الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne démocratique et populaire

وزارة التعليم العالي و البحث العلمي
Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب البليدة
Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا
Faculté de Technologie

قسم الإلكترونيك
Département d'Électronique

Mémoire de Master

Filière : Télécommunication

Spécialité : Réseaux et Télécommunications

Présenté par

KONATE Kadidiatou

&

MAIGA Samba Amidou

Mise en Place d'une Solution VPN sous pfSense

Proposé par : Pr. M. Bensebti

Année Universitaire : 2021-2022

REMERCIEMENTS

En premier lieu, nous tenons à remercier Dieu le tout puissant qui nous a donné la force et la patience pour accomplir notre travail.

En second lieu, nos remerciements vont tout droit à M. Bensebti pour tout ce qu'il nous a appris, pour sa présence, sa disponibilité, sa gentillesse et son soutien.

Nos vifs remerciements vont également aux membres du jury pour l'intérêt qu'ils ont porté à notre mémoire en acceptant d'examiner notre travail.

Nous souhaitons adresser nos remerciements les plus sincères aux personnes qui nous ont apporté leur aide et qui ont contribué à l'élaboration de ce mémoire.

Nous tenons enfin à remercier du plus profond de notre cœur, nos chers parents et notre patrie qui nous ont accompagnés et soutenus durant notre cursus.

DÉDICACES

Je dédie ce modeste travail,

A ma famille qui m'a doté d'une éducation digne en me couvrant d'amour et qui a fait de moi ce que je suis aujourd'hui ;

Particulièrement à mon très cher père qui a beaucoup contribué à mon éducation ;

Et à mon adorable mère qui m'a soutenue de près et de loin ;

A mes sœurs qui m'ont toujours encouragé durant ces années d'études.

Konaté Kadidiatou

Je dédie cet humble mémoire,

A mon cher père qui s'est beaucoup sacrifié pour que je puisse arriver là où je suis actuellement ;

A ma chère mère qui a également renoncé à tout pour nous, jamais ni les mots, ni les actes ne seront suffisants pour la remercier ;

A mes frères, ma sœur, qui m'ont toujours soutenu ;

A Kassongué Mariam ;

Et à toutes les personnes que j'ai connues et qui m'ont aidées, un grand MERCI à tous.

.

Maïga Samba Amidou

ملخص: مهمتنا هي إنشاء شبكة افتراضية خاصة من عميل إلى موقع باستخدام 3 أجهزة ونقطة وصول لاسلكية وكابلات RJ45. الخاصة LAN يمكن فقط للشبكة الافتراضية الخاصة للشركة منح الموظفين عن بُعد وصولاً آمنًا إلى شبكة بشبكة الشركة؛ OpenVPN بالشركة. للقيام بذلك، نستخدم جهازًا كعميل، مما سيسمح للعاملين عن بُعد بالاتصال عبر أخيرًا، الاختبارات التي تم إجراؤها على شبكتنا مثل pfSense. الخاص بنا تحت VPN وجهاز آخر يستضيف خادم تعطي نتائج جيدة Wireshark اختبارات إمكانية الوصول والتحليلات عن طريق التقاط الحزم بواسطة.

كلمات المفاتيح: VPN؛ OpenVPN؛ عميل VPN إلى موقع؛ وايرشارك ؛pfSense.

Résumé : Notre travail consiste à mettre en place un réseau privé virtuel Client-to-site à l'aide de 3 machines, d'un point d'accès sans fil et des câbles RJ45. Seul un réseau privé virtuel d'entreprise peut donner l'accès de façon sécurisée aux employés à distance au réseau local de l'entreprise. Pour ce faire, nous utilisons une machine comme client, ce qui va permettre à un télétravailleur de se connecter à travers OpenVPN au réseau de l'entreprise ; et une autre machine qui héberge notre serveur VPN sous pfsense. Enfin les tests effectués sur notre réseau tels que les tests d'accessibilités et d'analyses en capturant des paquets par Wireshark donnent de bons résultats.

Mots clés: VPN; OpenVPN; VPN Client-to-site; Wireshark; PfSense.

Abstract: Our job is to set up a client-to-site virtual private network using 3 machines, a wireless access point and RJ45 cables. Only a corporate virtual private network can securely give remote employees access to the corporate LAN. To do this, we use a machine as a client, which will allow a teleworker to connect through OpenVPN to the corporate network; and another machine that hosts our VPN server under pfsense. Finally, the tests carried out on our network such as accessibility tests and analyzes by capturing packets by Wireshark give good results.

Keywords: VPN; OpenVPN; VPN Client-to-site; Wireshark; PfSense.

Table des Matières

Listes des Figures

Liste des tableaux

Liste des abréviations

AES : Advanced Encryptions Standard

AH : Authentification Header

ACL : Access Control List

BSD: Berkeley Software Distribution

CA: Certificat Autority

DES : Data Encryptions Standard

DoS: Denial of Service

DMZ: Demilitarized Zone

ESP: Encapsulating Security Payload

HIDS: Host Intrusion Detection System

HTTP: Hyper Text Transfer Protocol

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

IKE: Internet Key Exchange

IP: Internet Protocol

ICMP: Internet Control Message Protocol

ISO: International Standardization Organisation

IPsec: Internet Protocol Security

L2TP: Layer Two Tunnelling Protocol

LAN: Local Area Network

MAN: Metropolitan Area Network

MD5: Message Digest5

NAT: Network Address Translation

NAS: Network Access Server

NIDS: Network Intrusion Detection System

OSI: Open System Interconnect

PPP: Point to Point Protocol

PPTP: Point to Point Tunneling Protocol

Pfsense: Packet Filter Sense

SSL: Secure Sockets Layer

SHA: Secure Hash Algorithm

TLS: Transport Layer Security

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

VLAN: Virtual Local Area Network

VPN: Virtual Private Network

WAN: Wide Area Network

Introduction Générale

L’accès à distance a beaucoup évolué aujourd’hui, notamment grâce aux nouvelles technologies mobiles et réseaux qui s'offrent à nous. Ainsi, la crise sanitaire mondiale du COVID-19 a nécessité la mise en place de mesures de confinement et de limitation des déplacements aux seuls motifs indispensables.

Face à cette situation exceptionnelle et inédite, les administrations, entreprises ou organisations ont adopté des modalités de télétravail qui supposent un accès à distance à des systèmes et à des données parfois sensibles.

L’adoption massive du travail à distance pendant une période prolongée, et les inévitables facteurs de vulnérabilité qui en découlent, laissent présager la multiplication des cyberattaques (ransomware, phishing, DDoS) et de brèches de confidentialité parfois sous des formes nouvelles. On a alors recours à des algorithmes de cryptage, pour garder nos données confidentielles. Pour garantir la confidentialité et l’authenticité des données échangées les entreprises font recours à la solution VPN.

Le principe de la connexion VPN (Virtual Private Network) est de créer un tunnel sécurisé à travers un réseau peu sûr tel qu'Internet jusqu'au réseau de l'entreprise. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

Dans notre projet de fin d’études, nous allons essayer d’étudier cette solution de VPN sous le pare-feu pfSense.

Pour cela, notre mémoire sera organisé comme suit :

- Nous allons détailler des généralités sur les réseaux, dans le premier chapitre.
- Le deuxième chapitre concernera la sécurité informatique et les dispositifs de sécurité.
- Le troisième chapitre est consacré aux réseaux Privés Virtuels : leurs principes de fonctionnement, les différents types et les différents protocoles utilisés pour sa réalisation.
- Un dernier chapitre qui est porté sur la mise en œuvre d’une solution VPN.
- Une conclusion générale viendra clôturer notre mémoire.

Chapitre 1

Généralités sur les Réseaux

1.1 Introduction

Actuellement, les réseaux informatiques sont devenus incontournables dans pratiquement tous les domaines de la vie : banques, assurance, santé, administration, entreprises ou organisations, universités ...etc.

Les besoins de communication de données informatiques entre systèmes plus ou moins éloignés sont multiples : transmission de messages (messagerie), partage de ressources (imprimante, disque dur, internet), transfert de fichiers (FTP), consultation de bases de données, gestion de transactions, télécopie, télétravail.

Au cours de ce chapitre, nous aborderons quelques généralités sur les réseaux et nous le terminerons par une conclusion.

1.2 Généralités sur les réseaux

1.2.1 Définition d'un réseau

Un réseau est un ensemble d'équipements interconnectés pouvant communiquer (ou échanger des informations). Il a pour but de transmettre des informations d'un équipement ordinateur à un autre.

1.2.2 Classification des réseaux

On distingue plusieurs types de réseaux qui se différencient entre eux en fonction de la distance entre les systèmes informatiques, ou encore en fonction de la technologie qui permet de les mettre en œuvre. [1]

- **Les réseaux locaux, ou LAN (Local Area Network) :** Un réseau LAN permet de connecter deux ou plusieurs centaines de machines à l'intérieur d'une même enceinte (Entreprise, administration...etc.), sur de courte distance (quelques kilomètres au maximum). On fait généralement appel à la technologie Ethernet pour relier les postes de travail.
- **Les réseaux métropolitains, ou MAN (Métropolitain Area Network) :** Interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants. Ainsi un MAN permet à deux équipements distants de communiquer comme s'ils faisaient partie d'un même réseau local, Un

MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).

- **Les réseaux étendus, ou WAN (Wide Area Network) :** Sont des réseaux destinés à transporter des données à l'échelle d'un pays voire même d'un continent ou de plusieurs continents. Le réseau est soit terrestre, il utilise dans ce cas une infrastructure au niveau de sol essentiellement de grands réseaux de fibre optiques, soit hertzien, comme le réseau satellitaire.
- **Les réseaux privés virtuels, ou VPN (Virtual Private Network) :** Les réseaux privés virtuels consistent en l'interconnexion de LAN à l'échelle nationale ou internationale. Ces réseaux restent privés et sont transparents pour l'utilisateur. Ils permettent en fait, par exemple pour une entreprise, de s'affranchir de certaines contraintes, telles que la localisation géographique. Ils rendent possible une transmission plus sécuritaire des données sur un réseau publique, en particulier sur Internet.

1.2.3 Les types des réseaux

- **Internet :** L'internet est par définition un ensemble de réseaux d'ordinateurs interconnectés, utilisant le protocole TCP/IP. C'est un service donnant l'accès à un réseau mondial mettant en contact divers mediums de communication et des serveurs, procurant aux utilisateurs une possibilité de partage d'informations, de recherche sur des sujets, d'échange de messages et dossiers à l'aide des courriers électroniques. [1]
- **Intranet :** L'intranet est la partie sécurisée d'un réseau informatique (d'une entreprise ou d'une organisation) basé sur les mêmes technologies que l'Internet (protocoles de communication TCP/IP, serveur, browser, e-mail, etc.). Il est destiné à l'échange et au partage d'informations entre des programmes et/ou des utilisateurs connus et autorisés. L'intranet est généralement connecté au réseau Internet pour permettre la communication avec le monde extérieur. [1]
- **Extranet :** Un extranet est une extension du système d'information de l'entreprise à des partenaires situés au-delà du réseau. L'accès à l'extranet doit être sécurisé dans la mesure où cela offre un accès au système d'information à des personnes situées en dehors de l'entreprise. Il peut s'agir soit d'une authentification simple (authentification par nom d'utilisateur et mot de passe) ou d'une authentification forte (authentification à l'aide d'un certificat). Il est conseillé d'utiliser HTTPS pour toutes les pages web consultées depuis l'extérieur afin de sécuriser le transport des requêtes et des réponses http et d'éviter notamment la circulation du mot de passe en clair sur le réseau. [1]

1.2.4 Architecture des réseaux

On distingue deux types d'architecture de réseaux : le poste à poste et le client/serveur.

- **Le réseau client/serveur :** De nombreuses applications fonctionnent selon un environnement client/serveur, cela signifie que des machines clientes (des machines faisant partie du réseau) contactent un serveur, une machine généralement très puissante en termes de capacités d'entrée-sortie, qui leur fournit des services.

- **Le réseau poste à poste (peer to peer) :** Dans une architecture d'égal à égal (appelée aussi « poste à poste », en anglais peer to peer, notée P2P), contrairement à une architecture de réseau de type client/serveur, il n'y a pas de serveur dédié. Ainsi chaque ordinateur dans un tel réseau joue à la fois le rôle de serveur et de client. Cela signifie notamment que chacun des ordinateurs du réseau est libre de partager ses ressources. [2]

1.2.5 Topologie des réseaux

Il existe trois topologies de base pour concevoir un réseau : bus, anneau et étoile.

- 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. [2]

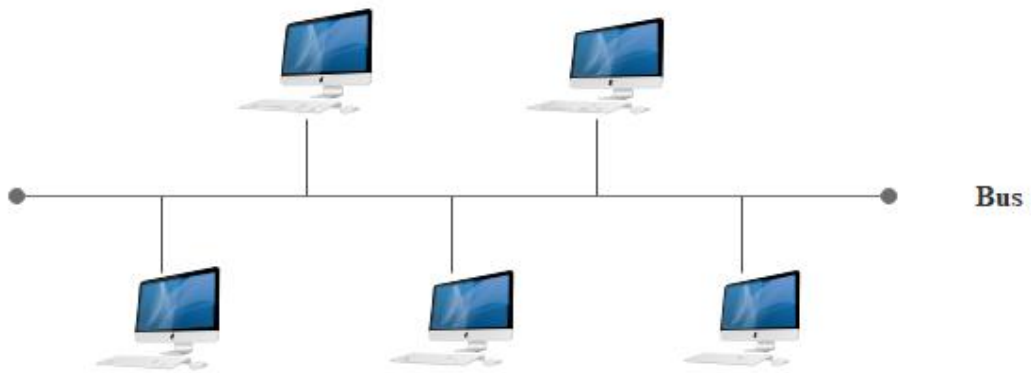

Figure 1.1 – Topologie en bus.

- **Topologie en étoile :** Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur (en anglais hub, littéralement moyen de roue). [2]

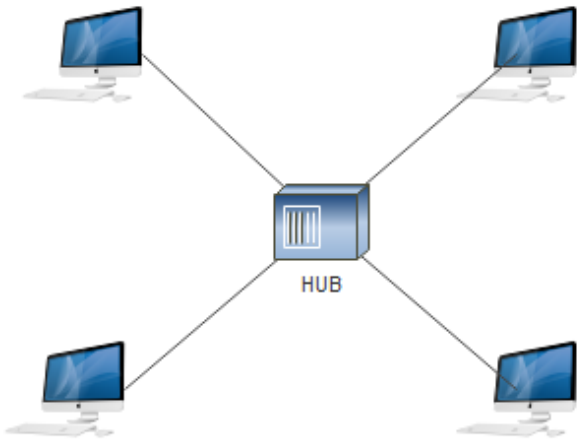

Figure 1.2 – Topologie en étoile.

- **Topologie en anneau :** Dans un réseau possédant une topologie en anneau, les ordinateurs sont situés sur une boucle et communiquent chacun à leur tour. [2]

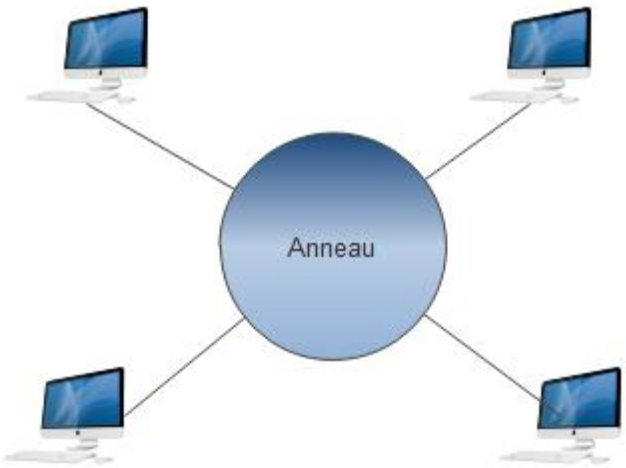

Figure 1.3 – Topologie en anneau.

1.2.6 Equipement d'interconnexion

- **Répéteur :** Un répéteur (en anglais repeater) est un équipement simple permettant de regénérer un signal entre deux nœuds du réseau, afin d'étendre la distance de câblage d'un réseau. 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. [3]
- **Concentrateur :** Un concentrateur est un élément matériel permettant de concentrer le trafic réseau provenant de plusieurs hôtes, et de régénérer le signal. [3]
- **Pont (bridge) :** Un pont est un dispositif matériel permettant de relier des réseaux travaillant avec le même protocole. [3]
- **Commutateur :** Un commutateur (en anglais *switch*) est un pont multiport, c'est-à-dire qu'il s'agit d'un élément actif agissant au niveau 2 du modèle OSI. [3]
- **Passerelle applicative :** Une passerelle applicative (en anglais « gateway ») est un système matériel et logiciel permettant de faire la liaison entre deux réseaux, afin de faire l'interface entre des protocoles réseau différents. [3]

1.2.7 Le Modèle OSI (Open System Interconnection)

a) Définition :

OSI signifie Open Systems Interconnection, ce qui se traduit par Interconnexion de systèmes ouverts. Ce modèle a été mis en place par l'ISO afin de mettre en place un standard de communications entre les ordinateurs d'un réseau, c'est-à-dire les règles qui gèrent les communications entre des ordinateurs.

Le modèle OSI est un modèle qui comporte 7 couches, les couches du modèle OSI sont les suivantes [4]:

	Modèle OSI
7	Application
6	Présentation
5	Session
4	Transport
3	Réseau
2	Liaison de données
1	Physique

Table 1.1 – Les couches du modèle OSI.

- **La couche application :** assure l'interface avec les applications. Il s'agit donc du niveau le plus proche des utilisateurs, géré directement par les logiciels.
- **La couche présentation :** définit le format des données manipulées par le niveau applicatif (leur représentation, éventuellement leur compression et leur chiffrement) indépendamment du système.
- **La couche session :** définit l'ouverture et la destruction des sessions de communication entre les machines du réseau.
- **La couche transport :** est chargée du transport des données, de leur découpage en paquets et de la gestion des éventuelles erreurs de transmission.
- **La couche réseau :** permet de gérer l'adressage et le routage des données, c'est-à-dire leur acheminement via le réseau.
- **La couche liaison données :** définit l'interface avec la carte réseau et le partage du média de transmission.
- **La couche physique :** définit la façon dont les données sont physiquement converties en signaux numériques sur le média de communication (impulsions électriques, modulation de la lumière, etc.).

1.2.8 Le modèle TCP/IP

a) Définition :

TCP/IP est une suite de protocoles. Le sigle TCP/IP signifie « Transmission Control Protocol/Internet Protocol » et se prononce « T-C-P-I-P ». Il provient des noms des deux protocoles majeurs de la suite de protocoles, c'est-à-dire les protocoles TCP et IP).

TCP/IP représente d'une certaine façon l'ensemble des règles de communication sur internet et se base sur la notion adressage IP, c'est-à-dire le fait de fournir une adresse IP à chaque machine du réseau afin de pouvoir acheminer des paquets de données. [4]

b) Découpage en couches :

Le modèle OSI est un modèle qui comporte 7 couches, tandis que le modèle TCP/IP n'en comporte que 4. En réalité le modèle TCP/IP a été développé à peu près au même moment que le modèle OSI, c'est la raison pour laquelle il s'en inspire mais n'est pas totalement conforme aux spécifications du modèle OSI.

Le modèle TCP/IP, inspiré du modèle OSI, reprend l'approche modulaire (utilisation de modules ou couches) mais en contient uniquement quatre [4]:

Modèle OSI		Modèle TCP/IP	
7	Application	4	Application
6	Présentation		
5	Session		
4	Transport	3	Transport (TCP/IP)
3	Réseaux	2	Internet (IP)
2	Liaison de donnée	1	Accès au réseau
1	Physique		

Table 1.2 - Comparaison entre le modèle TCP/IP et le modèle OSI.

Comme on peut le remarquer, les couches du modèle TCP/IP ont des tâches beaucoup plus diverses que les couches du modèle OSI, étant donné que certaines couches du modèle TCP/IP correspondent à plusieurs couches du modèle OSI.

Les rôles des différentes couches sont les suivants [4]:

- **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 les mécanismes permettant de connaître l'état de la transmission
- **Couche Application** : elle englobe les applications standard du réseau (Telnet, SMTP, FTP, ...)

1.3 Conclusion

Les réseaux permettent l'échange de beaucoup de ressources qui sont souvent des données confidentielles et par conséquent, on observe une augmentation des risques de cyberattaque.

2 Chapitre 2

Sécurité Informatique

2.1 Introduction

Comme des données confidentielles circulent sur les réseaux, la sécurité des communications est devenue une préoccupation importante des utilisateurs et des entreprises.

D'où la nécessité de mettre en place des mécanismes de contrôle d'accès et des protocoles sécurisés qui apportent plusieurs services : l'authentification, la confidentialité, l'intégrité, la non-répudiation.

Dans ce chapitre, nous allons parler des mécanismes qui assurent différents services de la sécurité informatique, ses objectifs, puis sa terminologie, ensuite nous parlerons des attaques, suivies des éléments à sécuriser sur le réseau et la stratégie de sécurité.

2.2 Sécurité informatique :

Le système d'information est généralement défini par l'ensemble des données et des ressources matérielles et logicielles de l'entreprise permettant de les stocker ou de les faire circuler. Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger.

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu. [5]

2.2.1 Objectifs de sécurité informatique

La sécurité informatique vise généralement cinq principaux objectifs [5]:

- L'**intégrité**, c'est-à-dire garantir que les données sont bien celles que l'on croit être ;
- La **confidentialité**, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées ;
- La **disponibilité**, permettant de maintenir le bon fonctionnement du système d'information ;
- La **non-répudiation**, permettant de garantir qu'une transaction ne peut être niée ;
- L'**authentification**, consistant à assurer que seules les personnes autorisées aient accès aux ressources.

