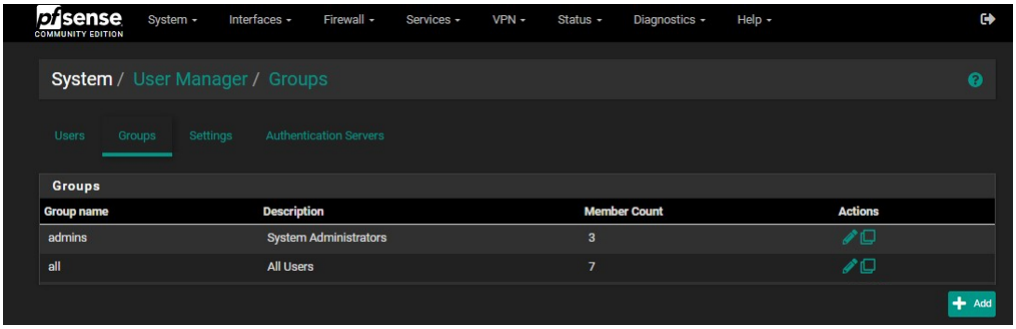

FIGURE 3.27 – L'ajout du groupe

on clique sur "Move to members" pour les ajouter, on clique sur save pour valider (figure 3.28).

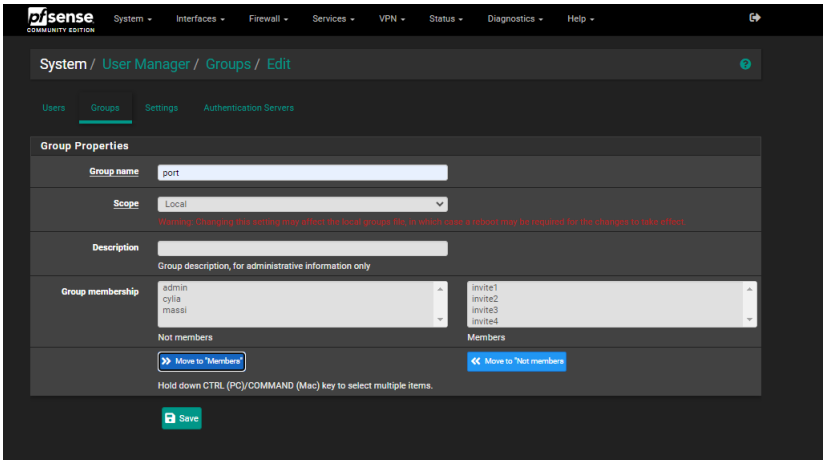

FIGURE 3.28 – Création du groupe

- Maintenant, nous devons modifier les autorisations du nouveau groupe.

- Sur les propriétés de groupe, on localise la zone *Assigned Privileges* et clique sur le bouton "Add".
- On sélectionne les autorités suivantes (figure 3.29) :

1. User-Services : Captive Portal long
2. WebCfg-Services : Captive Portal
3. WebCfg-status : Captive Portal

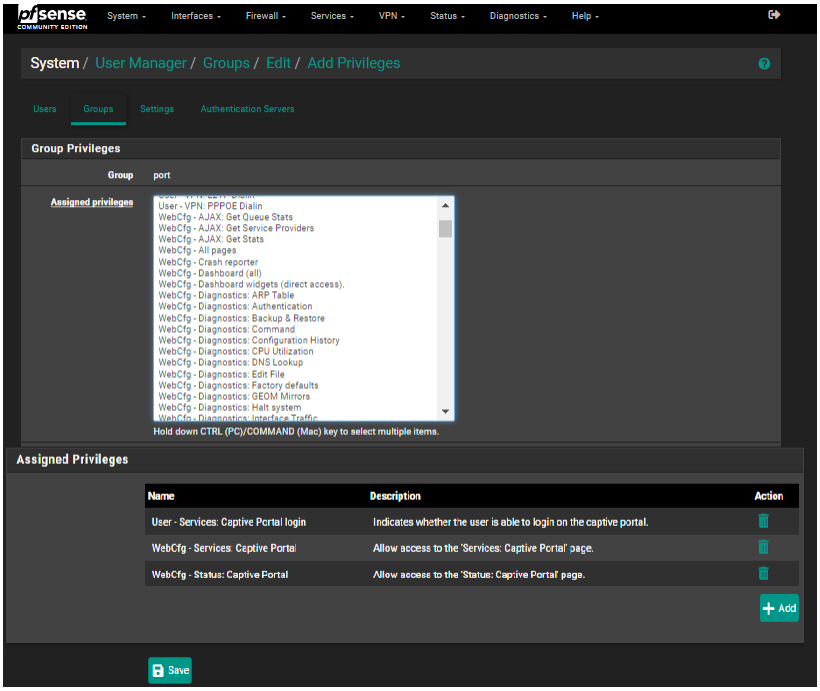

FIGURE 3.29 – Autorisation du groupe

La figure 3.30 représente une liste des utilisateurs crées et leur groupe. On distingue plusieurs utilisateurs regroupé dans des groupes différents. Le groupe *admins* contient les administrateurs, ce groupe est essentiel pour la gestion du pare-feu et des autres fonctionnalités du système. Les membres de ce groupe possèdent des privilèges administratifs étendus, leur permettant d'accéder à toutes les configurations, de gérer les utilisateurs et les groupes et de configurer les interfaces réseau.

Le groupe *port* contient des individus qui se connectent au réseau via le portail captif et doivent s'authentifier avant d'accéder à Internet.

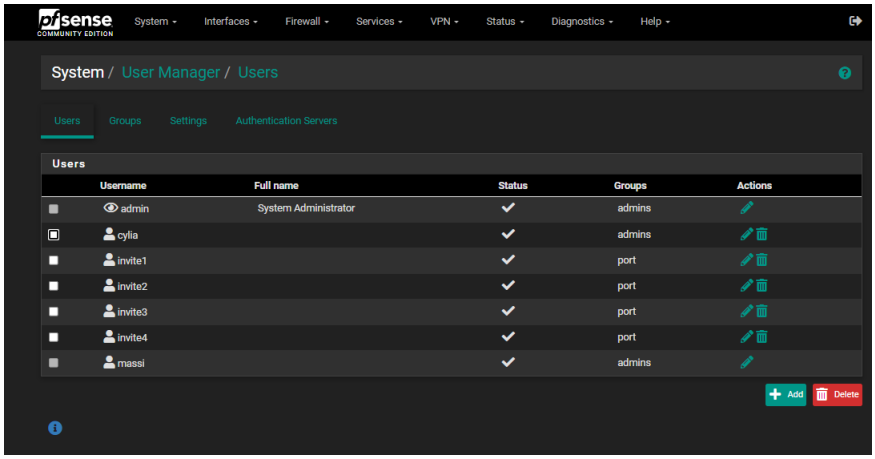

FIGURE 3.30 – Les utilisateurs créés

3.5.2 Configuration du portail captif

Après avoir créé des utilisateurs et des groupes, l'étape suivante consiste à configurer le portail captif. Cette configuration permet d'assurer que seuls les utilisateurs autorisés peuvent se connecter en les redirigeant vers une page de connexion où ils doivent s'authentifier. Le portail captif offre des options pour personnaliser les règles d'accès, définir des délais de session et même personnaliser l'apparence des pages de connexion.

Voici comment procéder pour configurer le portail captif :

- Sur le menu services> Captive portal. On clique sur "Add".
- Sur l'écran du portail captif, on a effectué la configuration suivant : on coche l'activation de *partial captif*, on choisit l'interface où le portail captif doit être activé dans notre cas le réseau LAN, et on ajoute l'URL désirée pour rediriger l'utilisateur après une authentification.
- Sur la zone d'authentification, nous choisissons base de données local sur l'onglet *Serveur d'authentification* et on coche sur *privilèges d'authentification locale* comme indiqué dans la figure 3.32. On sauvegarde pour terminer la configuration *Pfsense Captive Portal*.
- Si on essaie d'accéder à Internet, une fenêtre s'affiche, comme dans la figure 3.33. On s'identifie pour avoir accès à l'interface Google.
- On peut aussi modifier cette interface, sur menu Diagnostics>Edit File, on choisit le dossier *etc* ensuite *inc* et on cherche le fichier *captiveportal.inc*. A partir de la on peut faire les modifications (figure 3.34).
- Après avoir fait les modifications que nous voulons, l'interface du portail captif s'affiche, comme dans la figure 3.35.

