REPUBLIQUE DU BENIN

****

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

****

INSTITUT UNIVERSITAIRE LES COURS SONOU

MEMOIRE DE FIN DE FORMATION EN LICENCE PROFESSIONNELLE

Domaine : Sciences et Technologies

Filière : Sécurité des Systèmes et Réseaux Informatique (SSRI)

THEME :

TOUT SUR LE VPN : CONFIGURATION ET DÉPLOIEMENT

TOUT SUR LE VPN : Configuration et déploiement

Réalisé par :

ASSOGBA Ninon Gael B.

&

HOULONON Hans

Maitre Mémoire :

Dr. Ing Hospice OLUBI

Enseignant chercheur

Expert en Sécurité Informatique

Maitre Stage :

M. Sarlas ALLADAYE

ANNEE-ACADEMIQUE : 2024-2025

ENGAGEMENT

L'institut Universitaire « Les Cours Sonou » n'entend donner aucune approbation ni improbation aux opinions émises dans ce mémoire. Ces opinions doivent être considérées comme propres à leur auteur.

DEDICACE 1

Je dédie ce mémoire à :

- Mon Père Sébastien A. ASSOGBA ;
- Ma Mère Célestine Y. ADJE ;
- Mes frères (Luc, Arnaud, Marie-Laurent).

DEDICACE 2

Je dédie ce mémoire à :

- Mon Père HOULONON A. Janvier ;
- Ma Mère LOUGBEHON Christine ;
- Mes sœurs.

REMERCIEMENT

Nous remercions l'Eternel Dieu tout-puissant pour sa protection et ses grâces infinies, pour son assistance tout au long du stage et dans la rédaction du présent mémoire.

Nous tenons également à remercier :

♣ Monsieur Fabrice SONOU, Président Directeur Général de l'Institut Universitaire Les Cours SONOU, ainsi que tous les autres membres de l'administration pour m'avoir mis dans de bonnes conditions afin que je suive une formation de qualité ;

♣ Tous les enseignants de l'Institut Universitaire Les Cours SONOU pour la qualité de l'enseignement que nous recevons d'eux ;

♣ Monsieur OLUBI Hospice notre directeur de mémoire, pour sa rigueur, sa patience, sa disponibilité et pour avoir accepté de nous orienter dans l'accomplissement de ce travail en dépit de ses nombreuses responsabilités ;

♣ Monsieur SARLAS ALLADAYE, Directeur Général de TPAPY, pour m'avoir accepté dans ses locaux pour mon stage, et avoir mis à ma disposition tout ce dont j'avais besoin pour le bon déroulement de mon travail ;

♣ Monsieur OLOUBO Abdel pour leurs nombreux conseils et appuis techniques tout au long de la réalisation de notre projet de fin d'étude.

♣ Les membres du jury, et nous exprimons notre sincère gratitude pour le temps et l'attention consacrés à évaluer notre mémoire, ainsi que pour vos précieux commentaires et suggestions.

♣ Tous nos camarades de la filière SSRI et à tous ceux qui, de près ou de loin ont contribué à la mise en œuvre de ce document.

LISTES DES SIGLES ET ABBREVIATIONS

A.R.P : Address Résolution Protocol

A.C.L : Access Control List

B.N.C : Bayonet Neill-Concelman

C.S.M.A/C.D : Carrier Sense Multiple Access with Collision Detect

D.N.S : Domain Name System

M.P.L.S : Multi Protocol Label Switching

F.D.D.I : Fiber Distributed Data Interface

F.T.P : File Transfer Protocol

S.M.F : Single Mode Fiber

L.A.N : Local Area Network

P.A.N : Personal Area Network

M.A.N : Métropolitain Area Network

W.A.N : Wide Area Network

H.T.T.P : HyperText Transfer Protocol

I.C.M.P : Internet Control Message Protocol

I.P : Internet Protocol

T.C.P : Transmission Control Protocol

U.D.P : User Datagram Protocol

S.M.T.P : Simple Mail Transfer Protocol

S.T.P : Shielded Twisted Pair

N.N.T.P : Network News Transfer Protocol

M.A.C : Media Access Control

D.L.C.I : Data Link Connection Identifier

L.L.C : Layer Link Control

P.D.U : Protocol Data Unit

I.A.N.A : Internet Assigned Numbers Agency

V.L.A.N : Virtual Local Area Network

N.A.T : Network Address Translation

N.A.S : Network Access Server

P.P.T.P : Point to Point Tunneling Protocol

L.2.F : Layer 2 Forwarding

L.2.T.P : Layer 2 Tunneling Protocol

M.P.P.E : Microsoft Point to Point Encryption

G.R.E : Generic Routing Encapsulation

P.P.P : Point-to-Point

O.S.I : Open Systems Interconnection

U.T.P : Unshielded Twisted Pair

LISTES DES FIGURES ET ILLUSTRATIONS

LISTES DES TABLEAUX

RESUME

Notre projet consiste à mettre en place un réseau privé virtuel (VPN) client-to-site. A cet effet, seul un réseau privé virtuel a la capacité de permettre à des employés distants d'accéder de manière sécurisée au réseau local de l'entreprise. Pour cela, nous avons utilisé notre machine comme client, ce qui nous a permis de nous connecter à travers OpenVPN au réseau de l'entreprise, nous avons également disposer d'une machine nous a permis d'héberger notre serveur VPN sous pfsense. Enfin, nous avons effectués des tests de pings pour vérifier la connectivité réseau.

Mots-clés : VPN, OpenVPN, VPN Client-to-site, Pfsense.

ABSTRACTS

Our project involves setting up a client-to-site virtual private network (VPN). Only a VPN can provide remote employees with secure access to the company's local network. To this end, we used our machine as a client, enabling us to connect via OpenVPN to the corporate network, and we also had a machine that enabled us to host our VPN server under pfsense. Finally, we carried out ping tests to verify network connectivity.

Key words : VPN, OpenVPN, VPN Client-to-site, Pfsense.

SOMMAIRE

INTRODUCTION GENERALE

1. Contexte et justification :

De nos jours, la communication dans un réseau informatique est indispensable pour toute entreprise. A l'origine, la communication était simple du fait qu'une société était composée d'une seule entité ou de plusieurs entités géographiquement proches. Mais suite au progrès considérable de la communication, les menaces et les besoins sont apparus lorsque celles-ci ont commencé à s'implanter sur plusieurs sites, tout autour d'un pays ou même à l'étranger ce qui rend ainsi la transmission d'informations plus complexes, lente et parfois non-sécurisée. Et comme tout progrès engendre de nouveaux défis, il est devenu important de mettre en place des moyens de connectivités sécurisées, afin d'assurer à la fois l'intégrité, la confidentialité et la disponibilité des données échangées. Le VPN (Virtual Private Network) s'est alors imposé comme une réponse fiable et économique à ces nouveaux défis. Il permet aux entreprises de relier de manière sécurisée leurs différentes implantations à travers Internet, tout en donnant la possibilité aux employés nomades ou en télétravail d'accéder aux ressources internes, comme s'ils étaient physiquement dans les locaux de l'entreprise.

2. Problématique :

Dans un contexte de transformation numérique accélérée au Bénin, les entreprises plus précisément les PME sont de plus en plus exposées aux cyberattaques et aux risques liés à la confidentialité des échanges de données. Face à l'essor du télétravail et des connexions à distance, l'usage des VPN est devenu une nécessité pour garantir la sécurité des communications et des ressources internes. Cependant, plusieurs défis freinent l'adoption efficace des VPN par les entreprises béninoises :

- **Manque d'expertise technique** : De nombreuses PME ne disposent pas de personnel qualifié pour configurer et gérer un VPN sécurisé.
- **Coût élevé des solutions existantes** : Les solutions commerciales comme Cisco AnyConnect ou Fortinet VPN sont souvent hors de portée des budgets des entreprises locales.

- **Problèmes d'infrastructure** : La qualité fluctuante de la connexion Internet au Bénin peut impacter les performances des VPN.
- **Menaces croissantes** : Les entreprises béninoises sont de plus en plus ciblées par des cyberattaques, notamment des intrusions réseau et du vol de données.

Dans ce contexte, il est essentiel de proposer une solution VPN adaptée aux réalités des entreprises béninoises, permettant à la fois de sécuriser leurs communications et de rester accessible en termes de coût et de complexité d'implémentation.

3. Objectifs :

✓ **Objectif général :**

L'objectif est de configurer et déployer un VPN sécurisé et optimisé pour les entreprises béninoises, en prenant en compte les défis liés aux infrastructures locales et aux besoins spécifiques en matière de cybersécurité.

✓ **Objectifs spécifiques :**

➢ Étudier les différents types de VPN et leurs implications en entreprise.

➢ Implémenter un VPN en environnement simulé et évaluer sa performance dans des conditions similaires à celles du Bénin.

➢ Mettre en place des mécanismes de sécurité adaptés aux menaces locales (intrusions, phishing, attaques MiTM).

➢ Proposer une solution accessible et documentée pour faciliter l'adoption des VPN par les entreprises locales.

4. Organisation du mémoire :

Afin de présenter notre travail, nous avons structuré notre mémoire en trois chapitres :

Le premier chapitre consiste à faire part de quelques notions fondamentales à savoir sur l'architectures des réseaux informatiques et leurs sécurités. Quant au deuxième chapitre, il est consacré à l'étude du réseau privé virtuel (VPN), les différentes topologies et architecture du réseau ainsi que protocoles utilisés afin de garantir la sécurité et

confidentialité du réseau. Ensuite, le troisième chapitre portera sur la mise en place d'un réseau VPN dans un environnement simulé, avec les étapes de déploiement, les tests réalisés et l'analyse des résultats. Enfin, une conclusion générale vient clôturer ce mémoire, résumant les éléments essentiels qui ont été abordé

CHAPITRE I : PRESENTATION DE LA STRUCTURE D'ACCUEIL

PRESENTATION DE LA STRUCTURE DE BLUE LIFE TECH (BLT)

BLUE LIFE TECH est une entreprise spécialisée dans une large gamme de services technologiques et d'expertise. Nous proposons des solutions adaptées aux besoins de nos clients dans les domaines du génie logiciel, de la maintenance, du graphisme, de la communication, de l'électricité et de l'énergie, des réseaux informatiques et de la sécurité, ainsi que des formations.

Dans le domaine du génie logiciel, notre équipe qualifiée est prête à concevoir et à réaliser des sites web, des applications mobiles et desktop, en respectant vos exigences et vos objectifs. Nous offrons également des services d'assistance et de conseil en génie logiciel, ainsi que la maintenance et l'hébergement de vos sites et applications.

La maintenance est un aspect essentiel pour garantir le bon fonctionnement de vos équipements technologiques. Nous nous occupons de la maintenance et de l'entretien de vos ordinateurs, onduleurs, téléphones portables et autres appareils électroniques. Nous assurons également l'installation de logiciels et de systèmes d'exploitation, ainsi que les mises à jour nécessaires pour maintenir vos équipements à jour.

Notre expertise en graphisme vous permet de bénéficier de créations visuelles de qualité. Nous concevons et réalisons des maquettes, des logos, des flyers, des dépliants, des bâches, des cartes de visite, des spots publicitaires, des jingles et des montages vidéo. Notre objectif est de donner une identité visuelle attrayante à votre entreprise et de vous aider à vous démarquer. La communication est un élément clé pour promouvoir votre entreprise. Nous vous accompagnons dans la gestion de vos pages sociales, la réalisation de campagnes publicitaires, ainsi que l'envoi de mails et de messages WhatsApp ciblés pour atteindre votre audience de manière efficace.

L'électricité et l'énergie sont des domaines dans lesquels nous excellons également. Nous proposons des services de dimensionnement et d'installation de réseaux électriques, ainsi que des solutions de maintenance électrique pour assurer la sécurité et la performance de vos installations. De plus, nous sommes spécialisés dans l'installation de panneaux solaires, que ce soit en site isolé ou en autoconsommation, vous permettant ainsi de bénéficier d'une source d'énergie renouvelable et économique.

Pour assurer une connectivité fiable et sécurisée, nous proposons des services de configuration de réseaux informatiques et de sécurité. Notre expertise comprend la configuration

des caméras analogiques et IP, la mise en place de routeurs Mikrotik et de nanostations M2 et M5, ainsi que d'autres équipements essentiels pour garantir un réseau performant et sécurisé.

Enfin, nous sommes fiers de proposer des formations dans divers domaines. Que ce soit pour apprendre à utiliser les outils de développement web, mobile et desktop, les outils de graphisme et de montage vidéo, ou pour acquérir des compétences en maintenance informatique et en conception d'intelligences artificielles, nous sommes là pour vous accompagner et vous permettre d'élargir vos connaissances et vos compétences.

Chez BLUE LIFE TECH, notre objectif est de fournir des solutions technologiques complètes et adaptées à vos besoins, en vous accompagnant à chaque étape. Nous mettons à votre disposition notre expertise en matière de développement full stack avec des Frameworks tels que Laravel et Symfony. Nous concevons des applications web performantes et sécurisées, répondant à vos besoins spécifiques.

Pour les passionnés de développement mobile, nous proposons des formations sur Flutter, vous permettant de créer des applications mobiles à la fois pour Android et iOS avec une seule base de code. Vous pourrez ainsi atteindre un large public avec des applications élégantes et fluides.

Notre équipe de graphistes qualifiés est spécialisée dans l'utilisation d'outils tels que Adobe After Effects, Illustrator, Photoshop et Canvas. Nous créons des designs uniques et percutants, allant des animations vidéo aux illustrations vectorielles en passant par la retouche photo.

En matière de bureautique, nous proposons des formations sur les logiciels incontournables tels que Microsoft Word, Excel et PowerPoint. Vous apprendrez à maîtriser ces outils essentiels pour améliorer votre productivité et optimiser vos tâches quotidiennes.

Enfin, nous offrons également des services de conseil en stratégie digitale, d'analyse de données, d'optimisation SEO et de gestion de projet. Nous vous accompagnons dans la définition de vos objectifs et dans la mise en place des meilleures pratiques pour assurer votre succès dans l'environnement numérique.

- **Direction Générale**

  Le Directeur Général est le responsable principal de l'entreprise. Il définit la stratégie globale de l'entreprise, prend des décisions importantes et supervise toutes les activités ;

L'Assistant(e) de Direction soutient le Directeur Général dans ses fonctions administratives et organisationnelles. Il peut être chargé de la planification des réunions, de la gestion des calendriers et de la correspondance, ainsi que de la coordination des projets ;

- **Secretariat**

Le Chef(fe) de Secrétariat est responsable de la gestion efficace du secrétariat de l'entreprise. Il supervise les tâches administratives quotidiennes et assure un fonctionnement fluide du bureau ;

L'Assistant(e) Administratif(ive) aide le Chef(fe) de Secrétariat dans ses tâches, telles que la gestion des appels téléphoniques, la rédaction de courriers et la coordination des rendez-vous.

- **Département Commercial et Marketing**

Le Chef(fe) des Ventes dirige l'équipe commerciale de l'entreprise. Il élabore des stratégies de vente, supervise les performances des ventes et assure le développement de nouveaux marchés. - Les Commerciaux sont chargés de promouvoir les produits et services de l'entreprise, de conclure des ventes et de fidéliser la clientèle.

- Le Chargé(e) de Marketing est responsable de la planification et de la mise en œuvre des stratégies marketing de l'entreprise, y compris la publicité, la promotion des ventes et le marketing digital.

- Le Community Manager gère les interactions de l'entreprise sur les réseaux sociaux, crée du contenu engageant et assure la gestion de la réputation en ligne de l'entreprise.

- **Département Technique**

Le Directeur(trice) Technique supervise les activités techniques de l'entreprise, notamment le développement de logiciels, la maintenance informatique, la conception graphique et les services d'électricité et d'énergie.

- Les membres de l'équipe technique, tels que les Ingénieurs Logiciels, les Développeurs Web et Mobile, les Graphistes, les Techniciens en Maintenance, les Installateurs Électriciens et les Administrateurs Réseau, sont spécialisés dans différents domaines techniques et contribuent à la réalisation des projets de l'entreprise.

- **Département Formation**

Le Responsable Formation est chargé de concevoir et de mettre en œuvre les programmes de formation de l'entreprise. Il identifie les besoins en formation, planifie les sessions de formation et évalue les résultats.

- Les Formateurs dispensent les formations aux employés et aux clients de l'entreprise. Ils possèdent une expertise dans leur domaine et utilisent des méthodes pédagogiques efficaces pour transmettre des connaissances et des compétences.

- **Administration et Finance:**

Le Responsable Administratif et Financier supervise les opérations administratives et financières de l'entreprise. Il est responsable de la gestion des ressources financières, de la comptabilité, de la facturation et de la gestion des fournisseurs.

- Le Comptable est chargé de la tenue des comptes de l'entreprise, de l'établissement des déclarations fiscales et de la préparation des rapports financiers.

- L'Assistant(e) Administratif(ive) apporte un soutien administratif au département, notamment dans la gestion des documents, la préparation des réunions et la coordination des déplacements.

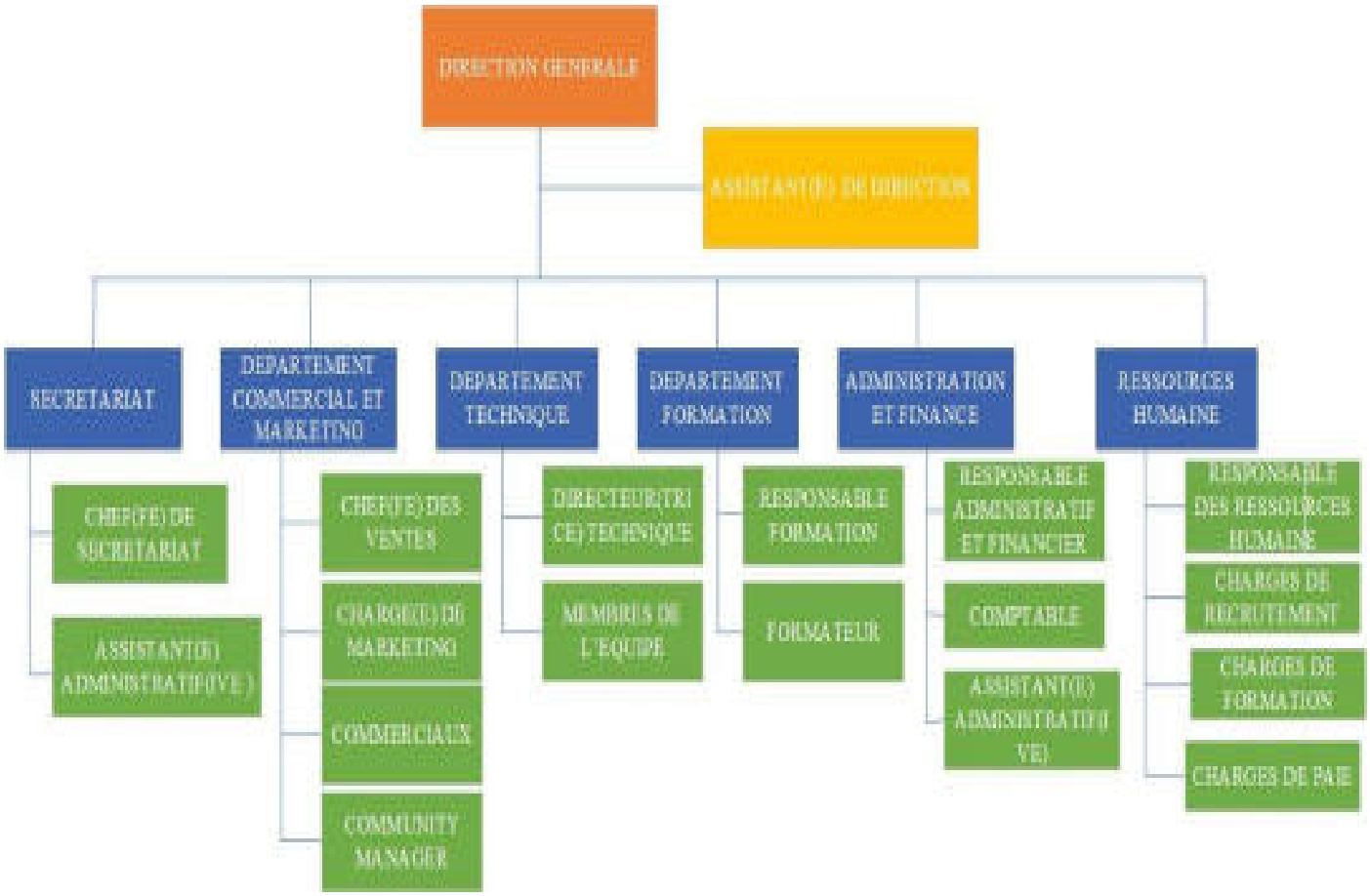
- **Ressources Humaines:**

Le Responsable des Ressources Humaines gère les ressources humaines de l'entreprise, y compris le recrutement, la gestion des talents, la formation, la paie et les relations sociales.

- Les Chargés de Recrutement sont responsables du processus de recrutement de l'entreprise, de la rédaction des offres d'emploi à la sélection des candidats.

- Les Chargés de Formation planifient et organisent les programmes de formation pour les employés, en fonction de leurs besoins en développement professionnel.

- Les Chargés de la Paie sont responsables de l'établissement des bulletins de paie, du suivi des congés et des absences, et de la gestion des avantages sociaux.



CHAPITRE II : GÉNÉRALITÉS SUR LES RÉSEAUX INFORMATIQUES

1.1 Définition d'un réseau informatique

Un réseau informatique est un ensemble d'équipements matériels et logiciels interconnectés les uns avec les autres dans le but de partager des ressources (données).

1.2 Topologie d'un réseau

On distingue deux types de topologies dans un réseau : la topologie physique et la topologie logique.

1.2.1 La topologie physique

La topologie physique c'est l'organisation physique des équipements dans le réseau c'est-à-dire comment les équipements (qu'il s'agisse de machines ou des switchs ou des routeurs, ...) sont mis et placés dans le réseau. On distingue souvent les topologies physiques suivantes :

- ✓ **Topologie en bus**

Une topologie en bus est l'organisation la plus simple d'un réseau. En effet, dans une topologie en bus tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire de câble, généralement coaxial. En effet, le mot « bus » fais référence à la ligne physique qui relie les machines du réseau. Par contre, elle est grandement vulnérable étant donné que si l'une des connexions est défectueuse, le réseau tout entier est affecté

- ✓ **Topologie en étoile :**

Dans une topologie en étoile, les ordinateurs du réseau sont connectés à un équipement central appelé concentrateur (hub). Contrairement aux réseaux construits sur une topologie en bus, les réseaux avec une topologie en étoile sont beaucoup moins vulnérables car une des connexions peut être débranchée sans affecter le reste du réseau. En revanche, le point vulnérable de ce réseau est le concentrateur, en cas de défaillance de ce dernier plus aucune communication entre les ordinateurs du réseau n'est possible.

- ✓ **Topologie en anneau :**

La topologie en anneau se caractérise par une connexion circulaire de la ligne de communication. Les informations circulent de stations en stations, en suivant l'anneau, donc dans

un seul sens. La plupart des grandes entreprises ont des réseaux en anneau, car ils sont très fiables et peuvent facilement être étendus.

✓ **Topologie maillée :**

Le réseau en maillage est une topologie de réseau dans laquelle chaque nœud est connecté à tous les autres nœuds du réseau. Cette configuration permet une transmission de données plus fiable et plus rapide, car il existe plusieurs chemins possibles entre deux nœuds. Par contre, elle est plus coûteuse et plus difficile à mettre en place que d'autres topologies de réseau. (1)

1.2.2 La topologie logique

Par contradiction à la topologie physique, la topologie logique reflète la façon dont les données transitent sur les lignes de communication. Les topologies logiques les plus courantes souvent sont : Ethernet, le Token Ring, FDDI (Fiber Distributed Data Interface)

1.3 Architectures réseaux

En agrandissant le contexte de la définition du réseau aux services qu'il apporte, il est possible de distinguer deux modes de fonctionnement :

- **Architecture d'égal à égal** (Peer to Peer parfois appelée poste à poste), dans lequel il n'y a pas d'ordinateur central et chaque ordinateur joue un rôle similaire.
- **Architecture de type client-serveur**, ou un ordinateur (serveur) fournit des services réseau aux ordinateurs clients.

