REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira, Bejaia
Faculté des Sciences Exactes
Département d'informatique

Mémoire de fin de cycle

En vue de l'obtention du diplôme de master Professionnel en informatique
Option Administration et sécurité des réseaux

Thème

Solution VPN d'accès distant à l'intranet de l'université de Bejaia : Application au réseau VLAN de la scolarité

Réalisé par :

Mlle BRAHMI THiziri
Mlle SAHI Sara

Devant le Jury compose de :

Président : Mr SALHI Nadir
Examinateur : Mr BAADACHE Abderrahmane
Examinateur : Mlle AIT HATRI Fatima.
Encadreur : Mr TOUAZI Djoudi

Promotion : 2017/2018

Remerciements

Nous tenons dans un premier temps à remercier le bon dieu le tout puissant qui nous a donné le courage et la volonté pour mener à bien ce modeste travail.

En préambule à ce mémoire nous souhaitons adresser nos remerciements les plus sincères aux personnes qui nous ont apportées leur aide et qui ont contribuées à l'élaboration de ce mémoire ainsi qu'à la réussite de cette année universitaire.

Nous exprimons notre reconnaissance à Monsieur **TOUAZI Djoudi** d'avoir joué pleinement son rôle de promoteur en étant à nos côtés tout au long de l'étude de notre projet, ses conseils et orientations nous ont guidés jusqu'à l'aboutissement de ce travail.

Aussi nous exprimons notre profonde gratitude et sincère reconnaissance aux membres du jury, d'avoir accepte d'examiner ce travail.

Enfin, nous adressons nos plus sincères remerciements à nos parents et ami(e)s, pour leur soutien et encouragements au cours de la réalisation de ce mémoire. Merci à tous et à toutes.

Dédicace

Je dédie ce modeste travail,

Résultat de toutes mes années d'étude :

A mon cher papa, à ma chère maman, pour leur amour inconditionnel, leur affection attentionnée, leurs soutien permanent, leurs conseils judicieux et leurs sacrifices sans limite, autant de phrases ne sauraient décrire ce que vous m'avez apporté pour être ce que je suis aujourd'hui. Que le Dieu, le tout puissant, vous accorde santé, bonheur et vous préserve de tout mal

Je vous aime tellement

A Mes sœurs et frère

Je dédie ce mémoire à mes très chères sœurs Nesma ,Wissem et Yasmine et mon petit frère chéri Arris, tous les mots du monde ne sauraient exprimer l'immense amour que je vous apporte

A Ma chère binôme : Sara et toute sa famille

A ma meilleure amie, la source de mon bonheur : Yasmine

A mes chers amis : djidji, wissem, dida, wassila

Brahmi Thiziri

Dédicace

Je dédie ce modeste travail,

Résultat de toutes mes années d'étude :

A mon cher papa, à ma chère maman, pour leur amour inconditionnel, leur affection attentionnée, leur soutien permanent, leurs conseils judicieux et leurs sacrifices sans limite, autant de phrases ne sauraient décrire ce que vous m'avez apporté pour être ce que je suis aujourd'hui. Que le Dieu, le tout puissant, vous accorde santé, bonheur et vous préserve de tout mal

Je vous aime tellement

A Ma sœur

Je dédie ce mémoire à ma très chère sœur Imène, tous les mots du monde ne sauraient exprimer l'immense amour que je t'apporte

A Ma chère binôme : THiziri et toute sa famille

Sahi Sara

Liste des Abréviations

AES: Advanced Encryption Standard.

AH: Authentification Header.

BGP: Border Gateway Protocol.

DDoS: Distributed Denial of Service.

DES: Data Encryption Standard.

DH: Diffie Hellman .

DHCP: Dynamic Host Configuration Protocol.

DMZ: Demilitarized zone.

DNS: Domain Name System.

DoS: Denial of Service.

DSA: Digital Signature Algorithm.

ESP: Encapsulation Security Payload.

FCS: Frame Check Sequence.

FDDI: Fiber Distributed Data Interface.

FTP: File Transfer Protocol.

H-IDS: Host Based Intrusion Detection System.

Http: Hypertext Transfer Protocol.

IDS: Intrusion Detection System.

IP: Internet Protocol.

IP SEC: Internet Protocol Security.

ISO: International Standard Organisation.

LAN: Local Area Network.

MAN: Metropolitan Area Network.

MD5: Message Digest 5.

NAT: translation d'adresses.

N-IDS: Network Based Intrusion Detection System.

OLSR: Optimized Link State Routing.

OSI: Open Systems Interconnection.

PAN: Personal Area Network.

PKI: Public Key Infrastructure.

PPP: Point to Point Protocol.

RIP: Routing Information Protocol.

RSA: Rivest Shamir Adleman.

SHA1: Secure Hash Algorithm 1.

SMTP: Simple Mail Transfer Protocol.

SSH: Secure Shell.

TCP: Transmission Control Protocol.

VLAN: Virtual Area Network.

VMware: Virtual Machine.

VPN: Virtual Private Network.

WAN: Wide Area Network.

Table des matières

Liste des figures

Liste des tableaux

Introduction générale

De nos jours, les réseaux informatiques sont devenus indispensables, pratiquement dans tous les domaines de la vie. Les besoins de communication de données informatiques entre systèmes plus ou moins éloignés sont multiples : transmission de données, partage de ressources, transfert de fichiers, consultation de bases de données, gestion de transactions, etc.…

Aux débuts de l'apparition des réseaux, la préoccupation principale était de pouvoir acheminer des paquets d'une source vers une destination indépendamment de leur qualité de réception. Les trafics qui circulaient sur les réseaux n'étaient pas encore autant diversifiés pour rencontrer les problèmes que nous percevons aujourd'hui.

La confidentialité et la vie privée sur Internet sont régulièrement remises en question, car l'échange des données sur Internet est beaucoup plus vulnérable que sur un réseau interne et cela est dû au chemin emprunté, qui n'est pas défini à l'avance. Ce qui l'expose à une multitude de menaces potentielles et non potentielles et comme il peut être aussi écouté par un utilisateur malveillant afin d'exploiter les vulnérabilités du réseau pour essayer d'accéder à des informations sensibles dans le but de les lires, les modifier ou les détruire.

Il est donc indispensable pour les entreprises de se munir des mécanismes, qui garantit une protection d'échange de données entre les entités d'un réseau public et empêcher les utilisateurs non autorisées d'y accéder.

L'objectif de notre projet, est alors de palier aux problèmes cités au part avant par l'implémentation d'une solution de sécurité, garantissant un transfert de donnée sécurisé entre les deux réseaux de l'université Targa Ouzemour et Aboudaou en passant par le réseau public. Cette solution permet également aux enseignants et aux responsables d'accéder d'une manière fiable et sécurisée aux ressources du réseau de l'université à distance de chez eux par exemple et sans être physiquement présent. Cette sécurisation va garantir la confidentialité, l'intégrité et la disponibilité.

Et pour cela, nous avons mené une étude critique de sécurité du réseau, puis nous avons adopté l'approche suivante : l'ajout d'une ligne spécialisée entre les deux réseaux de l'université, la mise en œuvre des VPN site à site entre ces deux réseaux, ainsi que la mise en place d'un VPN accès distant pour permettre un accès distant au réseau.

Le premier chapitre sera subdivisé en deux parties, dont la première est consacrée aux généralités des réseaux informatiques, où nous présentons les concepts fondamentaux d'un réseau :les types d'un réseau, ses topologies, les équipements d'interconnexion les plus utilisées, les deux modèles réseaux, le protocole IP, le système DNS et en fin le protocole DHCP. Puis, dans la deuxième partie nous intéressons à la sécurité informatique, ses objectifs, quelques types d'attaques, des stratégies qui assurent une protection contre ces attaques.

Dans le deuxième chapitre, nous définirons brièvement l'université de Bejaïa, ainsi qu'une présentation de l'infrastructure de son réseau intranet, les faiblesses de ce dernier en terme de sécurité, et enfin la solution proposée pour répondre à ses diagnostiques.

Le troisième chapitre concerne l'étude du moyen que nous avons choisi, afin de répondre aux besoins du réseau (les VPN), ses fonctionnalités, son principe de fonctionnement, ses types les plus fréquents, et enfin les principaux protocoles qu'il mit en œuvre.

Le quatrième chapitre est dédié à la partie pratique, dans laquelle nous allons présenter l'environnement de travail, ainsi que la configuration du pare-feu PfSense et la mise en œuvre des VPN.

Enfin, notre mémoire s'achève avec une conclusion générale, résumant les éléments essentiels qui ont été abordés.

1.1. Introduction

Les réseaux informatiques constituent un ensemble d'équipements reliés entre eux afin de s'échanger tout type d'informations.

L'expansion et l'importance grandissante des réseaux informatiques ont engendré le problème de sécurité des systèmes de communication. Ainsi partager les données directement entre machines est un souci majeur.

Il s'avère indispensable de renforcer les mesures de sécurités, dans le but de maintenir la confidentialité, l'intégrité et le contrôle d'accès au réseau pour réduire les risques d'attaques.

1.2. Généralités sur les réseaux informatiques

1.2.1. Définition d'un réseau informatique

Un réseau informatique est un ensemble de terminaux interconnectés entre eux par des nœuds et des liens de communication, pour échanger des informations numériques et fournir un service d'acheminement des paquets.[1]

1.2.2. Les types des réseaux

En fonction de la taille, du débit des informations, des types de protocoles de communication il existe plusieurs types de réseaux [1]:

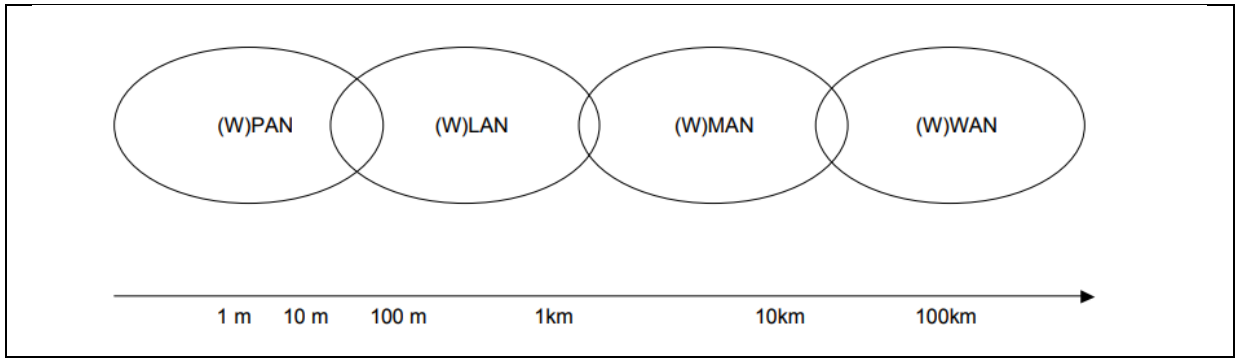

Figure 1.1 : présentation des types des différents réseaux[1]

1.2.2.1. Les réseaux personnels (PAN)

Ils interconnectent sur quelques mètres des équipements personnels d'un même utilisateur, tels que les terminaux GSM, portables...etc.

1.2.2.2.Les réseaux locaux(LAN)

Un réseau local est un ensemble d'ordinateurs séparés au maximum de quelques kilomètres, appartenant à une même organisation. Généralement la technologie Ethernet est utilisée pour relier les postes de travail.

La vitesse de transfert de données d'un réseau local est élevée, elle est au minimum de 10 Mbits/s.

1.2.2.3. Les réseaux étendus(WAN)

Un réseau étendu est un ensemble d'ordinateurs séparés au maximum de quelques centaines de kilomètres, appelés aussi réseaux longue distance.
Les réseaux étendus peuvent être aussi définis comme une interconnexion de plusieurs réseaux locaux.

La vitesse de transfert de données d'un réseau étendu est généralement moins grande que celle d'un réseau local.

1.2.2.4.Les réseaux métropolitains (MAN)

Les réseaux métropolitains s'agissent d'une série de réseaux Locaux, permettant de relier des ordinateurs géographiquement proches (situés dans une même ville).Les équipements d'un réseau métropolitain sont interconnectés par des liens à haut débit(en général en fibre optique).

1.2.3. Les topologies des réseaux

Une topologie de réseau correspond à l'architecture physique ou logique, définissant la façon dont les équipements sont interconnectés (le chemin de câblage) ou bien la façon dont les données transitent dans les lignes de communication (le chemin réel emprunté par les données) Les topologies logiques les plus courantes sont Ethernet, Token Ring et FDDI. [1]

1.2.3.1. La topologie en bus :

La topologie en bus est une organisation très simple d'un réseau, dans laquelle les ordinateurs sont reliés à une même ligne de transmission à l'aide d'un câble (de type coaxial en général).

- **Avantages**

  - facile à mettre en œuvre.
  - fonctionnement très simple.

- **Inconvénients**

  - Elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau en est affecté.
  - A chaque ajout d'un ordinateur au réseau, les performances se dégradent et la possibilité de collisions augmente.

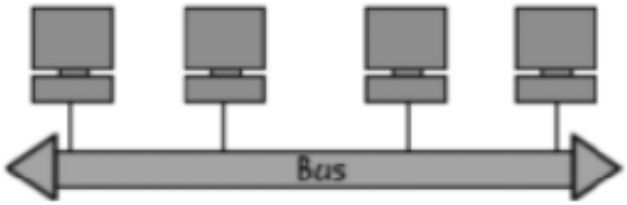

Figure 1.2 : La topologie en bus. [1]

1.2.3.2. La topologie en étoile

La topologie en étoile est une organisation d'un ensemble de stations reliées à un système matériel central (concentrateur, commutateur…) auquel les stations sont reliées par un câble.

Dans cette topologie la communication entre deux points ne peut prendre qu'un seul chemin possible.

- **Avantages**
  - Facilité de câblage.
  - Faible possibilité de vulnérabilité, car un câble défectueux ne déconnecte qu'un seul ordinateur sans paralysé le reste du réseau.
- **Inconvénients**
  - Une panne au niveau de système central provoque la déconnexion de toutes les stations connectées dessus.

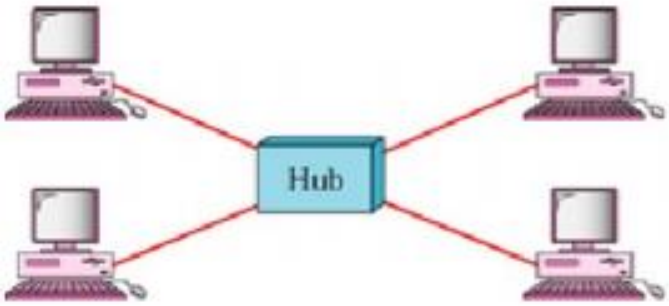

Figure 1.3 : la topologie en étoile. [1]

1.2.3.3. La topologie en anneau

Une topologie en anneau se caractérise par une connexion circulaire de la ligne de communication. Les ordinateurs sont théoriquement situés sur une boucle et communiquent chacun à leur tour à l'aide d'un jeton qui permet à chaque station de prendre la parole.

❖ **Avantages**

- un débit bande passante élevé.
- La gestion des collisions.

❖ **Inconvénients**

- La panne d'une station peut provoquer la panne de tout le réseau.
- La difficulté d'insertion d'une nouvelle station au réseau.

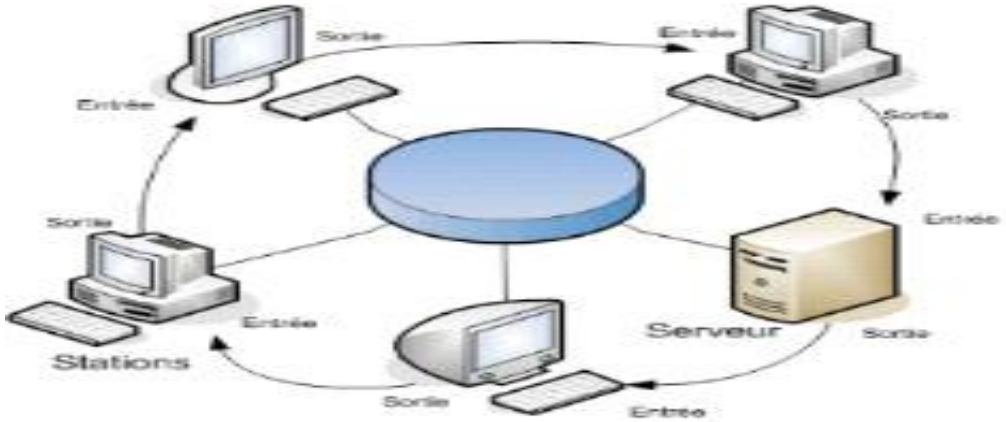

Figure 1.4 : la topologie en anneau.[2]

1.2.4. Les équipements de base d'un réseau informatique

Afin de pouvoir interconnecter les réseaux entre eux, des différents types de matériels sont mis en place:[2]

- **Répéteur :** un répéteur est un dispositif permettant d'interconnecter des réseaux locaux. Il amplifie et répète les signaux qui lui parviennent.
- **Pont (bridge) :** Un pont est un dispositif réservé à la connexion de réseaux utilisant les mêmes trames et les mêmes espaces d'adressage.
- **Concentrateur (hub):** Un concentrateur est un dispositif permettant de connecter divers éléments de réseau.
- **Commutateur(Switch) :** Un commutateur est un dispositif permettant de relier divers éléments tout en segmentant le réseau. contrairement au hub, il n'émet pas les trames sur l'ensemble des ports mais uniquement à la station destinatrice.
- **Routeur (router) :** Un routeur est un dispositif comportant différentes interfaces (ports), permettant de relier des réseaux différents de telle façon à permettre la circulation de données d'un réseau à un autre de façon optimale grâce à une table de routage.
- **Passerelle (Gateway) :** Une passerelle est un dispositif permettant d'interconnecter des architectures de réseaux différents. Elle a pour fonction de convertir les protocoles de haut niveau.

1.2.5.Les modèles de réseaux

Il existe deux types de modèles de réseau de base : le modèle de référence (OSI) et le modèle d'applications (TCP/IP).

1.2.5.1. Le modèle de référence OSI (Open Systems Interconnection)

C'est une norme de description de l'architecture générale des réseaux informatiques.il peut être vu aussi comme un modèle universel, sur lequel s'appuierait les développeurs et les fabricants de matériel réseau.

Il a été mis en place par l'ISO, afin de normaliser les communications échangées dans un réseau.

L'architecture d'un réseau est définie par l'ensemble des couches et la description des protocoles et des services de chacune d'elles. [3] [4]

Le schéma ci-dessous représente la structure en couches d'une manière générale :

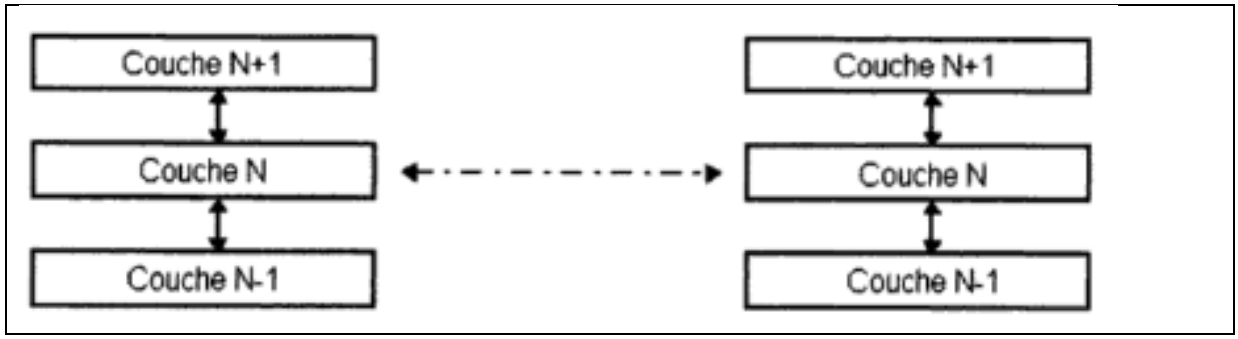

Figure 1.5 : la structure en couches.[3]

1.2.5.1.1. Notion de couche, de protocole et de service

- **Une couche**

C'est un ensemble de fonctions particulières, elle utilise les fonctionnalités de la couche inférieure et propose ses fonctionnalités à la couche supérieure.

- **Un protocole**

C'est un ensemble de règles d'échange réalisant un service.

- **Un service**

C'est une description abstraite de fonctionnalités fournies aux entités de la couche N+1 par la couche N à l'aide d'une interface.

1.2.5.1.2. Les couches du modèle OSI

Le modèle OSI comporte sept couches, chacune assure un ensemble de fonctionnalités prédéfinies à réaliser, selon des règles et des formats des échanges (protocoles) : [3] [4]

- **La couche physique**

C'est la transmission bit à bit des signaux sur un canal de communication entre les interlocuteurs. Cette couche doit garantir la bonne transmission des données en termes de qualité de services.

- **La couche liaison de données**

Elle gère la communication entre deux hôtes reliés par un support physique et définit l'interface avec la carte réseau et le partage du média de transmission.

- **La couche réseau**

Elle gère les communications de proche en proche entre machines: routage et adressage des paquets.

- **La couche transport**

Elle gère le transport des données de bout en bout, et la gestion éventuelle des erreurs de transmission.

- **La couche session**

Elle permet l'ouverture et la fermeture de session et gère la synchronisation des échanges et les transactions.

- **La couche présentation**

Cette couche s'intéresse à la syntaxe et à la sémantique des données transmises, elle traite l'information de manière à la rendre compatible entre tâches communicantes.

- **La couche application**

Cette couche est le point de contact entre l'utilisateur et le réseau, elle offre à l'utilisateur les services de base offerts par le réseau.

La figure suivante illustre les couches du modèle OSI et leurs protocoles.

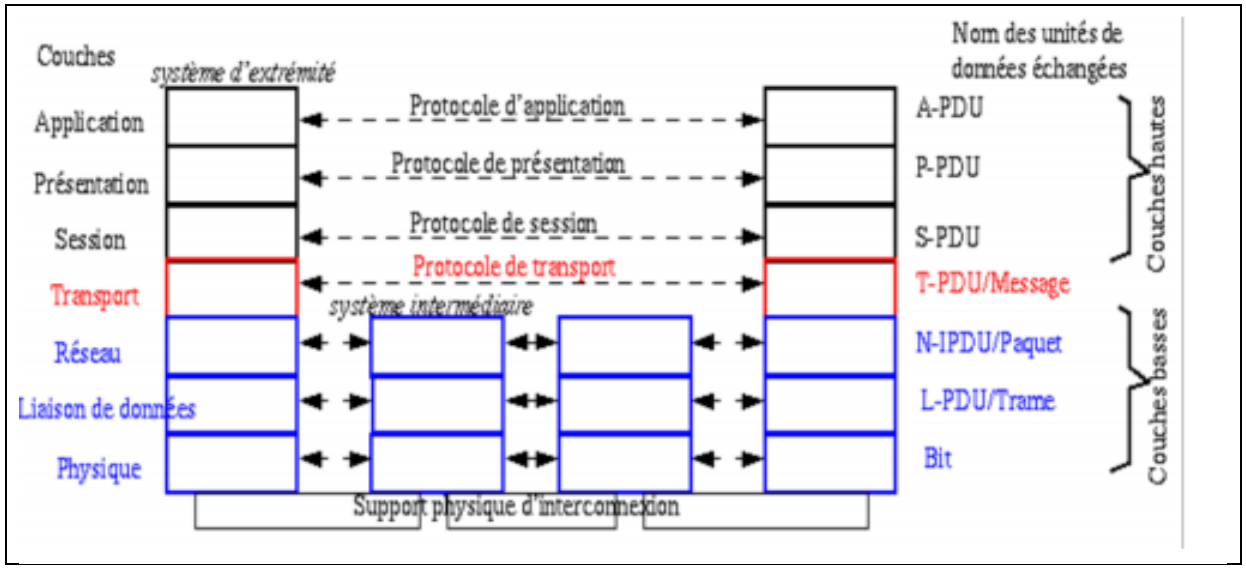

Figure 1.6 : Les couches du modèle OSI et leurs protocoles. [1]

1.2.5.2. Le modèle d'applications TCP/IP

C'est une architecture réseau en quatre couches, Conçue pour modéliser le réseau Internet dans laquelle deux principaux protocoles sont utilisés :[1]

- **IP (**Internet Protocol) de niveau réseau, qui assure un service sans connexion.
- **TCP** (Transmission Control Protocol) de niveau transport, qui assure un service Fiable avec connexion.

1.2.5.2.1. Les couches du modèle TCP/IP

Le modèle TCP/IP comporte quatre couches, chacune assure un ensemble de fonctionnalités comme suit : [1] [3]

- **La couche hôte réseau**

Elle regroupe la couche physique et la couche liaison de données du modèle OSI, son rôle est de permettre à un hôte d'envoyer des paquets IP quel que soit le type du réseau utilisé.

- **La couche internet**

Son rôle est de permettre l'acheminement des paquets de données (datagrammes) indépendamment les uns des autres jusqu'à la destination.

- **La couche Transport**

Son rôle est le même que celui de la couche transport du modèle OSI. Elle assure l'acheminement des données,ainsi que les mécanismes permettant de connaitre l'état de la transmission.

- **La couche application**

Elle englobe les applications standards du réseau.

1.2.6. Le protocole IP

- **Définition**

Le protocole IP assure le service attendu de la couche réseau du modèle TCP/IP, il permet l'élaboration et le transport des paquets des données entre le nœud source et destination et offre un environnement non fiable et sans connexion.
Les données circulent sur internet sous forme de datagrammes (données encapsulées), en passant par chaque nœud du réseau.il faut donc disposer d'un mécanisme permettant d'identifier d'une manière unique chacun de ces nœuds. [1]

- **L'adresse ipv4**

L'identifiant logiciel unique d'un nœud est l'adressage IP. L'adresse IP est codée sur 32 bits, noté sous forme de 4 nombres de 8 bits chacun, compris entre 0 et 255.

A.B.C.D est la forme qui représente l'adresse IP ou A, B, C et D représentent un octet qui s'écrit sur 8 bit et c'est donc un entier compris entre 0 et 255.
Ces adresses doivent être uniques, car elles sont utilisées pour identifier les composants du réseau dans le but de se reconnaitre. [1]

- **Les classes des adresses IP**

Il s'agit d'une division des adresses IP afin de faciliter la recherche de n'importe quel ordinateur dans le réseau, en commençant d'abord par la recherche du réseau auquel il appartient l'ordinateur recherché.

Il existe cinq classes d'adresses IP : classe A, classe B, classe C, classe B, classe E.
Chaque classe est caractérisée d'une manière unique par un format spécial de son adresse IP de la manière suivante : « Adresse réseau, Adresse machine **» [**10]

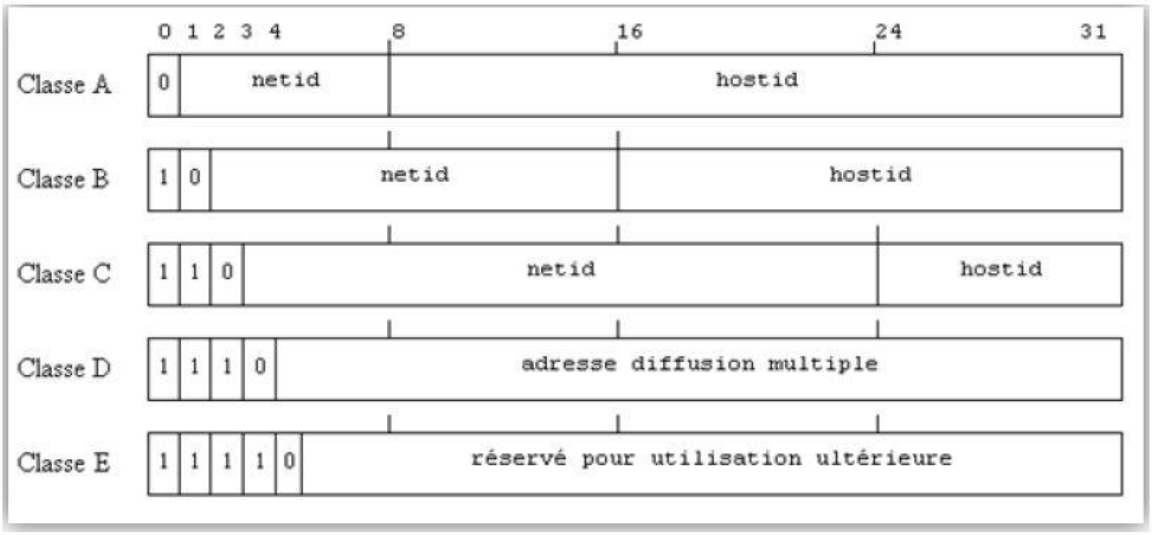

Figure 1.8 Caractéristiques des classes des adresses IP.[9]

1.2.7. Le système DNS (Domain Name System)

Est un service de résolution, permettant d'utiliser des noms symboliques à la place des adresses IP localement ou à l'échelle mondial.

Un nom DNS correspond généralement à une seule adresse IP, alors qu'une adresse IP peut cependant être associée à plusieurs noms DNS.[9]

1.2.8. Le protocole DHCP (Dynamic Host Configuration Protocol)

Le protocole DHCP est un protocole de la couche réseau de type Client/serveur, permet d'affecter automatiquement et à la demande les adresses nécessaires à la communication sur le réseau (adresse IP, masque de sous-réseau, adresse de la passerelle, etc ...).