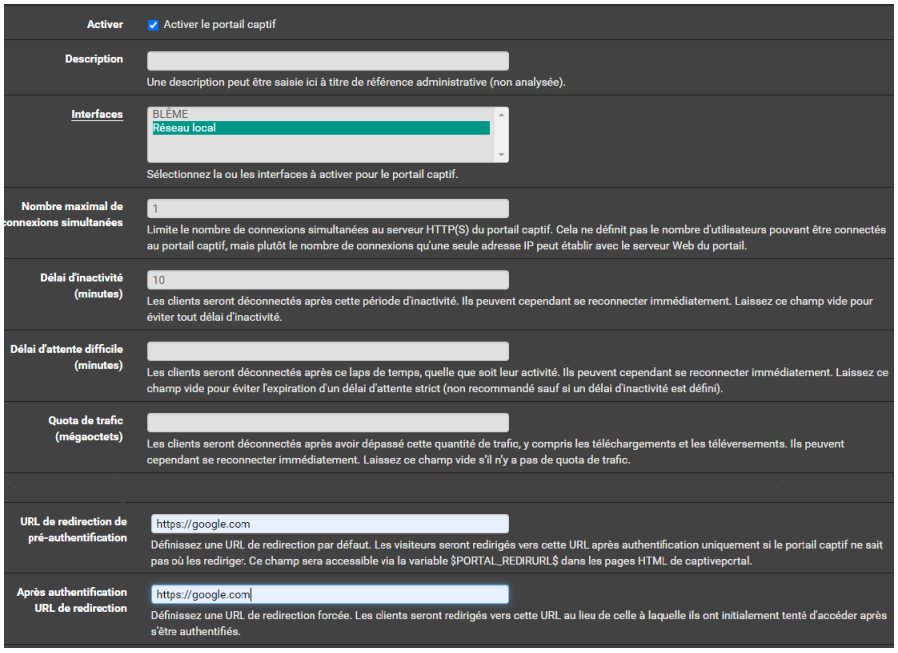

FIGURE 3.31 – Configuration portail captif

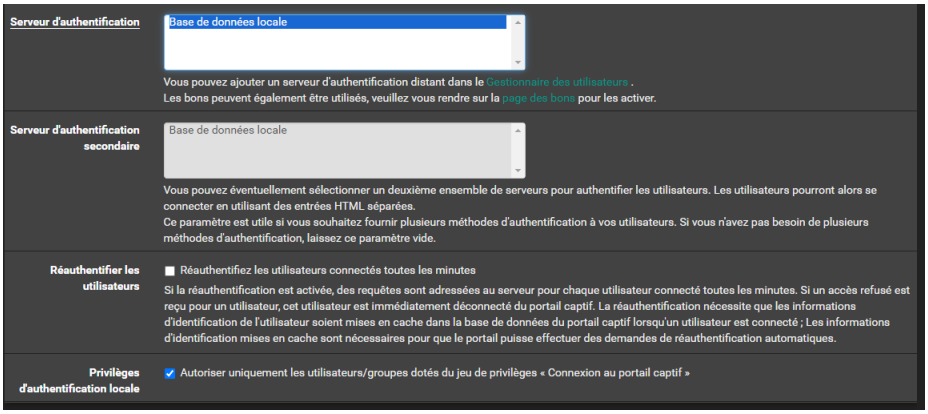

FIGURE 3.32 – L'authentification portail captif

FIGURE 3.33 – L'interface de portail captif

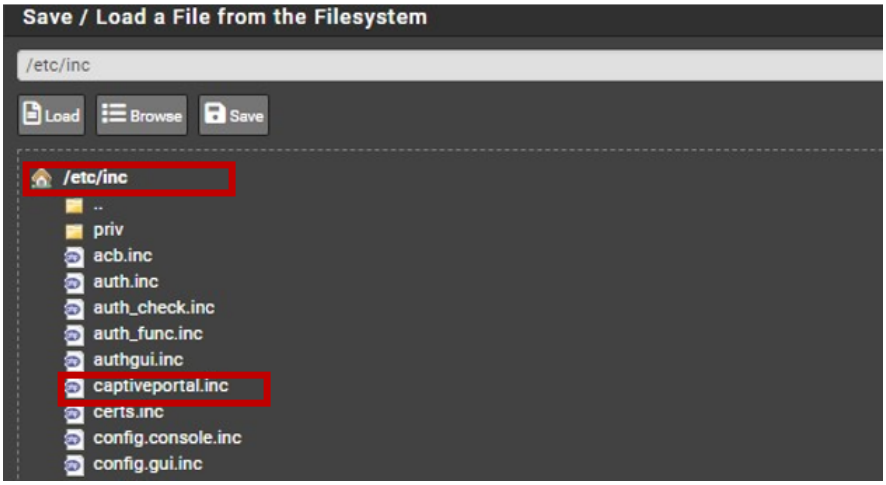

FIGURE 3.34 – L'interface de portail captif

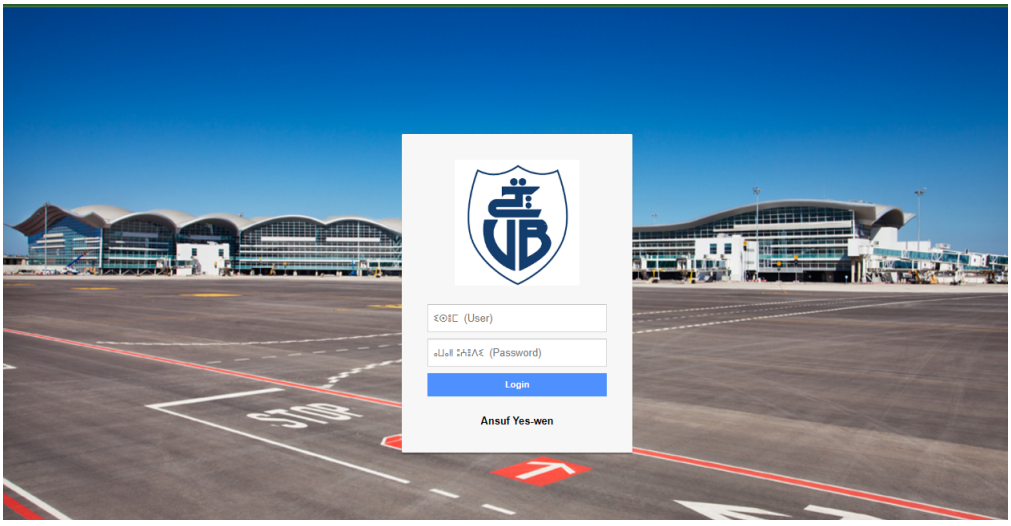

FIGURE 3.35 – L'interface de portail captif

3.6 Filtrage via AdGuard

Le filtrage consiste à bloquer l'accès à certains sites web et à des publicités indésirables afin de limiter leur accessibilité. Dans notre situation, nous optons pour *AdGuard* en tant que outil spécifique pour cette tâche. Il est possible d'intégrer *AdGuard* à *Pfsense* afin d'améliorer la sécurité du réseau en filtrant les URLs. Cela permet de contrôler et de limiter l'accès à des sites particuliers en fonction des besoins de sécurité de l'entreprise. Pour appliquer *AdGuard* sur *Pfsense*, il est nécessaire de configurer afin qu'il puisse analyser et filtrer le trafic web entrant et sortant à travers le pare-feu *Pfsense*, ce qui renforce la sécurité du réseau. Voici les étapes générales pour configurer AdGuard sur *Pfsense* :

3.6.1 Activer SSH

Secure Shell (SSH) est un outil essentiel pour les administrateurs système et les développeurs pour gérer les systèmes et les applications de manière sécurisée. L'activation de SSH permet de se connecter à *Pfsense* à distance via un terminal, ce qui est nécessaire pour effectuer certaines modifications de configuration qui ne sont pas disponibles via l'interface web.
Afin d'activer SSH sur *Pfsense*, il faut accédé à la section "Advanced" dans le menu "system", sur l'onglet "Admin Access", on parcoure jusqu'à la section "Secure Shell", cochons la case "Enable Secure Shell" pour activer SSH, puis on clique sur "Save" pour enregistrer.

3.6.2 Shellcmd

Le shellcmd est utile car il permet aux administrateurs de *Pfsense* d'automatiser des tâches qui ne sont pas directement supportées par l'interface graphique. Cela inclut la configuration avancée, la surveillance du système, la gestion des services et d'autres actions personnalisées nécessitant l'utilisation de commandes shell. En ajoutant des commandes shellcmd, vous étendez la fonctionnalité de *Pfsense* tout en conservant un contrôle centralisé et une gestion simplifiée via l'interface web.
Voici les étapes à suivre pour installer Shellcmd :

- Pour installer le package shellcmd sur *Pfsense*, dans le menu "System", nous avons sélectionne "Package Manager", nous avons recherché "shellcmd" sur la barre de recherche dans l'onglet "Available Packages", puis nous cliquons sur "Install" et on confirme l'installation.
- Après avoir terminé l'installation, nous allons sur le menu "Services" puis "Shellcmd", pour configurer des commandes système personnalisées sur notre pare-feu.
  Le champ "Command" est utilisé pour saisir la commande shell que l'on souhaite exécuter, par exemple, `"/usr/local/bin/screen -S AdGuardHome_screen -d -m /opt/AdGuardHome/AdGuardHome"`, pour démarrer le système *AdGuard Home*. Le champ

"Shellcmd Type" permet de choisir le type de commande shell, comme illustré sur la figure 3.36.

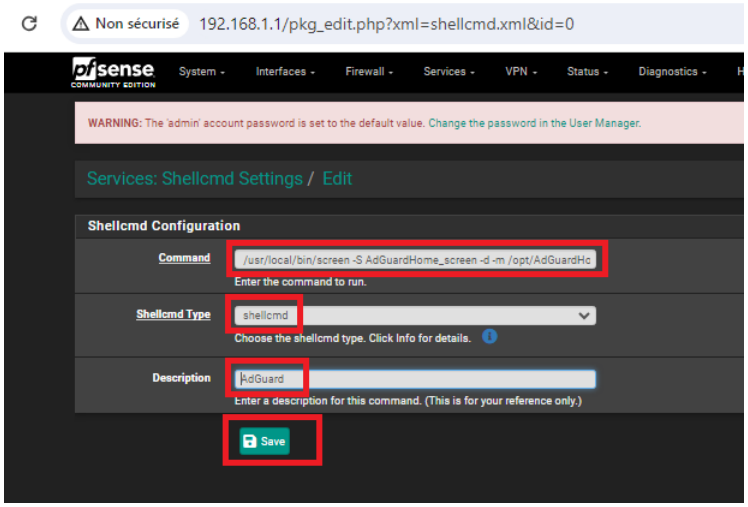

FIGURE 3.36 – Ajouter de commandes

3.6.3 Changement du port du DNS Resolver

Il est conseillé de modifier le port du DNS Resolver sur *Pfsense* afin d'éviter les attaques visant les services DNS. Le port DNS par défaut est très connu et fréquemment utilisé par des attaquants qui cherchent à perturber ou à mettre en péril les messages réseau. Grâce à l'utilisation d'un port non standard pour le DNS Resolver, nous améliorons la sécurité en diminuant la prévisible et en rendant plus difficile pour les attaquants de cibler spécifiquement ce service. Cela favorise une meilleure protection de notre infrastructure en réduisant les dangers liés à l'utilisation des services DNS.

- Pour modifier les paramètres du DNS Resolver, accédons à "Services" dans le menu principal, sélectionnons "DNS Resolver", on ajuste les configurations telles que l'activation de DNS resolver, spécifiant le port utilisé pour répondre aux requêtes DNS, on choisit "Localhost" comme interface réseau utilisée pour répondre aux requêtes des utilisateurs, comme le montre la figure 3.37.
- On sélectionne l'interface WAN comme interface réseau sortantes, on active DNSSEC afin de vérifier l'authenticité des réponses DNS, on active le mode de transfert pour rediriger les requêtes vers les serveurs DNS et on enregistre DHCP et les mappages DHCP statiques dans le résolveur DNS afin de résoudre les noms d'hôte des clients, comme indiqué par la figure 3.38.

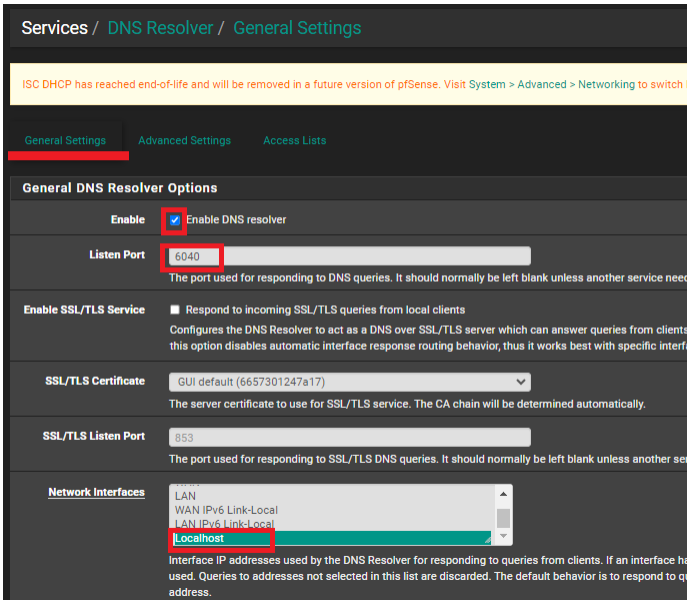

FIGURE 3.37 – Activation de DNS resolver

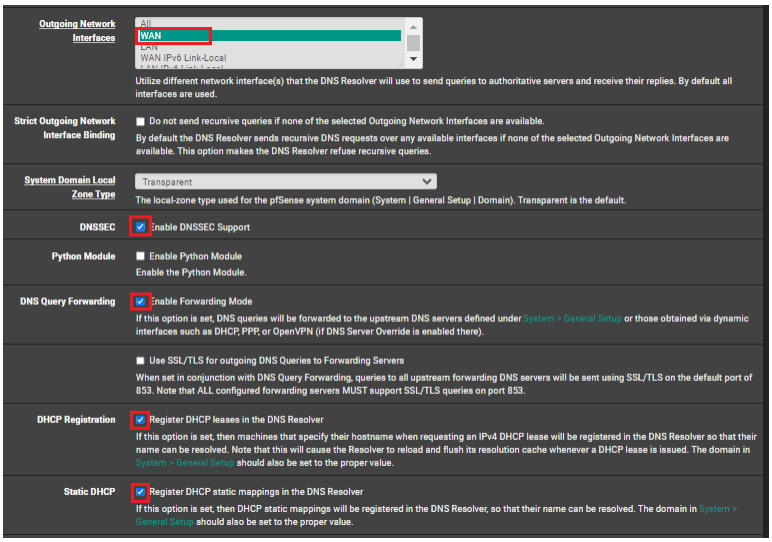

FIGURE 3.38 – DNS resolver

3.6.4 Installation AdGuard

Afin d'installer *AdGuard*, il est nécessaire de se connecter à distance à *Pfsense* en utilisant *Putty*, utilisé principalement pour accéder à distance et administrer des serveurs informatiques. Après avoir installé *Putty*, télécharger depuis le site officiel *Putty* Download, nous devrons saisir l'adresse IP publique de notre serveur *Pfsense* dans le champ "Host Name (or IP address)". Nous indiquons le port SSH, appuyez sur "Open" pour commencer la connection, tel que représenté la figure 3.39

- Après avoir connecter, Putty nous demandera de nous authentifier. On insère le nom d'utilisateur et le mot de passe associés à notre compte administrateur sur *Pfsense*, ce mot de

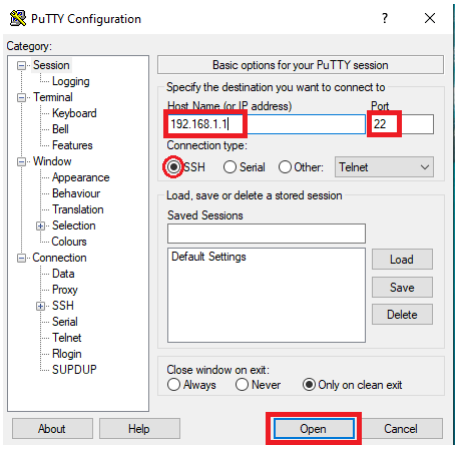

FIGURE 3.39 – Putty

passe ne serra pas visible sur la fenêtre pour des raisons de sécurité, comme on peut le voir sur la figure 3.40. On choisi l'option "shell(8)" pour débuter l'installation d'*AdGuard* et d'ajouter d'autres configurations nécessaires.

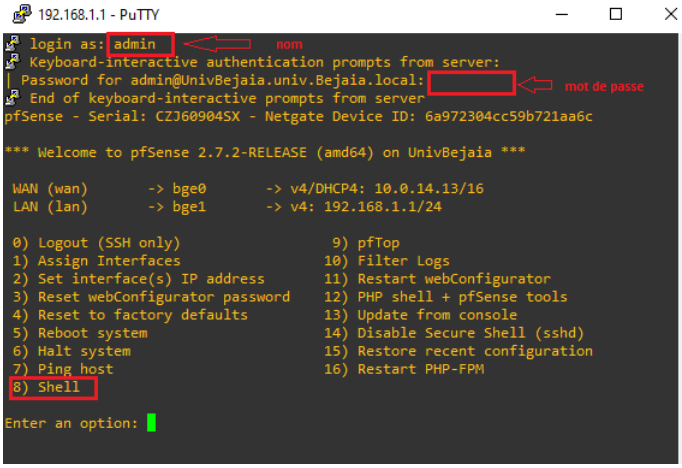

FIGURE 3.40 – Authentification sur Putty

- Une fois qu'on a saisi l'option "shell", on tape les commandes suivant pour télécharger le fichier *AdGuard*.
  - "cd /" cette commande permet de se déplacer dans le répertoire racine du système de fichier.
  - "mkdir opt" est une commande qui permet de créer le dossier "opt".
  - "cd opt" permet de se déplacer dans le répertoire "opt".
  - "fetch" est une commande utilisée pour télécharger des fichiers depuis une URL spécifiée. Dans notre cas, elle est utilisée pour télécharger le fichier compressé "`https://github.com/AdguardTeam/AdGuardHome/releases/download/v0.107.48/AdGuardHome_freebsd_amd64.tar.gz`" depuis GitHub.