1.4 Les supports de transmissions

Dans le but de relier les diverses entités d'un réseau, il est possible d'utiliser de divers supports physiques de transmission de données. L'une de ses possibilités est l'utilisation de câbles. Il existe de nombreux types de câbles, mais on distingue généralement :

- **Le câble de type coaxial**

Le câble coaxial (en Anglais coaxial cable) a longtemps été le câblage le plus utilisés, pour le simple fait qu'il soit peu coûteux et facilement manipulable (poids, flexibilité, …). Un câble coaxial est composé d'une partie centrale (appelée âme), c'est-à-dire un fil de cuivre, enveloppé dans un isolant, puis d'un blindage métallique tressé et enfin d'une gaine extérieure.

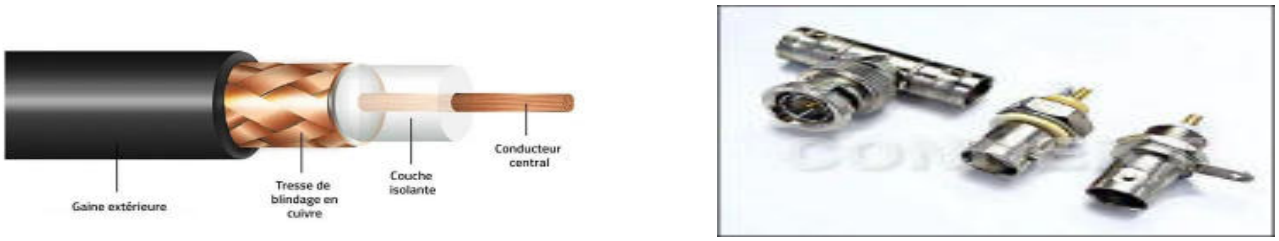


Figure 1 : Câble coaxial et le connecteur BNC

La capacité de transmission d'un câble coaxial dépend à la fois de sa longueur et des caractéristiques physiques de ses conducteurs ainsi que son isolant. Il existe deux grands types de câbles coaxiaux :

- ✓ Le câble coaxial fin (Thinnet ou 10base 2) : est un câble de diamètre de 6mm et peut transmettre un signal sur une distance d'environ de 185 mètres.
- ✓ Le câble coaxial épais (Thicknet ou 10base5) : thick Ethernet, il est de diamètre de 12mm et peux transmettre jusqu'à 500mètre sa bande passante est de 10Mb/s.

Le thinnet et le thicknet utilisent tous deux des connecteurs BNC (Bayonet Neill concelman) servant à relier les câbles aux ordinateurs. (3)

- ➢ **La paire torsadée**

Dans sa forme la plus simple, le câble à paire torsadée (twisted pair cable) est composé de deux brins de cuivre entrelacés de torsade et recouverts principalement que d'isolant. Le câble est pour la plupart du temps fabriqué à partir de plusieurs paires torsadées regroupées et placer à l'intérieur de la gaine productrice.

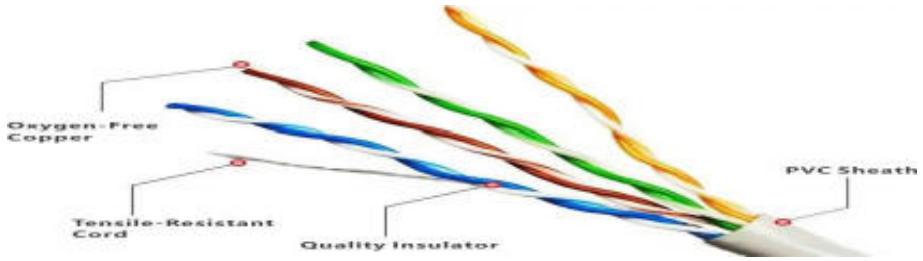


Figure 2 : Câble a paire torsadée

L'entrelacement permet de supprimer les bruits (interférences électriques) dus aux paires adjacentes ou aux autres sources (moteur, relais, transformateur…). En réseau informatique, on distingue plusieurs types de câbles à paires torsadées, UTP et STP sont les plus utilisées et les plus répondu pour les réseaux locaux. (3)

- **La paire torsadée non blindées (UTP)**

  Les caractéristiques de l'UTP :

  - l'UTP est composé de deux fils de cuivre recouverts d'isolant.
  - la longueur maximale d'un segment est de 100 mètres.

- **La paire torsadée blindées (STP)**

Le câble STP utilise une gaine de cuivre de meilleure qualité et plus protectrice que celle utilisé par le câble UTP. Les caractéristiques de ce câble :

- Les fils du cuivre d'une paire sont eux même torsadée ce qui fournit un excellent blindage pour le STP.

- Il permet une transmission plus rapide et sur une longue distance. (3)

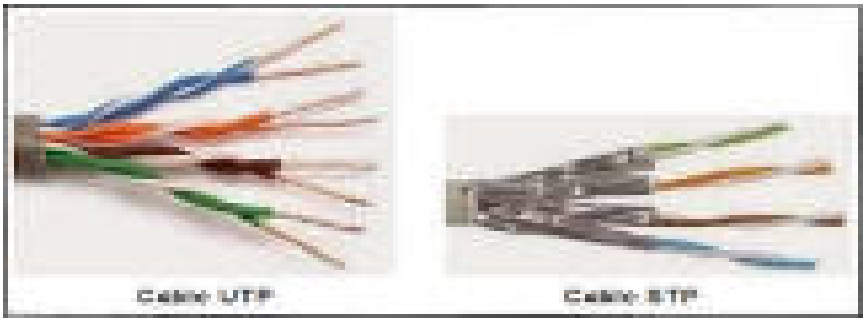


Figure 3 : Câble UTP et STP

- **Les connecteurs pour paires torsadées**

La paire torsadée se branche à l'aide d'un connecteur RJ-45. Ce connecteur est similaire au RJ-11 à la seule différence du nombre de branches, puisque le RJ-45 se compose de huit broches alors que RJ-11 n'en possède que six, voire quatre généralement.

Figure 4 : Connecteur RJ-45

➢ **La fibre optique**

Il s'agit du support de transmission le plus moderne et le plus performant. Il permet de transmettre des données sous forme d'impulsions lumineuses avec un débit supérieur à celui des autres supports filaires. La fibre optique et constitué d'un cœur, d'une gaine optique, et d'une enveloppe protectrice comme présentée par la figure suivante :

Figure 5 : Fibre Optique

Caractéristiques de la fibre optique :

- Légèreté
- Immunité au bruit
- Faible atténuation
- Tolère des débits de l'ordre de 100Mbits/s
- Largeur de bande de quelques dizaines de MH à plusieurs GH.

On distingue deux types de fibre optique :

- Les fibres multi modes : ou le cœur de la fibre est très volumineux ce qui permet la propagation de plusieurs modes (trajets) simultanément. Il existe deux sortes de fibre multi modes, une à saut d'indice et l'autre à gradient d'indice.

- Les fibres monomodes : SMF (single mode fiber) avec un cœur fin et ne peut transporter le signal que sur un seul trajet, elle permet de transporter le signal à une distance plus longue (50 fois) que celle de la multi mode.

1.5 Les équipements d'interconnexion

L'interconnexion de réseaux peut être locale : les réseaux sont sur le même site géographique ; dans ce cas, un équipement standard (répéteur, routeur etc....) suffit à réaliser physiquement la liaison. Elle peut aussi concerner des réseaux distants. Il est alors nécessaire de relier ces réseaux

par une liaison téléphonique (modems, etc..). Le choix d'un équipement d'interconnexion demeure un compromis entre les fonctions désirées et le coût.

- **Les répéteurs**

Un répéteur est un équipement qui permet d'étendre la portée du signal sur le support de transmission en générant un nouveau signal à partir du signal reçu. Le répéteur travaille uniquement au niveau physique (couche 1 du modèle OSI), c'est-à-dire qu'il ne travaille qu'au niveau des informations binaires circulant sur la ligne de transmission et qu'il n'est pas capable d'interpréter les paquets d'informations.

- **Le Hub (Host Unit Broadest)**

Un Hub est un élément matériel permettant de connecter le trafic réseau provenant de plusieurs hôtes, et de régénérer le signal. Il est ainsi une entité possédant un certain nombre de ports (généralement 4, 8,16 ou 32). Son unique but est de récupérer les données binaires parvenant sur un port et de les diffuser sur l'ensemble des ports.

- **Le Switch**

Un switch, également appelé commutateur réseau, est un boîtier doté de quatre à plusieurs centaines de ports Ethernet, et qui sert à relier plusieurs câbles ou fibre optique dans un réseau informatique. Il permet de créer des circuits virtuels, de recevoir des informations et de les envoyer vers un destinataire précis sur le réseau en les aiguillant sur le port adéquat. Les switchs ont plusieurs avantages : ils sécurisent les données transmises sur le réseau et ils peuvent être utilisés pour augmenter le nombre d'ordinateurs connectés sur un réseau Ethernet.

- **Les ponts**

Un pont est un dispositif matériel permettant de relier des réseaux travaillant avec le même protocole. Il fonctionne sur la couche liaison de données du modèle OSI, il est capable de filtrer les trames en ne laissant passer que celles dont l'adresse correspond à une machine située à l'opposé du pont. Ainsi, le pont permet de segmenter un réseau en conservant au niveau du réseau local les trames destinées au niveau local et en transmettant les trames destinées aux autres réseaux. Cela permet de réduire le trafic (notamment les collisions) sur chacun des réseaux et

d'augmenter le niveau de confidentialité car les informations destinées à un réseau ne peuvent pas être écoutées sur l'autre brin.

- **Le routeur**

Un routeur est un dispositif d'interconnexion permettant de relier plusieurs réseaux informatiques. Il permet d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter. La fonction de routage est notamment utilisée lorsqu'une adresse internet est partagée par plusieurs ordinateurs d'un même réseau.

- **Le Pare-feu (Firewall)**

Un firewall (ou pare-feu) est conçu pour assurer la protection des données dans un réseau (protection d'un ordinateur personnel relié à Internet par exemple, ou protection d'un réseau d'entreprise). Il permet d'assurer la sécurité des informations d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies par son administrateur.

1.6 Les types de réseau

On distingue plusieurs types de réseaux selon leur taille (en termes de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue. On définit généralement les catégories de réseaux suivantes :

- **Réseaux locaux (LAN)**

Un réseau local (LAN, local area network) désigne un ensemble d'ordinateurs et de périphériques interconnectés au sein d'une même organisation, sur une zone géographique restreinte à l'aide d'une même technologie (Ethernet ou WIFI). Un réseau local est donc un réseau sous sa forme la plus simple. La vitesse de transfert de données d'un réseau local peut se répartir entre 10Mbps (pour un réseau Ethernet standard) à 1 Gbps (gigabit Ethernet par exemple). La taille d'un réseau local peu atteindre jusqu'à 100 voire 1000 machines.

- **Réseaux personnels (PAN)**

Un réseau personnel (PAN) rassemble les appareils électroniques situés dans l'environnement immédiat d'un utilisateur. La portée d'un PAN s'étends généralement de quelques centimètres à

quelques mètres. L'un des exemples concrets les plus courants d'un PAN est la connexion entre une oreillette Bluetooth et un smartphone.

- **Réseau métropolitain (MAN)**

Un réseau métropolitain (MAN, Métropolitain Area Network) permet d'interconnecter plusieurs réseaux locaux situés à proximité géographique, généralement dans un rayon de quelques dizaines de kilomètres. Ainsi, un réseau métropolitain permet à deux machines distantes de communiquer comme si elles faisaient parties d'un même réseau local.

- **Réseaux étendus (WAN)**

Un réseau étendu (WAN, Wide Area Network) interconnecte plusieurs réseaux locaux à travers de grandes distances géographiques. Les WAN fonctionnent grâce à des équipements réseau appelés routeurs, qui permettent de déterminer le trajet le plus approprié pour atteindre une machine du réseau.

1.7 Notion de protocole

Un protocole est un ensemble de règle et de procédures normalisées permettant la communication entre processus, y compris lorsqu'ils s'exécutent sur des machines différentes. Il définit comment les données sont formatées, transmises, reçues et interprétées sur un réseau. Il existe différents types de protocole, chacun adapté à un usage spécifique : par exemple, le protocole ICMP sert à gérer les messages liés à l'état de la transmission et au contrôle des erreurs. Sur Internet, la majorité des communications repose sur une suite de protocoles interconnectés appelées TCP/IP. Elle contient, entre autres, les protocoles suivants : http, FTP, ARP, ICMP, IP, TCP, UDP, SMTP, Telnet, NNTP.

1.8 Le modèle OSI (Open Systems Interconnection)

La première évolution des réseaux informatiques a été marqué par une certaine anarchie, chaque constructeur développait sa propre technologie de manière indépendante. Pour pallier à cela, l'ISO (Organisation Internationale de normalisation) décida de mettre en place un modèle de référence théorique décrivant le fonctionnement des communications réseau. Le modèle de référence OSI décompose le processus de communication réseau en sept couches distinctes,

chacune illustrant une fonction réseau bien précise. Cette structuration des fonctions réseau est appelée organisation en couches.

1.8.1 Les 7 couches du modèle OSI sont les suivantes :

- **Couche 1 : couche physique**

C'est la première couche du modèle OSI qui définit les spécifications du média (câblage, connecteur, voltage, bande passante…).

- **Couche 2 : couche liaison de donnée**

La couche liaison de donnée s'occupe de l'envoi de la donnée sur le média. Cette couche est divisée en deux sous-couches : La sous-couche MAC (Média Access Control) est chargée du contrôle de l'accès au média. C'est au niveau de cette couche que l'on retrouve les adresses de liaison de donnée (MAC, DLCI). La sous-couche LLC (Layer Link Control) s'occupe de la gestion des communications entre les stations et interagit avec la couche réseau.

- **Couche 3 : couche réseau**

Cette couche gère l'adressage de niveau trois, la sélection du chemin et l'acheminement des paquets au travers du réseau.

- **Couche 4 : couche transport**

La couche transport assure la qualité de la transmission en permettant la retransmission des segments en cas d'erreurs éventuelles de transmission. Elle assure également le contrôle du flux d'envoi des données.

- **Couche 5 : couche session**

La couche session, elle sert à établir, gérer et fermer les sessions de communications entre les applications.

- **Couche 6 : couche présentation**

La couche présentation quant à elle spécifie les formats des données des applications (encodage MIME, compression, encryptions).

➢ **Couche 7 : Application**

Cette couche assure l'interface avec les applications, c'est la couche la plus proche de l'utilisateur

Figure 6 : Les 7 couches du modèle OSI

1.8.2 Les avantages du modèle OSI :

La division de la communication réseau en éléments plus simple et indépendants permet plusieurs avantages :

- Une meilleure compréhension du fonctionnement globale du réseau
- L'uniformisation des éléments afin de permettre le développement multi constructeur.
- La modularité, c'est-à-dire la possibilité de modifier ou d'améliorer une couche (par exemple en intégrant un nouveau support de transmission) sans impacter l'ensemble du système.

Afin d'assurer la communication entre les couches et entre les hôtes d'un réseau, OSI a recourt au principe d'encapsulation.

✓ **Encapsulation**

C'est une étape de conditionnement des données consistant à ajouter un en-tête de protocole déterminé avant que les données ne soient transmises à la couche inférieure.

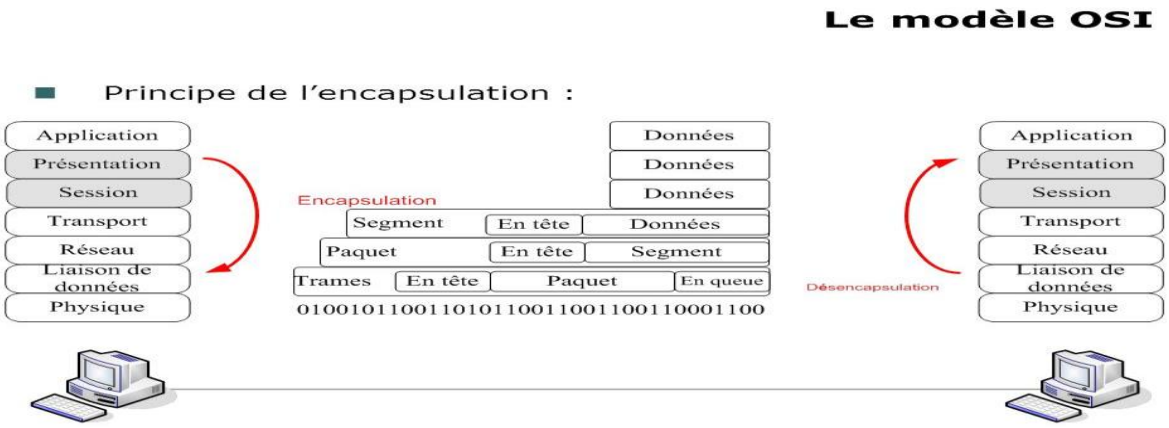


Figure 7 : Le principe de l'encapsulation

Lors de la communication entre deux hôtes, on fait référence à la communication d'égal à égal, c'est-à-dire que la couche N de la source communique avec la couche N du destinataire. Lorsqu'une couche de l'émetteur construit des données, elle encapsule ces dernières avec ses informations et les passes ensuite à la couche inférieure. Le système inverse se déroule au niveau du destinataire ou une couche reçoit les données de la couche inférieure, enlève les informations la concernant, puis passe à la transmission des informations restantes à la couche supérieure. Les données transitant à la couche N de la source sont donc les mêmes que les données transitant à la couche N du destinataire. (4)

- ✓ Pour identifier les données lors de leur passage au travers d'une couche, l'appellation PDU (Unité de données de protocole) est utilisée.

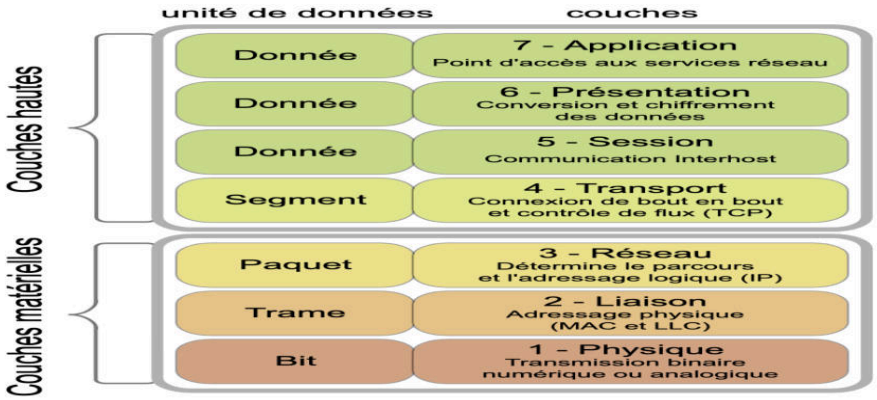


Figure 8 : Identification des données

1.9 Le modèle TCP/IP

1.9.1 Présentation de TCP/IP

TCP/IP est un ensemble de protocoles. Le sigle TCP/IP qui signifie « Transmission Control Protocol/Internet Protocol ». TCP/IP constitue l'ensemble des règles fondamentales régissant la communication sur internet. Cette architecture repose sur le principe de l'adressage IP, qui consiste à attribuer une adresse unique à chaque machine du réseau afin d'assurer l'acheminement des paquets de données vers leurs destinations.

Cette suite est conçue pour répondre à un certain nombre de critères parmi lesquels on a:

- ❖ L'acheminement fiable des paquets de données sur le réseau ;
- ❖ L'utilisation d'un système d'adressage unique par machine ;
- ❖ Le contrôle des erreurs de transmission de données.

TCP/IP est un modèle qui comprends 4 couches :

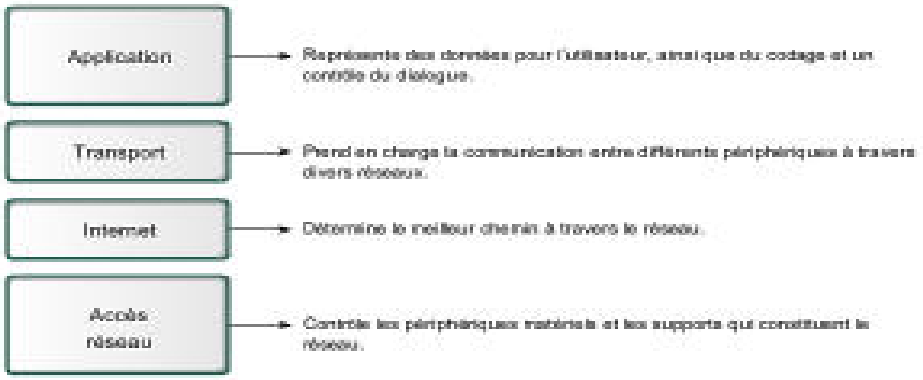


Figure 9 : Les 4 couches TCP/IP

- ➢ **Les rôles des différentes couches sont les suivants :**
  - **Couche Accès réseau :** elle spécifie la forme sous laquelle les données doivent être acheminées quel que soit le type de réseau utilisé.
  - **Couche Internet :** : elle est chargée de fournir le paquet de données (datagramme).
  - **Couche Transport** : elle assure l'acheminement des données, ainsi que le mécanisme permettant de connaitre l'état de la transmission.
  - **Couche Application** : elle englobe les applications standard du réseau.

1.9.2 Comparaison entre le modèle TCP/IP et le modèle OSI

Les deux modèles sont très semblables dans la mesure où les deux sont des modèles de communication à couche et utilisent l'encapsulation de données.

On constate par contre deux grandes différences :

- TCP/IP regroupe certaines couches du modèle OSI dans des couches plus générales.
- TCP/IP est plus qu'un modèle de conception théorique, c'est sur lui que repose le réseau.

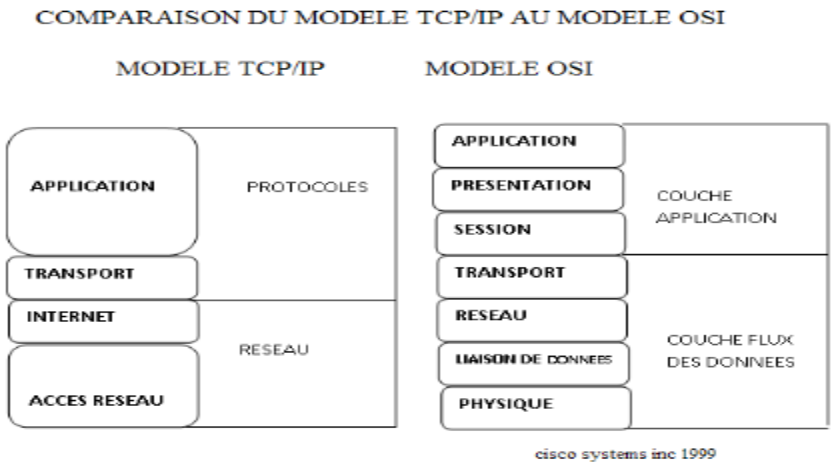


Figure 10 : Les modèle TCP/IP et OSI

1.10 Le protocole UDP (User Datagram Protocol)

UDP est un protocole de transport (couche 4 du modèle OSI) sans connexion fonctionnant au-dessus du protocole de réseau IP (couche 3 du modèle OSI). C'est un protocole facile pour la mise en œuvre, en revanche il n'est pas fiable (perte de messages, messages non ordonnés, . . .). Les messages qu'envoi UDP sont appelés datagrammes.

