REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEURE ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE MOULOUD MAMMERI DE TIZI OUZOU

FACULTE DU GENIE ELECTRIQUE ET INFORMATIQUE

DEPARTEMENT ELECTRONIQUE

En vue de l'obtention du diplôme de Master
Filière : Electronique
Option : réseaux et télécommunication

THEME

Etude et mise en place d'un réseau VPN

Réalisé par :

Rahmani Tinhinan

Sadaoui Fadhila

Mémoire dirigé par :

M^{me} Lehdir Leila

Devant le jury composé de :

Président : Mr Allouache Djamal	maitre de conférence classe B
Promotrice : M^{me} Lehdir Leila	maitre de conférence classe
Examinateur : Mr Hameg Slimane	maitre de conférence classe B

PROMOTION 2016/2017

Dédicaces

On dédie ce modeste travail à :

Nos très chers parents à qui nous devons tout, nous profitons l'occasion de les remercier pour leurs encouragements, leurs aides, le soutien qu'ils nous ont porté et le sacrifice qu'ils ont fait pour nous, que Dieu les protège et les entoure de sa bénédiction.

Nos frères et sœurs et toute la famille.

Tous nos ami(e)s ainsi qu'à tous ceux qui nous sont chers.

Et à toute personne nous ayant fait part de son savoir.

Fadhila & Tinhinan

Sommaire

SOMMAIRE

SOMMAIRE

ACL : Access Control List

ATM : Asynchronous Transfer Mode

ARP : Address Resolution Protocol

BSD : Berkeley Software Distribution

CPA : Code Parasite Autopropageale

DDP : Disc Description Protocol

DECnet : Digital Equipment Coorporation

DHCP : Dynamic host configuration

DNS : Domaine Name System

EAP : Extensibl Authentication Protocol

FDDI : Fiber Distributed Data Interface

FTP : File Transfer Protocol

http : HyperText Transfer Protocol

https : HyperText Transfer Protocol secure

HOB : Host Unit Broadest

IANA : Internet Assigned Numbers Agency

ICANN : Internet Copporation Assidned Names and Number

IKE : Internet Key Exchange

ISAKMP : Internet Security Association Key Management Protocol

IPsec : Internet Protocol Security

IPX : Internetwork Packet Exchange

IP : Internet Protocol

ICMP : Internet Control Message Protocol

LAN : Local Area Network

L2F : Layer Two Forwording

L2TP : Layer Tow Tunneling Protocol

MAN : Metropolitain Area Network

MAU : Multistaion Access Unit

NAT : Network Address Translation

NNTP : Network News Transfert Protocol

OSI : Open System Interconnection

PAN : Personal Area Network

PPP : Point to Point Protocol

PPTP : Point to Point Tunneling Protocol

PSTN : Public Switched Telephone Network

PPPOE : Point to Point Protocol Over Ethernet

RAID : Redundant Array of Independent Disks

SSL : Secure Sochet Layer

STP : Shielded Twisted-Pair

UDP : User Datagram Protocol

UTP : UnShielded Twisted-Pair

VLAN : Vertual Local Area Network

VPN : Vertual Private Network

WAN : Wide Area Network

Introduction générale

De nos jours, la communication est un outil indispensable pour toute entreprise. A l'origine, la communication était facile du fait qu'une société était composée d'une seule entité ou de plusieurs entités géographiquement proches. Le problème et le besoins sont apparus lorsque celles ci ont commencé à s'implanter sur plusieurs sites, tout autour d'un pays ou même à l'étranger. Un commercial ne peut donc pas accéder aux informations de son entreprise s'il est en déplacement à l'autre bout du monde ou non connecté au réseau de l'entreprise.

Pour une interconnexion sécurisée entre les sites distants d'une même entreprise partageant les mêmes ressources ou avec des partenaires, on fait recours à des lignes spécialisées (LS), cette solution bien qu'elle est efficace présente des contraintes de point de vue cout de réalisation, de maintenance en cas de problème sur les câbles... Lorsque ce raccordement va se faire à l'échelle d'un pays voire d'un continent, il faut penser à une solution plus souple tout en minimisant le cout, Pour remédier à ce problème, la technologie VPN (Virtual Private Network) a été mise en place afin de permettre à un utilisateur n'étant pas connecté à un réseau interne de pouvoir quand même y accéder en totalité ou en partie au travers d'un réseau public (Internet).
Le principe du VPN est relativement simple, il a pour but de créer au travers d'un réseau public un tunnel crypté permettant de faire transiter des données jusqu'à un réseau privée disposant d'une connexion internet.

L'objectif principal de ce projet est basé sur la mise en place d'un réseau VPN en utilisant le VMware à fin de permettre un accès à distance vers un réseau LAN.
A fin de présenter notre travail, nous avons structuré notre mémoire comme suit :
Dans le premier chapitre nous allons donner une présentation générale sur les réseaux
Pour nous initier ensuite à la sécurité réseau et aux VPN dans le second chapitre, tant dis que le troisième c chapitre se portera sur la mise en place du réseau VPN , et en fin, nous terminerons par une conclusion.

I.1. Introduction

En reliant toutes les stations de travail, les périphériques , les terminaux et les autres unités de contrôle du trafic, le réseau informatique a permis aux entreprises de partager efficacement différents éléments(des fichiers, des imprimantes…) et de communiquer entre elles, notamment par courrier électronique et par messagerie instantanée. Il a permis aussi de relier les serveurs de données, de communication et de fichiers.

I.2. Définition d'un réseau

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

I.3. Intérêts d'un réseau.

Un réseau informatique peut servir à plusieurs buts distincts :

- Le partage de ressources (fichiers, applications ou matériels).
- La communication entre personnes (courrier électronique, discussion en direct..)
- La communication entre processus (entre des machines industrielles par exemple).
- La garantie de l'unicité de l'information (bases de données).
- Le jeu vidéo multi-joueurs.

Les réseaux permettent aussi de standardiser les applications, on parle généralement de groupware. Par exemple, la messagerie électronique et les agendas de groupe qui permettent de communiquer plus efficacement et plus rapidement.

Voici les avantages qu'offrent de tels systèmes :

- Diminution des couts grâce aux partages de données et de périphériques.
- Standardisation des applications.
- Accès aux données en temps utile.
- Communication et organisation plus efficace.

I.4. Topologie d'un réseau

L'arrangement physique, c'est-à-dire la configuration spatiale du réseau est appelé **topologie physique**. On distingue généralement les topologies suivantes :

- La topologie en bus
- La topologie en étoile
- La topologie en anneau
- La topologie en arbre

- la topologie maillée.

La topologie logique : par opposition à la topologie physique, représente la façon dont les données transitent sur les lignes de communication. Les topologies logiques les plus courantes sont Ethernet, Token Ring et FDDI.

I.4.A. Topologie physique

A.1. Topologie en bus

Dans une topologie en bus les ordinateurs sont reliés à une même ligne de transmission, Chaque PC est connecté par l'intermédiaire d'un connecteur BNC.

Cette topologie a pour avantage d'être facile à mettre en œuvre et de posséder un fonctionnement simple. En revanche, elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuse, l'ensemble du réseau est affecté.

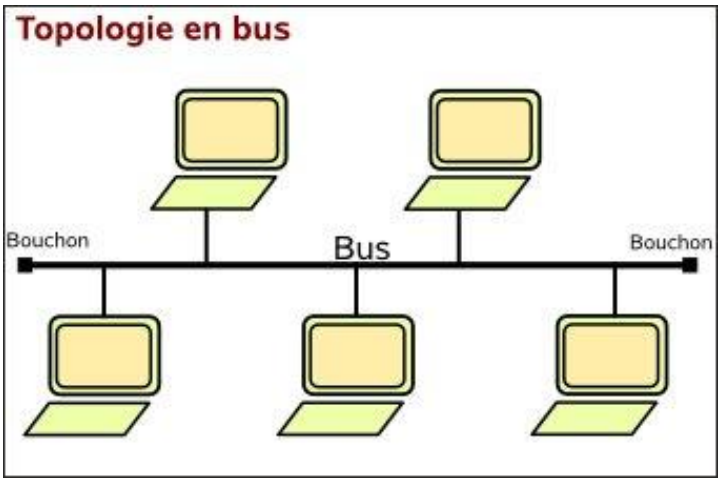


Figure I.1. Topologie en bus

A.2. Topologie en étoile

Dans une topologie en étoile, les ordinateurs du réseau sont reliés à un système matériel central appelé concentrateur (hub).

Contrairement aux réseaux construits sur une topologie en bus, les réseaux avec une topologie en étoile sont beaucoup moins vulnérables car une des connexions peu être débranchée sans paralyser le reste du réseau.

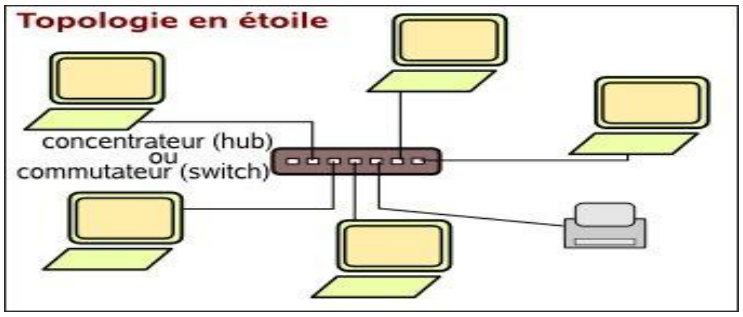


Figure II.2. Topologie en étoile

A.3. Topologie en anneau

La topologie en anneau se caractérise par une connexion circulaire de la ligne de communication.

Les informations circulent de stations en stations, en suivant l'anneau, donc dans un seul sens. Un jeton circule en boucle et permet à chaque station de prendre la parole à son tour. La station qui a le jeton émet des données qui font le tour de l'anneau. Lorsque les données reviennent, la station qui les a envoyées les élimine du réseau et passe le "droit d'émettre" à son voisin, et ainsi de suite.

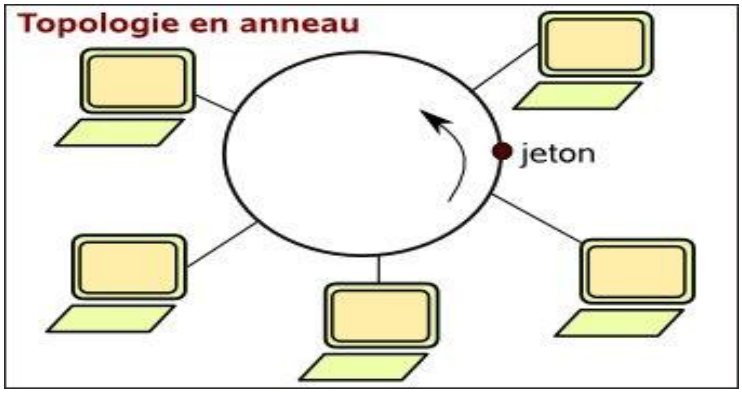


Figure I.3. Topologie en anneau

.

A.4. Topologie en arbre

Aussi connue sous le nom de *topologie hiérarchique*, le réseau est divisé en niveaux. Le sommet, le haut niveau, est connectée à plusieurs nœuds de niveau inférieur, dans la hiérarchie. Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur. Le tout dessine alors un arbre, ou une arborescence.

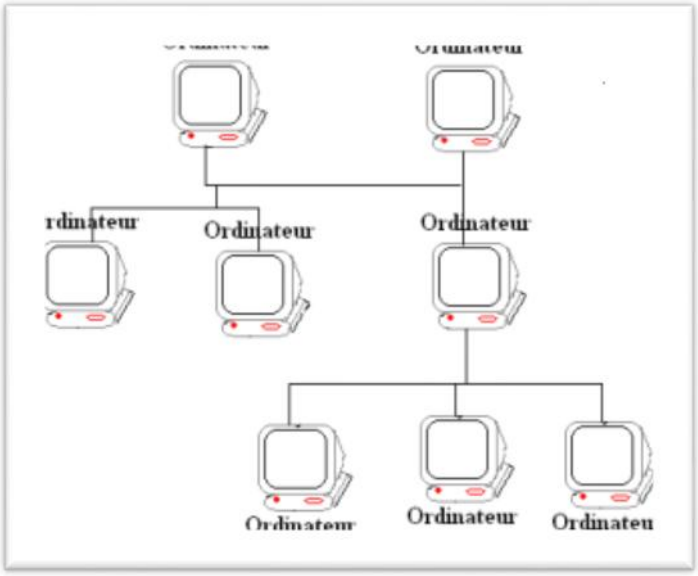


Figure I.4. Topologie en arbre

A.5. Topologie maillée

La topologie maillée est une topologie hybride de type étoile mais avec différents chemins pour accéder d'un nœud à un autre. C'est la méthode utilisée sur Internet: pour un transfert entre deux points, chaque nœud (un routeur intelligent, qu'on appelle Switch dans le jargon technique) va sélectionner en temps réel la route la plus rapide pour le transfert.

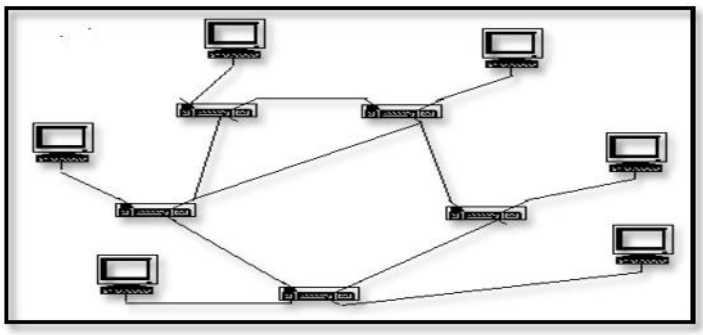


Figure I.5. Topologie maillée

Le principal avantage de ce type de topologie est l'adaptabilité: une ligne coupée ne perturbe pas les communications d'où son utilisation dans les réseaux sensibles.

I.4.B. Topologies logiques

B.1. Topologie Ethernet

Ethernet est aujourd'hui l'un des réseaux les plus utilisés en local. Il repose sur une topologie physique de type bus linéaire, c'est-à-dire tous les ordinateurs sont reliés à un seul

support de transmission. Dans un réseau Ethernet, la communication se fait à l'aide d'un protocole appelé CSMA/CD (Carrier Sense Multiple Access with Collision Detect), ce qui fait qu'il aura une très grande surveillance des données à transmettre pour éviter toute sorte de collision. Par conséquent un poste qui veut émettre doit vérifier si le canal est libre avant d'y émettre.

B.2. Le Token Ring

Il utilise la méthode d'accès par jeton (token). Dans cette technologie, seul le poste ayant le jeton a le droit de transmettre. Si un poste veut émettre, il doit attendre jusqu'à ce qu'il ait le jeton. Dans un réseau Token ring, chaque nœud du réseau comprend un MAU (Multi station Access Unit) qui peut recevoir les connexions des postes. Le signal qui circule est régénéré par chaque MAU.

B.3. Le FDDI(Fiber Distributed Data Interface)

La technologie LAN FDDI (Fiber Distributed Data Interface) est une technologie d'accès réseau utilisant des câbles fibres optiques. Le FDDI est constitué de deux anneaux : un anneau primaire et anneau secondaire. L'anneau secondaire sert à rattraper les erreurs de l'anneau primaire. Le FDDI utilise un anneau à jeton qui sert à détecter et à corriger les erreurs. Ce qui fait que si une station MAU tombe en panne, le réseau continuera de fonctionner.

B.4. L'ATM (Asynchronous Transfer Mode)

L'ATM (Asynchronous Transfer Mode, c'est-à-dire mode de transfert asynchrone) est une technologie très récente qu'Ethernet, Token Ring et FDDI. Il s'agit d'un protocole de niveau 2, qui a pour objectif de segmenter les données en cellules de taille unique. L'en-tête de chaque cellule comprend des informations qui permettent à la cellule d'emprunter son chemin. Les cellules ATM sont envoyées de manière asynchrone, en fonction des données à transmettre, mais sont insérées dans le flux de donnée synchrone d'un protocole de niveau inferieur pour leur transport.