— La commande "`tar -xvf AdGuardHome_freebsd_amd64.tar.gz`" est utilisée pour extraire les fichiers d'une archive tar.gz.
— La commande "cd AdGuardHome" permet d'accéder vers le dossier nommé "AdGuardHome".
— La commande "./AdGuardHome" est utilisée pour exécuter le fichier exécutable nommé "AdGuardHome" qui se trouve dans le dossier "AdGuardHome".
— Dès l'exécution du fichier, le nom de domaine sera affiché pour accéder à l'interface web AdGuard. D'après ce qui est montré la figure 3.41.

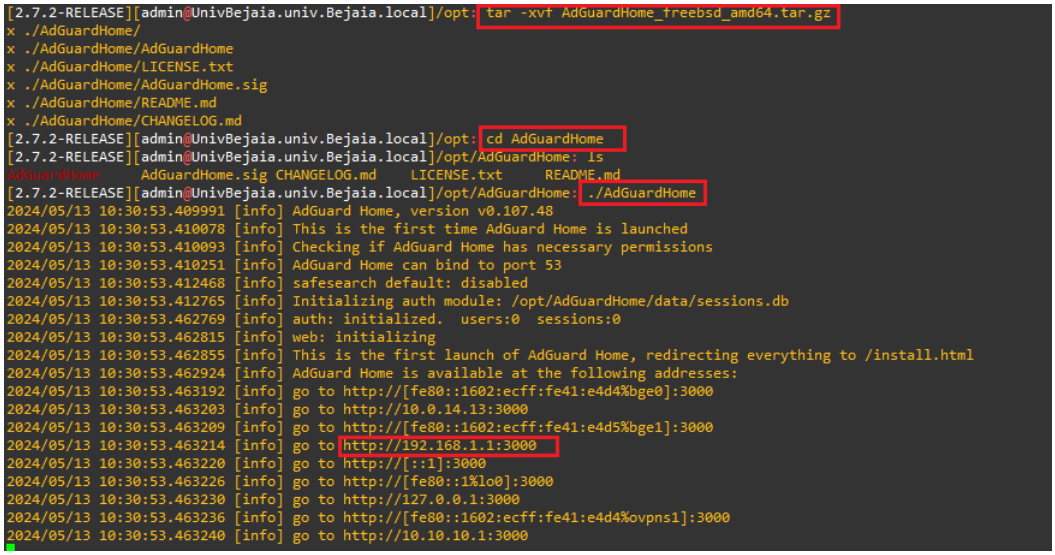

FIGURE 3.41 – Exécution du fichier

3.6.5 Interface web d'AdGuard

L'interface web d'AdGuardHome est essentielle pour configurer de manière précise les filtres de protection, de surveiller en temps réel l'activité du réseau et de faire les ajustements nécessaires pour assurer une protection efficace contre les publicités intrusives et autres dangers en ligne. De plus, elle facilite la gestion des listes de blocage, ce qui facilite la suppression, l'ajout ou la mise à jour des règles de filtrage afin de maintenir un environnement en ligne sécurisé et fluide.
Pour accéder à l'interface et effectuer les configurations nécessaires, voici les étapes à suivre :

- Dans le navigateur web on saisir le nom de domaine qu'on a obtenu lors de l'installation on obtient la fenêtre illustrée dans la figure 3.42, on clique "C'est parti" pour passer a une autre fenêtre.
- La fenêtre suivante permet de modifier le port selon notre préférence (la figure3.43).
- La fenêtre illustrée dans la figure3.44, permet de créer un utilisateur afin d'accéder à l'interface adGuard.
- La représentation de la figure 3.45 indique que la procédure d'installation est terminée et que nous sommes prêts à accéder au tableau de bord d'AdGuard.

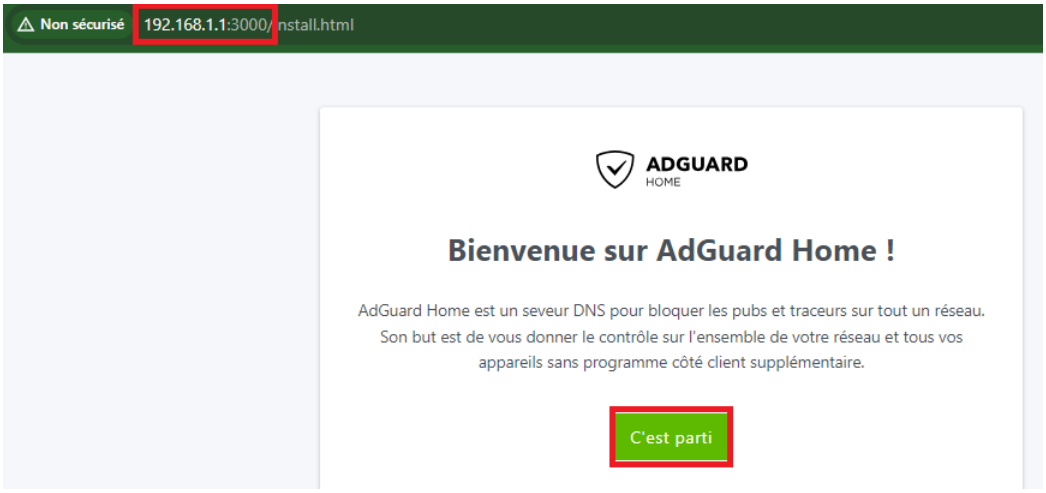

FIGURE 3.42 – Première fenêtre AdGuardHome

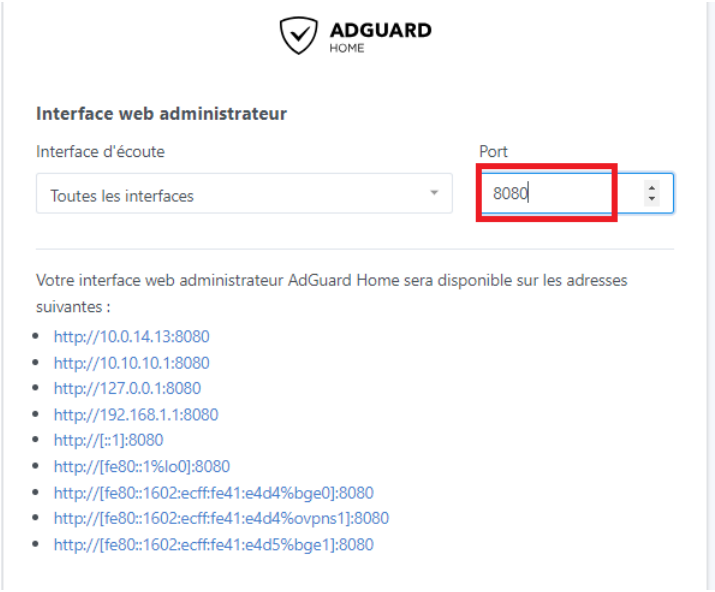

FIGURE 3.43 – Deuxième fenêtre AdGuardHome

- Nous visons à utiliser AdGuard afin de bloquer l'accès à certains sites web. Un blocage rapide grâce à une liste prédéfinie, qu'on peut la trouver sur l'onglet "Filtres" puis "Services bloqués" comme c'est illustrée dans la figure 3.46. On coche les sites que nous voulons bloqué, et tout en bas on clique sur "enregistrer".
- Sur la section "Règles de filtrage personnalisées", toujours dans l'anglet "Filtres", on peut bloqué un site qui n'apparaît pas dans la liste prédéfinie, en ajoutant le nom de domaine des sites qu'on espère bloquer et on clique sur "Appliquer". Comme on peut le voir dans la figure 3.47
- Sur l'onglet "Filtre" puis la section "Liste de blocage DNS" on active la liste de blocage en cochant la case *AdGuard DNS filter*, cela permet de bloquer automatiquement les domaines

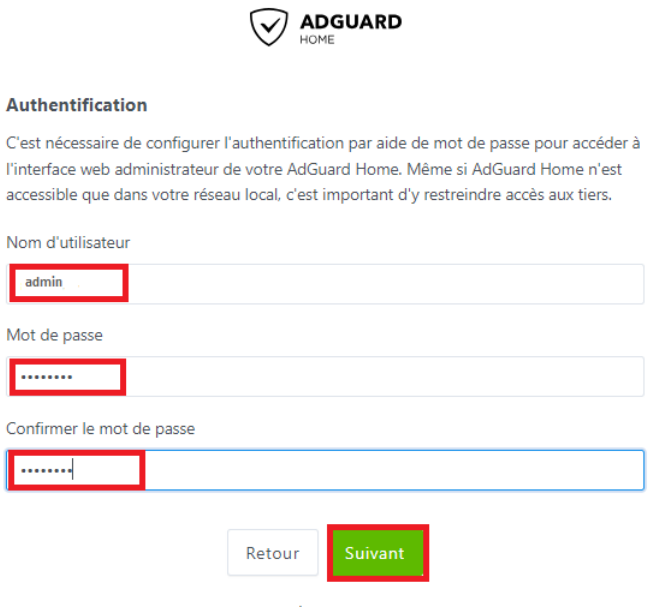

FIGURE 3.44 – Création d'un utilisateur

FIGURE 3.45 – Création d'un utilisateur

répertoriés, empêchant ainsi l'accès aux sites Web malveillants. Comme détaillé dans la figure 3.48.

3.7 Accès distant via VPN

OpenVPN est un serveur VPN sur *Pfsense*. Il permet d'accéder à l'ensemble des réseaux à distance de façon sécurisée. Le client et le serveur OpenVPN sont authentifiés à l'aide de certificats. Une autorité de certification et deux certificats : un certificat client et un certificat serveur. Ces deux certificats seront signés par l'autorité de certification. Ce type de VPN sert à établir un lien direct entre client VPN et le réseau de l'entreprise, grâce à un tunnel chiffré et sécurisé. Voici le schéma du notre configuration avec ce qui concerne les adresses des différents réseaux (figure 3.49) :

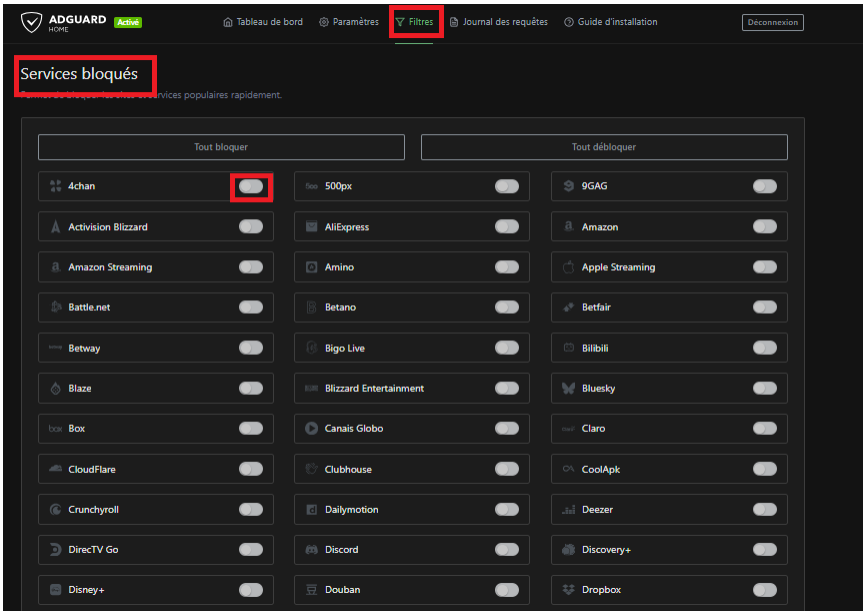

FIGURE 3.46 – Liste prédéfinie

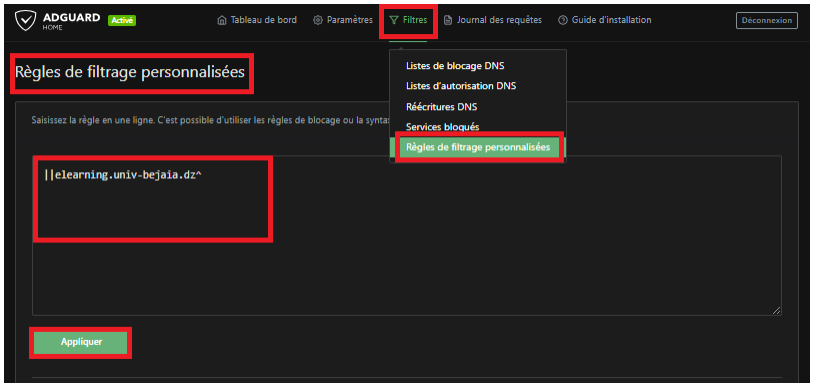

FIGURE 3.47 – Liste personnalisée

3.7.1 Installation OpenVPN

Pour commencer, il est nécessaire d'installer le package OpenVPN afin de configurer un VPN sécurisé. Voici les étapes détaillées pour effectuer cette installation :

- On accède au menu system>package manager.
- Dans l'onglet available packages on cherche "openvpn" sur la barre de recherche, et on clic sur "install" comme le montre la figure 3.50.
- Lors de l'installation du package, on observe clairement que le processus de téléchargement se déroule correctement comme l'indique la figure 3.51.
- Sur l'onglet "installed packages" on remarque que le package est bien installé comme l'illustre la figure 3.52. Cette section affiche une liste de tous les packages logiciels actuellement installés sur le système.