2-Sécurité des réseaux

2.1 Les Menaces

La menace est l'éventualité alarmante que quelque chose se produise, et qui peut porter atteinte à un système informatique, en d'autres termes, une menace est un événement ou action susceptible de violer la sécurité d'un système informatique. Parmi ces menaces, on distingue notamment :

- **Le virus**

Un virus est un programme malveillant conçu pour se reproduire en s'insérant dans d'autres fichiers exécutables. Tant que le virus n'a pas été exécuté, vous n'avez rien à craindre. Mais, lorsqu'il est activé, il peut vous endommager votre système, supprimer des données, formater un disque dur. La majorité des virus se propagent par courrier électronique en pièce-jointe.

- **Les Vers**

Un ver (en anglais worm) est un programme malveillant conçu pour se propager d'ordinateur à ordinateur via un réseau comme l'Internet. Ainsi, contrairement à un virus, le vers n'a pas besoin d'un programme hôte pour assurer sa reproduction. Son poids est très léger, ce qui lui permet de se propager à une vitesse impressionnante sur un réseau, et pouvant donc saturer ce dernier.

- **Le cheval de Troie**

Un cheval de Troie ou trojan n'est ni un ver, ni un virus, par ce qu'il ne se reproduit pas. Il s'introduit sur une machine dans le but de détruire ou de récupérer des informations confidentielles sur celle-ci. Généralement, il est utilisé pour créer une porte dérobée sur l'hôte infecté afin de mettre à disposition d'un pirate un accès à la machine depuis internet.

Les opérations suivantes peuvent être effectuées par intermédiaire d'un cheval de Troie :

- Récupération des mots de passe à l'aide de keylogger.
- La prise de contrôle à distance non autorisée d'un ordinateur.
- L'utilisation de la machine comme relais pour lancer d'autre attaques.
- L'exploitation de l'ordinateur comme serveur de spam.
- L'écoute du réseau (sniffing).

Il est possible d'intercepter toutes les trames que notre carte reçoit et qui ne nous sont pas destinées, grâce à un logiciel appelé 'sniffer'. Si quelqu'un se connecte par internet par exemple à ce moment-là, son mot de passe transitant en clair sur le net, il sera aisé de lire et c'est facile de savoir à tout moment quelles pages web regardent les personnes connectées au réseau.

- **Hijackers**

  Un Hijacker, ou pirate de navigateur, utilise les failles de sécurité d'internet explorer pour s'installer sur votre ordinateur. Ce genre de programme s'installe donc juste en

surfant sur le net, souvent sur des sites "louches" (sites de piratage, de patch noc pour jeux, ...).

- **Backdoor**

Une backdoor (en français, une porte dérobée) est un moyen qu'une personne malveillante utilise pour revenir dans un système. A titre illustratif, un pirate, après avoir accéder à une machine peut se créer un compte secret. Ainsi, il pourra revenir la prochaine fois facilement.

2.3 Les techniques d'attaques

- **Attaque par déni de service**

Une attaque par déni de service (en anglais Denial of Service, DoS) est une attaque qui a pour objectif la mise en hors-jeu du système qui est visée. Donc, la victime est incapable d'accéder à son réseau. Ce type d'attaque peut aussi bien être utilisé contre un serveur d'entreprise qu'un particulier relié à internet. Tous les systèmes d'exploitation sont également touchés : Windows, Linux, Unix. (6)

- **Attaque de l'homme de milieu (MitM)**

Cette attaque a pour objectif de s'introduire entre deux ordinateurs qui communiquent. Soient deux ordinateurs A et B qui veulent dialoguer. Lorsqu'un pirate décide de se faire passer pour l'ordinateur A auprès de B et de B auprès de A, toute communication vers A ou B passera par le pirate, l'homme du milieu.

- **Usurpation d'adresse IP (IP spoofing)**

C'est une technique qui consiste à envoyer des paquets IP en utilisant une adresse IP qui n'a pas été attribuée à l'expéditeur, cette méthode permet à l'attaquant de dissimuler son identité et de transmettre des paquets de manière anonyme, tout en contournant certaines mesures de sécurité réseau.

- **Le craquage de mot de passe**

Cette méthode consiste à tester plusieurs mots de passe afin de trouver le bon. Elle peut s'effectuer à l'aide d'une liste des mots de passe les plus courants (et de leur variantes), ou par la méthode de brute force (toutes les combinaisons sont essayées jusqu'à trouver la bonne), cette

technique longue, souvent peut utiliser à moins de bénéficier de l'appui d'un très grand nombre de machines.

- **Buffer OverFlow**

Un débordement de tampon (en anglais Buffer OverFlow ou BoF) est une attaque très utilisée des pirates. Cette attaque consiste à utiliser un programme résidant sur votre machine en lui envoyant plus de données qu'il n'est censé en recevoir afin que ce dernier exécute un code arbitraire. Il n'est pas rare qu'un programme accepte des données en paramètre. Ainsi, si le programme ne vérifie pas la longueur de la chaîne passée en paramètre, une personne malintentionnée peut compromettre la machine en entrant une donnée beaucoup trop grande.

Pour remédier à cela des moyens de protection ont été conçu dans le but de protéger les données et les informations circulant sur le réseau.

2.4 Les moyens de protection

La sécurité est l'ensemble des moyens mis en place afin de limiter la vulnérabilité d'un système face aux menaces. Autrement dit, c'est l'ensemble des techniques qui assurent que les ressources du système d'information (matérielles ou logicielles) d'une organisation sont utilisées uniquement dans le cadre où il est prévu qu'elles le soient. Les exigences fondamentales de la sécurité Informatiques se résument à assurer :

- La disponibilité : L'information sur le système doit être toujours disponible aux personnes autorisées.
- La confidentialité : L'information sur le système ne doit être diffusée qu'aux personnes autorisées.
- L'Intégrité : L'information sur le système ne doit pouvoir être modifiée que par les personnes autorisées.

Ainsi comme moyen de protection, nous pouvons citer :

- **L'Authentification**

La première étape pour protéger les ressources d'un réseau est de pouvoir vérifier l'identité des utilisateurs. Cette vérification s'appelle l'authentification. L'authentification est la procédure mise

en œuvre notamment pour vérifier l'identité d'une entité et s'assurer que l'identité fournie correspond à l'identité de cette entité préalablement enregistrée. (7)

- **Les logiciels Antivirus**

Ce sont des logiciels qui permettent de détecter et de supprimer les virus informatiques sur n'importe quel type de stockage (disque-dur, disquette, CD-ROM). La plupart des ordinateurs possèdent un logiciel antivirus capables de détecter les logiciels viraux s'il est régulièrement mis à jour et correctement entretenu.

- **La cryptographie**

La cryptographie est un ensemble de technique qui permettent de modifier les données dans le but de cacher leur contenu, empêcher leur modification ou leur utilisation illégale. Ceci permet d'obtenir un texte, en effectuant des transformations inverse (ou encre des algorithmes de déchiffrement). Désormais, elle sert non seulement à préserver la confidentialité des données mais aussi à garantir leur intégrité et leur authenticité. La taille des clés de chiffrement dépende de la sensibilité des données à protéger plus ces clés sont longues plus le nombre de possibilités de les déchiffrer important, par conséquent il sera difficile de définir la clé. (7)

Les algorithmes de chiffrement se divisent en deux catégories :

- **Chiffrement symétrique :** Dans ce cas de chiffrement l'émetteur et le récepteur utilisent la même clé secrète qu'ils appliquent à un algorithme donné pour chiffrer ou déchiffrer un texte. Ce cryptage à un inconvénient puisqu'il faut que les deux parties possèdent la clé secrète, il faut donc la transmettre d'un bout à l'autre, ce qui risque sur un réseau non fiable comme internet car la clé peut ainsi être interceptée.
- **Chiffrement asymétrique :** ces systèmes se caractérisent par la présence d'une entité pour chaque interlocuteur désirant communiquer des données. Chaque interlocuteur possède une bi-clé ou couple de clés calculées l'une en fonction de l'autre. Une première clé, visible appelée clé publique est utilisée pour chiffrer un texte en clair. Une deuxième clé, secrète appelée clé privée est connu seulement par le destinataire, qui est utilisé pour déchiffrer un texte.

➢ **Le pare-feu(firewall)**

Un pare-feu est un système de sécurité de réseau informatique qui limite le trafic Internet entrant, sortant ou à l'intérieur d'un réseau privé. Ce logiciel ou cette unité matérielle-logicielle dédiée fonctionne en bloquant ou en autorisant sélectivement les paquets de données. Le pare feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

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

Figure 11 : Pare-feu

Le système firewall est un système logiciel ou matériel, constituant un intermédiaire entre le réseau local (ou la machine local) et un ou plusieurs réseaux externes. Il est possible de mettre un système pare-feu sur n'importe quelle machine et avec n'importe quel système pourvu que :

- La machine soit suffisamment puissante pour traiter le trafic.
- Le système soit sécurisé.
- Aucun autre service que le service de filtrage de paquets ne fonctionne sur le serveur.

❖ **Fonctionnement du pare-feu**

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

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

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

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

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

➢ **Les VLANs (Virtual Area Network)**

Un VLAN sert à créer des domaines de diffusion (domaine de broadcast) gérer par les commutateurs indépendamment d'emplacement où se situent les nœuds, ce sont des domaines de diffusion gérer logiquement.

➢ **Les ACL (Access Control List)**

Les listes de contrôle d'accès ont pour objectif de disposer d'une fonction de filtrage prenant en compte l'historique des connexions en cours, afin de ne pas accepter du trafic qui n'aurait pas été demandé à partir d'une zone précise du réseau. Les ACL semblent avoir toujours existé sur les routeurs et rares sont les configurations ou elles n'apparaissent pas. Elles servent principalement au filtrage des paquets sur les interfaces physiques.

➢ **VPN**

Un réseau privé virtuel (Virtual Private Network en anglais, abrégé en VPN) est une abstraction permettant de considérer plusieurs ordinateurs distants comme étant sur le même réseau local. Toute la partie de routage pour atteindre le ou les autres ordinateurs est gérée de façon transparente par le logiciel de VPN, créant un tunnel.

➢ **Pfsense**

Pfsense est un routeur/pare-feu open source basée sur le système d'exploitation Free BSD, qui peut être installé sur un simple ordinateur personnel comme sur un serveur. Il a pour particularité de gérer nativement les VLAN et dispose de très nombreuses fonctionnalités tels que faire un VPN ou portail captif. Voici l'architecture avec laquelle peut être utilisé le pfsense :

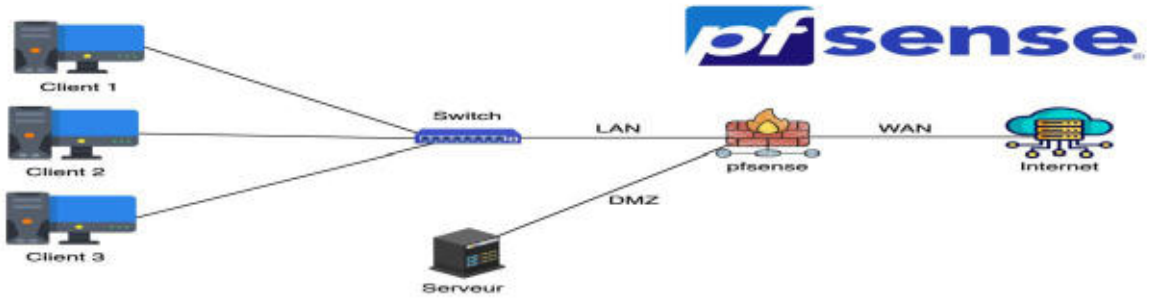


Figure 12 : Pfsense

❖ **Les principes de fonctionnement du pfsense**

Pfsense offre une multitude de fonctionnalités intéressantes comme par exemple :

- Pare-feu (sa fonction primaire) qui est basé sur le paquet filtrer il permet donc :

  -Le filtrage par adresse IP source et de destination, par protocole IP et par port.

  - Limitation de connexions simultanées.

  - La possibilité de router les paquets sur les passerelles spécifiques selon les règles.

- Table d'état : qui contient des informations sur les connexions réseaux.
- Traductions d'adresses réseau (NAT) ce qui permet de joindre une machine située sur le LAN à partir de l'extérieur.
- VPN pour sécuriser les données transitant sur le réseau.
- Serveur DHCP qui permet de distribuer automatiquement une configuration IP aux équipement présent sur le réseau.
- Serveur DNS (statique ou dynamique) qui permet de communiquer avec les autres périphériques présents sur le réseau grâce à leurs adresses IP.
- Une base de données locale peut être utilisée pour l'authentification.

❖ **Avantages d'utilisation de pfsense**

- Simplicité d'installation et d'administration.
- La mise à jour du système sans le réinstaller, package téléchargeable depuis le web.
- Solution riche et performante (basé sur un logiciel libre).

CHAPITRE III : RÉSEAU PRIVÉ VIRTUEL (VPN)

1.1 Définition d'un VPN

Un réseau privé virtuel (VPN) en anglais : Virtual Private Network est un système permettant de faire communiquer les postes des différents sites d'une société ensemble tout en assurant un moyen sécurisé d'acheminement des données échangées empruntant les réseaux de télécommunication publics. Le VPN est composé de deux mots "privé" et "virtuel". "privé" car il s'agit d'une communication LAN. Ce qui signifie que les données échangées ne doivent pas être accessible depuis l'extérieur (en dehors du VPN). "virtuel" car en réalité les réseaux LAN communiquant à l'aide d'un VPN ne sont pas interconnectés physiquement (câbles, commutateurs, etc.) comme c'est le cas dans un vrai LAN mais passent par internet pour échanger les données. Afin de rendre un réseau privé "virtuel" au milieu d'internet, un VPN créé ce qu'on appelle un "tunnel". (8)

1.2 Fonctionnement du VPN

Le VPN repose sur un protocole de tunnelisation qui permet de chiffrés les données par un algorithme cryptographique entre les deux réseaux.

Le VPN n'est pas un concept ce n'est qu'une implémentation. Il se caractérise par les obligations suivantes :

- ✓ Authentification des entités communicantes : le serveur VPN doit pouvoir être sûre de parler au vrai client et vice-versa.
- ✓ Authentification des utilisateurs : seules les bonnes personnes doivent pouvoir se connecter au réseau virtuel. On doit aussi pouvoir conserver les logs de connexions
- ✓ Cryptage du tunnel : les données échangées sur internet doivent être cryptées entre le client VPN et le serveur VPN et vice versa.

1.4 Topologie des VPN

Basés sur internet comme support de transmission, les VPN utilisent des protocoles d'encapsulation et d'authentification pour sécuriser les données. Au niveau des topologies, on retrouve des réseaux privés virtuels en étoile ou maillé.

- ➢ **VPN en étoile**

Dans cette topologie toutes les ressources sont centralisées au même endroit et c'est dans cette zone qu'on retrouve le serveur d`accès distant ou serveur VPN, dans ce cas de figure tous les employés du réseau s'identifient ou s'authentifient au niveau du serveur et pourront ainsi accéder aux ressources qui se situent sur l'intranet.

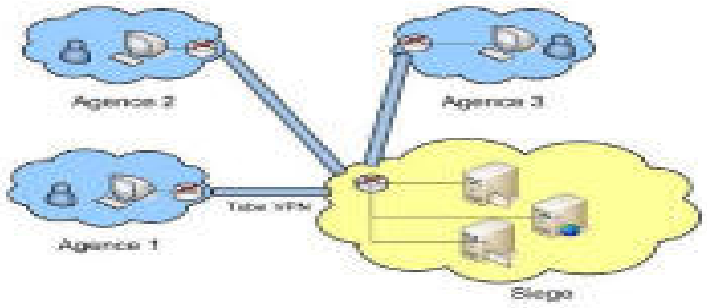


Figure 13 : VPN en étoile

- **VPN maillé**

Dans cette topologie les routeurs ou passerelles présents aux extrémités de chaque site seront considérés comme des serveurs d'accès distant, les ressources ici sont décentralisées sur chacun des sites autrement dit les employés pourront accéder aux informations présentes sur tous les réseaux.

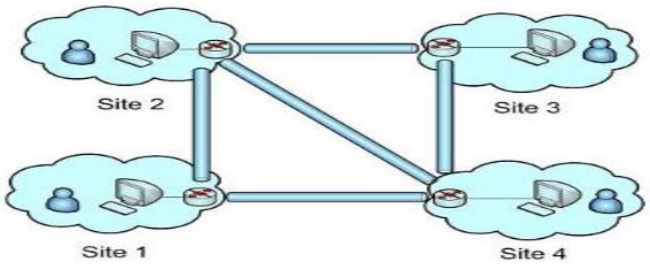


Figure 14 : VPN maillé

1.5 Les différents types de VPN

Parmi ces différents types nous pouvons cités :

- **Le VPN d'accès**

Le VPN d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au réseau privé. L'utilisateur se sert d'une connexion Internet pour établir la connexion VPN. Il existe deux cas :

- L'utilisateur demande au fournisseur d'accès de lui établir une connexion cryptée vers le serveur distant : il communique avec le NAS du fournisseur d'accès et c'est le NAS qui établit la connexion cryptée.
- L'utilisateur à en sa possession son propre logiciel client pour le VPN auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise.

Les deux méthodes possèdent chacune leurs avantages et leurs inconvénients :

-La première permet à l'utilisateur de communiquer sur plusieurs réseaux en créant plusieurs tunnels, mais nécessite un fournisseur d'accès proposant un NAS compatible avec la solution VPN choisie par l'entreprise. De plus, la demande de connexion par le NAS n'est pas cryptée ce qui peut poser des problèmes de sécurité.

-Sur la deuxième méthode ce problème disparaît puisque l'intégralité des informations sera cryptée dès l'établissement de la connexion. Par contre, cette solution nécessite que chaque client transporte avec lui le logiciel, lui permettant d'établir une communication cryptée. Quelle que soit la méthode de connexion choisie, Ce type d'utilisation montre bien l'importance dans le VPN d'avoir une authentification forte des utilisateurs.

➢ **Le VPN intranet**

Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants, l'intranet VPN est utilisé pour relier au moins deux intranets entre eux toutes en garantissant la sécurité, la confidentialité et l'intégrité des données. Un VPN permet aux utilisateurs éloignés de se connecter à un réseau. Dans ce cas, on parle de l'intranet VPN car il s'agit aussi de connecter plusieurs clients distants à un site de l'entreprise. Certaines données très sensibles peuvent être amenées à transiter sur le VPN (base de données clients, informations financières...). Des techniques de cryptographie sont mises en œuvre pour vérifier que les données n'ont pas été altérées. Il s'agit d'une authentification au niveau paquet pour assurer la validité des données, de l'identification de leur source ainsi que leur non-répudiation. La plupart des algorithmes utilisés font appel à des signatures numériques qui sont ajoutées aux paquets. La confidentialité des données est, elle aussi, basée sur des algorithmes de cryptographie. La technologie en la matière est suffisamment avancée pour permettre une sécurité quasi parfaite. Généralement pour la confidentialité, le codage en lui-même pourra être moyen à faible, mais

sera combiné avec d'autres techniques comme l'encapsulation IP dans IP pour assurer une sécurité raisonnable.

➢ **Le VPN extranet**

Une entreprise peut utiliser le VPN pour établir une communication avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers. Dans ce cadre, il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits de chacun sur celui-ci. Les utilisateurs externes n'ont pas accès à l'ensemble de l'Intranet, mais seulement à certaines zones donc l'accès à l'extranet est possible à partir de plusieurs endroits. L'accès dans un extranet est limité à certaines informations qui sont différents par rapport aux groupes et les rôles d'utilisateurs. Par exemple, les fournisseurs et les clients ont des droits d'accès différents.

1.6 Les différentes architectures des VPN

➢ **De Poste à Poste**

Les utilisateurs externes n'ont pas accès à l'ensemble de l'Intranet, mais seulement à certaines zones donc l'accès à l'Extranet est possible à partir de plusieurs endroits. L'accès dans un extranet est limité à certaines informations qui sont différents par rapport aux groupes et les rôles d'utilisateurs. Par exemple, les fournisseurs et les clients ont des droits d'accès différents.

✓ **Avantages et Inconvénients**

Le principal intérêt dans cette solution est que la conversation entre les deux postes est parfaitement protégée de bout en bout.

Par contre, elle présente de nombreux inconvénients :

- Un impact très important sur les performances en cas de fort débit puisque le cryptage est uniquement logiciel.
- Quand les postes se situent sur des locaux séparés par internet il est nécessaire que les deux extrémités puissent échanger leurs messages sur des protocoles et des ports qui doivent être autorisés par les firewalls situés sur chaque site, cela nécessite également des translations d'adresses puisque les machines concernées sont rarement dotées d'adresses IP publiques et cela n'est pas sans poser quelques problèmes.
- Ne peut être utilisé pour atteindre des matériels peu intelligents.

Figure 15 : VPN poste à poste

➢ **Poste à Site**

Un utilisateur distant a simplement besoin d'un client VPN installé sur son PC pour se connecter au site de l'entreprise via sa connexion internet. Le développement de l'ADSL favorise ce genre d'utilisation. Toutefois à interdire l'accès internet depuis le poste « localement ». Pour une question de sécurité, la navigation devra se faire via le réseau de l'entreprise. Ce point est important et rejoint la réflexion la plus large de la sécurité des sites mis en relation avec le VPN. Lorsque les niveaux de la sécurité sont différents, lorsque les deux sites sont reliés, le niveau de sécurité le plus bas est applicable aux deux, s'il existe une faille de sécurité sur un site (ou sur poste normale) celle-ci peut être exploitée.

✓ **Avantages et Inconvénients**

Parmi les avantages de cette solution, on trouve :

- L'accès du poste mobile peut se faire de n'importe quel point du monde avec un à accès Internet.
- Assurer la transition des données entre le poste distant et le site central d'une façon sécurisée grâce à l'authentification.
- L'avantage est que le côté de la connexion entre le poste et le pare-feu de l'entreprise est chiffré. Par contre, celui entre le pare-feu et les postes du réseau local ne l'est pas puisque le cryptage, côté site central, est assuré par le pare-feu.

Les inconvénients de cette configuration :

- Nécessite une installation logicielle sur le poste distant.
- Le cryptage exige une charge au poste distant, cela peut dégrader les performances.
- Le cryptage n'est pas assuré au-delà du firewall du site central.

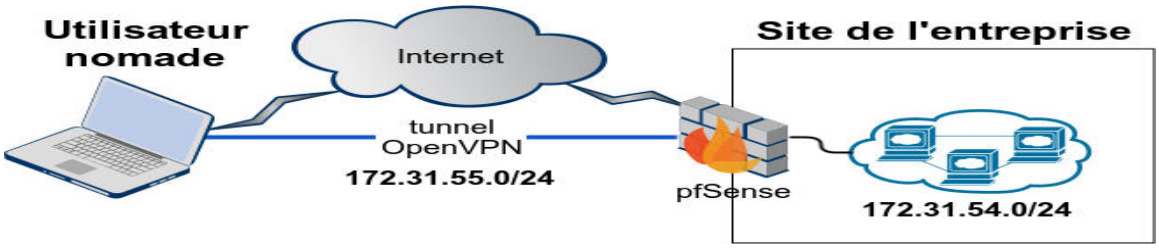


Figure 16 : Poste a site

➢ **De site à site**

Elle correspond à un type d'infrastructure de réseau étendu, c'est-à-dire que l'interconnexion entre les VPN remplace et améliore les réseaux privés existant. Elle est utilisée pour relier un site avec des filiales à moindre coût et en toute sécurité.

✓ **Avantages et Inconvénients**

Parmi les avantages fournis par cette configuration nous pouvons citer :

- Le cryptage est pris en charge par des processeurs spécialisés, pour de meilleures performances.
- Une facilité notable pour le contrôle de trafic autorisé.
- Aucun impact sur les performances des postes puisqu'il n'assure pas le cryptage.
- La possibilité d'initier les VPN d'un côté ou de l'autre.