Avec le réseau ATM, deux technologies existent pour le moment :

- La commutation des paquets
- La commutation des circuits

I.5. Architectures réseaux

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

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

I.6. Types de réseaux

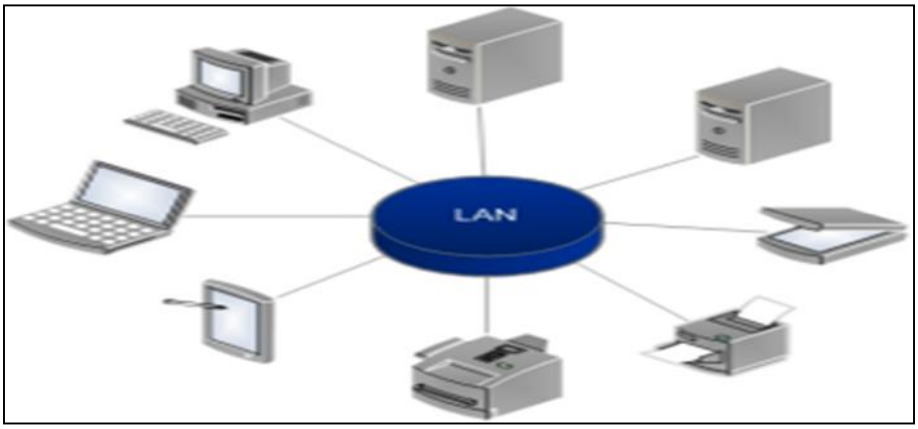
On distingue différents types de réseaux selon leur taille (en termes de nombre de machines), leur vitesse de transfert des données ainsi que leur étendue. On définit généralement les catégories de réseaux suivantes :

- **Réseaux personnels** ou PAN (Personal Area Network).
- **Réseaux locaux** ou LAN (Local Area Network).
- **Réseaux métropolitains** ou MAN (Metropolitain Area Network).
- **Réseaux étendus** ou WAN (Wide Area Network).

I.6.1. Réseaux locaux (LAN)

Un réseau local (LAN, local area network) désigne un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau à l'aide d'une même technologie (Ethernet ou WIFI).

Un réseau local est donc un réseau sous sa forme la plus simple. La vitesse de transfert de données d'un réseau local peut s'échelonner entre 10Mbps (pour un réseau Ethernet standard) à 1 Gbps (gigabit Ethernet par exemple). La taille d'un réseau local peu atteindre jusqu'à 100 voire 1000 machines.



Figue I.6. LAN

I.6.2. Réseau métropolitain (MAN)

Un réseau métropolitain (MAN, Metropolitain Area Network) interconnecte plusieurs réseaux locaux géographiquement proches (au maximum quelques dizaines de kilomètres)

avec un débit important. Ainsi, un réseau métropolitain permet à deux machines distantes de communiquer comme si elles faisaient parties d'un même réseau local.

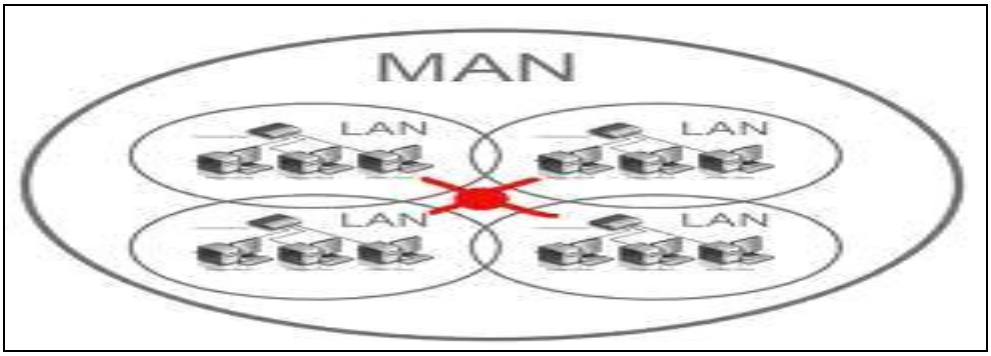


Figure I.7: Réseau MAN

Un MAN est formé d'équipements réseau interconnectés par des liens hauts débits (en général en fibre optique).

I.6.3. Réseaux étendus (WAN)

Un réseau étendu (WAN, Wide Area Network) interconnecte plusieurs réseaux locaux à travers de grandes distances géographiques.

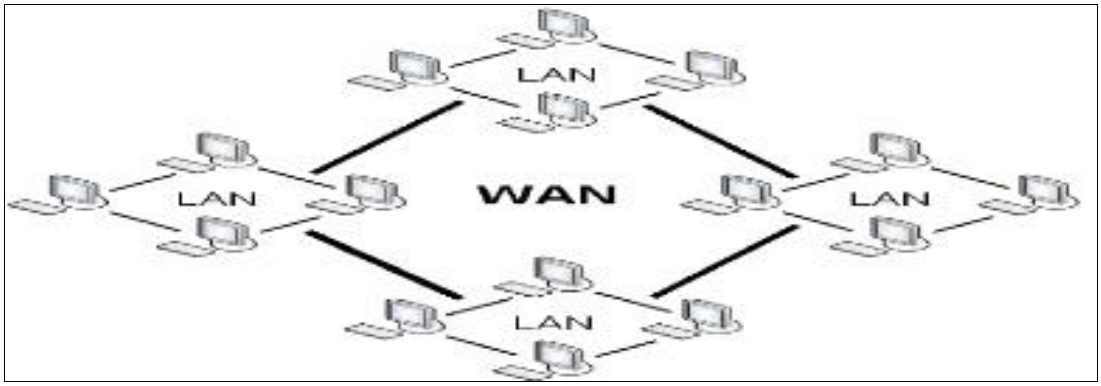


Figure I.8: Réseau WAN

Les WAN fonctionnent grâce à des équipements réseau appelés routeurs, qui permettent de déterminer le trajet le plus approprié pour atteindre une machine du réseau.

I.7. Supports de transmission

Pour relier les diverses entités d'un réseau, plusieurs supports physiques de transmission de données peuvent être utilisés. Une de ses possibilités est l'utilisation de câbles.

Il existe de nombreux types de câbles, mais on distingue généralement :

- Le câble de type coaxial.

- Le câble de type pair torsadé.
- La fibre optique.

En plus des liaisons physiques, actuellement il y'a des réseaux qui utilisent la liaison sans fil comme support de transmission.

I.7.1. Le Câble coaxial

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

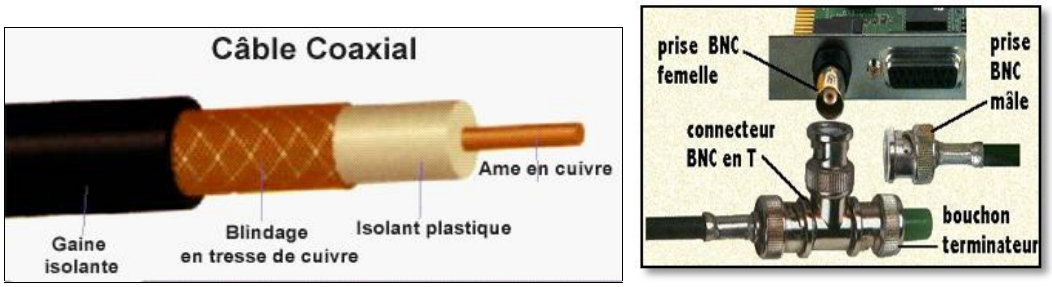


Figure I.9. Câble coaxial et le connecteur BNC

La capacité de transmission d'un câble coaxial dépend de sa longueur et les caractéristiques physiques des conducteurs et l'isolant.
Il existe deux grands types de câbles coaxiaux :

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

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

I.7.2. La paire torsadée :

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

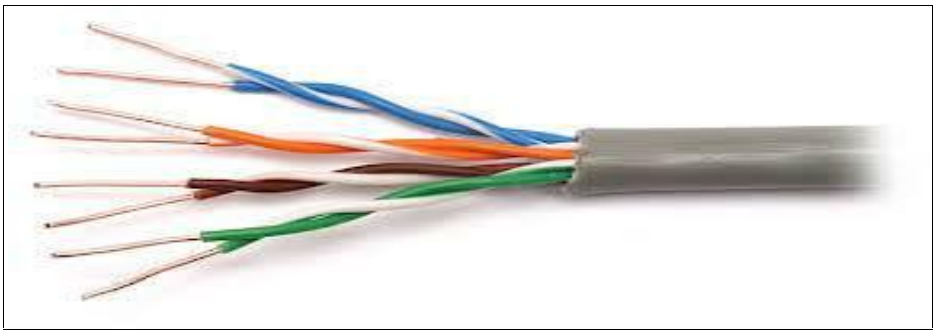


Figure I.10.Câble a paire torsadées

L'entrelacement permet de supprimer les bruits (interférences électriques) dus aux paires adjacentes ou aux autres sources (moteur, relais, transformateur…)

On réseau informatique.

.on distingue plusieurs types de câbles à paires torsadées, UTP et STP sont les plus utilisées et les plus répondu pour les réseaux locaux.

.I.7.2.A. La paire torsadée non blindées (UTP) :

Les caractéristiques de UTP :

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

I.6.2.B. La paire torsadée blindée (STP) :

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

Les caractéristiques de ce câble :

- Les fils du cuivre d'une paire sont eux même torsadée ce qui fournit un excellent blindage pour le STP.
- Il permet une transmission plus rapide et sur une longue distance.

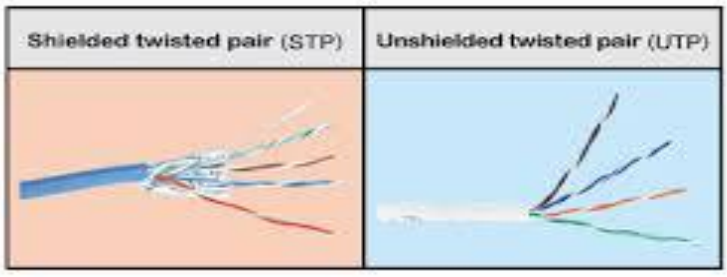


Figure I.11 : Câble UTP et STP

Les connecteurs pour paire torsadé :

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

I.7.3. La fibre optique :

Le support de transmission le plus récent et apprécié. Il permet de transmettre des données sous forme d'impulsions lumineuses avec un débit supérieur à celui des autres supports filaires.

La fibre optique et constitué d'un cœur, d'une gaine optique, et d'une enveloppe protectrice comme présentée par la figure suivante

Figure 1.12: Fibre optique

Caractéristiques de la fibre optique

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

On distingue deux types de fibre optique :

- **Les fibres multi modes** : ou le cœur de la fibre est très volumineux ce qui permet la propagation de plusieurs modes (trajets) simultanément. Il existe deus sortes de MMF ; une à saut d'indice et l'autre à gradient d'indice.
- **Les fibres monomodes** : SMF (single mode fiber) avec un cœur fin et ne peut transporter le signal que sur un seul trajet, elle permet de transporter le signal à une distance plus longue (50 fois) que celle de la multi mode.

I.7.4. Les ondes radio :

Les ondes radio sont des supports sans fil utilisées avec des réseaux de toutes tailles .elle servent à relier des ordinateurs distants dans une zone géographique étendue.

- Ces ondes peuvent atteindre une vitesse de transmission de 11Mbits/s
- Les liaisons radio sont utilisées pour à permettre plusieurs réseaux de communiquer ensemble sans avoir à passer par un câble
- Les ondes radio utilisent des fréquences radio pour l'émission**.**

I.8. Les différents dispositifs de la connectivité

I.8.1. Les répéteurs :

Un répéteur est un équipement simple permettant de régénérer 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.

D'autre part, un répéteur peut permettre de constituer une interface entre deux supports physiques de types différents, c'est-à-dire qu'il peut par exemple permettre de relier un segment de paire torsadée à un brin de fibre optique

Figure I.9: Répéteur

I.8.2. Hub (Host Unit Broadest) :

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

Le hub permet de connecter plusieurs machines entre elles, parfois disposées en étoile, ce qui lui vaut le nom de Hub, pour illustrer le fait qu'il s'agit du point de passage des communications des différentes machines.

Figure I.14: Hub

I.7.3. Switch

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

Figure I.15: Switch

I.8.4. Les ponts

Un pont est un dispositif matériel permettant de relier des réseaux travaillant avec le même protocole. Il fonctionne sur la couche liaison de données du model OSI, il est capable de filtrer les trames en ne laissant passer que celles dont l'adresse correspond à une machine située à l'opposé du pont.

Ainsi, le pont permet de segmenter un réseau en conservant au niveau du réseau local les trames destinées au niveau local et en transmettant les trames destinées aux autres réseaux. Cela permet de réduire le trafic (notamment les collisions) sur chacun des réseaux et d'augmenter le niveau de confidentialité car les informations destinées à un réseau ne peuvent pas être écoutées sur l'autre brin.

I.8.5. Les routeurs

Un routeur est un équipement d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter.

La fonction de routage est notamment utilisée lorsqu'une adresse internet est partagée par plusieurs ordinateurs d'un même réseau.

Figure I.16: Routeur

I.8.6. passerelles

Les passerelles (Gateway) permettent de faire la liaison entre deux réseaux, afin de faire l'interface entre des protocoles réseau différents.

Lorsqu'un utilisateur distant contacte un tel dispositif, ce dernier examine sa requête et, si jamais celle-ci correspond aux règles que l'administrateur réseau a définies, la passerelle crée une liaison entre les deux réseaux. Les informations ne sont donc pas directement transmises, mais traduites afin d'assurer la continuité des deux protocoles.

I.9. Notion de protocole

Un protocole est une méthode standard qui permet la communication entre des processus (s'exécutant éventuellement sur différentes machine), c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau. Il en existe plusieurs selon ce que l'on attend de la communication. Certains protocoles seront par exemple spécialisés dans l'échange de fichiers le (ftp), d'autres pourront servir à gérer simplement l'état de la transmission et des erreurs (c'est le cas du protocole ICMP)…

Sur internet, les protocoles utilisés font partie d'une suite de protocoles, c'est-à-dire un ensemble de protocoles reliés entre eux. Cette suite de protocole s'appelle TCP/IP. Elle contient, entre autres, les protocoles suivants : http, FTP, ARP, ICMP, IP, TCP, UDP, SMTP, Telnet, NNTP.

I.10. Le modèle OSI (Open Systems Interconnection)

La première évolution des réseaux informatiques a été des plus anarchiques, chaque constructeur développant presque sa propre technologie. Pour palier à cela, l'ISO (Organisation Internationale de normalisation) décida de mettre en place un modèle de référence théorique décrivant le fonctionnement des communications réseau Le modèle de référence OSI comporte sept couches numérotées, chacune illustrant une fonction réseau bien précise. Cette répartition des fonctions réseau est appelée organisation en couches.

I.10.1. Les 7 couches du modèle OSI sont les suivantes :

- **Couche 1** : **Couche physique**

  La couche physique définit les spécifications du média (câblage, connecteur, voltage, bande passante…).

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

  La couche liaison de donnée s'occupe de l'envoi de la donnée sur le média. Cette couche est divisée en deux sous-couches :

  La sous-couche MAC (Média Access Control) est chargée du contrôle de l'accès au média. C'est au niveau de cette couche que l'on retrouve les adresses de liaison de donnée (MAC, DLCI).

  La sous-couche LLC (Layer Link Control) s'occupe de la gestion des communications entre les stations et interagit avec la couche réseau.

- **Couche 3** : **Couche réseau**

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

- **Couche 4 : Couche transport**

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

- **Couche 5 : Couche session**

  La couche session établit, gère et ferme les sessions de communications entre les applications.