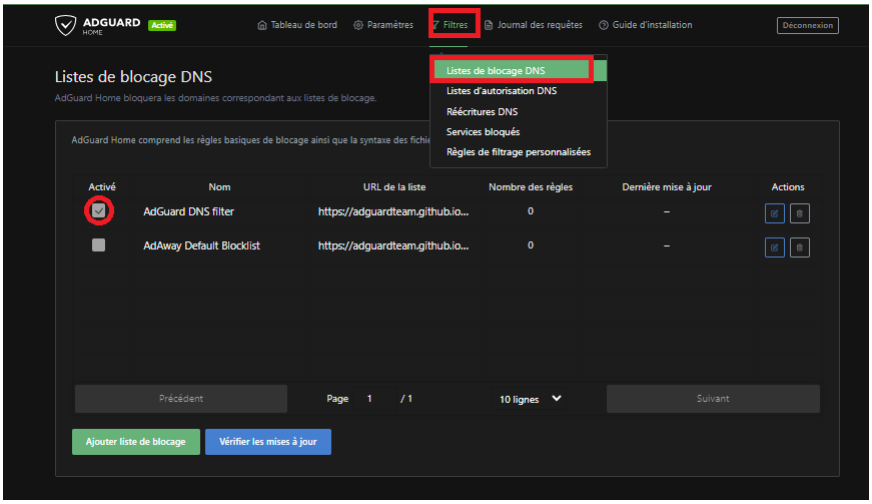

FIGURE 3.48 – Active la liste de blocage

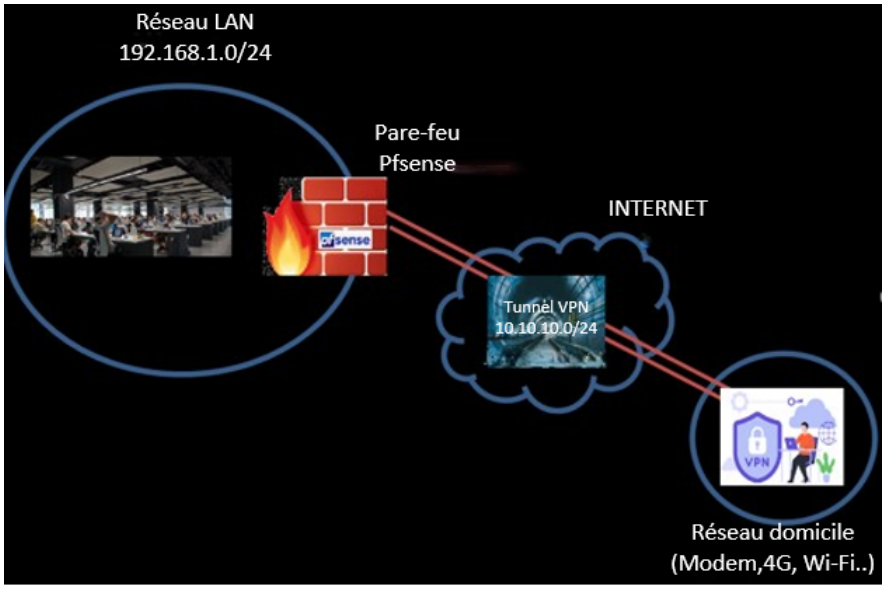

FIGURE 3.49 – Schéma de tunnel VPN

3.7.2 La gestion des certificats

L'importance des certificats dans un VPN réside dans la vérification de l'identité des serveurs et des clients. Ils garantissent l'authenticité des clés publiques utilisées par chaque partie, ce qui est crucial pour garantir la sécurité des communications.

La gestion des certificats implique la sécurisation de la création des clés publiques et privées requises. Cela assure que seules les connexions authentiques sont créées, ce qui renforce la confidentialité et la sécurité des échanges de données via le VPN.

Voici les éléments essentiels à prendre en compte lors de la gestion des certificats pour OpenVPN :

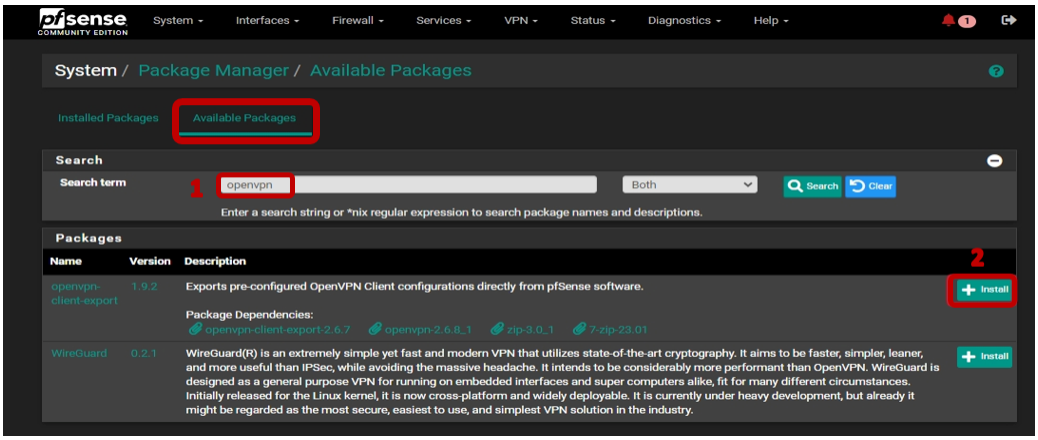

FIGURE 3.50 – Recherche OpenVPN

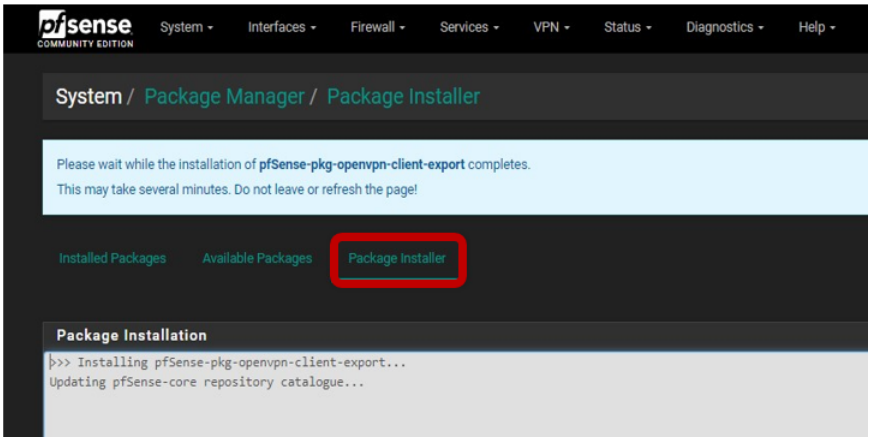

FIGURE 3.51 – Téléchargement OpenVPN

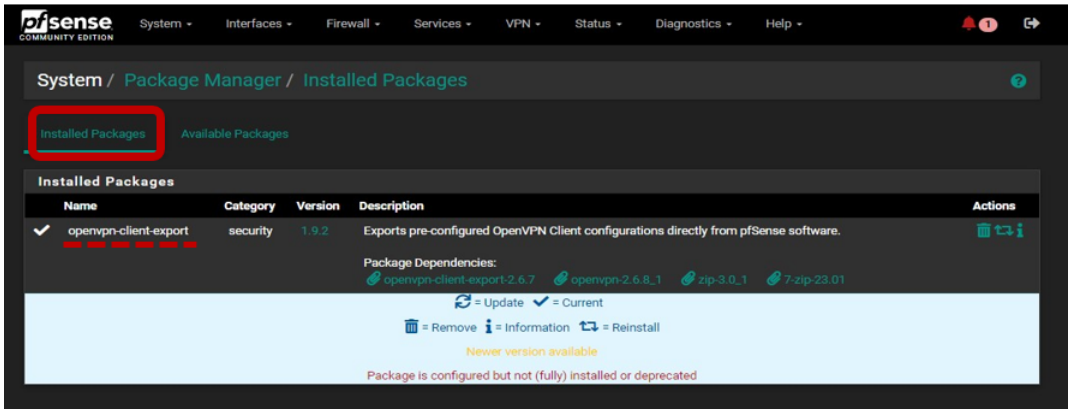

FIGURE 3.52 – Fin du téléchargement

3.7.2.1 Crée l'autorité de certification

La sécurité des communications numériques est assurée par une autorité de certification. Elle consiste à vérifier l'identité des serveurs et des utilisateurs en ligne en leur attribuant des certificats numérique. Ces certificats ont pour objectif de s'assurer que les connexions sur Internet sont sécu-

risées et fiables, en assurant que seuls les utilisateurs légitimes peuvent accéder aux informations sensibles et que les échanges de données sont protégés contre les intrusions.

- Pour crée l'autorité de certification on accède au menu system>certificates.
- Dans l'onglet *Authorities*, on clique sur le bouton "Add" (figure 3.53).

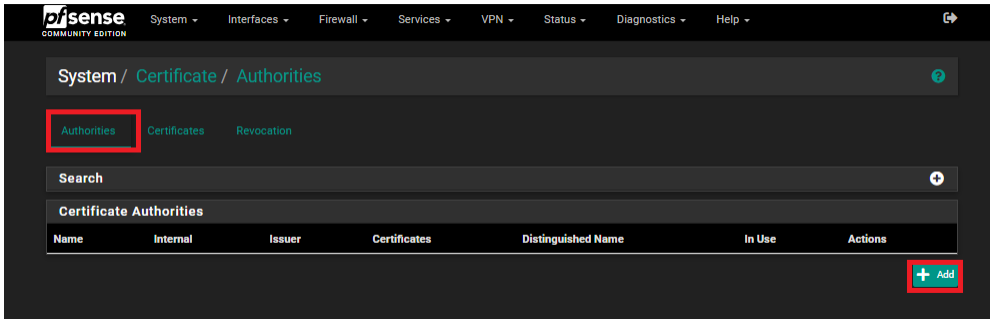

FIGURE 3.53 – Onglet d'autorité

- On donne un nom à l'autorité de certification, dans notre cas "vpn", ce nom sera visible seulement dans le *Pfsense*. On sélectionne la méthode "Create an internal Certaficate Authority" qui permet de créer une nouvelle autorité de certification. Le champ "Common Name" sert à afficher le nom de certificat, en suite on appuie sur le bouton "Save" situé en bas pour enregistre et finir la création (figure 3.54).
- Lorsque l'autorité de certification est créée, elle doit être affichée dans l'interface, comme illustré dans la figure 3.55.

3.7.2.2 Création de certificat serveur

Une fois que l'autorité de certification est crée, un autre certificat doit être généré pour le serveur VPN. L'importance de ce certificat du serveur VPN réside dans sa capacité à authentifier le serveur auprès des clients VPN, garantissant ainsi des connexions sécurisées et fiables.

- Toujours dans le menu system>certificates, cette fois-ci dans l'onglet "Certificates", on clique sur le bouton "Add/Sing" comme l'illustre la figure 3.56.
- On choisit la méthode "Create an internal Certificate" puisqu'il s'agit d'une création, dans le champ "Descriptive name" on lui donne un nom ("cer server" donne notre cas) et on sélectionne l'autorité de certification au niveau du champ "Certificate authority", il s'agit de l'autorité que nous avons créée auparavant. La validité et la durée de vie du certificat est fixée à 3650 jours par défaut comme représente dans la figure 3.57.
- Le type de certificat est sélectionné dans le champ "Certificate Type". Comme illustré dans la figure 3.58.
- Après avoir cliqué sur "Save" pour valider la création du certificat, il apparaît dans la liste des certificats du Pare-feu comme indiqué dans la figure 3.59.