Les inconvénients de cette configuration :

- Aucune protection de données entre les postes et les firewalls puisque le tunnel n'est établi qu'entre les deux firewalls.
- La connexion des VPN nécessite que les deux extrémités soient bien identifiées soit par une adresse IP publique fixe, soit par un nom référencé dans des DNS officiels.

1.7 Les différents protocoles utilisés pour l'établissement d'un VPN

La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP. Les Protocoles de tunneling niveau 2 supportent plusieurs protocoles de liaisons de données (Ethernet, PPP, FR, MPLS, etc.). Les Protocoles de tunneling niveau 3, tels que IPSEC, supportent uniquement les couches cibles utilisant le protocole IP.

1.7.1 Les tunnels de niveau 2 (liaison de donnée)

- ✓ Protocoles : PPTP, L2TP.
- ✓ PPTP (Point-to-Point Tunneling Protocol) a été développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.
- ✓ L2TP (Layer Two Tunneling Protocol) est une évolution de PPTP et de L2F, reprenant les avantages des deux protocoles.
- ✓ L2F (Layer Two Forwarding) développé par Cisco est remplacé par L2TP.
- ✓ PPTP et L2TP dépendent des fonctionnalités du protocole PPP (Point to Point Protocole). (9)

➢ **Point-to-Point Tunneling Protocole (PPTP)**

Le protocole PPTP (Point to Point Tunneling Protocol), est un protocole qui utilise une connexion Point to Point Protocol à travers un réseau IP en créant un réseau privé virtuel (VPN). Il est en même temps une solution très employée dans les produits VPN commerciaux à cause de son intégration au sein des systèmes d'exploitation tels que Windows. Tout en étant un protocole de niveau 2, Le PPTP permet aussi l'encryptage des données ainsi que leur compression.

- Microsoft chiffrement MPPE (RC4 40 ou 128 bits).

- Protocole réseau qui encapsule des trames PPP dans des datagrammes IP.

- Compresse éventuellement les communications.

- PPTP crée ainsi un tunnel de niveau 3 défini par le protocole GRE (Generic Routing Encapsulation).

-Utilise les canaux de communication :

• Port TCP 1723

• Protocole IP 47 (GRE). (9)

❖ **Inconvénients :**

- Faiblesse de l'authentification (attaques faciles par force brute).
- Mauvaise gestion des mots de passe dans les environnements mixtes Windows 95/NT.
- Identification des paquets non implémentée (vulnérabilité à la mascarade d'adresse).

❖ **Avantages :**

- Facile à installer sur Windows.
- Utilise l'authentification Radius des Windows.

Pour pallier à ces failles, Microsoft ont créé PPTPv2. Ce protocole a donc supprimé une grande partie des failles de sécurité. Cependant ce protocole est toujours vulnérable à des attaques hors-ligne visant à deviner le mot de passe. C'est pourquoi, actuellement, PPTP n'est pas recommandé pour des applications où la sécurité est un facteur très important.

➢ **Le Protocole PPP (Point-to-Point Protocol)**

Le protocole PPP (Point -to-Point Protocol) est un protocole qui sert à transférer des données sur un lien synchrone ou asynchrone. Utilisé dans les liaisons d'accès au réseau Internet ou sur une liaison entre deux routeurs. Son rôle est d'encapsuler un paquet IP pour le transporter vers le nœud suivant et sa fonction consiste à indiquer le type des informations transportées dans le champ de données de la trame.

- Il est full duplex et garantit l'ordre d'arrivée des paquets.
- Il encapsule les paquets IP, IPX et Netbeui dans des trames PPP, puis transmet ces paquets encapsulés sur la liaison point à point. (9)

➢ **Le protocole L2TP (Layer Two tunneling Protocol)**

- Protocole réseau qui encapsule des trames PPP pour les envoyer sur des réseaux IP, X25, relais de trames ou ATM. (9)

- Utilise le port UDP 1701.

- Par défaut, utilise le protocole IPsec.

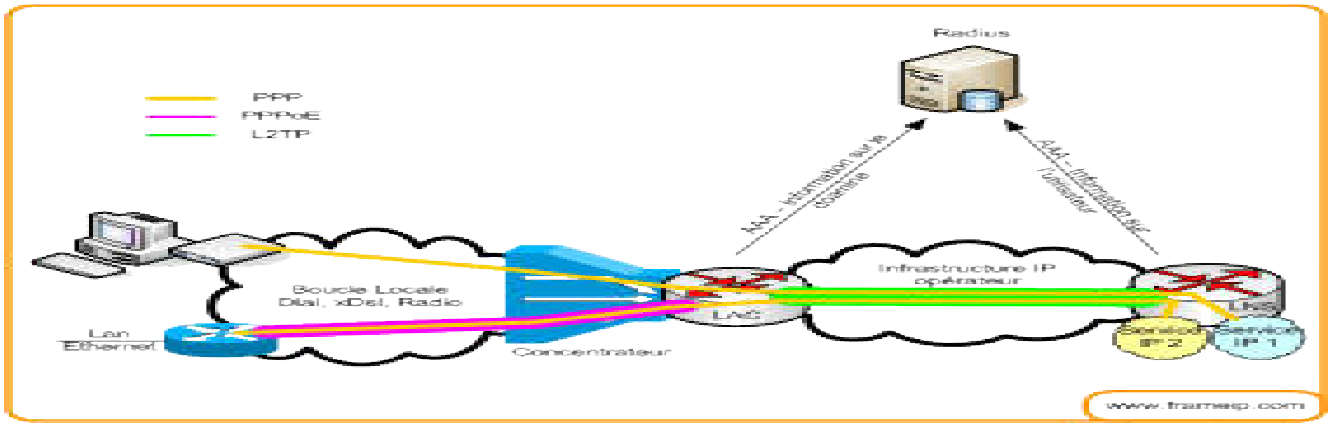


Figure 17 : Schéma réseau utilisé pour les protocoles

❖ **Inconvénients :**

- L2TP repose sur UDP lui-même repose sur IP. Au total, l'empilement total des couches protocolaires est assez lourd : IP/PPP/L2TP/UDP/IP/Couche2.
- Empilement des couches lorsque qu'un client surf sur le web. (9)

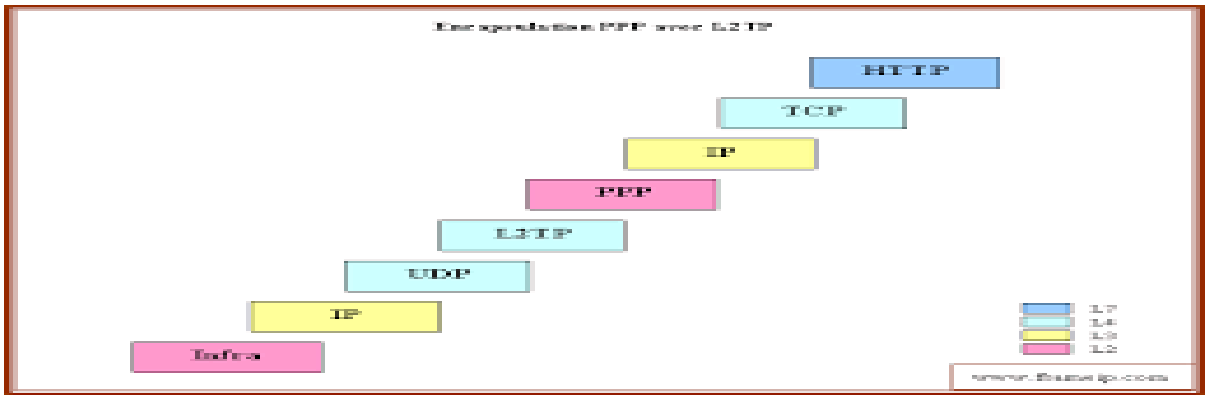


Figure 18 : Figure encapsulation PPP avec L2TP

❖ **Avantages**

- Facile à installer sur Windows.

➢ **Le Protocole L2F (Layer 2 Forwarding)**

Le protocole L2F (Layer 2 Forwarding ou transfert de couche 2) protocole développé par CISCO. Il permet à un serveur d'accès distant de véhiculer le trafic sur PPP et transférer ces données jusqu'à un serveur L2F (routeur). Le serveur L2F désencapsule les paquets et les envoie sur le réseau.

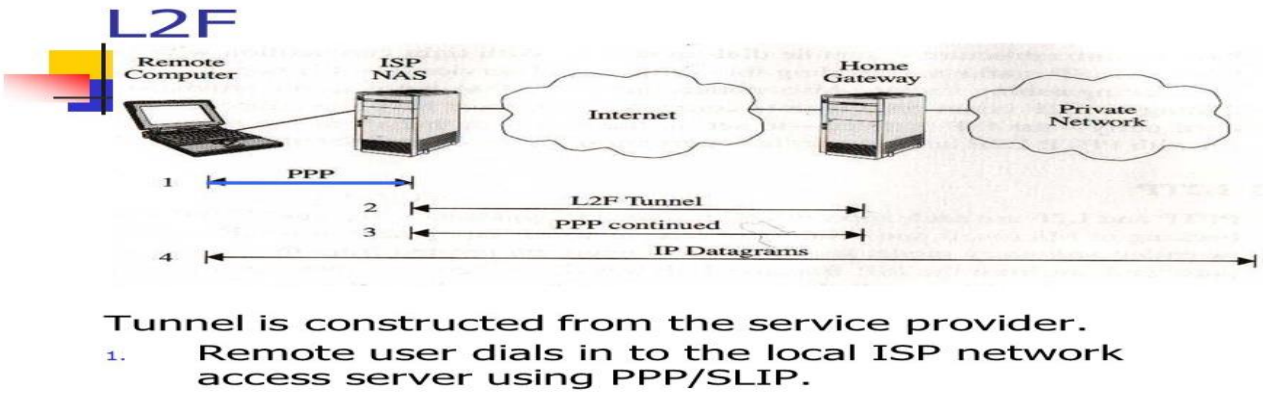


Figure 19 : Tunnel L2F

1.7.2 Les tunnels de niveau 2 et 3

- **MPLS**

Le protocole MPLS (Multi Protocol Label Switching) est pour la plupart du temps considéré comme situé dans un niveau intermédiaire entre le niveau 2 et le niveau 3. C'est la raison pour laquelle on lui affecte souvent un niveau hybride 2.5 qui n'existe pas dans les couches OSI traditionnelles. Son placement en tant que protocole de VPN peut être contesté lorsqu'il est utilisé dans ses fonctions de base. En effet, il ne met pas en œuvre certaines fonctions de sécurité telles que le cryptage, ce qui est en principe un prérequis du VPN. (10)

- **Fonctionnalités :**

La première fonctionnalité de MPLS consiste à accélérer la transmission des informations au sein d'un backbone IP, car l'acheminement est conçu sur la reconnaissance d'un Label qui permet dans le réseau de transit de ne plus se préoccuper de l'adresse mais de traiter le message en fonction de ce Label. La seconde est de permettre la création de VPN (Virtual Private Network) ou groupe fermé d'utilisateurs. (10)

MPLS est une technologie toujours en cours de standardisation à l'IETF. L'un des objectifs initiaux était d'accroître la vitesse du traitement des datagrammes dans l'ensemble des équipements intermédiaires. Cette volonté, avec l'introduction des giga routeurs, est désormais passée au second plan. Depuis, l'aspect "fonctionnalité" a largement pris le dessus sur l'aspect "performance", avec notamment les motivations suivantes :

- Intégration IP/ATM.
- Création de VPN.
- Flexibilité : possibilité d'utiliser plusieurs types de médias : (ATM, FR, Ethernet, PPP, SDH).
- Routage multicast.

- **Principe MPLS :**

Basée sur la permutation d'étiquettes, un mécanisme de transfert simple offre des possibilités de nouveaux paradigmes de contrôle et de nouvelles applications. Au niveau d'un LSR (Label Switch Router) du nuage MPLS, la permutation d'étiquette est réalisée en analysant

une étiquette entrante, qui est ensuite permutée avec l'étiquette sortante et finalement envoyée au saut suivant.

A l'entrée du réseau MPLS, les paquets IP se voient insérés un label par le "Ingress Label Edge Routeur" ou "Ingress LER" (interface d'entrée ou point de départ d'une donnée). Les LER sont les routeurs MPLS se situant à la périphérie du réseau de l'opérateur. Les paquets labélisés sont ensuite commutés vers le cœur du réseau selon son numéro de label. Les routeurs MPLS du cœur de réseau, les Label Switching Router, commute ensuite les labels jusqu'au LER de sortie (Egress LER). Le chemin qui a été pris par le paquet, et préalablement établi, au travers du réseau s'appelle un Label Switched Path (LSP).

En se basant uniquement sur les labels, les LSR du nuage MPLS commutent les paquets labellisés jusqu'à l'Egress LSR qui supprime les labels et remet Les paquets à leur destination finale. L'affectation des étiquettes aux paquets dépend des groupes ou des classes de flux FEC (forwarding équivalence classes). Les paquets appartenant à une même classe FEC sont traités de la même manière. Le chemin établi par MPLS appelé LSP (Label Switched Path) est emprunté par tous les datagrammes de ce flux.

L'étiquette est ajoutée entre la couche 2 et l'en-tête de la couche 3 (dans un environnement de paquets) ou dans le champ VPI/VCI (identificateur de chemin virtuel/identificateur de canal virtuel dans les réseaux ATM (Asynchronous Transfert Mode)).

Le switch LSR du nuage MPLS lit simplement les étiquettes, applique les services appropriés et redirige les paquets en fonction des étiquettes. Ce schéma de consultation et de transfert MPLS, offre la possibilité de contrôler explicitement le routage en fonction des adresses source et destination, facilitant ainsi l'introduction de nouveaux services IP.

1.8 Niveau 3 :

Ces protocoles agissent au moins au niveau 3 (niveau paquet).

- **SSL/TLS**

Ces protocoles connaissent un essor considérable en raison de leur simplicité de mise en œuvre. Utilisant généralement le port (443), ils parviennent facilement à traverser les pares-feux. Dans certain cas, ils ne nécessitent qu'un simple navigateur pour être utilisables. Ils sont implémentés de façon native dans d'autres logiciels (client de messagerie, client FTP).

➢ **SSH**

Le SSH est souvent utilisé afin de protéger des communications de type console (équivalent de Telnet) ou transferts de fichiers (de type FTP notamment). Son adoption reste limitée, car il est moins répandu que les protocoles SSL/TLS et possède un champ d'application plus restreint. Cependant, il reste toujours un protocole à considérer pour certains usages.

➢ **IPSec**

IPsec (Internet Protocol Security) est une continuité de protocoles normalisés par l'IETF qui fournit des services de sécurisation des données au niveau de la couche réseau. Il présente l'avantage d'être à la fois commun aux normes Ipv4 et Ipv6. (11)

Il assure les services ci-dessous :

- Confidentialité : service visant à rendre impossible l'interprétation de données par un tirs non-autorisés. C'est la fonction de chiffrement qui assure ce service en transformant des données intelligibles (en clair) en données inintelligibles (chiffrées).

- Authentification : service qui permet de s'assurer qu'une donnée provient bien de l'origine de laquelle elle est censée provenir.

-intégrité : service qui consiste à s'assurer qu'une donnée n'a pas été altérée accidentellement ou frauduleusement.

-Protection contre le rejeu : service qui permet d'empêcher les attaques consistant à envoyer de nouveau un paquet valide intercepté précédemment sur le réseau pour obtenir la même autorisation que ce paquet à entrer dans le réseau. Ce service est assuré par la présence d'un numéro de séquence.

-Gestion des clés : mécanisme de négociation de la longueur des clés de chiffrement entre deux éléments IPSEC et d'échange de ces clés.

Figure 20 : Exemple d'emplois entre Site distant

❖ **Mécanisme de sécurité**

IPsec fait appel à deux mécanismes de sécurité pour le trafic IP :

- AH (Authentification Header).
- ESP (Encapsulation Security Payload) Le but du protocole AH est de remettre au destinataire final un message possédant une identification sécurisée.

✓ **AH :**

Le protocole AH permet d'assurer l'intégrité des données en mode non connecté et l'authentification de l'origine des datagrammes IP sans chiffrement des données. Son principe est d'ajouter un bloc au datagramme IP. Une partie de ce bloc servira à l'authentification, tandis qu'une autre partie, contenant un numéro de séquence, assurera la protection contre le rejet (11).

AH est approprié lorsque la confidentialité n'est pas requise ou n'est pas permise.

✓ **ESP :**

Le protocole ESP assure, en plus des fonctions réalisées par AH, la confidentialité des données et la protection partielle contre l'analyse du trafic, dans le cas du mode tunnel. C'est pour ces raisons que ce protocole est le plus largement employé.

Le mécanisme est différent de celui d'AH. En effet, ce protocole utilise les mécanismes d'encapsulation et de chiffrement des données. (11)

La technologie IPSEC présente deux modes de fonctionnement qui sont :

- Le mode « transport »
- Le mode « tunnel ».

Dans le cas du mode transport, les données sont prises au niveau de la couche 4 du modèle OSI (couche transport). Elles sont cryptées et signées avant d'être transmise à la couche IP. Ce mode est relativement facile à mettre en œuvre.

Le défaut présenté par le mode transport, est que, étant donné que le mécanisme s'applique au niveau de la couche transport, il n'y a pas d'adresse masquer. C'est pourquoi un deuxième mode peut être mis en œuvre, le mode tunnel, dans lequel l'encapsulation IPsec a lieu après que

les données envoyées par l'application ont traversé la pile de protocole jusqu'à la couche IP incluses. Dans ce cas, il y a bien masquage des adresses.

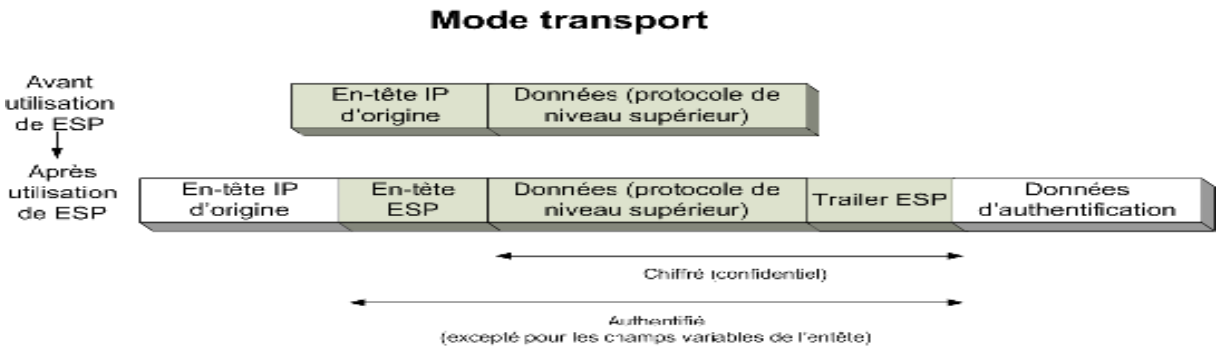


Figure 21 : Utilisation d'ESP en mode transport

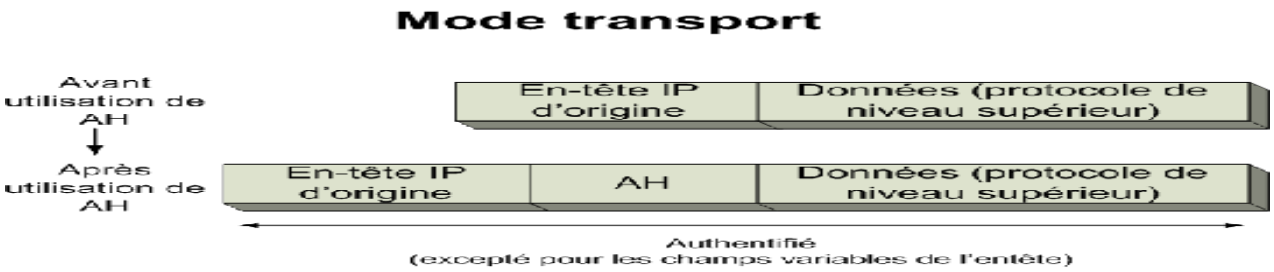


Figure 22 : Utilisation d'AH en mode transport

- **Prérequis :**

  Une passerelle IPsec et IPsec sur les clients.

- **Inconvénients**

  - IPsec ne permet d'identifier que des machines et non pas des utilisateurs => Mettre en place un système d'authentification.

  - IPsec à cause de la lourdeur des opérations de cryptage/décryptage réduit les performances globales des réseaux.

- **Utilisation :**

  -Intranet, extranet (Sites à sites).

CHAPITRE IV : MISE EN PLACE D'UNE SOLUTION VPN

1.1 Présentation du projet

Avant d'entamer la phase de réalisation de notre solution qui va permettre un accès externe à notre réseau d'entreprise via une connexion VPN de type OpenVPN, nous allons définir l'architecture de l'implémentation à réaliser.

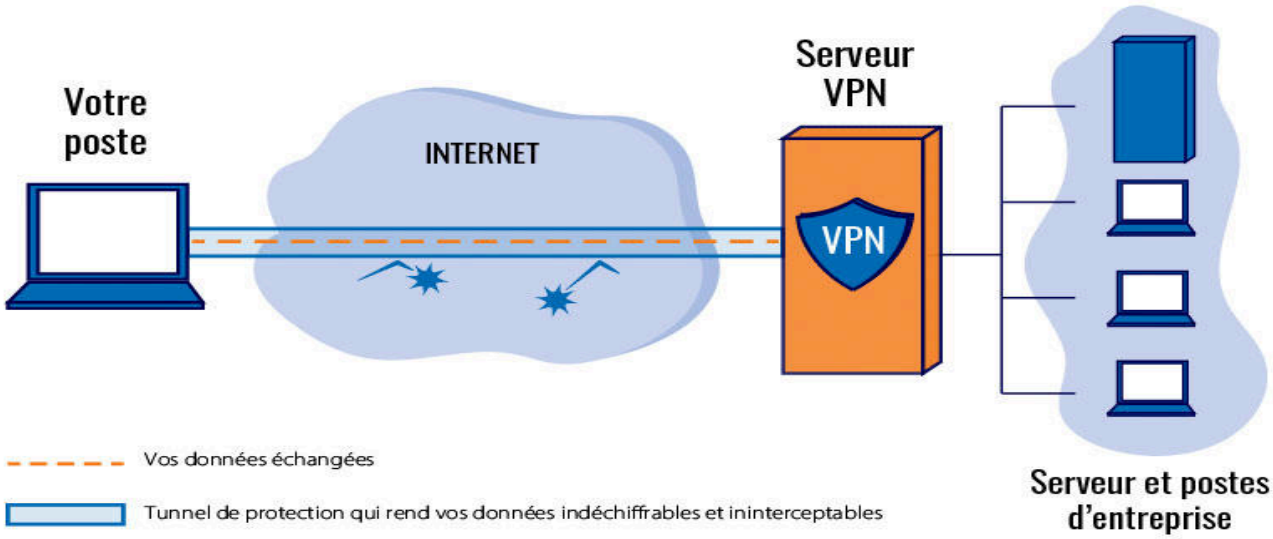


Figure 23 : Schéma d'un Réseau VPN

1.2 Description de l'environnement de travail

1.2.1 Notion de virtualisation

La virtualisation consiste à effectuer un travail sur un système d'exploitation qui est différent de celui de la machine hôte. Cette méthode offre plusieurs avantages notamment la possibilité de tester un système ou des logiciels dans un environnement simulé, tout en permettant l'exécution de plusieurs systèmes d'exploitation sur un seul et même ordinateur.

1.2.2 VMware Workstation

De façon simple, VMware est une solution logicielle professionnelle, puissante et complète qui nous permet de gérer l'ensemble de nos machines virtuelles locales sur le réseau.