- **Couche 6 : Couche présentation**

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

- **Couche 7 : Couche application**

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

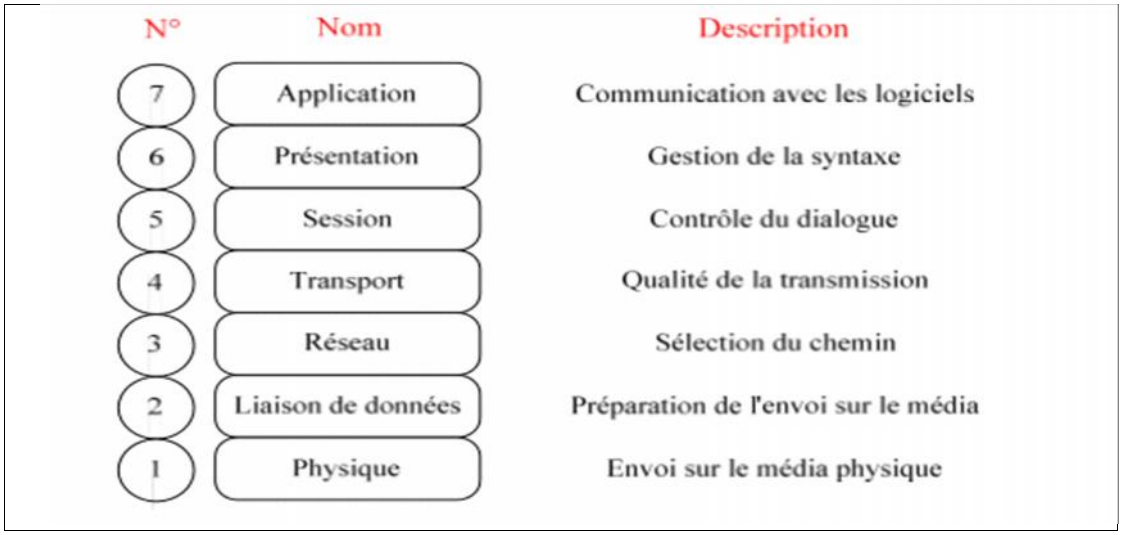


Figure I.17 : Les 7 couches du modèle OSI

I.10.2. Les Avantages du modèle OSI :

Une division de la communication réseau en éléments plus petits et plus simples pour :

- ✓ une meilleure compréhension.
- ✓ L'uniformisation des éléments afin de permettre le développement multi constructeur.
- ✓ La possibilité de modifier un aspect de la communication réseau sans modifier le reste (Exemple : un nouveau média)

Pour communiquer entre les couches et entre les hôtes d'un réseau, OSI a recourt au principe d'encapsulation**.**

- ❖ **Encapsulation** : processus de conditionnement des données consistant à ajouter une en-tête de protocole déterminé avant que les données ne soient transmises à la couche inférieure

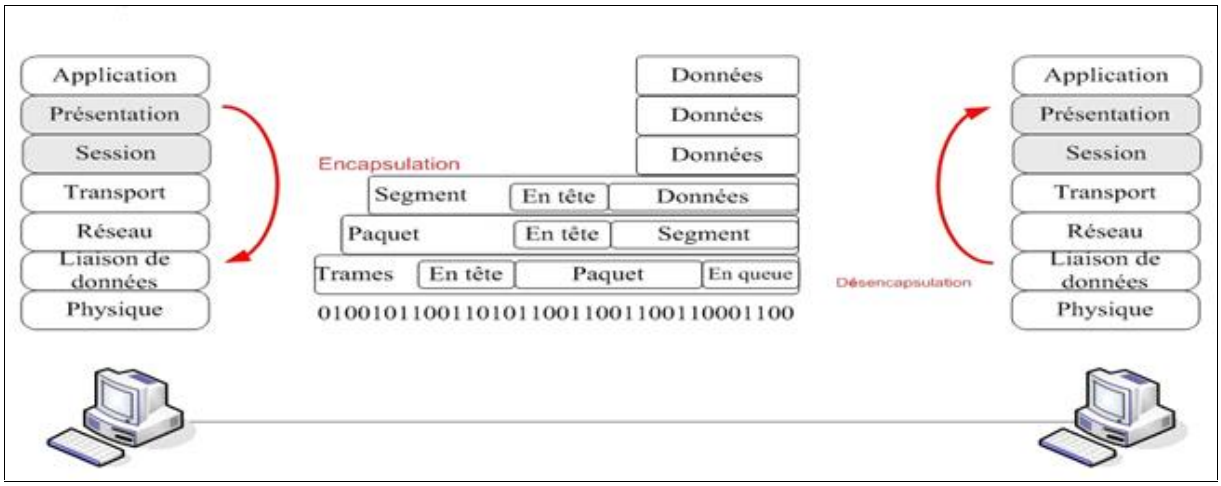


Figure I.18: Principe de l'encapsulation

Lorsque 2 hôtes communiquent, on parle de communication d'égal à égal, c'est-à-dire que la couche N de la source communique avec la couche N du destinataire. Lorsqu'une couche de l'émetteur construit des données, elle encapsule ces dernières avec ses informations puis les passe à la couche inférieure. Le mécanisme inverse a lieu au niveau du destinataire ou une couche réceptionne les données de la couche inférieure, enlève les informations la concernant, puis transmet les informations restantes à la couche supérieure. Les données transitant à la couche N de la source sont donc les mêmes que les données transitant à la couche N du destinataire.

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

Figure I.19 : Identification des données

I.11. Le modèle TCP/IP

I.11.1. Présentation de TCP/IP

TCP/IP est une suite de protocoles. Le sigle TCP/IP signifie «Transmission Control Protocol/InternetProtocol». .

TCP/IP représente d'une certaine façon l'ensemble des règles de communication sur internet et se fonde 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.*

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

- Acheminement des paquets de données sur le réseau.
- Utilisation d'un système d'adressage.
- Contrôle des erreurs de transmission de données.

TCP/IP est un modèle comprenant 4 couches :

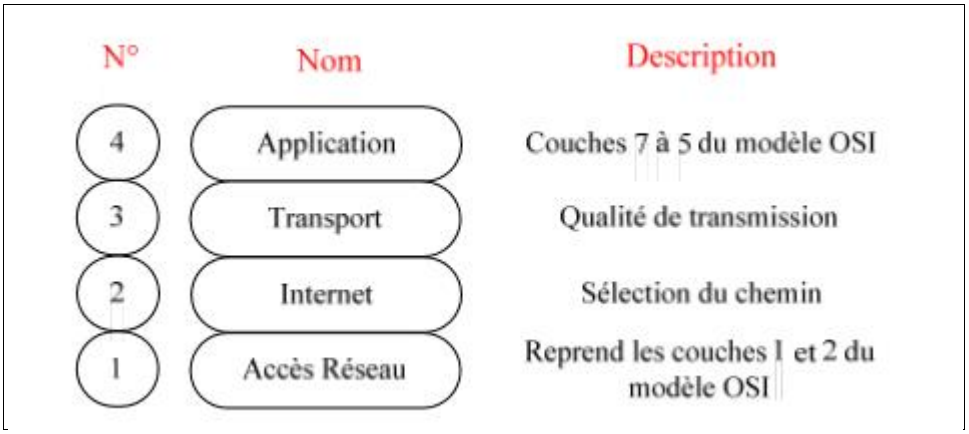


Figure I.20: Les 4 couche TCP/IP

- **Les rôles des différentes couches sont les suivants :**
  - **Couche Accès réseau** : elle spécifie la forme sous laquelle les données doivent être acheminées quelque 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.

I.11.2 Comparaison entre le modèle TCP/IP et le modèle OSI

Ces deux modèles sont très similaires, dans la mesure où les 2 sont des modèles de communication à couche et utilisent l'encapsulation de données.

On remarque cependant deux différences majeures :

• TCP/IP regroupe certaines couches du modèle OSI dans des couches plus générales

• TCP/IP est plus qu'un modèle de conception théorique, c'est sur lui que repose le réseau

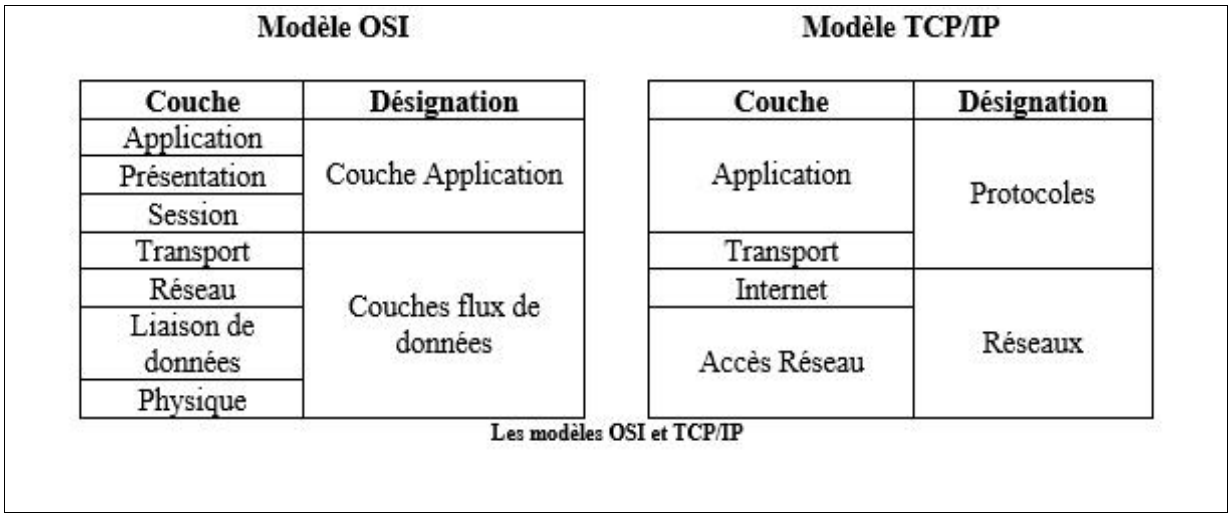


Figure I.21 : Les modèles OSI et TCP/IP

I.12. Protocole UDP (User Datagram Protocol)

UDP est un protocole de transport (couche 4 du modèle OSI) sans connexion qui fonctionne au dessus du protocole de réseau IP (couche 3 du modèle OSI). C'est un protocole simple a mettre en ouvre, cependant il n'est pas fiable (perte de messages, messages non ordonnes, . . .) Les messages qu'envoi UDP son appelés datagrammes.

I.13.Format de l'adresse IP

I.13.1. Notation d'adresse IP

Sur internet, les ordinateurs communiquent entre eux grâce au protocole IP (Internet Protocol), qui utilise des adresses numériques, appelées adresses IP, c'est l'ICANN (Internet Corporation for Assigned Names and Numbers, remplaçant l'IANA, internet
Assigned Numbers Agency, depuis 1998) qui est chargée d'attribuer des adresses IP publiques, c'est-à-dire les adresses IP des ordinateurs directement connectés sur le réseau public internet.

Ces adresses servent aux ordinateurs du réseau pour communiquer entre eux, ainsi chaque ordinateur d'un réseau possède une adresse IP unique sur ce réseau.

Une adresse IP (Internet Protocol) est constituée d'un nombre binaire de 32 bits. Pour faciliter la lecture et la manipulation de cette adresse on la représente plutôt en notation décimale pointée, par exemple :

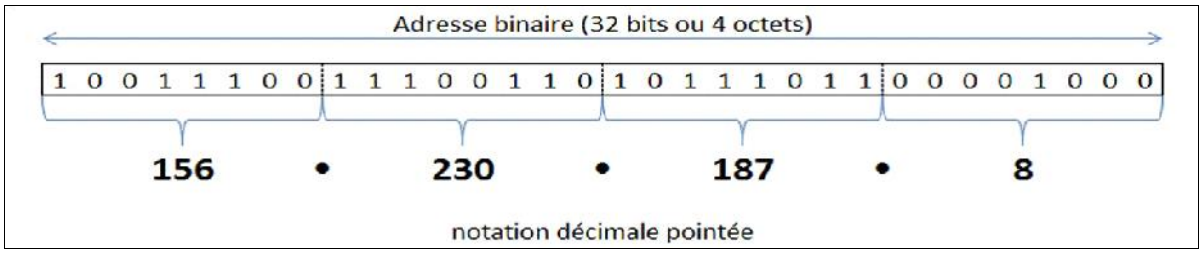


Figure I.22 : adresse IP

I.13.2. Structure

Une adresse IP d'un équipement, codée sur 4 octets, contient à la fois un identifiant réseau (Net ID) et un identifiant équipement (Host ID)

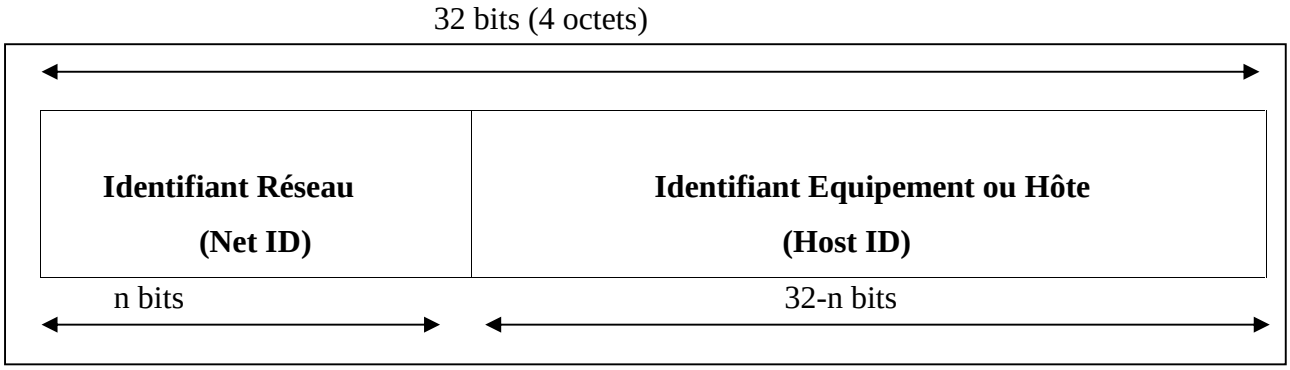


Figure I.23 : Structure d'adresse IP

Dans le cas des réseaux « standards » (sans sous-réseaux) la partie Identifiant Réseau peut être codée sur 1, 2 ou 3 octets. Le nombre de bits restants pour la partie HostID détermine le nombre d'équipements pouvant être connectés sur le réseau.

I.13.3. Classes d'adresses IP

En fonction du nombre d'équipements pouvant être connectés à un réseau, les adresses IP appartiennent à la **classe A, B ou C**.

- **Le format d'une adresse IP selon sa classe est le suivant :**

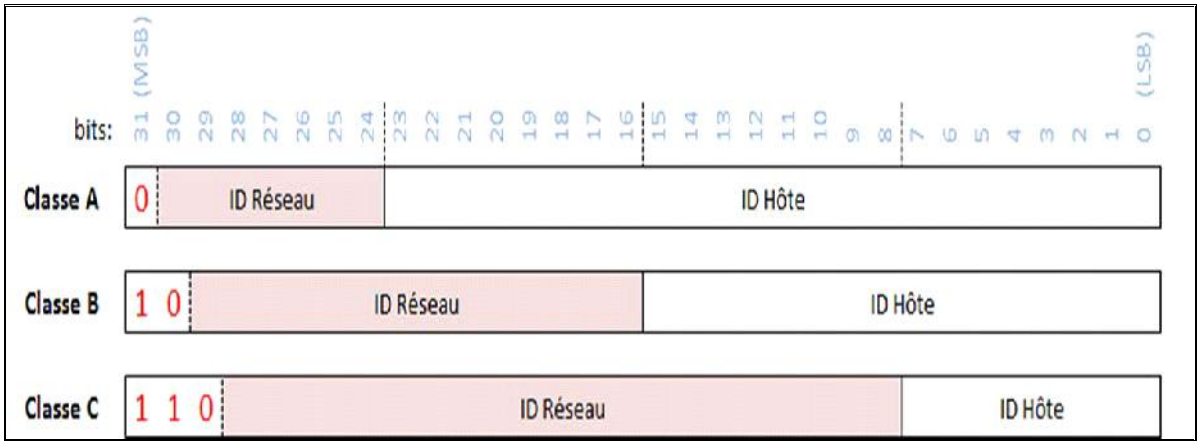


Figure I.24 : Les classes d'adresse IP

L'adresse IP du réseau est une adresse IP avec tous les bits de la partie « ID Hôte » à 0. C'est donc une Adresse réservée et non attribuable à un équipement.

Une autre combinaison est réservée. C'est celle où tous les bits de la partie « ID Hôte » sont à1. Cette adresse est l'adresse de diffusion (broadcaste) et sert à désigner tous les hôtes du réseau.

I.13.4 Masques de sous réseaux

I.13.4.A. Format

Une adresse IP est toujours associée à un « masque de sous-réseau », c'est grâce à celui-ci que l'on peut extraire de l'adresse IP, le numéro de la machine et l'adresse réseau / sous réseau auquel il appartient.

Par défaut, lorsqu'il n'y a pas de sous réseaux, les masques sont :

@ En classe A : 255.0.0.0

@ En classe B : 255.255.0.0

@ En classe C : 255.255.255.0

I.12.4.B. Adresses Public / Adresses Privée

Sont celles qu'il est possible d'utiliser pour une connexion à l'Internet. Elles sont attribuées par l'IANA (Internet Assigned Numbers Authority) auprès de qui il faut s'enregistrer.

Tout ordinateur d'un réseau local voulant se connecter à Internet doit disposer de sa propre adresse IP.

- **Adresse public**

Une adresse IP dite “publique” est une adresse qui est unique au niveau mondial et qui est attribuée à une seule entité. A titre d’exemple l’adresse IP : 198.133.219.25 est celle du constructeur Cisco et que seul Cisco a le droit de l’utiliser.

- **Adresse privée**

Une adresse IP dite “privée” est une adresse qui n’est pas unique au niveau mondial et donc qui peut être attribuée à plusieurs entités en même temps. La restriction pour que cela soit autorisé est qu’une adresse IP privée ne peut pas sortir vers l’extérieur ou plus simplement ne peut pas sortir sur Internet.

Classe d’adresses privées	**Plage d’adresses privées**
Réseau privé de classe A	De 10.0.0.1 à 10.255.255.254
Réseau privé de classe B	De 172.16.0.1 à 172.31.255.254
Réseau privé de classe C	De 192.168.0.1 à 192.168.255.254

Tableau I.1: Classe et plage des adresses privée

Conclusion

L’utilisation des réseaux d’ordinateurs partagent des serveurs(apporte une grande souplesse). Les réseaux permettent l’accès à de très nombreuses ressources et c’est pour cela qu’on observe une augmentation de la demande sur l’utilisation des réseaux. Par conséquent, les risques augmentent.