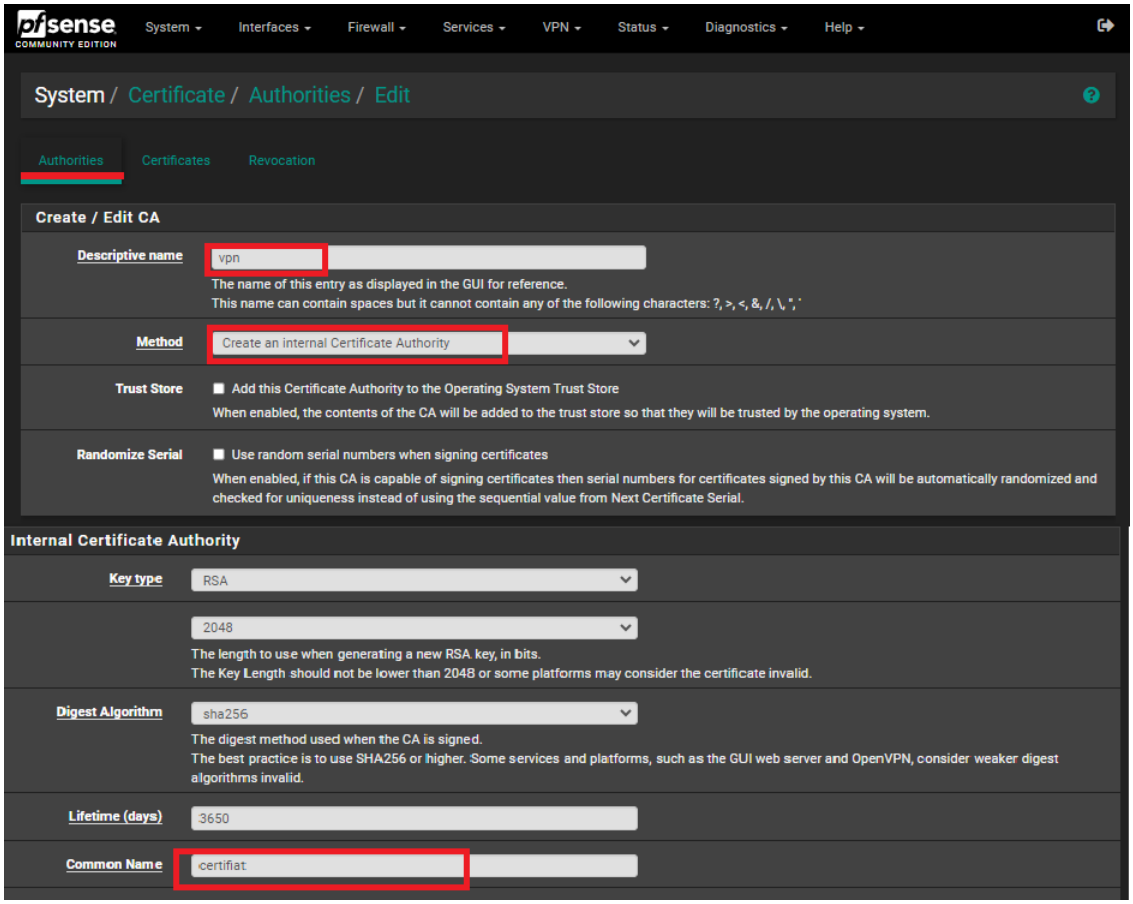

FIGURE 3.54 – Création d'autorité

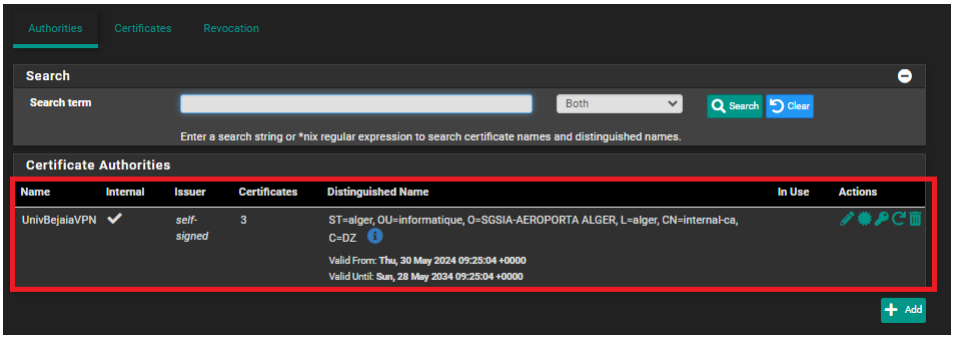

FIGURE 3.55 – Fin de création d'autorité

3.7.2.3 Création des utilisateurs VPN

Il est essentiel de mettre en place un utilisateur VPN afin de garantir la sécurité des connexions à distance et de contrôler qui peut accéder aux ressources réseau. Chaque utilisateur a ses propres identifiants qui restreignent l'accès aux seules personnes autorisées, ce qui renforce la protection des données sensibles et garantit une sécurité maximale lors du travail à distance.
Afin de créer un utilisateur VPN, il est nécessaire de suivre ces étapes :

- Dans le menu System>User Manager>User, nous ajoutons un identifiant et un mot de passe,

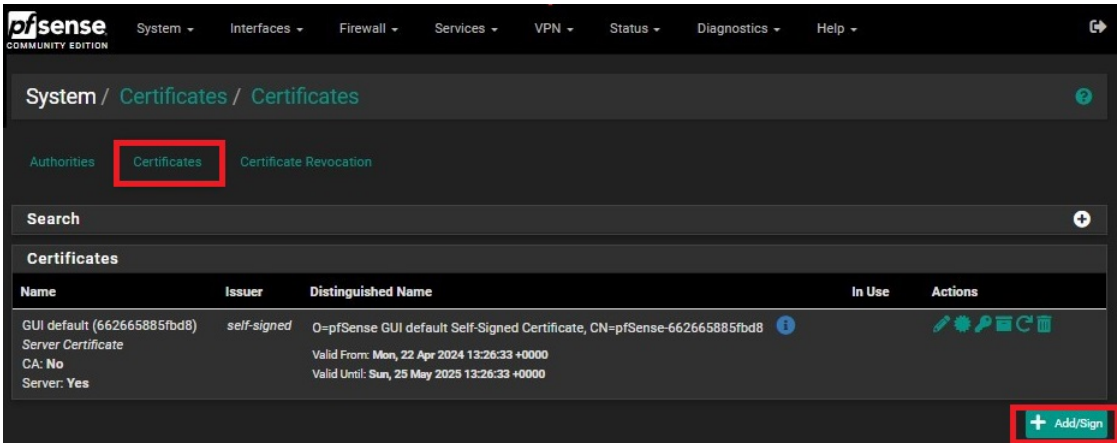

FIGURE 3.56 – Add de certificat

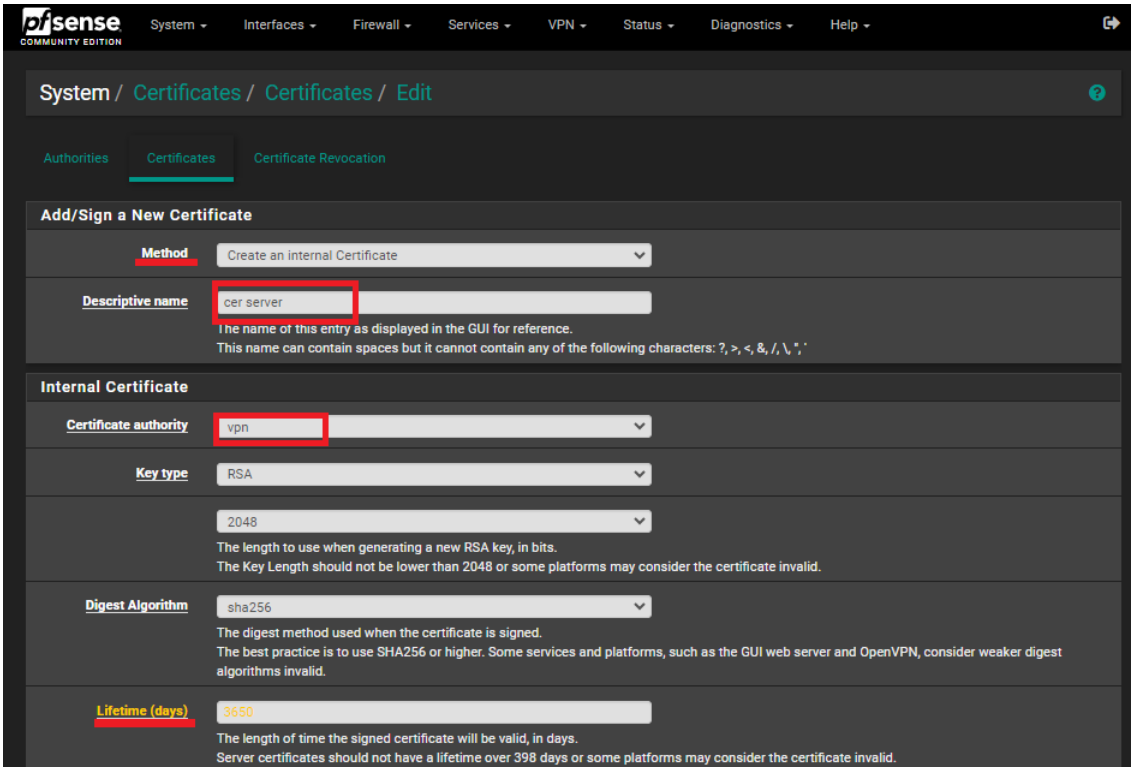

FIGURE 3.57 – Nomination de certificat

tout comme nous l'avions fait pour le portail captif. En plus de cela, nous sélectionnons l'option "Click to create a user certificate", ce qui ajoutera le formulaire de création du certificat juste en dessous. Afin de générer le certificat, nous appuyons sur notre organisme de certification et on sauvegarde, de la façon indiquée sur la figure 3.60.

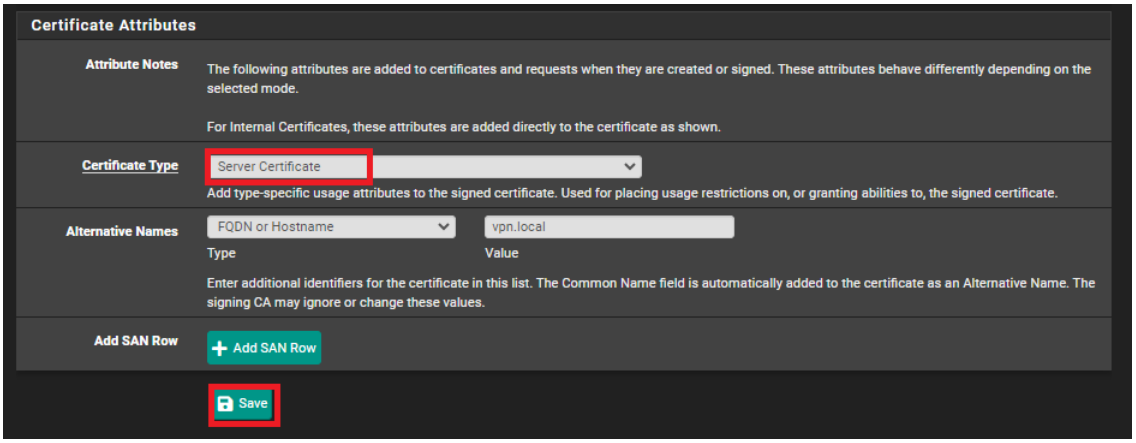

FIGURE 3.58 – Type de certificat

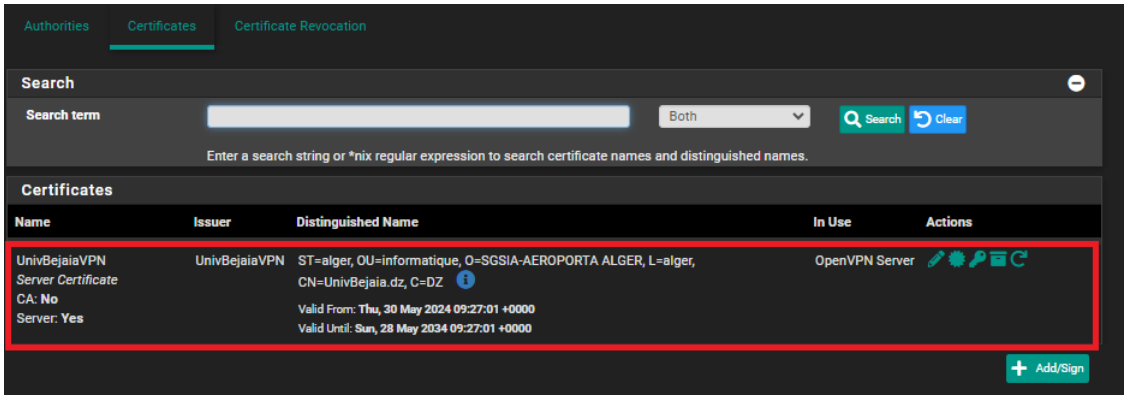

FIGURE 3.59 – Validation du certificat server

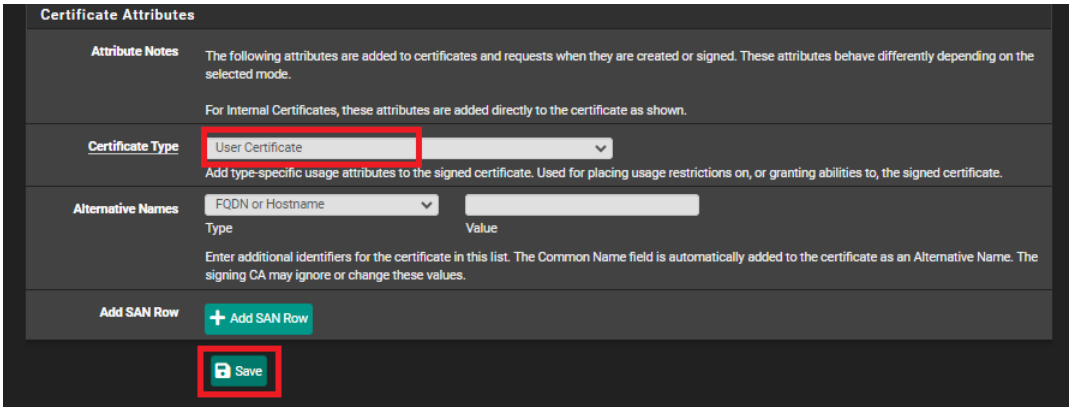

FIGURE 3.60 – Ajouter d'un utilisateur VPN

3.7.3 Configuration OpenVPN

Après avoir obtenu un certificat et un compte utilisateur, nous pouvons commencer à configurer le VPN. Avec cette configuration il est possible de mettre en place un réseau privé virtuel. En utilisant des tunnels chiffrés, cette configuration offre aux utilisateurs distants la possibilité de se connecter de manière sécurisée au réseau interne de l'entreprise via Internet. Cela garantit

la protection des données sensibles lors de leur transmission entre les utilisateurs distants et les serveurs internes. Ceci assure la confidentialité des échanges et l'intégrité des informations, offrant un accès sécurisé aux ressources réseau depuis n'importe quel endroit.
Pour cela, nous suivons les étapes suivantes :