1.2.3 Free BSD

FreeBSD est un système d'exploitation Unix libre. Le nom vient de l'association d'une part de free qui signifie à la fois « libre » et « gratuit » dans l'anglais courant, et d'autre part

de Berkeley Software Distribution (BSD), l'UNIX développé à l'université de Berkeley. Free prend un sens plus connoté dans ce nom : il signifie que le logiciel peut être utilisé gratuitement même pour un usage commercial, que les sources complètes sont disponibles et utilisables avec un minimum de restrictions quant à leur usage, leur distribution et leur incorporation dans un autre projet (commercial ou non), et enfin que n'importe qui est libre de soumettre son code source pour enlever un bug ou améliorer le logiciel, ce code étant incorporé aux sources après accord. (12)

L'objectif du projet FreeBSD est de fournir un système qui puisse servir à tout, avec le moins de restrictions possibles.

1.2.4 PfSense

PfSense est une distribution gratuite et personnalisée de FreeBSD qui peut transformer un ancien ordinateur en un routeur et un pare-feu complet. PfSense a été créé en 2004 en tant que fork du populaire projet m0n0wall. La principale différence entre pfSense et m0n0wall est que pfSense est conçu principalement pour être installé sur des PC au lieu d'appareils intégrés, ce qui permet à pfSense d'offrir plus de flexibilité et de fonctionnalités. PfSense est très flexible et peut facilement être adapté à de nombreuses applications allant d'un routeur domestique à un pare-feu pour un grand réseau d'entreprise.

PfSense est facile à installer et à entretenir, offrant une interface utilisateur Web très utile. PfSense inclut de nombreuses fonctionnalités que l'on ne trouve souvent que dans les routeurs commerciaux coûteux.

1.3 Création de la machine virtuelle

Pour installer VMware, la machine Windows doit disposer des caractéristiques suivantes :

Mémoire	8 GB
Processeur	Intel Core I5

Tableau 1: Caractéristique minimum de la machine

Figure 24 : Page d'accueil de vmware

Pour créer une nouvelle machine sur VMware, on clique sur « create a new virtual machine » dans la figure ci-dessus, après on clique sur « next », c'est arrivé à ce niveau que nous allons choisir le fichier du disque image de pfsense pour son installation.

Ensuite après avoir passé cette étape, on clique sur « next » jusqu'à atteindre la figure ci-dessous :

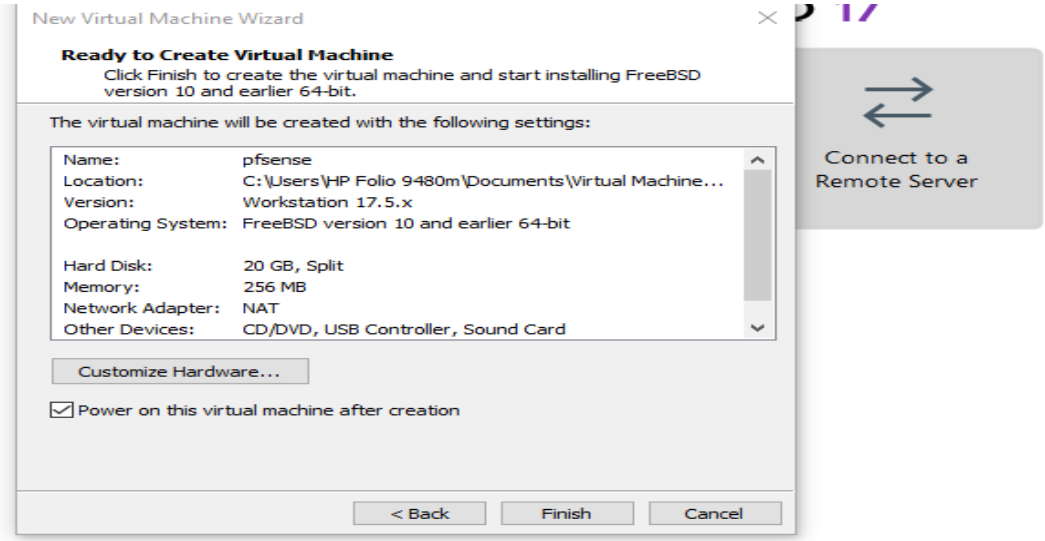


Figure 25 : Fin de création de la machine virtuelle

On clique ensuite sur « customize hardware… » pour la configuration des deux cartes réseaux dont on a besoin pour installer pfsense

- La première en mode bridge reliée au réseau WAN.
- La deuxième en NAT reliée au réseau LAN selon la figure suivante :

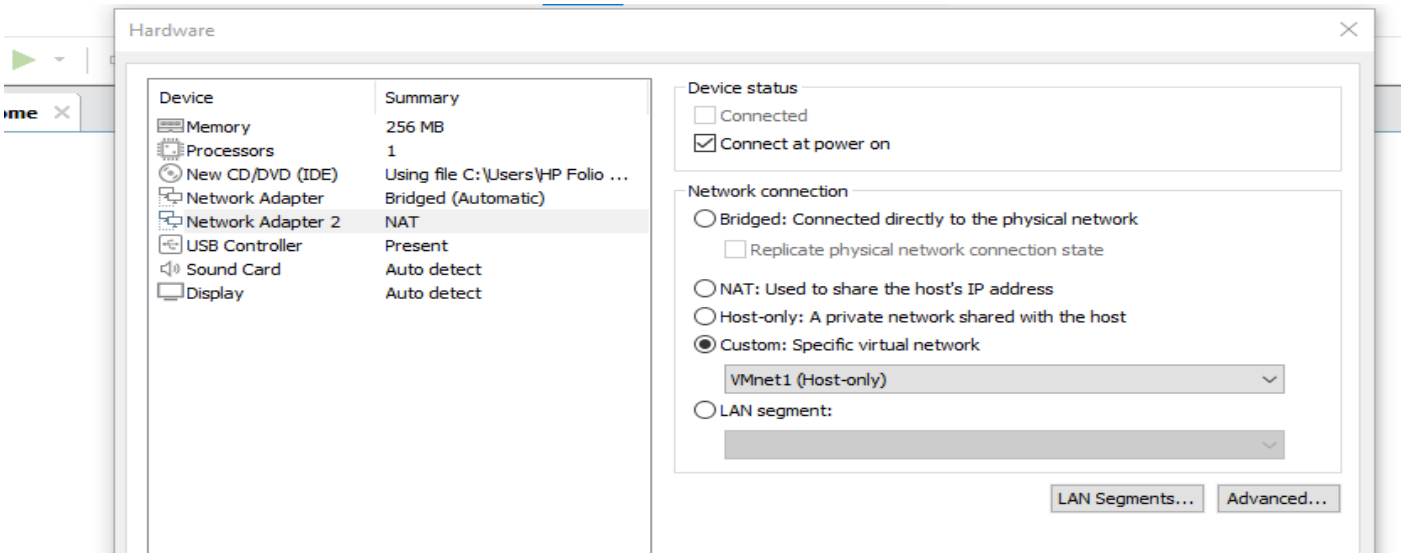


Figure 26 : Carte Réseau

Nous sommes ainsi à la fin de notre première étape qui est la création de notre machine virtuelle.

1.4 Installation et configuration de pfsense sous vmware

1.4.1 Installation de pfsense

Après avoir démarré notre machine à partir du cd de l'image Iso de pfsense, nous allons laisser le setup démarrer automatiquement et après quelques secondes on clique sur la touche « Entrée » pour valider.

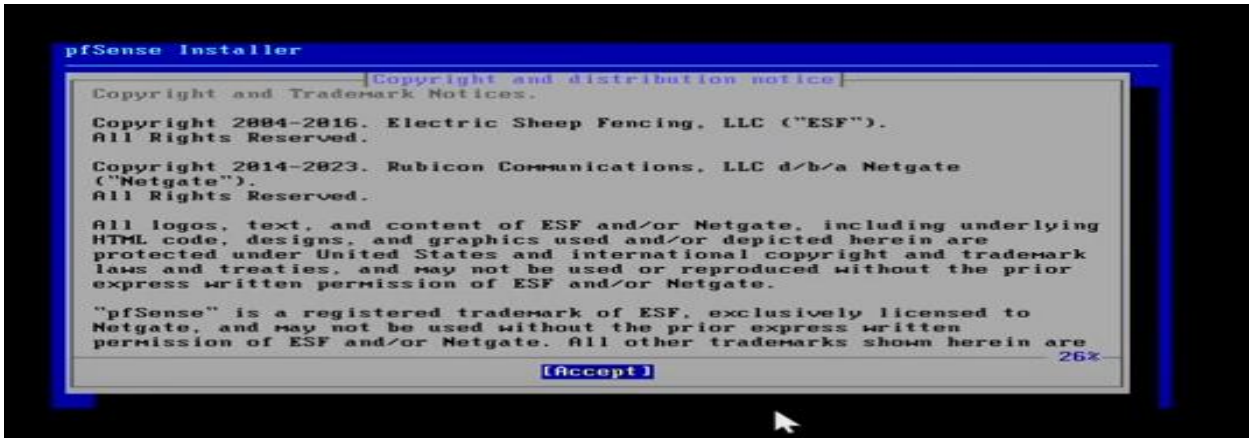


Figure 27 : Validation de l'installation

Ensuite nous allons tomber sur l'interface d'installation, on choisit « Install » et on fais un clique sur « Entrée » pour valider le « ok »

Figure 28 : Lancement de l'installation

Une fois l'installation achevé, on clique sur « Entré » sur les prochaines interfaces qui s'afficheront, ce qui nous conduira ensuite sur l'interface qui va nous permettre de sélectionner le disque dur virtuel en appuyant sur la touche « Espace ». On clique ensuite sur « ok » et « Yes » sur la page suivante qui s'affichera.

Après avoir passé cette étape, une installation se lancera sur l'extraction et la copie des fichiers. Après avoir terminé cette étape, on clique sur « Reboot » pour permettre à pfsense de se redémarrer avec la nouvelle installation.

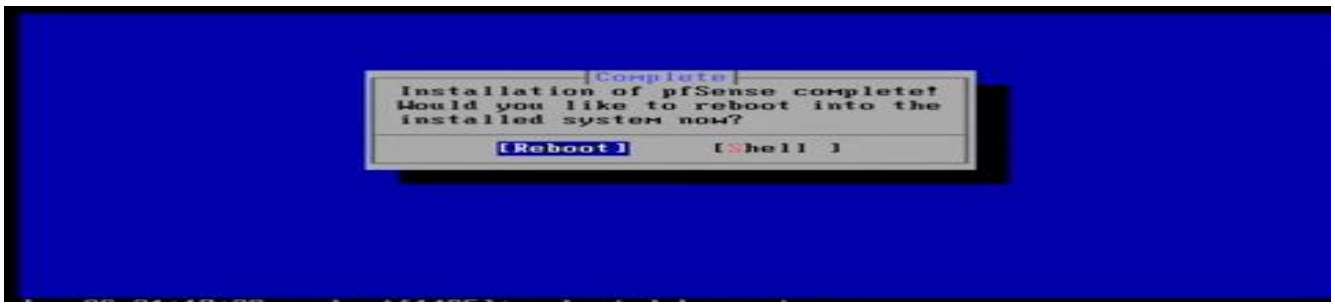


Figure 29 : redémarrage de pfsense

Au cours de l'installation, pfsense va faire la détection automatique des listes des cartes réseaux disponibles.

L'écran principale suivant s'affiche :

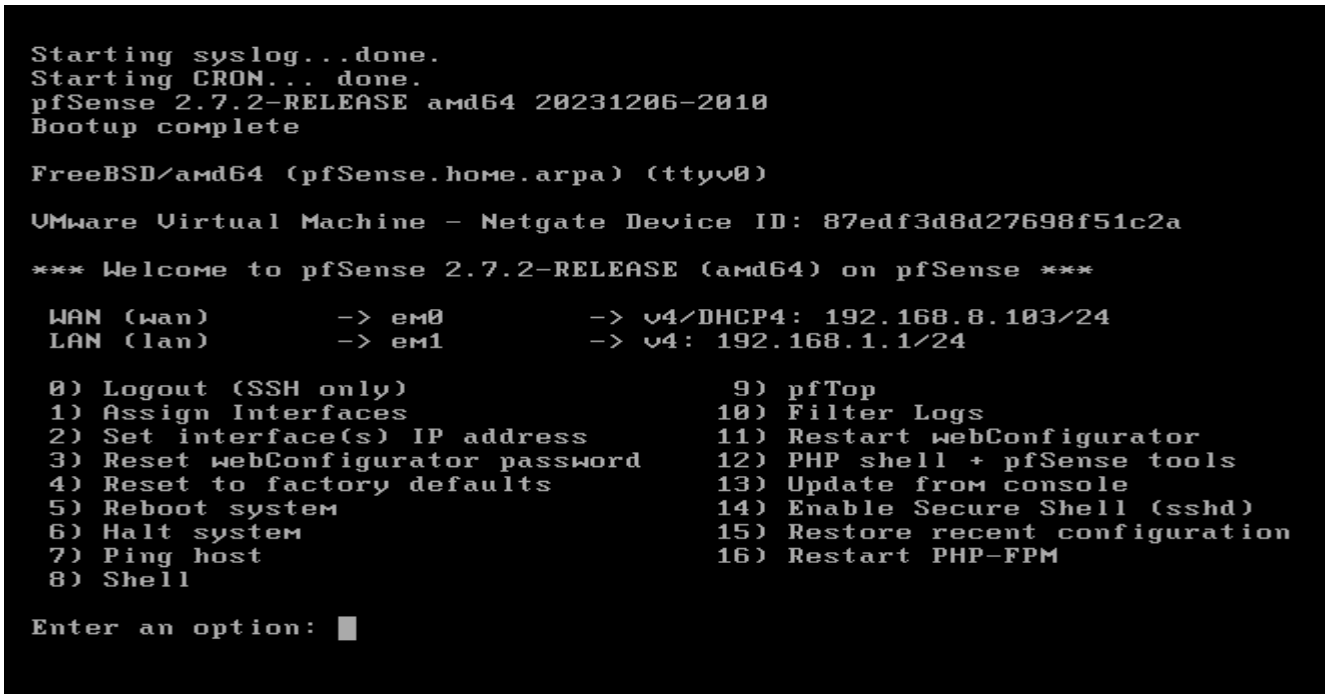


Figure 30 : Visualisation des interfaces réseaux

Une fois dans le menu de pfsense, on tape le choix 2 : « Set Interface IP address ». Pour affecter une adresse IP sur la passerelle de LAN de la machine de pfsense.

Enfin on aura le menu suivant :

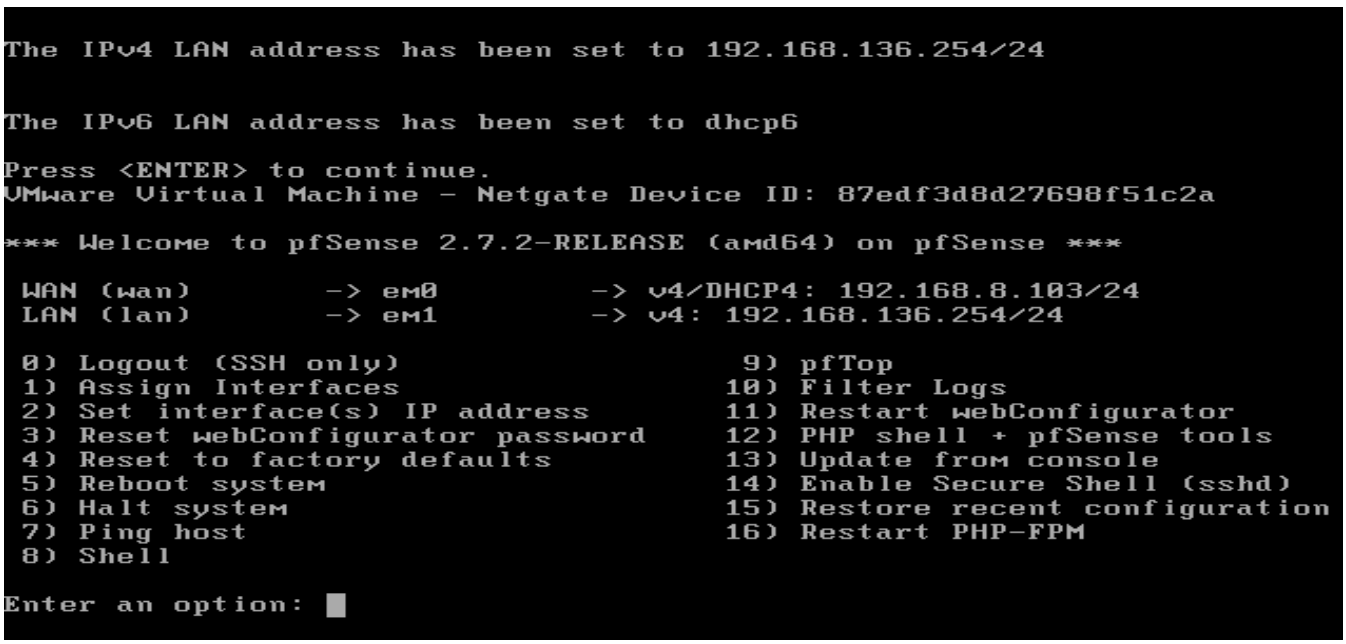


Figure 31 : Fin de l'installation

Pfsense		
Type de réseau	**WAN**	**LAN**
IP de l'interface	**192.168.8.103**	**192.168.136.254**
Masque de sous-réseaux	**255.255.255.0**	**255.255.255.0**

Tableau 2 : Tableau récapitulatif des interfaces WAN et LAN

1.4.2 Configuration de pfsense via l'interface web

L'étape suivante consiste à accéder à l'interface web du pfsense. Pour cela, on ouvre notre navigateur web et on tape : http://192.168.136.254, par défaut on met :

-identifiant : admin

-Mot de passe : pfsense

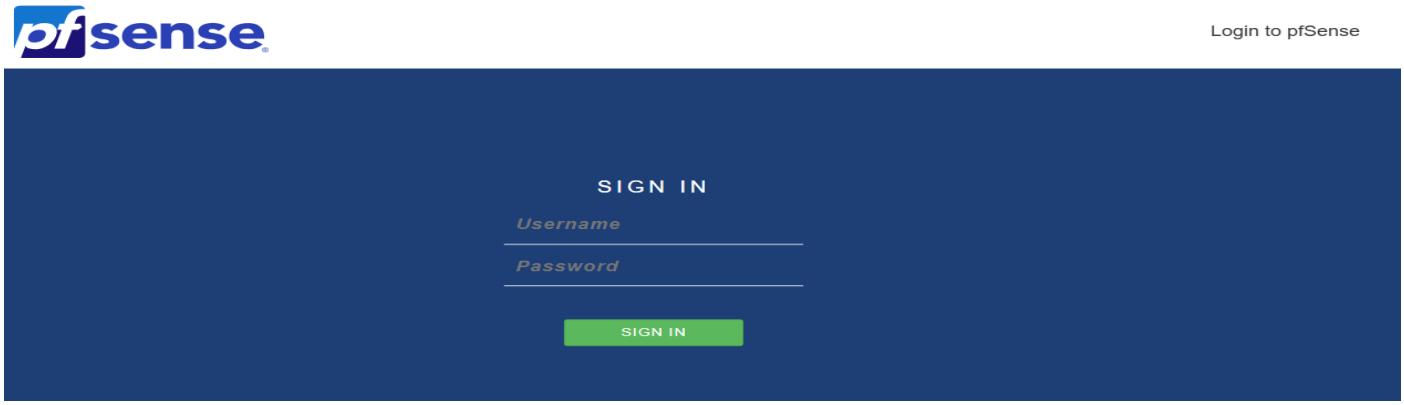


Figure 32 : Page de connexion de l'interface web

Une fois arrivée dans l'interface web, nous allons ensuite cliquer dans « system » puis « General setup » pour avoir accès à la page d'accueil de pfsense.

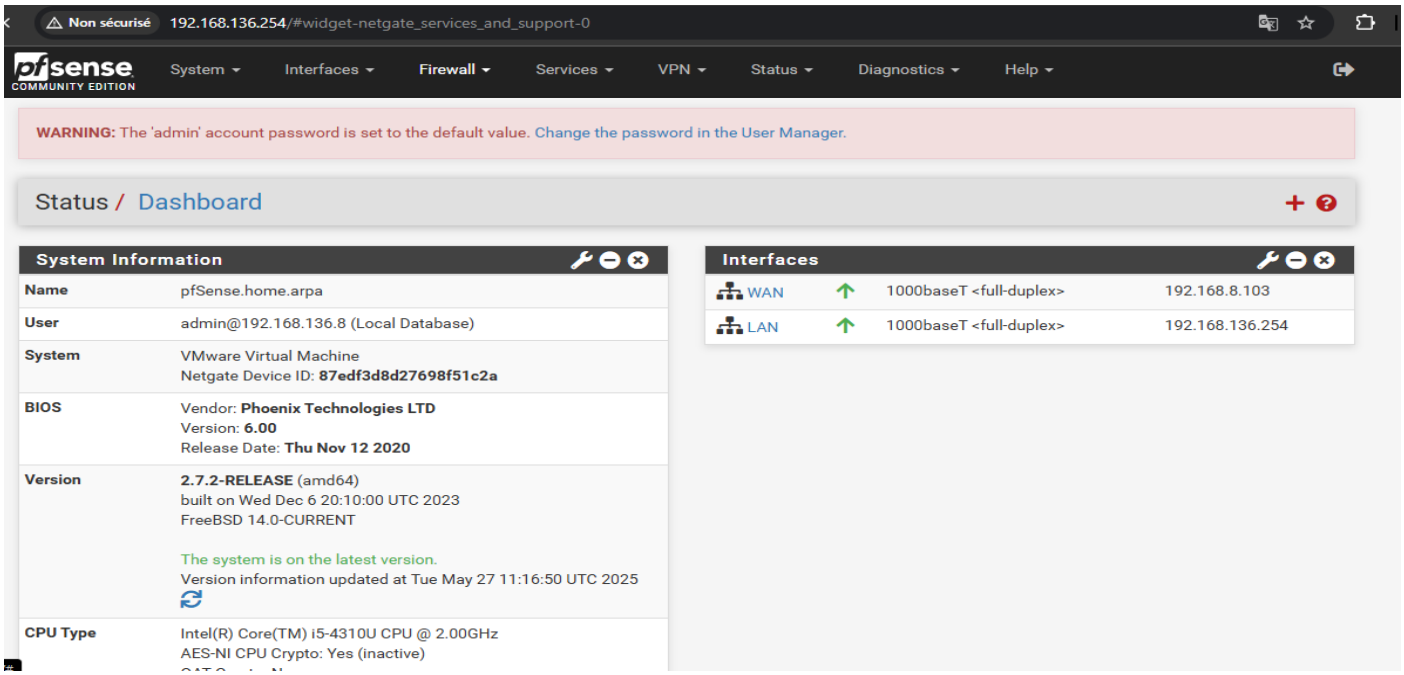


Figure 33 : Page d'accueil de pfsense

1.5 Mise en place du VPN Client-to-Site

Dans cette partie, nous allons voir les différentes étapes à suivre afin de configurer et de mettre en place un serveur/client VPN via OpenVPN.

1.5.1 Présentation de OpenVPN

OpenVPN permet à des pairs de s'authentifier entre eux à l'aide d'une clé privée partagée à l'avance, de certificats électroniques ou de couples de noms d'utilisateur/mot de passe. Il utilise de manière intensive la bibliothèque d'authentification OpenSSL ainsi que le protocole SSLv3/TLSv1. Disponible avec une multitude d'environnements tel que Solaris, OpenBSD, FreeBSD, NetBSD, Linux (Debian, Redhat, Ubuntu, etc.), Mac OS X, Windows 2000, XP, Vista, 7, 8 ,10 et 11, ainsi que les systèmes mobiles Android et iOS, il offre de nombreuses fonctions de sécurité et de contrôle.

OpenVPN n'est pas compatible avec IPsec ou d'autres logiciels VPN. Le logiciel 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.

1.5.2 Présentation d'Open SSL

OpenSSL est une boîte à outils de chiffrement comportant deux bibliothèques, libcrypto et libssl, fournissant respectivement une implémentation des algorithmes cryptographiques et du protocole de communication SSL/TLS, ainsi qu'une interface en ligne de commande, openssl.