II.1. Introduction

De nos jours, l'utilisation de l'internet n'est plus sur. Souvent les transmissions de données ainsi que les sites web ne sont pas protégés et sont vulnérables aux attaques des cybers criminels. La sécurité d'un réseau est un niveau de garantie pour que l'ensemble des machines fonctionnent d'une façon optimale.

Dans ce chapitre, nous allons présenter les attaques les plus fréquentes et les notions de sécurité et en particulier le VPN.

II.2. Les techniques d'attaques

- **Attaque contre la communication**

Est un type d'attaque contre la confidentialité, qui consiste à accéder aux informations transmises ou stockées, l'information n'est pas altérées par celui qui en prélève une copie. Ces attaques sont donc indétectables par le système et peuvent seulement être réparées par des mesures préventives.

- **Interposition**

Ce type consiste à tromper les mécanismes d'authentification pour ce faire passer pour un utilisateur (personne disposant des droits dont on a besoin) pour compromettre la confidentialité, l'intégrité ou la disponibilité (le ip spoofing qui est un vol d'adresse IP).

- **Coupure**

  Est un accès avec modification des informations transmises sur des communications, il s'agit donc d'une attaque contre l'intégrité.

II.3. Les types d'attaques

1) Les attaques logicielles

- **Les virus**

Les Virus informatiques (appelés véritablement « CPA ou Code Parasite Autopropageable » sont des codes qui ont la particularité: de s'auto reproduire, d'infecter (contaminer), d'activer et d'altérer ou même détruire le fonctionnement du système ou de l'information stockée.

- **Les vers**

Un ver est un programme indépendant, qui se copie d'un ordinateur en un autre ordinateur. La différence entre un ver et un virus est que le ver ne peut pas se greffer à un autre programme donc l'infecter.

Il va simplement se copier via un réseau ou internet ,ordinateur en ordinateur .ce type de réplication peut donc non seulement affecter un ordinateur , aussi dégrader les performances du réseau dans une entreprise.

- **Le cheval de Troie**

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

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

- Récupération des mots de passe grâce à keylogger
- Administration illégale à distance d'un ordinateur
- Relais utilisé par les pirates pour effectuer des attaques
- Serveur de spam (envoi en masse des e-mail)
- L'écoute du réseau (sniffing)

  Grâce à un logiciel appelé 'sniffer', il est possible d'intercepter toutes les trames que notre carte reçoit et qui ne nous sont pas destinées.

  Si quelqu'un se connecte par internet par exemple à ce moment la, son mot de passe transitant en clair sur le net .il sera aisé de lire et c'est facile de savoir à tout moment quelles pages web regardent les personnes connectées au réseau.

2) Autres attaques

- **Attaque par déni de service (dos dinial of service)**

Est un type d'attaque visant à rendre indispensable pendant un temps indéterminé les services aux ressources d'une organisation .Il s'agit la plus part de temps d'attaques à l'encontre des serveurs d'une entreprise, afin qu'il ne puisse être utilisés et consultés.

Le principe de ces attaques consiste à envoyer des paquets IP ou des données de grande taille afin de provoquer une saturation ou un état instable des machines victimes et de les empêcher ainsi d'assurer les services réseau qu'elles proposent.

- **attaque de l'homme de milieu**

Consiste à faire passé les échanges réseaux entre deux systèmes par le biais d'un troisièmes, sous contrôle d'un pirate .Ce dernier peut transformer à sa façon les données volées, tout en masquant à chaque acteur de l'échange la réalité de son interlocuteur.

- **Balayage de port**

C'est une technique servant à chercher les ports ouverts sur un serveur de réseau .Elle est utilisée par les administrateurs des système informatique pour contrôler la sécurité des serveurs de

leurs réseaux .la même technique aussi utilisée par les pirates pour trouver les failles dans les systèmes informatiques. Un balayage de port effectué sur un système tiers est généralement considéré comme une tentative d'intrusion.

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

C'est une technique qui consiste à envoyer des paquets IP en utilisant une adresse IP qui n'a pas été attribuée à l'expéditeur, cette technique permet au pirate d'envoyer des paquets anonymement.

- **Le craquage de mot de passe**

Cette technique consiste à essayer plusieurs mots de passe afin de trouver le bon. Elle peut s'effectuer à l'aide d'une liste des mots de passe les plus courants (et de leur variantes), ou par la méthode de brute force (toutes les combinaisons sont essayées jusqu'à trouver la bonne), cette technique longue, souvent peut utiliser à moins de bénéficier de l'appui d'un très grand nombres de machines.

Pour remédier à cela une sécurité a été établé afin de protéger les données, les informations circulant sur le réseau.

- La sécurité est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système informatique contre les menaces accidentelles ou intentionnelles auxquelles il peut être confronté. En d'autres mots, c'est l'ensemble des techniques qui assurent que les ressources du système d'information (matérielles ou logicielles) d'une organisation sont utilisées uniquement dans le cadre où il est prévu qu'elles le soient.

Les exigences fondamentales de la sécurité Informatiques se résument à assurer:

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

. II.4. Les méthodes de protection

- **Antivirus :**

Logiciel permettant de détecter et de supprimer les virus informatique sur n'importe quels types de stockage (disque dur, disquette, CD-ROM…..). Pour être efficace ce type de logiciel demande une mise à jour très fréquente au cours desquelles il mémorise les nouvelles formes de virus de circulation.

- **La cryptographie**

Est un ensemble de technique permettant de transformer les données dans le but de cacher leur contenu, empêcher leur modification ou leur utilisation illégale. Ce ci permet d'obtenir un texte, en effectuant des transformations inverse (ou encre des algorithmes de déchiffrement). Désormais, elle sert non seulement à préserver la confidentialité des données mais aussi à garantir leur intégrité et leur authenticité.

La taille des clés de chiffrement dépendent de la sensibilité des données à protéger .plus ces clés sont longues plus le nombre de possibilités de les déchiffrer important, par conséquent il sera difficile de devenir la clé.

Les algorithmes de chiffrement se divisent en deux catégories :

- **Chiffrement symétrique :**

Dans ce cas de chiffrement l'émetteur et le récepteur utilisent la même clé secrète qu'ils appliquent à un algorithme donné pour chiffrer ou déchiffrer un texte.

Ce cryptage à un inconvénient puisqu'il faut que les deux parties possèdent la clé secrète, il faut donc la transmettre d'un bout à l'autre, ce qui risque sur un réseau non fiable comme internet car la clé peut ainsi être interceptée.

- **Chiffrement asymétrique**

Ces systèmes se caractérisent par la présence d'une entité pour chaque interlocuteur désirant communiquer des données. Chaque interlocuteur possède une bi-clé ou couple de clés calculées l'une en fonction de l'autre.

Une première clé, visible appelée clé publique est utilisée pour chiffrer un texte en clair.

Une deuxième clé, secrète appelée clé privée est connu seulement par le destinataire, qui est utilisé pour déchiffrer un texte.

- **Le pare –feu (firewall)**

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

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

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

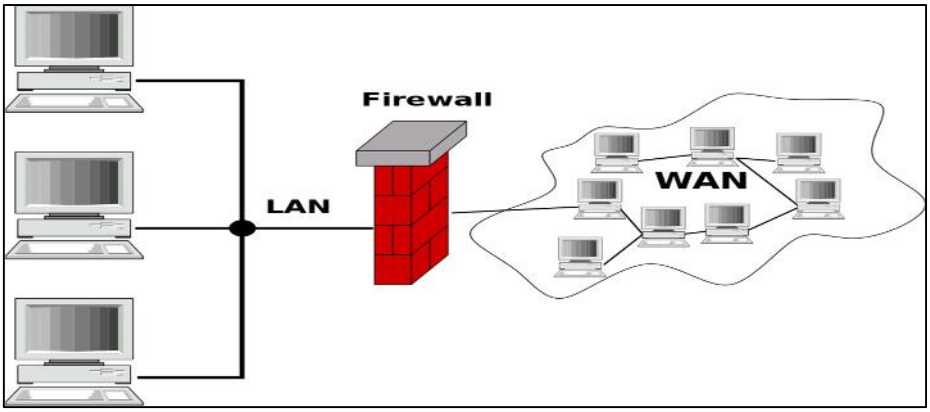


Figure II.1 : pare-feu

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

❖ **Le fonctionnement de pare-feu :**

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

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

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

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

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

- **Les VLAN (virtual Area Network)**

Un VLAN permet de créer des domaines de diffusion (domaine de brodcast) gérer par les commutateurs indépendamment d'emplacement ou se situent les nœuds, se sont des domaines de diffusion gérer logiquement.

- **Le NAT(Network Address Translation)**

Dans les entreprises de grandes tailles, différent réseaux interconnecté peuvent utiliser les même adresse IP. Pour que la communication soit possible entre nœuds des deux cotés, il est nécessaire de modifier les références de l'émetteur de paquets afin qu'il n'y ait pas de conflits et que la transmission soit fiable.

Des équipements de translation d'adresse NAT (Network Address Tranlation) sont chargés d'adopter cette fonctionnalité. Ils permettent le changement d'une adresse IP par une autre

Trois types d'adresse sont possibles :

- La translation de port PAT (Port Address Traslation), joue sur une allocation dynamique des ports TCP ou UDP, en conservant l'adresse IP d'origine.
- La conversion dynamique d'adresses (NAT dynamique) change à la volée d'adresse IP par rapport à une externe disponible dans une liste.
- La conversion statique d'adresse (NAT statique), effectue également un changement d'adresse IP, mais une table est maintenue, permettant à une adresse IP interne de toujours être remplacée par la même adresse IP externe.

- **Les ACL (Acces control list)**

Les listes de contrôle d'accès ont pour objectif de disposer d'une fonction de filtrage prenant en compte l'historique des connexions en cours, afin de ne pas accepter du trafic qui n'aurait pas été demandé à partir d'une zone précise du réseau.

Les ACL sembles avoir toujours existé sur les routeurs et rares sont les configurations ou elles n'apparaissent pas. Elles servent principalement au filtrage des paquets sur les interfaces physiques.

- **PFsens**

Définition

Pfsense est un routeur/pare-feu open source basé sur le système d'exploitation Free BSD, qui peut être installé sur un simple ordinateur personnel comme sur un serveur.

Il a pour particularité de gérer nativement les VLAN et dispose de très nombreuses fonctionnalités tels que faire un VPN ou portail captif.

Voici l'architecture avec laquelle peut être utilisé le pfsens

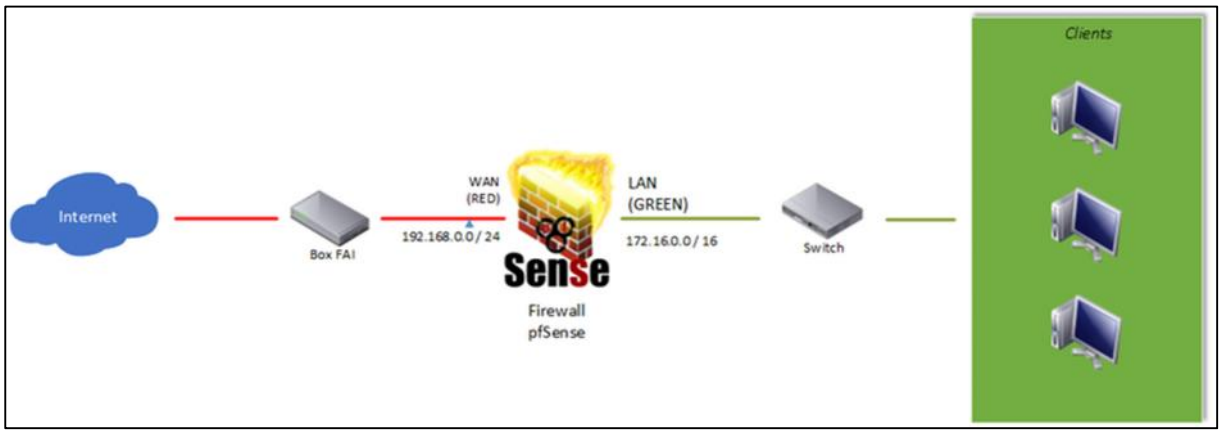


Figure II.2 : pf sense

❖ **Les principes de fonctionnement de Pfsense**

Pfsense offre une multitude de fonctionnalités intéressantes comme par exemple :

- Pare-feu (sa fonction primaire) qui est basé sur le paquet filtrer il permet donc :
  - Le filtrage par adresse IP source et de destination, par protocole IP et par port.
  - Limitation de connexions simultanées.
  - La possibilité de router les paquets sur les passerelles spécifiques selon les règles.

- Table d'état : qui contient des informations sur les connexions réseaux.
- Traduction d'adresses réseaux (NAT)ce qui permet de joindre une machine situé sur le LAN à partir de l'extérieur.
- VPN pour sécurisé les données transitant sur le réseau.
- Serveur DHCP qui permet de distribuer automatiquement une configuration IP aux équipements présents sur le réseau.
- Serveur DNS (statique ou dynamique) qui permet de communiquer avec les autres périphériques présents sur le réseau grâce à leurs adresses IP.
- Serveur PPPOE (point to point Protocol Over Ethernet) un protocole d'encapsulation sur ppp et ethernet.
- une base de donnée locale peut être utilisée pour l'authentification .

  Avantage d'utilisation de pfsense :

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

- **VPN** (Virtual Private Network)

II.5. Le concept de réseau privé virtuel

a) Introduction

Les réseaux locaux type LAN permettent de faire communiquer les ordinateurs d'un site d'une société . Ces réseaux sont relativement sûr car ils sont quasiment toujours derrière une série de pare-feu ou coupés d'Internet et que le chemin emprunté par les données ne quitte pas l'entreprise et il est connu. Ils peuvent toutefois être soumis à des attaques dites du « man-in-the-middle ».

Sur Internet, on ne sait pas par où passent les données car les chemins changent. Ces données peuvent donc être écoutées ou interceptées. Il n'est donc pas envisageable de faire connecter deux LAN entre eux par Internet sans moyen de sécuriser l'acheminement des données échangées.

Il existe alors deux solutions :

- relier les deux sites par une ligne spécialisée mais hors de prix
- créer un réseau privé virtuel sécurisé autrement dit un VPN. On encapsule (en anglais tunneling) les données dans un tunnel crypté

Voici comment peut se schématiser une Réseau Privé Virtuel ou VPN :

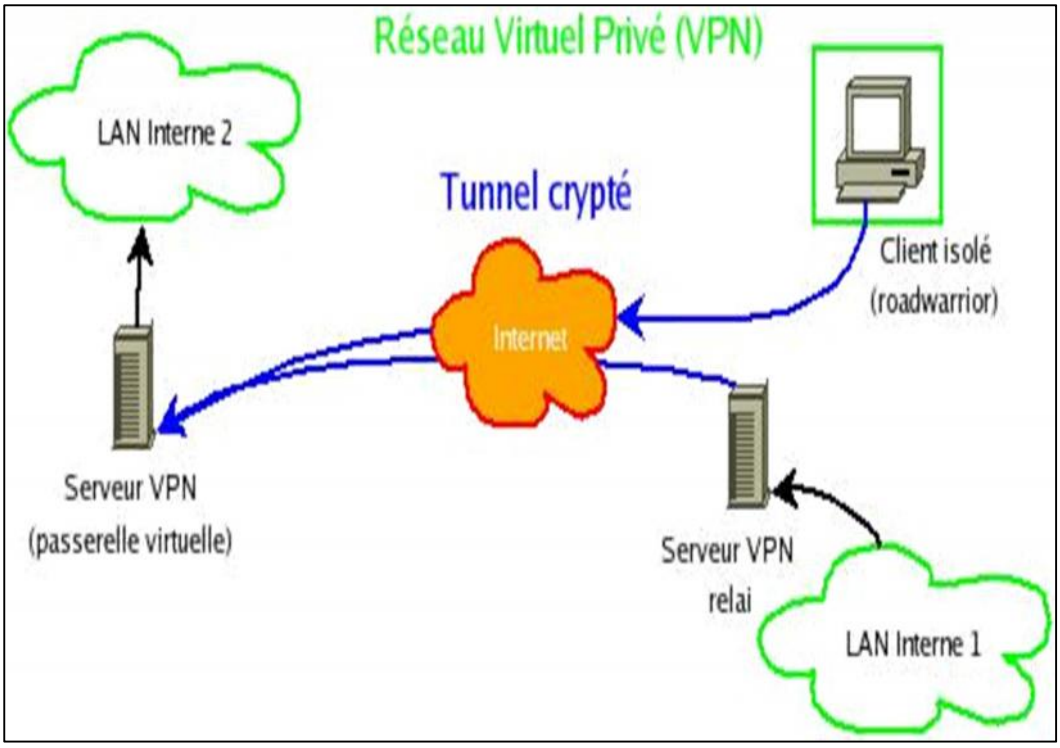


FIGURE II.3 : schéma d'un VPN

Mais alors pourquoi réseau virtuel privé ?