Le but principal étant la simplification de l'administration d'un réseau, mais aussi il est très pratique dans le cas de réseau où le stock d'adresses IP est limité, alors que de nombreux ordinateurs sont susceptibles de se connecter. [9]

1.3. Sécurité des réseaux informatiques

1.3.1.Définition de la sécurité informatique

Le système d'information est généralement défini par l'ensemble des données et des ressources matérielles et logicielles, propres à l'entreprise permettant de les stocker ou de les faire circuler. La sécurité informatique consiste à assurer que ces ressources sont uniquement utilisées dans le cadre prévu.

En d'autres termes, la notion de sécurité informatique c'est l'ensemble des méthodes et des techniques nécessaires à la mise en œuvre de moyens visant à empêcher l'utilisation non-

autorisée et réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles.[6]

1.3.2. Objectifs de la sécurité des réseaux informatiques

D'une manière générale, la sécurité d'un réseau informatique vise à assurer les objectifs suivants:[6]

- **La confidentialité :** C'est la propriété qui garantit que les informations transmises ne sont compréhensibles que par les entités autorisées.
- **L'authentification :** a pour but de s'assurer que les données reçues proviennent bien de l'entité émettrice (vérification de l'identité d'un utilisateur).
- **L'intégrité :**a pour but de s'assurer que les données reçues sont bien celles que l'on croit être et n'ont pas étaient modifiées ou altérées par des personnes non autorisées lors du transport dans le réseau.
- **La disponibilité :**a pour but de s'assurer que l'information sur le système, soit disponible aux personnes autorisées (garantir l'accès aux données).
- **La non-répudiation :** permettant de garantir qu'une transaction (envoi ou réception d'un message) ne peut être niée.

1.3.3. Quelques types d'attaques

Les attaques réseaux sont aujourd'hui nombreuses, elles permettent à une personne mal intentionnée de s'approprier des ressources, de les bloquer ou de les modifier, en voici quelques-unes: [6] [7]

- **Attaque par déni de service (DoS) :** En général, le déni de service vise l'exploitation des faiblesses de l'architecture d'un réseau ou d'un protocole.
  Le but d'une telle attaque n'est pas de récupérer ou d'altérer des données sur une machine distante, mais de paralyser un service ou un réseau complet et le rendre indisponible pendant une période indéterminée.

- **Ecoute du réseau (sniffer):**grâce à des logiciels qui, à l'image des analyseurs de réseau, il est possible d'écouter le trafic sur un réseau et d'intercepter ou de capturer certaines informations qui transitent sur un réseau local et qui ne nous sont pas destinées.
  C'est l'une des raisons qui font que la topologie en étoile autour d'un hub n'est pas la plus sécurisée, puisque les trames qui sont émises en «broadcast» sur le réseau local peuvent être interceptées. De plus, l'utilisateur n'a aucun moyen de savoir qu'un pirate a mis son réseau en écoute.

- **Intrusion :** en général L'intrusion a pour objectif la réalisation d'une menace. Le principal moyen pour prévenir les intrusions est lefirewall.

- **L'attaque IP spoofing :** Est une technique consistant à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine.
  Cette attaque est difficile à mettre en œuvre et nécessite une bonne connaissance du Protocole TCP.

- **Les programmes cachés ou virus :** les virus existent au début de l'apparition de l'informatique, ils peuvent être définis comme un exécutable qui exécute des opérations plus ou moins destructrices sur votre machine et qui peuvent perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté.
  On classe généralement les virus selon leur mode de propagation et de multiplication.

- **Le craquage de mots de passe :**Cette méthode consiste à essayer plusieurs mots de passe afin de trouver le bon.
  Elle peut s'effectuer à l'aide d'un dictionnaire des mots ou par la méthode de brute force.

1.3.4. Notion de politique de sécurité

Une politique de sécurité définit un certain ensemble de règles et de procédures, permettant d'assurer un niveau de sécurité conforme aux besoins de l'organisation.

Elle est aussi une façon de définir les évènements que l'on veut éviter dans le fonctionnement d'un système.[8]

Sa mise en œuvre se fait selon les quatre étapes suivantes:[11]

- Enumérer les besoins de l'entreprise en termes de sécurité, les risques et leurs conséquences.
- Pour éviter les risques identifiés au-dessus, un ensemble de règles et de procédures sont mis en œuvre.
- La surveillance et la détection des vulnérabilités du système d'information et les failles concernant les applications et les matériaux utilisés.
- Définir les solutions à mettre en place en cas d'une menace signalée.

1.3.5. Stratégies de sécurité

Afin de sécuriser le système d'information, protéger les entrées et sorties sur le réseau et faire face aux attaques citées ci-dessus, citons quelques solutions à ces dernières:[6]

1.3.5.1. La cryptographie

La cryptographie est l'ensemble des techniques et méthodes permettant le chiffrement et le déchiffrement des messages, afin de garantir la sécurité des données circulées sur un réseau non sur (comme internet).elle permet d'assurer l'authenticité, l'intégrité et la confidentialité des données.
Il existe deux types de clés : clé symétrique (privé) et clé asymétrique (publique) comme illustré dans le schéma suivant :

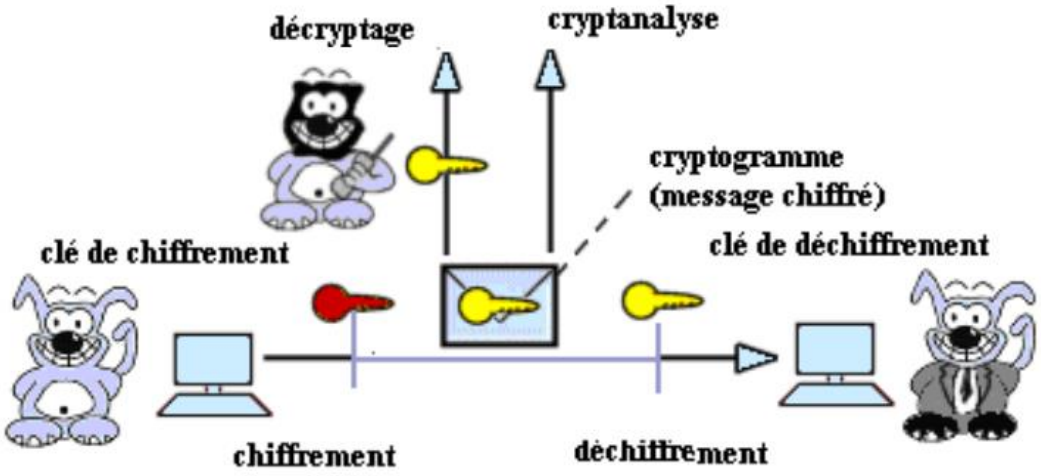

Figure 1.9 : Mécanisme de chiffrement [11]

Actuellement il existe deux grands principes de cryptage :

1.3.5.1.1. La cryptographie symétrique

La cryptographie à clé privée ou symétrique est basée sur une même clé unique, partagée entre les deux interlocuteurs afin de pouvoir crypter et décrypter le message.

Cette technique est très efficace en terme de rapidité d'exécution et assez économe en ressources CPU, par contre elle pose un problème de la distribution des clés dans un réseau étendu.

Les algorithmes de réalisation des opérations de cryptographie sont : DES, triple DES ou le récent AES.

Figure 1.10 : Chiffrement Symétrique. [11]

1.3.5.1.2 La cryptographie asymétrique

Dans ce système de cryptage, chaque utilisateur dispose de deux clés différentes l'une est privée (secrète) n'est connue que par l'utilisateur, et l'autre publique et donc accessible par tout le monde.

Les deux clés sont liées d'une manière mathématique par un algorithme de chiffrement, de telle manière qu'un expéditeur envoie sa clé publique à ses interlocuteurs, qui l'utilisent pour chiffrer les données avant de les lui envoyer.

Cette technique nécessite des clés plus longues pour une meilleure sécurité. Les algorithmes à clé publique les plus fréquemment employés sont les suivants: RSA, DSA, DH.

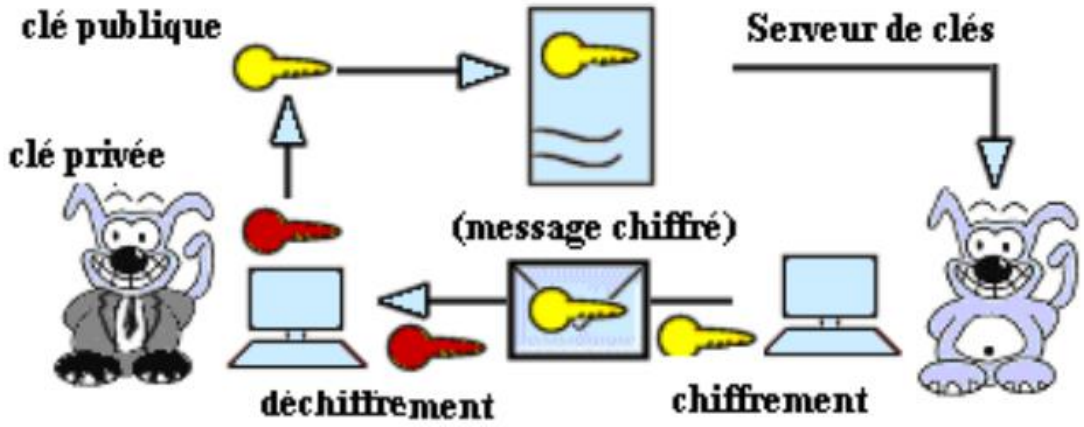

Figure 1.11 : Chiffrement asymétrique.[11]

1.3.5.2 La signature numérique

Ce paradigme assure les trois objectifs de la sécurité suivants: l'authenticité de l'expéditeur, l'intégrité du message reçu ainsi la non-répudiation.

La clé privée est utilisée pour signer électroniquement un message qui sera déchiffré à la réception à l'aide de la clé publique correspondante.

1.3.5.3 L'infrastructure de clés publiques ou PKI :

L'infrastructure PKI repose sur la notion de chiffrement asymétrique. Un certificat est utilisé par le détecteur de clés pour s'authentifier.

Cette infrastructure offre la possibilité aux utilisateurs, d'obtenir les clés publiques nécessaires qui permettent d'effectuer des opérations cryptographiques.

1.3.5.4. Programme antivirus

Les logiciels antivirus sont des programmes informatiques, permettant de détecter et faire face à des programmes malveillants à plusieurs niveaux, tels que des virus et des vers.

La majorité des antivirus sont basés sur l'analyse de signature des fichiers, ou cette dernière doit donc être très régulièrement mise à jour sur le site de l'éditeur.

Il existe deux modes de protection :

- Généralisation de l'antivirus sur toutes les machines, ce qui nécessite une mise à jour régulièrement.
- Mise en place d'un antivirus sur les points d'entrée/sortie de données du réseau.

1.3.5.5 Un pare-feu (firewall)

Un pare-feu est une structure (logicielle et/ou matérielle), située entre le réseau local et le monde extérieur (Internet).Il permet d'appliquer une politique d'accès aux ressourcesafin de sécurisé les données du réseau des intrus.

Le trafic est analysé au niveau des datagrammes IP, un datagramme IP est détruit lorsqu'il n'est pas autorisé (la perte d'information est contrôlée).

Pour une meilleure protection des données une translation d'adresses (publique et privée) pourra être effectuée à l'aide de protocole NAT (Network Address Translation).

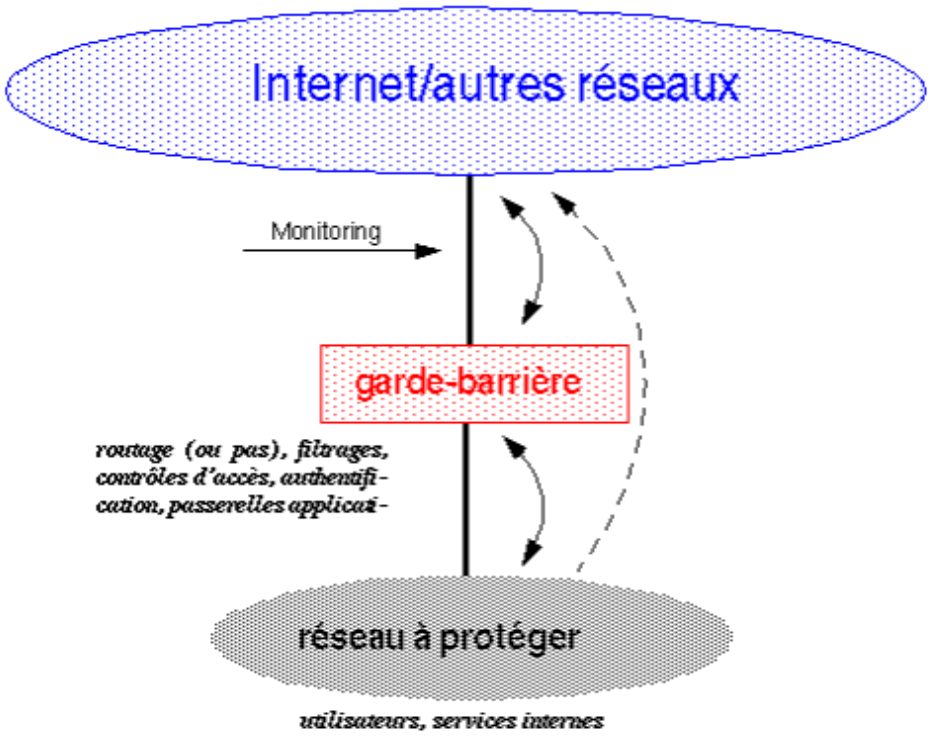

Figure 1.12 :L'architecture classique d'un pare-feu. [11]

- **Les avantages d'un pare-feu :**

- Autoriser l'accès entrants vers le serveur d'identification ou le serveur web institutionnel.

- Empêcher tous les utilisateurs non autorisés d'accéder aux machines et réseaux qui se connectent à Internet.
- Protéger les machines du trafic entrant.
- Offrir un niveau de sécurité d'accès au réseau.

1.3.5.6. Détection d'intrusion (IDS)

Même si l'intrus parvient à franchir les barrières de protection, il est encore possible de l'arrêter avant qu'il n'attaque à l'aide des systèmes de détection d'intrusions (IDS).

IDS est un ensemble de composants logiciels et matériels, qui a pour rôle la surveillance des données qui circulent sur ce système, et donc les outils de détection d'intrusion seront capables de réagir pour tout comportement anormal ou trafic suspect.

Nous pouvons distinguer généralement deux types d'IDS :

- Les N-IDS (Network Based Intrusion Detection System) : ils analysent en permanence le trafic et assurent la sécurité au niveau du réseau.
- Les H-IDS (Host Based Intrusion Detection System) : il analyse l'activité qui se déroule sur la machine et assurent la sécurité au niveau de cette dernière.

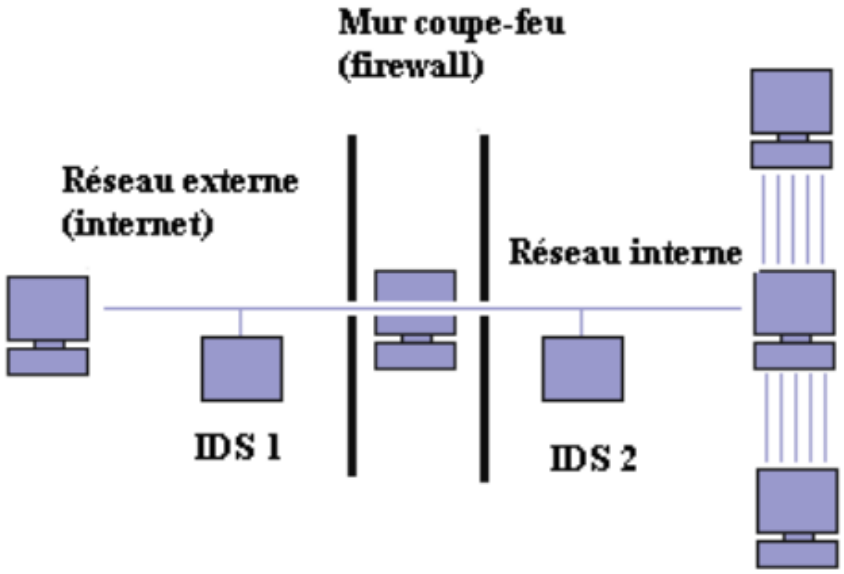

Figure 1.13: IDS (Intrusion Detection System) [11]

1.3.5.7. Zone Démilitarisée(DMZ)

Une zone démilitarisée est une interface de réseau privée, qui se situe au milieu du réseau local et le monde extérieur (internet). Une série de règles de connexion configurées sur le pare-feu font de cette interface une zone physiquement isolée entre les deux réseaux.

La DMZ permet de regrouper des ressources nécessitant un niveau de protection intermédiaire.[9]

1.3.5.8. Le serveur mandataire (Proxys)

Le proxy est un composant logiciel qui joue un rôle complémentaire avec le pare-feu, repose sur un accès à un autre réseau généralement internet.

Le serveur mandataire est particulièrement utilisé dans le cadre de trafics au niveau applicatif (HTTP, FTP, SMTP…) et permet de protéger les accès extérieurs.

Le stockage de pages web dans un cache est dû aux serveurs mandataires configurés pour http à fin d'accélérer le transfert d'informations fréquemment consultées vers des clients connectés.[9]

1.3.5.9. Les VPN (Virtuel Privat Network)

Un VPN (réseau virtuel privé) joue un rôle essentiel dans les architectures modernes de sécurité.

Un VPN peut être défini comme un chemin virtuel ou un tunnel sécurisé entre une source et une destination, dans lequel les données sont cryptées. Il permet aux postes distants faisant partie du réseau local de communiquer avec la source à travers le réseau public et partager des documents de manière complètement sécurisée comme s'ils étaient dans le même espace privé**.**[9]

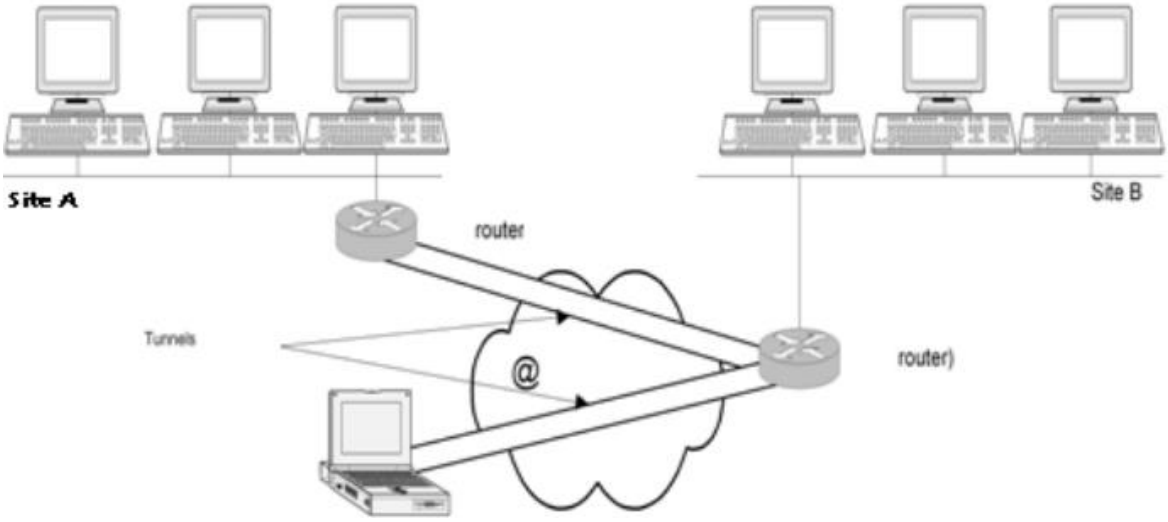

Figure 1.16: VPN (Virtual Private Network).[11]

1.3.5.10. Les VLAN (Virtual Area Network)

Un VLAN est un réseau local qui regroupe un ensemble de machines, de façon logique et non physique.

Un réseau local virtuel a pour objectif l'optimisation de l'utilisation de la bande passante, l'augmentation de la sécurité et la meilleure administration des réseaux.

1.3.5.10.1 Les types de VLAN :

- **VLAN par port (vlan de niveau 1) :**

Une machine appartenant à un vlan est représenté par le port auquel elle est connectée. L'administrateur rempli la table (port/ Vlan) qui se trouve dans le commutateur en précisant les vlan effectuésà chaque port.

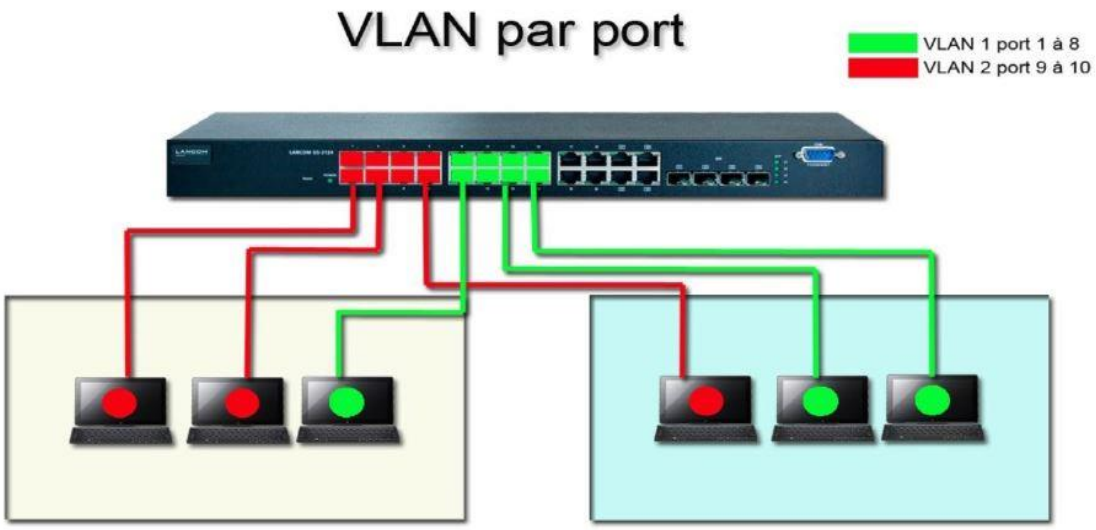

Figure 1.17 : VPN (VLAN par Port)[11]

- **Vlan par adresse mac :**

L'adresse mac d'une machine est affectée à un vlan, en pratique, c'est encore le port qui est affecté à un Vlan d'une façon dynamique. L'administrateur saisit dans la table du commutateur le couple adresse MAC/VLAN. Le commutateur affecte dynamiquement le port au vlan lorsqu'il découvre sur quel port la machine est connectée, Une deuxième table PORT/VLAN est donc gérer.

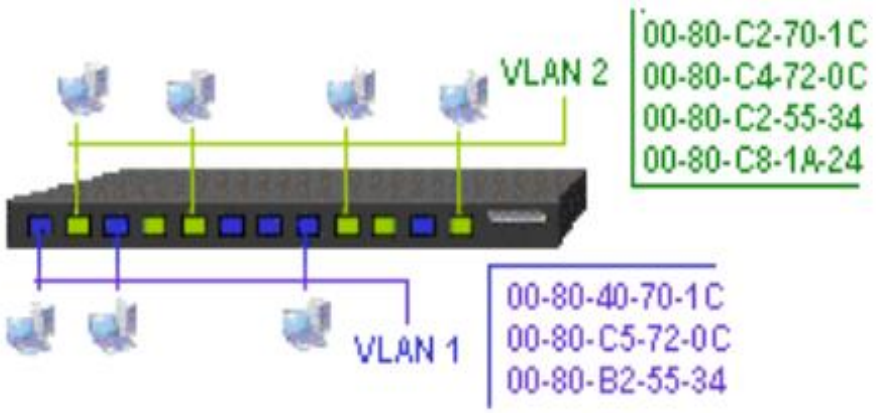

Figure 1.18 : VPN (VLAN par Adresse IEEE).[11]

❖ **VLAN par sous-réseau (VLAN de niveau 3):**

Une adresse IP est affectée à un VLAN et une table adresse/VLAN est remplit par l'administrateur. Lorsque le commutateur identifie le port auquel la station est appartienne, il l'affect a son vlan.

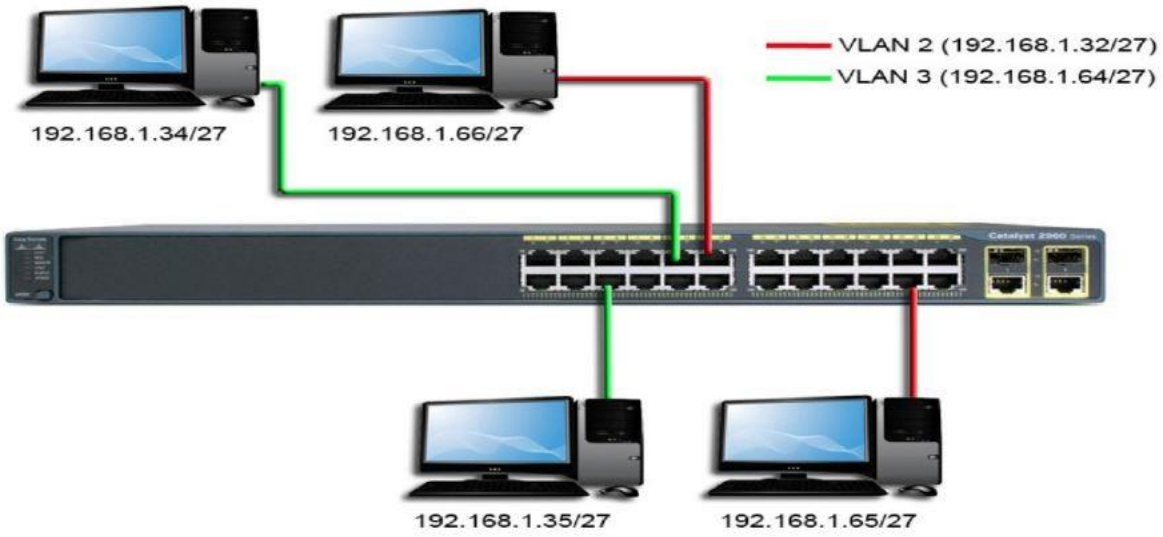

Figure 1.19 : VLAN par sous-réseau (adresse IP).[10]

❖ **Vlan par protocole :**

Le vlan par protocole est la dernière catégorie des vlan dans lequel l'appartenance au vlan dépend du protocole utilisé par la station.

➢ **Avantages des VLAN**

Parmi les avantages liés à la mise en place des VLAN on cite :

- la segmentation du réseau ce qui simplifie la gestion.
- Meilleurs performances, grâce à la réduction de la quantité de trafic sur le réseau.
- La bonne utilisation de *la bande passante*, ce qui réduit les couts.

1.5. CONCLUSION :

Dans ce chapitre, nous avons défini les notions fondamentales et les généralités associées aux réseaux informatiques en présentant la notion d'un réseau, ses types, quelques topologies, les équipements d'interconnexion de base, ainsi que les deux modèles de réseau : le modèle de référence OSI et le modèle d'applications TCP/IP. Nous avons conclu cette partie par les deux services réseaux (DNS et DHCP).

Ensuite, nous avons traité le principe de la sécurité informatique dont les différentes attaques et les stratégies de sécurité à entreprendre pour y remédier.

2.1. Introduction

Ce présent chapitre, sera consacré à une étude sur l'une des solutions adaptée au problème de la confidentialité (les VPN). Dans ce qui suit, nous allons présenter ce qu'est pour nous un VPN. Nous établirons en suite une classification de ces VPN, puis nous présentons rapidement les protocoles les plus utilisés

2.2. Définition d'un VPN (Virtual Private Network)

Un VPN est l'une des solutions adaptée au problème de sécurité des communications entre deux entités à travers un réseau peu sûr comme peut l'être le réseau Internet. Ces communications reposent sur un tunnel sécurisé qui permet la circulation des données de façon cryptée de bout en bout du tunnel. [13]

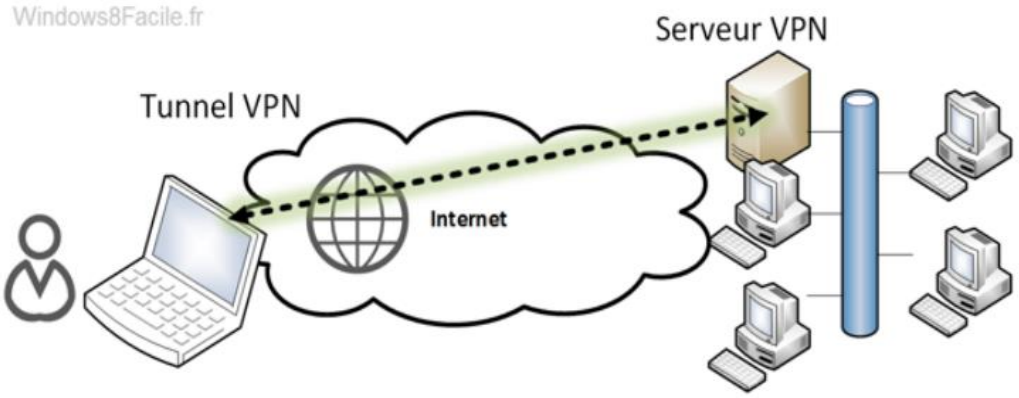

Figure 2.1 : schéma d'un réseau VPN [14]

2.3. Les fonctionnalités d'un VPN

Un réseau privé virtuel a pour but d'assurer un certain nombre de fonctionnalités, qui reposent sur les principes de sécurité les plus importants. [15]

2.3.1. Authentification des utilisateurs

Qui a pour but d'assurer que tous les utilisateurs qui accèdent au réseau virtuel sont autorisés.