1.6 Mise en place du serveur OpenVPN

La première chose dont on aura besoin est de définir une autorité de certification interne avec son propre certificat pour pouvoir ensuite auto signer les différents certificats que nous avons allons créer. On aura donc besoin à la fois d'un certificat (au niveau de pfsense) pour le serveur et pour le client qui seront ensuite signer par l'autorité de certification interne que nous aurons créée, on va d'abord commencer par la création de notre autorité de certification.

1.7.1 Création du certificat d'autorité (CA)

Pour se faire nous allons cliquer sur « système » puis sur « certificates » dans la fenêtre principale de pfsense.

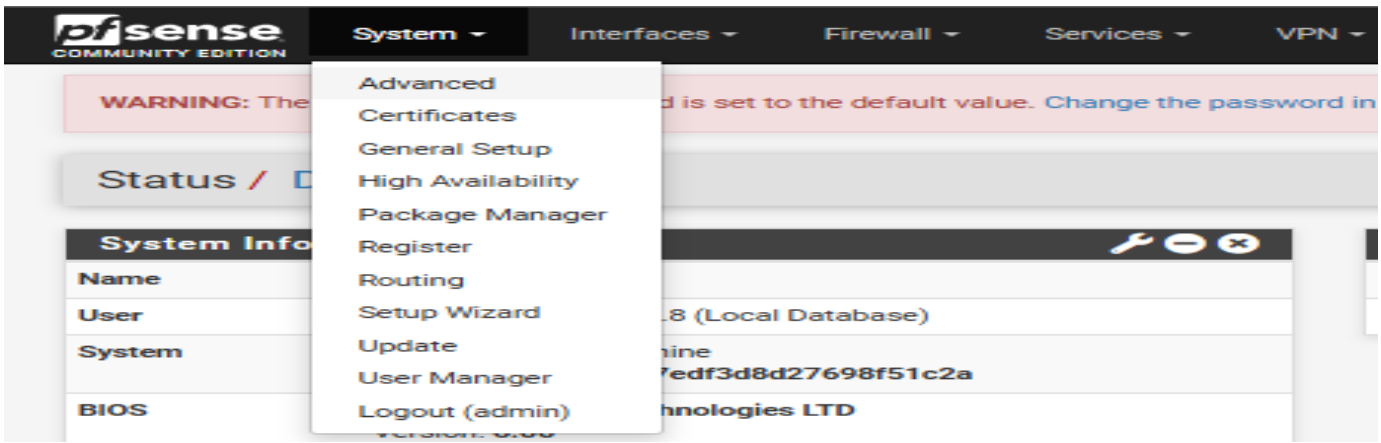


Figure 34 : Accès à l'interface web

Une fois dans l'onglet « certificates authorities », cliquer sur ajout « +Add » pour la création d'un nouveau certificat d'autorité.

Nous allons remplir les champs comme suit :

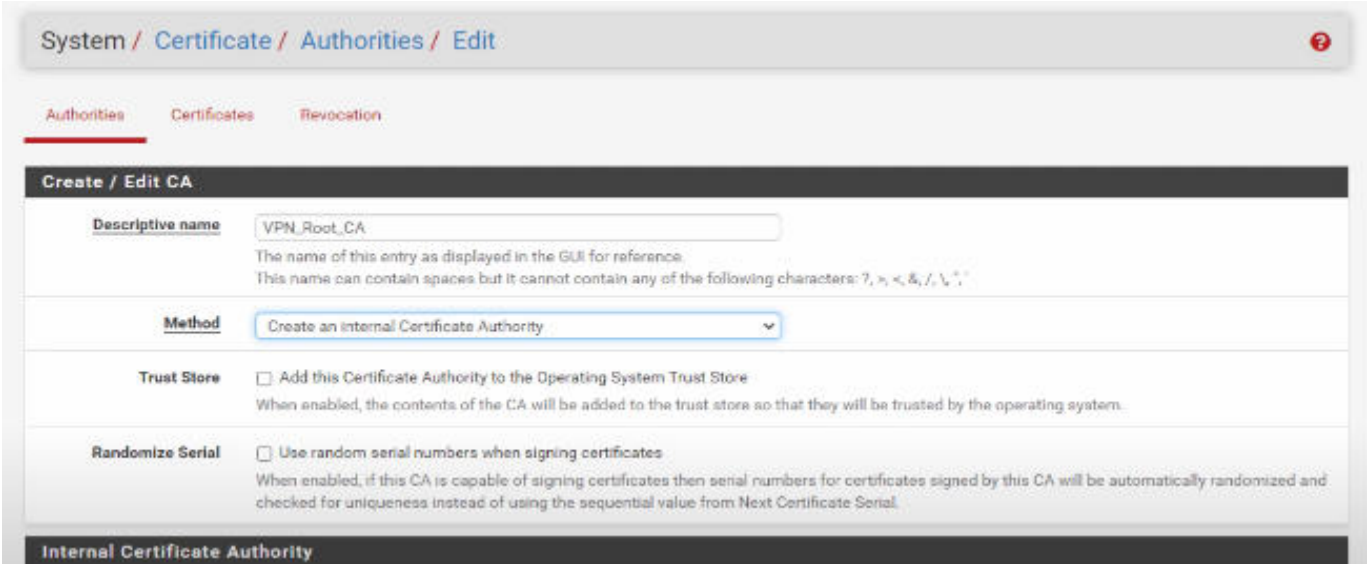


Figure 35 : Création du certificat d'autorité

Ensuite, nous allons remplir le formulaire « Internal Certificate Authority » comme suit :

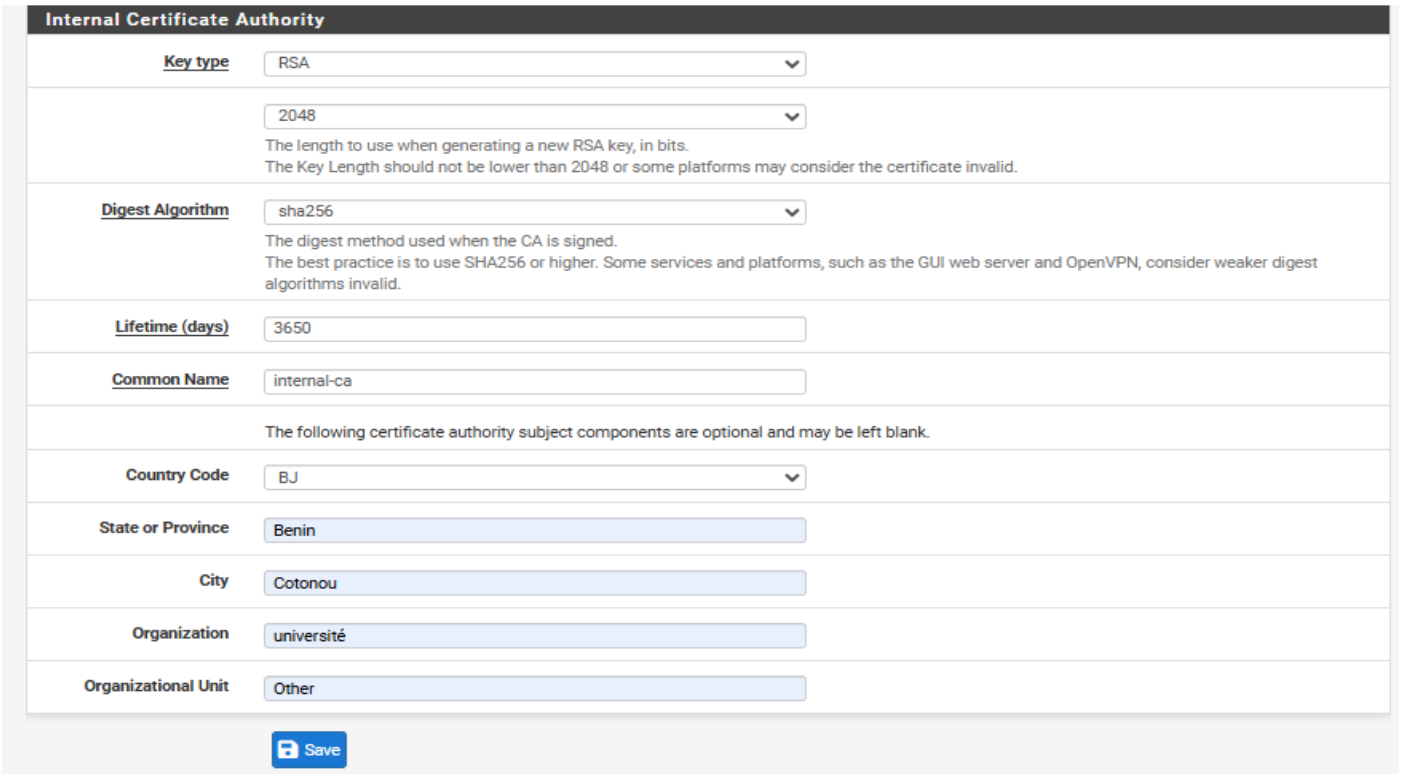


Figure 36 : Création du certificat d'autorité

Après avoir cliqué sur « save » nous pouvons voir que notre certificat est bel et bien créé.

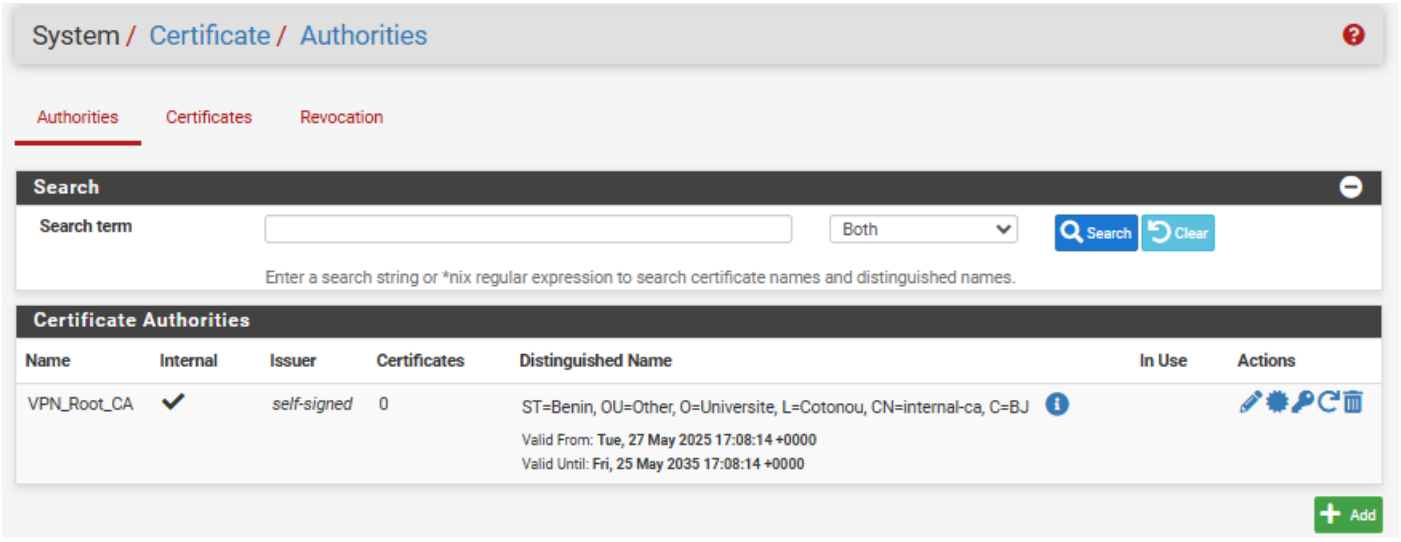


Figure 37 : Fin de la création du certificat d'autorité

1.7.2 Création du certificat serveur

Pour créer notre certificat serveur, on clique sur l'onglet « certificates » juste à côté de l'onglet « authorities ». Ensuite, on clique sur le bouton ajout « +Add » pour la création de notre certificat serveur.

Nous allons donc remplir notre formulaire comme suit :

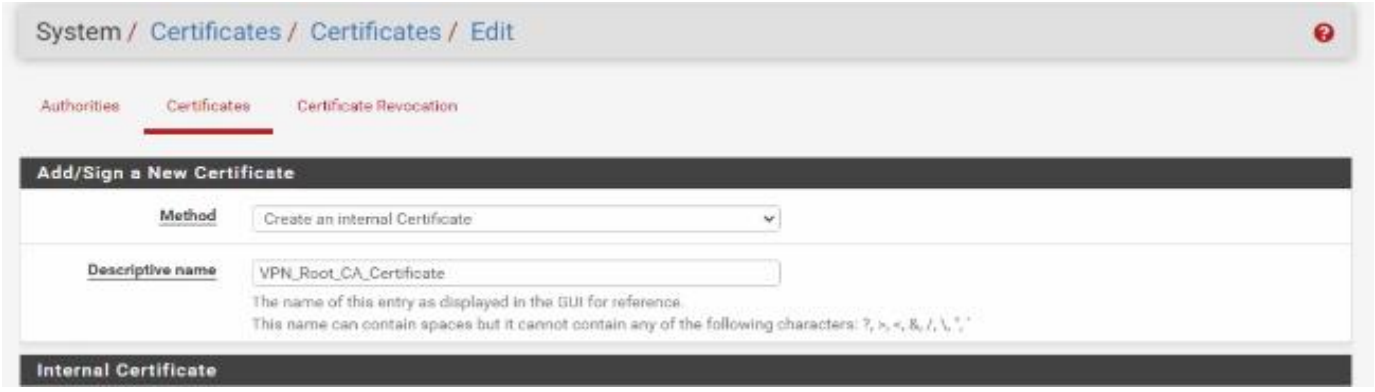


Figure 38 : Création du certificat serveur

Ensuite, le formulaire « Internal Certificates » est rempli de la même manière que celle de la figure 38. Passons ensuite au formulaire « Certificates Attributes », que nous allons remplir comme suit :

Figure 39 : Création du certificat serveur

Après avoir sauvegarder les information « save », nous pouvons voir que notre certificat serveur est bel et bien créé.

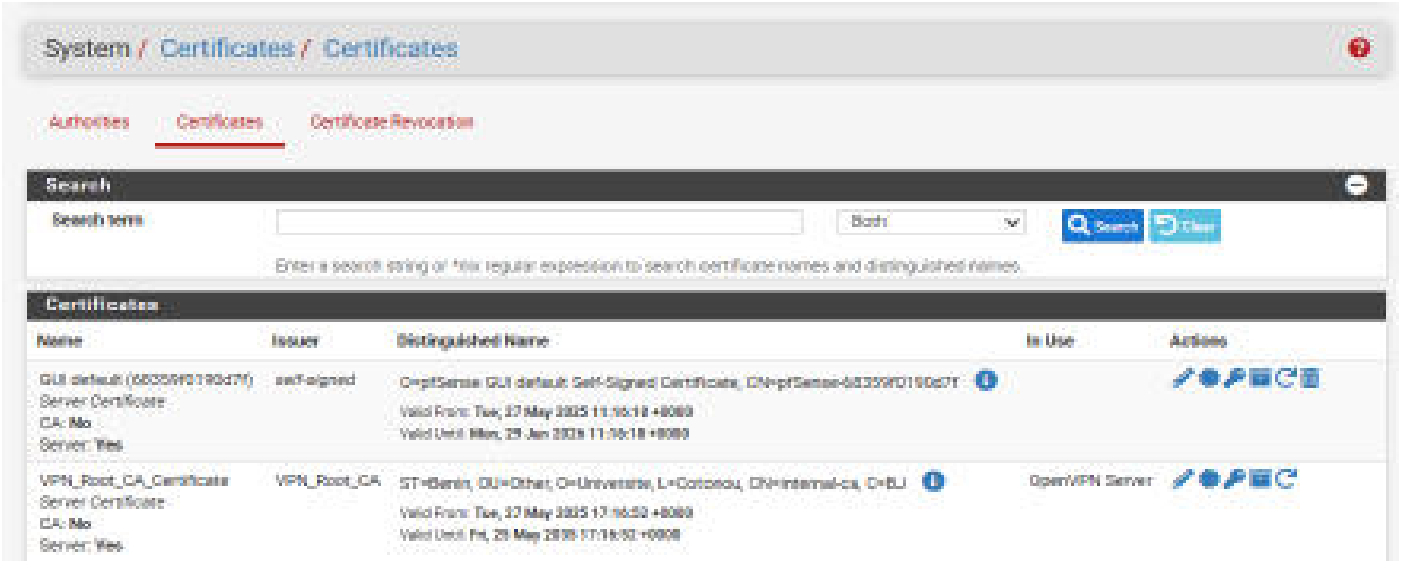


Figure 40 : Fin de la création du certificat serveur

1.7.3 Configuration du serveur OpenVPN

Pour la configuration de notre serveur OpenVPN, nous allons cette fois cliquer sur « VPN » et choisir l'option « OpenVPN ».

Après avoir cliqué sur « OpenVPN » nous allons ensuite cliquer sur « Wizards ».

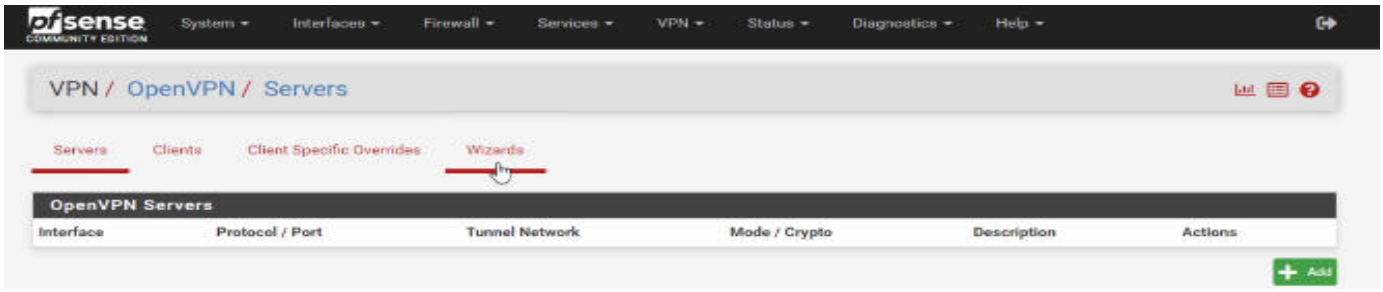


Figure 41 : Configuration d'OpenVPN

Après avoir cliqué sur « Wizards » on clique ensuite sur « Next ». Au niveau de l'option « choose a certificate authority », on choisit notre certificat d'autorité créer et on clique sur « Next ».

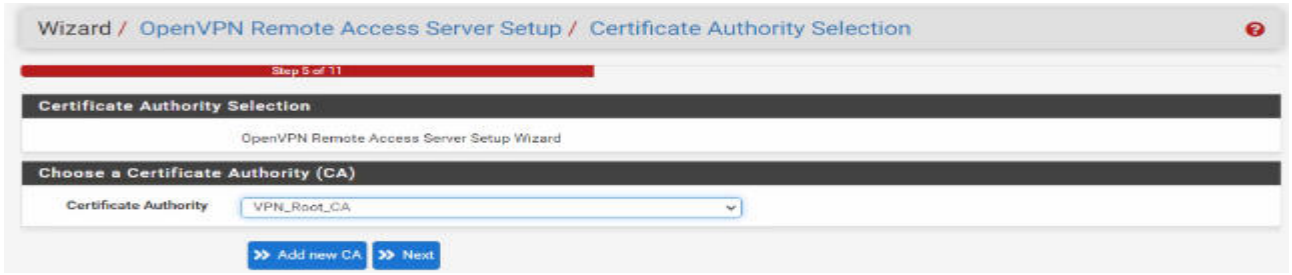


Figure 42 : Choix du certificat d'autorité

Dans la page suivante, on va choisir notre certificat serveur créé et on clique sur « Next ». Une fois à l'étape 9/11, nous allons remplir le formulaire comme suit :

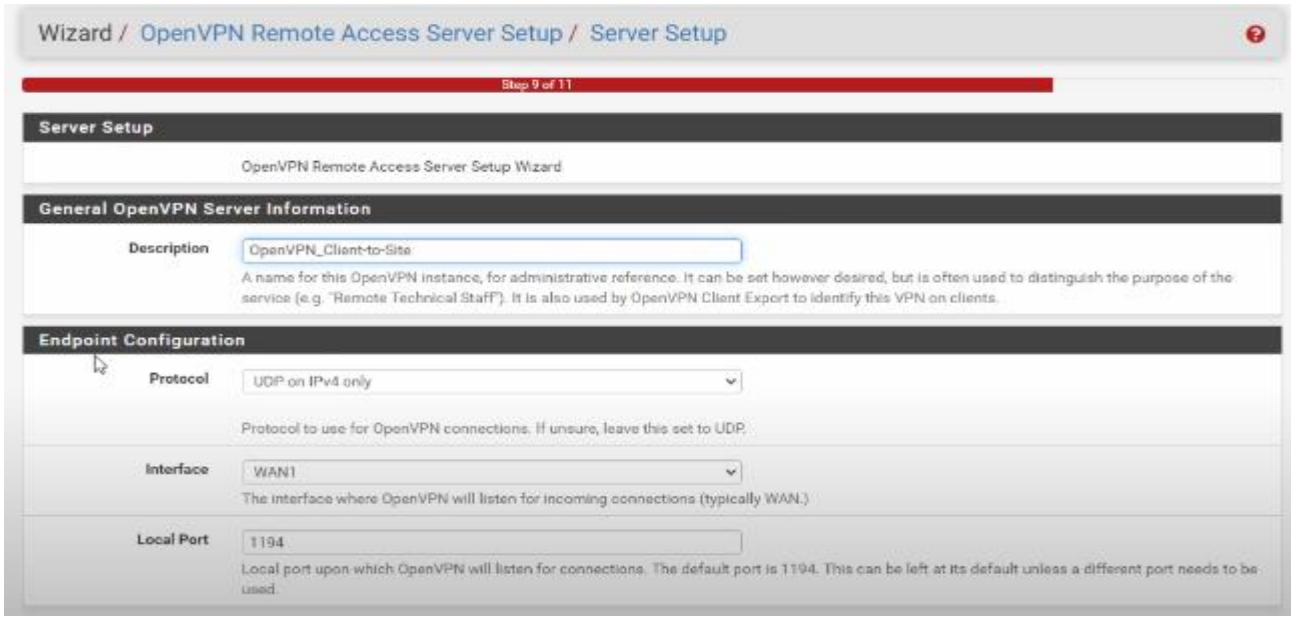


Figure 43 : Configuration d'OpenVPN

Dans le formulaire du « tunnel settings », nous allons mettre au niveau de notre « IPv4 Local Network » notre adresse réseau local qui est le 192.168.136.0/24 et garder les informations restantes par défaut.