Virtuel simplement parce que le VPN relie deux réseaux physiques LAN par une liaison qui n'est pas réellement sûre et surtout pas dédiée à cet usage. Et privé parce que les données sont encryptées et que seuls les deux réseaux se voient mais ne sont pas vus de l'extérieur.

Pour résumer le VPN permet de mettre deux sites en relation de façon sécurisée à très faible coût par une simple connexion Internet. Mais cela se fait au détriment des performances car le passage par Internet est plus lent que sur une liaison dédiée.

b) Le fonctionnement du VPN

Le VPN repose sur un protocole de tunnelisation qui est un protocole permettant de chiffrer les données par un algorithme cryptographique entre les deux réseaux.

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

- authentification des entités communicantes : le serveur VPN doit pouvoir être sûr de parler au vrai client VPN et vice-versa
- authentification des utilisateurs : seuls les bonnes personnes doivent pouvoir se connecter au réseau virtuel. On doit aussi pouvoir conserver les logs de connexions
- gestion des adresses : tous les utilisateurs doivent avoir une adresse privée et les nouveaux client vont obtenir une facilement
- cryptage du tunnel : les données échangées sur Internet doivent être cryptées entre le client VPN et le serveur VPN et vice-versa
- les clés de cryptage doivent être régénérées souvent (automatiquement)
- le VPN peut supporter tous les protocoles afin de réaliser un vrai tunnel comme s'il y avait réellement un câble entre les deux réseaux.

II.5.1. Les différents types de VPN

- Le VPN d'accès
- Intranet VPN
- Extranet VPN

a) Le VPN d'accès :

Le VPN d'accès est utilisé pour permettre à des utilisateurs itinérants d'accéder au 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 crypte vers le serveur distant ; il communique avec le NAS du fournisseur d'accès et c'est le NAS qui établit la connexion cryptée.
- ✓ L'utilisateur possède son propre logiciel client pour le VPN auquel cas il établit directement la communication de manière cryptée vers le réseau de l'entreprise.

Les deux méthodes possèdent chacune leurs avantages et leurs inconvénients :

- ✓ La première permet à l'utilisateur de communiquer sur plusieurs réseaux en créant plusieurs tunnels, mais nécessite un fournisseur d'accès proposant un NAS compatible avec la solution VPN n'est pas cryptée ce qui peut poser des problèmes de sécurité.
- ✓ Sur la deuxième méthode ce problème disparaît puisque l'intégralité des informations sera cryptée des l'établissement de la connexion. Par contre, cette solution nécessite que chaque client transporte avec lui le logiciel, lui permettant d'établir une communication cryptée. Quelle que soit la méthode de connexion choisie, ce type d'utilisation montre bien l'importance dans le VPN d'avoir une authentification forte des utilisateurs

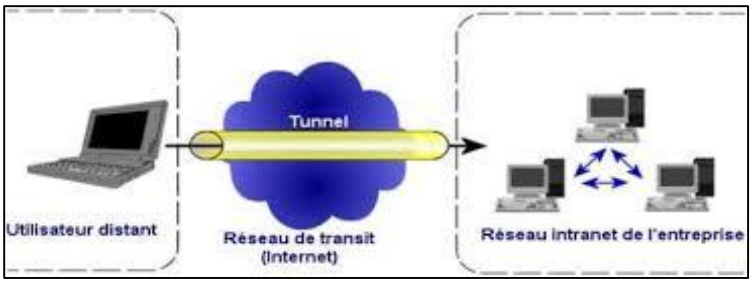


Figure II.4 : VPN d'accès

b) L'intranet VPN

Dans une entreprise l'Intranet met à la disposition des employés des documents divers (texte, vidéo, image…), ce qui permet d'avoir un **accès centralisé** et cohérent aux informations de l'entreprise.

L'intranet peut remplir plusieurs fonctions :

- Mise à disposition de documents techniques
- Mise à disposition d'informations sur l'entreprise
- Forums de discussion, listes de diffusion, chat en direct
- Gestion de projets, agenda, aide à la décision
- Un échange de données entre collaborateurs
- Moteur de recherche de documentations
- Portail vers internet

- Messagerie électronique
- Annuaire du personnel
- Visioconférence

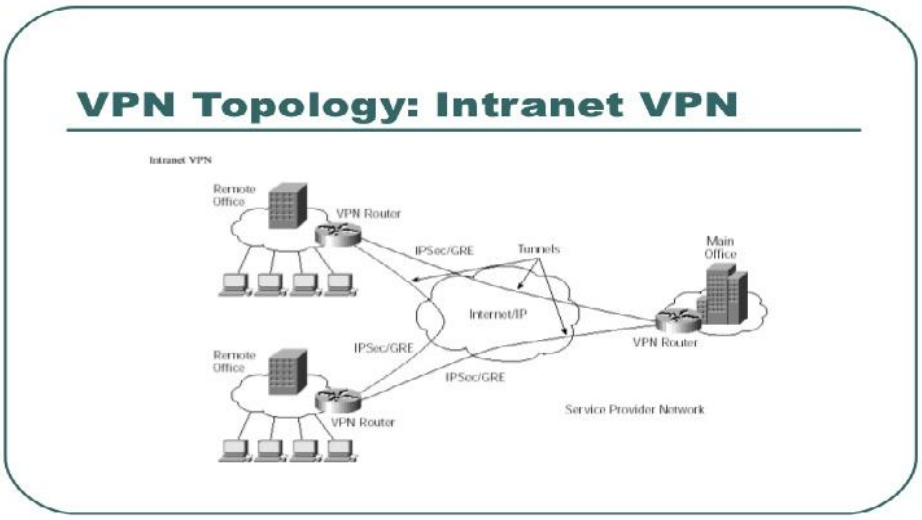


Figure II.5: Intranet VPN

a) **L'extranet VPN**

Une entreprise peut utilisée le VPN pour communiquer avec ses clients et ses partenaire. Elle ouvre alors son réseau local à ces derniers. Dans ce cadre, il est fondamental que l'administrateur du VPN puisse tracer le client sur le réseau et gérer les droits de chacun sur celui-ci.

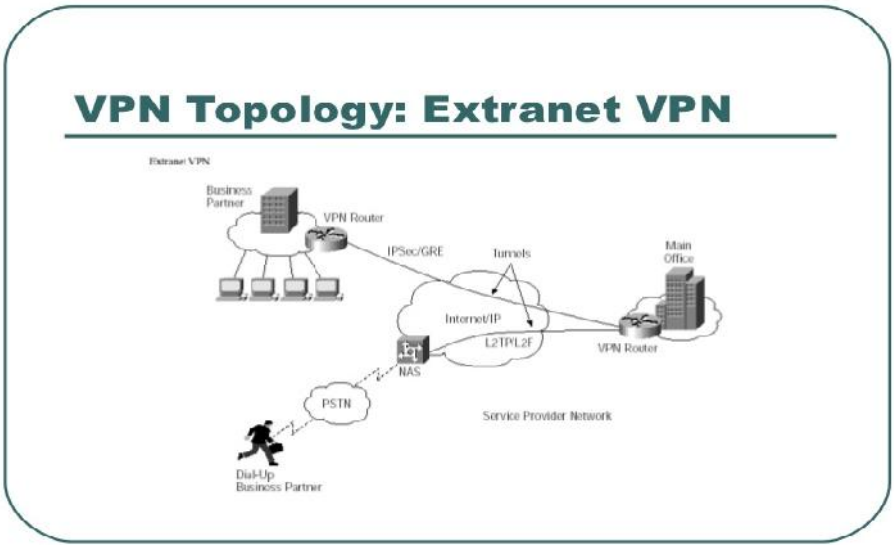


Figure II.6 : Extranet VPN

II.5.2 Les différentes architectures des VPN

a) De poste à poste

C'est le cas d'utilisation le plus simple. Il s'agit de mettre une relation deux serveurs.

Le cas d'utilisation peut être le besoin de synchronisation de base de données entre deux serveurs d'une entreprise disposant de chaque coté d'un accès internet. L'accès réseau complet n'est pas indispensable dans ce genre de situation.

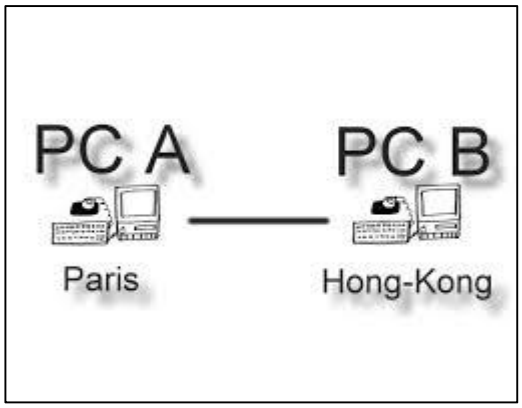


Figure II.7. VPN poste à poste

a) De poste à site

Un utilisateur distant a simplement besoin d'un client VPN installé sur son PC pour se connecter au site de l'entreprise via sa connexion internet. Le développement de l'ADSL favorise ce genre d'utilisation.

Toutefois à interdire l'accès internet depuis le poste « localement ». Pour une question de sécurité, la navigation devra se faire via le réseau de l'entreprise.

Ce point est important et rejoint la réflexion la plus large de la sécurité des sites mis en relation avec VPN. Lorsque les niveaux de la sécurité sont différents, lorsque les deux sites sont reliés, le niveau de sécurité le plus bas est applicable aux deux, s'il existe une failles de sécurité sur un site (ou sur poste normale, celle-ci peut être exploitée.

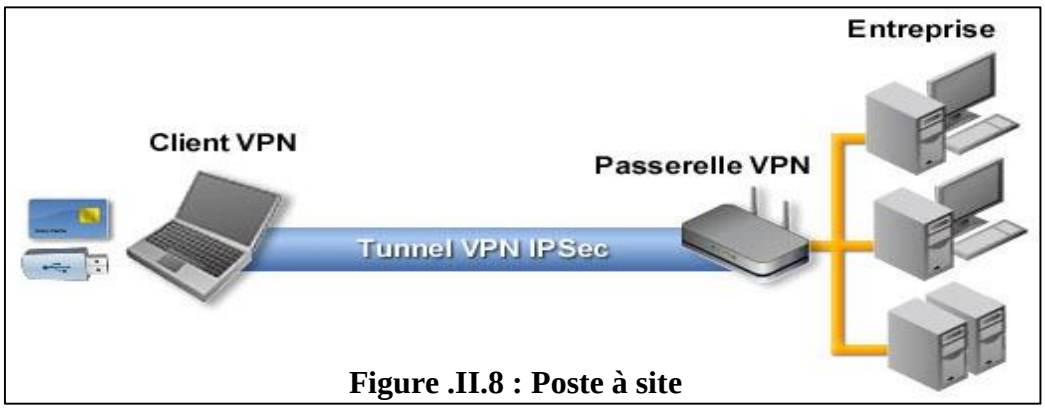


Figure .II.8 : Poste à site

C) De site à site

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

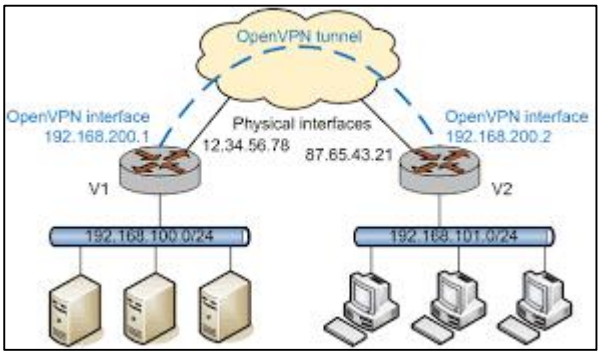


Figure II.9. : site à site

II.5.3. Les implémentations historiques de VPN

a) Catégories de protocoles

1) Classement par Niveau OSI

Il existe deux catégories de protocoles VPN :

- Les protocoles nécessitant parfois/souvent du matériel particulier :
  - Les protocoles de niveau 2 (Couche Liaison) dans la pile TCP/IP : PPTP, L2F et L2TP
  - Les protocoles de niveau 3 (Couche Réseau) dans la pile TCP/IP : IPSec
- Les protocoles ne nécessitant qu'une couche logicielle :
  - Les protocoles de niveau 4 (Couche Transport) : OpenVPN en SSL

2) Classement par Système d'exploitation

Voici les protocoles classés par OS

- Disponibles nativement sous Windows
  - PPTP et IPSec/L2TP
- Protocoles disponibles sous Linux et Windows par logiciel annexe :
  - OpenVPN
- Disponibles sous Linux

b) Les principaux protocoles de VPN

Les principaux protocoles de tunneling VPN sont les suivants :

- PPTP (*Point-to-Point Tunneling Protocol*) est un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.
- L2F (*Layer Two Forwarding*) est un protocole de niveau 2 développé par Cisco, Northern Telecom et Shiva. Il est désormais quasi-obsolète
- L2TP (*Layer Two Tunneling Protocol*) est l'aboutissement des travaux de l'*IETF* (RFC 2661) pour faire converger les fonctionnalités de *PPTP* et *L2F*. Il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP.
- **IP Sec** est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP

1) Le protocole PPTP(*Point To Point Tunneling Protocol)*

Le principe du protocole PPTP (RFC2637) (*Point To Point Tunneling Protocol*) est de créer des trames avec le protocole PPP et de les crypter puis de les encapsuler dans un paquet IP.

Cela permet de relier les deux réseaux par une connexion point-à-point *virtuelle* acheminée par une connexion IP sur Internet. Cela fait croire aux deux réseaux qu'ils sont reliés par une ligne directe.

On garde, ainsi les adresses des réseaux physiques dans la trame PPP cryptées et cette trame est acheminée normalement sur Internet vers l'autre réseau.

Il permet les opérations suivantes :

- L'authentification se fait par le protocole MS-CHAP (Challenge Handshake Authentification Protocol) version 2 ou avec le protocole PAP (Password Authentification Protocol)
- L'encryptions se fait par le protocole MPPE (Microsoft Point-to-Point Encryption). Cela crée un tunnel de niveau 3 (Réseau) géré par le protocole GRE (Generic Routing Encapsulation).

La compression peut se faire avec le protocole MPPC (Microsoft Point to Point Compression)

- On peut ajouter autant de protocole que l'on veut dans le protocole PPTP pour l'encryptions et la compression des données.

La connexion se passe donc ainsi :

- Le client se connecte à Internet par son modem par le protocole PPP (classiquement)

- Le client se connecte alors au serveur VPN par une connexion IP encapsulant les paquets GRE/PPP cryptés. Ainsi cela forme deux connexions l'une sur l'autre
  - la connexion normale à Internet : elle achemine le trafic vers/depuis Internet
  - la connexion virtuelle au dessus de la connexion Internet : elle achemine le trafic vers/depuis le réseau VPN

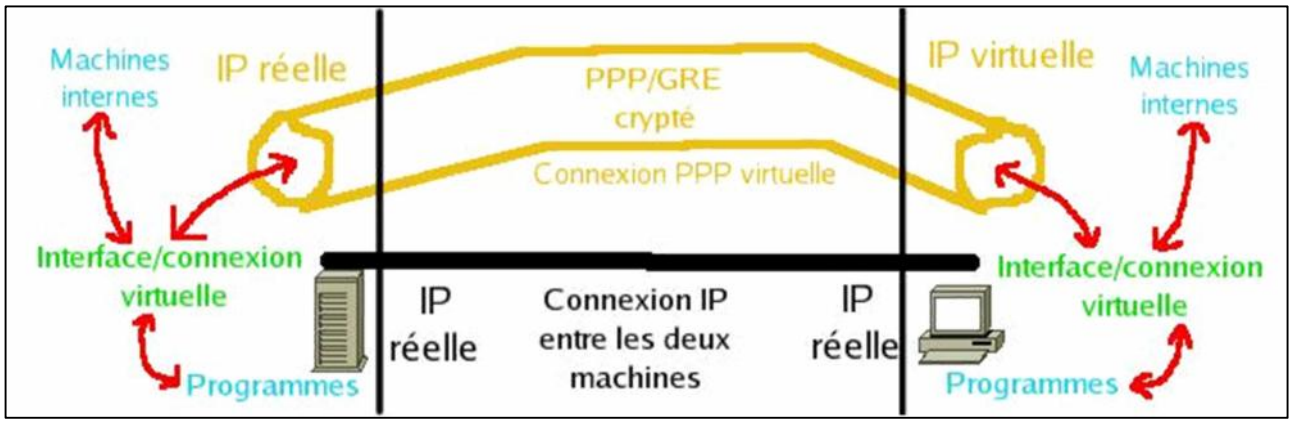


Figure II.10. Protocol PPTP

- A la fin de la connexion c'est le serveur qui ferme le tunnel

On obtient donc une connexion PPP au dessus de la connexion Internet ou Ethernet qui nous donne accès au serveur VPN PPTP. Cette connexion PPP obtient une IP de la plage définie dans la configuration de PPTP Sur le serveur, on a une connexion de son IP publique vers l'IP virtuelle du client et sur le client c'est l'inverse.