Toutes les connexions et les interactions déjà effectuées sur le réseau sont sauvegardées dans un historique.

2.3.2. Gestion d'adresses

Son principe repose sur la gestion de distribution d'adresses privées aux utilisateurs, où chaque client qui se connecte au réseau doit avoir facilement une adresse privée unique qui doit rester confidentielle.

2.3.3. Cryptage des données

Pour une meilleure sécurité des données qui transitent sur le réseau public, un chiffrement est nécessaire.

Il existe plusieurs méthodes de chiffrement des données transportées dans le but d'empêcher leur divulgation et d'assurer les objectifs de sécurité.

Le principe du chiffrement repose sur le chiffrement de l'information à l'émission et son déchiffrement à la réception.

2.3.4. Gestion de clés

Le chiffrement des données est réalisé au moyen d'une clé de chiffrement et de déchiffrement qui doit être générée et régénérée.

Il existe deux types de chiffrement : le chiffrement à clé privée (symétrique) et le chiffrement à clé publique (asymétrique). Le choix d'un chiffrement doit répondre aux besoins appropriés donc à l'algorithme de chiffrement.

2.3.5. Prise en charge multi-protocole

Plusieurs protocoles sont souvent utilisés dans les réseaux publics (en particulier le protocole IP) pour un transfert de données efficace. Ces protocoles doivent être supportés par la solution VPN.

2.3.6. Intégrité des données

Elle a pour but d'assurer que les données n'ont pas été altérées ou modifiées lors de leurs parcours entre la source et la destination.

En général des fonctions de hachages qui ressemblent à une somme de contrôle sont utilisées par les réseaux privés virtuels, pour garantir la confidentialité du contenu.

Cette fonction est appliquée à la donnée pour obtenir un condensa (haché) qui sera envoyé au destinataire.

2.4. Principe de fonctionnement d'un VPN

Un réseau VPN repose sur un protocole appelé "protocole de tunneling", qui consiste à créer un tunnel qui se représente sous la forme d'un chemin virtuel.

L'établissement d'une communication nécessite une identification des deux entités communicantes d'une manière unique. Ensuite les données sont chiffrées par l'émetteur et acheminées jusqu'au destinataire en empruntant ce chemin virtuel.

Le tunneling en d'autres termes est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation, où les paquets IP avec des adresses internes sont confiés à un équipement tel qu'un routeur ou un pare-feu. Celui- ci les envoie sur un canal public (généralement internet) à l'extrémité distante.

Pour cela les paquets internes sont encapsulés dans les paquets IP, avec les adresses IP publiques des extrémités sources et destinataires. À l'arrivée chaque paquet est désencapsulé par la station distante. [13]

2.5. Les Différents types des VPN

On peut distinguer trois grandes catégories de VPN: les VPN site à site, site à poste et poste à poste où chacune d'entre elles présente ses avantages et ses inconvenants. [13] [14]

2.5.1. VPN site à site (LAN to LAN)

Ce type de VPN est généralement utile au sein d'une entreprise possédant plusieurs sites distants, qui a pour but de relier deux sites (deux intranets) ou bien le site de l'entreprise et celui d'un client d'une façon transparente afin d'établir une liaison sécurisée.

La communication à distance entre les machines est réalisée en utilisant les adresses privées de chaque réseau.

Le plus important dans ce type de réseau est de garantir la sécurité et l'intégrité des données, c'est pour cela que les données sont chiffrées dans chaque communication. Par conséquent, le chiffrement, l'authentification et l'acheminement des paquets sont mis en place par l'interconnexion de deux éléments matériels (routeurs ou pare-feu) situés entre le réseau interne et le réseau public de chaque site.

❖ **Avantages**

- Des processeurs spécialisés prennent en charge le chiffrement afin d'améliorer les performances.
- Les équipements situés aux limites prennent en charge les VPN. Ce qui engendre la transparence des données qui circulent dans les tunnels.
- Facilité de contrôle du trafic autorisé.

❖ **Inconvénients :**

- Le tunnel est établi uniquement entre les deux firewalls. Par conséquent, les informations transportées entre les postes et les firewalls ne sont pas sécurisées.
- La nécessité d'identification des deux entités communicantes par une adresse IP publique fixe ou par un nom référencier dans des DNS officiels.
- Pour des raisons de sécurités ainsi que la gestion de la bande passante, le trafic entre les deux sites est limité.

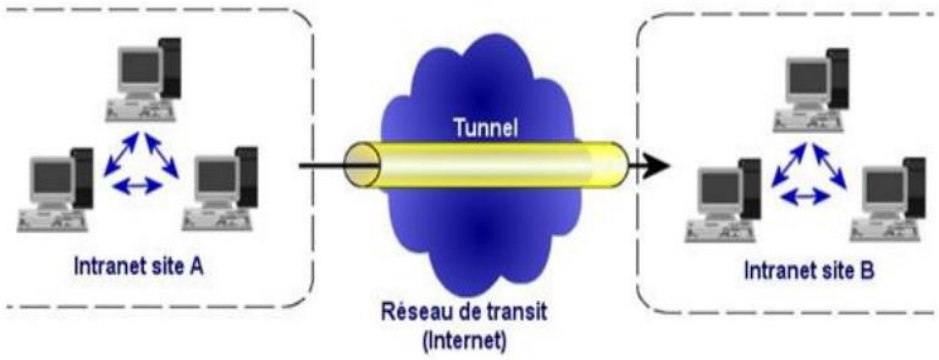

Figure 2.2 : Architecture d'un VPN Site à Site. [14]

2.5.2. VPN poste à site (Host to Lan):

Ce type de VPN est utilisé pour permettre à des utilisateurs d'accéder à distance aux ressources du réseau privé, en assurant la sécurité des données transportées.

Pour l'implémentation de cette solution, un logiciel qui gère le type de protocole choisi est nécessaire du côté des terminaux distants et du coté des équipements installés (parfeu, routeur…) au bout du site central.

- **Avantages :**
  - Le poste nomade peut accéder à n'importe quel point doté d'un accès internet.
  - Le transport des données entre le poste distant et le site central est sécurisé grâce à l'authentification.
- **Inconvénients :**
  - Chaque poste distant doit être doté d'un logiciel installé.
  - Le chiffrement n'est pas assuré au-delà du parefeu du site central.
  - La fiabilité est moindre à cause de la charge du poste distant imposé par le chiffrement

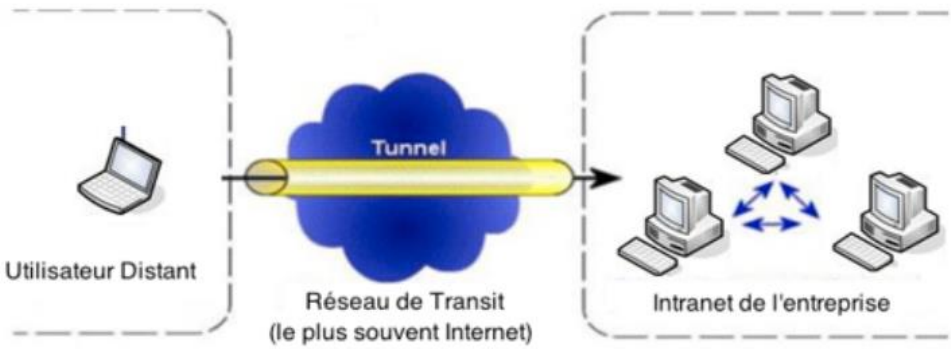

Figure 2.3 : Architecture d'un VPN poste à site. [14]

2.3.5.3. VPN Poste à Poste (Host to Host):

Ce type de VPN est utilisé pour assurer un transport de données sécurisé entre deux postes ou plus, généralement entre un poste et un serveur, sur le même réseau ou sur deux réseaux distants qui se basent à leur tour sur un VPN site à site.

Dans ce cas, un composant physique n'est pas nécessaire mais un logiciel client sur le poste "émetteur" et un logiciel serveur sur le poste "destinataire" sont obligatoires**.**

❖ **Avantages**

- adapté aux communications sensibles, dans lesquelles les données échangées sont parfaitement sécurisées.

❖ **Inconvénients**

- faibles performances dans le cas d'un débit très fort, car le chiffrement est uniquement au niveau logiciel.
- cette solution est inadaptée aux matériels peu intelligents.

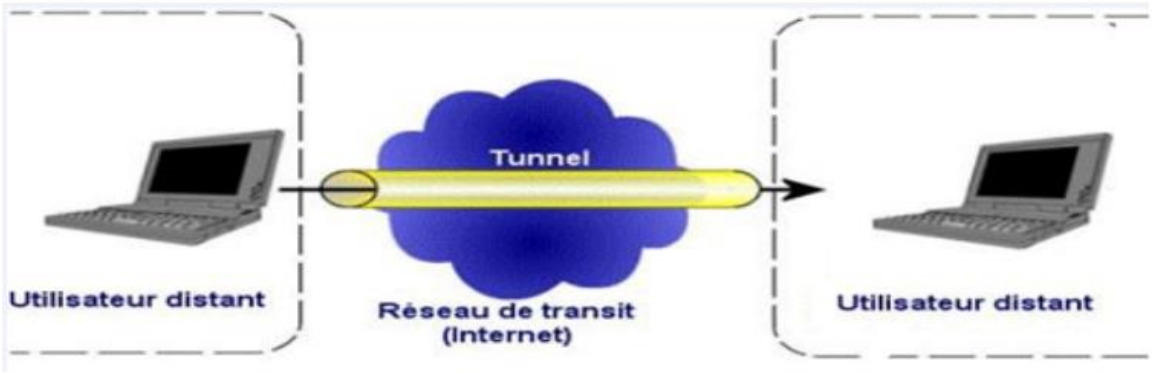

Figure 2.4 : Architecture d'un VPN poste à poste. [14]

2.6. Principaux protocoles de VPN

Voici les protocoles les plus utilisés dans le cadre de tous les types des VPN, qui seront mis en œuvre dans ce qui suit.

La classification de ces protocoles est basée sur leur appartenance aux couches OSI, mais ce classement peut se révéler arbitraire pour certains d'entre eux qui recouvrent en fait plusieurs niveaux.[13]

2.6.1 Niveau 2 :

À ce niveau (niveau 2 du modèle OSI), pour une communication point à points les VPN encapsulent les données dans des trames en ajoutant des en-têtes. Par la suite ces trames seront véhiculées à travers le tunnel. [13]

2.6.1.1 PPP (Point to Point Protocol)

Est un protocole Point à Point comme son nom l'indique. Il est généralement employé entre un client d'accès à distance et un serveur d'accès réseau.

Ce protocole propose une méthode standard pour le transport de données sur une liaison simple synchrone ou asynchrone.

La transmission peut être effectuée dans les deux sens, en mode full duplex avec garantie de l'ordre d'arrivée des paquets.

PPP est le fondement des deux protocoles PPTP et L2TP qui sont utilisés dans les connexions VPN sécurisées.

Le protocole PPP transmit les paquets IP encapsulé dans des trames PPP à travers la liaison point à point. Il est également un protocole de contrôle du lien "Link Control Protocol" destiné à établir, configurer et tester la liaison de données.[16]

Le format d'une trame PPP est décrit ci-dessous :

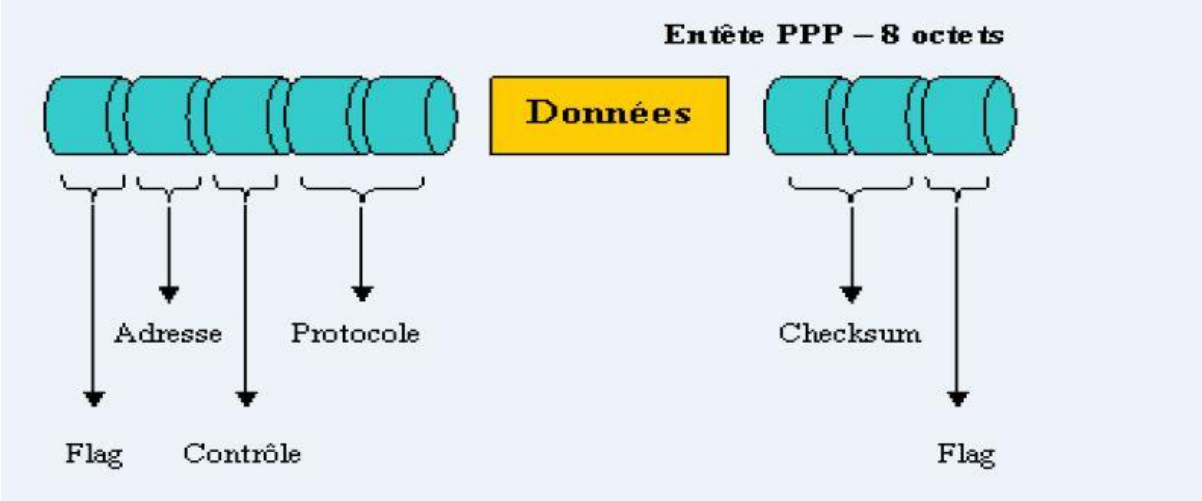

Figure 2.5 : Format d'une trame PPP. [21]

Voici une brève description de chaque champ de la trame PPP : [21]

- **Flag (Fanion) :** il se situe à chaque fois, entre deux trames et il est utilisé dans le but de les séparer. Sa valeur est égale à « 01111110 ».

On trouve un seul drapeau entre chaque deux trames différentes, afin de distinguer chacune d'elles.

- **Adresse :** dans ce cas les stations ne peuvent pas avoir un adressage individuel, par conséquent la valeur de ce champ est à « 0xFF » pour toutes les stations.

- **Contrôle :** ce champ doit avoir la valeur « 0x03 » pour chaque station.

- **Protocole :** il est sur 16 bits, sa valeur doit obligatoirement être impaire (L'octet de poids fort étant pair) et elle est définie dans La RFC « assign number ».

- **Données :** Il est sur une longueur de 0 à 1500 octets, cette dernière est obtenue par le drapeau de fin de trame moins deux octets de contrôle.

Ce champ contient le datagramme du protocole supérieur indiqué dans le champ précédent "protocole".

- **FCS (Frame Check Sequence) :** Dit aussi Checksum, il contient la valeur de la somme de contrôle de la trame.

Lors de la réception d'un paquet, le contenu du FCS est vérifié par PPP. Ce qui est conformes à X25.

2.6.1.2 PPTP (Point to Point tunneling Protocol)

Le protocole PPTP a été développé par un consortium créé par Microsoft, il est très simple à installer et à configurer sur votre ordinateur portable et appareil mobile mais assez limité.

Le protocole PPTP assure une communication sécurisée entre un client distant et un serveur privé basée soit sur un VPN sur demande à travers des réseaux qui reposent sur TCP/IP ou bien entre deux ordinateurs dans le même réseau local.

Dans le but de réaliser un transfert de données sécurisé sur internet ou un autre réseau public basé sur IP, les paquets PPP sont encapsulés dans des datagrammes.
Une trame PPP (un datagramme IP ou IPX ou Appletalk) est encapsulée dans un en-tête GRE (Generic Routing Encapsulation) puis en un en-tête IP.

Les adresses IP source et de destination qui correspondent respectivement au client et au serveur se trouvent dans l'en-tête IP. [17]

Le format d'une trame PPTP est décrit ci-dessous :

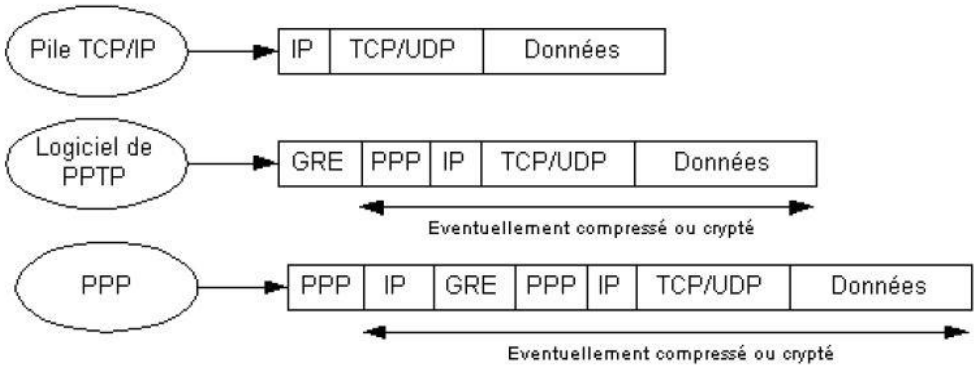

Figure 2.6: Format d'une trame PPTP. [18]

2.6.1.3 L2F (Layer 2 Forwarding)

Est un protocole de tunneling de niveau 2 développé par Cisco, Northern Telecom et Shiva, son fonctionnement est assez voisin de PPTP.

Le protocole L2F permet à un serveur d'accès distant la transmission du trafic sur PPP et le transfert des données jusqu'à un serveur L2F qui seront dés-encapsulées et envoyées sur le réseau. [18]

2.6.1.4 L2TP (Layer Two Tunneling Protocol)

Il s'agit d'un protocole de tunneling appartient au niveau 2 du modèle OSI, dérivé des deux protocoles PPTP et L2F dans le but de converger leurs fonctionnalités en s'appuyant sur PPP. Il permet l'accès à un réseau privé par l'intermédiaire d'un réseau public (généralement Internet) au moyen d'une connexion à un VPN.

Ce protocole est implémenté sur la majorité des machines Windows, ce qui explique son succès. [19]

2.6.2 Niveau 2.5

2.6.2.1 MPLS (MultiProtocol Label Switching)

Il s'agit d'un protocole qui se situe entre la couche liaison de données et la couche réseau. C'est pour cela qu'on lui affecte un niveau dit « hybride 2.5 ».
Son inconvénient est de ne pas mettre en place certaines fonctions de sécurité telle que le cryptage. [13]

2.6.3 Niveau 3 et plus

Il s'agit de tous les protocoles appartenant au moins à la couche réseau du modèle OSI. Ils se caractérisent par la simplicité et la souplesse, Ce qui explique leurs succès croissant.

2.6.3.1 SSL /TLS (Secure Sockets Layer)

Il s'agit des protocoles qui offrent une très bonne solution de tunnelisation, grâce à ses principales caractéristiques dont la simplicité de sa mise en œuvre et sa facilité de franchissement des firewalls.

L'avantage de cette solution est la nécessité d'un seul navigateur WEB comme client VPN. En effet, il permet aux utilisateurs de mettre en place une connexion sécurisée au réseau depuis n'importe quel navigateur Web.

De nos jours, ils sont implémentés dans d'autres logiciels tels que client de messagerie, client FTP …). [21] [13]

Les différentes phases de fonctionnement du protocole sont :

- La Segmentation des paquets en paquets de taille fixe.
- La Compression des paquets.
- L'ajout du résultat de la fonction de hachage.
- Le chiffrement des paquets et du résultat du hachage en utilisant la clé symétrique.

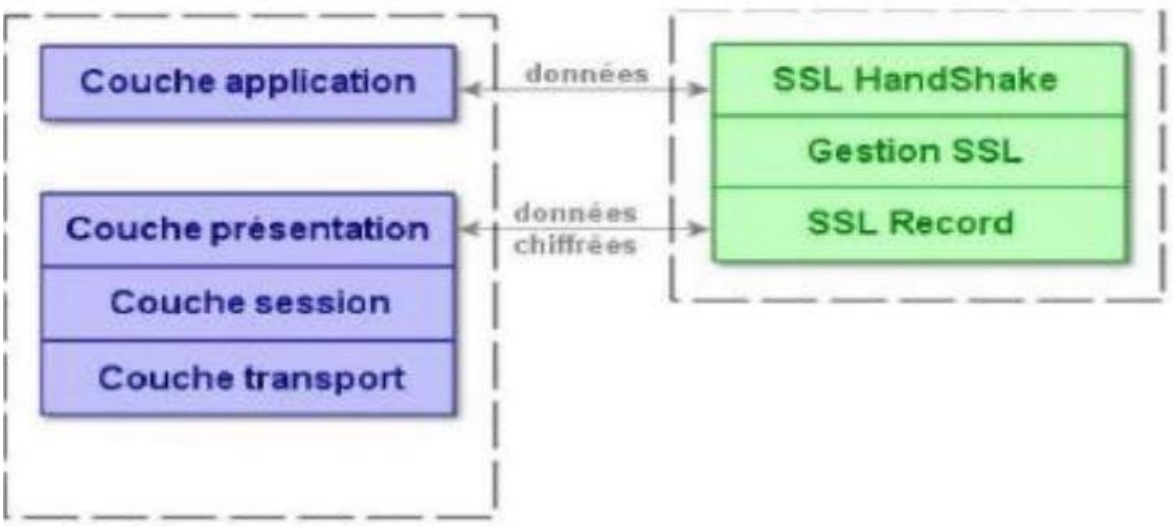

Figure 2.7: Ajout d'un en-tête SSL au paquet. [21]

❖ **Objectifs sécuritaires du protocole :**

Ce protocole assure trois objectifs de sécurité : La confidentialité, l'intégrité et l'authentification. Ci-après une explication de ces trois termes :

- **La confidentialité :** a pour but d'assurer que les données ne sont accessibles que par les personnes autorisées à avoir accès à ces données.
- **l'intégrité :** a pour but d'assurer que les données n'ont pas été altérées ou modifiées.
- **l'authentification :** a pour but d'assurer qu'une personne dit la vérité sur un ou plusieurs de ses attributs.

2.6.3.2 SSH (Secure Shell):

Sa fonctionnalité principale est d'une part d'assurer la protection et la sécurité des communications, de type console et Telnet et d'une autre part les transferts de données.

Il reste un protocole à considérer pour certaines tâches malgré ces limites face au succès grandissant de SSL/TLS ainsi que le champ d'application restreint. [13]

2.6.3.3 IP SEC (Internet Protocol Security)

Il s'agit d'un protocole de niveau 3 du modèle OSI. Sa fonction est d'assurer la sécurité de ce dernier, en se basant sur ces trois critères :

- La confidentialité en utilisant le chiffrement.
- L'authentification qui confirme l'identité de l'émetteur.
- L'intégrité des données qui assure la confidentialité et la protection des informations.

L'utilisation d'IPsec est valable grâce aux différents équipements, particulièrement les routeurs et les pare-feu, ainsi que les systèmes d'exploitation pour les micro-ordinateurs ou ordi phones (téléphone intelligent).
La protection des données échangées se fait par encapsulation du trafic des couches applicatives (l'ajout d'un en-tête IPSec à chaque datagramme IP). [13]

2.6.3.3.1 Les Services fournis par IPsec :

Les services de sécurité fournis par IPsec reposent sur deux protocoles différents qui constituent le cœur de la technologie IPsec : **[**13**]**

- ✓ **Le protocole AH (Authentification Header)**

Comme son nom l'indique, ce protocole se préoccupe en premier point par l'authentification, en deuxième point il assure l'intégrité des données ainsi que le service anti-rejeu. Par contre, il n'est pas prévu à l'origine pour assurer la confidentialité des flux.

Ce protocole se base sur des protocoles de Hachage tel que MD5 et SHA, qui se chargent de la création des mécanismes de signature numériques pour pouvoir authentifier et valider chaque paquet.

- ❖ **Principe de hachage**

Il s'agit de générer à partir d'une chaine de caractère de longueur variable une chaine de longueur fixe qui a généralement une longueur comprise entre 128 et 512 bits.

Un système de hachage est dit performant si :

- Le résultat de hachage ne pourra pas être obtenu à partir de deux messages différents.
- Il est également impossible de trouver le message d'origine à partir du résultat de hachage.

- ✓ **Le protocole ESP (Encapsulation Security Payload)**

Le protocole ESP garantit les trois objectifs de sécurité suivants : La confidentialité, l'intégrité et l'authentification des données échangées, ainsi qu'une protection contre le rejeu.
Les fonctions d'intégrité et d'authentification peuvent être utilisées sans chiffrement (ce qui peut satisfaire la plupart des cas d'usage d'AH).

2.6.3.4 OpenVPN

Comme son nom l'indique, OpenVPN est un protocole VPN Open source qui peut être utilisé pour relier de manière sécurisée deux réseaux privés ou plus et cela en utilisant Secure Socket Layer (SSL,) pour créer une authentification pour une connexion Internet cryptée.

VPN open source est le seul à supporter entièrement tandis que le protocole OpenSSL pour la session d'authentification, le protocole TLS pour l'échange de clef, l'interface EVP

(indépendante du chiffrement utilisé) fournie par OpenSSL pour chiffrer les données encapsulées, l'algorithme HMAC pour authentifier les données encapsulées, et pour multiplexer tout ceci au travers d'un unique port UDP. Le soft OpenVPN n'est pas compatible avec IPsec ou autres logiciels VPN. Celui-ci contient un exécutable pour les connexions du client et du serveur, un fichier de configuration optionnel et une ou plusieurs clés suivant la méthode d'authentification choisie. (VPN, SSL).

Le protocole OpenVPN offre une des meilleures combinaisons de performance et de sécurité

- **Avantages :**

✓ Il nécessite une configuration totale.
✓ Il assure un haut niveau de sécurité.
✓ Il permet de contourner les pare-feu.
✓ Il peut utiliser un large choix d'algorithmes de chiffrement.
✓ multi-plates-formes c'est-à-dire compatible avec Windows, Linux, Mac OS X, ect....

- **Inconvénients :**

✓ Son installation nécessite un logiciel tiers.
✓ Sa mise en palace est assez compliquée.
✓ Il est supporté par certains appareils mobiles, mais n'est pas aussi puissant que sa version fixe.[20]

2.7. Conclusion :

Tout au long de ce chapitre, nous avons effectué une présentation assez détaillé de la solution proposée, qui s'agit des réseaux privés virtuels (VPN), ensuite nous avons parlé des protocoles utilisés pour la réalisation de ce dernier.
Le chapitre suivant, quant à lui, sera consacré a la mise en ouvre de la solution proposer.

Chapitre 3: Etude de l'existant

3.1. Introduction

Dans ce chapitre, nous commencerons par une présentation globale de l'université de Bejaia, ainsi que la structure de son réseau intranet et la façon dont cette dernière est construite.

En fin nous exposerons les besoins et les points faibles du réseau suivis d'une solution proposée afin d'améliorer sa sécurité.

3.2. Présentation de l'université de Bejaïa

L'université de Bejaïa est un établissement public composée de 8 facultés, réparties sur deux campus Aboudaou et Targa Ouzemmou. Dans ce dernier où nous faisons notre mémoire existent trois facultés : Technologie, Sciences Exactes, Sciences de la Nature et des laboratoires de Recherche travaillant sur plusieurs domaines. Elle a réussi à mettre sur pied des formations en phase avec le monde du travail. Ce qui lui a permis d'être mieux à l'écoute des besoins de ses partenaires économiques, en matière de ressources humaines et de compétences.

L'université de Bejaïa vise à construire des passerelles d'échanges d'expériences et de compétences, mais aussi l'amélioration des méthodes pédagogiques. Elle a participé à plusieurs programmes d'échanges universitaires.

3.3. Présentation globale du réseau Intranet

Une meilleure compréhension de l'environnement informatique aide à déterminer la portée du projet, la solution à implémenter et permet d'apporter des améliorations au réseau. Il est indispensable de disposer d'informations sur l'architecture du réseau et les problèmes existants. En effet ces informations vont nous orienter vers un meilleur choix de la solution et de son déploiement.

Le réseau informatique de l'université de Bejaia est organisé selon une topologie physique qui est l'étoile étendue. Ce dernier est constitué de six zones distribuées géographiquement sur deux campus. Chaque zone distribue plusieurs blocs et chaque bloc connecte ses utilisateurs. Toute cette structuration à partir de chaque zone est sous forme arborescente.