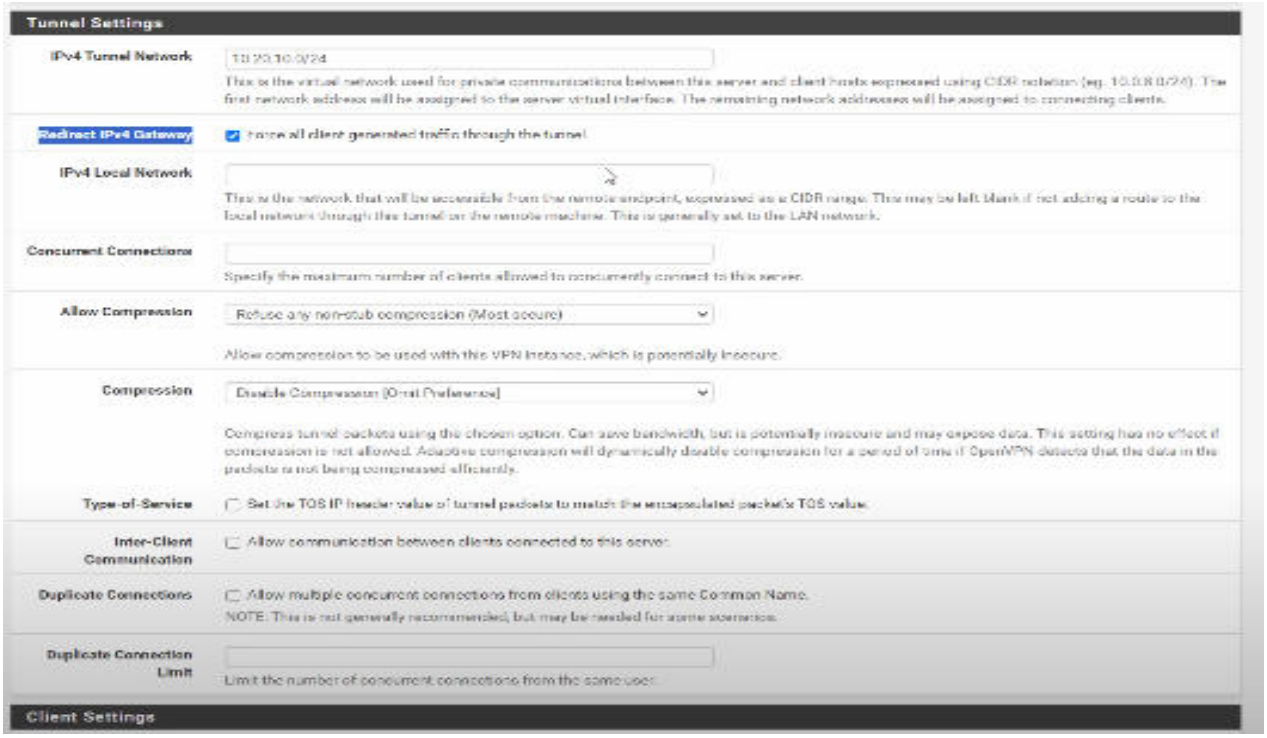


Figure 44 : Configuration d'OpenVPN

Ensuite, garder les formulaires « clients Settings » et « Advanced client settings » par défaut et cliquer sur « Next ». On passe ensuite à l'avant dernière étape qui va nous permettre de créer automatiquement des règles de pare-feu dans pfsense concernant la connexion VPN. Pour se faire, on coche la case « Firewall Rule » et celle de « OpenVPN Rule » et on clique ensuite sur « Next ». Ensuite, on clique sur « finish » dans la page suivante pour terminer la configuration ce qui marque ainsi la fin de la configuration de notre serveur OpenVPN.

Nous allons maintenant vérifier que notre tunnel VPN a bien été créer.

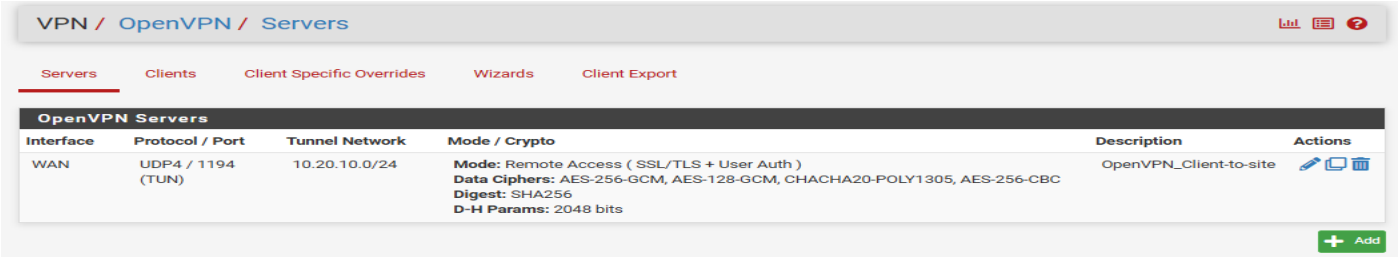


Figure 45 : Fin de la configuration d'OpenVPN

1.7.4 Configuration d'un client OpenVPN

Cette étape est importante pour établir la connexion entre le client et le serveur VPN. Nous allons donc cliquer sur « clients » juste à côté de l'option serveur comme nous pouvons le voir dans la figure 49, nous allons ensuite cliquer sur « +Add ». Les formulaires seront remplis comme suit :

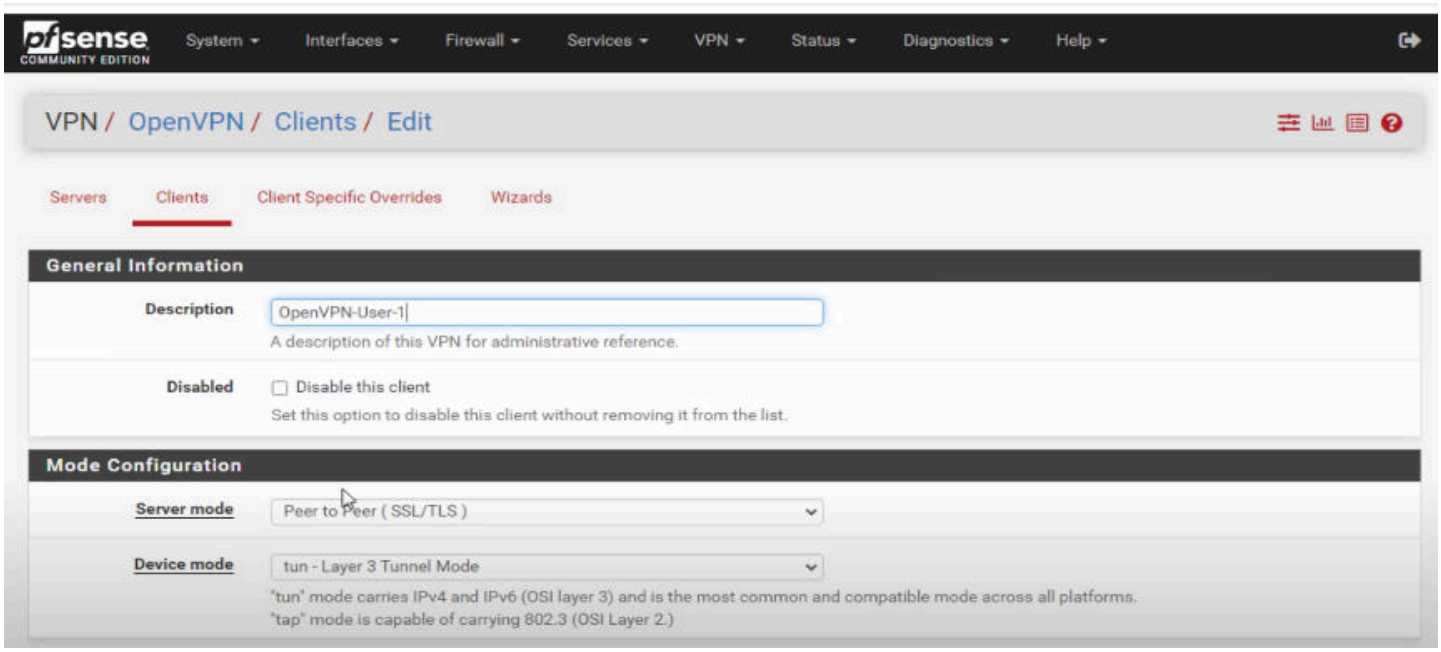


Figure 46 : Configuration d'un client OpenVPN

Dans le formulaire « Endpoint Configuration » nous allons mettre notre adresse IP WAN qui est le 192.168.8.103 comme mentionné dans le tableau 1.2.

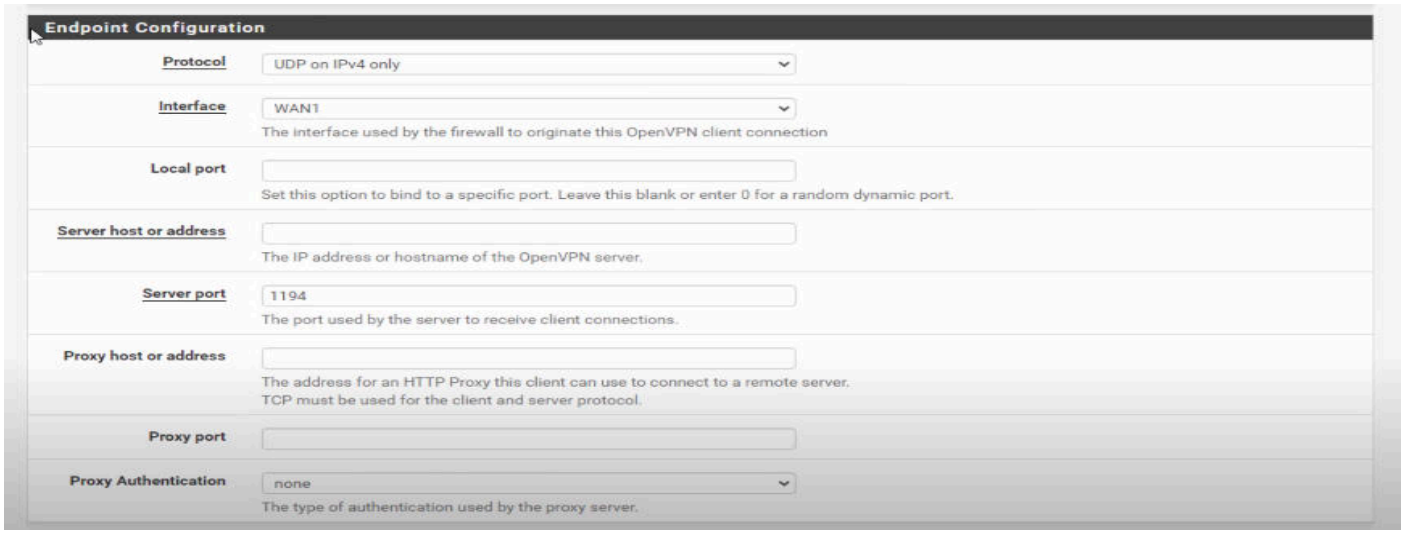


Figure 47 : Endpoint Configuration

Dans le formulaire « User Authentication Settings ». Nous allons le remplir comme suit :

Username : vpnuser1

Password : vpnuser1

Figure 48 : Paramètre d'authentification de l'utilisateur

Cette étape est importante car les informations d'identification entrée par le client seront utilisées pour l'authentification auprès du serveur OpenVPN.

Ensuite, le formulaire « cryptographic settings » sera rempli comme suit :

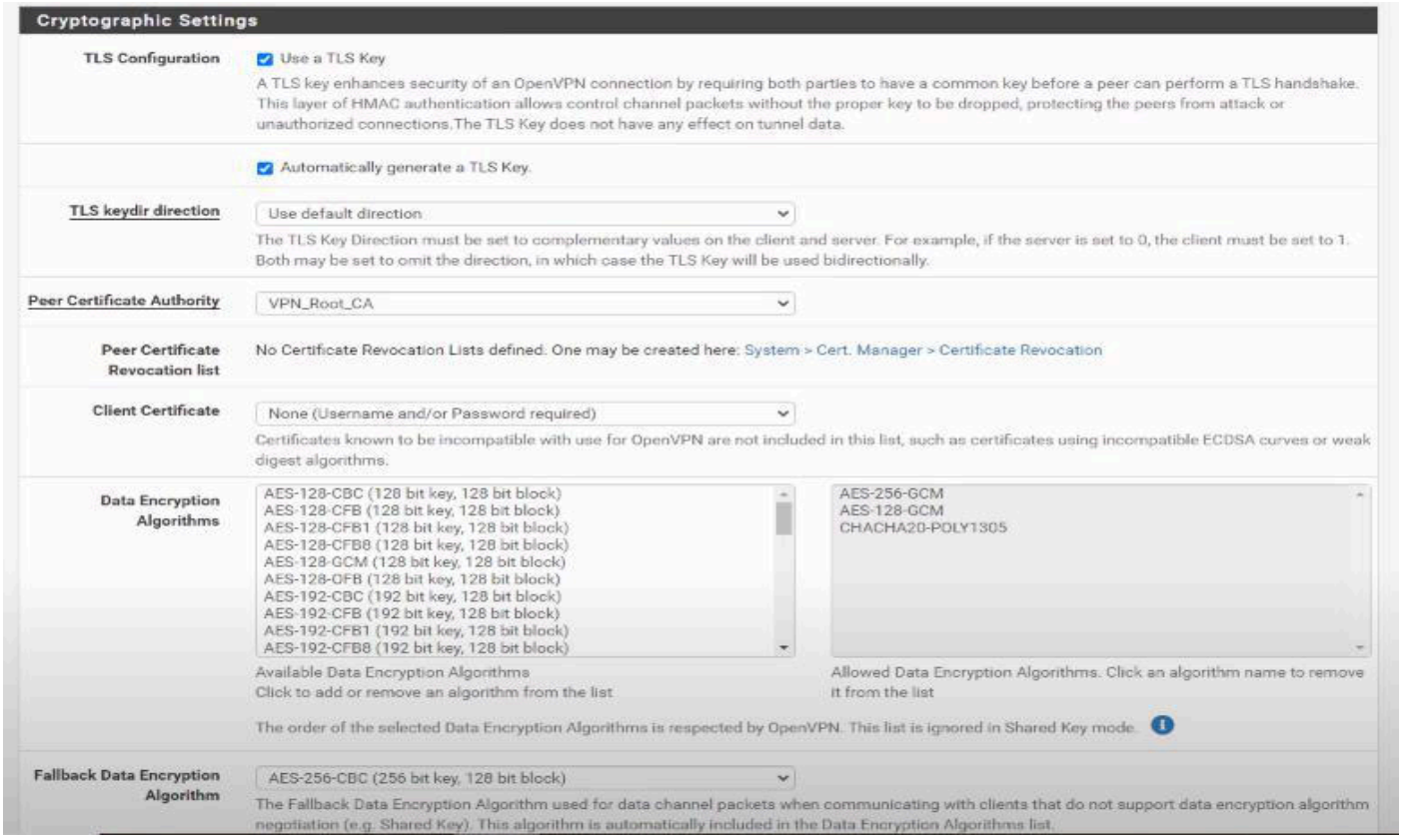


Figure 49 : Paramètre cryptographique

Les formulaires « Tunnel Settings », « Ping Settings » et « Advanced Configuration » sont tous garder par défaut. On clique ensuite sur « save » pour enregistrer les informations de notre configuration.

Vérifions que notre configuration est terminée.

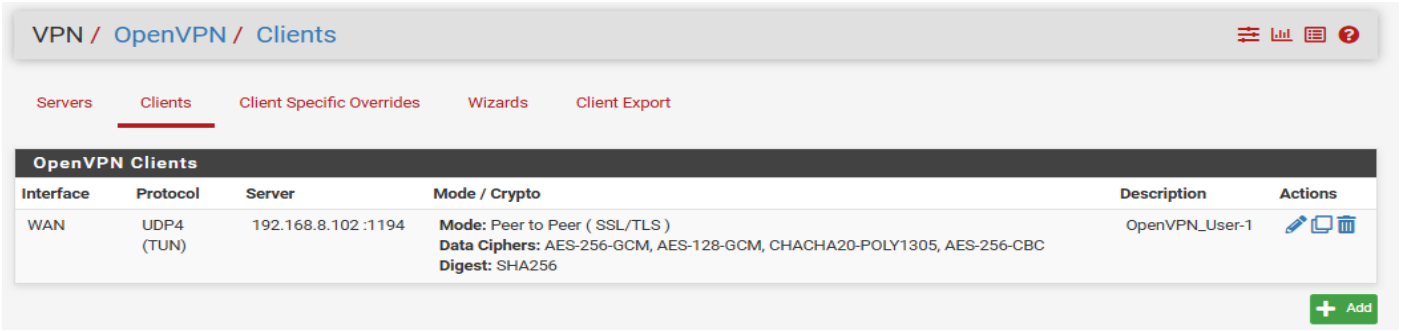


Figure 49 : Fin de configuration de notre Client OpenVPN

1.7.5 Création du certificat utilisateur

Pour créer le certificat utilisateur, on se rend dans le menu de notre pfsense ensuite on clique sur « System » puis ensuite sur le sous-menu « User manager » puis on clique sur le bouton ajout « +Add ». On remplit ensuite le formulaire « User Properties » comme suit :

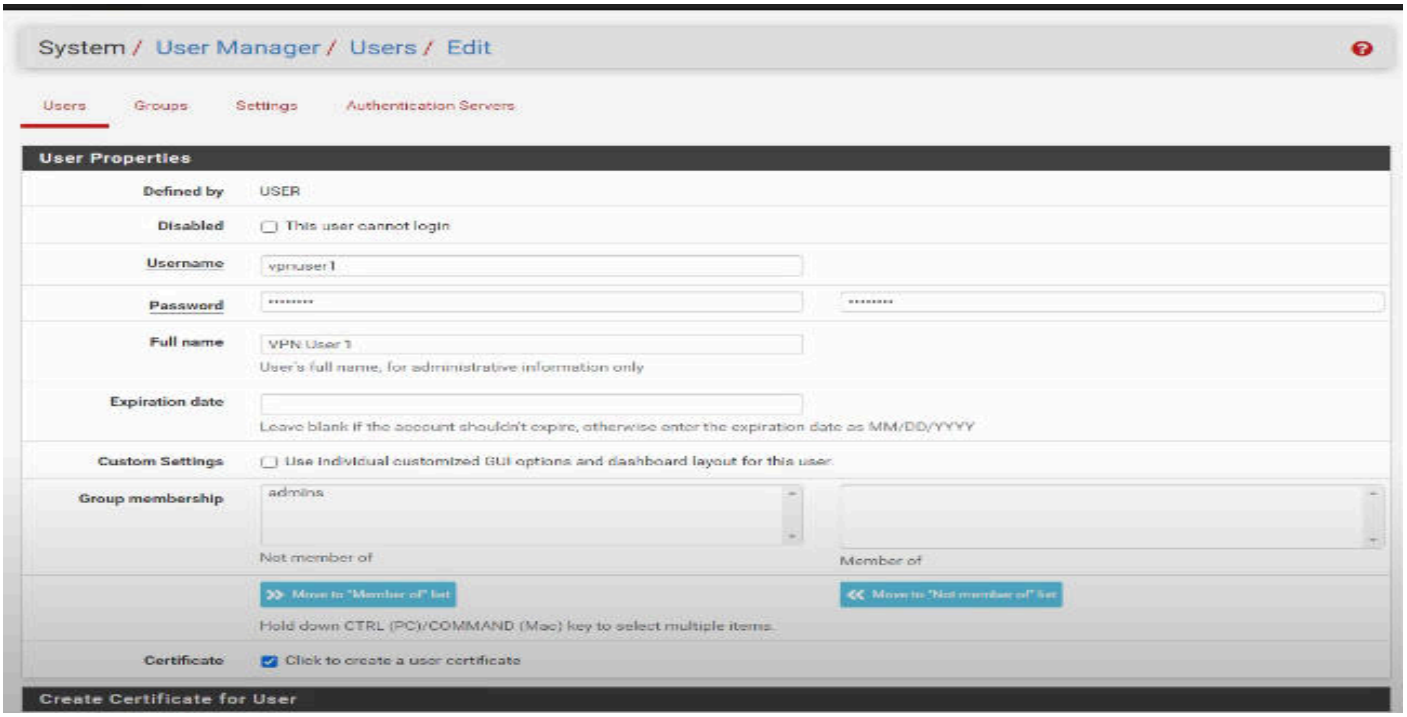


Figure 50 : Création du certificat utilisateur

Après avoir coché l'option « Certificate » nous allons passer ensuite à la création de notre certificat serveur en remplissant le formulaire « create certificate for User » comme suit :

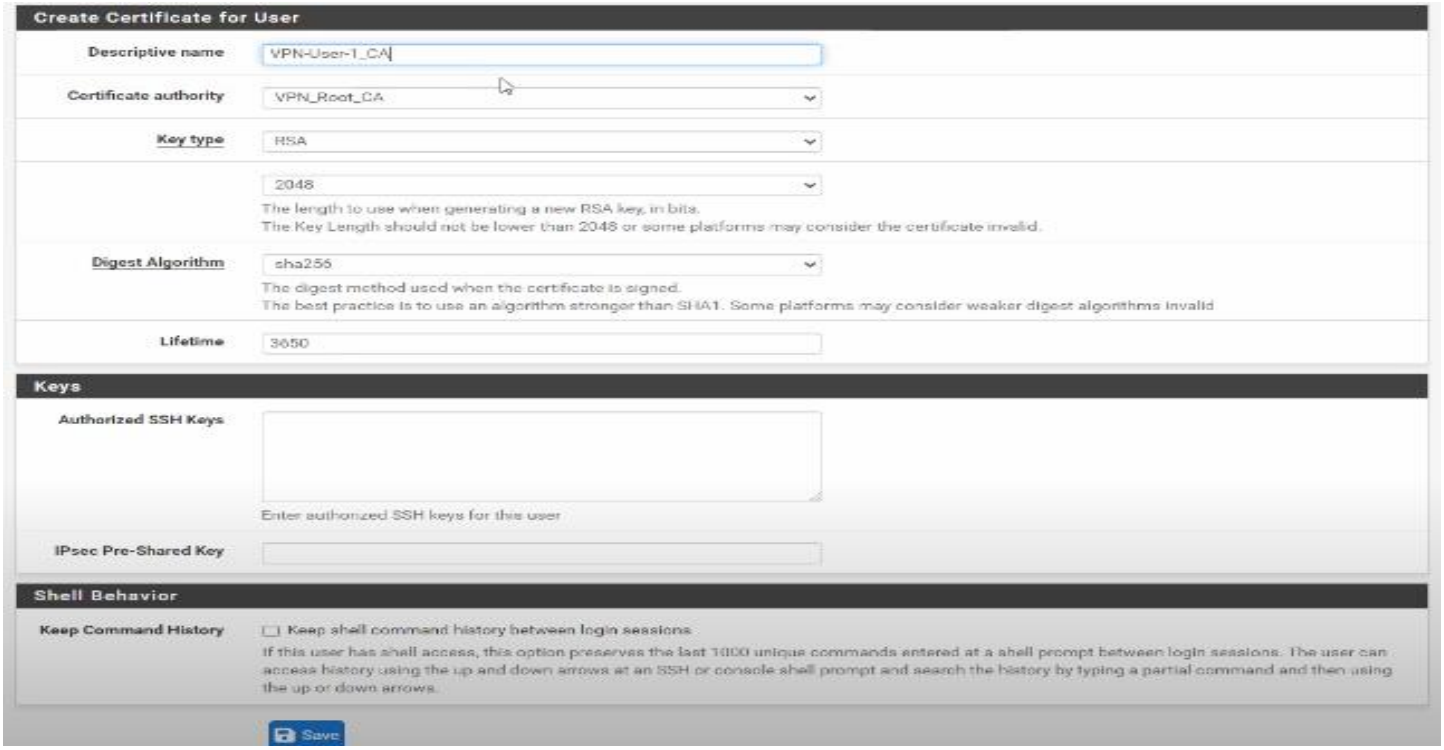


Figure 51 : création du certificat utilisateur

Nous avons ainsi terminé la configuration de notre certificat utilisateur.

1.7.6 Installation du package openvpn-client-export

Maintenant, passons à la récupération de notre configuration grâce à un plugin que nous allons installer. Nous allons donc aller dans le menu de notre pfsense et ensuite cliquer sur « System » puis ensuite sur « Package Manager ».