2.2.2 Terminologie de la sécurité informatique

La sécurité informatique utilise un ensemble de terme bien spécifique, que nous énumérons dans ce qui suit [6]:

- **Les vulnérabilités :** ce sont les failles de sécurité dans un ou plusieurs systèmes. Tout système vu dans sa globalité présente des vulnérabilités, qui peuvent être exploitables ou non.
- **Les attaques (exploits) :** elles représentent les moyens d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas exploitables.
- **Les contre-mesures** : ce sont les procédures ou techniques permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique (auquel cas il peut exister d'autres attaques sur la même vulnérabilité).
- **Les menaces :** ce sont des adversaires déterminés capables de monter une attaque exploitant une vulnérabilité.

2.2.3 Les attaques sur un système informatique

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque.

Les motivations des attaques sont de différentes sortes [6]:

- Obtenir un accès au système ;
- Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles ;
- Glaner des informations personnelles sur un utilisateur ;
- Récupérer des données bancaires ;
- S'informer sur l'organisation (entreprise de l'utilisateur, etc.) ;
- Troubler le bon fonctionnement d'un service ;
- Utiliser le système de l'utilisateur comme « rebond » pour une attaque ;
- Utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée.

2.2.3.1 Les différents types d'attaques

Il existe trois types d'attaques [6]:

1. **Attaque directe :** C'est la plus simple des attaques. L'hacker attaque directement sa victime à partir de son propre ordinateur.

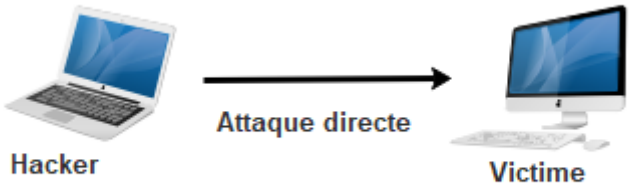

Figure 2.1 - Attaque directe.

2. **Attaque indirecte par rebond :** Cette attaque est très prise des hackers, car le principe est simple, les paquets d'attaques sont envoyés à l'ordinateur intermédiaire, qui récupère l'attaque vers la victime. D'où le terme de rebond qui permet de :

- Masquer l'identité (l'adresse IP) de l'hacker ;
- Utiliser éventuellement les ressources de l'ordinateur intermédiaire, car il est plus puissant pour l'attaque.

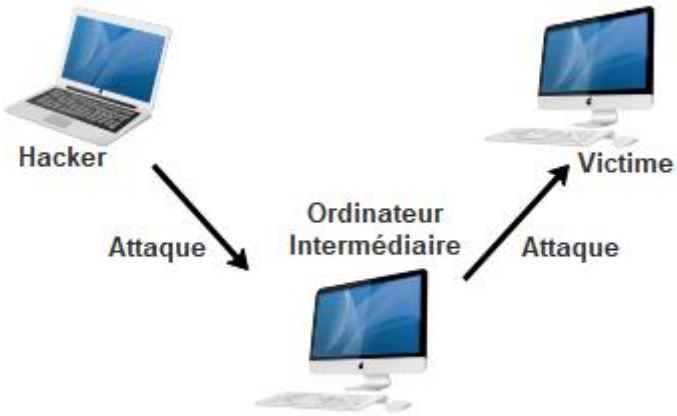

Figure 2.2 - Attaque par rebond.

1. **Attaque indirecte par réponse :** Cette attaque est dérivée de l'attaque par rebond. Cependant au lieu d'envoyer une attaque à la machine intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête, cette dernière va être envoyée à la machine.

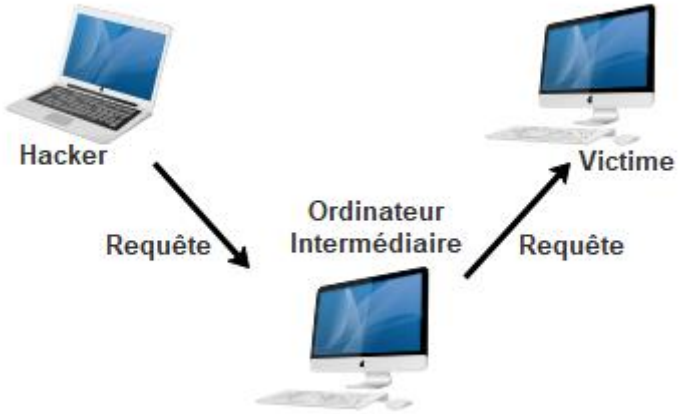

Figure 2.3 - Attaque indirecte par rebond.

2.2.3.2 Quelques attaques courantes

- **IP spoofing** : Le *spoofing IP* est une technique consistant à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine.
- **Le sniffing** : Grace à un logiciel appelé « sniffer », un dispositif permettant d'« écouter » le trafic d'un réseau, c'est-à-dire de capturer les informations qui y circulent.
- **Le Dos (Denial of Service)** : Le Dos est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services ou ressources d'une organisation. Il s'agit la plupart du temps d'attaques à l'encontre des serveurs d'une entreprise, afin qu'ils ne puissent être utilisés et consultés.
- **Le virus** : Un virus est un petit programme informatique situé dans le corps d'un autre, qui, lorsqu'on l'exécute, se charge en mémoire et exécute les instructions que son auteur a programmé.
- **Le scanning (appelé analyseur de réseaux) :** est un utilitaire permettant de réaliser un audit de sécurité d'un réseau en effectuant un balayage des ports ouverts (en anglais *port scanning*) sur une machine donnée ou sur un réseau tout entier. Le balayage se fait grâce à des sondes (requêtes) permettant de déterminer les services fonctionnant sur un hôte distant.
- **L'ingénierie sociale (social engineering)** : désigne l'art de manipuler des personnes afin de contourner des dispositifs de sécurité. Il s'agit ainsi d'une technique consistant à obtenir des informations de la part des utilisateurs par téléphone, courrier électronique, courrier traditionnel ou contact direct.

- **Le craquage de mots de passe (Brute force)** : Cette technique le cassage d'un mot de passe en testant tous les mots de passe possibles. Il existe un grand nombre d'outils, pour chaque système d'exploitation, permettant de réaliser ce genre d'opération. Ces outils servent aux administrateurs système à éprouver la solidité des mots de passe de leurs utilisateurs mais leur usage est détourné par les pirates informatiques pour s'introduire dans les systèmes informatiques.
- **Le flood** : un flood consiste à envoyer très rapidement de gros paquets d'informations à une personne. Cette dernière visée ne pourra plus répondre aux requêtes et le modem va donc se déconnecter, c'est cette méthode qui a été employée à grande échelle dans l'attaque des grands sites commerciaux. [6]

2.2.4 Les éléments à sécuriser dans un réseau

Les réseaux sont constitués de divers équipements d'une part et de liens filaires ou non filaires, qui, les relient d'autre part. Toute ou partie de ces équipements peuvent être gères par des programmes adaptés et plusieurs sorts de données y sont stockées.

Certains d'entre elles peuvent être l'objet de transferts selon des protocoles appelés protocole de réseaux. Dans ce cadre, la sécurité concerne celle du matériel, celle des programmes, celle des données et celle des protocoles. [6]

Avant de réaliser un système de sécurité, il faut spécifier d'abord les éléments à protéger. On dénombre trois types essentiels qui sont :

- **Matériel :** Mis à part les ordinateurs que les réseaux relient, le matériel inclut aussi, les équipements intermédiaires comme les répéteurs, commutateurs (switch), routeurs, serveur, modems, firewalls, etc. La limitation d'accès à chaque matériel participe à la sécurité de l'ensemble
- **Programme :** les programmes incluent les systèmes d'exploitation y compris les pilotes de périphériques ainsi que les logiciels programmes gérant les différents mécanismes de réseaux. Les services permettant une meilleure gestion à distance et plus d'autonomie, on parle dans ce cas-là de services réseau tels que : DHCP, DNS, FTP, etc.
- **Données :** On distingue deux sortes de données, celles qui servent au fonctionnement du réseau comme les tables de routage, les bases de données de clients, les fichiers relatifs aux droits d'accès, etc. On trouve aussi des données qui ne sont pas en rapport avec le fonctionnement du réseau tels que : les documents et les archives.

2.2.5 Stratégies de sécurité

Elles consistent à déployer des moyens et des dispositifs visant à sécuriser le système d'information ainsi que de faire appliquer les règles définies dans une politique de sécurité. En voici Les principaux dispositifs permettant de sécuriser un réseau contre les attaques.

2.2.5.1 Un pare-feu

Un pare-feu (appelé aussi coupe-feu, garde-barrière ou firewall en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante [7]:

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

Le système firewall est un système logiciel, reposant parfois sur un matériel réseau dédié, constituant un intermédiaire entre le réseau local (ou la machine locale) 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.

Dans le cas où le système pare-feu est fourni dans une boîte noire « clé en main », on utilise le terme d'« Appliance ».

a) Principes de fonctionnement d'un pare-feu

Un système pare-feu contient un ensemble de règles prédéfinies 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 les communications ayant été explicitement autorisées :

"Tout ce qui n'est pas explicitement autorisé est interdit".

- Soit d'empêcher les échanges qui ont été explicitement interdits.

La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.

2.2.5.2 Zone Démilitarisée

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, un serveur de messagerie, un serveur FTP public, etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise. On parle ainsi de « zone démilitarisé » (notée DMZ pour DeMilitarized Zone) pour désigner cette zone isolée hébergeant des applications mises à disposition du public. La DMZ fait ainsi office de « zone tampon » entre le réseau à protéger et le réseau hostile. [7]

Les serveurs situés dans la DMZ sont appelés « bastions » en raison de leur position d'avant-poste dans le réseau de l'entreprise.

La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante [7]:

- Traffic du réseau externe vers la DMZ autorisé ;
- Traffic du réseau externe vers le réseau interne interdit ;
- Traffic du réseau interne vers la DMZ autorisé ;
- Traffic du réseau interne vers le réseau externe autorisé ;
- Traffic de la DMZ vers le réseau interne interdit ;
- Traffic de la DMZ vers le réseau externe refusé.

La DMZ possède donc un niveau de sécurité intermédiaire, mais son niveau de sécurisation n'est pas suffisant pour y stocker des données critiques pour l'entreprise.

Il est à noter qu'il est possible de mettre en place des DMZ en interne afin de cloisonner le réseau interne selon différents niveaux de protection et ainsi éviter les intrusions venant de l'intérieur.

2.2.5.3 La technologie AAA

Le contrôle d'accès consiste à définir les accès au réseau et les services disponibles après identification. Le terme AAA est souvent utilisé pour désigner les facettes suivantes de la sécurité :

- Authentification (en anglais Authentication) : il s'agit de la vérification de l'identité d'un utilisateur ; généralement assurée par le protocole RADIUS un protocole d'authentification standard.
- Autorisation (en anglais Authorization) : il s'agit des droits accordés à un utilisateur, tels que l'accès à une partie d'un réseau, à des fichiers, le droit d'écriture, etc.
- Comptabilité (en anglais Accounting) : il s'agit des informations récoltées pendant toute la durée de la session, après identification de l'utilisateur. [7]

2.2.5.4 Liste de contrôle d'accès (ACL)

Basée sur les adresses MAC des équipements autorisés à se connecter au réseau sans fil. Cette précaution un peu contraignante permet de limiter l'accès au réseau à un certain nombre de machines. [7]

2.2.5.5 Proxy

Un serveur proxy (traduction française de «proxy server», appelé aussi «serveur mandataire») est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local (utilisant parfois des protocoles autres que le protocole TCP/IP) et internet.

La plupart du temps le serveur proxy est utilisé pour le web, il s'agit alors d'un proxy HTTP. Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP, ...). [7]

2.2.5.6 Les réseaux privés virtuel

Un réseau privé virtuel repose sur un protocole, appelé protocole de tunnelisation (tunneling), c'est-à-dire un protocole permettant aux données passant d'une extrémité du VPN à l'autre d'être sécurisées par des algorithmes de cryptographie. Ce réseau est dit virtuel car il relie deux réseaux « physiques » (réseaux locaux) par une liaison non fiable (Internet), et privé car seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent « voir » les données. Le système de VPN permet d'obtenir une liaison sécurisée à moindre coût.

2.2.5.7 Systèmes de détection d'intrusion

On appelle IDS (Intrusion Detection System) un mécanisme écoutant le trafic réseau de manière furtive afin de repérer des activités anormales ou suspectes et permettant ainsi d'avoir une action de prévention sur les risques d'intrusion.

Il existe deux grandes familles distinctes d'IDS [7]:

- Les N-IDS (Network Based Intrusion Detection System), ils assurent la sécurité au niveau du réseau.
- Les H-IDS (Host Based Intrusion Detection System), ils assurent la sécurité au niveau des hôtes.

2.2.6 La cryptographie

Il existe à l'heure actuelle deux grands algorithmes de cryptographie : l'algorithme de cryptographie symétrique (à clé secrète) et l'algorithme de cryptographe asymétrique (à clé publique et privée) [8].

2.2.6.1 La cryptographie symétrique

La cryptographie symétrique se fondent sur une même clé pour chiffrer et déchiffrer un message. L'un des problèmes de cette technique est que la clé, qui doit rester totalement confidentielle, doit être transmise au correspondant de façon sûre. La mise en œuvre peut s'avérer difficile, surtout avec un grand nombre de correspondants car il faut autant de clés que de correspondants. Les algorithmes de chiffrement symétrique très utilisés sont : DES ; 3DES ; AES [8].

2.2.6.2 La cryptographie asymétrique

La cryptographie asymétrique se base sur le principe de deux clés [8]:

- Une publique, permettant le chiffrement ;
- Une privée, permettant le déchiffrement.

Comme son nom l'indique, la clé publique est mise à la disposition de quiconque désire chiffrer un message. Ce dernier ne pourra être déchiffré qu'avec la clé privée, qui doit rester confidentielle. Les cryptographies asymétriques très utilisés sont : RSA (chiffrement et signature) ; DSA (signature) ; Protocole d'échange de clés Diffie-Hellman DH (échange de clé).

2.2.6.3 Fonction de hachage

Une fonction de hachage est une fonction qui convertit un grand ensemble en un plus petit ensemble, l'empreinte. Il est impossible de la déchiffrer pour revenir à l'ensemble d'origine, ce n'est donc pas une technique de chiffrement. L'empreinte d'un message ne dépasse généralement pas 256 bits (maximum 512 bits pour SHA-512) et permet de vérifier son intégrité. Les fonctions de hachage très utilisées sont : MD5 ; SHA-1 ; SHA-256.

2.2.6.4 Signature électronique

La signature numérique est un mécanisme permettant de garantir l'authenticité de l'expéditeur (fonction d'authentification) et de vérifier l'intégrité du message reçu.

La signature numérique assure également une fonction de non-répudiation, c'est-à-dire qu'elle permet d'assurer que l'expéditeur a bien envoyé le message (autrement dit elle empêche l'expéditeur de nier avoir expédié le message).

2.3 Conclusion

Au cours de ce chapitre, nous avons défini les notions fondamentales dans les réseaux informatiques et les stratégies de sécurité à prendre pour remédier aux attaques. Le prochain chapitre sera consacré aux VPNs.

3 Chapitre 3

Les Réseaux Privés Virtuels

3.1 Introduction

A l'heure où la mobilité est souvent remise en question dans le domaine professionnel mais aussi à cause de la pandémie de la Covid-19 qui a poussé les entreprises à recourir au télétravail, Il est de plus en plus nécessaire de pouvoir offrir des solutions d'accès distants à ses utilisateurs .

Ces accès se doivent d'être sécurisés et fiables. Le facteur le plus important dans une stratégie d'accès distant est de gérer l'intégrité et la confidentialité des données de l'entreprise pour des raisons évidentes de sécurité, car toutes les informations sensibles à une entreprise ne peuvent pas être stockées sur un serveur accessible par tout le monde depuis internet.

La solution pour répondre à ce besoin de transmission sécurisé consiste à utiliser Internet comme support de transmission en encapsulant les données à transmettre de façon chiffrée par de protocole d'encapsulation. On parle alors de réseau privé virtuel RPV ou VPN (Virtual Private Network), c'est à dire le réseau ainsi virtuellement créé.

Dans ce chapitre, nous aborderons les principales caractéristiques des VPN, à travers certaines définitions et principes de fonctionnement.

3.2 Présentation d'un réseau privé virtuel

3.2.1 Définition

VPN (Virtual Private Network) ou RPV (Réseau Privé Virtuel) est une technique permettant d'établir un canal chiffré entre deux nœuds quelconques de l'Internet, ces nœuds pouvant eux-mêmes être des routeurs d'entrée de réseaux. On aura ainsi établi une sorte de tunnel qui, à travers l'Internet, reliera deux parties éloignées l'une de l'autre du réseau d'une même entreprise pour donner l'illusion de leur contiguïté. Mais le chiffrement permet aussi d'établir un VPN personnel pour un utilisateur, par exemple entre son ordinateur portable et le réseau local de l'entreprise [6].

3.2.2 Principe de fonctionnement

Un réseau VPN repose sur un protocole appelé « protocole de tunneling ». Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme Internet.

Les données à transmettre peuvent être prises en charge par un protocole différent d'IP. Dans ce cas, le protocole de tunneling encapsule les données en ajoutant un entête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de dé encapsulation. [9]

3.2.3 Les fonctionnalités d'un réseau privé virtuel

Un réseau privé, repose sur les principes fondamentaux de la sécurité, en assurant la mise en oeuvre de diverses fonctionnalités [9]:

Un système de VPN doit pouvoir mettre en œuvre les fonctionnalités suivantes :

3.2.3.1 Authentification d'utilisateur

Seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel. De plus, un historique des connexions et des actions effectuées sur le réseau doit être conservé.

3.2.3.2 Gestion d'adresses

Chaque client sur le réseau doit avoir une adresse privée. Cette adresse privée doit rester confidentielle. Un nouveau client doit pouvoir se connecter facilement au réseau et recevoir une adresse.

3.2.3.3 Cryptage des données

Lors de leurs transports sur le réseau public les données doivent être protégées par un cryptage efficace.

3.2.3.4 Gestion de clés

Les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.

3.2.3.5 Prise en charge multi protocole

La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier le protocol IP.

3.2.4 Type de VPN

ll existe 3 types standards d'utilisation des VPNs selon leur mode d'utilisation [9]:

3.2.4.1 VPN d'accès (Host to LAN)

Un 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 (Network Access Server) du fournisseur d'accès et c'est le NAS qui établit la connexion cryptée.

L'utilisateur possède son propre logiciel client pour le VPN auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise. (Figure 3.1)

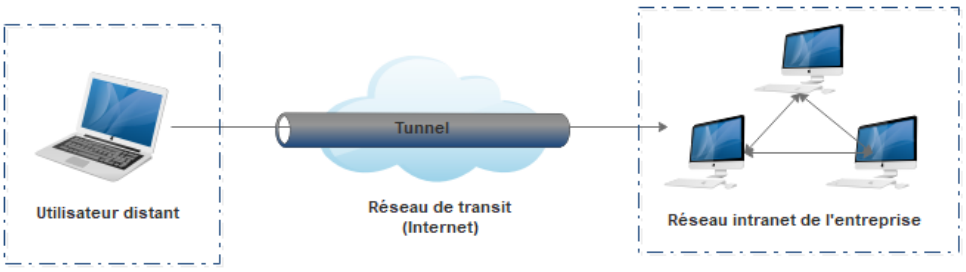

Figure 3.1 – VPN poste à site.

3.2.4.2 Intranet VPN (LAN to LAN)

L'intranet VPN est utilisé pour relier au moins deux intranets entre eux, comme l'illustre la Figure 3.2. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants. Le plus important dans ce type de réseau est de garantir la sécurité et l'intégrité des données. 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. Le coût matériel des équipements de cryptage et de décryptage ainsi que les limites légales interdisent l'utilisation d'un codage « infaillible ». 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. [9]

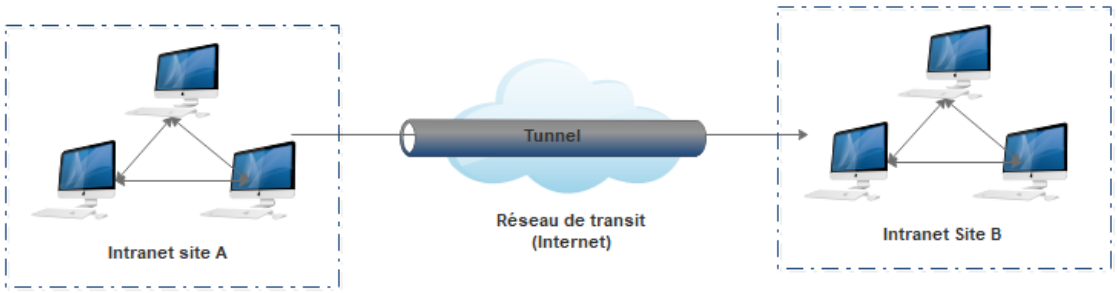

Figure 3.2 – VPN site à site.

3.2.4.3 Extranet VPN (Host to Host)

L'extranet VPN est utilisé pour connecter deux ordinateurs distants entre eux pour des raisons de confidentialité. On crée donc un VPN entre eux, et toutes les données y transmises sont encryptées et compréhensibles que par les deux paires correspondantes. (Figure 3.3)

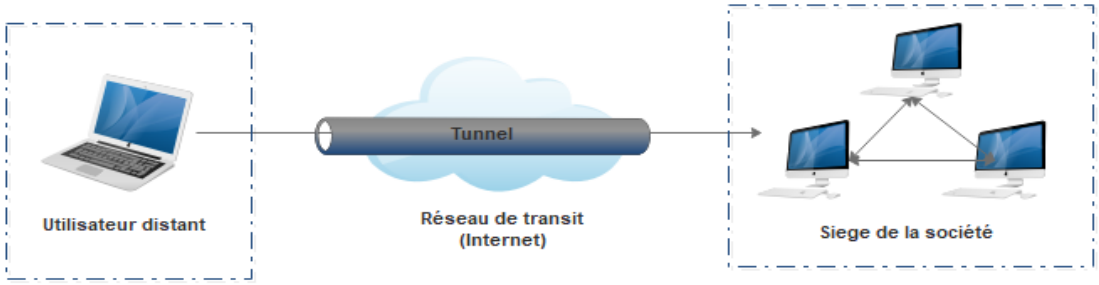

Figure 3.3 – VPN poste à poste.