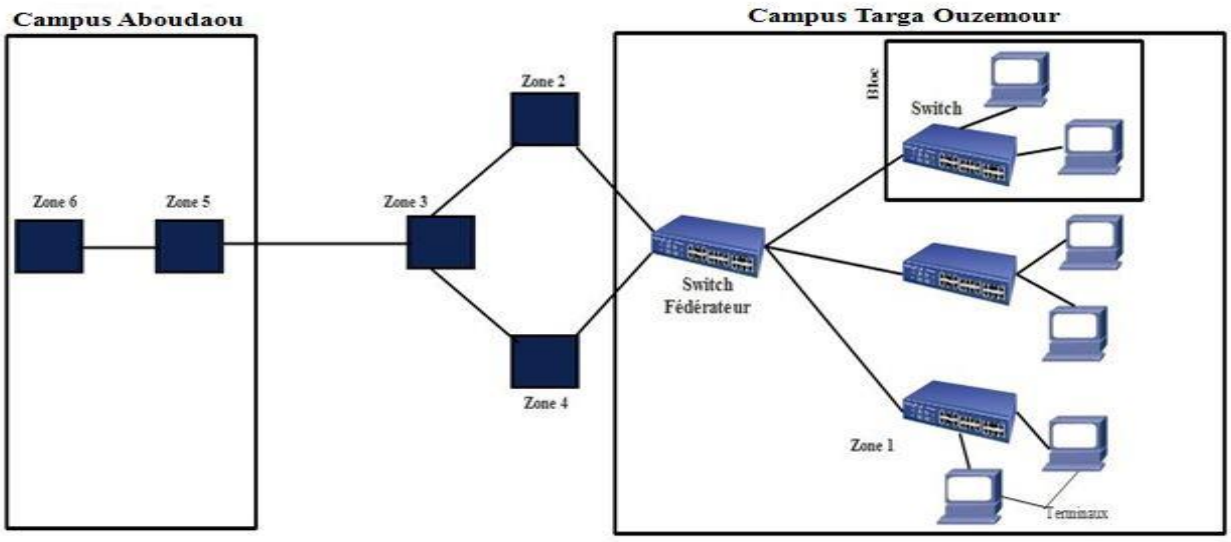

Figure 3.1: La topologie physique du réseau local de l'université de Bejaia.

Le centre de calcul est la racine du réseau local de l'université, par le fait d'héberger la source du réseau interne et tous les services dans une zone démilitarisée, sécurisée par un firewall très puissant sous le regard des techniciens qui pilote l'administration et la sécurité du réseau.

Parmi les six zones du réseau, La zone 1 est la zone principale, donc l'épine dorsale du réseau. Pour cela, le centre de calcul est dirigéà partir de cette dernière.

L'interconnexion entre les deux campus est réalisée au moyen de la fibre optique, en passant par le centre d'amplification d'Algérie Telecom de Béjaia.

Le regroupement des blocs se fait sur la base de la proximité géographique, en d'autres termes les blocs proches les uns des autres en termes physique sont regroupés dans la même zone de la manière suivante :

- **Zone 1 :**

1. Centre de calcul.
2. Bloc 01 (Enseignement-administration)
3. Bloc 11 chimie industrielle.
4. Bloc 5.
5. Faculté de technologie.

- **Zone 2 :**

6. Génie des procédés.

7. Nouvelle bibliothèque (informatique).

8. Nouvelle bibliothèque 250 place.

9. Bloc des enseignants.

10. l'auditorium.

- **Zone 3 :**

11. Bloc d'hydraulique

12. Faculté des sciences exactes.

13. Hall de technologie.

14. Centre culturel et CNAS.

15. Labo de recherche.

16. Moyen généraux.

17. Rectorat.

18. Bibliothèque centrale.

- **Zone 4 :**

19. Bloc 10 Labo électronique.

20. Bloc 12.

21. Bloc 9.

22. Département de biologie.

23. Faculté des sciences naturelle et vie.

24. Haut tension.

- **Zone 5 :**

25. Bloc 02.

26. Bloc 03.

27. Bloc 07.

28. Bibliothèque central.

- **Zone 06 :**

29. Bibliothèque 750.

30. Bibliothèque 250.

31. Bloc enseignement 01.

32. Bloc enseignement 02.

L'organisation des zones en blocs est illustrée par le schéma suivant :

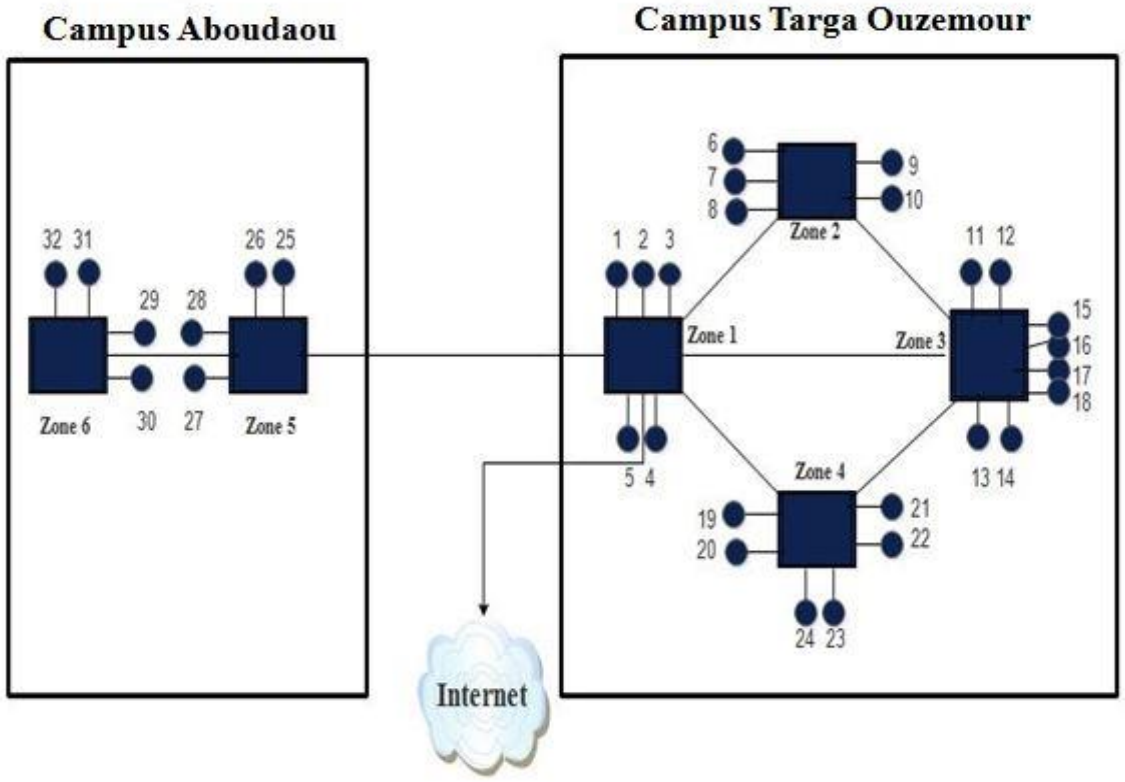

Figure 3.2 : Description des zones constituant le réseau Intranet de l'université.

3.3.1. Description D'une zone

Pour des raisons d'administration, le réseau de l'université est décomposé en zones, où chaque zone se base sur un modèle en couches, qui a été choisi en fonctions de certaines de ces caractéristiques :

- **La hiérarchisation :** qui a pour avantage la spécification de fonctionnalités de chaque couche d'une manière unique.

- **L'évolution :** la répartition de chaque zone en plusieurs blocs facilite la gestion et la planification du l'évolution.
- **La gestion :** c'est plus facile de gérer un bloc contenant moins de postes (la gestion des pannes…).

Le tableau ci-après décrit la structure en couches:

Equipement	**Description**
Les Terminaux	Les stations terminales ou les imprimantes réseau.
Switch (La couche d'accès)	c'est le point qui permet à n'importe quel équipement terminal du réseau, d'avoir accès à ce dernier, et à ce niveau que tous les services de niveau 2 sont définis, tel que l'appartenance à un Vlan.
Switch fédérateur (La couche de distribution)	C'est le point d'entrée /sortie vers l'extérieur car c'est à ce niveau que le routage et le filtrage sont accomplis.

Tableau 3.1 : la description de la structure en couches.

La structure en couche de la zone 2 du réseau est illustrée par le schéma ci-dessous :

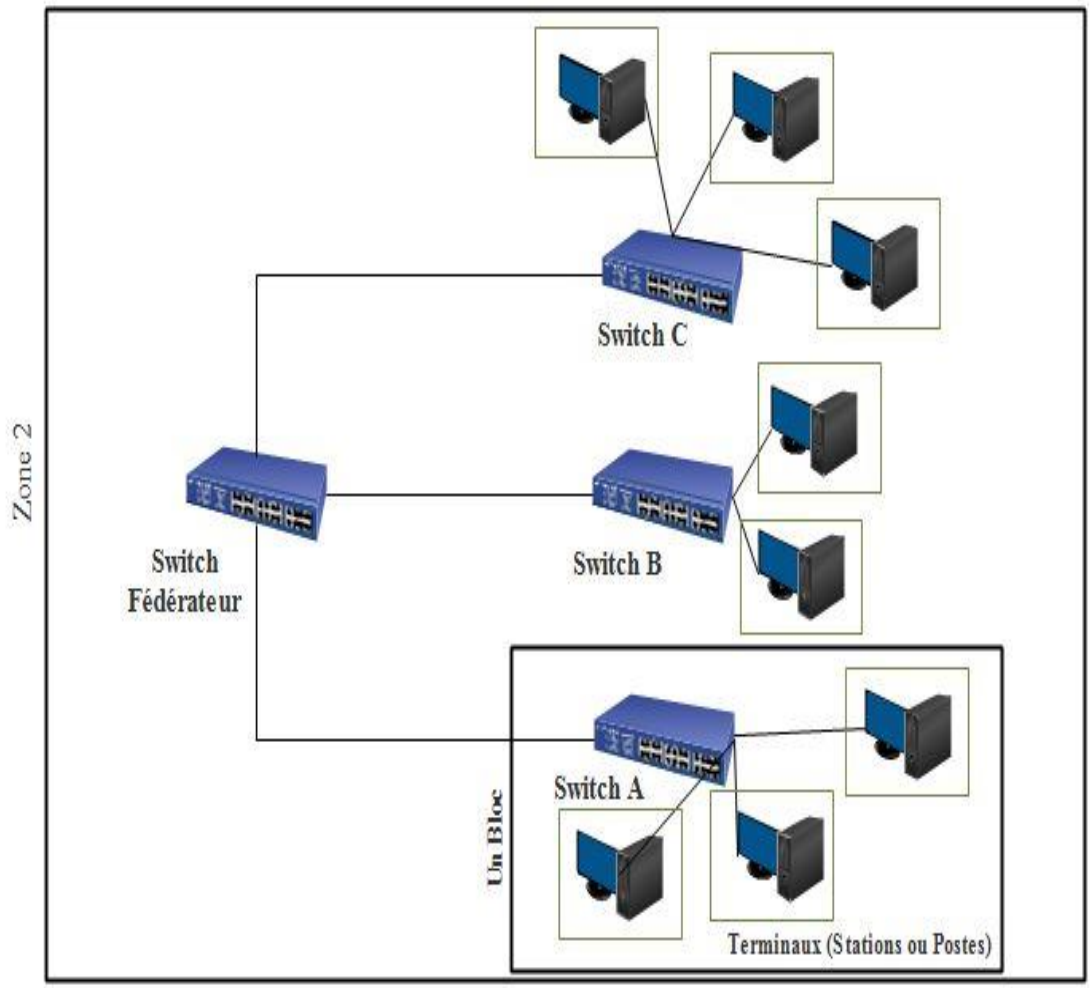

Figure 3.3 : la structure en couche de la zone 2

3.3.2. Description de la Zone 1

La connexion vers l'extérieur est réalisée à l'aide de la zone 1, qui est le backbone du réseau (le cœur du réseau) et c'est l'a que se passe toute l'administration du réseau. Plusieurs équipements contribuent à l'activité de cette zone :

- Un routeur : il permet l'interconnexion du réseau local et l'extérieur par l'acheminement des paquets de ou vers internet.

- Un pare-feu : il se charge de filtrage des paquets et il permet aussi le routage inter-LAN car l'une de ces interfaces est reliée directement à un switch fédérateur. L'autre interface donne sur une zone qui héberge les différents serveurs du réseau.

- un switch fédérateur : il connecte six zones, quatre liaisons connectent quatre zones au campus de Targa et une liaison connecte le campus d'Aboudaou, lequel à travers un autre switch fédérateur connecte deux autres liaisons menant vers deux zones du campus d'Aboudaou.

- les serveurs : les différents serveurs existants sont :
  - le serveur Web.
  - le serveur DHCP.
  - le serveur DNS.
  - le serveur FTP.
  - le serveur de messagerie (Mail).
  - le serveur de Téléphonie IP.
  - le serveur proxy ou encore le serveur d'authentification (RADIUS).

Cette description de la zone 1 est illustrée dans la figure ci-dessous :

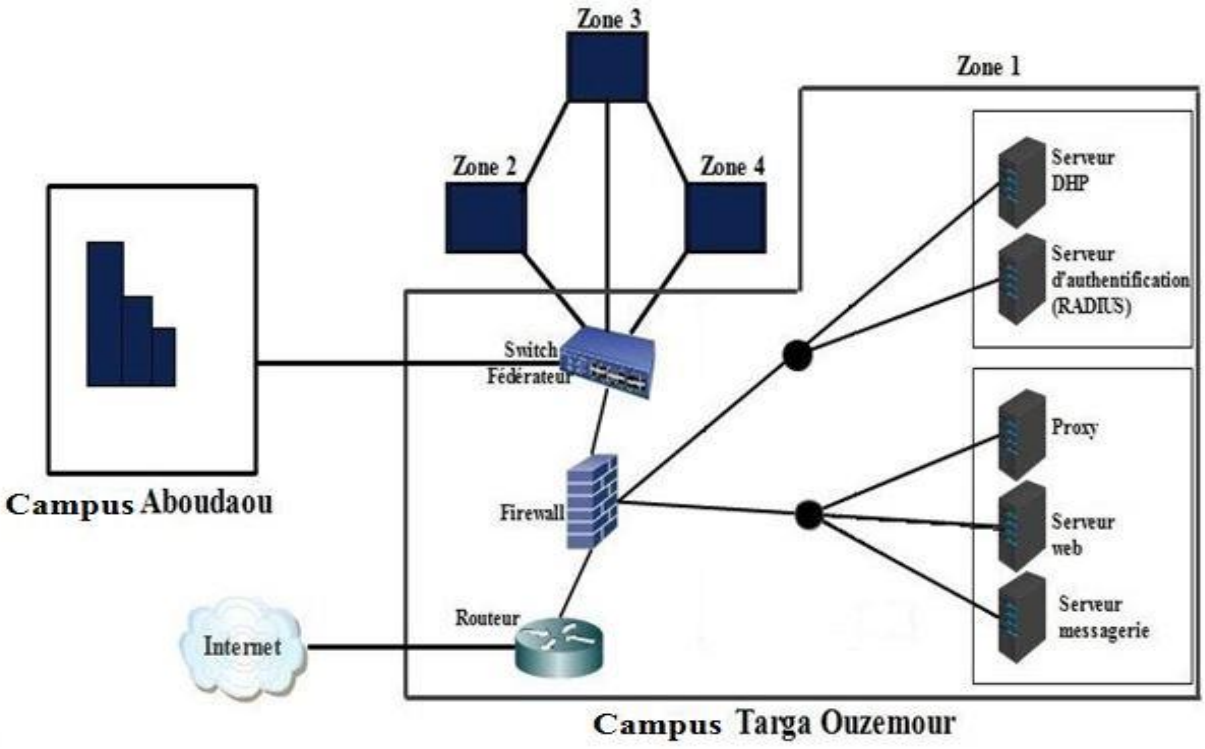

Figure 3.4 : Description de la Zone 1 (backbone)

3.4. Diagnostique de la situation du réseau

L'étude que nous avons menée, nous a permis de relever quelques activités non encore réalisées au niveau du réseau de l'université à savoir :

- Ces derniers temps des enseignants, des responsables souhaitent se connecter au réseau de l'université, en dehors de l'infrastructure sécurisée de l'entreprise dans le but d'avoir accès à certaines ressources prédéfinies de l'université, (généralement des données et des applications), et de continuer leur travail à distance sans y être physiquement présent. A cet effet il faudra trouver une solution qui garantit l'accès

distant aux ressources du réseau en assurant le contrôle d'accès et les droits des utilisateurs.

- tous les utilisateurs ont accès à internet, l'ouverture d'un tel accès engendre une sécurité moindre, principalement l'exposition à des virus ou à des fichiers indésirables susceptibles d'endommager les postes clients ou le réseau lui-même. D'autre part, il engendre un problème de confidentialité des données, où n'importe quel utilisateur du réseau qui possède un logiciel sniffé sur son pc, aura la possibilité d'écouter les communications du réseau.

- la liaison entre le réseau de l'université « Targa » et le réseau de l'université« Aboudaou» est réalisée au moyen de la fibre optique, en passant par le réseau public. Et comme le nombre de machines augmente de plus en plus la surcharge du réseau est imminente.

3.5. Solution proposée

- Une bonne organisation à l'aide des VLAN, permettra une amélioration de l'usage du réseau en termes d'efficacité et de performance. D'autre part la séparation du réseau des deux campus est devenue une nécessité primordiale, en ajoutant une nouvelle ligne spécialisée vers le campus Aboudaou.

- Pour répondre aux problèmes d'attaques d'une manière idéale, nous adoptons une architecture sécurisée basée sur un firewall dans le but de filtrer les communications autorisées et protéger le réseau local contre les tentatives d'intrusion et ce qui représente une sécurité supplémentaire rendant le réseau ouvert sur internet.

- pour répondre au besoin d'accès à distance avec toute sécurité et garantir la confidentialité du trafic de l'utilisateur distant, nous proposons la mise en place d'un VPN qui se base sur la création d'un tunnel virtuel entre une machine sur Internet où les données transmises seront chiffrées. Ce dernier est doté d'une adresse IP et une passerelle d'accès du réseau de l'université.

- Afin que les deux réseaux distants, puissent communiquer en toute sécurité, nous adoptons un VPN site to site qui sera également basé sur un tunnel virtuel entre ces deux sites.

❖ **Architecture proposée**

Après les critiques et les suggestions sur le réseau actuel, nous avons proposé une nouvelle architecture réseau qui consiste à séparer le réseau de l'université de Béjaia en deux réseaux. Une salle d'administration est rajoutée au niveau du campus d'Aboudaou qui va contenir tous les serveurs nécessaires.
Un VPN site à site est placé entre les deux réseaux des deux campus pour sécuriser les communications entre ces derniers.

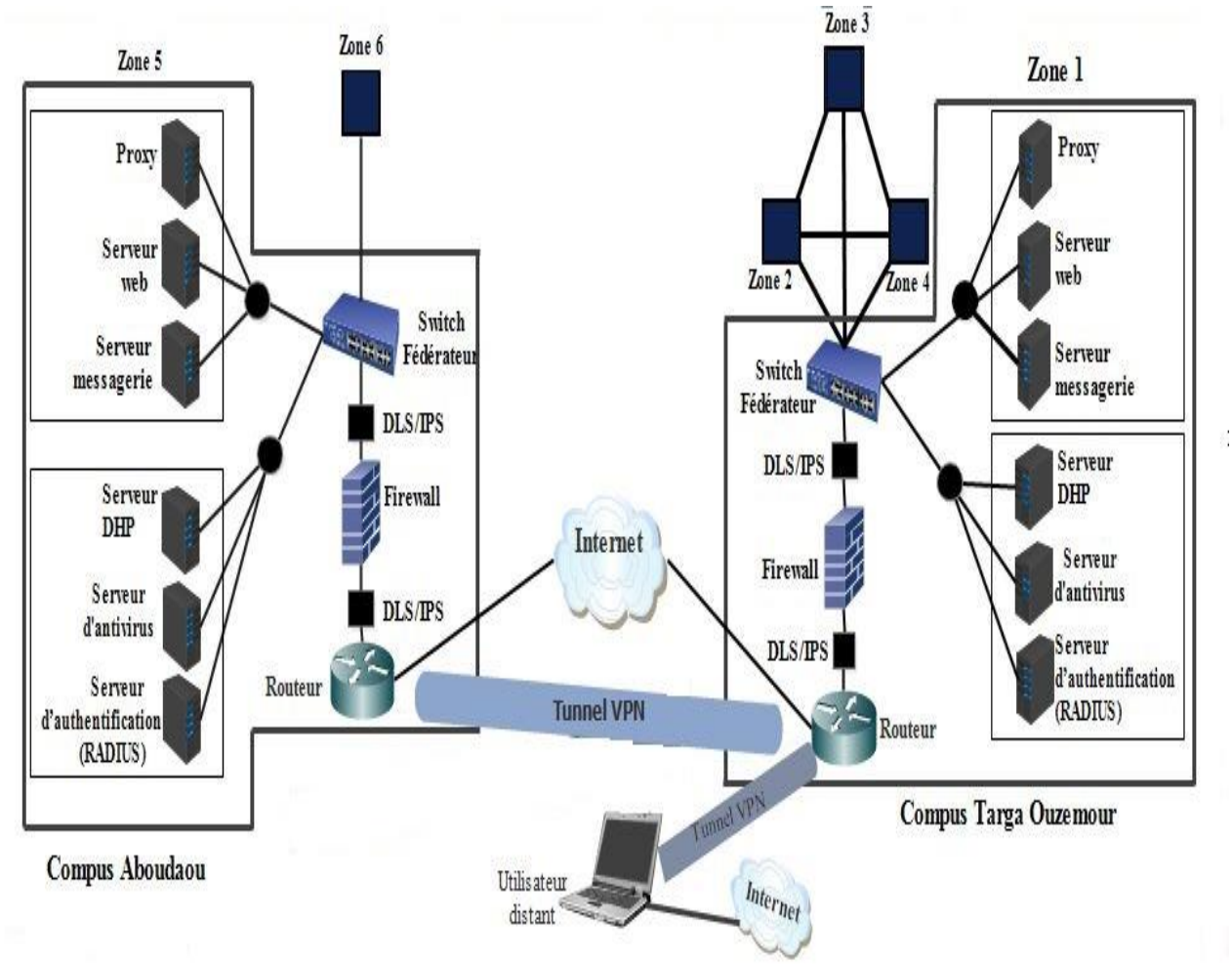

Figure 3.5 : La nouvelle architecture proposée.

3.6. Conclusion :

Dans ce chapitre nous avons présenté l'université de Bejaia, ainsi que la structure de son réseau, puis nous avons spécifié ses besoins et faiblesses en termes de sécurité.
Enfin nous avons adopté quelques solutions afin d'assurer une meilleure sécurité de réseau, qui serons développés dans le dernier chapitre.

Chapitre 4 : Solution de sécurité proposée

4.1. Introduction

Après la concrétisation de notre étude dans le chapitre précèdent, la mise en œuvre d'une architecture sécurisée basée sur les firewalls et les VPN est la meilleure solution à laquelle nous avons abouti, pour passer à la dernière étape de notre travail qui est la réalisation de notre projet.

Dans ce chapitre nous décrirons l'environnement de travail utilisé et les principales étapes de configuration pour mettre en œuvre un VPN site à site et un VPN d'accès distant.

4.2. Description de l'environnement de travail

La virtualisation s'agit de la création d'une version virtuelle d'une entité physique. Elle peut s'appliquer aux applications, aux serveurs, aux stockages et aux réseaux dans le but de réduire les dépenses informatiques. [22]

4.2.1. VMware Workstation 14

VMware (Virtual Machine) est un logiciel qui répond aux problèmes suivants :

- La difficulté d'exécution de plusieurs systèmes d'exploitation et applications sur la même machine physique.
- Le nombre de partitions est limité.

VMware permet la création d'une ou plusieurs machines virtuelles, qui peuvent fonctionner en même temps et qui sont reliées au réseau local avec une adresse IP différente. [22]

❖ **Avantages des VM**

- ✓ L'exécution de plusieurs systèmes d'exploitation sur le même serveur physique.
- ✓ La répartition des ressources systèmes entre les machines virtuelles.
- ✓ Assurer la protection de la sécurité au niveau matériel.
- ✓ Déplacer et copier des machines virtuelles aussi facilement.

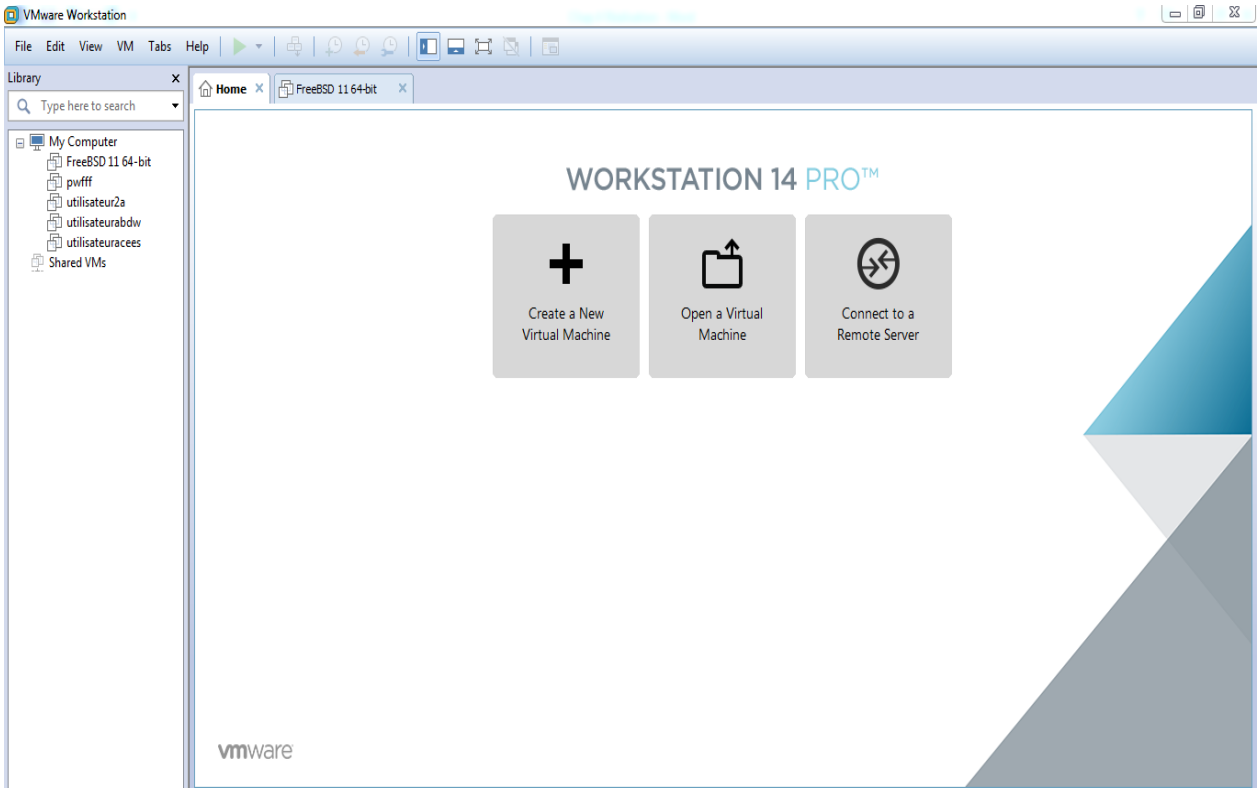

Figure 4.1 : VMware Workstation 14

4.2.2. Le pare-feu Pfsense

❖ **Définition**

C'est un pare-feu de nouvelle génération, qui possède également les fonctionnalités d'un routeur et qui peut être installé sur un simple ordinateur personnel comme sur un serveur.

Pfsense possède une infrastructure simplifiée et permet d'intégrer de nouveaux services, tels que la mise en place d'un VPN. Il est réputé pour sa fiabilité, après une installation en mode console il s'administre ensuite simplement depuis une interface web et gère nativement les VLAN. [23]

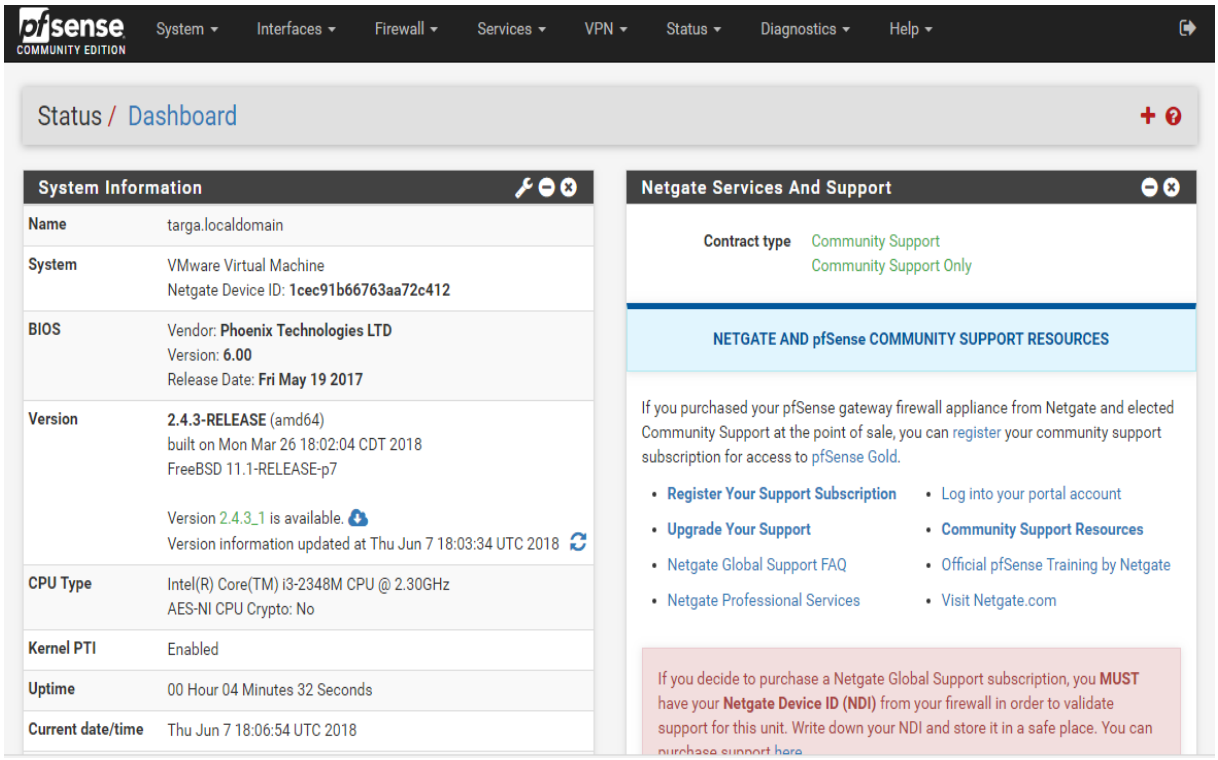

Figure 4.2 : l'interface de Pfsense.