- Nous accédons au menu VPN> OpenVPN.
- Dans l'ongle "Servers", on clique sur "add" pour céer une nouvelle configuration. Sur l'onglet "Server Mode" on choisit "Remote Access (SSL/TLS + User Auth)". Ce mode utilise SSL/TLS pour sécuriser les connexions et l'authentification des utilisateurs. Pour le VPN, le protocole s'appuie sur de l'UDP. UDP est sélectionné en raison de ses performances et de sa capacité à gérer les communications en temps réel, tandis que le port est utilisé pour faciliter les connexions VPN entrantes. Pour l'interface, nous allons conserver "WAN" puisque c'est bien par cette interface que l'on va se connecter en accès distant. Comme indiquée sur la figure 3.61.

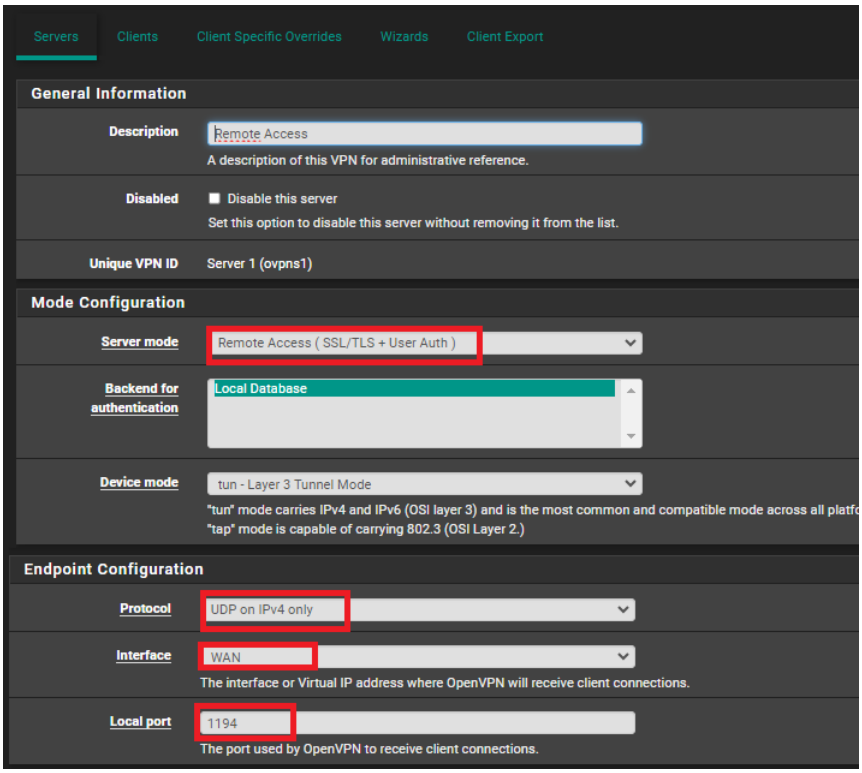

FIGURE 3.61 – Configuration d'accès distant open VPN

- Un peu plus bas dans la page, au niveau du champ "Peer CertificateAuthority" on sélectionner notre autorité de certification, cela permet au serveur VPN de vérifier l'authenticité des certificats des clients. Ensuite, dans le champ "Server certificate" on sélectionne le certificat serveur. Comme indiquée sur la figure 3.62.
- Passons maintenant à la configuration de notre tunnel VPN. Sur l'onglet "IPv4 Tunnel Network" il s'agit de l'adresse du réseau privé virtuel (VPN). Cela offre au client la possibilité

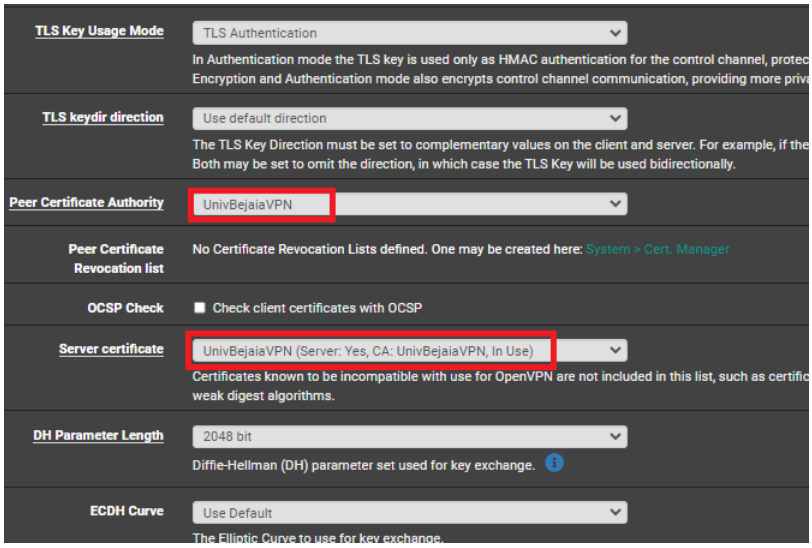

FIGURE 3.62 – Autorité de certificat OpenVPN

de communiquer de manière sécurisée avec le réseau interne en recevant une adresse IP dans le réseau sur sa carte réseau. En ce qui concerne l'onglet *IPv4Local Network*, ce champ fournit les adresses réseau des réseaux locaux que nous souhaitons exploiter à travers ce tunnel VPN.

- Sur l'onglet topologie, il est recommandé d'utiliser la topologie "net30 - isolated /30 network per client" pour que chaque client soit isolé dans un sous-réseau (de la plage réseau VPN), ce qui empêche les communications directes entre les clients et renforce la sécurité du réseau. En ajustant les paramètres DNS avancés pour les clients VPN, nous fournissons un domaine par défaut "UnivBejaia.lan" et définissons le serveur DNS, garantissant ainsi une résolution cohérente des noms de domaine et un accès sécurisé aux services internes. Comme le montre la figure 3.63.

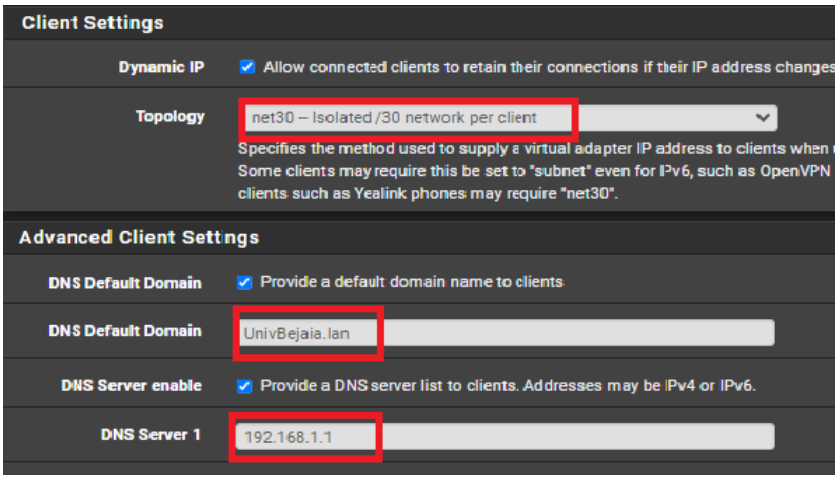

FIGURE 3.63 – Choisie la topologie er DNS

- Dans la zone "Custom options", on saisi "auth-nocache". Cette option est essentielle afin de

renforcer la sécurité de la connexion VPN. En refusant de stocker les identifiants d'authentification sur le cache, il offre une protection supplémentaire contre le vol de ces informations sensibles et en bas de la page on valide notre configuration.

- Sur la figure 3.64, on voit que notre configuration est prête.

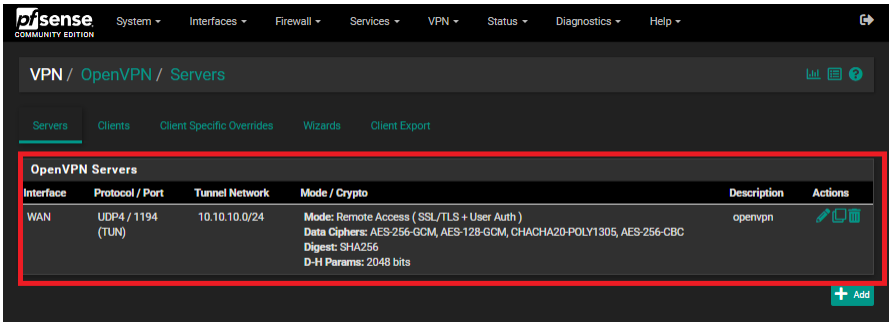

FIGURE 3.64 – Validation configurations VPN

3.7.3.1 Exporter le client OpenVPN

En exportant un client OpenVPN, nous permettons à l'utilisateur final d'établir facilement une connexion sécurisée au serveur OpenVPN, en fournissant tous les paramètres nécessaires, y compris le fichier de configuration, les certificats et clés requises.

- Nous devons accéder au menu "OpenVPN" puis dans l'onglet "Client Export". Si on souhaite utiliser un nom de domaine spécifique pour se connecter, on sélectionne l'option "Other" pour l'onglet "Host Name Resolution" et on choisit le nom de domaine dans l'onglet "Host Name". Il y a d'autres options possibles, notamment par l'adresse IP publique. On ajoute "auth-nocache" dans l'onglet "additional configuration options". Les autres options peuvent être laissées par défaut, comme sur la figure 3.65. On clique sur le bouton "Save as default" en bas de page pour enregistrer.
- Afin d'utiliser OpenVPN sur ordinateur, il est nécessaire de télécharger la configuration "Bundled Configuration" au format archive pour récupérer tous les fichiers nécesaires. Si nous souhaitons utiliser OpenVPN sur notre téléphone portable, on choisit la configuration "Inline Configuration". Comme c'est représenté dans la figure 3.66.