3.3 Protocoles utilisés pour réaliser une connexion VPN

3.3.1 Le protocole PPP (Point-To-Point Protocol)

C'est un ensemble de protocoles standard garantissant l'interopérabilité des logiciels d'accès distant de divers éditeurs, il permet de transférer des données sur un lien synchrone ou asynchrone, il est full duplex, garantie l'ordre d'arrivée des paquets et encapsule les paquets IP,

IPX dans des trames PPP, puis transmet ces paquets encapsulés au travers de liaison point à point. [7]

3.3.2 Le protocole PPTP (Point-to-Point Tunneling Protocol)

Le principe du protocole PPTP est de créer des paquets sous le protocole PPP et de les encapsuler dans des datagrammes IP. PPTP crée ainsi un tunnel de niveau 3 défini par le protocole Gre (Generic Routing Encapsulation). Le tunnel PPTP se caractérise par une initialisation du client, une connexion de contrôle entre le client et le serveur ainsi que par la clôture du tunnel par le serveur. Lors de l'établissement de la connexion, le client effectue d'abord une connexion avec son fournisseur d'accès Internet. Cette première connexion établie une connexion de type PPP et permet de faire circuler des données sur Internet. Par la suite, une deuxième connexion dial-up est établie. Elle permet d'encapsuler les paquets PPP dans des datagrammes IP. C'est cette deuxième connexion qui forme le tunnel PPTP. Tout trafic client conçu pour Internet emprunte la connexion physique normale, alors que le trafic conçu pour le réseau privé distant, passe par la connexion virtuelle de PPTP [9]

3.3.3 L2TP (Layer Two Tunneling Protocol)

Le protocole L2TP est un protocole réseau qui encapsule des trames PPP pour les envoyer sur des réseaux IP, X25, relais de trames ou ATM. Lorsqu'il est configuré pour transporter les données sur IP, le protocole L2TP peut être utilisé pour faire du tunnelling sur Internet. Dans ce cas, le protocole L2TP transporte des trames PPP dans des paquets IP. La maintenance du tunnel est assurée à l'aide de messages de commandes au format L2TP tandis que le protocole UDP est utilisé pour envoyer les trames PPP au sein de trames L2TP. [9]

3.3.4 IPSEC (Internet Protocol Security)

IPSec, définit par la RFC 2401, est un protocole qui vise à sécuriser l'échange de données au niveau de la couche réseau. Le réseau Ipv4 étant largement déployé et la migration vers Ipv6 étant inévitable, mais néanmoins longue, il est apparu intéressant de développer des techniques de protection des données communes à Ipv4 et Ipv6. Ces mécanismes sont couramment désignés par le terme IPSec pour Ip Security Protocols. IPSec est basé sur deux mécanismes.

- Le premier, AH, pour Authentification Header vise à assurer l'intégrité et l'authenticité des datagrammes IP. Il ne fournit par contre aucune confidentialité : les données fournies et transmises par Ce « protocole » ne sont pas encodées.

- Le second, Esp, pour Encapsulating Security Payload peut aussi permettre l'authentification des données mais est principalement utilisé pour le cryptage des informations.

Bien qu'indépendants ces deux mécanismes soient presque toujours utilisés conjointement. Enfin, le protocole Ike permet de gérer les échanges ou les associations entre protocoles de sécurité. Avant de décrire ces différents protocoles, nous allons exposer les différents éléments utilisés dans IPSec. [9]

3.3.5 Le protocole SSL/TLS (Secure Sockets Layer /Transport Layer Security)

La Transport Layer Security (TLS) ou « Sécurité de la couche de transport », et son prédécesseur la Secure Sockets Layer (SSL) ou « Couche de sockets sécurisée », sont des protocoles de sécurisation des échanges par réseau informatique, notamment par Internet. Le protocole SSL a été développé à l'origine par Netscape Communications Corporation pour son navigateur Web. L'organisme de normalisation Internet Engineering Task Force (IETF) en a poursuivi le développement en le rebaptisant Transport Layer Security (TLS). On parle parfois de SSL/TLS pour désigner indifféremment SSL ou TLS.

La TLS (ou SSL) fonctionne suivant un mode client-serveur. Il permet de satisfaire les objectifs de sécurité suivants :

- L'authentification du serveur ;
- La confidentialité des données échangées (ou session chiffrée) ;
- L'intégrité des données échangées ;
- De manière optionnelle, l'authentification du client (mais dans la réalité celle-ci est souvent assurée par la couche applicative).

Le protocole est très largement utilisé, et sa mise en œuvre est facilitée par le fait que les protocoles de la couche application, comme le HTTP, n'ont pas à être profondément modifiés pour utiliser une connexion sécurisée, mais seulement implémentés au-dessus de la SSL/TLS, ce qui pour le HTTP a donné le protocole HTTPS.

Un groupe de travail spécial de l'IETF a permis la création de la TLS et de son équivalent en mode non-connecté UDP, la DTLS. Depuis qu'il est repris par l'IETF, le protocole TLS a connu quatre versions : TLS v1.0 en 1999, TLS v1.1 en 2006, TLS v1.2 en 2008 et TLS v1.3 en 2018. [8]

3.4 Conclusion

Tout au long de ce chapitre, nous avons effectué une présentation des réseaux privés virtuels (VPNs) ainsi que les protocoles utilisés pour les réaliser. Le chapitre suivant, sera consacré à la Mise en place du réseau VPN.

4 Chapitre 4

Mise en œuvre d’une Solution VPN

4.1 Introduction

Dans ce chapitre, nous mettrons en place une solution permettant à des utilisateurs distant d'accéder au réseau local privé de l'entreprise et d'assurer l'échange de données entre eux d'une façon sécurisée à travers un tunnel VPN.

4.2 Architecture à implémenter

Avant de commencer la mise en œuvre de notre solution VPN Client-to-site, nous allons définir l'architecture de l'implémentation à réaliser, pour cela nous avons illustré la figure ci-dessous suivie de la description qui lui est associée.

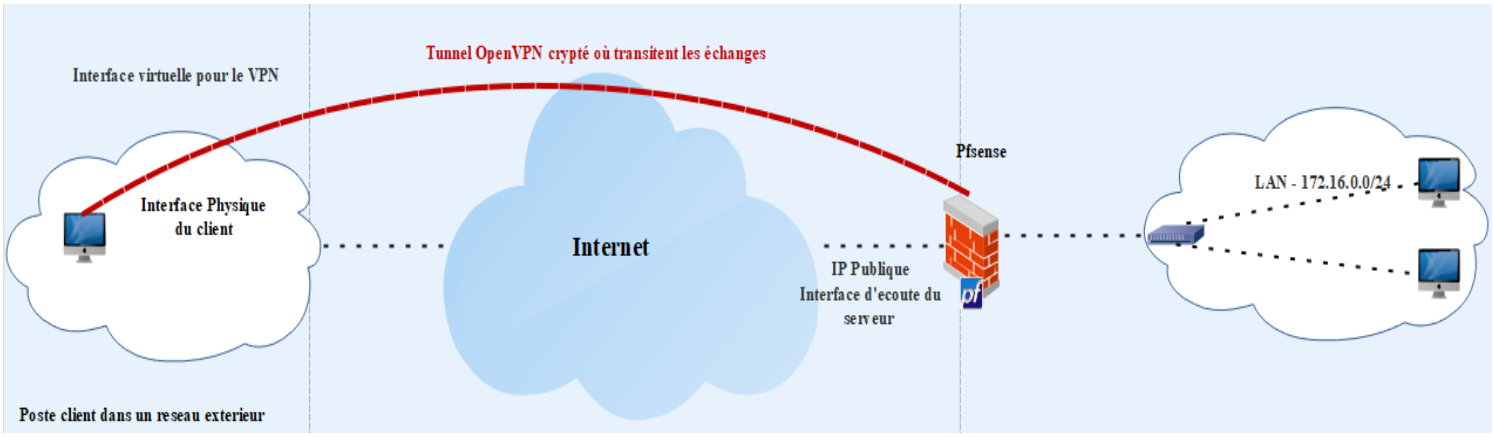

Figure 4.1 – Schema global de la mise en place d'une solution VPN.

Comme la figure 4.1 le montre, il s'agit de mettre en place une solution VPN Host-to-LAN (Client-to-site) qui permettra un accès externe à notre réseau d'entreprise via une connexion VPN SSL de type OpenVPN qui s'appuiera sur un équipement de type Firewall pfSense et se fera par le biais d'une authentification locale.

Un VPN Host-to-LAN signifie que nous allons donner la possibilité à un client (utilisateur) qui est sur un autre LAN de pouvoir travailler comme s'il était dans le même LAN que le serveur et ainsi de pouvoir profiter des ressources de notre réseau local.

Cela passe par la création d'un tunnel qui traverse un autre réseau local (LAN) ou même Internet par lequel passent des données cryptées.

Pour la mise en place de notre solution, nous disposons d'un serveur sous pfSense installé sur un hyperviseur « Hyper-V » sur une machine Windows 10 comportant deux

interfaces. Une des interfaces se situe dans le LAN (dans notre cas hn0 pour le réseau 172.16.0.0/24) et l'autre sur le WAN (dans notre cas hn1 pour le réseau 192.168.43.0/24). Nous disposons également d'un client sous Windows 10 c'est à dire une autre machine qui nous permettra de tester notre service OpenVPN depuis un réseau extérieur au LAN.

Le client qui est sur le réseau externe (dans notre cas 192.168.43.0/24) se connecte sur le LAN (172.16.0.0/24) par le VPN et possède une interface (virtuelle) dans le LAN qui lui permet de travailler comme s'il était physiquement dans le réseau local.

4.3 Description de l'environnement de travail

4.3.1 Notion de virtualisation

La virtualisation consiste, en informatique, à exécuter sur une machine hôte des systèmes d'exploitation dans un environnement isolé, on parle alors de virtualisation système ou des applications. Ces ordinateurs virtuels sont appelés « serveur privé virtuel » ou encore « environnement virtuel ». [8]

4.3.2 Hyper-V

Hyper-V, également connu sous le nom de Windows Server Virtualisation, est un système de virtualisation basé sur un hyperviseur 64 bits de la version de Windows Server 2008. Il permet à un serveur physique de devenir Hyperviseur et ainsi gérer et héberger des machines virtuelles communément appelées VM (virtual machines).

Grâce à cette technologie, il est possible d'exécuter virtuellement plusieurs systèmes d'exploitation sur une même machine physique et ainsi d'isoler ces systèmes d'exploitation les uns des autres.

Les ressources de l'hyperviseur sont alors mutualisées pour différentes VM, ce qui présente un intérêt économique car auparavant il fallait envisager une machine physique par serveur.

Il est possible d'utiliser la console Hyper-V sur Windows 7. Dans le sens inverse, de nombreux systèmes d'exploitation peuvent tourner à l'intérieur de Hyper-V :

Bien évidemment pour les systèmes d'exploitation Microsoft Windows (sauf version familliale) . [8]

4.3.3 pfSense

PfSense, ou «Packet Filter Sense » est un système d'exploitation open source ayant pour but la mise en place de routeur/pare-feu basé sur le système d'exploitation FreeBSD. À l'origine un fork de m0n0wall, il utilise le pare-feu à états Packet Filter ainsi que des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. pfSense convient pour la sécurisation d'un réseau domestique ou d'entreprise.

Après l'installation manuelle nécessaire pour assigner les interfaces réseaux, il s'administre ensuite à distance depuis l'interface web. pfSense gère nativement les VLAN (802.1q).

Comme sur les distributions Linux, pfSense intègre aussi un gestionnaire de paquets pour installer des fonctionnalités supplémentaires, comme un proxy ou un serveur de voix sur IP[10]

- PfSense est une distribution Free BSD dédiée firewall / routeur.
- Le firewall est basé sur Paquet Filter. Toute la configuration du système est stockée dans un fichier xml (/cf/conf/config.xml).
- Les Performances sont liées au matériel.

L'installation ainsi que la configuration pfSense se réalisera sur un système d'exploitation de type Free BSD. Il est possible d'émuler le système d'exploitation Free BSD grâce à VMware, Virtualbox ou Hyper-V.

PfSense offre quatre options de connectivité VPN :

- **OpenVPN :** OpenVPN est une solution flexible, puissante solution de VPN SSL supportant une large gamme de systèmes d'exploitation client.
- **IPSec :** permet la connectivité avec tout dispositif de support standard IPsec. Ceci est le plus généralement utilisé pour la connectivité du site aux installations PfSense.

- **L2TP :** Cette option va gérer le Layer 2 Tunneling Protocol (L2TP) qui signifie protocole de tunnellisation de niveau 2. Il s'agit d'un protocole réseau utilisé pour créer des réseaux privés virtuels (VPN).

- **PPTP :** est une option populaire VPN, car presque tous les OS sont dotés d'un client PPTP, y compris toutes les versions de Windows depuis Windows 95 OSR2. Le serveur pfSense PPTP peut utiliser une base de données d'utilisateur local, ou d'un serveur RADIUS pour l'authentification.

4.3.4 FreeBSD

FreeBSD est un système d'exploitation Unix libre pour les plates-formes modernes de type serveur, station de travail et systèmes embarqués.

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

FreeBSD offre des possibilités avancées en matière de réseau, de performance, de sécurité et de compatibilité. [8]

4.3.5 Wireshark

Wireshark est un analyseur de paquets libre et gratuit. Il est utilisé dans le dépannage et l'analyse de réseaux informatiques, le développement de protocoles, l'éducation et la rétro-ingénierie.

Wireshark utilise la bibliothèque logicielle Qt pour l'implémentation de son interface utilisateur et pcap pour la capture des paquets ; il fonctionne sur de nombreux environnements compatibles UNIX comme GNU/Linux, FreeBSD, NetBSD, OpenBSD ou Mac OSX, mais également sur Microsoft Windows. Il existe aussi entre autres une version en ligne de commande nommée TShark. Ces programmes sont distribués gratuitement sous la licence GNU General Public License. [8]

4.4 Création de la machiner virtuelle sous Hyper-V

La démarche à suivre pour la création de notre machine virtuelle « pfSense » se décrit comme suit :

Il nous faut d'abord nous rendre sur le site officiel du logiciel de « pfSense » à l'adresse www.pfsense.org/download/ pour télécharger l'image ISO. Dans notre cas nous téléchargeons la version 2.6.0

	Minimale
CPU	2 cœurs
Mémoire RAM	2 GO
Disque Dur	60 GO
Carte réseau	2 cartes réseaux

Table 4.1 - Les prérequis matériels.

Pour créer notre machine virtuelle, nous allons ouvrir hyperviseur Hyper-V sur notre machine Windows 10 en nous rendant dans le « Gestionnaire Hyper-V ». Et en cliquant dessus pour accéder à la console d'administration d'hyperviseur Hyper-V.

Pour commencer la création de la nouvelle machine, on clique sur « Démarrez l'assistant de nouvelle machine virtuelle » et on ajoute un nom.

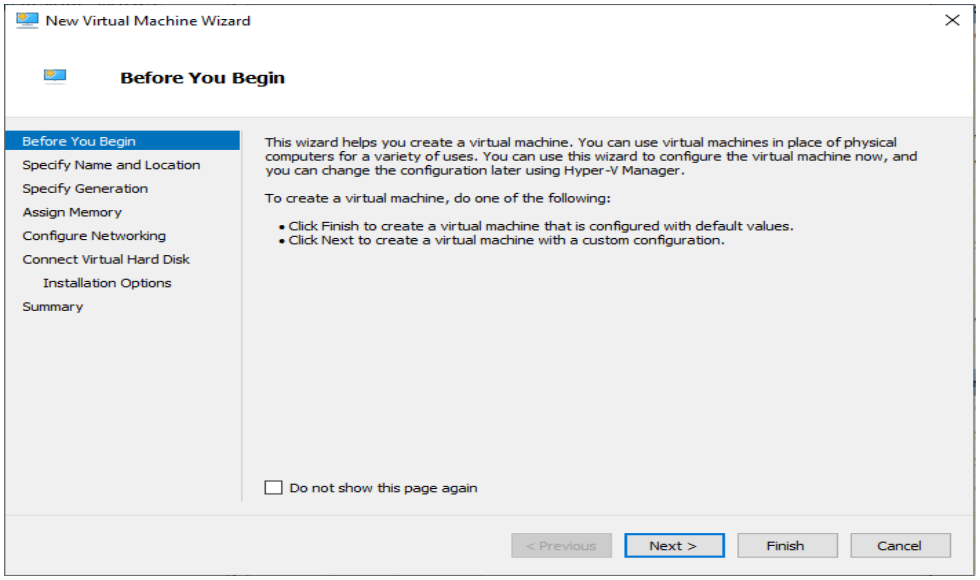

Figure 4.2 - Création de la machine virtuelle.

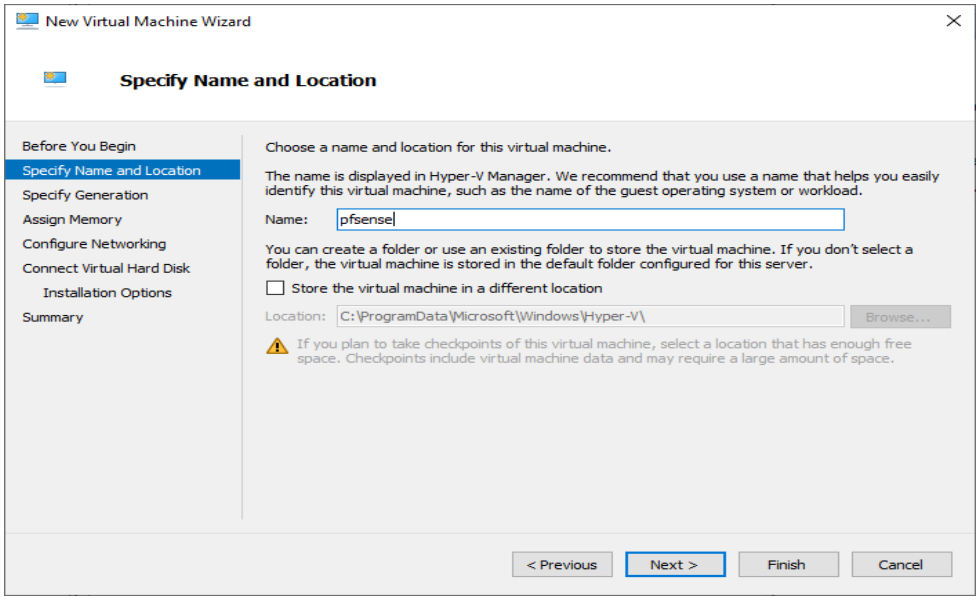

Figure 4.3 – Affectation d'un nom à la machine virtuelle.

Après on clique sur suivant et on sélectionne la génération de machine virtuelle appropriée : Génération 1.

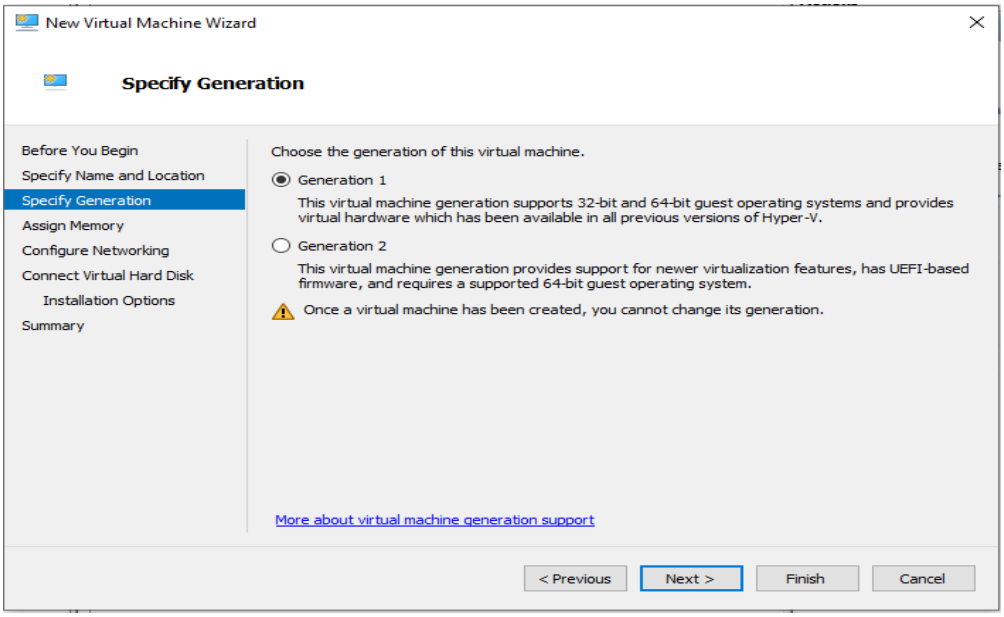

Figure 4.4 – Choix de Génération de la machine virtuelle.

On choisisse la mémoire que nous voulons attribuer sur notre système virtualisé (2 GO est préférable).

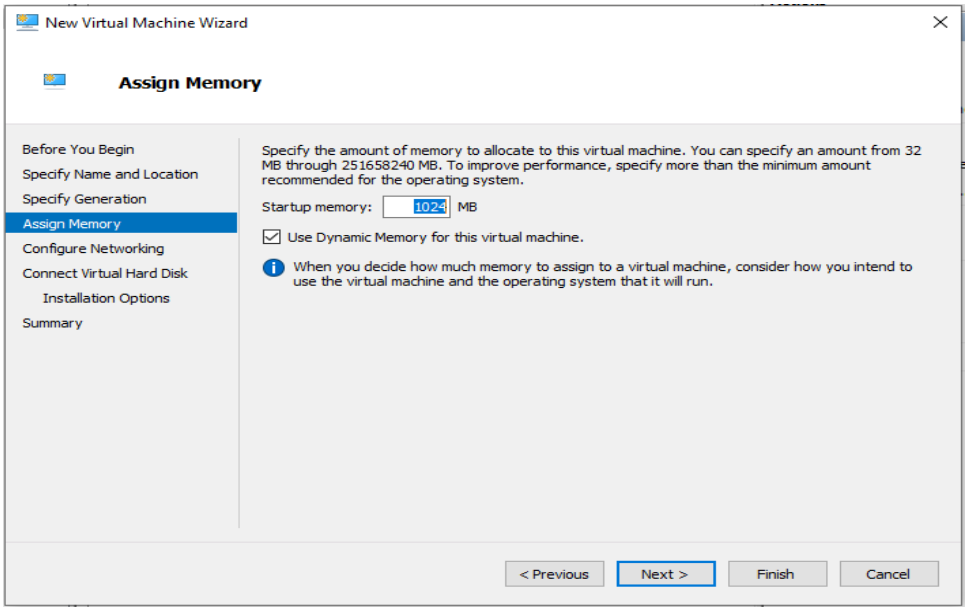

Figure 4.5 – Affectation d'une memoire à la machine virtuelle.