❖ **Principales fonctionnalités**

Le pare-feu Pfsense peut jouer le rôle de :

✓ **Un fournisseur de services tel que :**

- Relais DNS.
- Serveur DHCP.
- Portail captif de connexion.

✓ **Un routeur tel que :**

- La mise en place des VPNS.
- Implémentation des protocoles de routage : RIP, OLSR, BGP.

✓ **Un firewall tel que :**

- la traduction d'adresses : NAT.
- le filtrage de paquets entre WAN et LAN et entre deux réseaux reliés par un VPN.

4.4.3. Présentation générale de la solution proposée

Nous allons présenter l'architecture réseau proposée pour la mise en œuvre des deux types des VPN site à site et accès distant, ainsi que le plan d'adressage utilisé pour aboutir à la solution proposée.

4.4.3.1. Le plan d'adressage

-	Adresse IP locale	Adresse IP Internet
Site Targa	192.168.108.0	192.168.43.243
Site Aboudaou	192.168.93.0	192.168.43.129

Tableau 4.1 : le plan d'adressage des deux sites.

4.3.2 L'architecture du LAN avec la solution proposée

4.3.2.1 L'architecture site à site (site to site)

Dans le but d'interconnecter dans des meilleurs conditions de sécurité les deux sites de l'université Targa et Aboudaou, nous avons opté pour la solution de la mise en place d'un VPN Site-to-Site, en utilisant deux routeurs Pfsense et les rôles client/serveur d'OpenVPN intégrés à ceux-ci, ce qui fournit un service de sécurité fiable grâce à un tunnel sécurisé qui transporte les données transmises entre ces deux sites comme si on était dans le même réseau local.

Nous avons donc au-moins un client sur chaque réseau, chacun d'eux est connecté à son firewall PfSense. Ces deux routeurs vont être connectés entre eux via OpenVPN à travers internet.

La figure suivante illustre cette solution proposée :

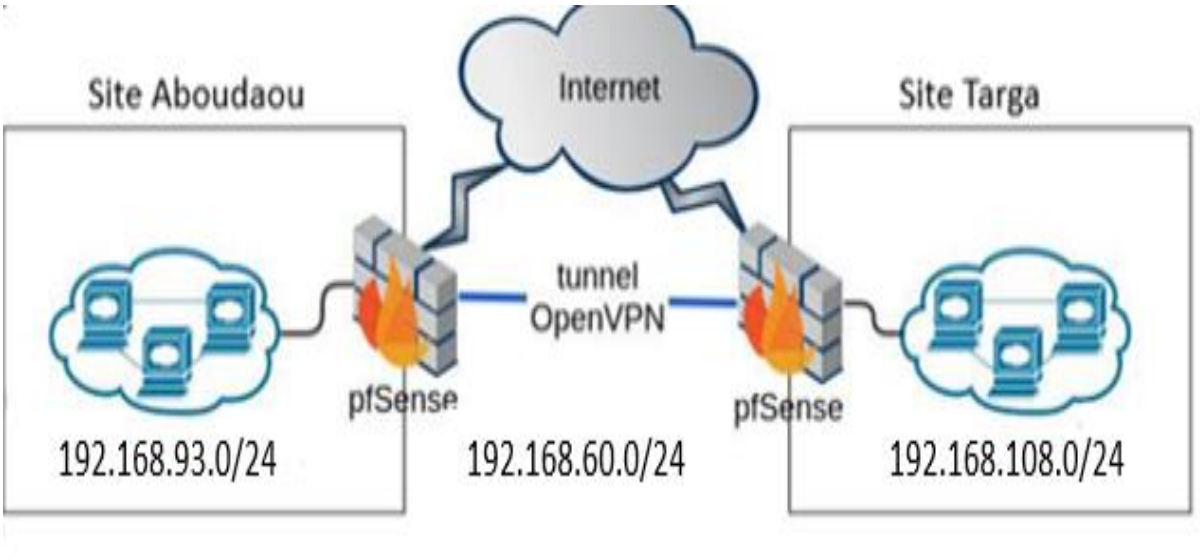

Figure 4.3 : L'architecture site à site proposée.

4.3.2.2 L'architecture accès distant (remote acess)

Afin d'autoriser à des utilisateurs nomades de l'université, un accès sécurisé aux ressources existantes et au système d'informations local sans être physiquement présent, nous avons proposé une mise en œuvre des VPN d'accès distant en se basant sur le protocole OpenVpn.

Cette solution assure le contrôle et la sécurité de cette connexion grâce à un simple accès Internet et un tunnel sécurisé.

Nous avons donc un firewall PfSense sur le site principal, connectés à un utilisateur nomade via OpenVPN à travers internet.

La figure suivante illustre cette solution proposée :

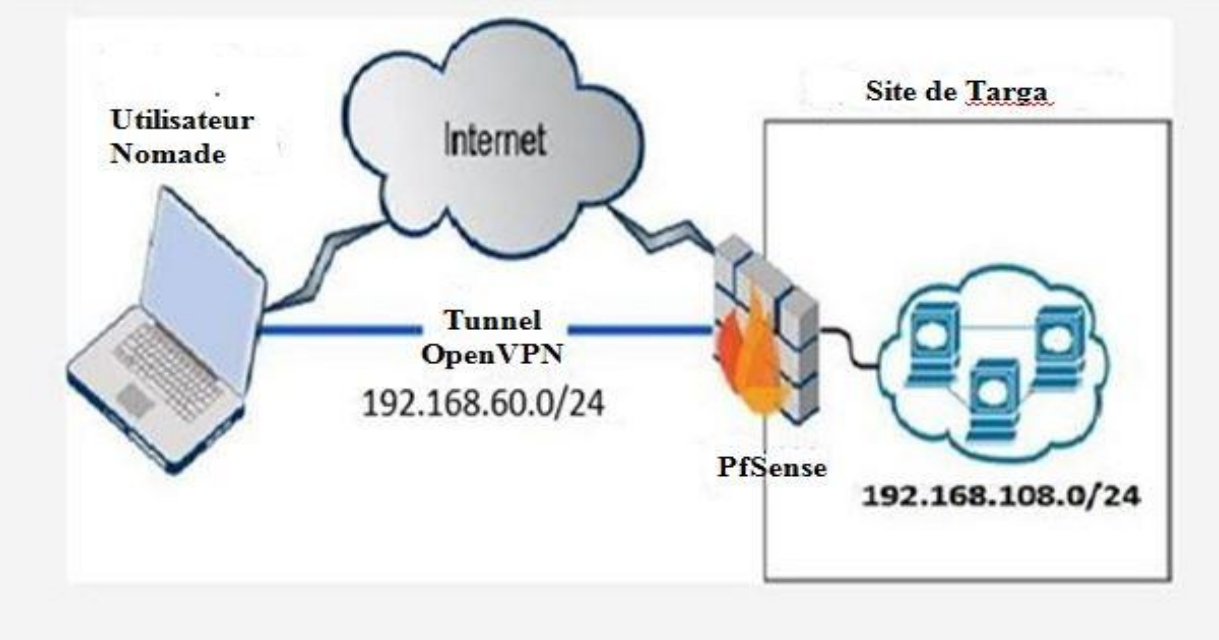

Figure 4.4 : L'architecture accès distant proposée.

4.4. Implémentation de la solution proposée

4.4.1. Création des machines virtuelles

Cette étape s'agit de la création de deux machines virtuelles où chacune d'entre elles représente un des deux sites.

- Targa: représente le site de Targa (site principal).
- Aboudaou: représente le site d'Aboudaou (site distant).

La figure suivante représente la première étape de la création d'une machine virtuelle :

Figure 4.5 : création d'une machine virtuelle.

Les différents équipements nécessaires au fonctionnement des deux machines crées sont obligatoirement attribués, principalement la mémoire et les cartes réseaux

Cette étape est illustrée dans la figure suivante :

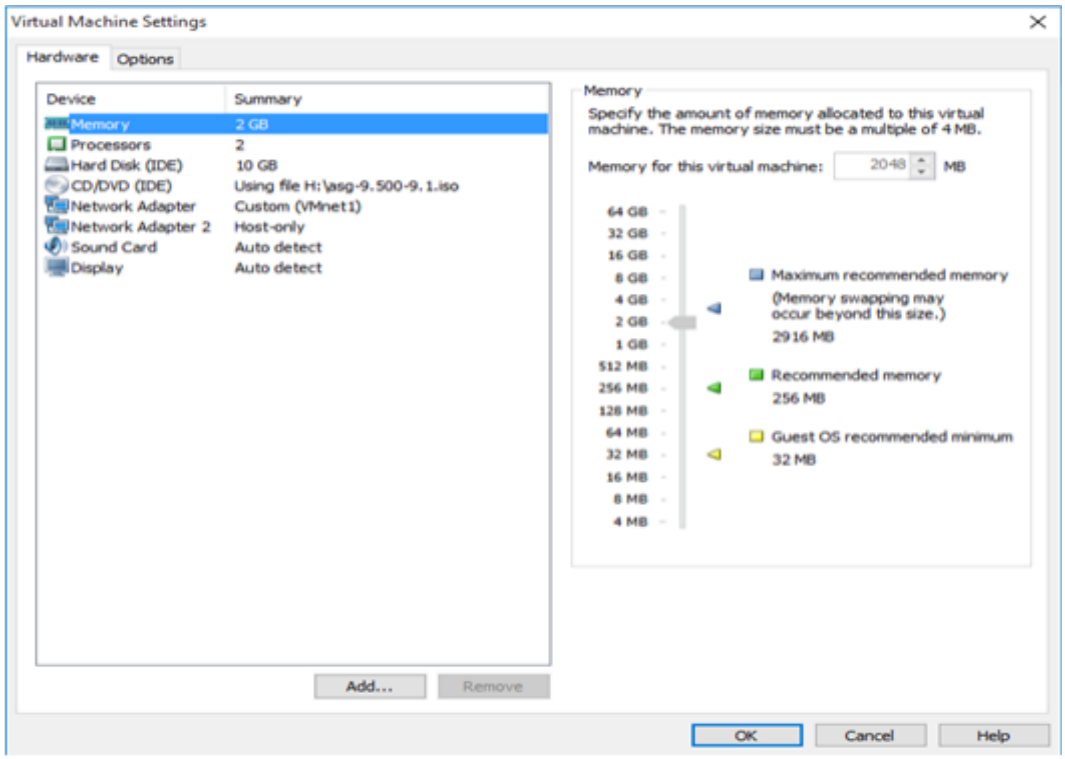

Figure 4.6 : attribution des matériels pour chaque machine.

A la fin de l'installation, une interface noire apparait contenant quelques informations propres à la machine virtuelle crée, principalement l'adresse IP du LAN attribuée ainsi que l'adresse du WAN.

Cette étape est illustrée dans la figure suivante :

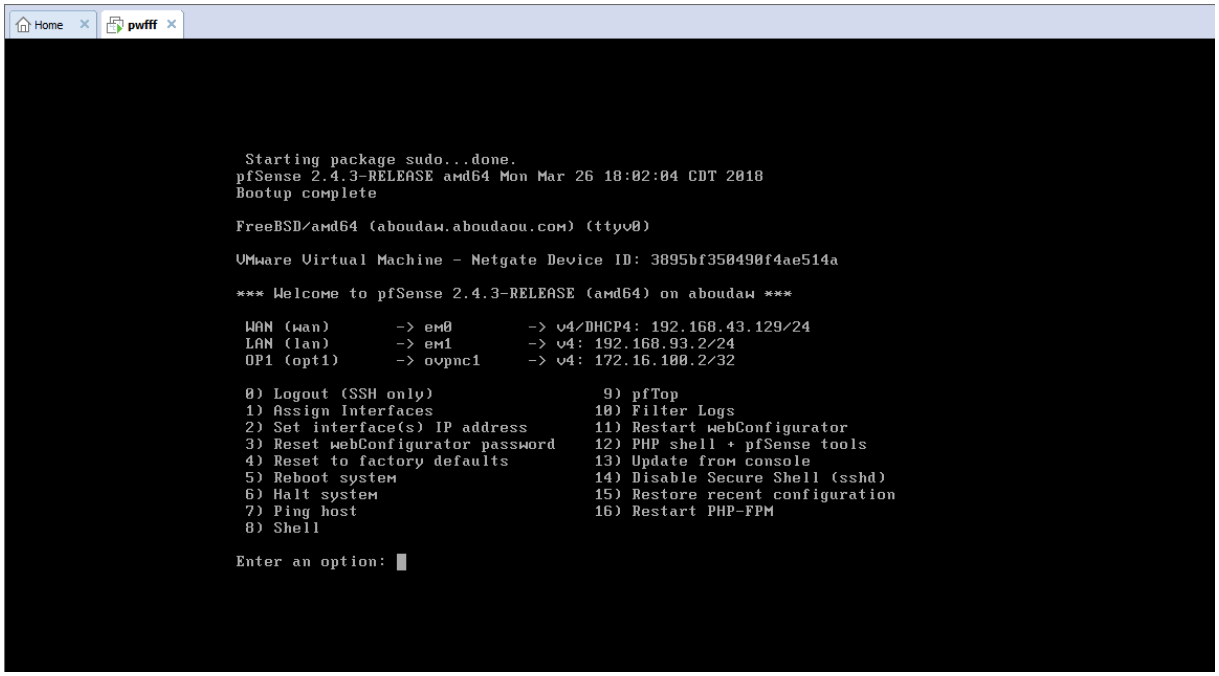

Figure 4.7: fin d'installation de la machine pfsensepwfff.

4.4.2. Configuration du pare-feu Pfsense

La configuration du pare-feu Pfsense, doit initialement passer par la page d'authentification. La première étape consiste à se rendre sur le site du pare-feu Pfsense et insérer quelques informations initiales sur l'université, suivi d'un mot de passe propre à l'administrateur avec lequel il aura accès à l'interface du pare-feu, comme c'est décrit ci-dessous :

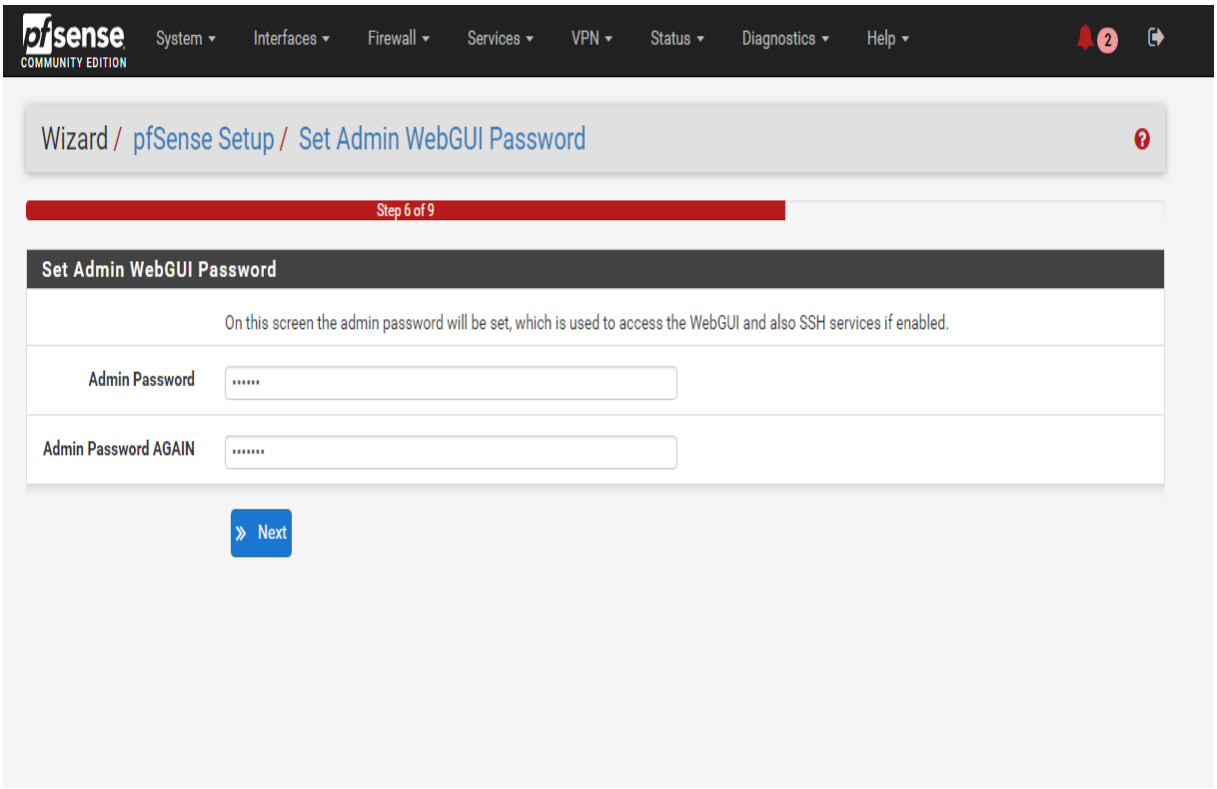

Figure 4.8 : configuration de la page d'authentification.

4.4.2.1 Configuration des VPN site à site

- **Configuration du premier PfSense (coté serveur)**

La première étape, est de se connecter à l'interface web du PfSense à partir du navigateur (192.168.108.21 qui représente le site de Targa).L'accès à cette interface est réalisé par la saisi de login et de mot de passe déjà introduit par l'administrateur.

Le serveur OpenVpn est créé à partir de l'onglet VPN du menu, en cliquant sur le bouton OpenVpn. Une fois sur l'interface d'administration consacrée à OpenVPN, on clique sur le bouton « servers » puis « +add », comme c'est décrit ci-dessous :

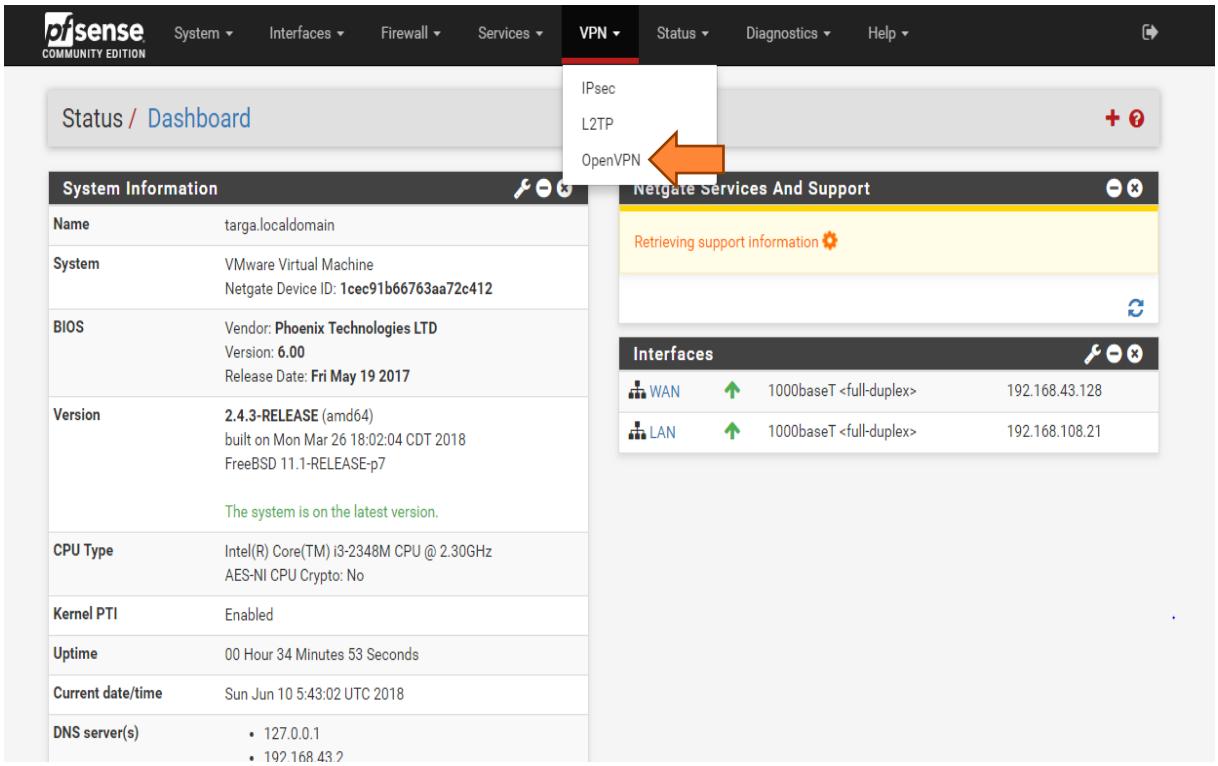

Figure 4.9: L'interface d'accès au serveur OpenVPN.

Une authentification par clés partagées est utilisée en sélectionnant «Peer to Peer (SharedKey) » pour le champ « Server mode » et le choix du port qui convient.

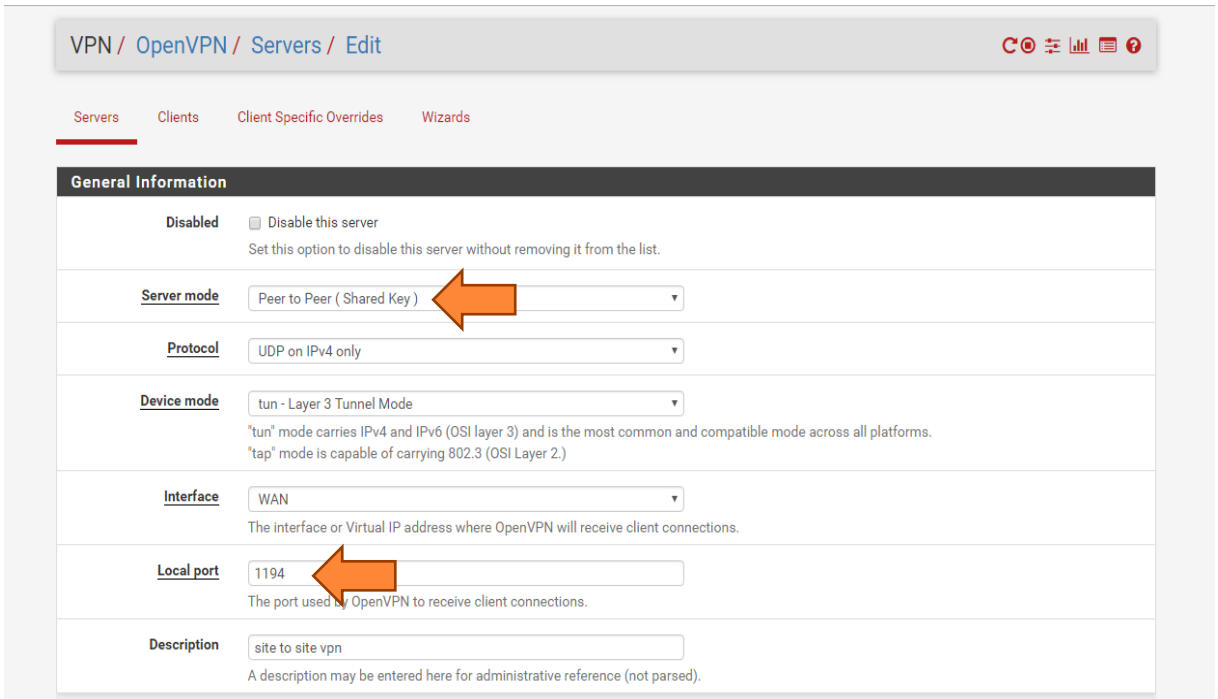

Figure 4.10 :l'interface de création du serveur OpenVPN.

La partie « Cryptographic Settings » permet de gérer les paramètres d'encryption.

La case de TLS configuration : Automatically generate a TLS key» doit être cochée, ce qui nous permet de choisir les options d'encryption.

Dans la case « DH ParameterLength » nous choisissons la taille de la clé d'encryption adéquate.

Pour la case « encryptionAlgorithm » nous permet de sélectionner l'algorithme qui nous convient.

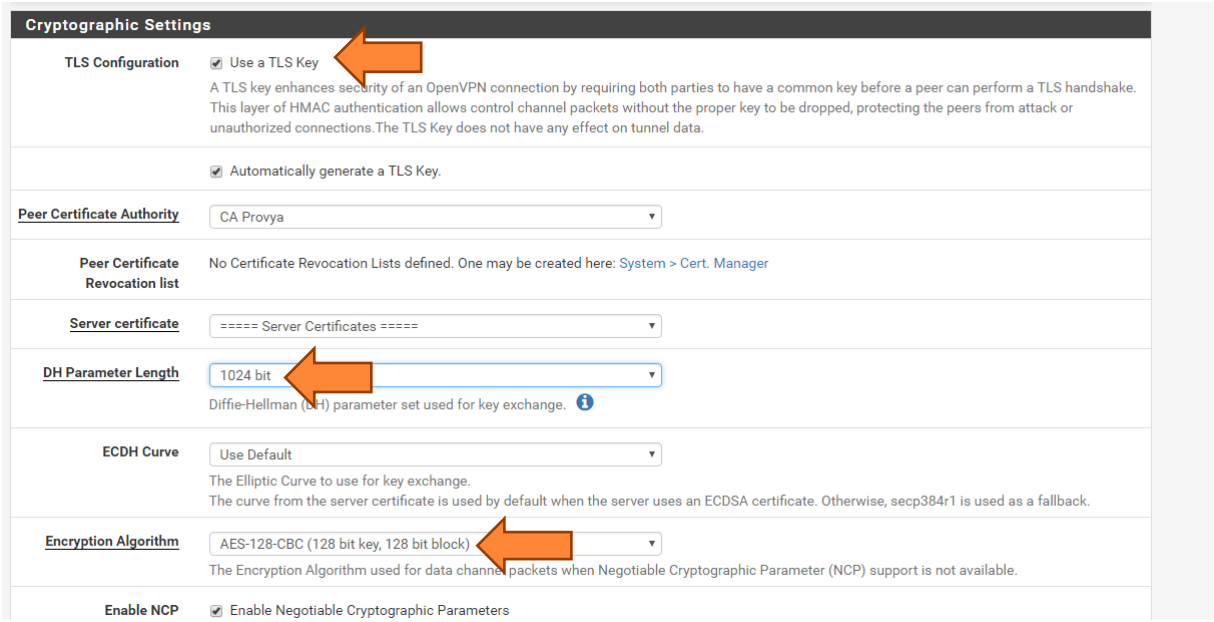

Figure 4.11 : L'interface du choix des paramètres d'encryption.

Il est obligatoire de remplir la partie « IPv4 Tunnel Network » par une adresse différente de celle des deux réseaux distants et c'est sur cette dernière que les données vont être transportées. Cette adresse est dite « adresse de tunnel », dans notre cas « 192.168.60.0 ».

Il est aussi obligatoire de renseigner la partie « IPv4 Remote network(s) » par l'adresse de réseau distant, qui est l'adresse du réseau LAN d'Aboudaou « 192.168.93.0 » dans notre cas.

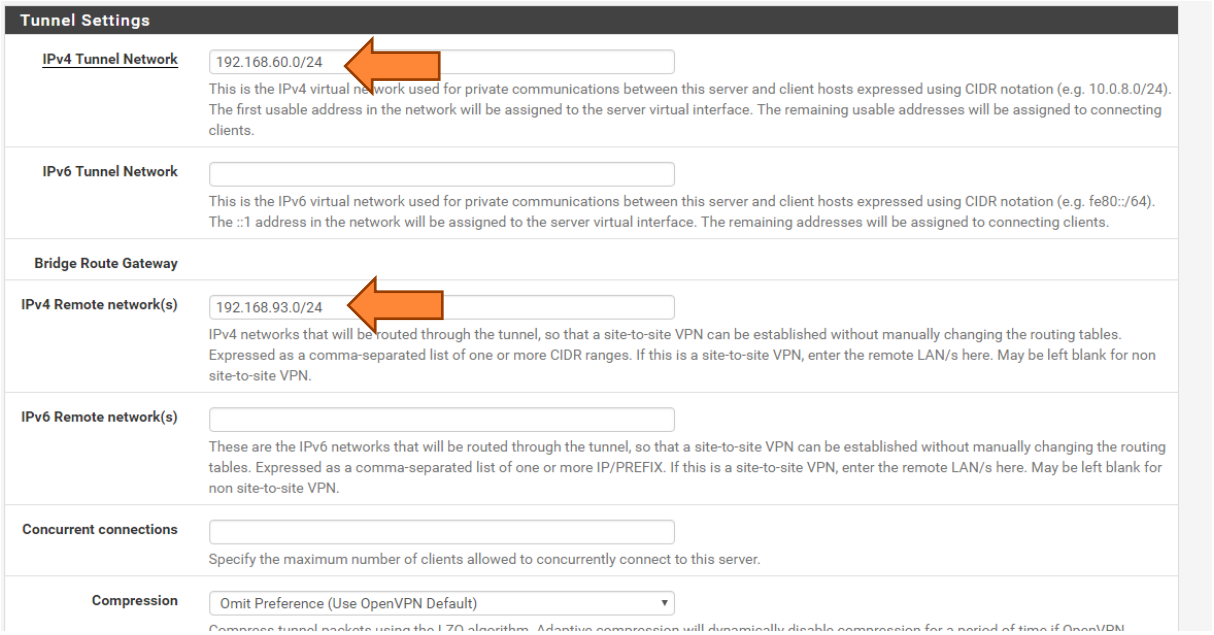

Figure 4.12 :L'interface d'affectation d'une adresse au tunnel.