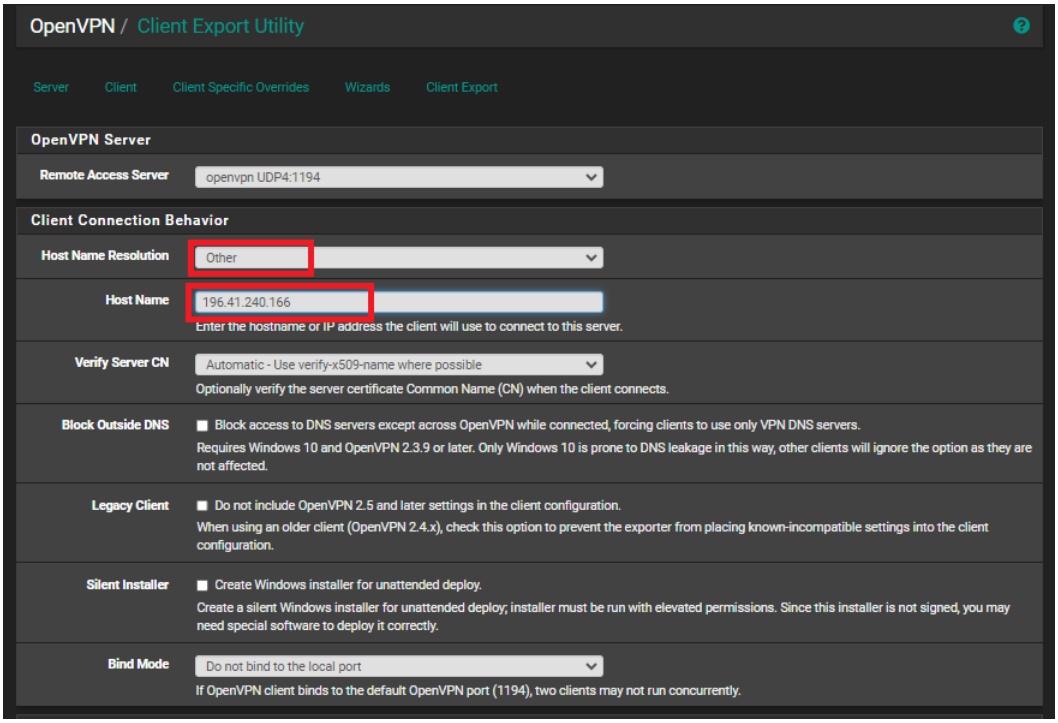

FIGURE 3.65 – L'onglet client export

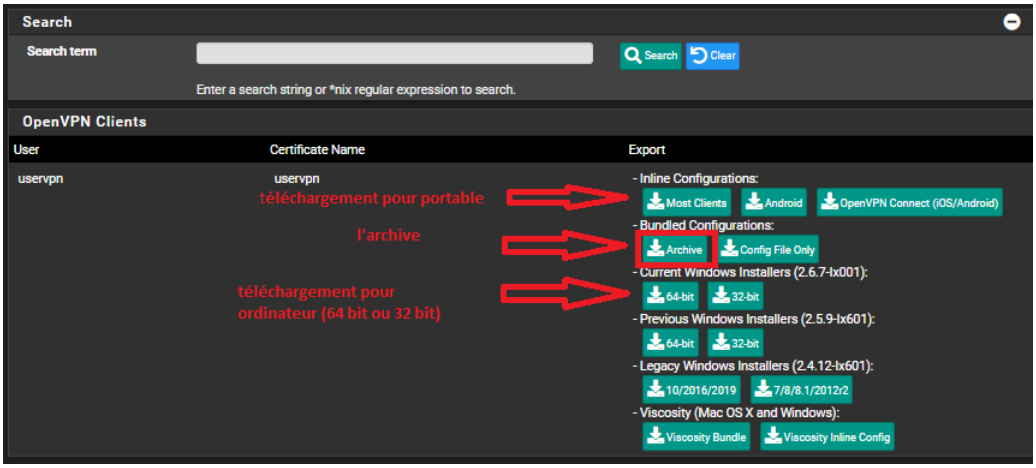

FIGURE 3.66 – Téléchargement de configuration

3.7.3.2 Règles pour OpenVPN

Nous devons configurer une règle de pare-feu pour permettre aux clients de se connecter au serveur via VPN, en autorisant le trafic entrant sur le port et le protocole spécifiques utilisés par le VPN. Une fois la connexion VPN établie, il est nécessaire de créer des règles supplémentaires pour autoriser l'accès aux ressources internes. Cela implique de définir des règles de pare-feu spécifiques pour chaque type de ressource comme par exemple les serveurs web, les serveurs de fichiers et les bases de données. Ces règles doivent permettre le trafic provenant des adresses IP attribuées aux clients VPN vers les adresses IP et les ports des ressources internes, garantissant ainsi un accès

sécurisé et contrôlé.

Voici les étapes détaillées pour accomplir cette tâche :

- On sélectionne le menu Firewall>WAN. Une nouvelle règle doit être créée en cliquant sur "Add", en optant pour le protocole UDP. Pour la destination, optons pour notre adresse IP publique donc sélectionnons "WAN address". Dans la liste des ports, choisissons OpenVPN ou notre port personnalisé. En appuyant sur "save" nous avons enregistré la création et autorisé le trafic entrant via un VPN (figure 3.67).

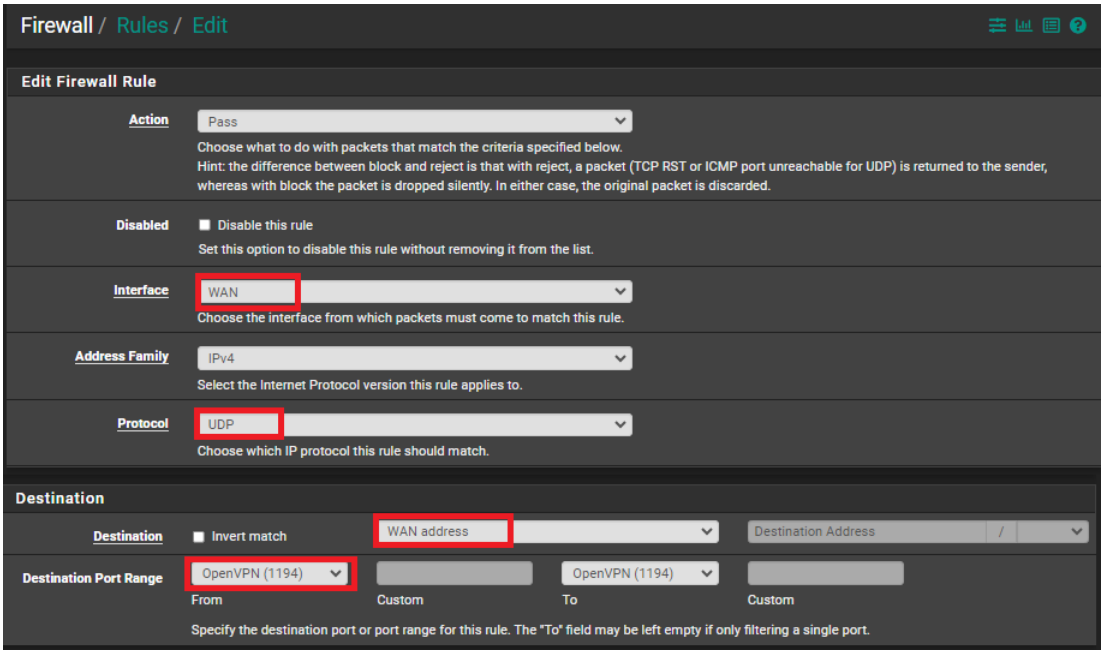

FIGURE 3.67 – Autorisation du flux OpenVPN

- Nous Ajoutons deux nouvelles règles pour autoriser l'accès aux ressources internes, cette fois-ci sur l'ongle *OpnVPN*. La règle qui suit sert à autoriser l'accès en RDP à l'hôte, qui fait parti du réseau autorisé dans la configuration du VPN, au travers du tunnel VPN. Pour la destination, ce sera donc notre hôte et le port 3389 pour le RDP, comme le montre la figure 3.68.
- La deuxième règle elle sert à autoriser tout type de protocole (on choisit notre protocole en fonction de nos besoins), comme illustré dans la figure 3.69.

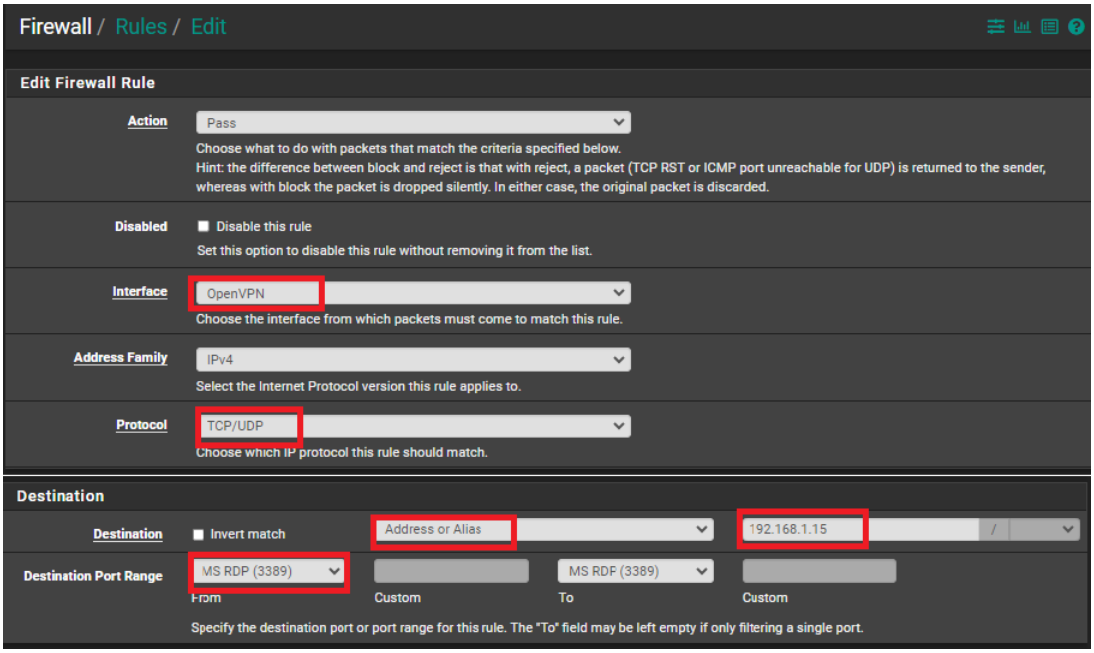

FIGURE 3.68 – Première règle d'interface OpenVPN

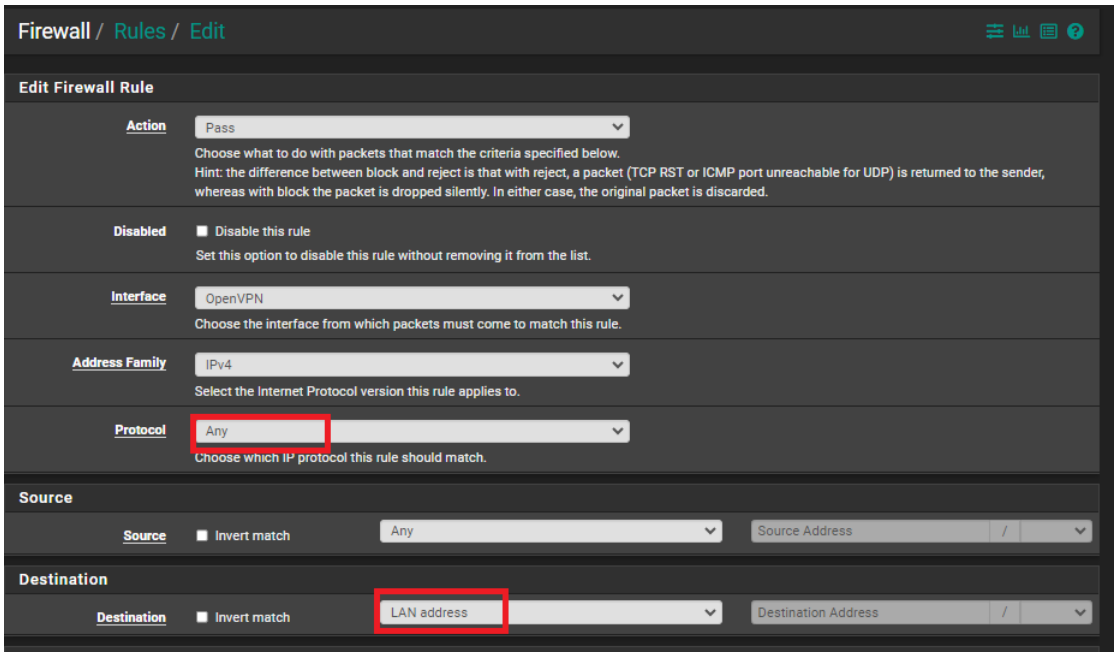

FIGURE 3.69 – Deuxième règle d'interface OpenVPN

3.7.4 Tester l'accès distant

Pour tester l'accès distant depuis un poste client sous ordinateur (ou un smartphone) via OpenVPN, il est essentiel de suivre une série d'étapes pour installer et configurer le client OpenVPN. Cette procédure permettra d'établir une connexion sécurisée, offrant ainsi la possibilité d'accéder aux ressources internes à distance tout en préservant la sécurité des données échangées.