L'étape suivante consiste à configurer la mise en réseau, on sélectionne WAN dans le menu déroulant Connexion. Nous ajouterons LAN plus tard.

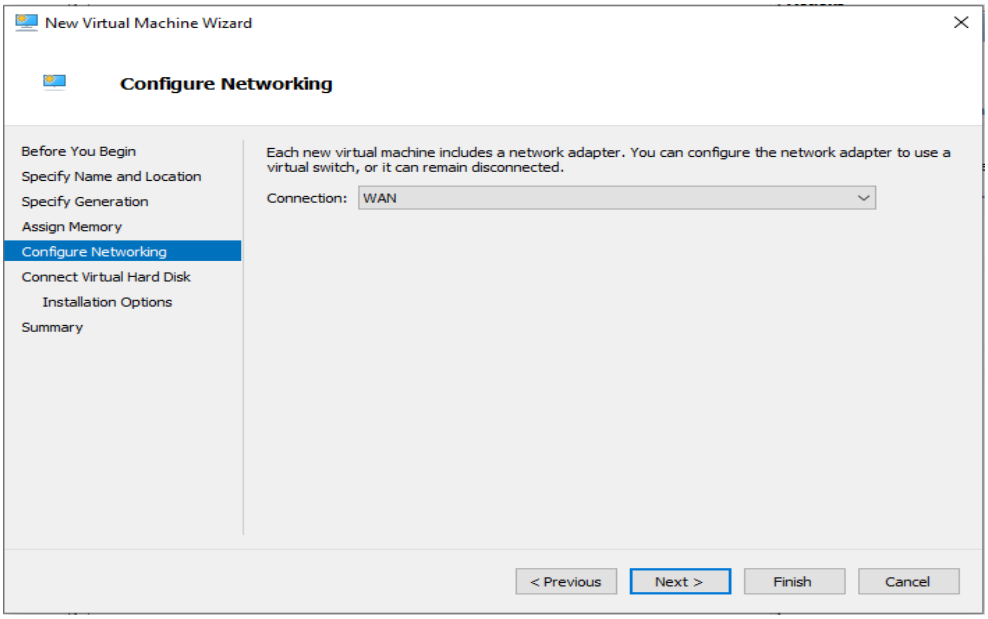

Figure 4.6 – Choix de l'interface WAN de la machine virtuelle.

Afin de configurer un disque dur virtuel pour la machine virtuelle, on sélectionne « Créer un disque dur virtuel » et on attribue 20 Go au pfSense.

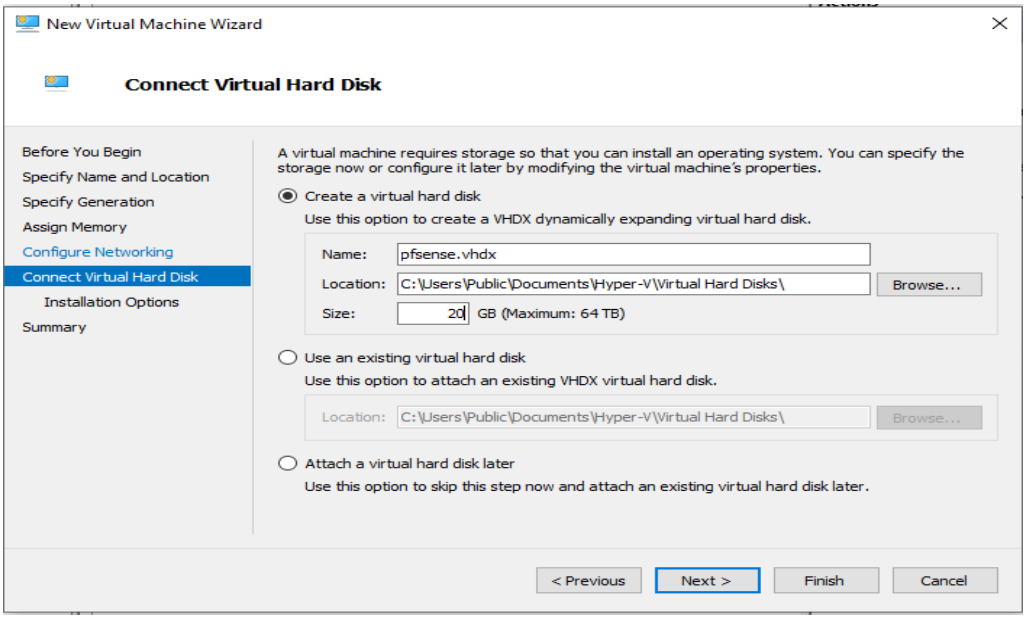

Figure 4.7 – Création d'un disque dur virtuel à la machine virtuelle.

Après on sélectionne « Installer un système d'exploitation à partir d'un CD/DVD-ROM amorçable » pour accéder à l'ISO du programme d'installation de pfSense.

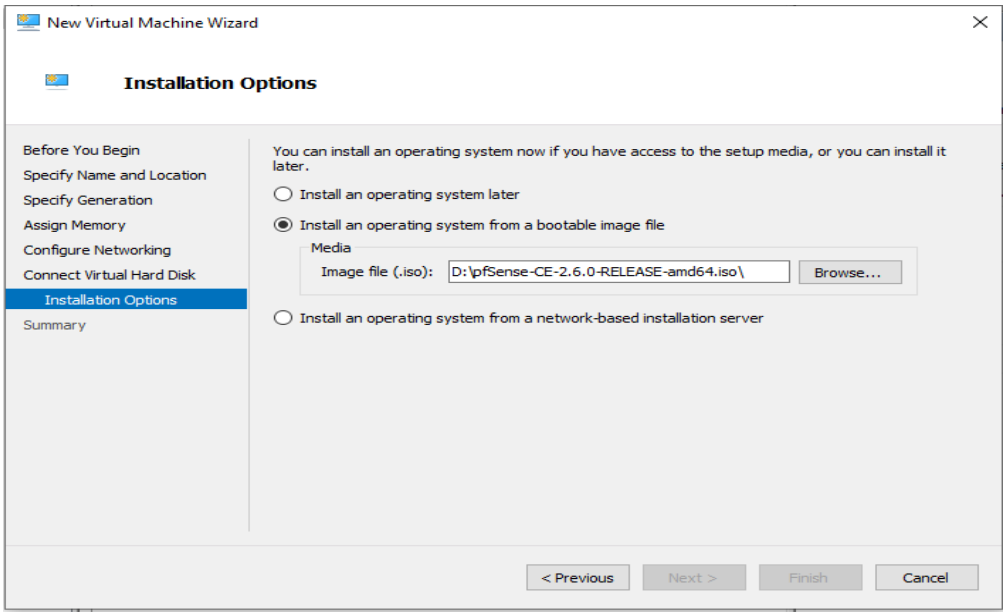

Figure 4.8 – Choix de l'ISO du programme d'installation de la machine virtuelle.

Maintenat passons en revue les informations de la machine virtuelle pour terminer l'assistant d'installation.

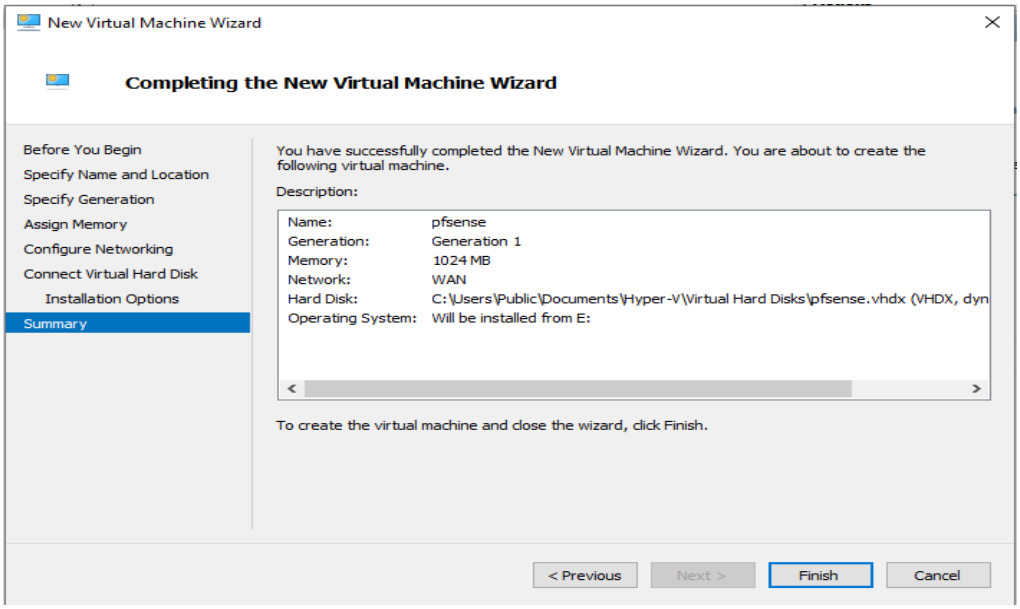

Figure 4.9 – Fin de création de la machine virtuelle.

4.5 Installation et configuration de pfSense sous Hyper-V

4.5.1 Installation de pfSense

- On démarre notre machine à partir du cd de l'image iso de pfSense ;

- A l'écran de bienvenue, on laisse le setup démarrer automatiquement après quelques secondes, on appui sur la touche « Entrée » pour accepter.

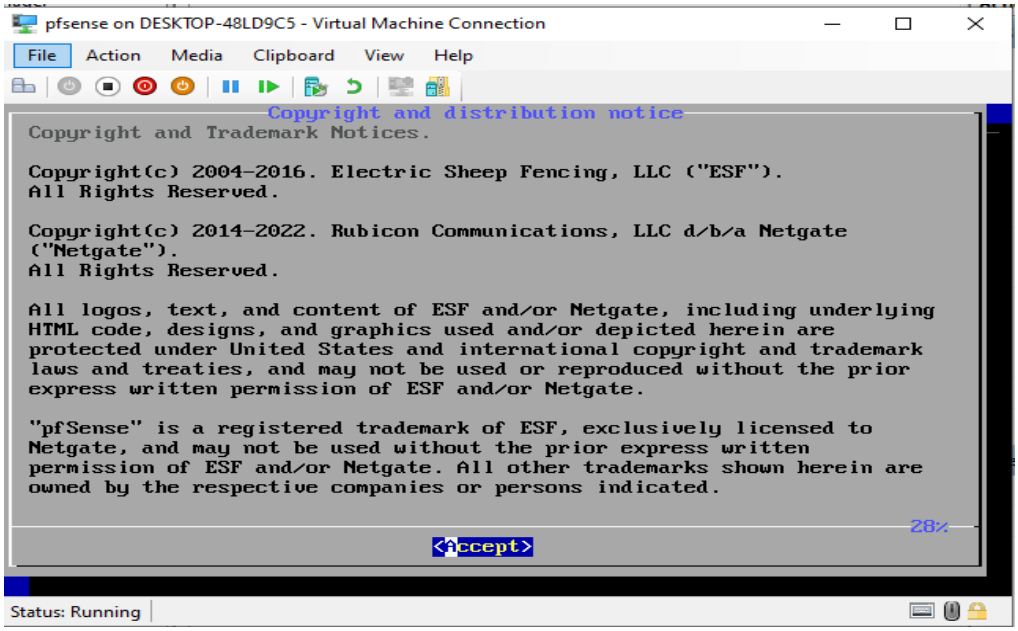

Figure 4.10 – Acceptation de l'installation.

Après on vérifie qu'on est bien sur « Install » et on appuie sur « Entrée » pour faire OK.

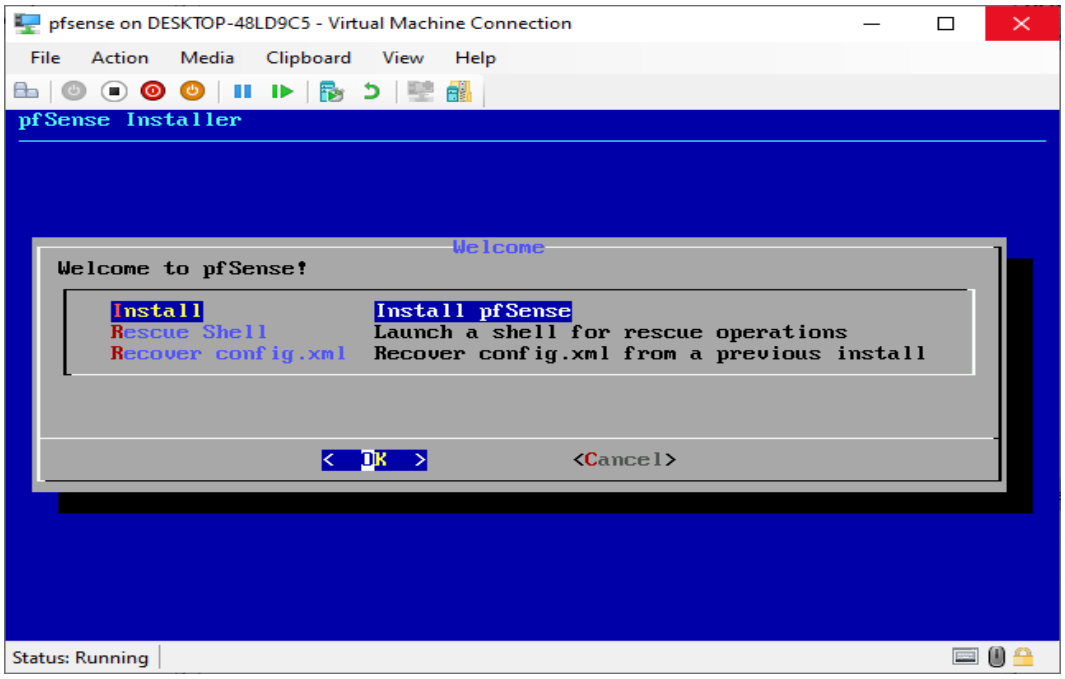

Figure 4.11 – Lancement de l'installation.

Une fois l'installation terminée, on sélectionne « Redémarrer » et on éjecte l'ISO.

La machine virtuelle pfSense va démarrer rapidement et demander les affectations d'interface. On sélectionne « n » pour ne pas configurer les VLAN maintenant.

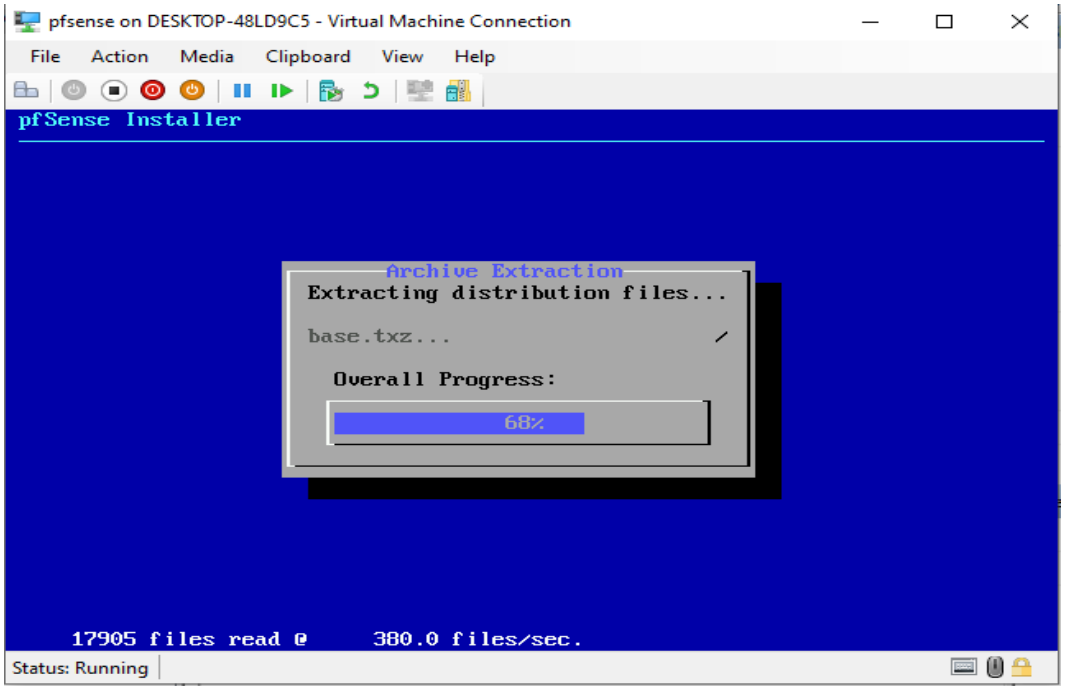

Figure 4.12 – Installation et copie des fichiers.

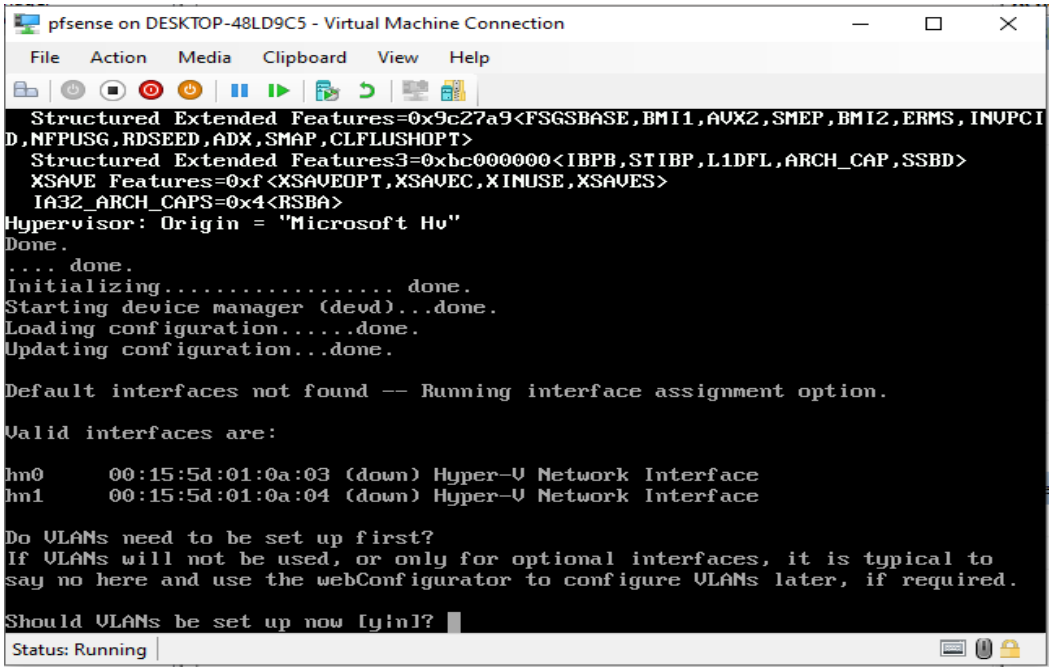

Figure 4.13 – Détection des cartes réseaux.

Dans l'étape suivante, on affecte les interfaces WAN et LAN aux adaptateurs réseaux appropriés.

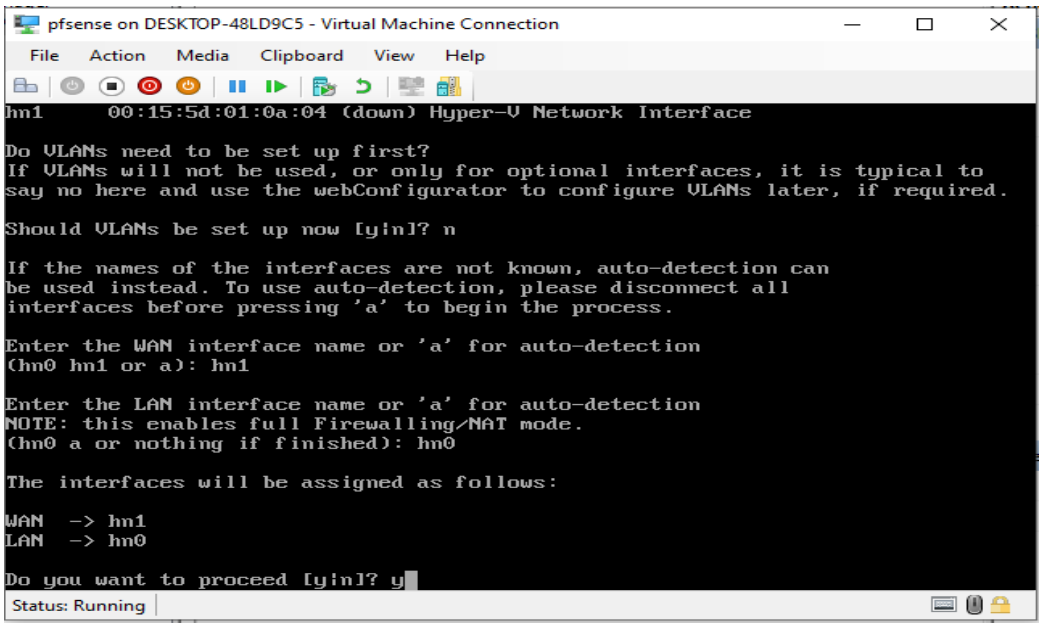

Figure 4.14 – Affectation des interfaces.

Après avoir attribué les interfaces, le logiciel pfSense terminera le démarrage.