Apres la sauvegarde de notre configuration par le bouton « save », notre serveur VPN est affiché sous forme d'un tableau contenant les informations que nous avons effectué au part avant.

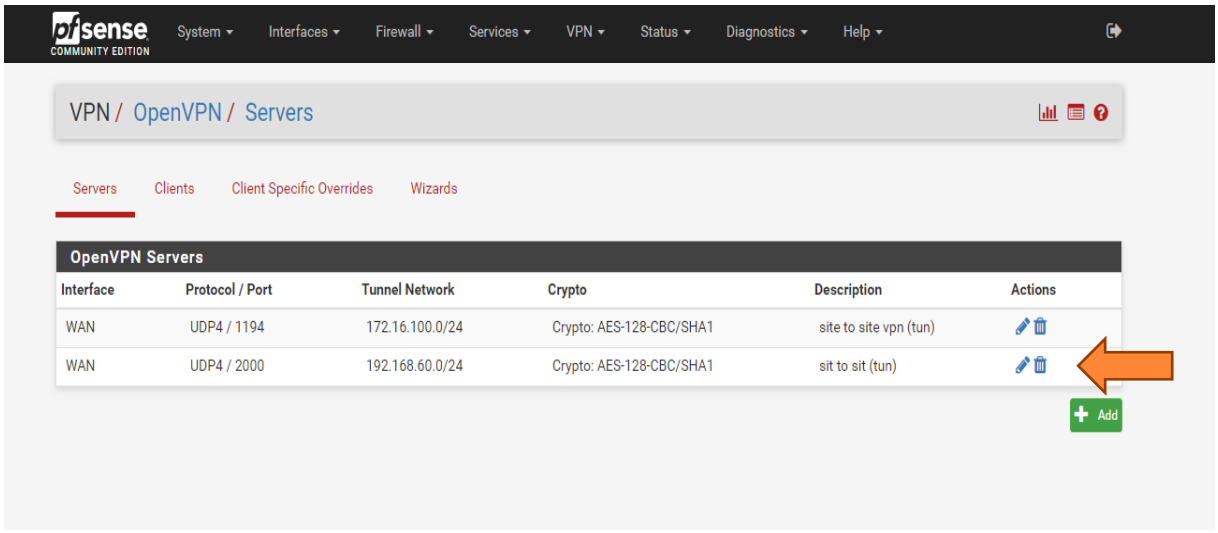

Figure 4.13 :l'interface du serveur OpenVPN.

Dans le cas où les interfaces WAN utilisées par deux machines ou VMs appartiennent à un même réseau local, cette configuration de l'interface WAN est nécessaire.

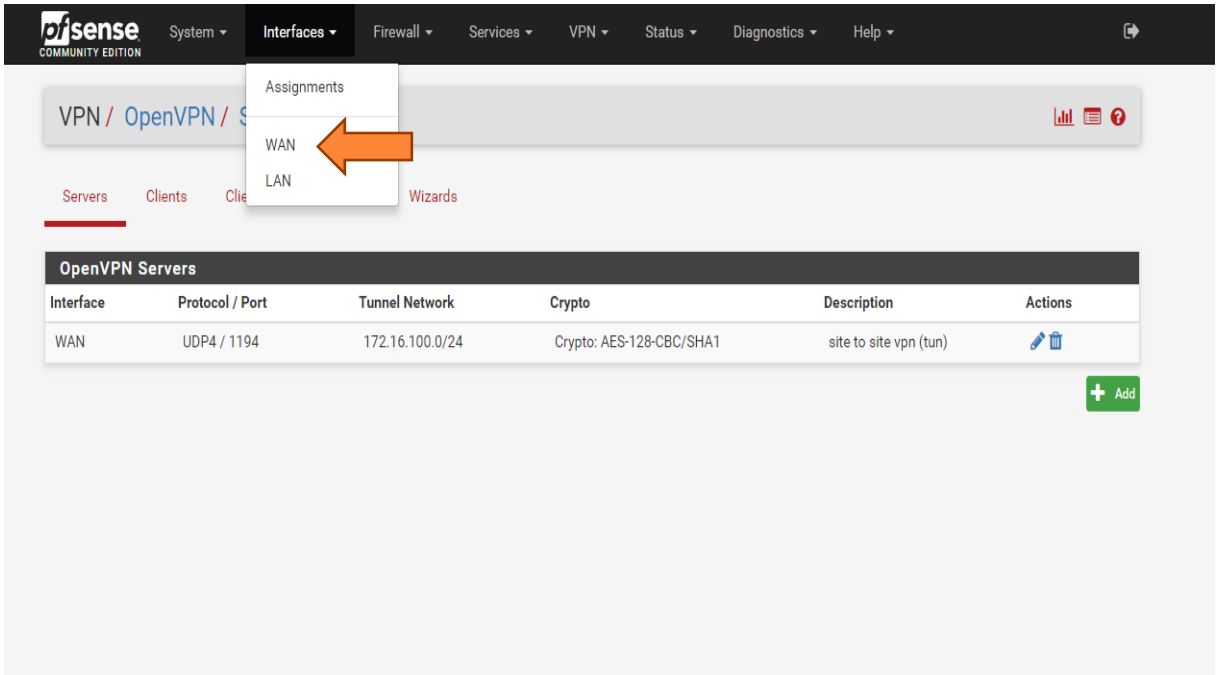

Figure 4.14 :La configuration de l'interface WAN du serveur OpenVPN.

Dans cette interface WAN nous devons décocher les deux cases « Block private networks and loopbackaddresses » et « Block bogon networks » de la partie « Reserved Network », ce qui permet de ne pas bloquer le futur client VPN, puis nous cliquons sur « save » pour enregistrer les modifications.

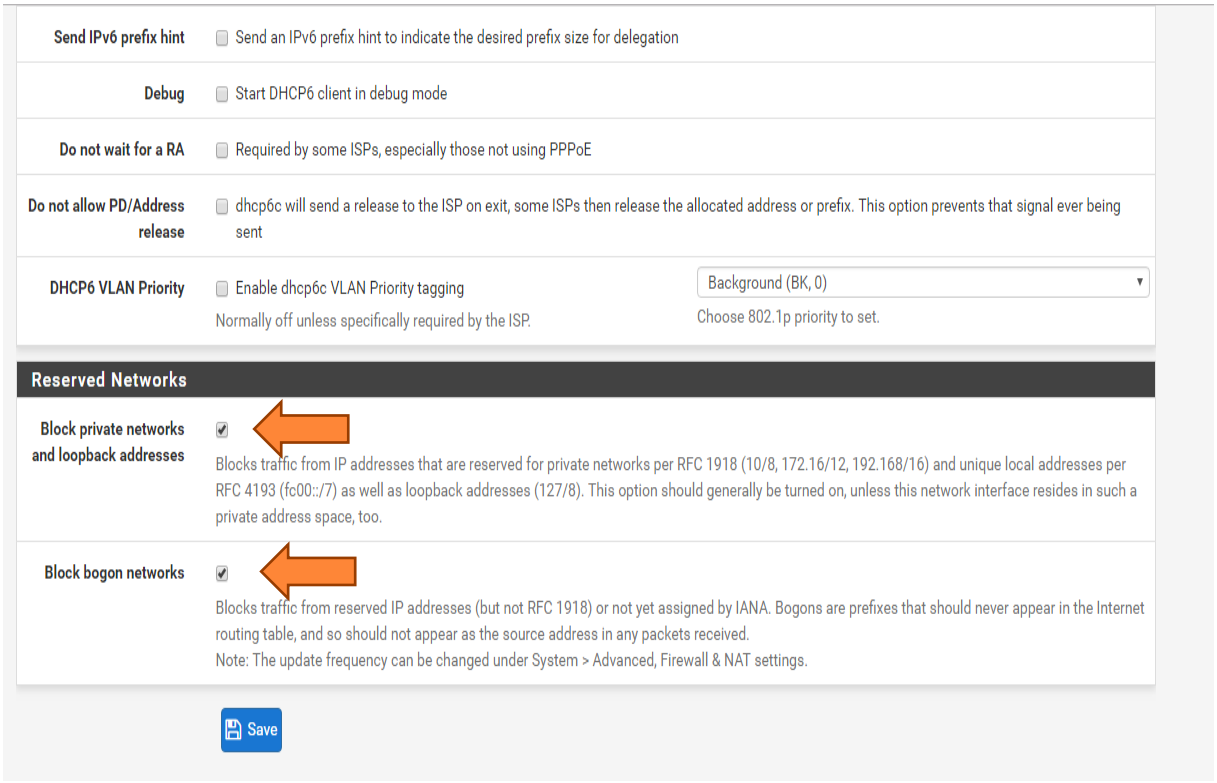

Figure 4.15 : la configuration de l'interface WAN.

Dans le but de réaliser une connexion du client OpenVPN vers le serveur OpenVPN, il est obligatoire de configurer le firewall de ce dernier.

Pour cela nous cliquons sur « Rules » de l'onglet « Firewall » de la barre de navigation.

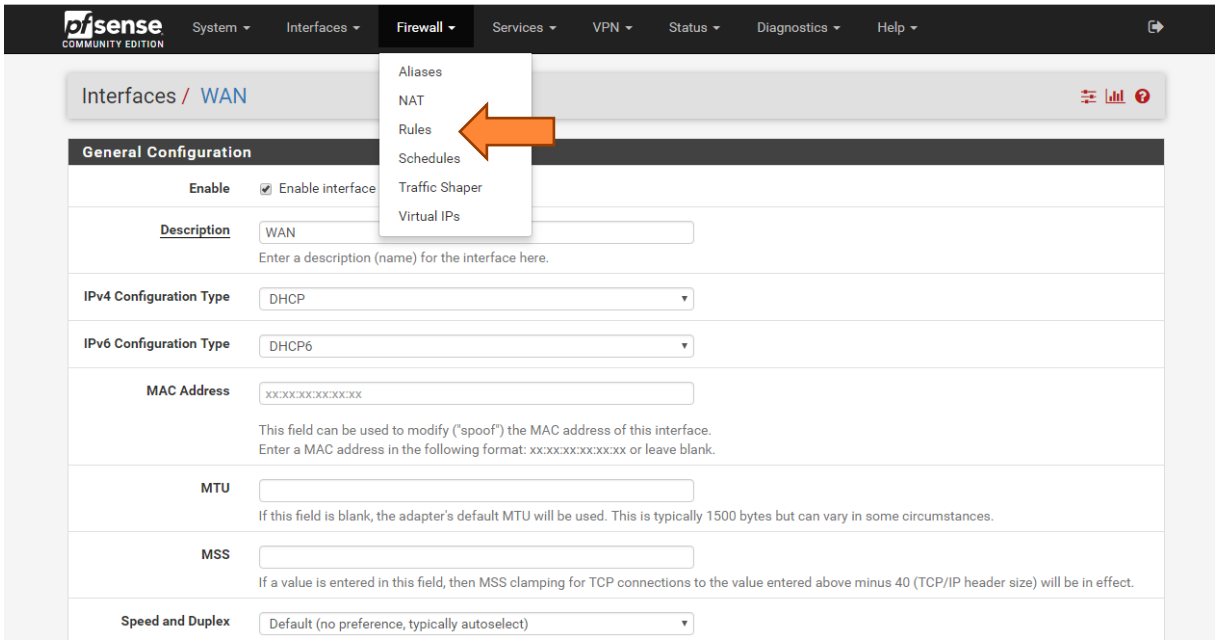

Figure 4.16 : interface de configuration du firewall.

Dans l'onglet WAN qui se trouve sur la page de configuration de firewall déjà accédée dans l'étape précédente, nous cliquons sur le bouton « Add » afin d'ajouter une nouvelle règle.

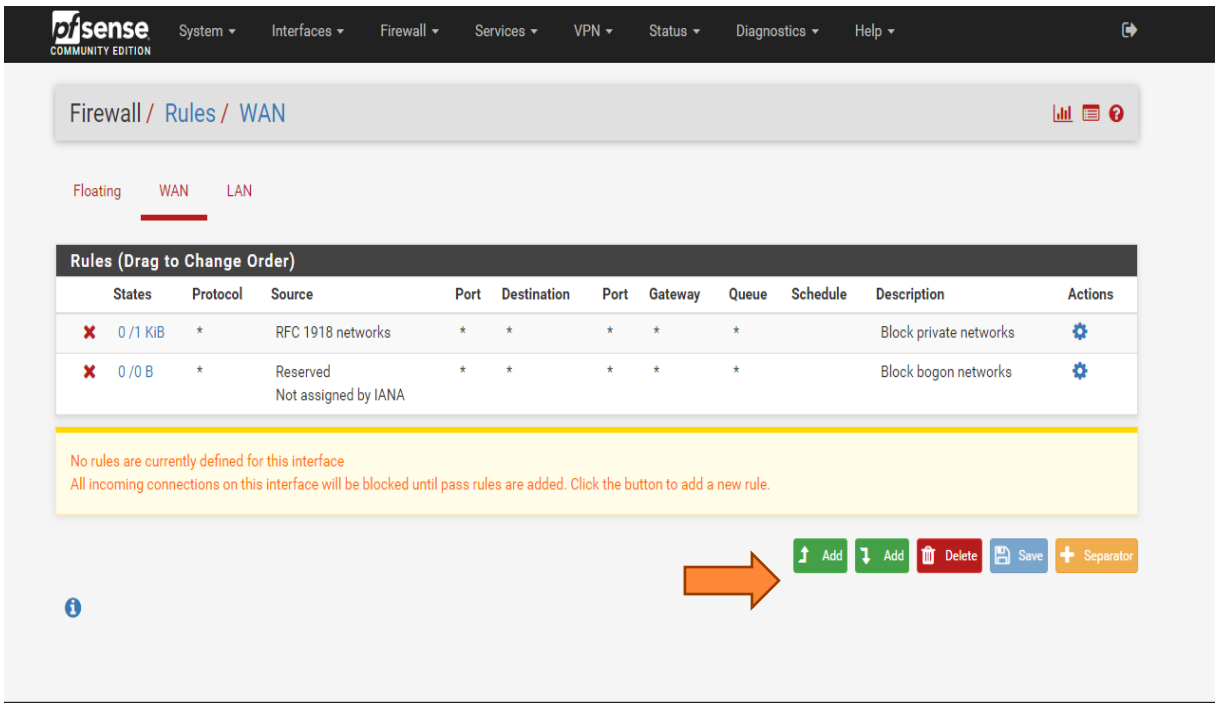

Figure 4.17 :L'interface d'ajout d'une règle firewall.

Une fois sur la page d'administration des règles du firewall, nous remplirons quelques champs par des informations qui dépendront de la configuration que nous avons faite, lors de la création de notre serveur OpenVPN.

Dans notre cas nous avons laissé le champ « Interface » à « WAN », le champ « AddressFamilly » à IPv4, et pour le champ « Protocol » nous avons sélectionné le protocole que nous avons déjà utilisé « UDP ».

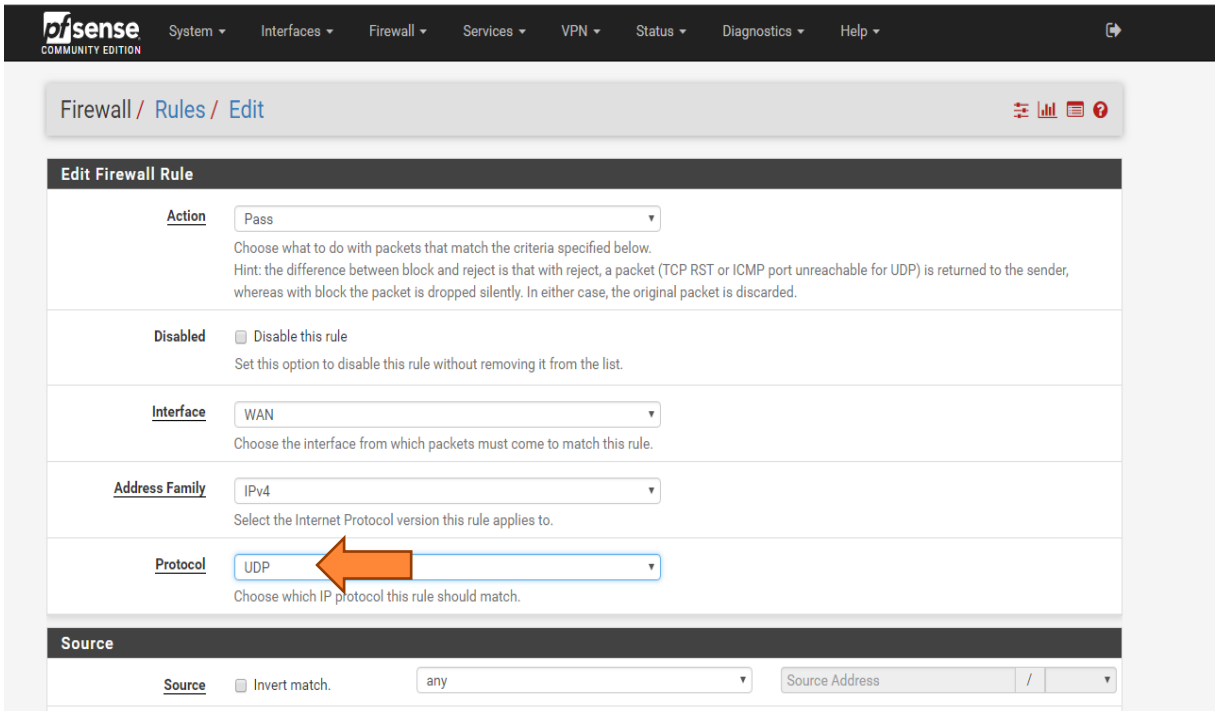

Figure 4.18 : l'interface dédiée à la configuration de la règle du firewall.

Dans la partie « source » de la même interface d'administration nous pouvons sélectionner « any » pour le champ « source » si nous désirons d'accepter toutes les sources.

Pour la partie « destination » nous choisissons l'option « this firewall (self) » pour le champ « destination », le port « 1994 » que nous avons déjà choisi lors de la création de notre serveur OpenVPN.

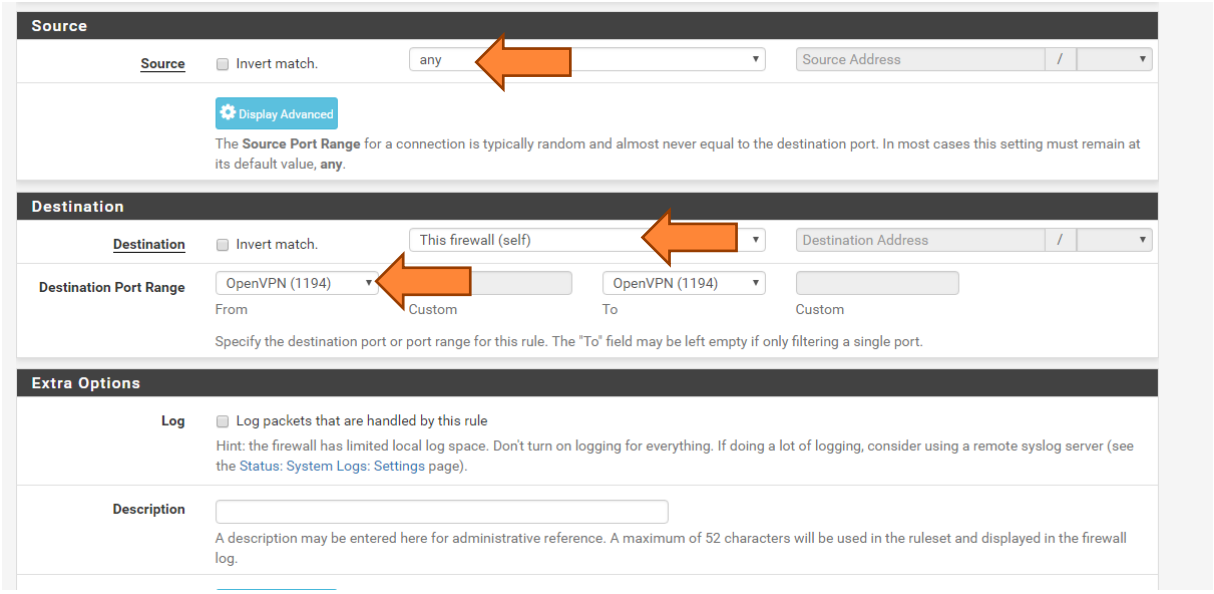

Figure 4.19 : L'interface d'attribution des paramètres de la règle du firewall.

❖ Configuration du second PfSense (coté client)

Cette étape s'agit de la configuration du PfSense de la partie client. Après avoir connecter à l'interface web de notre seconde PfSense depuis le navigateur (192.168.93.2 dans notre cas) nous cliquons sur l'onglet VPN puis OpenVPN de la barre des tâches.

Une fois sur la page d'administration consacrée à Open VPN, nous devons nous rendre sous l'onglet « Clients », puis nous cliquons sur le bouton « Add » pour ajouter un client.

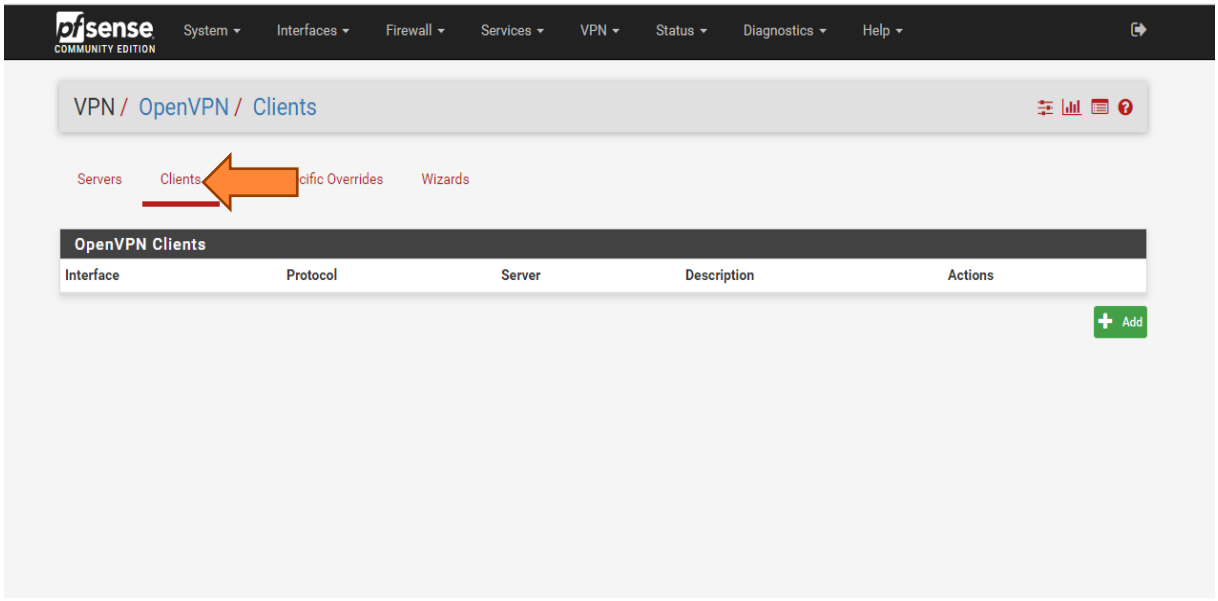

Figure 4.20 :l'interface d'ajout d'un client PfSense.

Dans la partie « General Information », nous devons changer le « Server mode » en « Peer to Peer (Shared Key), et affecter l'adresse du WAN distant au champ « Server host or address ».

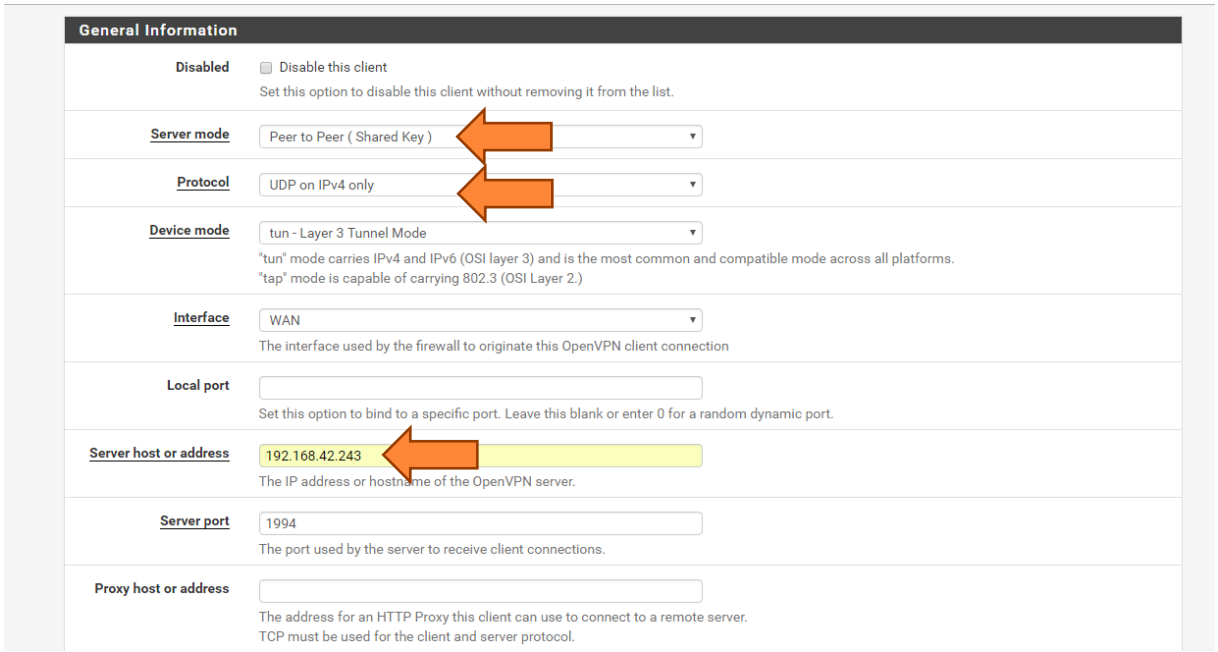

Figure 4.21 :L'interface de création d'un client OpenVPN.

Dans la partie « Tunnel Settings », nous devons renseigner l'adresse de la case (IPv4 Tunnel Network) qui est l'adresse du tunnel qui était déjà choisie dans la configuration du serveur OpenVPN.

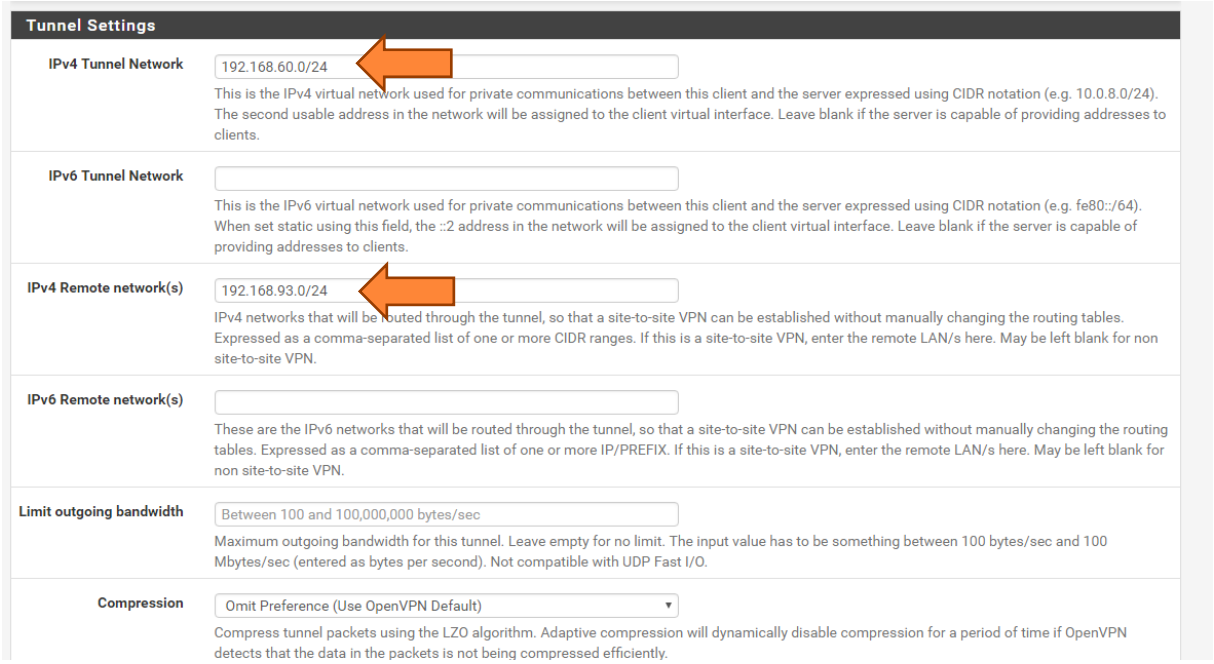

Figure 4.22 :L'interface d'affectation d'adresses au client.