- On commence par installer le client OpenVPN (pour un portable on télécharge l'application sur Google Play). Ce qui se fait très facilement, sans difficulté particulière.
- Après avoir fini l'installation on extrait le contenu de l'archive ZIP téléchargé depuis le *Pfsense* et qui contient la configuration, on le colle dans le dossier "C : Programmes OpenVPN Config "

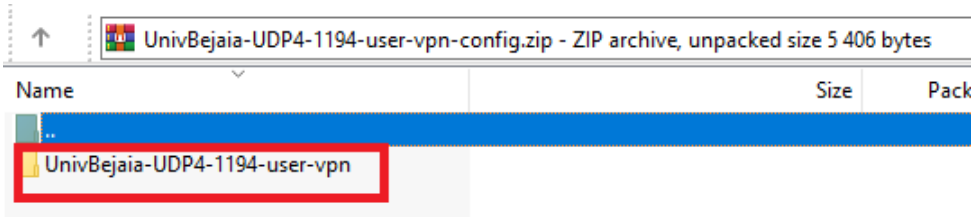

FIGURE 3.70 – Archive ZIP

- Ensuite sur l'icône OpenVPN effectuons un clic droit et cliquez sur "Connecter" comme sur la figure 3.72

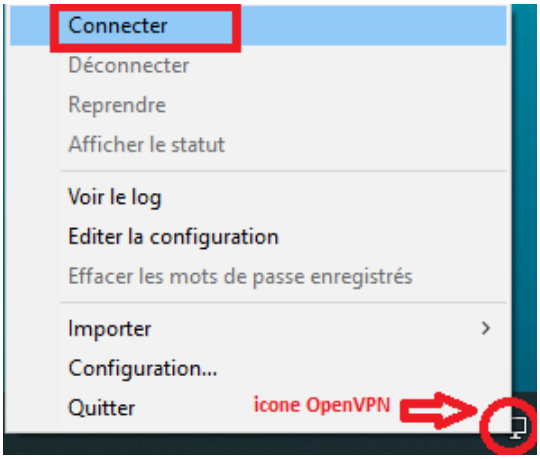

FIGURE 3.71 – Icone OpenVPN

— On fournit le nom d'utilisateur et le mot de passe sur la fenêtre qui s'affiche, comme c'est illustré sur la figure 3.72.

- Lorsque le tunnel VPN est actif, l'icône devient vert. On remarque aussi qu'une adresse IP est fourni pour le client comme illustré dans la figure 3.73. Désormais, notre VPN est prêt à être utilisé.

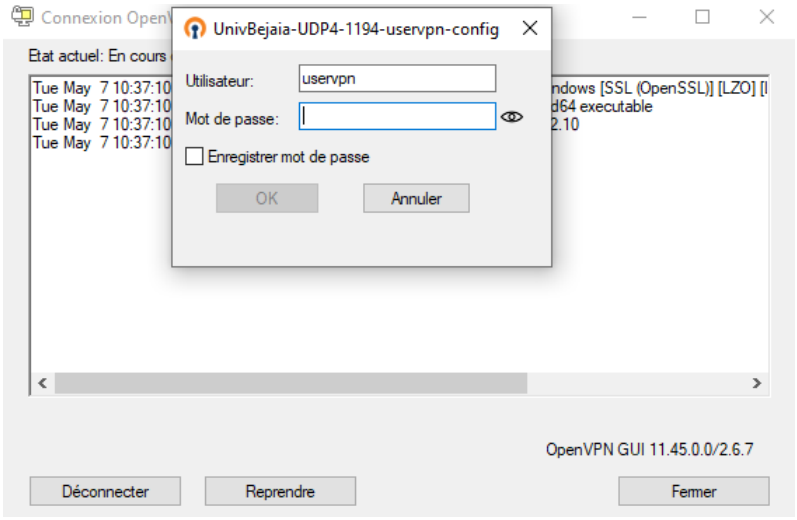

FIGURE 3.72 – Nom d'utilisateur et le mot de passe

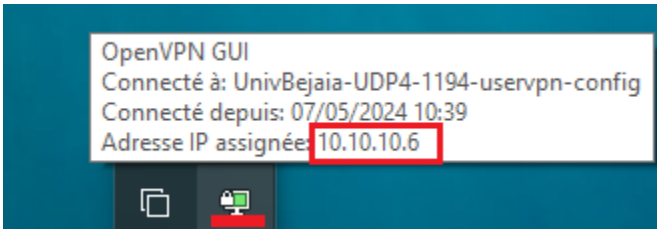

FIGURE 3.73 – VPN actif

3.8 Conclusion

En conclusion, ce chapitre a détaillé la mise en œuvre de notre solution réseau. Nous avons installé et configuré *Pfsense*, mis en place un portail captif, intégré AdGuard et configuré un accès distant via VPN.

Ces mesures ont permis de créer une infrastructure réseau sécurisée qui répond à nos besoins. Cette réalisation nous a offert une expérience précieuse en appliquant des solutions théoriques dans un environnement réel, assurant ainsi une gestion optimale du réseau.

Conclusion et perspectives

Le réseau informatique est devenu essentiel pour chaque entreprise afin de continuer à mener ses activités. Chaque réseau existant peut subir des menaces et des attaques à chaque fois qu'il s'ouvre sur internet, et pour cela faut sécurisé ces réseaux.

Dans notre mémoire, notre objectif a été d'améliorer la sécurité du réseau de la SGSIA contre les menaces et les attaques éventuelles qui risquent de l'atteindre. Pour cela on met en place un pare-feu, dans notre cas il s'agit de *Pfsense*, qui permet de sécuriser le réseau d'entreprise contre les intrusions et les failles de systèmes et des attaques, en filtrant tout information et fichier qui rentre et sort du réseau privé vers Internet. Le portail captif a été utilisé dans le but de contrôler et limiter l'accès à Internet qui inclut l'authentification pour renforcer la sécurité. Afin de filtrer la navigation sur le web et bloquer les publicités indésirables et les sites web inappropriés on a exploité AdGuard. Pour le bien-être des employés et pour améliorer leur environnement de travail, nous avons autorisé l'accès à distanceà leur poste de travail grâce à l'un des services de Pfsence qui s'agit de OpenVPN.

Notre stage nous a permis d'améliorer nos connaissances et la disponibilité du matériel nous a facilité l'apprentissage et l'acquisition des compétences dans le domaine de la sécurité des réseaux notamment le pare-feu *Pfsense* et certains outils logiciels ainsi leur fonctionnement et leur rôle dans la sécurité d'entreprise. Dans ce cadre, nous avons atteint l'objectif fixé au début de notre mémoire.

En perspective, nous prévoyons d'étudie comment l'intelligence artificielle et l'apprentissage automatique peuvent être utilisés pour améliorer la détection des menaces, la prévention des intrusions, et la réponse aux incidents dans les réseaux d'entreprise.

Bibliographie

[1] Document Fourni par SGSIA(MISSIONS DE LA SGSIA), 14 mars 2024.

[2] Document Fourni par SGSIA(Organigramme), 14 mars 2024.

[3] Document Fourni par SGSIA(presentation), 14 mars 2024.

[4] https ://www.cloudflare.com/fr-fr/learning/access-management/what-is-the-remote-desktop-protocol/, consulté le 11 juin 2024.

[5] https ://www.techno-science.net/glossaire-definition/Ordinateur.html, Consulté le 20 mars 2024.

[6]]https ://blog.netwrix.fr/2019/07/24/tout-ce-quil-faut-savoir-sur-les-equipements-reseau/, Consulté le 20 mars 2024.

[7] https ://www.alamyimages.fr/photos-images/topologie-de-rConsulté le 26 mars 2024.

[8] https ://www.pinterest.com/pin/593138213444742842/, Consulté le 26 mars 2024.

[9] https ://www.istockphoto.com/fr/photo/ordinateur-de-bureau-gm667294056-121742559, Consulté le 26 mars 2024.

[10] https ://www.shutterstock.com/fr/, Consulté le 27 mars 2024.

[11] https ://datascientest.com/protocoles-reseau-tout-savoir, Consulté le 30 mars 2024.

[12] Philippe ATELIN. *Réseaux informatiques : Notions fondamentales.* ENI, 3 eme edition, 2009.

[13] Nadia BATTAT. *Les système de sécurité.* Mémoire de fin de cycle, Université A. Mira de Bejaia, 2022.

[14] Jean-François CARPENTIER. *La sécurité informatique dans la petite entreprise Etat de l'art et Bonnes Pratiques.* ENI, 3 eme edition, 2016.

[15] Jean-François CHALLE. *Administration et sécurité des réseaux.* Charleroi, Belgique, 2015.

[16] Ghada TINOUILINE Célina CHERAFT. *Configuration et sécurisation de réseau de l'entreprise Général Emballage à base des Liaisons Virtuelles.* Mémoire de fin de cycle, Université A. Mira de Bejaia, 2023.

[17] Dominique SERET Danièle DROMARD. *Architecture des réseaux.* PEARDON, 1 ere edition, 2009.

[18] José DORDOIGNE. *Réseaux informatiques Notions fondamentales (Protocoles, Architec tures, Réseaux sans fil, Sécurité, IP v6,. . .).* ENI, 5 eme edition, 2013.

[19] Yann DUCHEMIN. *introduction à l'interconnexion de réseau.* 1 ere edition, 2001.

[20] Damien BANCAL Franck EBEL. *Sécurité informatique Ethical Hacking Apprendre l'attaque pour mieux se défendre.* ENI, 1 ere edition, 2009.

[21] Solange GHERNAOUTI. *Cybersécurité sécurité informatique et réseaux.* DUNOD, 5 eme edition, 2016.

[22] Pierre-Alain GOUPILLE. *technoogie des ordinateurs et des reseaux.* DUNOD, 7 eme edition, 2014.

[23] Silia DAOU Imane ADDA. *Mise en ?uvre d'une solution de sécurité basée sur le pare-feu PfSense pour l'Entreprise Portuaire de Béjaïa.* Mémoire de fin d d'études, Université A. Mira de Bejaia, 2021.

[24] Frédéric Jacquenod. *Normalisation des réseaux.* 1 ere edition, 2008.

[25] Christophe WOLFHUGEL Laurent BLOCH. *Sécurité informatique Principes et méthodes à l'usage des DSI, RSSI et administrateurs.* EYROLLES, 4 eme edition, 2013.

[26] Doug LOWE. *Les reseaux pour les nuls.* 10 eme edition, 2017.

[27] Jean-Luc MONTAGNIER. *Construire son réseau d'entreprise.* EYROLLES, 1 ere edition, 2001.

[28] Guy PUJOLLE. *Initiation aux reseaux : cours et exercices.* EYROLLES, Paris, 2000.

[29] Guy PUJOLLE. *les réseaux.* EYROLLES, Paris, 5 eme edition, 2006.

[30] Guy PUJOLLE. *les réseaux.* EYROLLES, Paris, 8 eme edition, 2014.

[31] André VAUCAMPS Romain LEGRAND. *CISCO : Notions de bases sur les réseaux.* ENI, 2014.

[32] Innokenty RUDENKO. *Configuration IP des routeurs Cisco.* EYROLLES, 1 ere edition, 2000.

[33] Claude SERVIN. *réseaux et telecoms :cours avec 129 exercices corrigés.* DUNOD, 2 eme edition, 2006.

[34] Abderrahmane SIDER. *Technologies Internet.* Support de cours.m2, Université A. Mira de Bejaia, 2017.

[35] Pascal URIEN. *Introduction à la Cyber Sécurité.* TELECOM PARIS, 1 ere edition, 2021.

[36] Titouan SOULARD Vincent SENETRAIRE, Jean-Manassé POUABOU. *Les Réseaux de zéro : comprendre les réseaux par la pratique.* EYROLLES, 2022.

[37] John WILEY. *Sécurité informatique pour les nuls.* WILEY, 1 ere edition, 2010.

[38] Yasmine MOKRANI Yasmina BENNACER. *Les outils d'administration et sécurité des réseaux informatiques : cas d'étude Sonatrach.* Mémoire de fin de cycle, Université A. Mira de Bejaia, 2021.

[39] Mohand YAZID. *Cours et Travaux Pratique : Administration des réseaux.* Support de cours.m2, Université A. Mira de Bejaia, 2022.

RÉSUMÉ

Le réseau informatique est essentiel pour chaque entreprise afin de mener ses activités. Chaque réseau existant peut subir des menaces et des attaques lorsqu'il est connecté à Internet, c'est pourquoi nous avons opté pour une solution de sécurisation. Notre objectif est d'améliorer la sécurité du réseau de la SGSIA contre les menaces et attaques potentielles. Pour cela, nous avons mis en place un pare-feu, *Pfsense*, qui sécurise le réseau contre les intrusions et les failles en filtrant les informations et fichiers entrant et sortant. Un portail captif contrôle et limite l'accès à Internet en incluant une authentification. Pour filtrer la navigation et bloquer les publicités et sites inappropriés, nous utilisons AdGuard. Nous avons aussi autorisé l'accès à distance grâce à OpenVPN pour améliorer l'environnement de travail des employés. Notre stage nous a permis d'améliorer nos connaissances et compétences en sécurité des réseaux, notamment sur le pare-feu Pfsense et certains outils logiciels. Nous avons atteint l'objectif fixé au début de notre mémoire.

Mots clés : SGSIA, Pfsense, AdGuerd, portail captif, OpenVPN

ABSTRACT

The computer network has become essential for every company to continue its activities. Every existing network can be subjected to threats and attacks whenever it connects to the Internet, which is why we opted for a security solution. Our objective is to improve the security of the SGSIA network against potential threats and attacks. For this, we have implemented a firewall, *Pfsense*, which secures the network against intrusions and vulnerabilities by filtering incoming and outgoing information and files. A captive portal controls and limits Internet access by including authentication. To filter browsing and block unwanted ads and inappropriate websites, we use AdGuard. We have also enabled remote access via OpenVPN to improve the employees' work environment. Our internship allowed us to enhance our knowledge and skills in network security, particularly with the Pfsense firewall and certain software tools. We achieved the goal set at the beginning of our dissertation.

Keywords : SGSIA, Pfsense, AdGuard, captive portal, OpenVPN