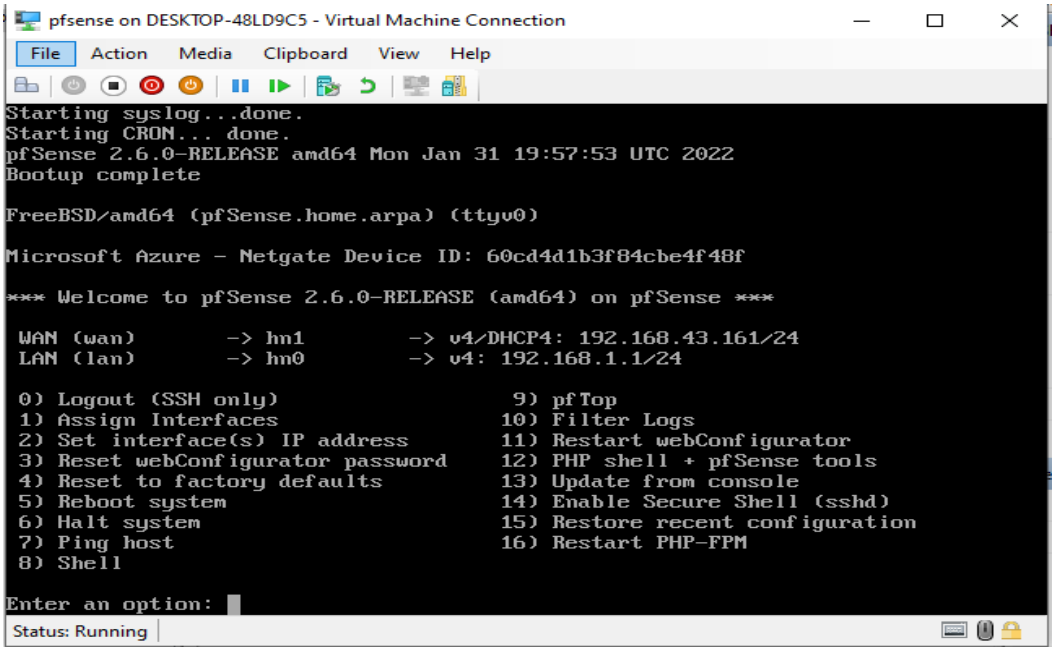

Figure 4.15 – Fin du démarage.

Dans le menu de pfSense, on tape le choix 2 : « Set LAN IP adresse ». Pour affecter une adresse IP sur la passerelle de LAN de la machine de pfSense.

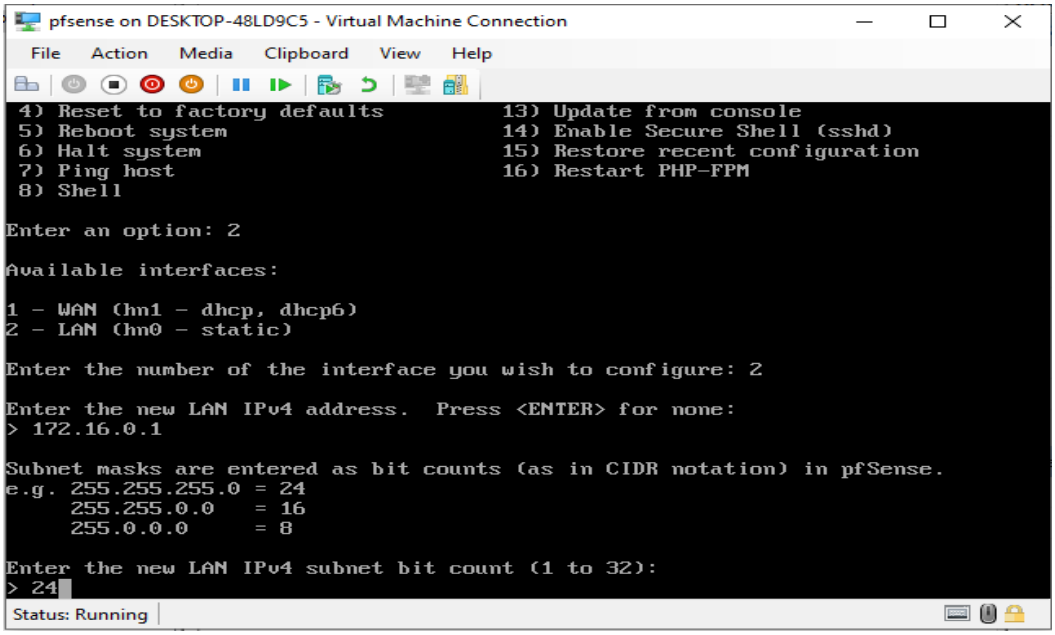

Figure 4.16 – Choix de l'IP et du masque de sous réseau.

Enfin on aura le menu suivant

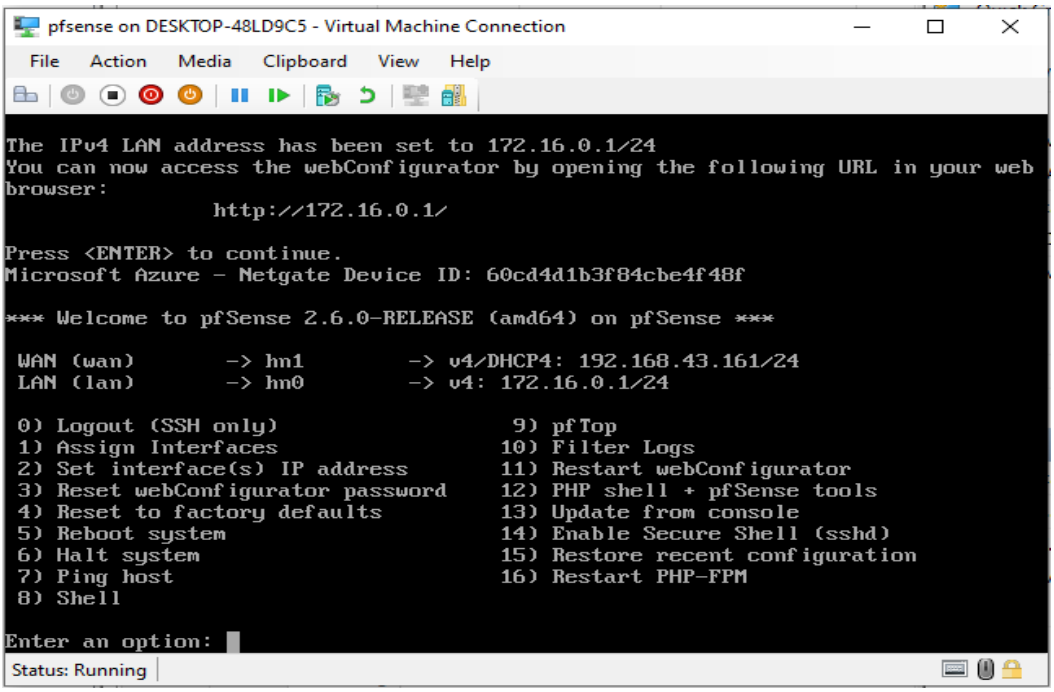

Figure 4.17 – Fin de l'installation .

pfSense		
Type de réseau	WAN	LAN
IP de l'interface	192.168.43.161	172.16.0.1
Masque de sous réseau	255.255.255.0	255.255.255.0

Table 4.2 - Tableau récapitulatif des interfaces.

4.5.2 Configuration de pfsense via l'interface web

On ouvre ensuite notre navigateur Web, puis on tape http://172.16.0.1, par défaut on met :

- Identifiant : admin
- Mot de passe : pfSense

Après l'identification, on serait appelé à faire la configuration initiale pour préparer notre serveur comme sur la figure 4.19.

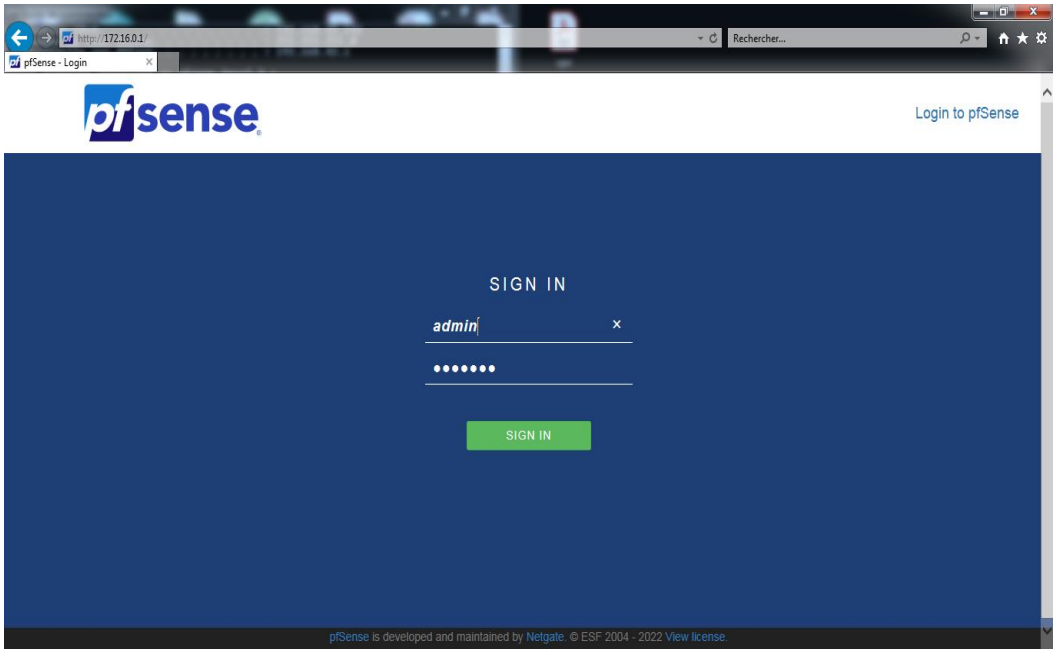

Figure 4.18 – Page de connexion de l'interface web.

On arrive enfin, à l'interface web. Allons ensuite dans « System », puis « General Setup ».

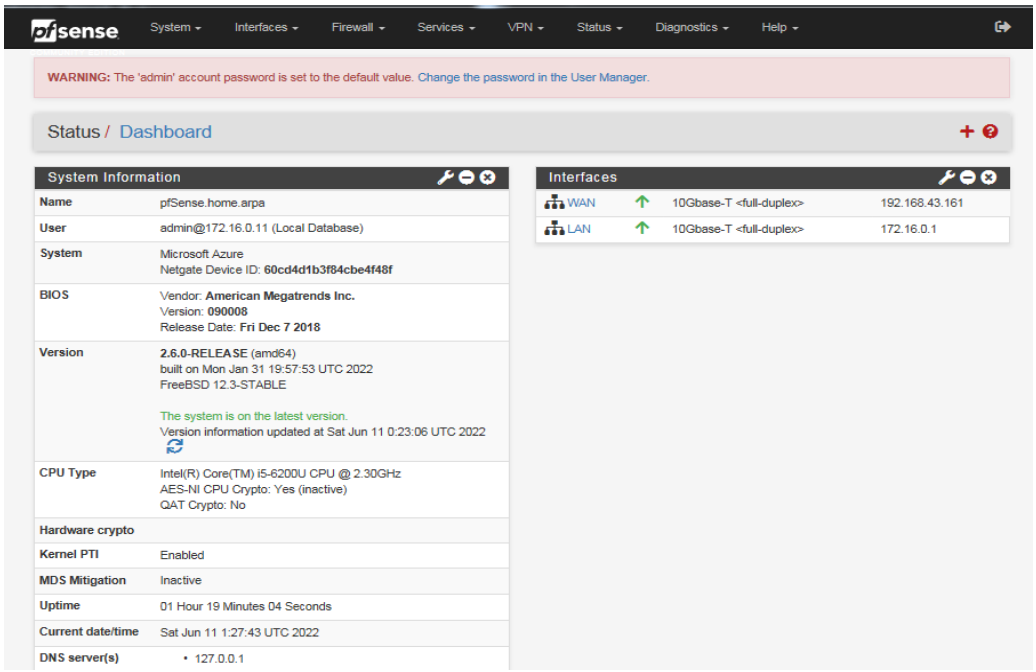

Figure 4.19 – Page d'accueil de pfSense.

4.6 Mise en place d'une Solution VPN

Nous allons voir, dans ce qui suit, les étapes à suivre afin de configurer et de mettre en place un serveur/client VPN via OpenVPN.

4.6.1 Présentation d'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 et 10, 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. [8]

4.6.2 Présentation d'OpenSSL

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. [8]

4.6.3 Critères de choix d'utilisation d'Openvpn / Openssl

- OpenVPN est un protocole très sécurisé, capable d'utiliser des clés de cryptage 256 bits et des algorithmes de chiffrement haut de gamme.
- Le protocole OpenVPN peut facilement contourner tout pare-feu qu'il rencontre.
- Comme OpenVPN peut utiliser TCP et UDP, il vous offre plus de contrôle sur vos connexions.
- OpenVPN fonctionne sur un grand nombre de plates-formes. Quelques exemples incluent Windows, macOS, iOS, Android, Linux, routeurs, FreeBSD, OpenBSD, NetBSD, et Solaris.OpenVPN prennent en charge Perfect Forward Secrecy.

4.6.4 Configuration du serveur OpenVPN

Nous aborderons dans ce qui suit les principales configurations à mettre en place au pare-feu (pfSense), le serveur OpenVPN et le client.

Nous suivrons les étapes suivantes afin de mettre en place un tunnel VPN en utilisant l'assistant « Wizard »

On commence, par mettre en place le service OpenVPN sur le firewall. Pour cela, nous allons dans le menu « VPN » ensuite le sous-menu « OpenVPN ».

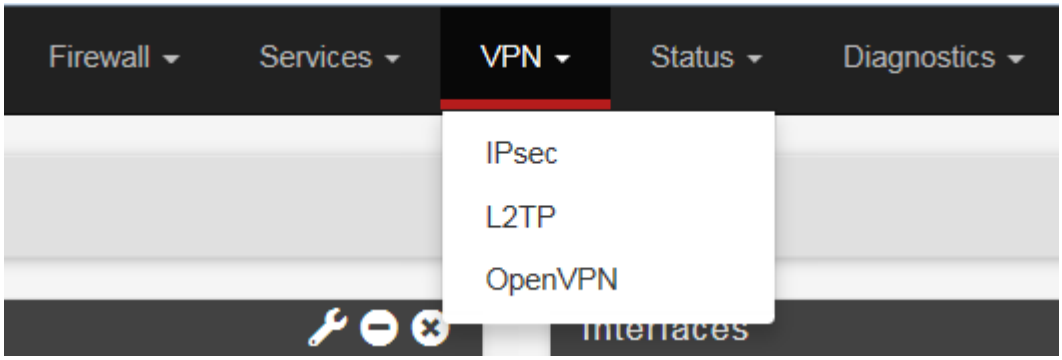

Figure 4.20 - Choix du protocole VPN.

Nous allons utiliser l'assistant pour configurer OpenVPN. Pour cela on clique sur « Wizards ».

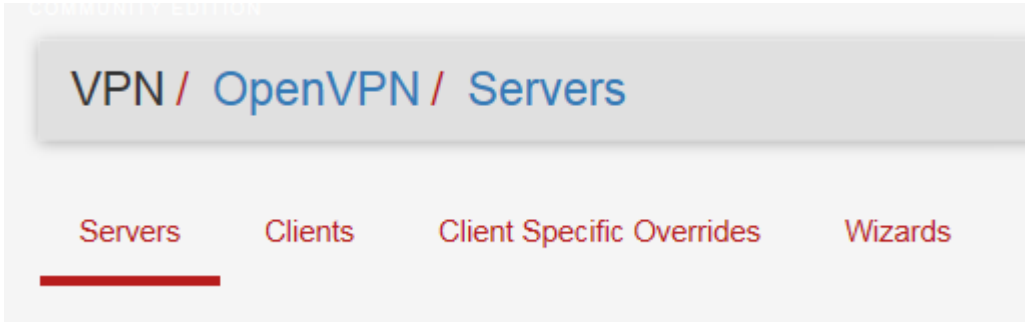

Figure 4.21 - Configuration OpenVPN par l'assistant « Wizards » .

Après le lancement de « Wizards » dans la liste déroulante, on définit le type d'authentification « Type of Server », dans notre cas nous choisissons « Local User Access » pour des utilisateurs locaux, ensuite on clique sur « Next ».

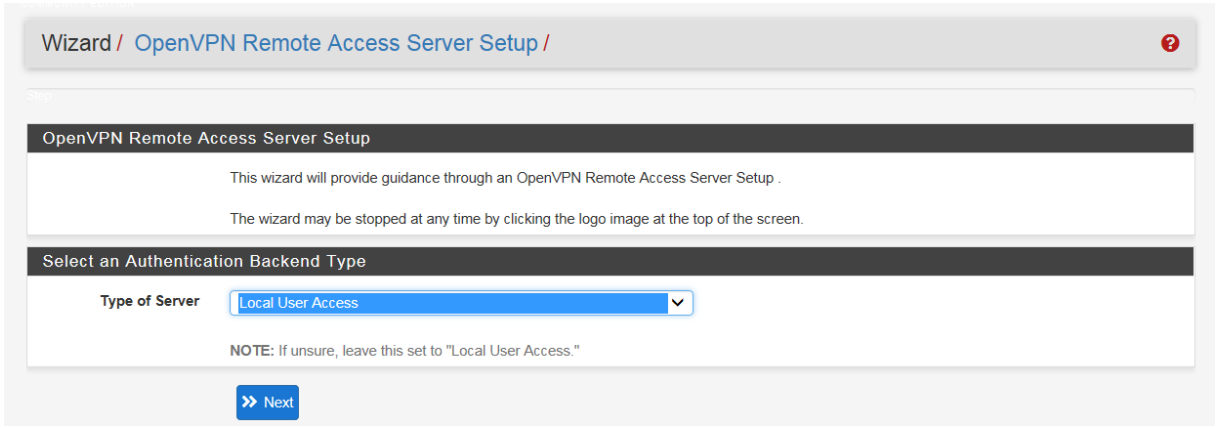

Figure 4.22 - Choix du serveur d'authentification.

4.6.4.1 Création des certificats

a) Création d'autorité de certification

On commence par créer une nouvelle autorité de certification (CA) en cliquant sur « Add new CA » en remplissant les champs comme suit :

Description name: pfSense_CA

Key lengh: 2048

Lifetime: 3650

Country Code: DZ

State or Province: Blida

City : Blida

Organization : Université

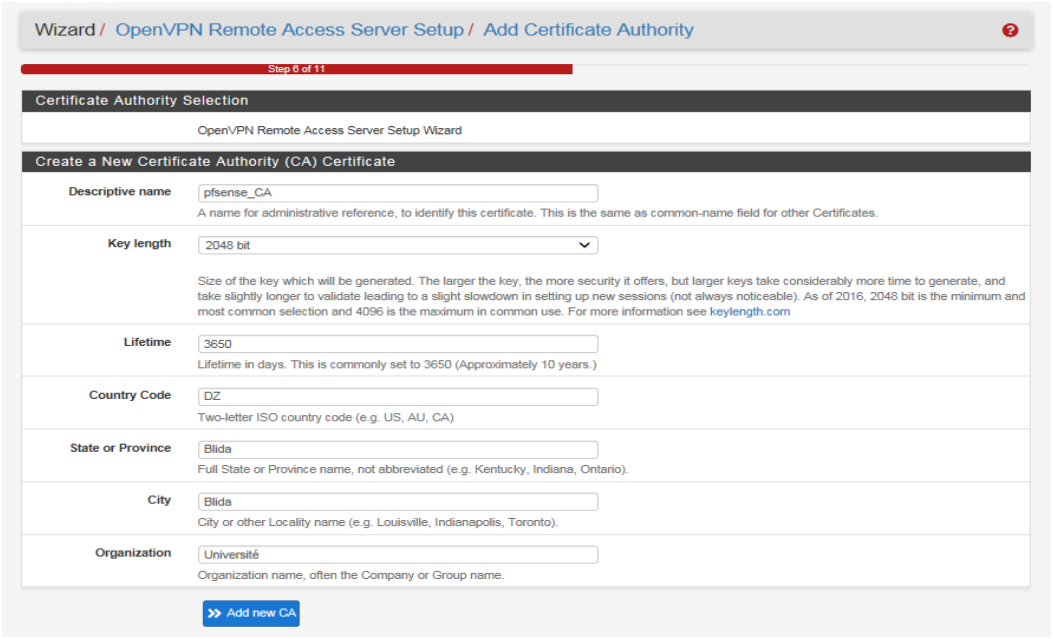

Figure 4.23 - Création de l'autorité de certification.

b) Création du certificat serveur

Ensuite, on crée un certificat pour le serveur VPN en question, on laisse les champs préremplis selon nos informations précédentes, en saisissant une description « VPN_Serveur_Certificat » dans notre cas ensuite on clique sur « Create new certificate ».

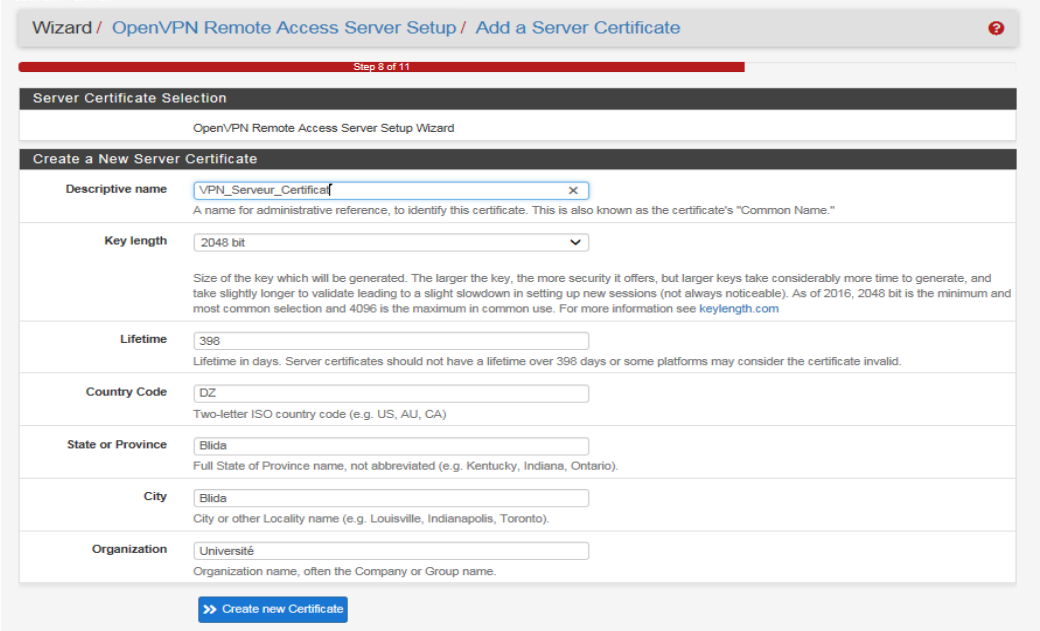

Figure 4.24 - Création du Certificat pour le serveur VPN.