Voici à quoi ressemble notre client OpenVPN :

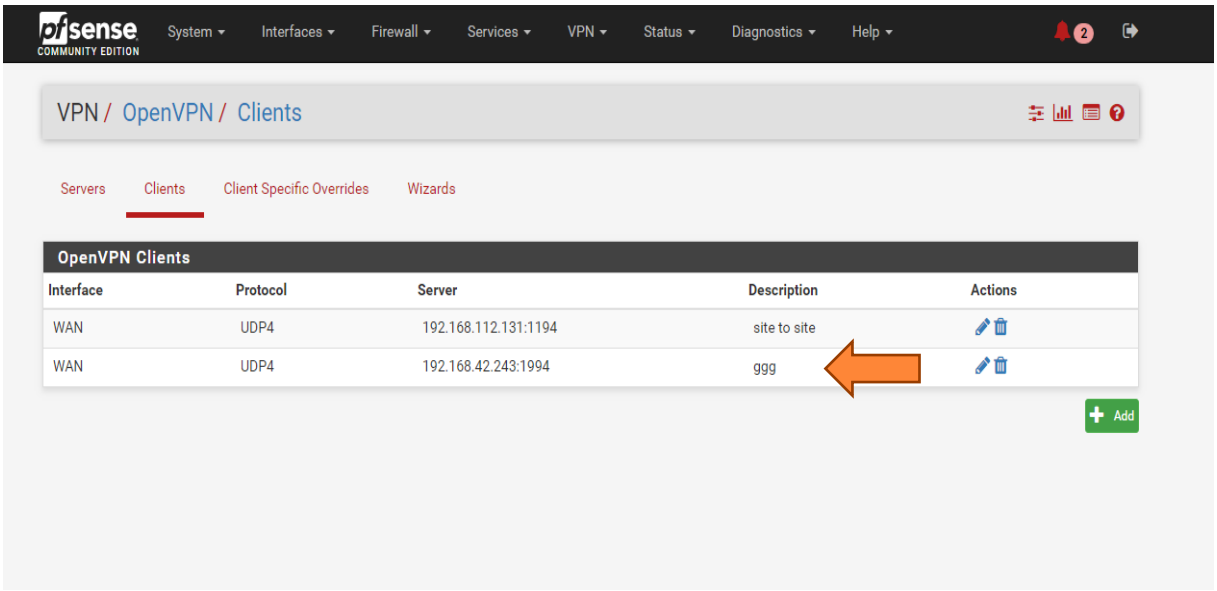

Figure 4.23 :l'interface du client OpenVPN.

Dans cette étape nous devons copier la clé générée par le serveur OpenVPN.

Sur la page d'administration de notre serveur OpenVPN, nous cliquons sur « VPN » de la barre des taches puis nous choisissons « OpenVPN ».

Une fois sur la page dédiée à notre serveur OpenVPN, nous Scrollons jusqu'à la partie cryptographique Settings, puis nous copions la clé qui a été généré.

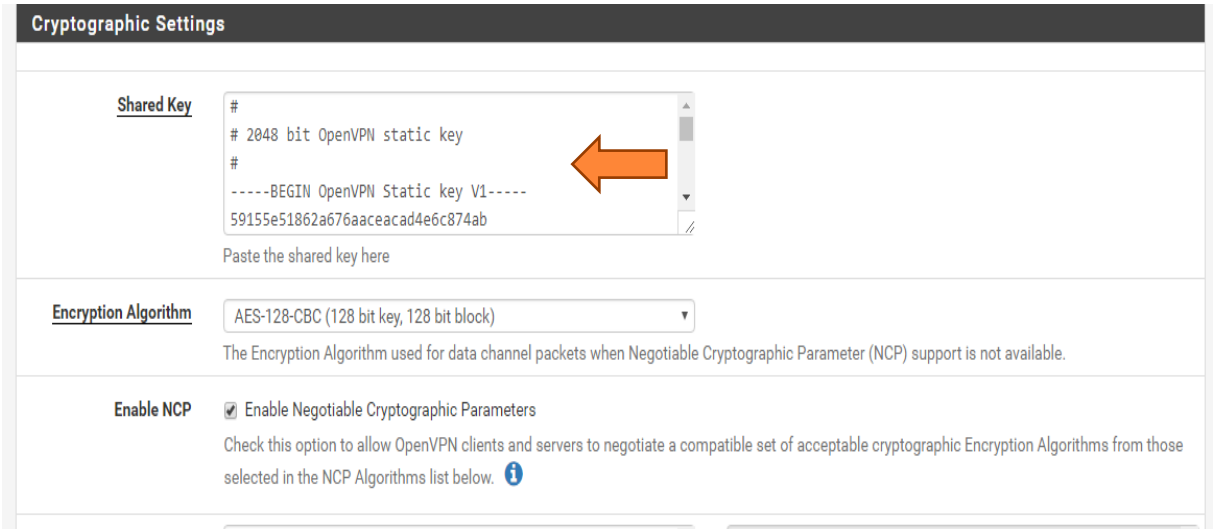

Figure 4.24 : La génération de la clé par le serveur OpenVPN.

Sur la page dédiée au client OpenVPN, rendez-vous sur le crayon « VPN » de la barre des taches, puis « OpenVPN » puis « Edit» du client déjà crée, ensuite nous scrollons jusqu'à la partie « Cryptographic Settings » et nous collons la clé déjà copiée.

A la fin nous devons sauvegarder la configuration, en cliquons sur le bouton « Save » en bas de la page.

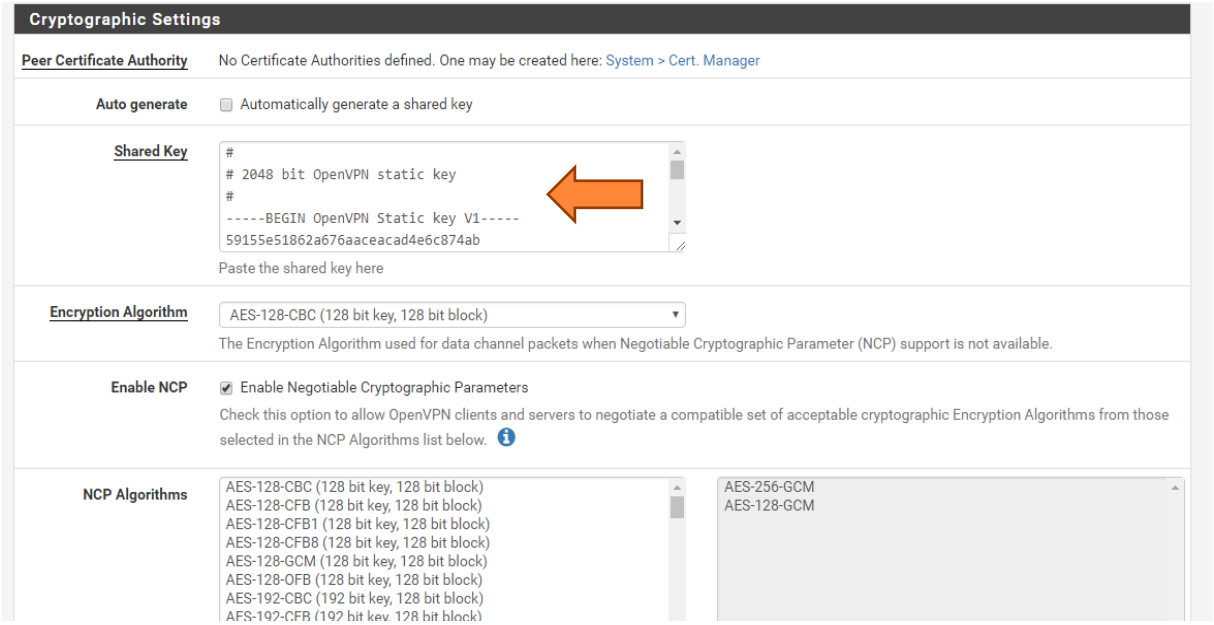

Figure 4.25 : le partage de la clé générée par le serveur.

Pour s'assurer que la liaison est bien fonctionnelle rendez-vous sous l'onglet « Status » de la barre de navigation, puis cliquez sur « OpenVPN ».

Nous pouvons voir dans la figure suivante que la liaison est bien opérationnelle donc notre VPN site-to-site est enfin fonctionnel.

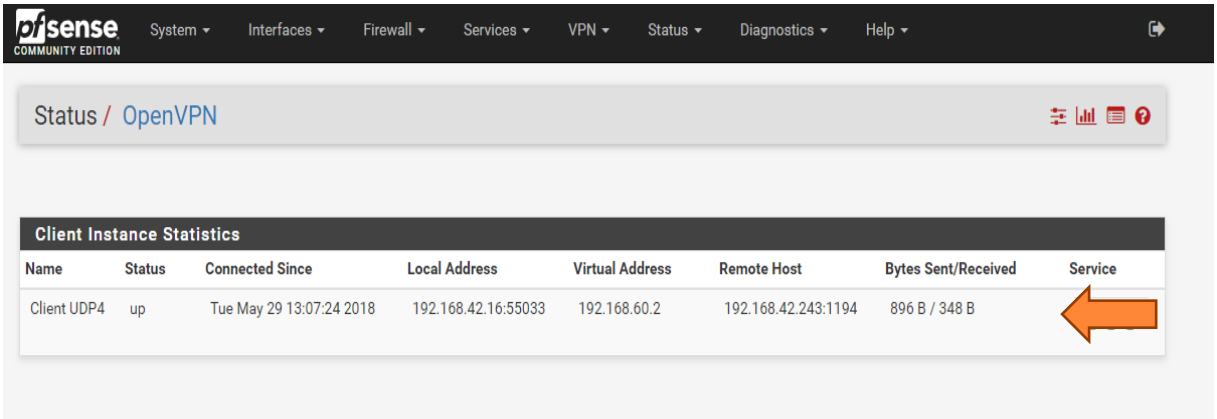

Figure 4.26 : Le fonctionnement de la liaison OpenVPN.

Nous avons besoin d'une autre règle sur les firewalls de nos PfSense. Pour cela, il faut se rendre sur l'interface web du PfSensede « Targa » puis aller sous l'onglet « Firewall », et nous cliquons sur « Rules Sur la page dédiée au firewall, nous cliquons sur l'onglet « OpenVPN », puis sur « Add ».

Sur la page qui apparait, nous choisissons d'accepter tous les types de protocoles « anny ». (Nous devrons refaire les mêmes étapes pour le PfSense de « Aboudaou ».

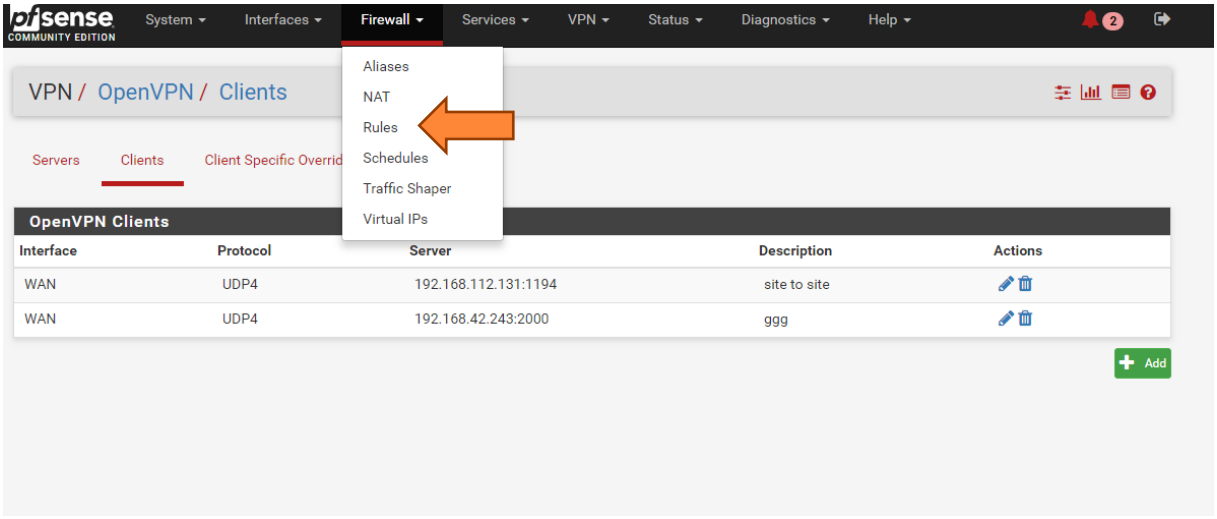

Figure 4.27 : Création d'une règle de firewall.

Nous essayons maintenant de communiquer avec une machine du réseau LAN distant, depuis le réseau de l'université de « Targa ».

Dans la figure suivante nous observons la bonne réception des paquets transmis et dans le bon ordre.

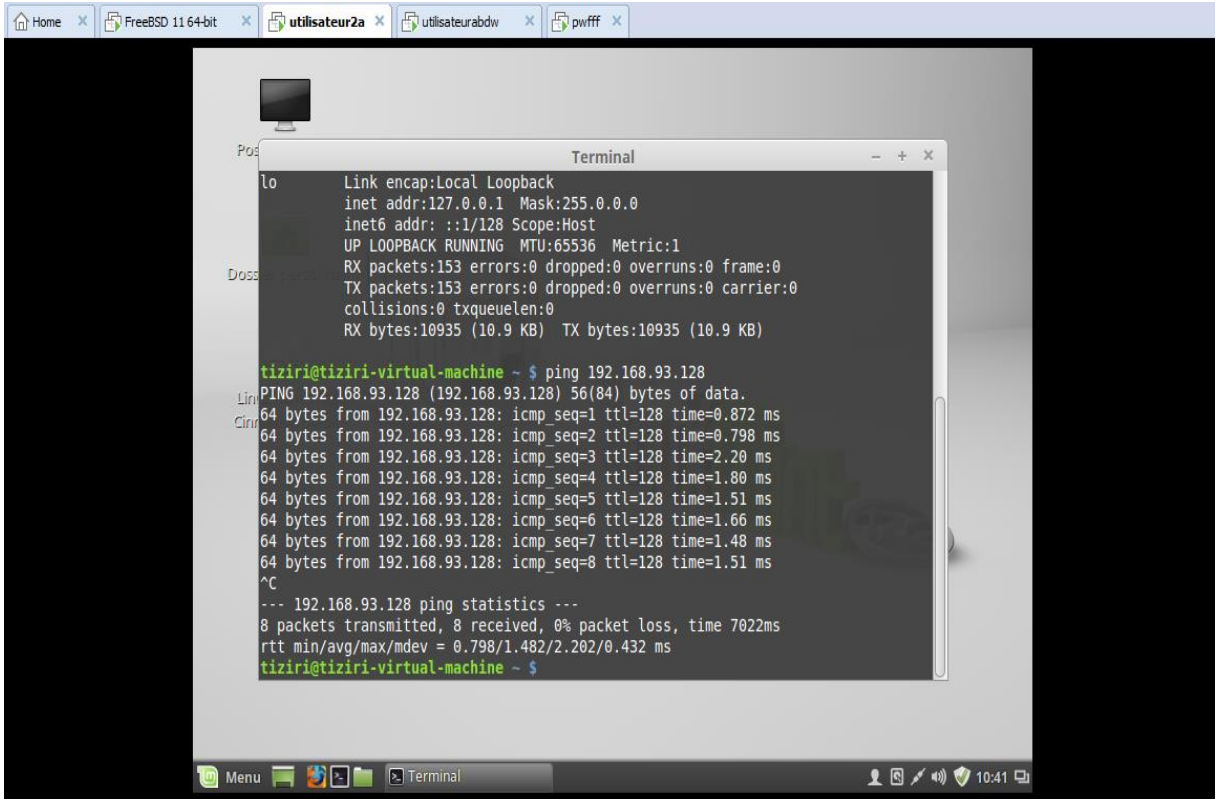

Figure 4.28 :l'envoie des paquets depuis le site de Targa au site d'Aboudaou.

Dans la figure qui suit nous allons tester la transmission des paquets envoyés depuis le site d'Aboudaou au site de Targa.

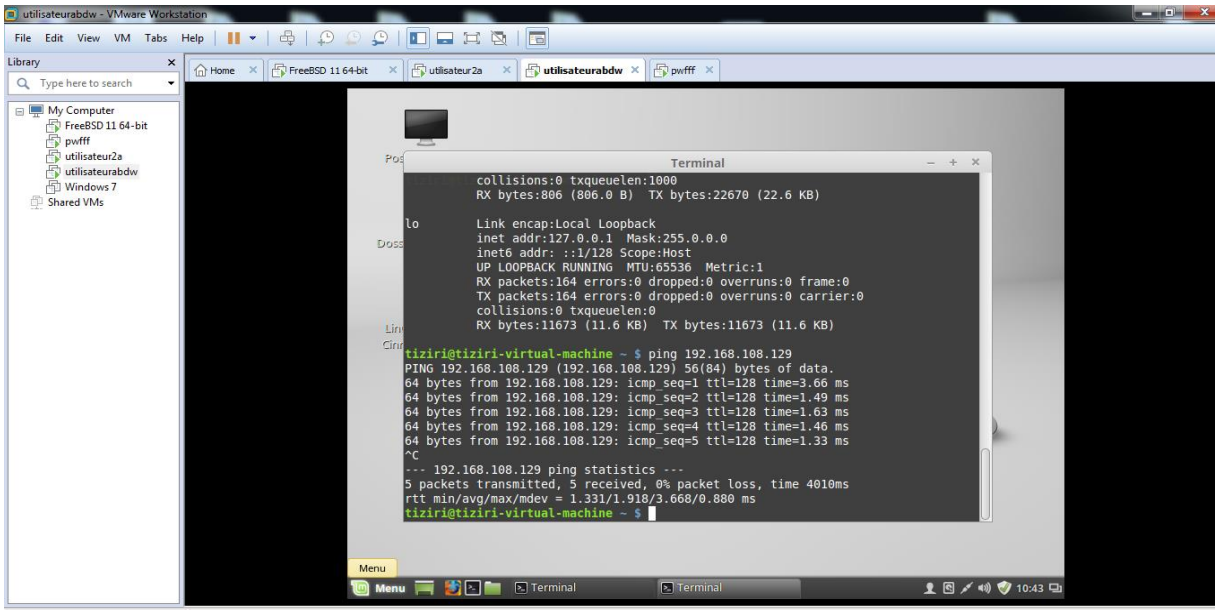

Figure 4.29 :l'envoie des paquets depuis le site d'Aboudaou au site de Targa.

4.4.2.2 Configuration des VPN accès distant

Le but de cette partie, est d'offrir un accès distant aux ressources existantes pour tous les utilisateurs nomades, en se basant sur un certificat couplé à un login et un mot de passe.

❖ **Création d'une autorité de certification**

Dans le menu « System », nous cliquons sur « Cert Manager », puis nous remplissons les champs utiles.

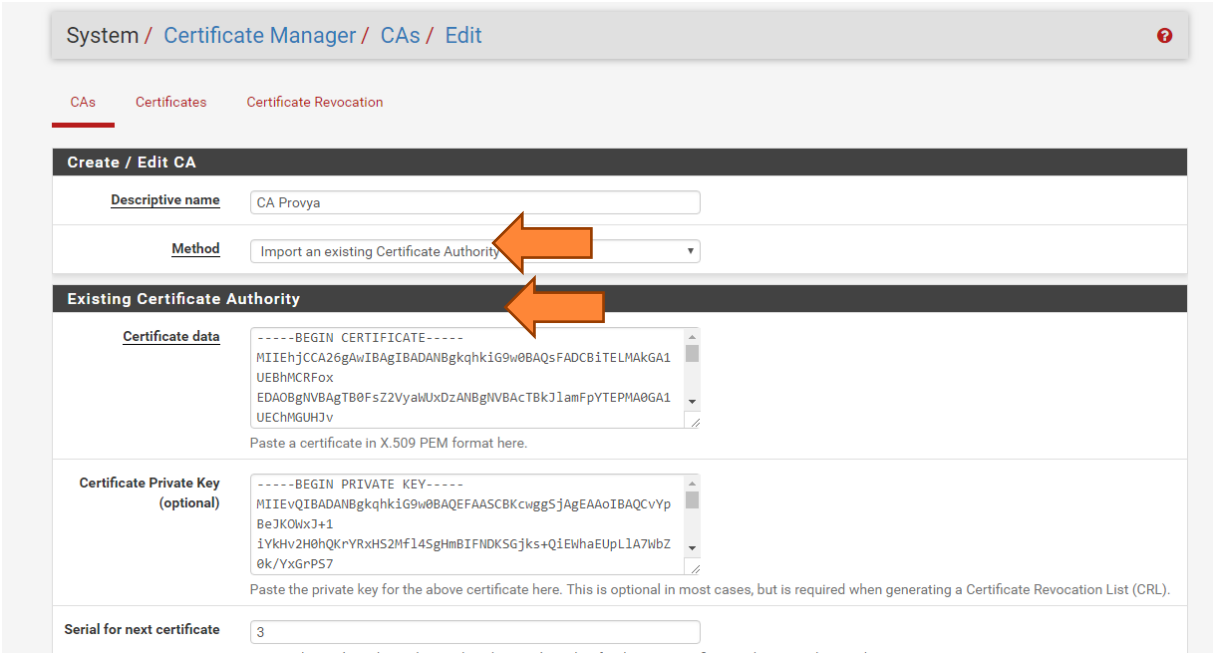

Figure 4.30 : L'interface de création d'une autorité de certification.

Notre autorité de certification est représentée dans la figure suivante :

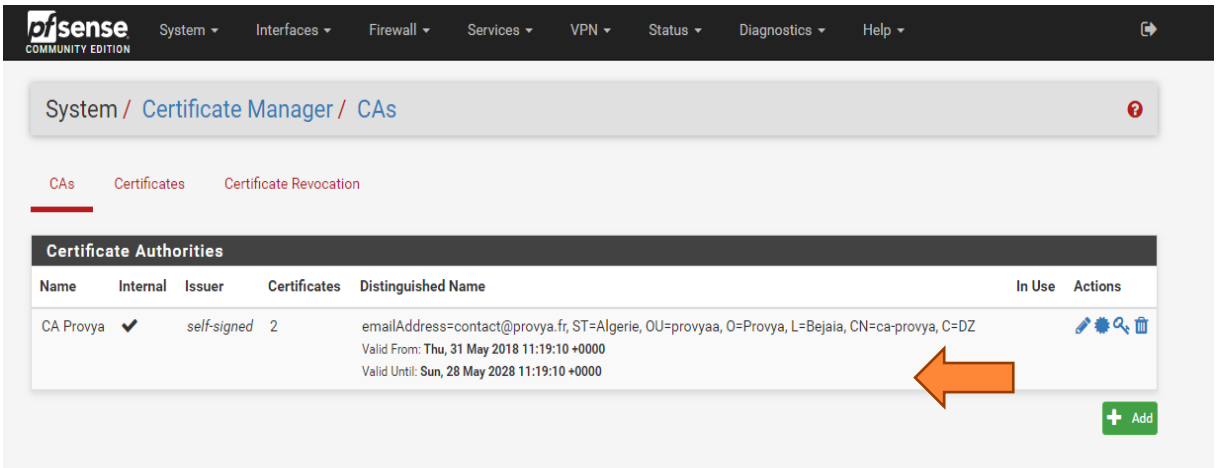

Figure 4.31: l'interface dédiée à l'autorité de certification.

❖ Création d'un certificat serveur

Dans le menu « System » nous appuyons sur l'onglet « Cert Manager » et nous basculons sur le bouton « Certificates », puis « Add » et nous choisissons les informations adéquates à notre configuration.

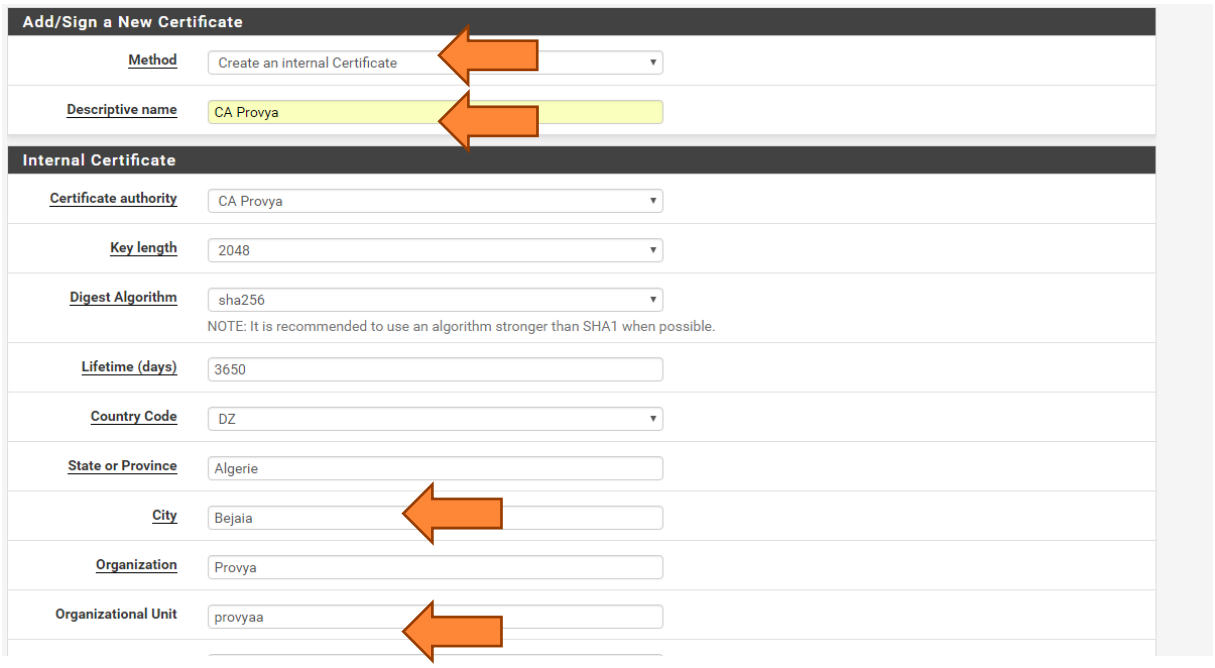

Figure 4.32 : l'interface de création d'un certificat serveur.

❖ Création d'un certificat client

Pour créer un certificat client, nous procédons de la même manière que pour la création d'un certificat serveur, mais nous choisissons le type « User Certificate » pour le champ « Certificate Type ».

A la fin nous obtenons les certificats suivants :

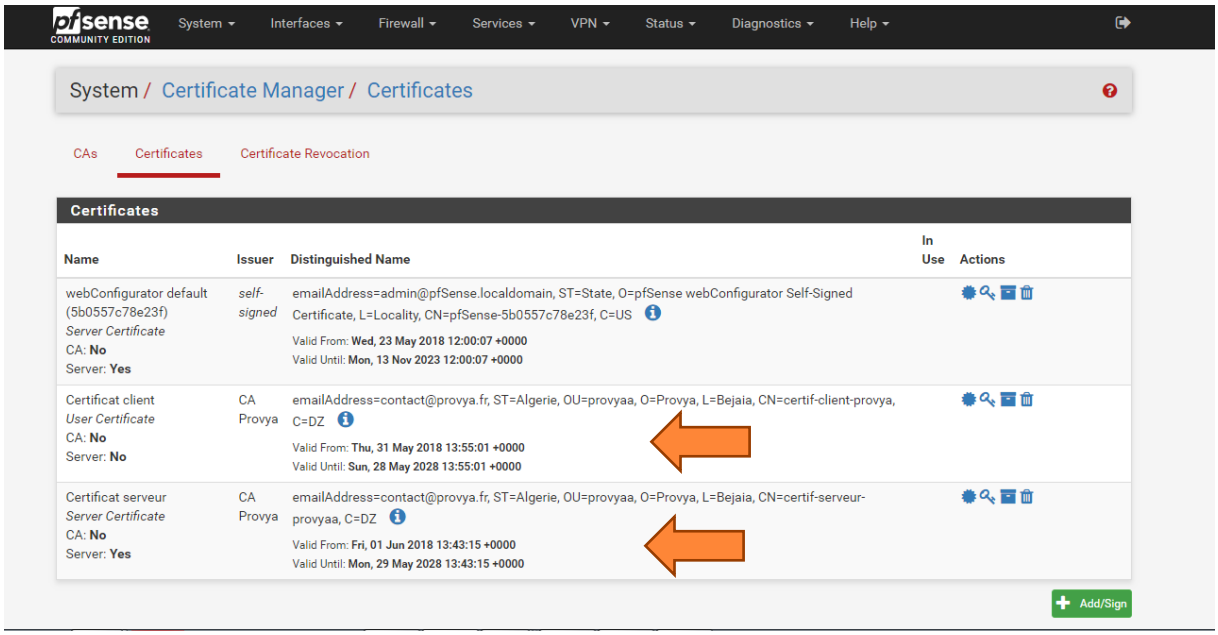

Figure 4.33 : l'interface qui illustre les certificats créés.