Après avoir cliqué sur « package manager », on clique ensuite sur « Available Packages » et on saisit « openvpn » dans la barre de recherche. Ensuite, nous allons cliquer sur le bouton « Install » de l'extension nommée « openvpn-client-export »

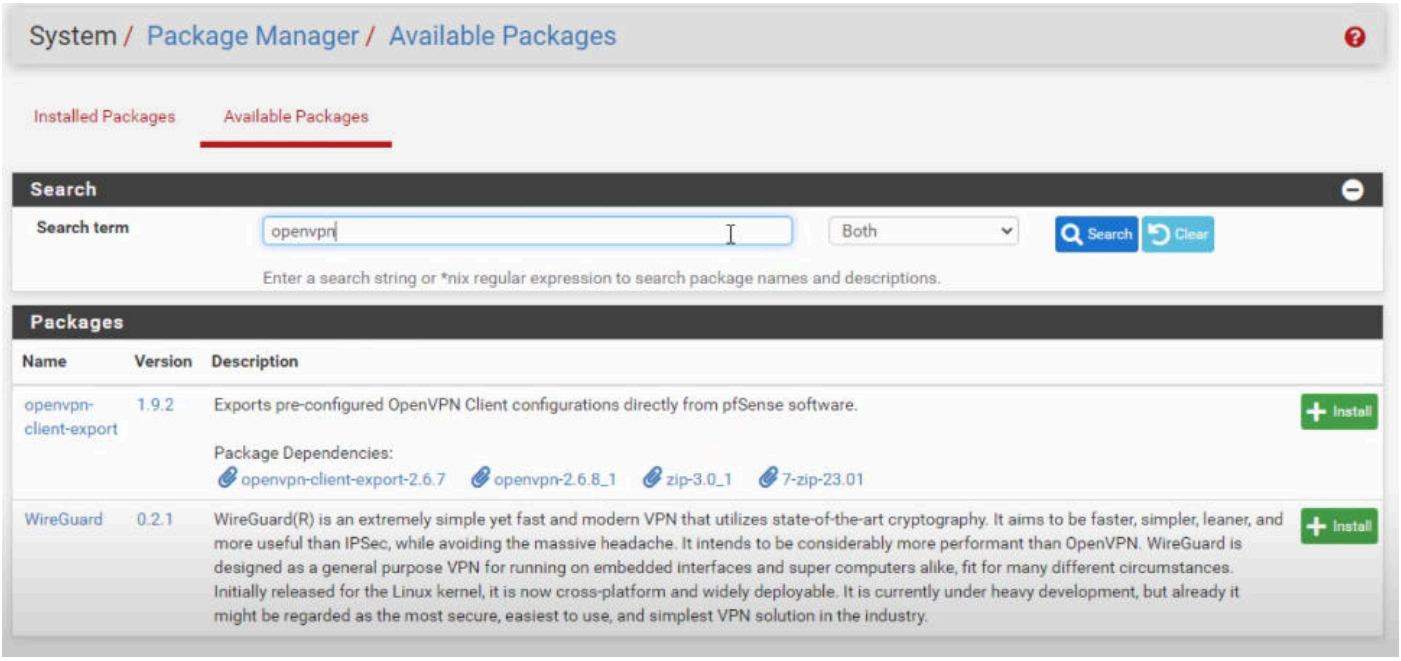


Figure 52 : Installation du package openvpn-client-export

Après avoir confirmé l'installation de ce plugin, l'installation débutera et s'achèveras après quelques minutes.

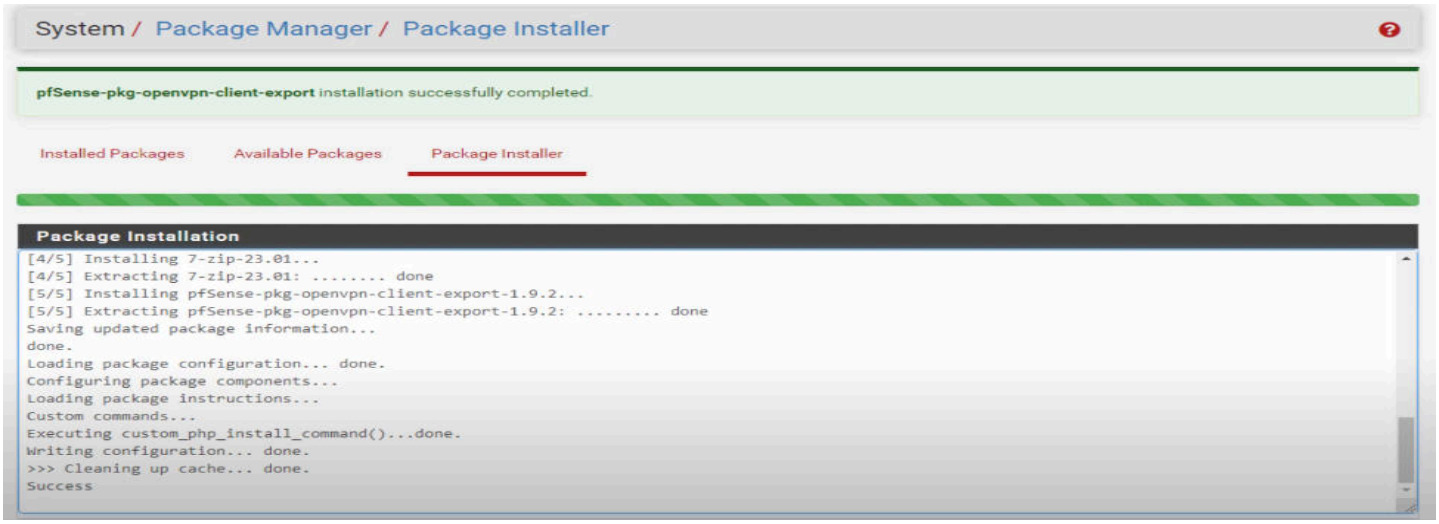


Figure 53 : Fin de l'installation du package openvpn-client-export

1.7.7 Téléchargement du package OpenVPN

Pour pouvoir télécharger le package OpenVPN, nous allons revenir dans le menu principal de pfsense et ensuite cliquer sur « VPN » puis « OpenVPN », une nouvelle option nommée « client Export » va s'ajouter nous allons cliquer dessus. Ce qui nous reconduira vers la page ci-dessous :

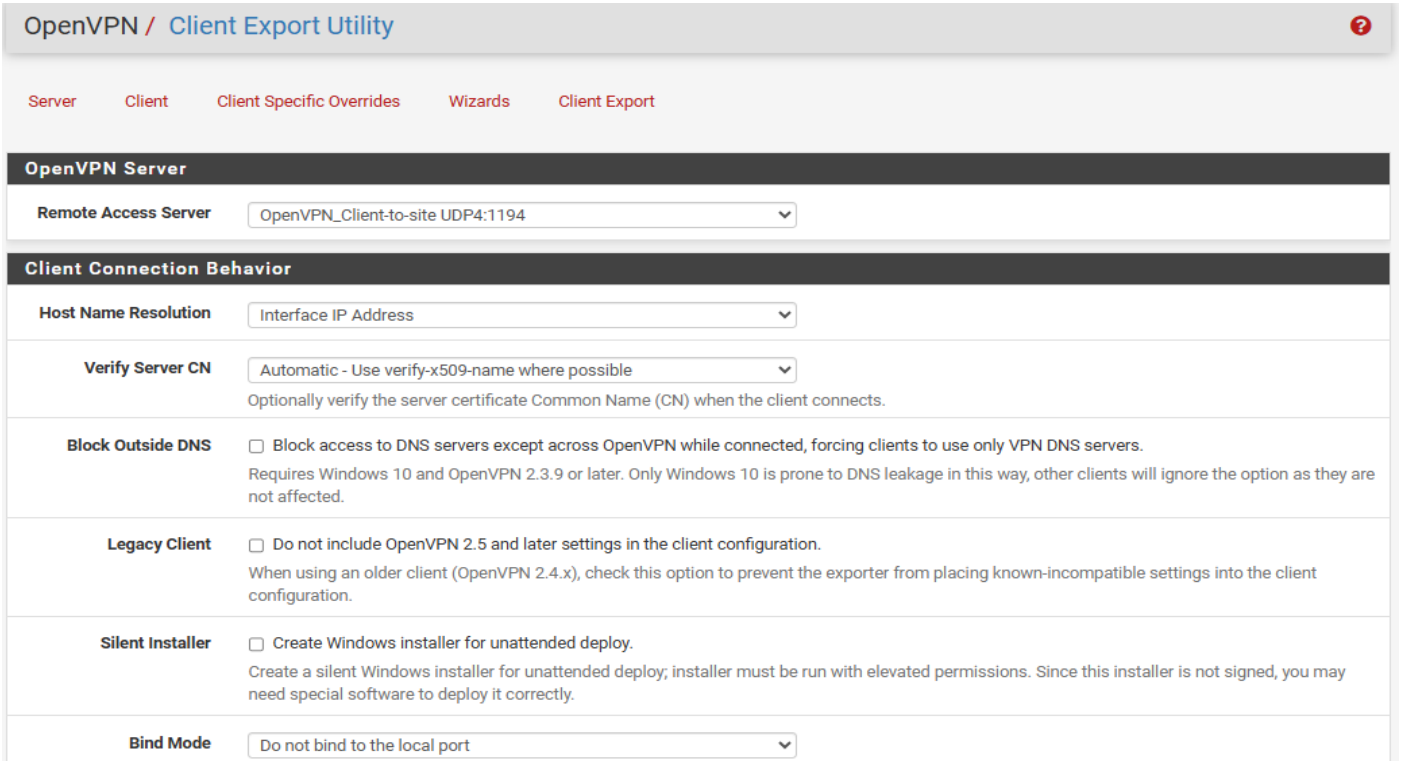


Figure 54 : Téléchargement du package OpenVPN

En glissant vers le bas nous allons retrouver plusieurs liens de téléchargement pour obtenir la configuration dont nous avons besoin pour la connexion au VPN. Choisissez celui qui correspond à votre système d'exploitation.

Dans notre cas nous avons choisi :

- Previous Windows Installers (2.5.9-Ix601)

-64 bits

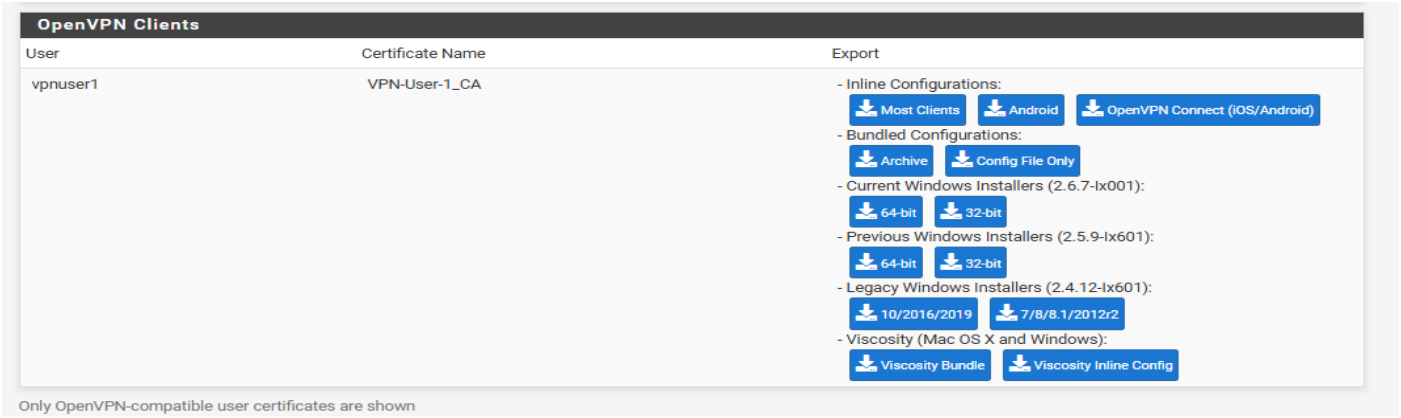


Figure 55 : Lien de téléchargement du package

1.7.8 Installation du client OpenVPN

Après avoir finaliser le téléchargement de notre package, nous allons ensuite le déplacer dans notre bureau.

Figure 56 : fichier d'installation du package

Après avoir passé cette étape, nous allons exécuter notre fichier « **En tant qu'administrateur** ».

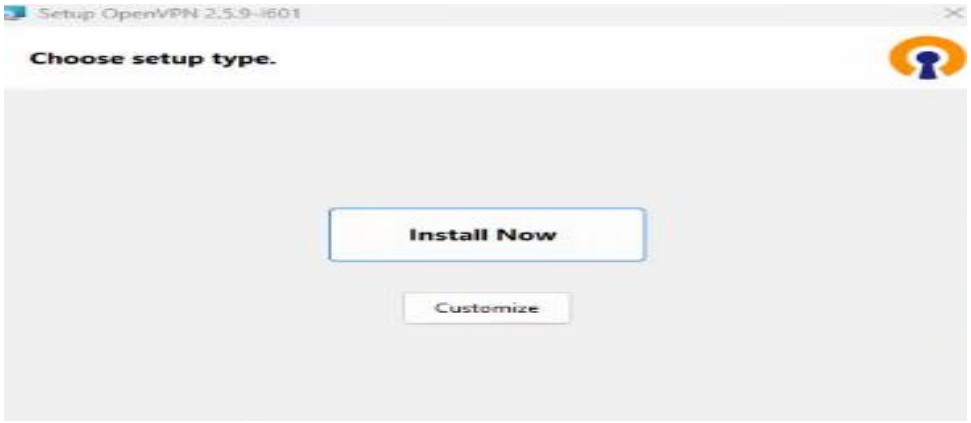


Figure 57 : Installation du package

Après installation du package le logiciel sera disponible sur le bureau de notre machine

Figure 58 : Installation du package

Nous allons ensuite lancer « OpenVPN GUI » en faisant un double-clic sur l'application. Une icône d'écran avec un petit Cárdenas apparaitra dans la barre des tâches.

Figure 59 : Fin d'installation du package

1.7 Tests

Nous allons donc faire le test de notre réseau VPN mis en place.

1.7.1 Connexion du client Windows vers le serveur VPN

Nous allons faire un clic droit sur l'icône et ensuite cliquer sur « Connecter ».

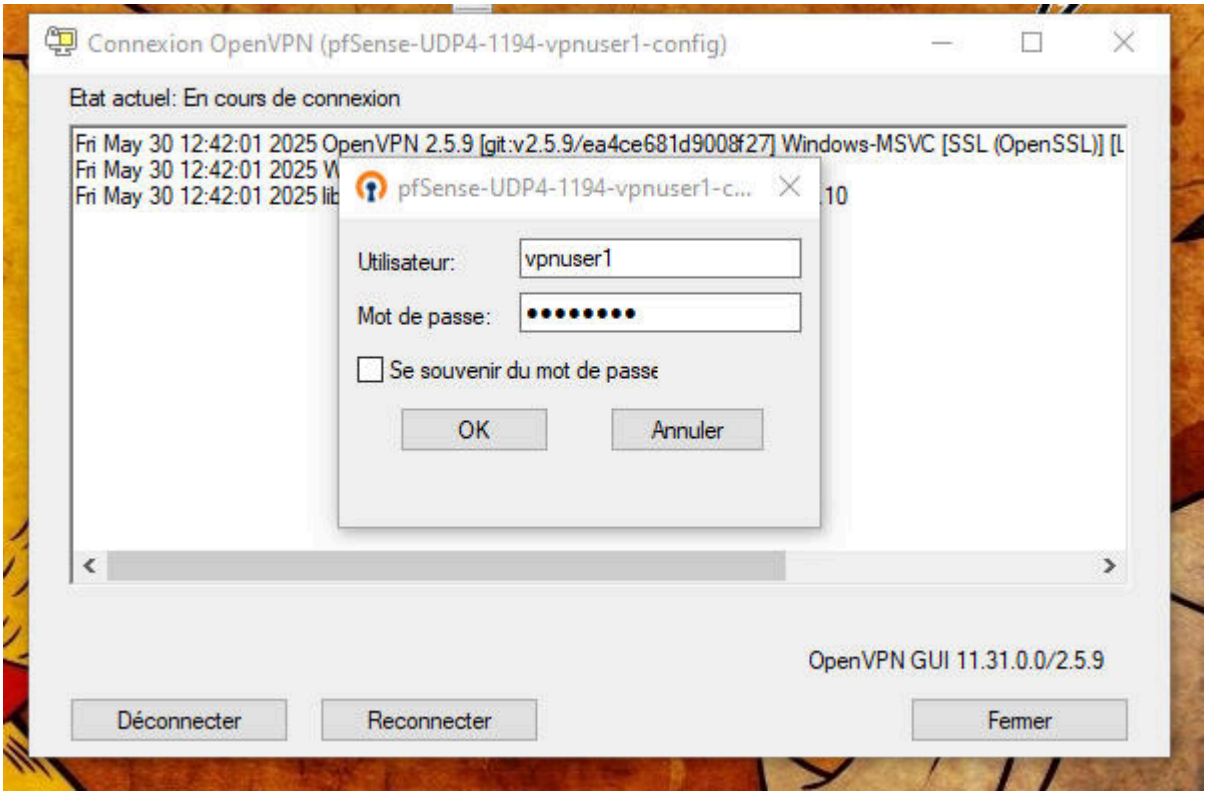


Figure 60 : Authentification de l'utilisateur

Après avoir entré les informations de connexion, patientez quelques secondes pour que la connexion puisse s'établir

Figure 61 : Connexion établie

1.7.2 Tests de la connectivité par la commande ping

Lorsqu'on entre dans notre invite de commande et qu'on test un ping à destination de l'adresse IP du serveur situé dans le réseau Local, on peut remarquer que le ping abouti ce qui confirme donc que la communication entre notre poste client et notre serveur VPN est établie.

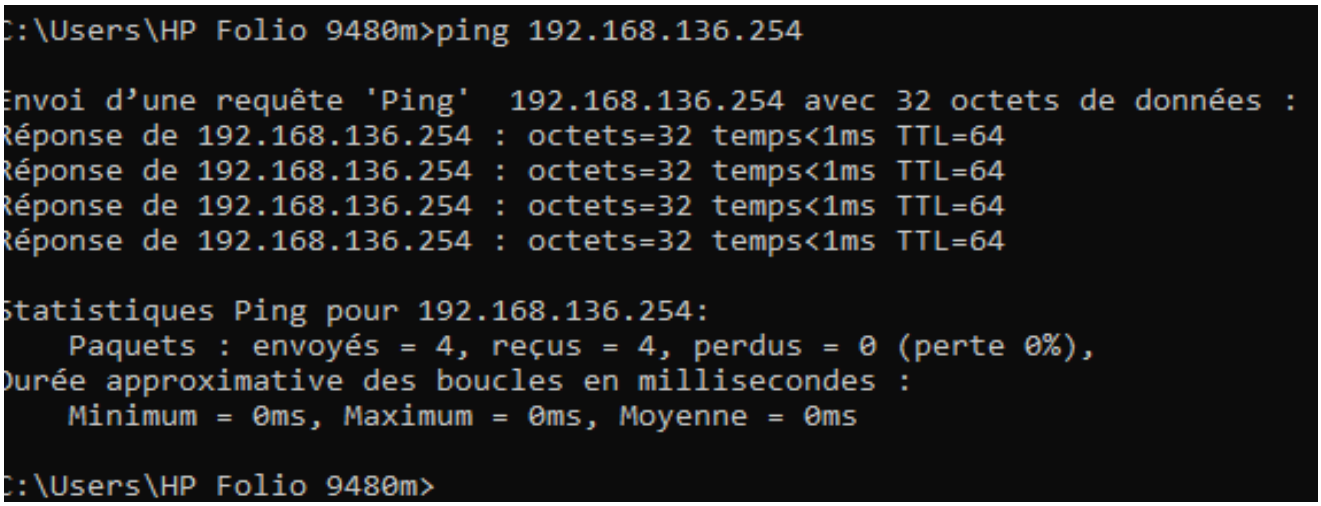


Figure 62 : Test de connectivité entre le client et le serveur

Dans ce dernier chapitre, nous avons mis en place un réseau VPN qui va nous permettre un accès à distance sécurisé vers un réseau local LAN.

Pour cela, nous avons d'abord commencer par l'installation de l'outil de virtualisation VMware, afin de créer un environnement de test constitué d'un pare-feu pfsense installé sur un serveur et un poste client. Nous avons ensuite configuré le client utilisateur pour qu'il puisse se connecter à distance au réseau LAN via le tunnel VPN. Les tests de connectivités effectuer à l'aide de la commande « ping » confirment que la connexion est fonctionnelle.

CONCLUSION GENERALE

Le développement des besoins de communication entre sites distants au sein des entreprises à conduit à la naissance des VPN. Ces réseaux privés virtuels ont pour objectif principal d'offrir aux utilisateurs et aux administrateurs les mêmes conditions d'usage, de performance et de sécurité à travers un réseau public que celles disponibles sur un réseau privé.

Nous avons, d'abord, consacré un chapitre sur les réseaux privés virtuels pour voir les différents types de VPN, leurs moyens de fonctionnement et les différents protocoles utilisées. OpenVPN est l'un des meilleurs protocoles de tunneling basé sur SSL/TLS pour l'authentification et le cryptage dans la mise en œuvre de réseaux privés virtuels.

En effet, Le présent travail présentes les résultats obtenues lors de la mise en œuvre d'un réseau VPN (OpenVPN), nous avons ainsi grâce a cette nouvelle technologie permis à un utilisateur l'accès à distance vers un réseau privé afin de partager de manière protéger leurs données à travers des protocoles de sécurités qui sont les principaux outils qui ont permis l'implémentation de notre VPN.

Ce travail a été enrichissant pour nous car nous avons fait la découverte de nouveaux protocoles de sécurités réseaux, nous avons aussi découvert un nouveau pare-feu (pfsense), ce qui fais que nous avons donc vécu de nouvelle expérience.

Cependant, nous avons rencontré de difficultés en commençant d'abord par le mauvais débit de connexion internet, ensuite la difficulté à pouvoir relier la machine serveur-client pour que les deux puissent communiquer parce que c'était une toute nouvelle découverte pour nous.

REFERENCES BIBLIOGRAPHIQUE

[1] Stallings williams (2019). *Cryptographie et sécurité réseaux : Principes et pratique.*

[2] Kurose, James F, Ross (2018). *Réseaux informatiques*

[3] Bénabou, Roland (2022). *Cybersécurité des PME : Guide de mise en place de réseau sécurisé.*

[4] Ministère du numérique et de la digitalisation, Bénin (2023). *Rapport sur la cybersécurité et les enjeux du numérique.*

[5] OpenVPN Technologies Inc. (2023). *OpenVPN Documentation et Guide de configuration.*

[6] Pfsense.org (2023). *Documentation Officielle de pfsense : Firewall, VPN, NAT.*

WEBOGRAPHIE

1. https://www.toutinformatique.fr/qu-est-ce-que-la-topologie-du-reseau.com: Consulté le 17/02/2025

2. https://web.maths.unsw.edu.au/~lafaye/CCM/initiation/topologi.htm : Consulté le 17/02/2025

3. https://www.memoireonline.com/01/16/9413/m_Apport-de-la-fibre-optique-face-aux-enjeux-de-la-NTIC-dans-la-ville-de-kinshasa1.html : Consulté le 22/02/2025

4. https://www.ionos.fr/digitalguide/serveur/know-how/le-modele-osi-reference-pour-les-standards/ : Consulté le 04 /03/2025

6. http://cisco.ofppt.info/ccna1/course/module1/1.4.3.1/1.4.3.1.html : Consulté le 12/03/2025

7. https://www.qiminfo.ch/reseaux-securite-informatique/ : Consulté le 20/03/2025

8. https://staff.univ-batna2.dz/sites/default/files/khernane-nesrine/files/cours7-les_reseaux_prives_virtuelsvpn.pdf : Consulté le 04/04/2025

9. https://docshare02.docshare.tips/files/12479/124793198.pdf : Consulté le 17/04/2025

10. https://www.redhat.com/fr/topics/edge-computing/le-multiprotocol-label-switching-mpls-quest-ce-que-cest : Consulté le 07 /05/2025

11. https://www.frameip.com/ipsec/ : Consulté le 18/05/2025

12. https://fr.wikipedia.org/wiki/FreeBSD : Consulté le 27/05/2025

TABLE DES MATIERES