4.6.4.2 Configuration au niveau de serveur OpenVPN

Nous arrivons ensuite sur étape « 9/11 » dans la partie « General Information ». On remplir les champs comme suit :

Interface : WAN

Protocol : UDP on IPV4 only

Local Port : 1194, nous pouvons choisir un autre port

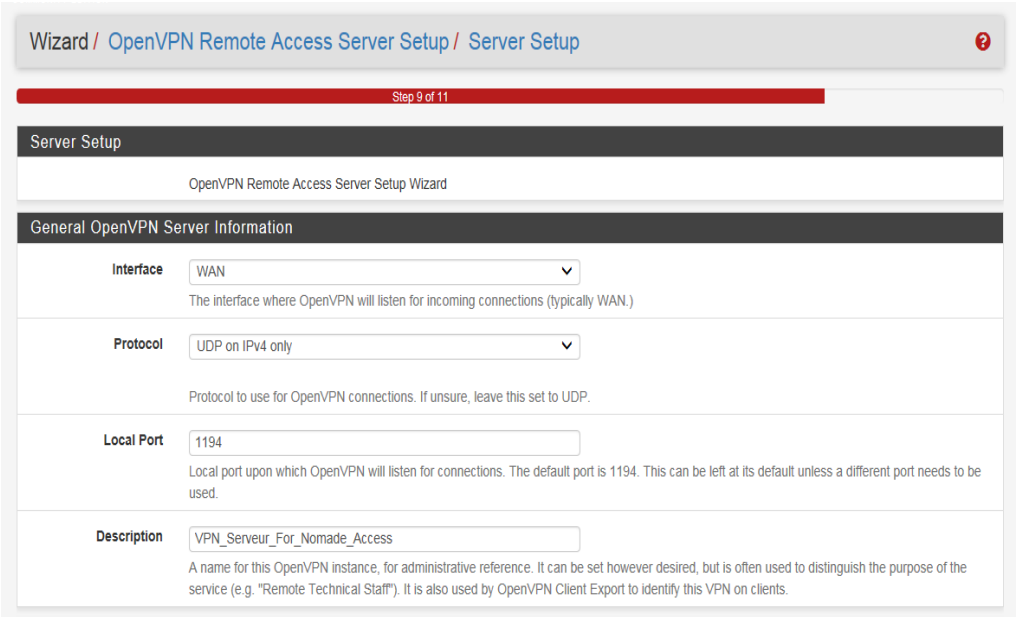

Figure 4.25 - Configuration serveur OpenVPN.

L'étape suivante concernera les paramètres de sécurités mise en place pour le chiffrement de la communication entre le client et le serveur OpenVPN. On laissera les cases cochées et on sélectionne l'algorithme de chiffrement AES-256-GCM ainsi que Auth Digest Algorithm sur SHA256 pour plus de sécurité.

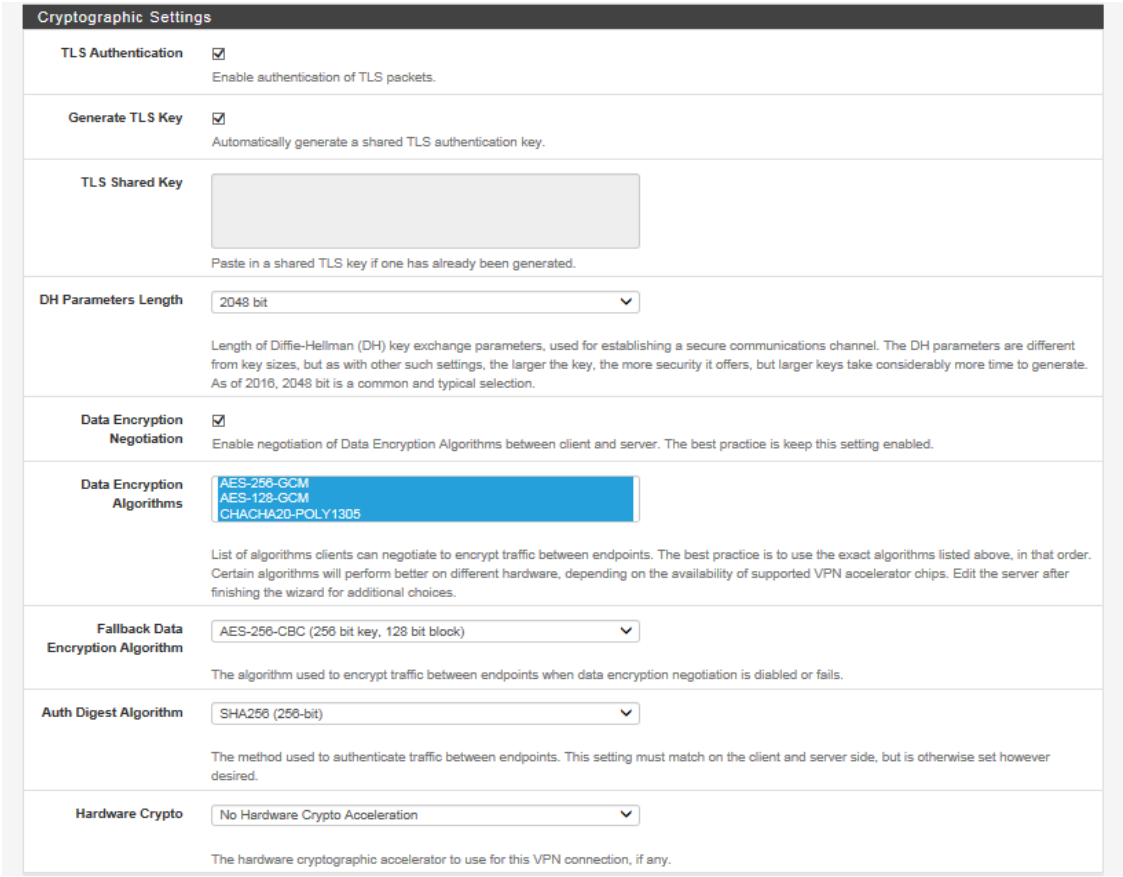

Figure 4.26 - Paramètre de chiffrement.

Ensuite, on arrive aux paramétrages du tunnel VPN. Pour cela on définir :

- L'adresse réseau de notre tunnel VPN.
- L'adresse du réseau LAN qu'on souhaite atteindre depuis le VPN.

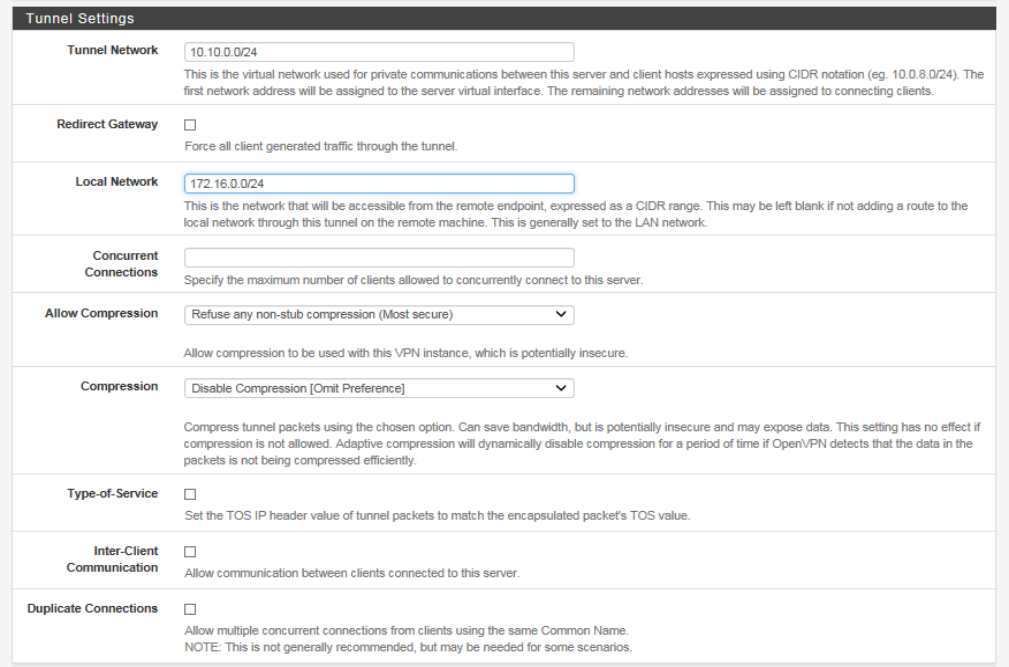

Figure 4.27 - Configuration du tunnel.

On arrive ensuite dans le dernier paragraphe, « Client settings » permettant de définir des options sur le client qui se connectera à distance comme un nom d'un domaine, l'attribution d'adresses DNS, NTP, ensuite on clique sur « Next ».

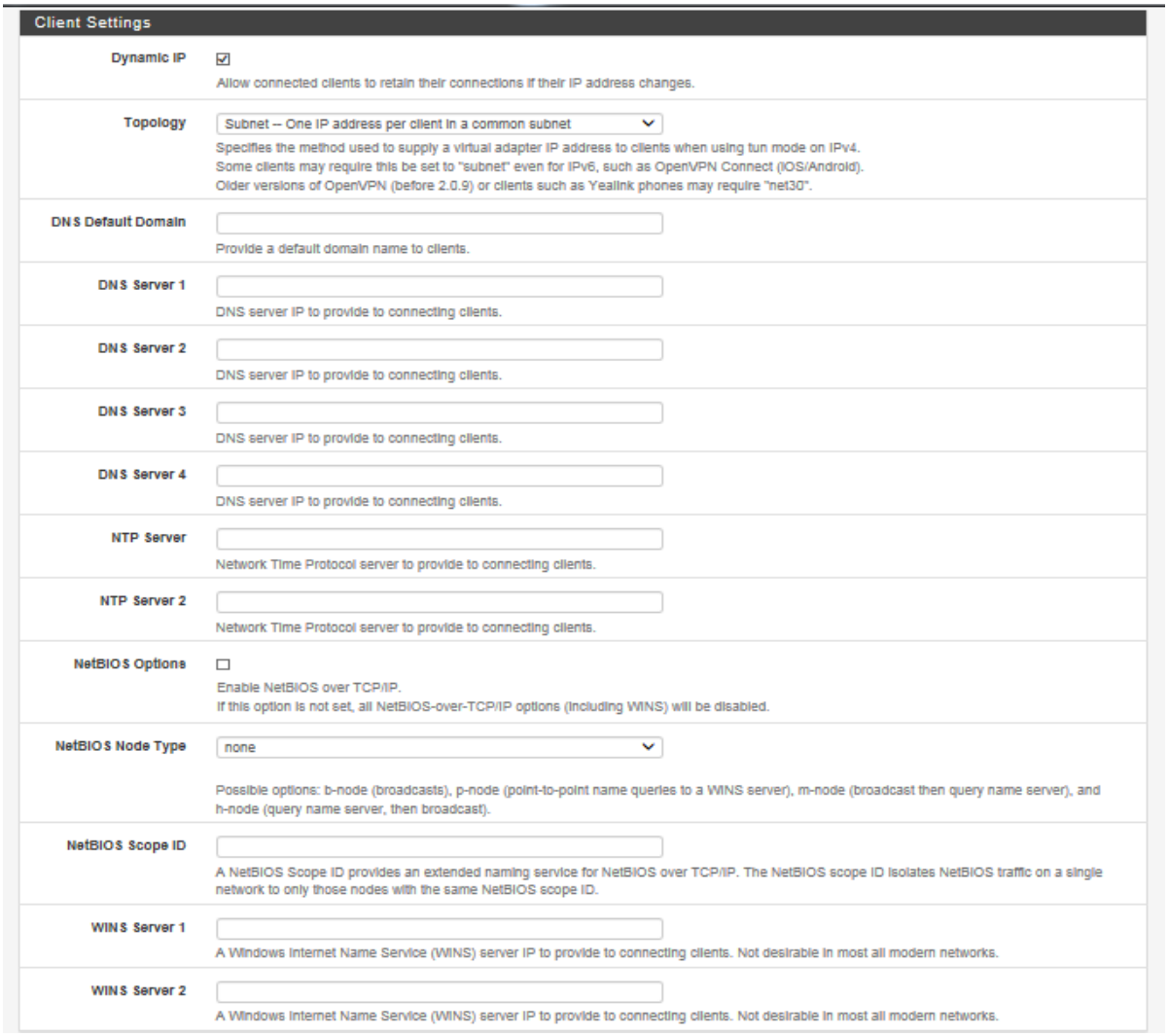

Figure 4.28 - Attribution d'adresse IP.

L'avant dernière étape nous permet de créer automatiquement des règles de pare-feu dans pfSense concernant la connexion VPN. Pour cela, on coche les options d'ajout des « Firewall Rule » ainsi que les « OpenVPN rule » et on clique sur Next.

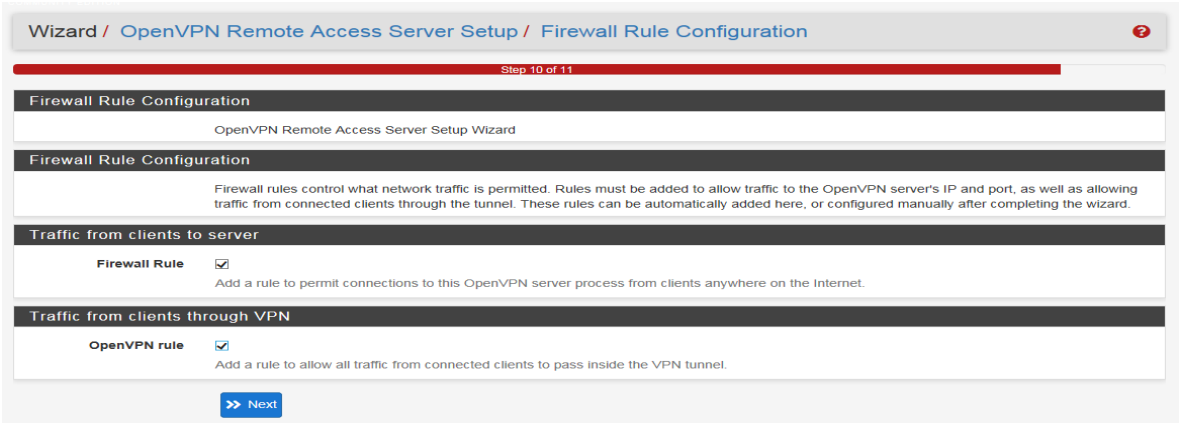

Figure 4.29 - Création des règles sur le Firewall.

Et enfin, on clique sur Finish, pour terminer cette configuration

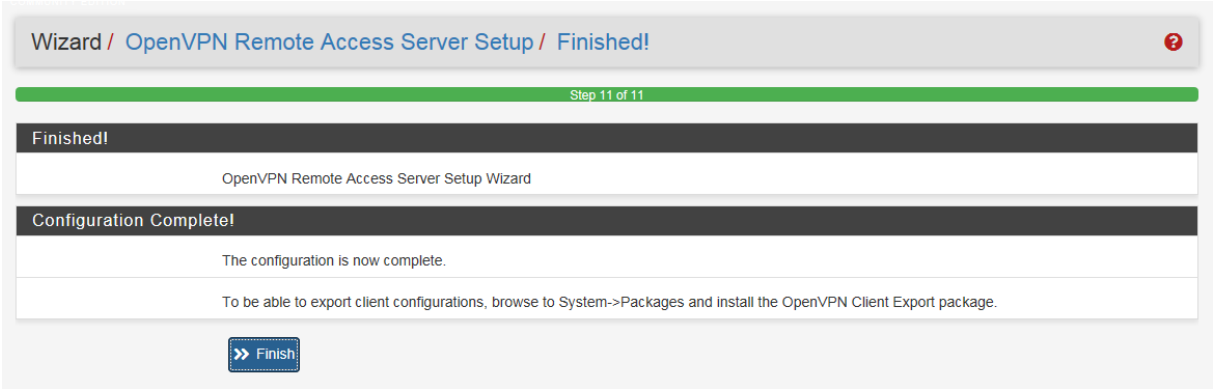

Figure 4.30 - Fin de la configuration OpenVPN.

Vérifions que le tunnel VPN a bien été créé

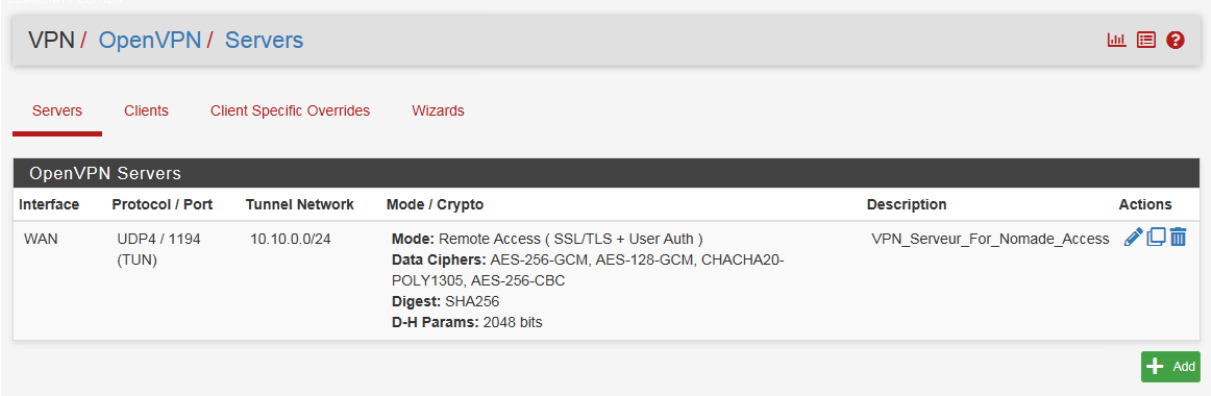

Figure 4.31 - Vérification de la création tunnel VPN.

4.6.4.3 Génération des clients OpenVPN préconfigurés

Nous allons créer un utilisateur pour que celui-ci se connecte à distance par la suite.

Pour cela, on se rend dans le menu « System », puis dans le sous-menu « User Manager ».

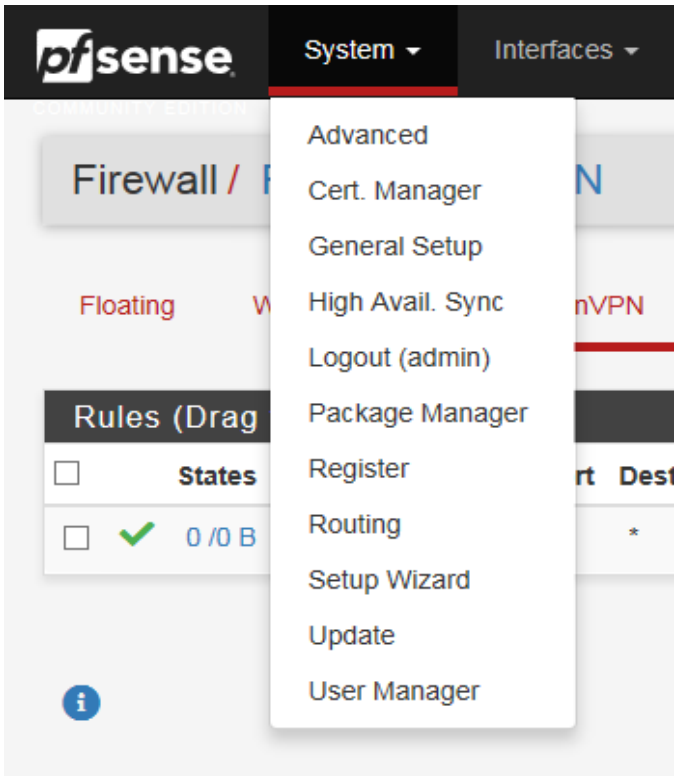

Figure 4.32 - Création d'utilisateur OpenVPN.

On coche la case « Certificate » pour créer un certificat pour cet utilisateur précisément, et lui donne un nom ensuite on clique sur « Save » pour terminer.

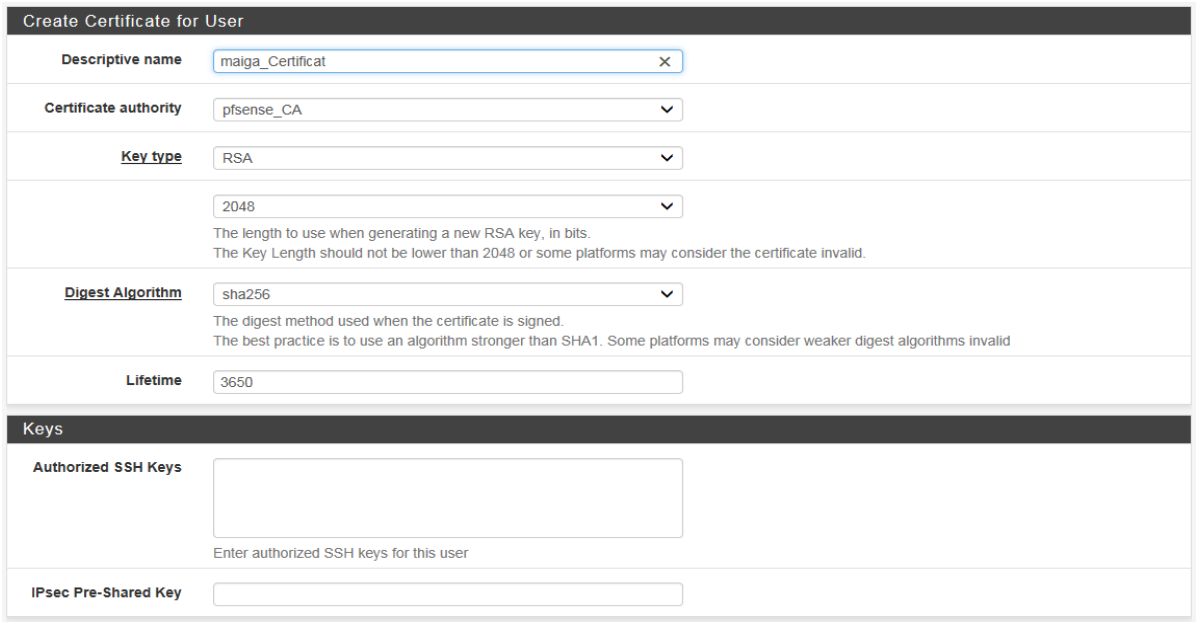

Figure 4.33 - Création de certificat utilisateur.