❖ Création des utilisateurs

Pour créer notre utilisateur, nous cliquons sur l'onglet « Users » et nous affectons à chaque champ un choix qui lui convient.

Nous affectons à chaque utilisateur un nom d'utilisateur et un mot de passe.

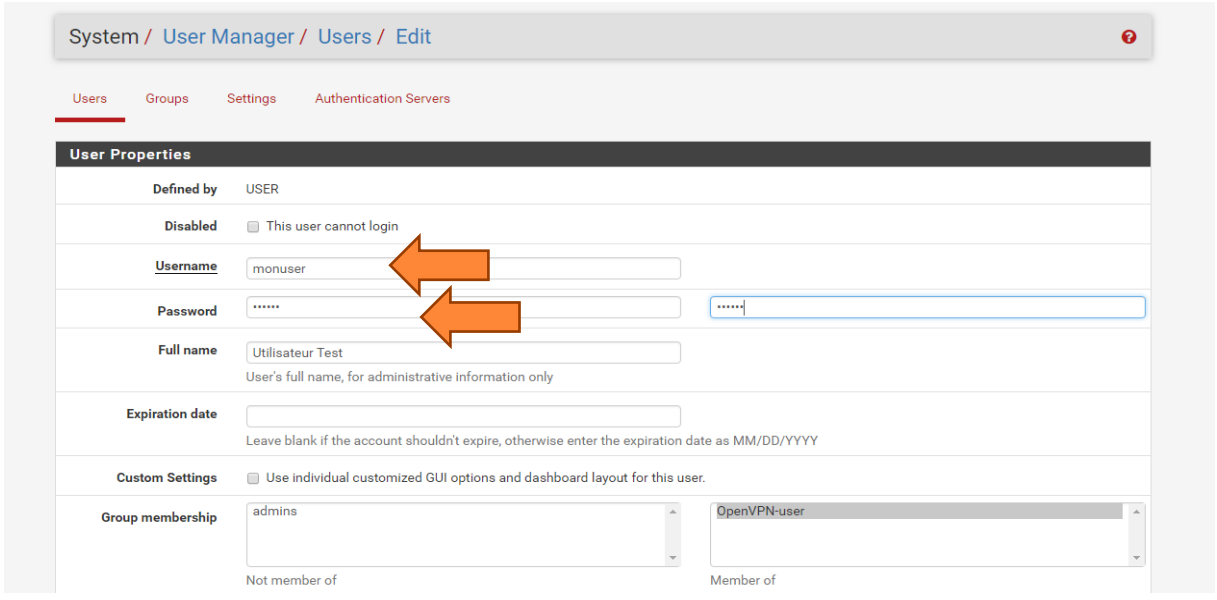

Figure 4.34 : l'interface de création d'un utilisateur.

Voici l'interface de notre utilisateur :

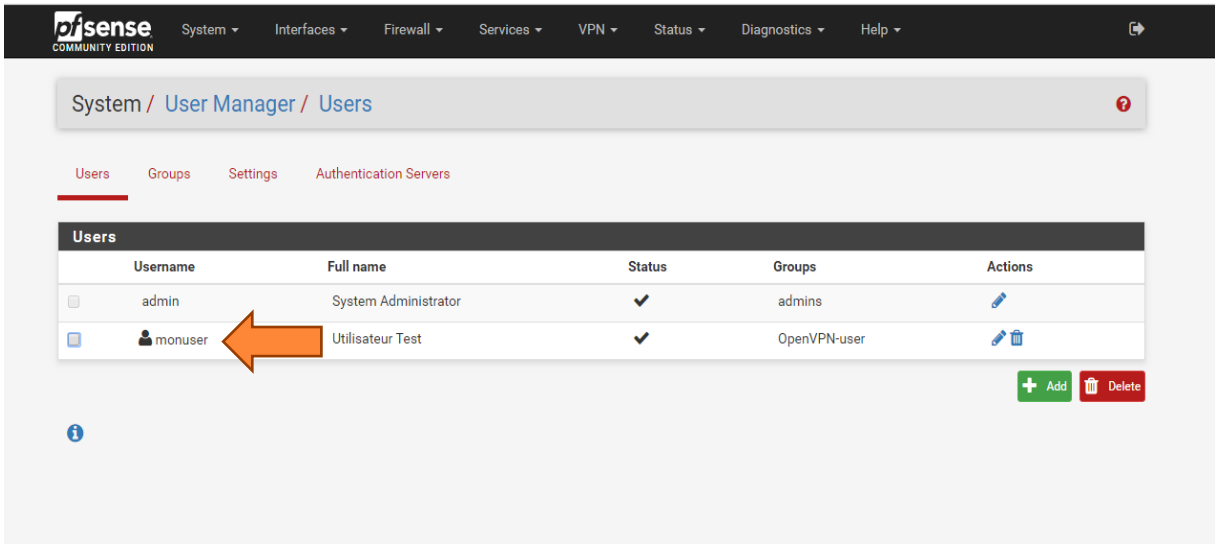

Figure 4.35 : l'interface dédiée à l'utilisateur.

❖ Création du serveur OpenVPN

La création se fait comme dans la partie « site à site », sauf que dans le champ « Server mode » on choisit « Remote Access ».

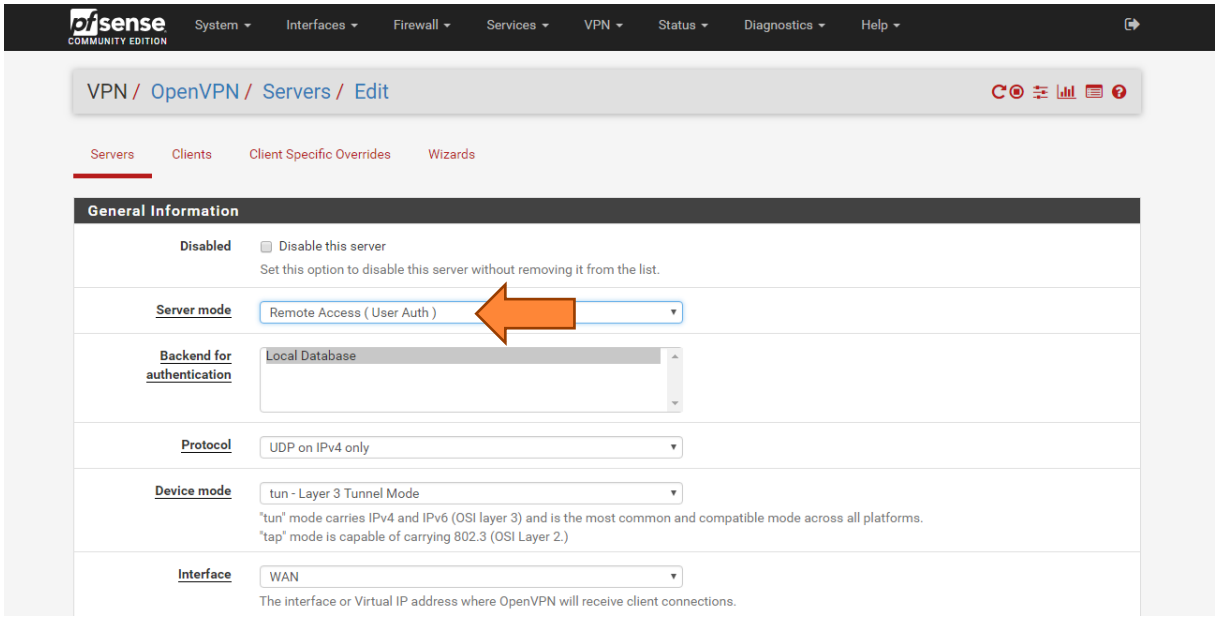

Figure 4.36 : l'interface dédiée au serveur OpenVPN.

❖ Téléchargement du package OpenVPN

Il nous reste maintenant, à télécharger le package « OpenVPN ». Pour cela, rendez-vous sur l'onglet « System », puis « Package Manager », puis nous cliquons sur « Avalaible Package » et on lance le téléchargement.

.

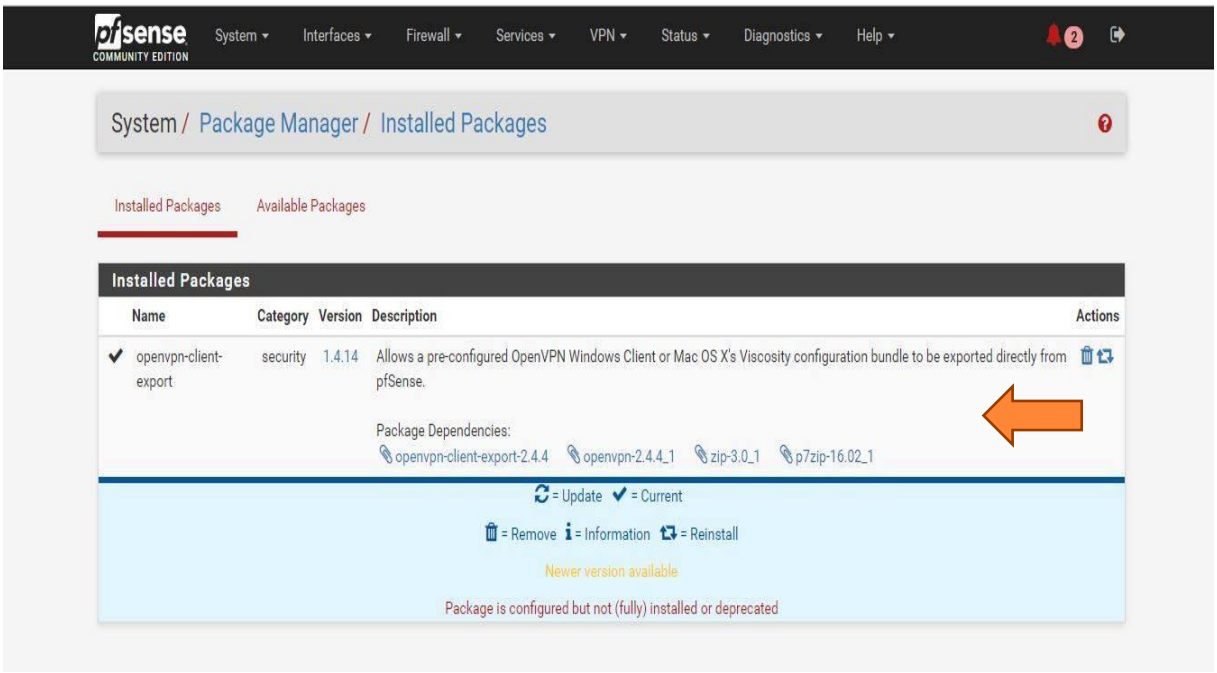

Figure 4.37 :l'installation du package OpenVPN.

La figure ci-dessous illustre le téléchargement de « Windows Vista and Later ».

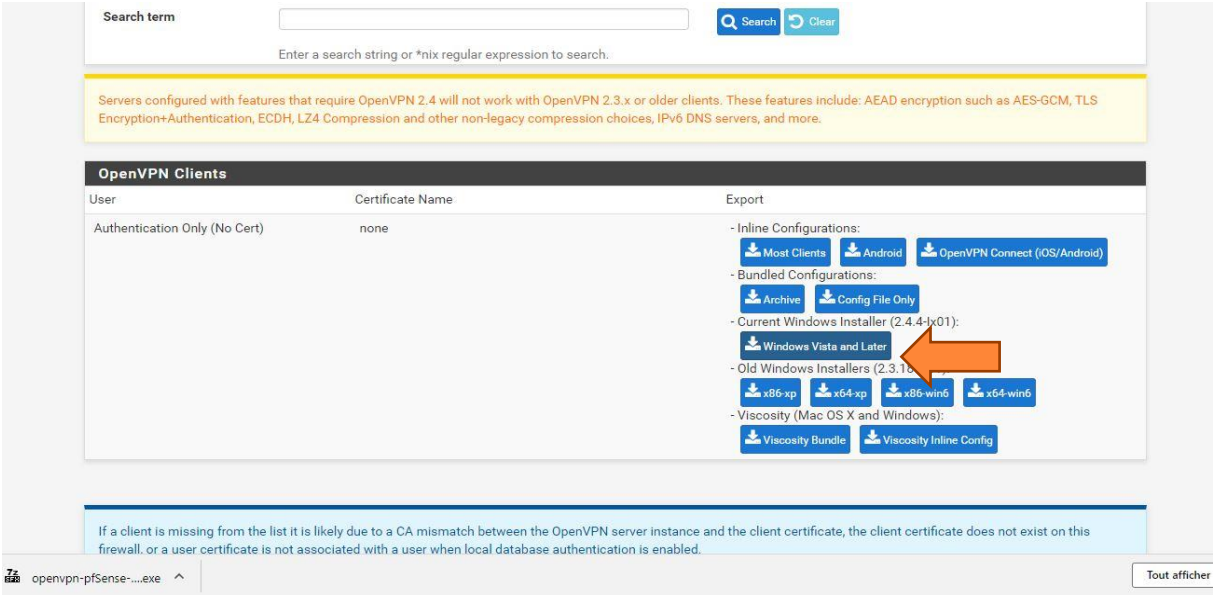

Figure 4.38 : le téléchargement de « Windows Vista and Later ».

Après l'installation, nous pouvons percevoir« OpenVPN » sur le bureau de notre Windows, maintenant nous essayons de pinger pour voir la transmission des paquets.

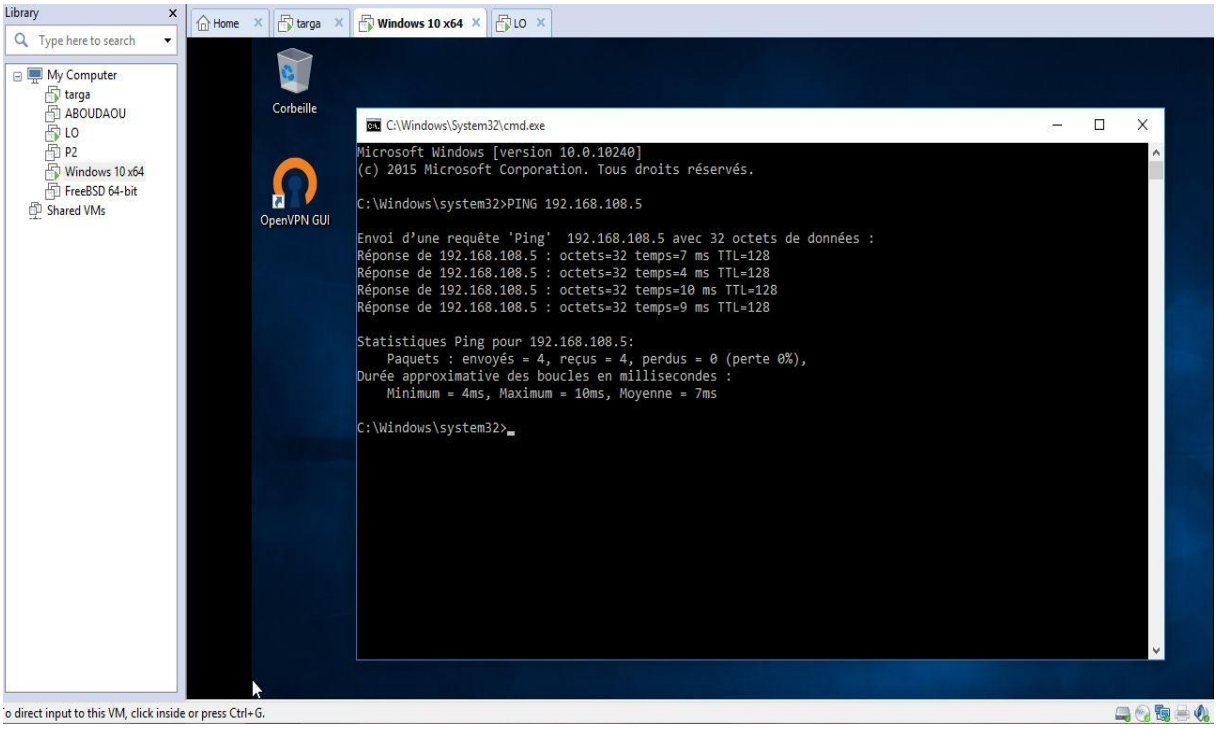

Figure 4.39: l'interface du test de connectivité.

La figure ci-dessous présente l'interface qui permet à l'utilisateur de s'authentifier pour pouvoir accéder à distance

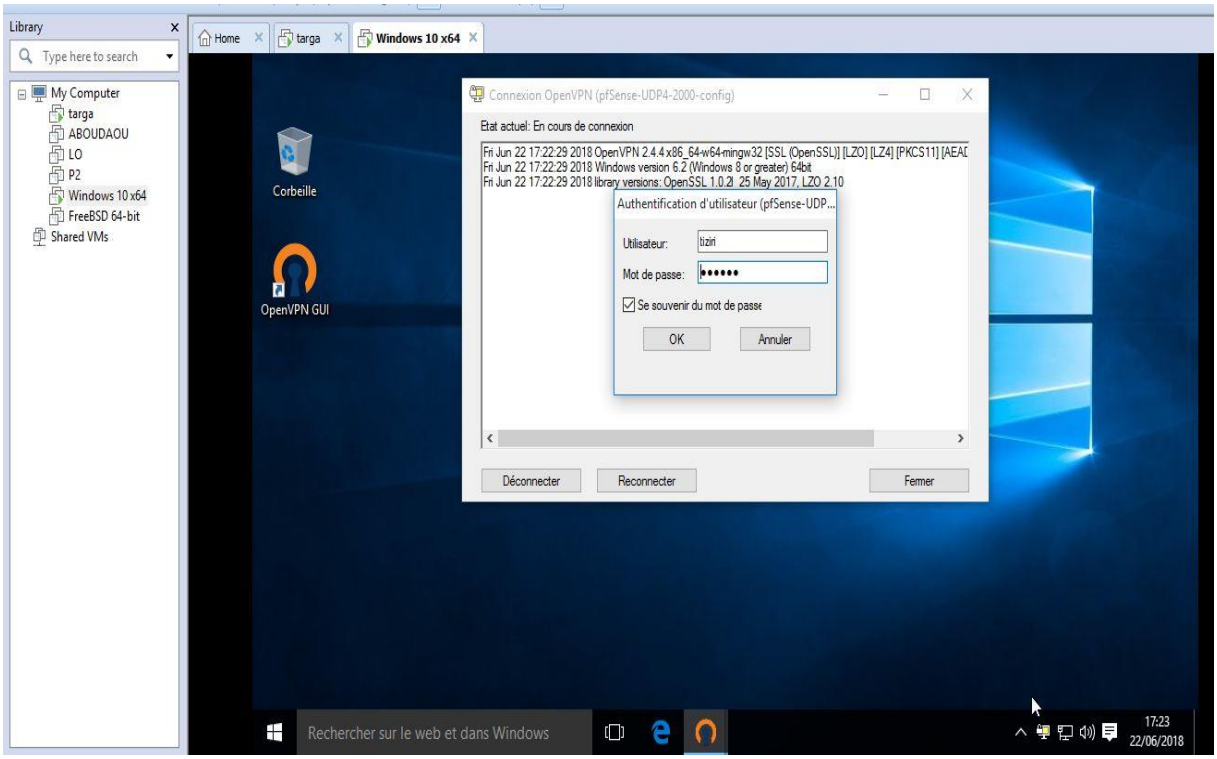

Figure 4.40: l'interface d'authentification d'un utilisateur nomade

.

La figure ci-dessous, montre la réussite de l'utilisateur à se connecter à distance à travers le tunnel qui s'affiche lors de la connexion.

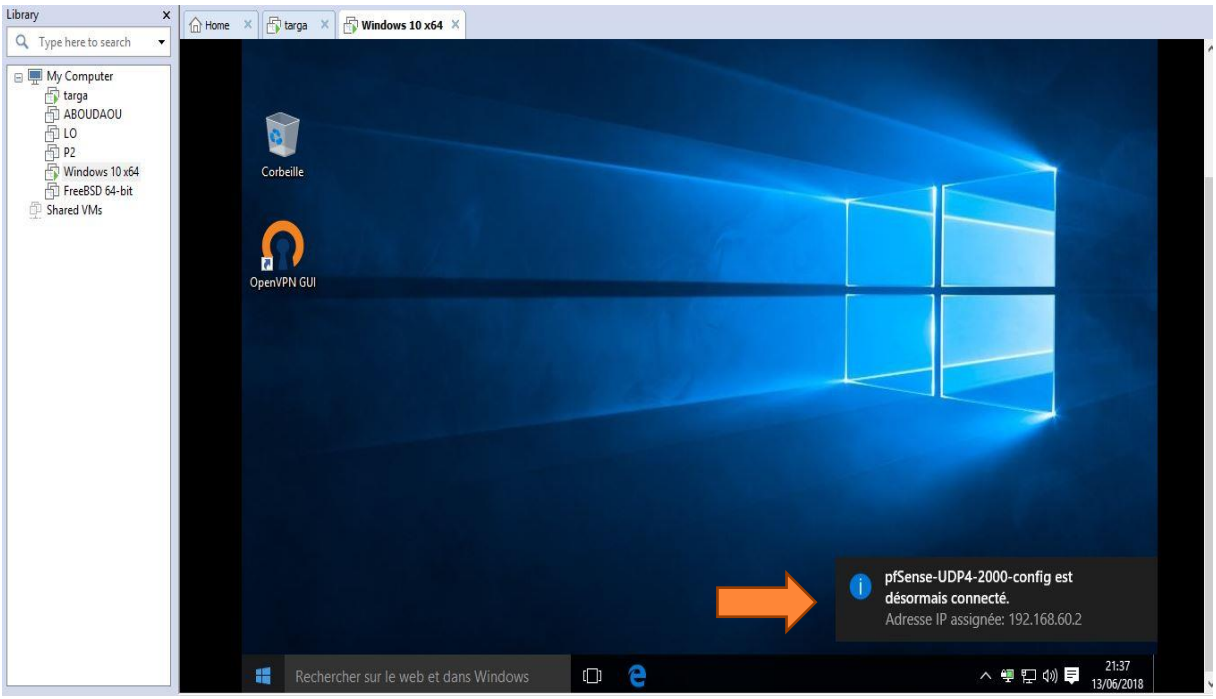

Figure 4.41: la connexion à distance d'un utilisateur nomade.

4.5. Conclusion

Dans ce chapitre, nous avons commencé par introduire l'environnement de travail, ensuite nous avons présenté brièvement la solution proposée qui décrit les deux types de VPN.

Enfin, sécuriser des communications entre les deux réseaux de l'université via un tunnel sécurisé et nous avons autorisé un accès distant aux utilisateurs. Nous avons pu constater cet objectif grâce aux captures ci-haut.

Conclusion général

Lors de la transmission et la réception des données entre des différentes entités, sois au sein d'une même entreprise ou avec l'extérieur, la transparence des données et le concept de confidentialité devront être garantis.

Dans notre travail, nous a avons d'abord menés une étude détaillée du réseau informatique de l'université de Bejaïa et relever les différentes insuffisances présentées en terme de sécurité.
Afin d'offrir principalement un moyen sécurisé et sûre qui permettra aux utilisateurs (enseignants, administrateurs, …) d'échanger les données entre les deux réseaux de l'université et d'accéder au réseau interne depuis l'extérieurs (leur domicile, place publiques) en passant par le réseau public, dans le but de poursuivre leurs activités sans pour autant risquer de compromettre la sécurité des ressources internes du réseau. Pour cela, nous avons en premier procédé à concevoir une nouvelle architecture du réseau, ensuite nous avons mis en place un VPN qui garantit un échange de données sécurisé entre les entités des deux réseaux et assure également un accès distant aux ressource avec un contrôle d'accès.
Ainsi la mise en œuvre du VPN s'est basée sur la solution SSL OpenVPN, qui a l'avantage d'offrir une facilité de configuration couplée à une sécurité optimale qui l'a distinguée des autres solutions VPN tout aussi efficaces mais plus complexes.
La réalisation de ce projet, nous a exigés des connaissances solides et avancées en administration et sécurité des réseaux, ce qui nous a permis de mettre en pratique les stratégies étudiées dans notre cursus universitaire, dans des livres et sur internet.

Perspectives

- La simulation du réseau avec GNS 3.
- Implémentation de la solution proposée sur les réseaux réels.

Bibliographie

[1] Jean-François Pillou, “Tout sur les réseaux et internet’’,4eme édition, Dunod 2012,2015.

[2] Pierre Erny. “LES RESEAUX INFORMATIQUES D’ENTREPRISE’’, 1998.

[3] Modèles OSI et TCP/IP valet G. novembre 2010.

[4] Philippe Atelin,“Réseaux informatiques Notions fondamentales (Normes, Architecture, Modèle OSI, TCP/IP, Ethernet, Wi-Fi,...)’’. Editions ENI, 2009.

[5] Fabrice Lemainque, “tout sur les réseaux sans fil’’, Dunod, Avril2009.

[6] Yves Lescop, ”sécurité informatique”, 2002.

[7] Nicolas Baudoin et Marion Karle, “ NT Réseaux : IDS et IPS, Rapport Ingéniorat’’, 2000.

[8] Louis Salvail, ”introduction à la sécurité informatique ”,2012.

[9]Stéphane Lohier et Aurélie Quidelleur, “le réseau internet - des services aux infrastructures’’,2010

[10] NEDJADI Yamina TIMERIDJINE Nadjette, “ Etude et configuration de liaisons virtuelles(VLAN et VPN) au sein de l'Entreprise Portuaire de Bejaia "EPB", Mémoire de fin d’études, Bejaia, 2016.

[11] TEME Edjouko.B et TIGANA Bakary, “Proposition d’une Architecture Sécurisée du Réseau Intranet del’Université´e A. Mira de Bejaia’’,Mémoire de fin d’études, Bejaia, 2007.

[12] SLIMANOU Dehia,“ Mise en place d'une solution VPN sur pare-feu Cas d'étude : Entreprise Tchin-Lait(Candia)’’ Mémoire de fin d’études, Bejaia, 2017.

[13] Jean-Paularchier,“les VPN –fonctionnement mise en œuvre et maintenance des réseaux privés virtuels

[14] Vincent Remazeilles. La sécurité des réseaux avec Cisco. Editions ENI, 2009

[15] Abid Yacine et Belhocine Meziane, “Proposition d’une architecture réseaux sécurisée pour l’université A.Mira de Bejaïa’’, Mémoire de Fin d’études , Bejaïa,2015

[16] Adrien Miller and Philippe Jean Dit Pannel. “ Sécurité avec ip : Les Solutions’’. 2003.

[17] Philippe Mathon. Windows Server 2003 : les services réseaux TCP/IP. Editions ENI, 2003.

[18] Andy Valencia, Morgan Littlewood and Tim Kolar. “Cisco layer two forwarding (protocol)" l2f"’’, Technical report, 2001.

[19] Etienne GALLET DE SANTERRE. Protocole l2tp. Techniques de l'ingénieur. Télécoms, (TE7579), 2006.

[20] markusfeilner, “OpenVPN : Building and Integrating Virtual Private Networks’’, April2006

[23] Marc-Henri PAMISEUX AND Bruno JOUSSEAUME," Pare-feu PFSENSE",4,2004

Webographie

[21] https://**www.frameip.com/vpn/**

[22] http ://www.vmware.com/fr/solutions/virtualization.html

Résumé

La sécurité des données est un paramètre très important voir crucial au sein d'une organisation, compte tenu des échanges d'informations qui se font au quotidien.

Le présent travail fait état de résultats obtenus lors de la mise en place d'un VPN distant et site-a-site sous parefeu pour l'université de Béjaia. Cela représente en première partie la liaison des deux campus Targua Ouzemour et Aboudaou. En deuxième partie, ça concerne l'accès distant d'un utilisateur vers le campus de Targua Ouzemour. Pour cela, nous avons utilisé le protocole OpenVPN très adéquat pour ce cas d'étude qui évolue dans le sens des infrastructures réseaux sécurisées et du système d'information progressant de façon exponentielle.

Après avoir vu quelques généralités sur les VPNs, nous nous sommes intéressés à un aspect plus approfondit qui est les protocoles utilisés pour sa création. Parmi ces protocoles nous avons pu choisir SSL pour ses qualités afin de l'utiliser pour la réalisation de notre projet.

Mots clés : VPN, Accès distant, Site-a-site, Pare-feu, Openvpn, SSL.

Abstract

Data security is a very important and crucial parameter within an organization, given the daily exchange of information.

The present work reports results obtained when setting up a remote and site-a-site firewall VPN for the University of Bejaia. This represents in the first part the link between the two Targua Ouzemour and Aboudaou campuses. In the second part, it concerns the remote access of a user to the Targua Ouzemour campus. To do this, we have used the OpenVPN protocol, which is very suitable for this case study, which is evolving in the direction of secure network infrastructures and the information system progressing exponentially.

After seeing some generalities about VPNs, we are interested in a more in-depth aspect which is the protocols used for its creation. Among these protocols we have been able to choose SSL for its qualities in order to use it for the realization of our project.

Keys words: VPN, Remote Access, Site-to-Site, Firewall, Openvpn, SSL.