Un paquet d'une connexion PPTP ressemble donc à ceci :

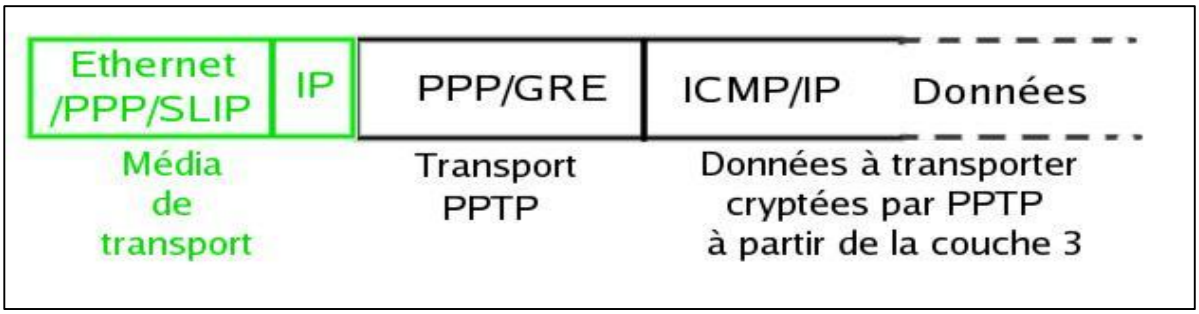


Figure II.11. Paquet de connexion

Il est encore beaucoup utilisé du fait qu'il est nativement intégré aux systèmes Windows. Mais les protocoles tels que IPSec ou OpenVPN sont bien meilleurs en sécurité et en performances.

2) **Le protocole L2TP(**Layer 2 Tunneling Protocol)

Le protocole L2TP (Layer 2 Tunneling Protocol), développé à partir du protocole point à point PPP, est sans conteste l'une des pierres angulaires des réseaux privés virtuels d'accès. Il rassemble en effet les avantages de deux autres protocoles de fractionnement en canaux : L2F (Layer 2 Forwarding), développé par Cisco Systems, et PPTP (Point-to-Point Tunneling), de Microsoft.

L2TP est une norme préliminaire de l'IETF (Engineering Task Force) actuellement développée et évaluée conjointement par Cisco Systems, Microsoft, Ascend, 3Com et d'autres acteurs clés du marché des réseaux. 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, L2TP peut être utilisé pour faire du tunnelling sur Internet. Mais L2TP peut aussi être directement mis en œuvre sur des supports WAN (relais de trames) sans utiliser la couche de transport IP. On utilise souvent ce protocole pour créer des VPN sur Internet. Dans ce cas, L2TP transporte des trames PPP dans des paquets IP. Il se sert d'une série de messages L2TP pour assurer la maintenance du tunnel et d'UDP pour envoyer les trames PPP dans du L2TP.

3) Le protocole IPSec (Internet Protocol Security)

IPsec est un protocole qui vise à sécuriser l'échange de données au niveau de la couche réseau. Il est compatible IPv4 et IPv6. IPsec est basé sur deux mécanismes :

Le premier AH (Authentification Header) permet d'assurer l'intégrité et l'authenticité des datagrammes IP.

Le second ESP (Encapsulating Security Payload) peut aussi permettre l'authentification des données mais il est principalement utilisé pour le cryptage des informations. Bien qu'indépendants ces deux mécanismes sont presque toujours utilisés conjointement.

IPSec est nativement un protocole de tunneling. Pourtant, ce protocole propose aussi des mécanismes de sécurisation des échanges entre utilisateurs des VPN. IPSec assure l'authenticité des extrémités, la confidentialité et l'intégrité des échanges grâce aux algorithmes et mécanismes de chiffrement.

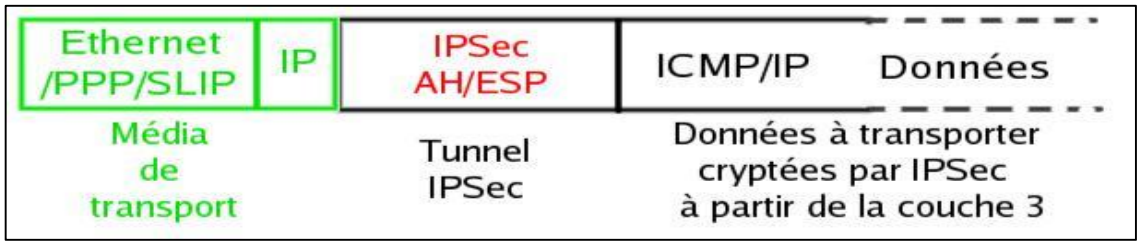


Figure II.12. Protocol IPsec

4) Le protocole MPLS(MultiProtocol Label Switching)

C'est un protocole développé en partie par Cisco pour faciliter le routage IP par les commutateurs. Il est assez peu employé. Il repose sur la communication de Label.
Le principe est de mettre un entier (le label) entre les couches 2 (liaison) et 3 (réseau) qui évite au routeur de remonter plus haut qu'il n'en a besoin. Ainsi, il a une table pour lui dire « si je reçois un paquet avec le numéro « n » je le réémet sur ma sortie S avec le label m ». Ceci évite d'avoir besoin de lire l'en-tête IP et de consulter sa table de routage IP

5) L'implémentation OpenVPN

Le Protocole **Open VPN** est une application informatique ouverte pour la mise en place de techniques de réseaux privés virtuels (VPN, en anglais Virtual Private Network), avec des connexions sécurisées point-par-point ou site-par-site, pour des configurations via routage ou pont, ainsi que pour les accès à distance. Il exploite un protocole de sécurité sur mesure qui utilise SSL/TLS pour les échanges clés.

Un protocole Open VPN permet à des homologues de s'authentifier mutuellement en utilisant une clé secrète pré-partagée, des certificats ou un nom d'utilisateur / mot de passe. Lorsqu'il est utilisé dans une configuration multi client-serveur, il permet au serveur de libérer un certificat d'authentification pour chaque client, en utilisant la signature et l'autorité de certification. Ce système utilise en grande partie la base de cryptage OpenSSL, ainsi que le protocole SSLv3/TLSv1 et contient de nombreuses fonctionnalités de sécurité et de contrôle.

Conclusion

Dans ce chapitre, nous avons présentés une introduction générale sur la sécurité informatique et les notions de base d'un réseau VPN qui permet donc aux réseaux privés de s'étendre et de se relier entre eux au travers d'internet.

III.1. Introduction

L'objectif de cette partie est de mettre en œuvre une solution permettant à des utilisateurs itinérants d'accéder au privé et d'assurer l'échange de données entre eux d'une façon sécurisé à travers un tunnel VPN.

III.2. Présentation du projet

Il s'agit de mettre en place une solution qui va permettre un accès externe à notre réseau d'entreprise via une connexion VPN de type OpenVPN qui s'appuiera sur un équipement de type Firewall Pfsense et se fera via VMware.

Schéma global

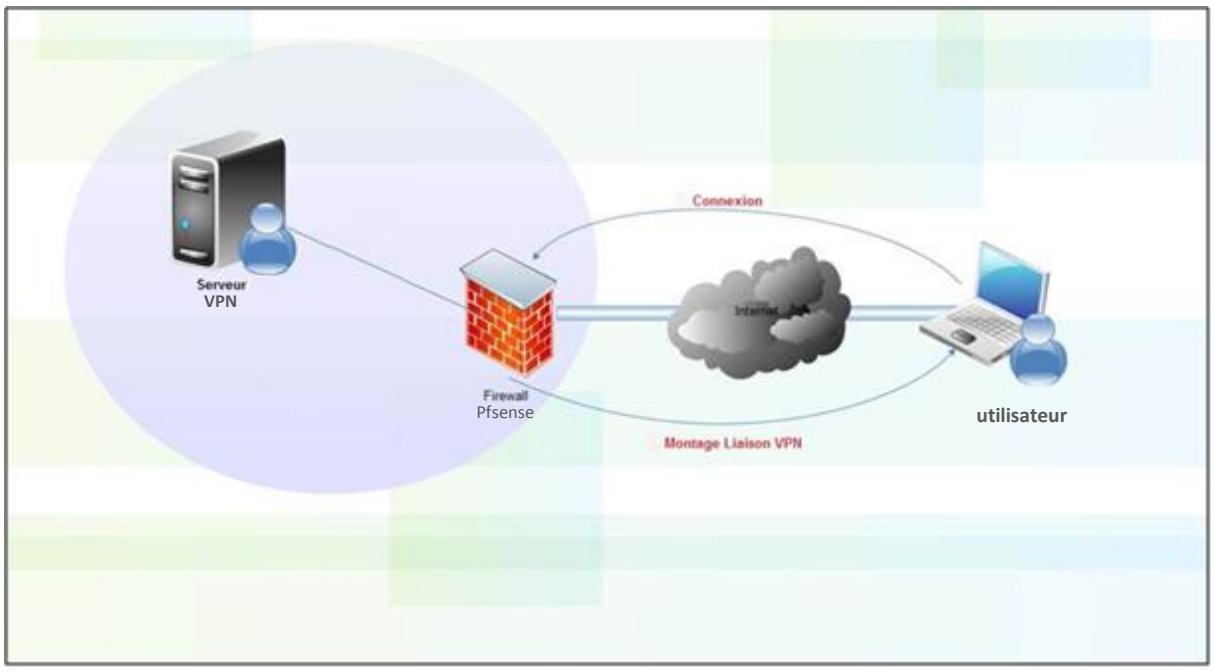


Figure III.1 : Schéma global d'un réseau VPN

III.3. Installation de et configuration de pfsense

III.3.1. Notion de virtualisation

La virtualisation permet de travailler sur un système d'exploitation différent de celui de la machine hôte. Ce procédé présente plusieurs avantages comme celui de tester un système et des logiciels dans un environnement fermé mais également de faire fonctionner plusieurs systèmes d'exploitation sur le même ordinateur.

- **Vmware workstation**

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

Apres avoir installer vmware workstation 12.5.1 sur notre machine windows nous allons passer à la configuration du réseau LAN.

III.3.2. Création de la machine virtuelle

Pour installer le vmware on choisit une machine Windows disposant des caractéristiques suivantes :

- Une RAM de 8G .
- un processeur Intel Core i5.

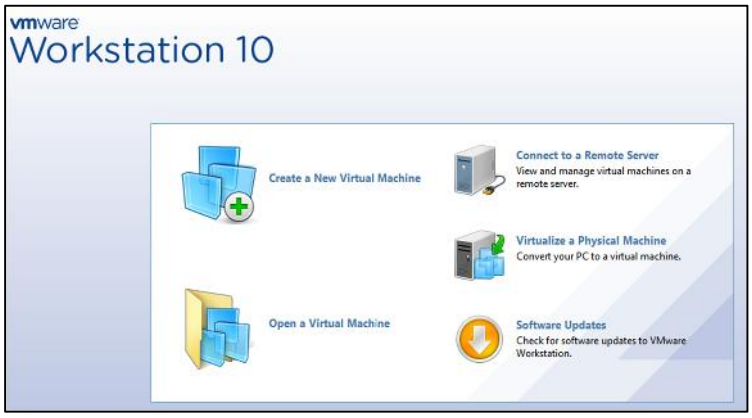


Figure III.2 : Page d'accueil de Vmware

Pour créer une nouvelle machine sous vmware, on clic sur « create a New virtual machine » dans la figure III.2 pour avoir la fenêtre suivante.

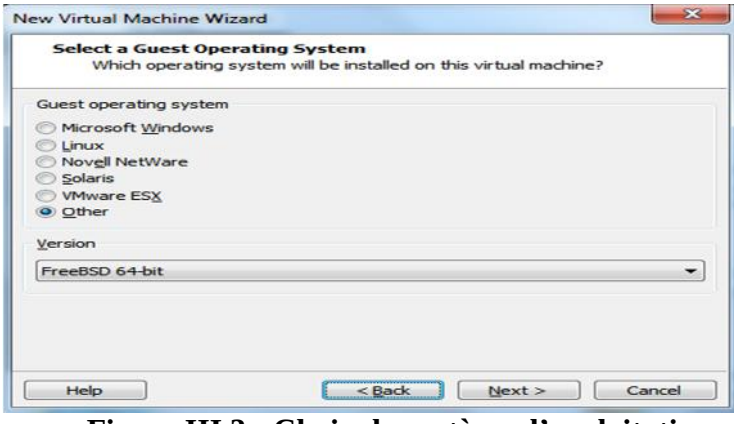


Figure III.3 : Choix du système d'exploitation

Dans cette fenêtre, nous allons choisir le système d'exploitation de notre machine qui est le freeBSD

Dans les étapes suivantes nous allons définir les paramètres de notre machine (capacité du disque dur, capacité de la RAM…) ainsi que deux cartes réseaux qui doivent être configurées:

- La première en mode bridge relié au réseau WAN comme l'illustre la figure suivante :

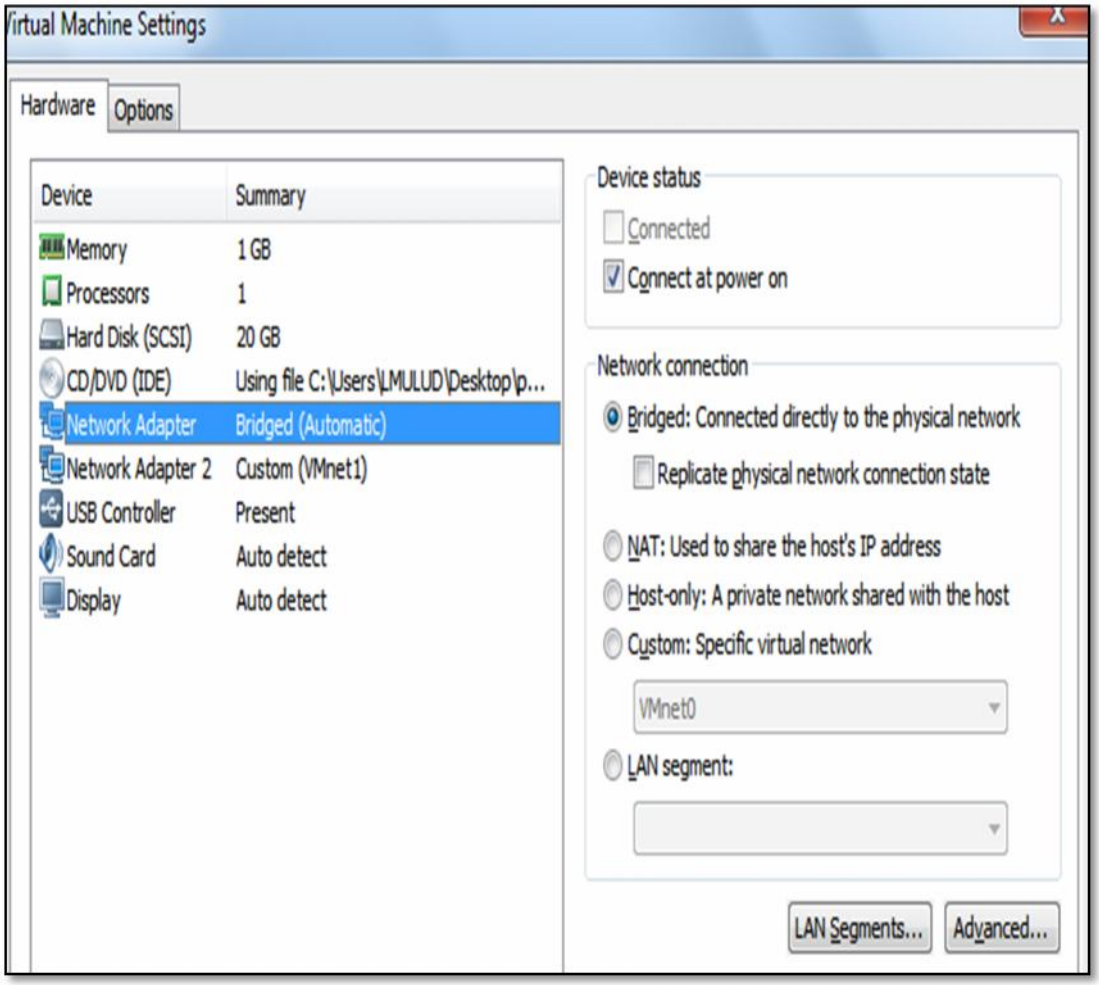


Figure III.4 : Carte réseau

- La deuxième en NAT reliée au réseau LAN selon la figure suivante :