Le certificat de l'utilisateur est enfin prêt

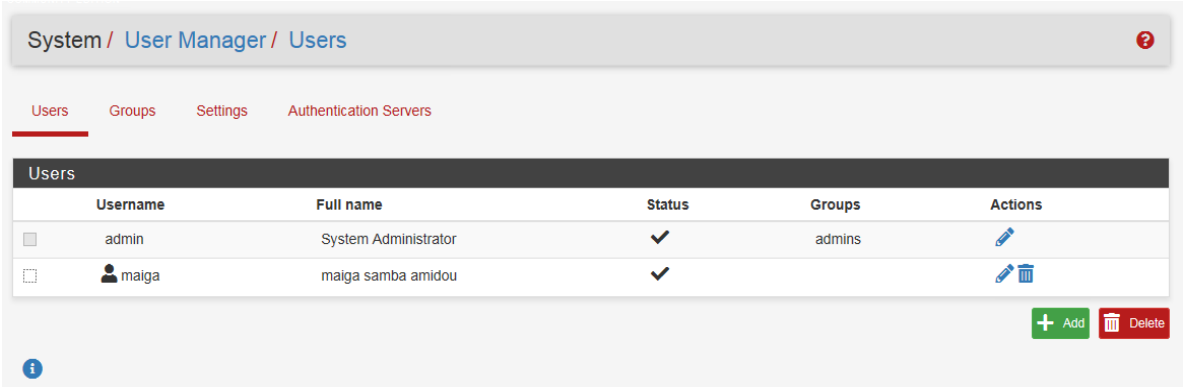

Figure 4.34 - Vérification de certificat utilisateur.

Maintenant nous allons pouvoir récupérer la configuration grâce à un plugin que nous allons installer. Allons dans le menu « System » et dans le sous-menu « Package Manager ».

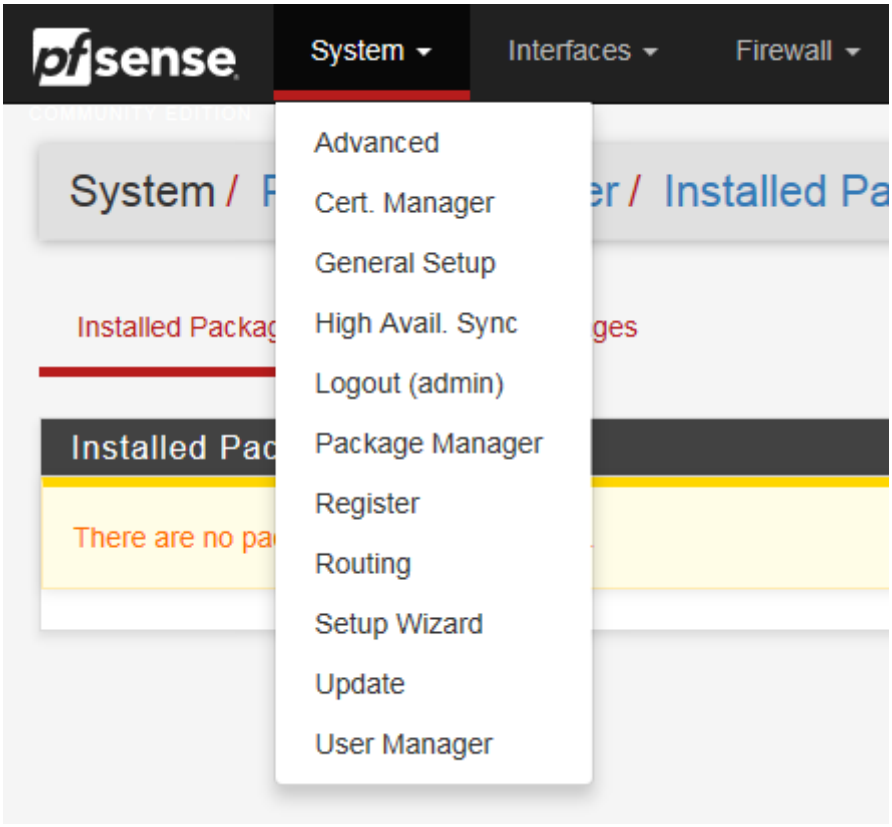

Figure 4.35 - Vérification de certificat utilisateur.

Dans la partie « Available Packages », saisissons « openvpn » dans la barre de recherche. Puis cliquons sur le bouton « Install » de l'extension nommée « openvpn-client-export ».

Figure 4.36 - Installation du package openvpn-client-export .

On confirme le choix d'installer ce plugin.

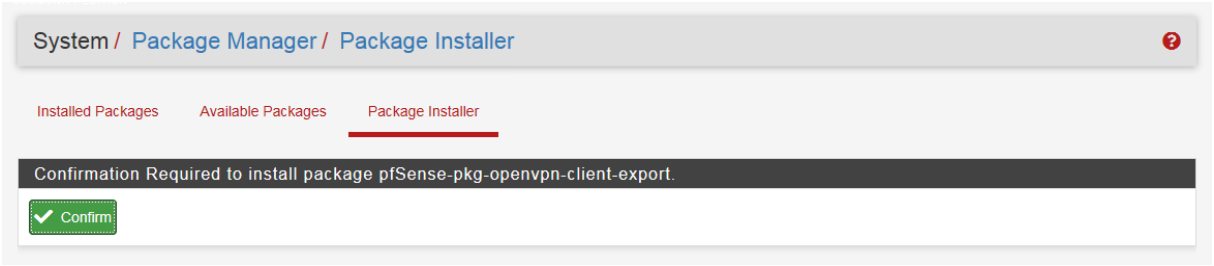

Figure 4.37 - Confirmation d'installation du package openvpn-client-export .

Après quelques instants, un message nous confirmera que l'installation s'est correctement déroulée.

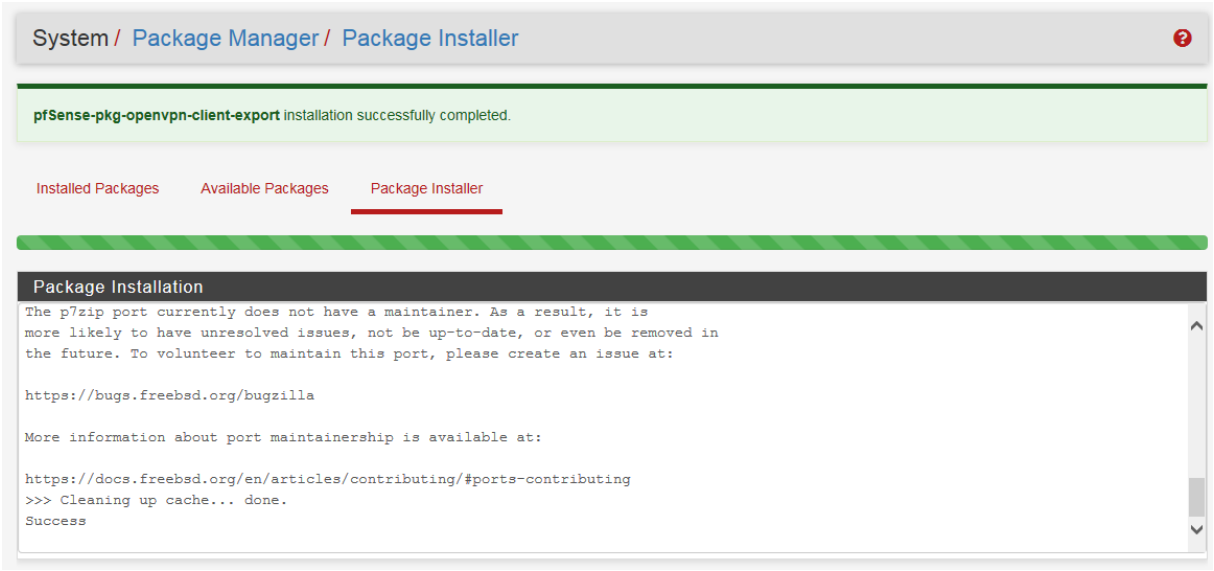

Figure 4.38 - Téléchargement du package openvpn-client-export.

Retournons dans le menu « VPN », sous-menu « OpenVPN ». Cliquons sur nouvelle catégorie appelée « Client Export ». Pour choisir la connexion VPN par laquelle nous souhaitons récupérer la configuration.

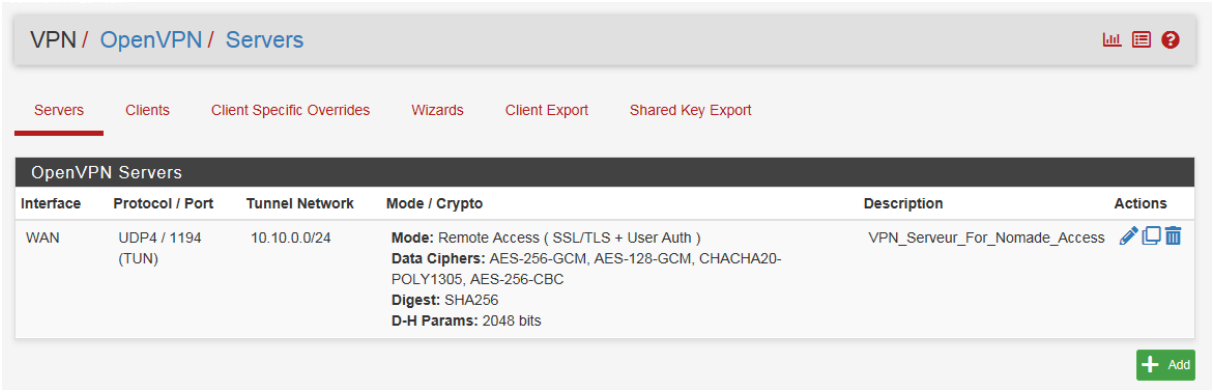

Figure 4.39 - Choix de la connexion du client OpenVPN.

Après authentification, le client aura accès à la page client Open VPN pour qu'il puisse télécharger le package qui contient le client Open VPN et la configuration intégrée.

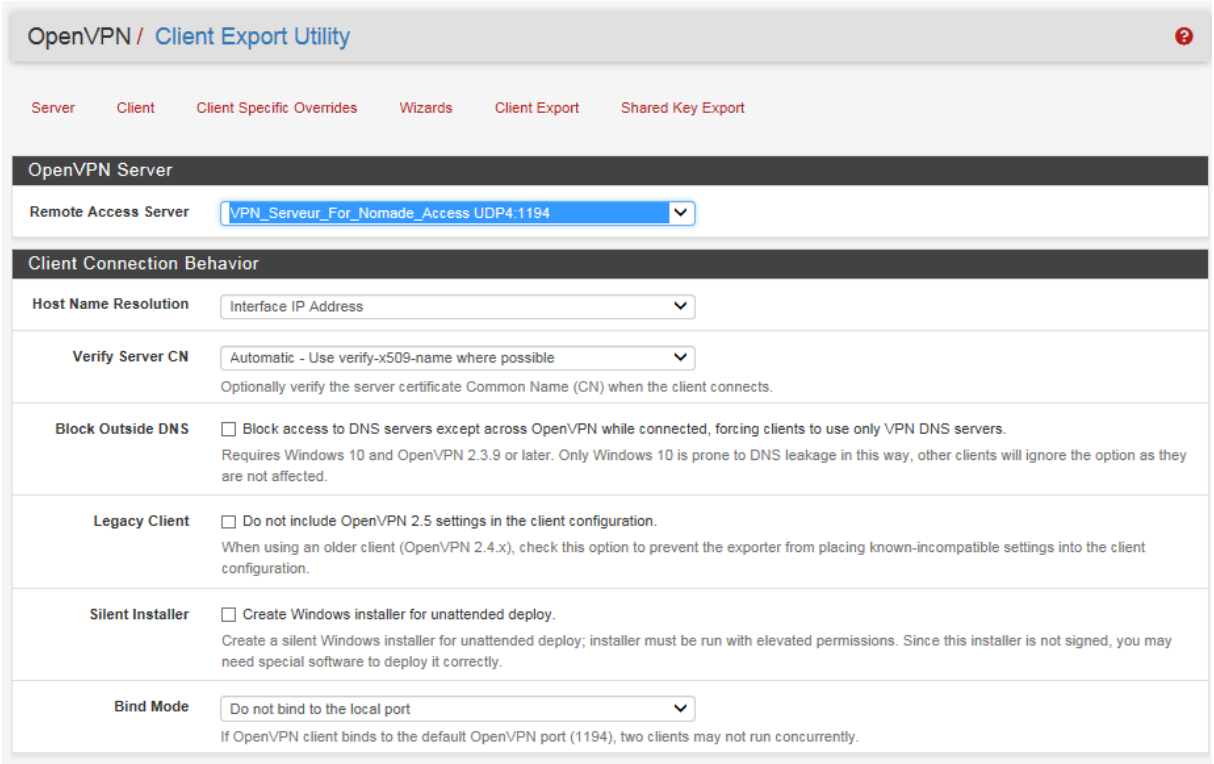

Figure 4.40 - Page client OpenVPN.

Dans la colonne « Export », nous disposons de plusieurs liens de téléchargement pour obtenir la configuration nécessaire à la connexion VPN.

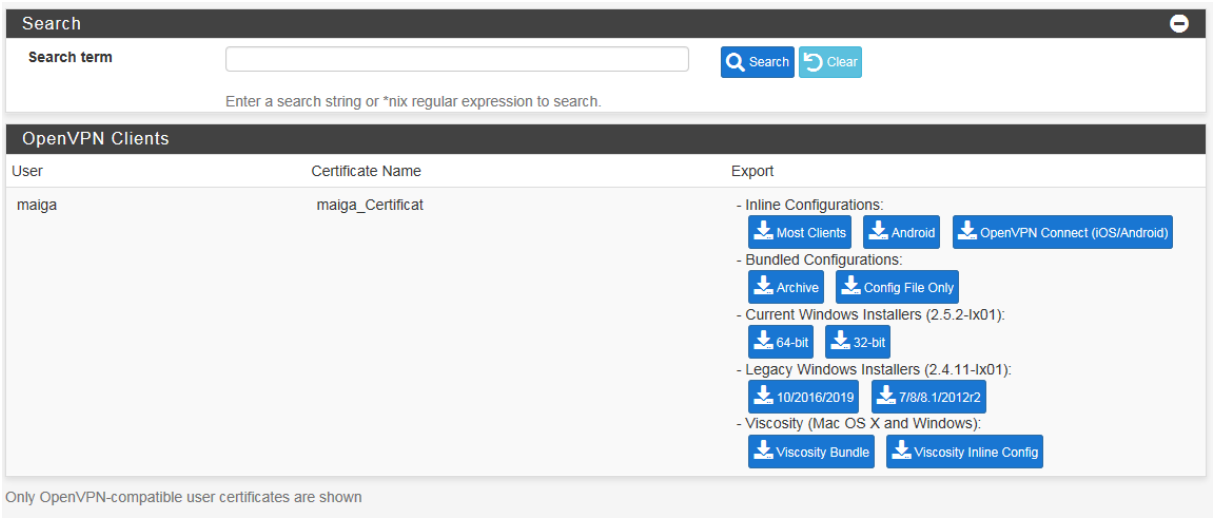

Figure 4.41 - Liens de téléchargement du package.

4.6.4.4 Installation du client OpenVPN

Dans la colonne « Export », on clique sur le bouton « 10/2016/2019 » pour télécharger le client OpenVPN totalement préconfiguré.

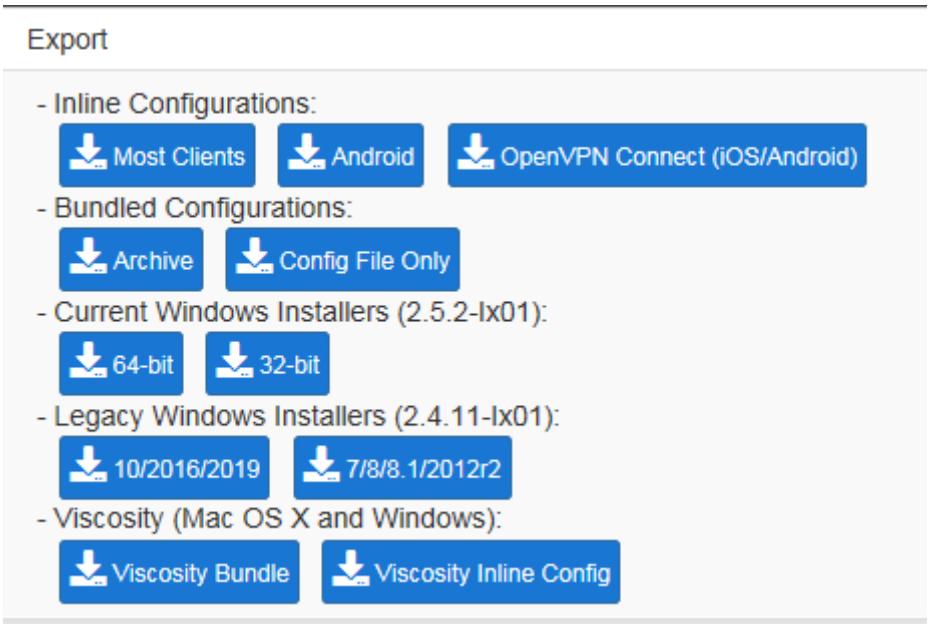

Figure 4.42 - Liens de téléchargement du package.

Déplaçons ce fichier d'installation sur notre machine Windows 10 via clé USB.

Figure 4.43 - Fichier d'installation du package.

Une fois le fichier d'installation préconfiguré d'OpenVPN présent sur notre poste client Windows 10, exécutons-le.

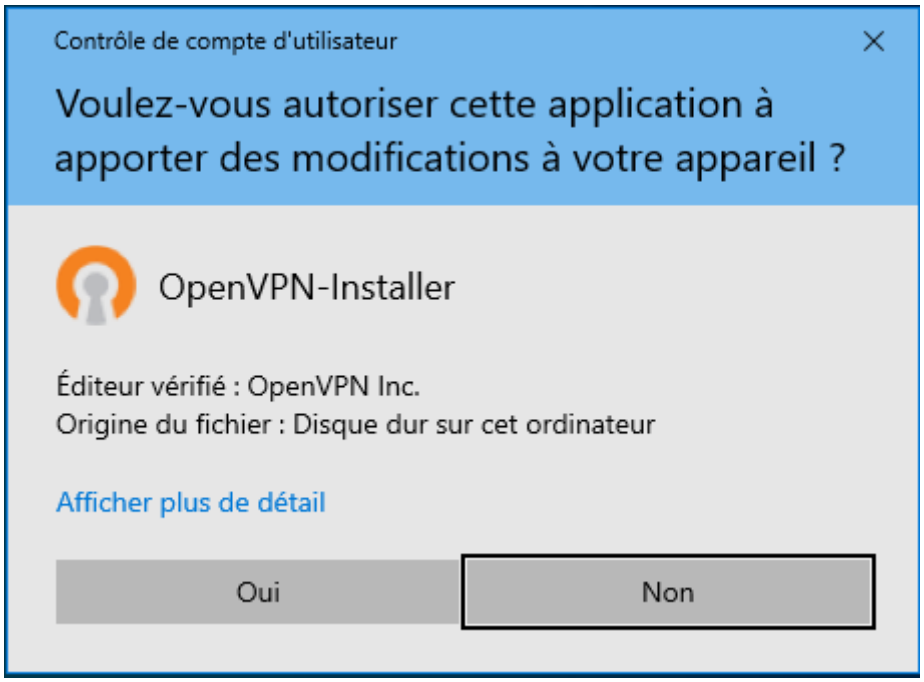

Figure 4.44 - Fichier d'installation du package.

Après l'installation le logiciel OpenVPN sera disponible sur le bureau de notre machine.

Figure 4.45 - Fichier d'installation du package

Nous pouvons maintenant lancer OpenVPN GUI. En faisant un double clic sur l'icône présent sur le bureau pour ouvrir l'application dans la barre des tâches représentée par un petit écran avec un cadenas.

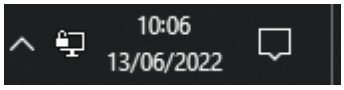

Figure 4.46 - Fichier d'installation du package.

4.7 Tests et évaluation

La partie présente consiste à illustrer les différents tests associés à la mise en place du réseau privé virtuel.

4.7.1 Connexion du client Windows vers le serveur VPN

Afin de s'assurer que la connexion du client Windows vers le serveur VPN s'est effectuée nous suivi les étapes qui se résument à ce qui suit :

4.7.1.1 Lancement du client OpenVPN

Après avoir lancé le client OpenVPN, nous devons fournir le nom d'utilisateur et le mot de passe que nous avons créé dans pfSense en fonction de notre configuration.