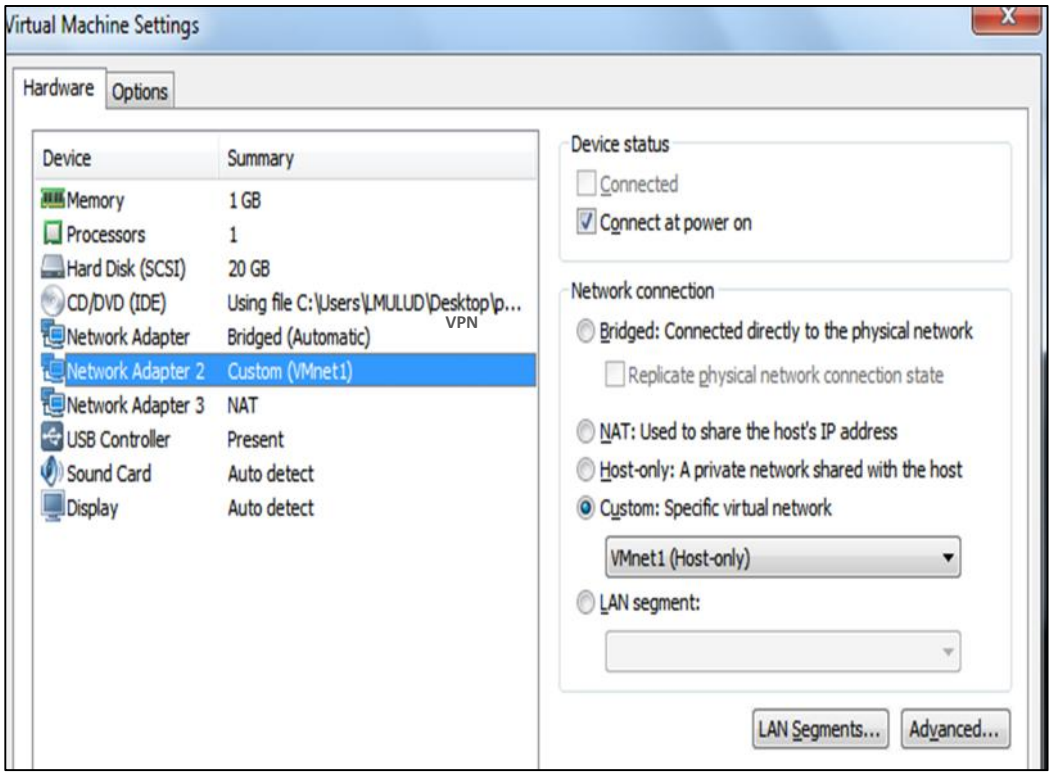


Figure III.5 : Carte réseau

II.3.3. Installation du pfsense

Une fois le vmware est installer et toutes les paramètres configuré, on lance le démarrage de la machine virtuelle avec la version l'ISO monté. Un menu de boot apparaît, selon les besoins on peut choisir de démarrer Pfsense avec certaines options activées. Si aucune touche n'est appuyée, Pfsense bootera avec les options par défauts (choix 1) au bout de 8 secondes.

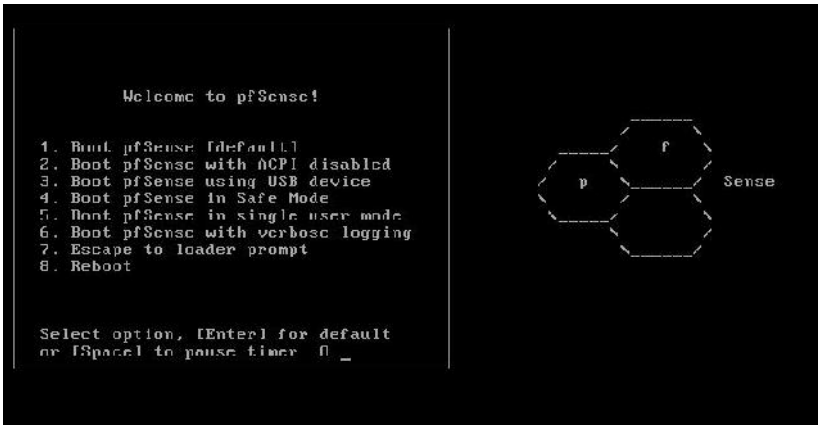


Figure III.6 menu de boot

L'installation démarre, dès le premier écran nous pouvons régler différents paramètres notamment la police d'écriture et l'encodage des caractères. On sélectionne "Accept these Settings".

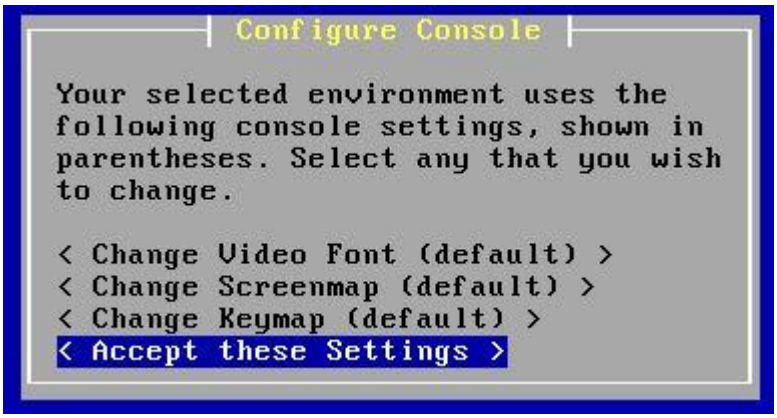


Figure III.7 : console

On choisit "**Quick/Easy Install**" pour procéder à l'installation rapide.

Figure III.8 : Sélection des tâches

Le message qui suit, nous informe que le disque dur sera formaté et toutes les données présentes dessus seront effacées. On sélectionne "**OK**" et on continue.

L'installation débute et copie les fichiers nécessaires sur le disque dur, nous devons par la suite choisir quel type de kernel (noyau), nous voulons installer, étant sur un ordinateur nous choisissons le "**Standard Kernel**".

Une fois l'installation finie, on choisit "**Reboot**" et nous redémarrons sur notre nouvelle installation.

Durant l'installation, pfsense va détecter automatiquement les listes des cartes réseaux disponibles nous allons avoir les interfaces réseaux que nous avons configurées précédemment.

L'écran principal suivant s'affiche :

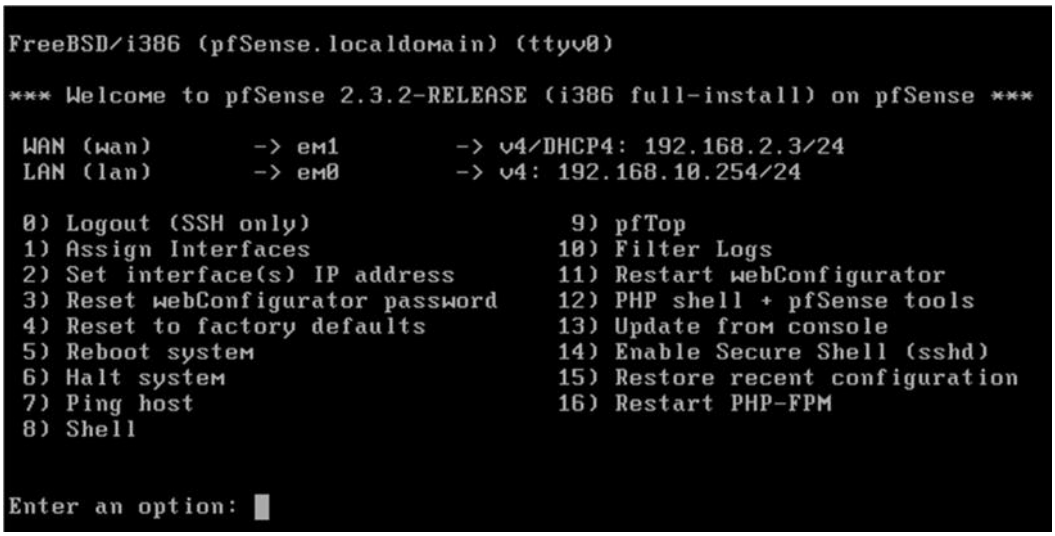


Figure III.9 : visualisation des interfaces réseaux

L'étape suivante consiste à configurer l'interface web du Pfsense en introduisant l'adresse IP : 192.168.10.254 dans une page web.

La page d'authentification suivante s'affiche :

Nous introduisons le nom, d'utilisateur « admin » ainsi que le mot de passe « pfsense » .

Figure III.10 : Identification du pfsense

On clic sur « login».

La page suivante s'affiche :

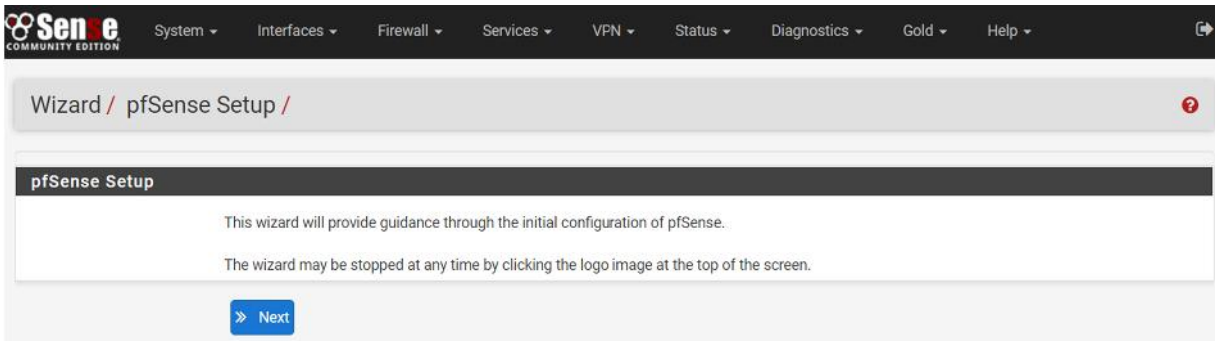


Figure III.11 : Installation

On clique s ur next, une page contenant des informations générale de pfsense s'affiche. Après l'avoir rempli la page suivante s'affiche :

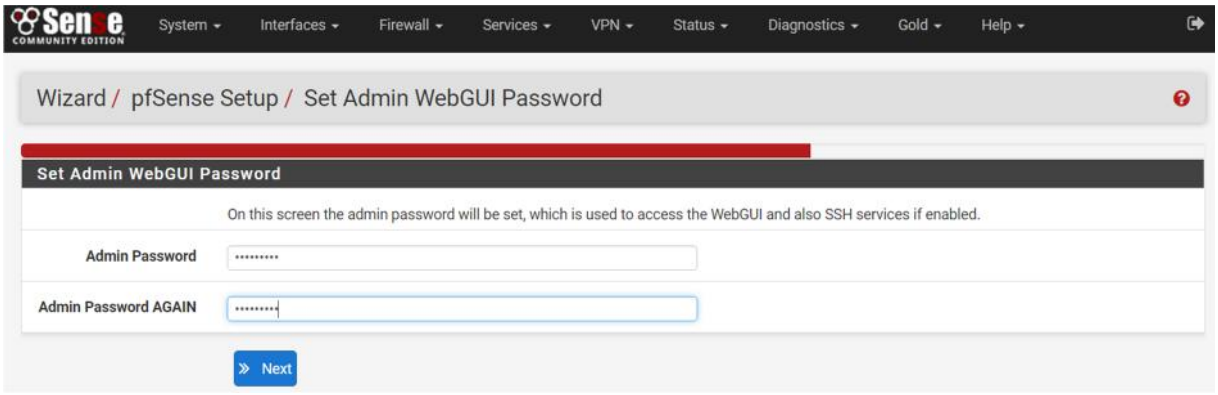


Figure III.12 : Identification

Nous allons attribuer un nouveau mot de passe en mesure de sécurité

III.4. configuration du réseau VPN :

Le premier élément dont on aura besoin est de définir une autorité de certification interne avec son propre certificat pour pouvoir ensuite auto signer les différents certificats que nous allons créer. On aura besoin à la fois d'un certificat pour le serveur c'est-à-dire au niveau de pfsense et également un certificat pour le client, ces derniers seront signer par l'autorité de certification interne que nous aurons crée. Nous allons commencer par créer notre autorité de certification

III.4.1. Création du certificat d'autorité

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

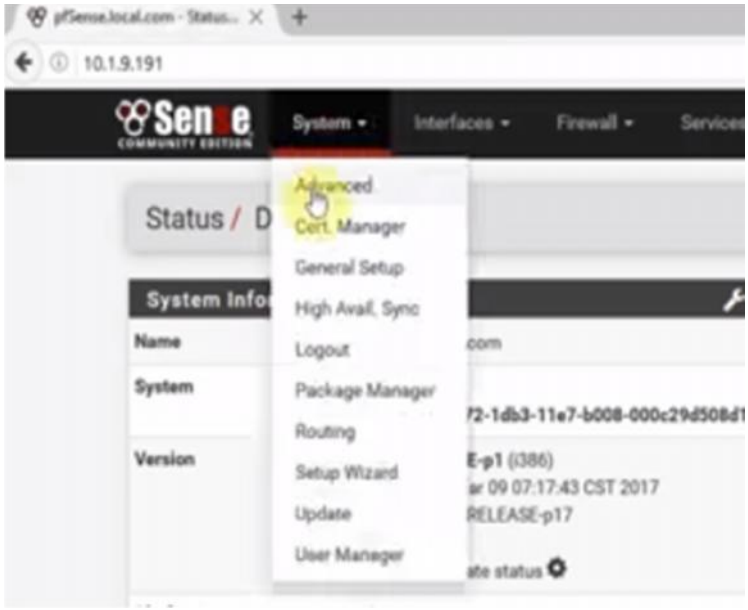


Figure III.13 : Accès à l'interface web

Dans l'onglet certificat d'autorité system« Cas » cliquer sur ajouter « + » a fin de créer une nouvelle autorité de certification .

Nous allons remplir le formulaire c'est dessus en choisissant la méthode « create an internal certificat » pour crée une autorité de certificat interne.

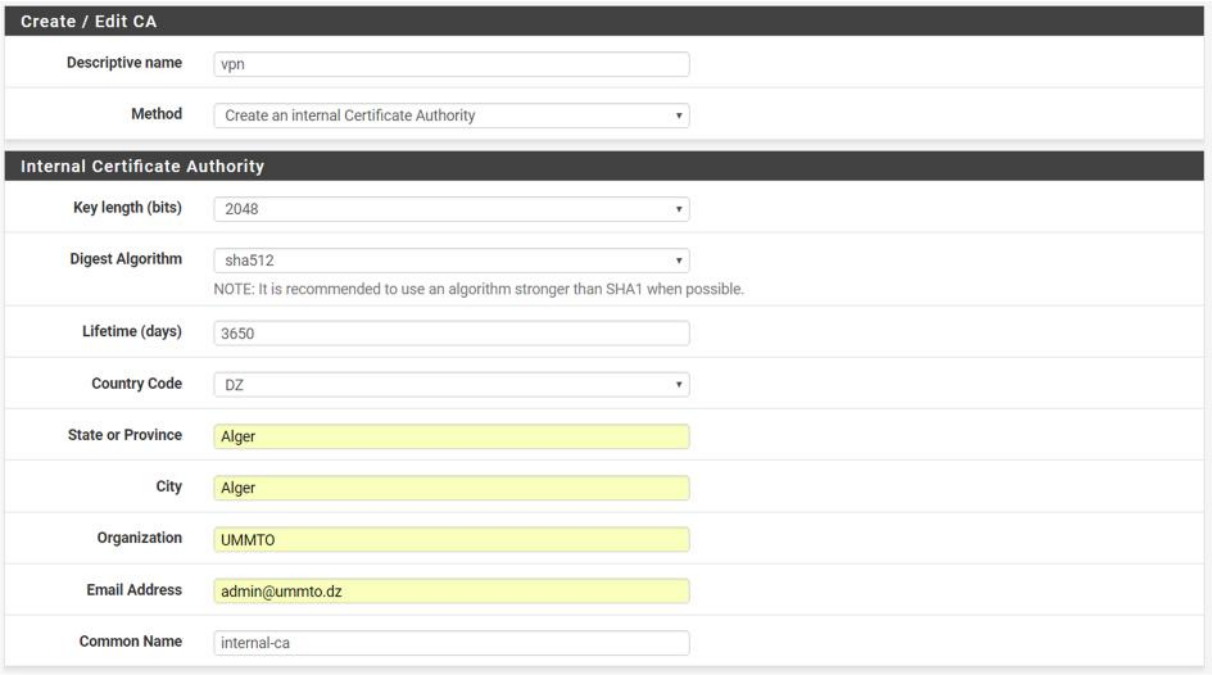


Figure III.14 Formulaire du certificat d'autorité

Une fois les données enregistrées le certificat d'autorité « CA » sera créé.