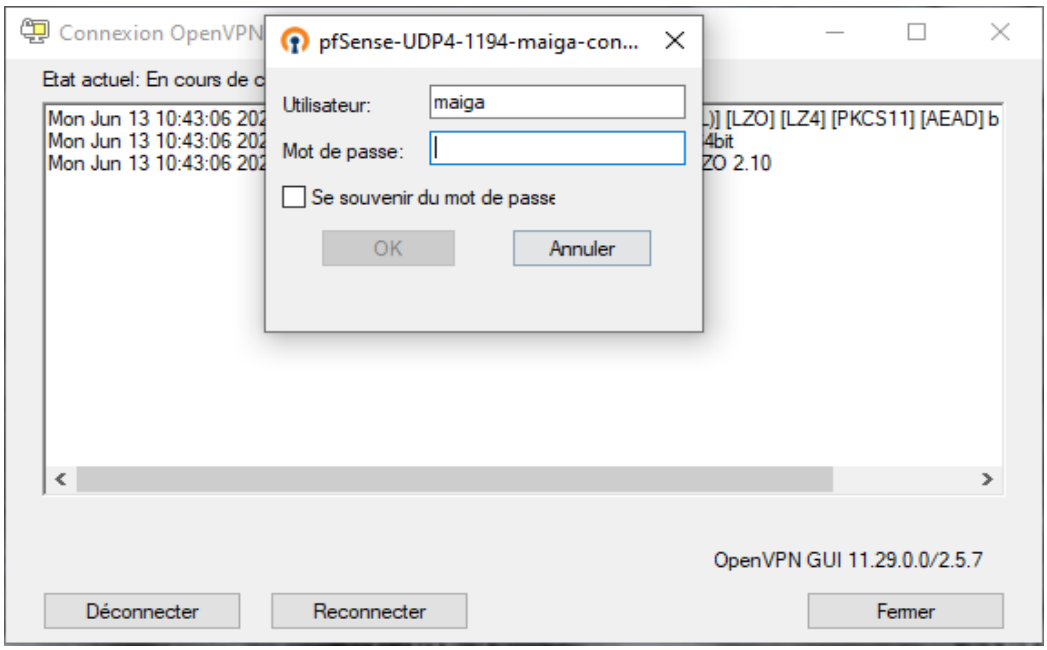

Figure 4.47 - Identification de l'utilisateur.

Après quelques instants, une fenêtre nous informera que nous sommes connectés à travers OpenVPN. Le client pourra désormais se connecter au serveur VPN et une adresse IP du tunnel lui sera assignée.

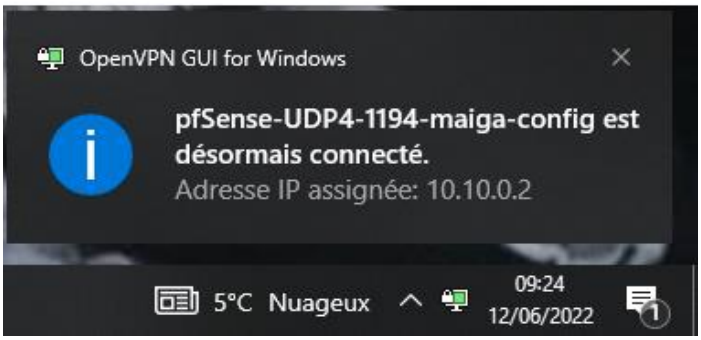

Figure 4.48 - Connexion de l'utilisateur via OpenVPN.

4.7.1.2 Test de la connectivité par la commande Ping

Lorsque nous tapons la commande « ipconfig », nous pouvons voir que notre machine à désormais une adresse sur le réseau VPN.

```
Carte inconnue OpenVPN TAP-Windows6 :

   Suffixe DNS propre à la connexion. . . :
   Adresse IPv6 de liaison locale. . . . .: fe80::6127:c6fa:c965:5c76%11
   Adresse IPv4. . . . . . . . . . . . . .: 10.10.0.2
   Masque de sous-réseau. . . . . . . . . : 255.255.255.0
   Passerelle par défaut. . . . . . . . . :
```

Figure 4.49 - Connexion VPN.

Faisons un ping à destination de l'adresse IP du serveur situé dans le réseau local

```
PS C:\Users\Bakary> ping 172.16.0.11

Envoi d'une requête 'Ping'  172.16.0.11 avec 32 octets de données :
Réponse de 172.16.0.11 : octets=32 temps=5 ms TTL=127
Réponse de 172.16.0.11 : octets=32 temps=5 ms TTL=127
Réponse de 172.16.0.11 : octets=32 temps=7 ms TTL=127
Réponse de 172.16.0.11 : octets=32 temps=5 ms TTL=127

Statistiques Ping pour 172.16.0.11:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 5ms, Maximum = 7ms, Moyenne = 5ms
```

Figure 4.50 - Test de connectivité.

Le ping abouti, la connexion à notre serveur VPN est désormais fonctionnelle depuis notre poste client.

4.7.1.3 Vérification du chemin emprunter vers le réseau local.

Vérifions l'itinéraire vers une destination de l'adresse IP du serveur situé dans le réseau local en lui envoyant des paquets d'écho ICMP (Internet Control Message Protocol).

- Avant la connexion du client au VPN, nous pouvons voir sur la Figure 3.51 les différentes routes ou chemins empruntés à travers internet vers notre réseau.

```
PS C:\Users\Bakary> netsh interface show interface

État admin    État          Type            Nom de l'interface
-------------------------------------------------------------------------
Activé        Déconnecté    Dédié           OpenVPN Wintun
Activé        Déconnecté    Dédié           OpenVPN TAP-Windows6
Activé        Connecté      Dédié           Wi-Fi
Activé        Déconnecté    Dédié           Ethernet

PS C:\Users\Bakary>
```

Figure 4.51 – L'etat de la carte du reseaux virtuelle avant la connexion au VPN.

```
PS C:\Users\Bakary> tracert 172.16.0.11

Détermination de l'itinéraire vers 172.16.0.11 avec un maximum de 30 sauts.

  1     3 ms     3 ms     2 ms  192.168.43.1
  2     *        *        *     Délai d'attente de la demande dépassé.
  3     *      193 ms   124 ms  10.49.61.161
  4     *        *        *     Délai d'attente de la demande dépassé.
  5    34 ms    31 ms    38 ms  10.49.87.42
  6    37 ms    20 ms   118 ms  192.168.156.76
  7    35 ms   113 ms    28 ms  10.44.47.65
  8    85 ms    25 ms    37 ms  10.44.47.50
```

Figure 4.52 - L'itinéraire vers le reseau local avant la connexion au VPN.

- Après le lancement de la connexion, nous remarquons sur la Figure 4.52 qu'il n'y a désormais qu'une seule route, celle du VPN vers notre réseau local donc le poste client est bien connecté à travers le VPN.

```
PS C:\Users\Bakary> netsh interface show interface

État admin    État          Type            Nom de l'interface
-------------------------------------------------------------------------
Activé        Déconnecté    Dédié           OpenVPN Wintun
Activé        Connecté      Dédié           OpenVPN TAP-Windows6
Activé        Connecté      Dédié           Wi-Fi
Activé        Déconnecté    Dédié           Ethernet
```

Figure 4.53 – L'état de la carte du réseau virtuelle après la connexion au VPN

```
PS C:\Users\Bakary> tracert 172.16.0.11

Détermination de l'itinéraire vers TOSHIBA-PC [172.16.0.11]
avec un maximum de 30 sauts :

  1     4 ms     6 ms     3 ms  10.10.0.1
  2     7 ms     5 ms     7 ms  TOSHIBA-PC [172.16.0.11]

Itinéraire déterminé.
```

Figure 4.54 - L'itinéraire vers le reseau local apres la connexion au VPN

4.7.1.4 Capture et analyse de paquet par Wireshark

Pour visualiser le trafic émis vers notre serveur, nous allons capturer les paquets sur le poste client local par Wireshark.

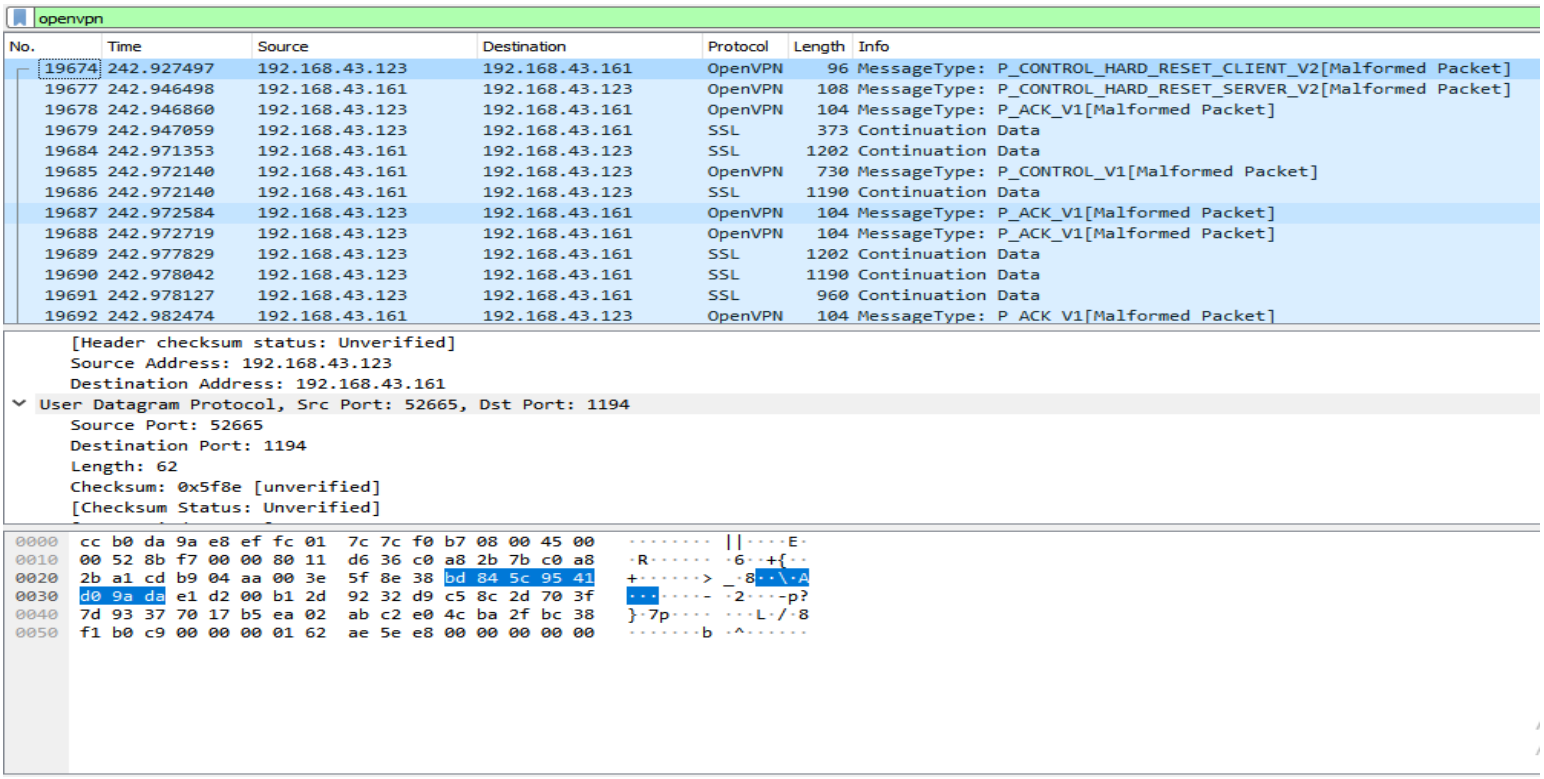

Figure 4.55 - Protocole OpenVPN sur SSL/TLS pour l'authentification et le cryptage.

Sur le volet 1, nous pouvons recenser les différents types de messages utilisés par le Protocol OpenVPN

- **P_CONTROL_HARD_RESET_CLIENT_V1 :** session d'initialisation par le client utilisant la méthode 1 de la clé d'échange TLS
- **P_CONTROL_HARD_RESET_SERVER_V1 :** Réponse à la session d'initialisation utilisant la méthode 1 de la clé d'échange TLS.
- **P_CONTROL_SOFT_RESET_V1 :** Demande de renégociation de la clé.
- **P_CONTROL_V1 :** Paquets échangés pendant la session d'initialisation.
- **P_ACK_V1 :** Accuse de réception d'un paquet de control.
- **P_DATA_V1** : Paquet de donnée.
- **P_CONTROL_HARD_RESET_CLIENT_V :** Session d'initialisation du client utilisant la méthode 2 de clé d'échange TLS.
- **P_CONTROL_HARD_RESET_SERVER_V2 :** réponses à la session d'initialisation utilisant la méthode 2 de la clé d'échange TLS.
- **P_DATA_V2 :** paquet de donne (ajout du champ peer id).

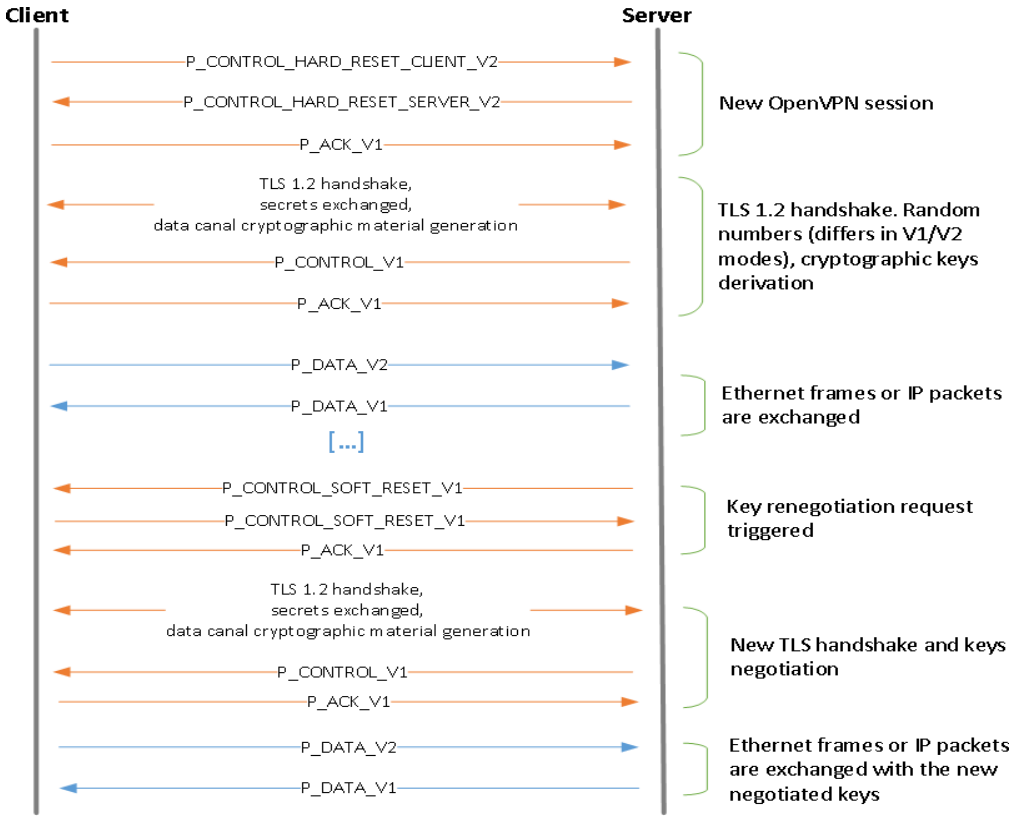

Figure 4.56 – Etablissement de session et renégotiation de clé .

Sur la Figure 3.55, nous constatons que les données du client passent par le réseau du tunnel VPN précédemment créé à l'adresse 10.10.0.0/24 et il est connecté au réseau local comme s'il était dans le même LAN que le serveur

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.0.2	172.16.0.11	ICMP	74	Echo (ping) request id=0x0001, seq=12422/34352, ttl=128 (reply in 2)
2	0.009003	172.16.0.11	10.10.0.2	ICMP	74	Echo (ping) reply id=0x0001, seq=12422/34352, ttl=127 (request in 1)
3	1.006858	10.10.0.2	172.16.0.11	ICMP	74	Echo (ping) request id=0x0001, seq=12423/34608, ttl=128 (reply in 4)
4	1.013397	172.16.0.11	10.10.0.2	ICMP	74	Echo (ping) reply id=0x0001, seq=12423/34608, ttl=127 (request in 3)
5	2.024375	10.10.0.2	172.16.0.11	ICMP	74	Echo (ping) request id=0x0001, seq=12424/34864, ttl=128 (reply in 6)
6	2.029990	172.16.0.11	10.10.0.2	ICMP	74	Echo (ping) reply id=0x0001, seq=12424/34864, ttl=127 (request in 5)
7	3.042975	10.10.0.2	172.16.0.11	ICMP	74	Echo (ping) request id=0x0001, seq=12425/35120, ttl=128 (reply in 8)
8	3.048343	172.16.0.11	10.10.0.2	ICMP	74	Echo (ping) reply id=0x0001, seq=12425/35120, ttl=127 (request in 7)

Figure 4.57 - Transite des echanges au travers du tunnel.

4.8 Propositions de perfectionnement

Nous avions une vision plus large de ce projet mais l'indisponibilité de certains équipements a limité notre travail.

Voici quelques propositions pour l'amélioration de ce projet à l'avenir :

- La machine qui sert de serveur VPN peut être remplacée par un mini-ordinateur à plusieurs cartes réseaux (au moins deux cartes réseaux l'une pour le LAN et l'autre le WAN) avec un processeur de dernière génération, une ram et un disque dur plus puissant.
- Utilisation d'un Modem/Routeur qui sera connecté à l'interface WAN de la machine servant de serveur pour faire le NAT Forwarding enfin qu'un utilisateur puisse avoir accès à travers le réseau privé virtuel, au réseau local depuis l'extérieur ou qu'il soit dans le monde.
- Nous pouvons ajouter un switch à notre architecture qui va relier l'interface LAN de la machine hébergeant le serveur et les machines du réseau local s'il en existe plusieurs.

4.9 Conclusion

Afin de s'assurer que la connexion du client Windows vers le serveur VPN s'est effectuée, nous avons, dans un premier temps, installé un client OpenVPN sur notre machine cliente sous Windows. Ensuite, nous avons effectué divers tests d'accessibilité de notre poste client vers le serveur à travers un réseau VPN en utilisant la commande « Ping » puis, nous avons vérifié par la commande Tracert (Trace Route) le chemin emprunté par le paquet pour arriver à notre réseau local afin de s'assurer qu'il s'agissait bien de celui du VPN. Et enfin nous

avons utilisé Wireshark pour capturer et analyser les paquets afin de vérifier le fonctionnement de notre réseau et les protocoles utilisés.

Conclusion Générale

La mise en place d'un réseau privé virtuel (VPN), dans le cadre de notre projet de fin d'étude nous a permis d'apprendre beaucoup d'informations concernant ces réseaux et les protocoles courants qu'ils utilisent d'où l'importance de la sécurité.

Nous avons, d'abord, consacré un chapitre sur les réseaux privés virtuel pour voir les différents types de VPN, leurs principes de fonctionnement et les protocoles utilisés. Nous avons ainsi constaté qu'OpenVPN est l'un des meilleurs protocoles de tunneling basé sur SSL /TLS pour l'authentification et le cryptage utilisé dans la mise en œuvre de réseaux privés virtuels. Par la suite, nous avons remarqué qu'il offre la combinaison parfaite de sécurité, de vitesse et de compatibilité multiplateforme.

En plus, nous avons mis en œuvre un réseau privé virtuel SSL client-to-site sous pfSense via OpenVPN a l'aide de 3 machines pour permettre à un poste client sur une machine sous Windows 10 d'accéder à distance à notre réseau local.

Afin de voir la faisabilité de ce travail, nous avons fait une réalisation pratique avec les 3 machines afin de vérifier le bon fonctionnement puis, nous sommes passés aux tests d'accessibilité, les captures et les analyses des paquets par Wireshark.

Ce travail a été enrichissant pour nous, car nous avons appris de nouveaux protocoles de sécurité réseau, rencontré un nouveau pare-feu (pfSense). Nous avons donc vécu de nouvelles expériences.

Par ailleurs, nous avons essayé de trouver des solutions aux problèmes auxquels nous avons été confrontés, d'où le déploiement des différentes connaissances acquises au cours de nos années d'études en réseau informatique à l'université.

Aussi, nous avons toujours vu des services offrant des VPN sur internet comme (ExpressVPN, PureVPN) mais, grâce à ce projet, nous avons eu l'opportunité de comprendre le mécanisme de base de ces réseaux, puis nous sommes passés à sa réalisation en utilisant les machines disponibles et nos propres moyens.

Cependant, nous avons rencontré des difficultés pour trouver des machines et aussi au moment de relier les cartes réseaux de ces dernières pour qu'elles communiquent car nous n'avions jamais tenter une telle expérience auparavant.

Enfin, nous souhaitons que ce travail soit un début pour de futurs projets et réalisations. Cette œuvre n'est pas complète et c'est pour cette raison que nous avons fait des propositions d'amélioration dans le dernier chapitre pour ceux qui auront plus d'opportunités que nous par rapport à la disponibilité des équipements et qui souhaiteraient continuer ce que nous avons commencé.

6. Références Bibliographiques

[1]	P.Jean-François, «Tout sur les Réseaux et Internet», Ed. DUNOD, 2015.
[2]	P.Jean-François, «Initiation aux réseaux», 2007, https://web.maths.unsw.edu.au/~lafaye/CCM/initiation/concept.htm, (consulté 08/03/2022).
[3]	P.Jean-François, «Equipements réseau», 2007, https://web.maths.unsw.edu.au/~lafaye/CCM/lan/concentrateurs.htm, (consulté 08/03/2022).
[4]	P.Jean-François, «Fonctionnement d'Internet», 2007, https://web.maths.unsw.edu.au/~lafaye/CCM/internet/tcpip.htm, (consulté 08/03/2022).
[5]	P.Jean-François, «Sécurité informatique», 2007, https://web.maths.unsw.edu.au/~lafaye/CCM/secu/secuintro.htm, (consulté 08/03/2022).
[6]	B.Laurent, W.Christophe, «Sécurité informatique», Ed. EYROLLES, 2005.
[7]	P.Jean-François, B.Jean-Phillipe, «Tout sur la Sécurité informatique», Ed. DUNOD, 2005.
[8]	https://wikimonde.com. (consulté 05/06/2022).
[9]	X.Lasserre,T.Klein, and all, «Réseaux privés Virtuels VPN», 2004,2007, http://www.frameip.com/vpn, (consulté 05/06/2022).