III.4.2. créer un certificat pour le serveur

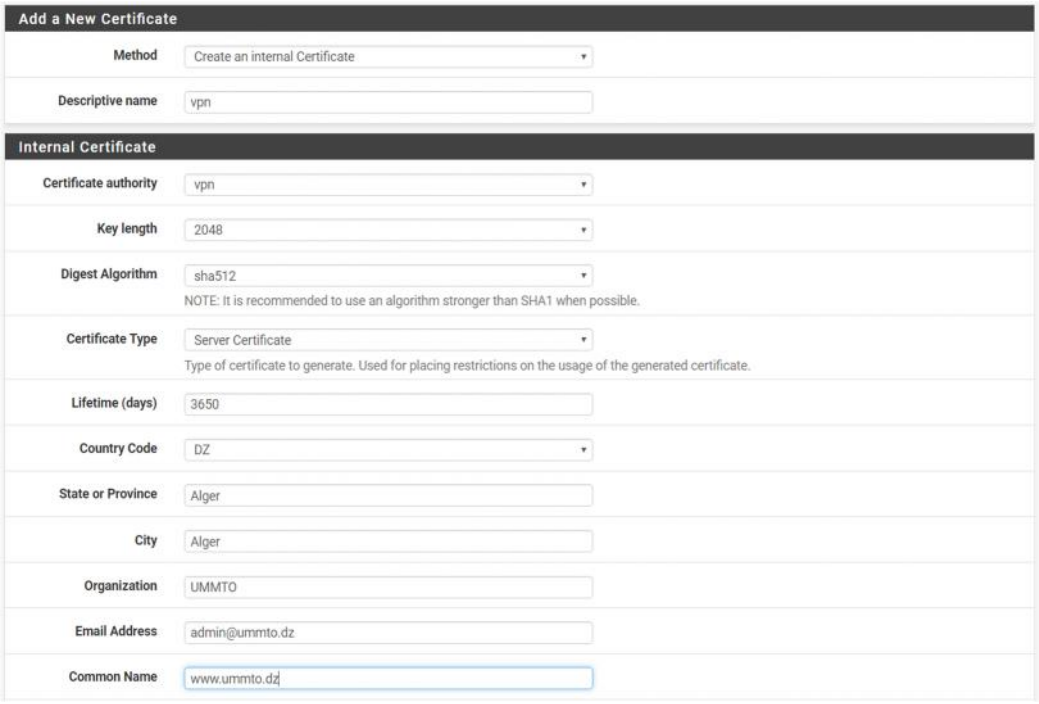


Figure III.15 Formulaire du certificat d'autorité

III.4.3. Créer un utilisateur ainsi que son certificat

A partir de l'onglet « système » en clic sur « user manager» en suite « user » et en fin « Add » pour ajouter un utilisateur autorisé à se connecter au VPN, celui-ci possédera son propre certificat qui sera généré lors de la création de l'utilisateur.

On rempli le formulaire et on clic sur « save ».

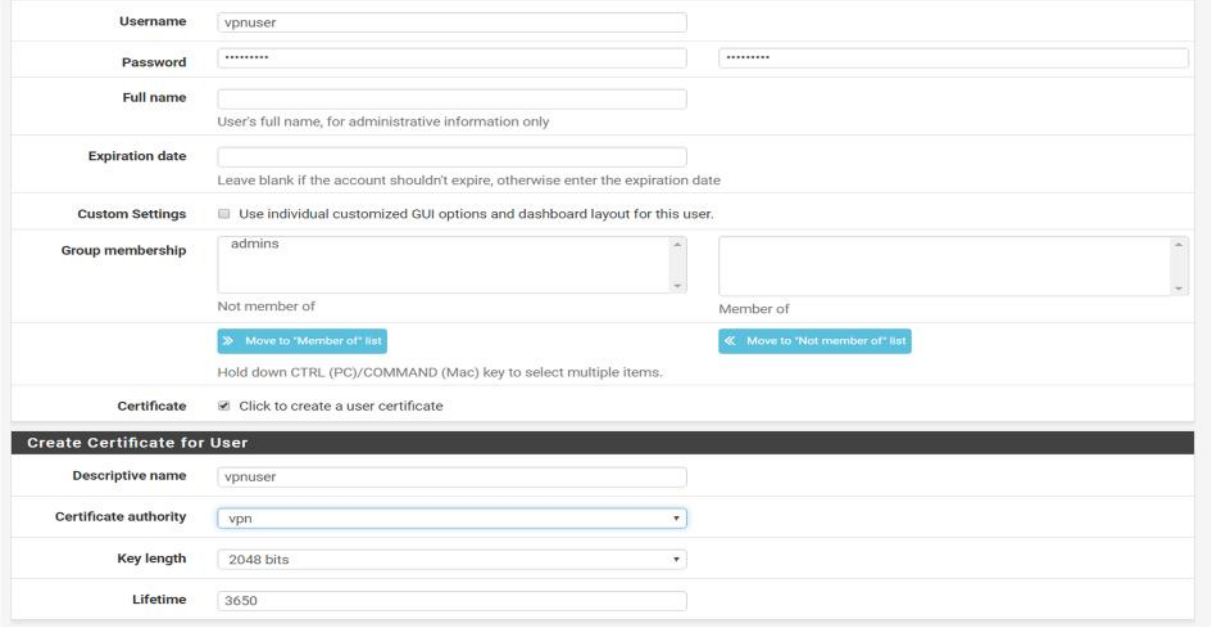


Figure III.16 : Formulaire de certificat de l'utilisateur

- Installation du client OpenVPN

Pour exporter ces certificats nous allons installer le paquet OpenVPN-client export disponible dans « system »=> « package manger => available packags.

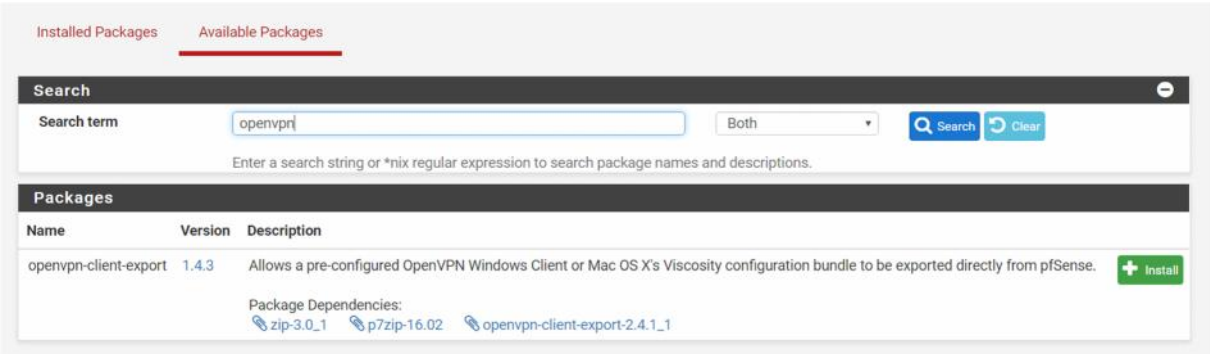


Figure III.17 : package

Installation du package :

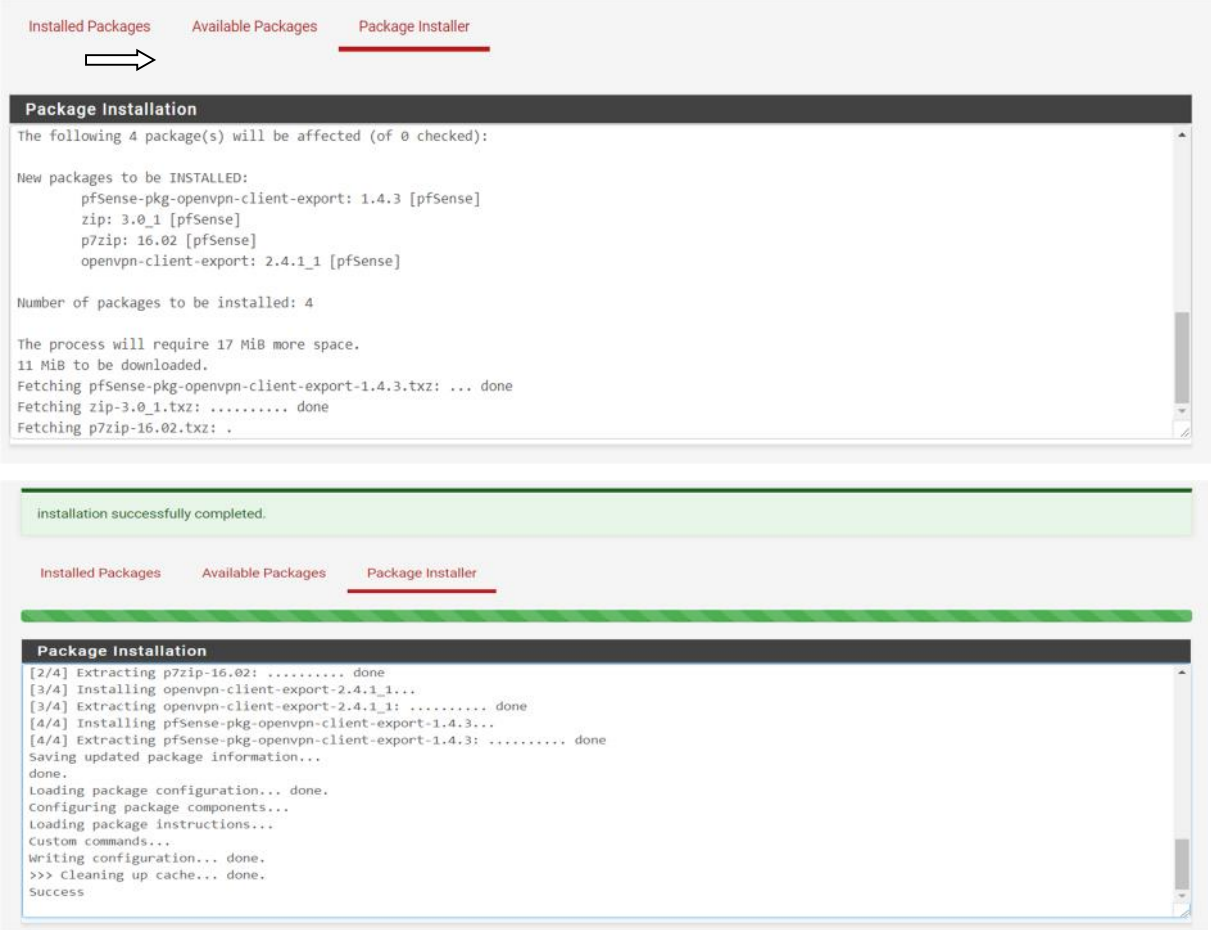


Figure III.18 : Installation du package

Nous avons installé avec succès l'utilitaire d'exportation Openvpn, maintenant il est temps d'effectuer la configuration du serveur Openvpn à partir de « VPN » => Openvpn => wizards

On choisit le type de serveur local « user » « access » et le certificat d'autorité (vpn).

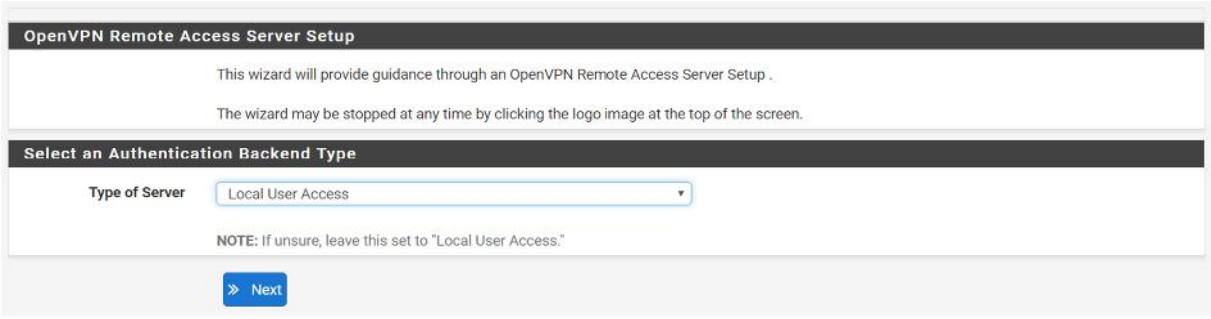


figure III.19 : Type de serveur

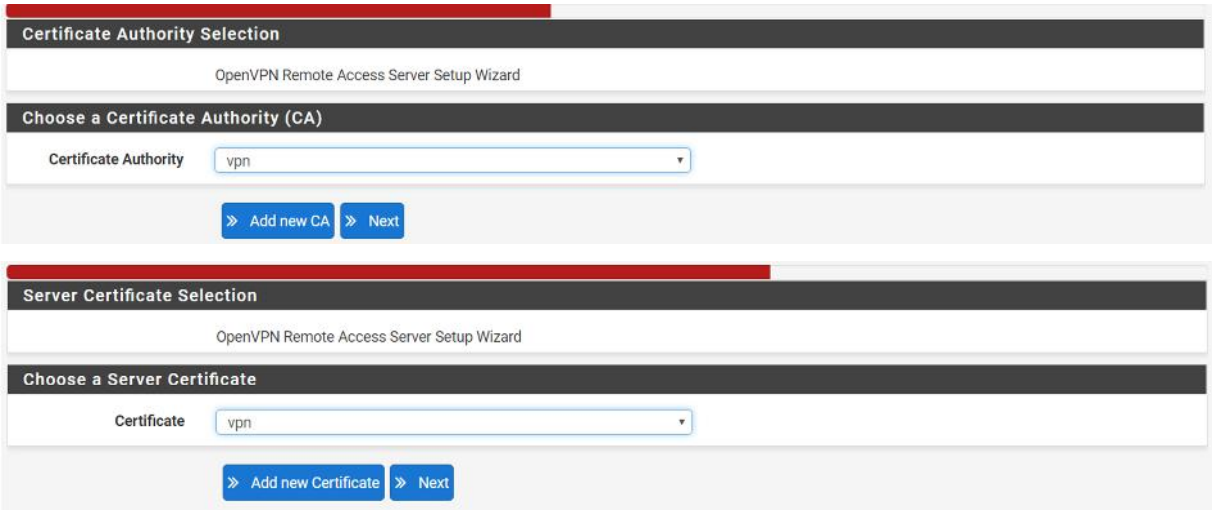


Figure III.20 : Le certificat du serveur

Nous choisissons aussi l'interface réseau qui est le WAN et nous spécifions le type de protocole de transmission (UDP), ainsi le numéro du port (qui est le 1194 par défaut).

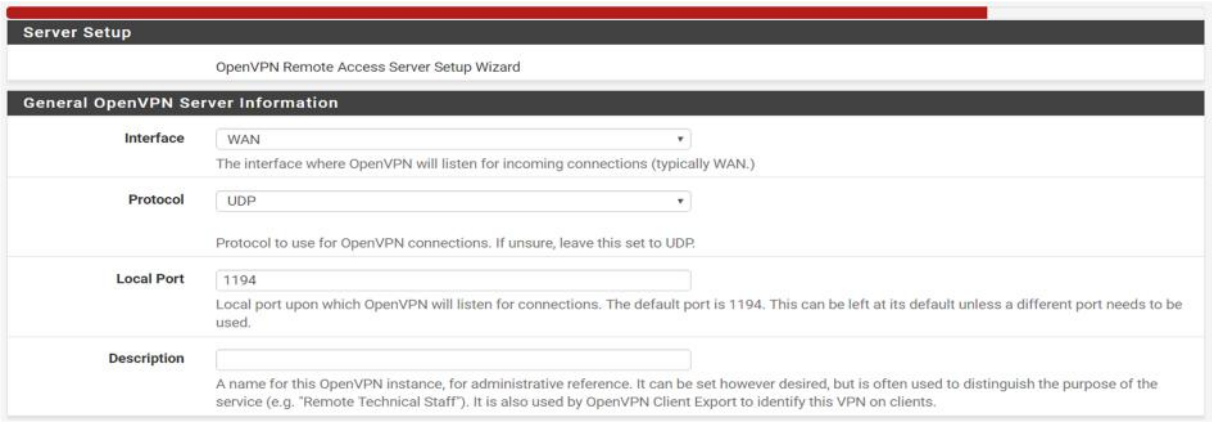


Figure III.21 : Information sur le serveur

On choisit les algorithmes de cryptographie

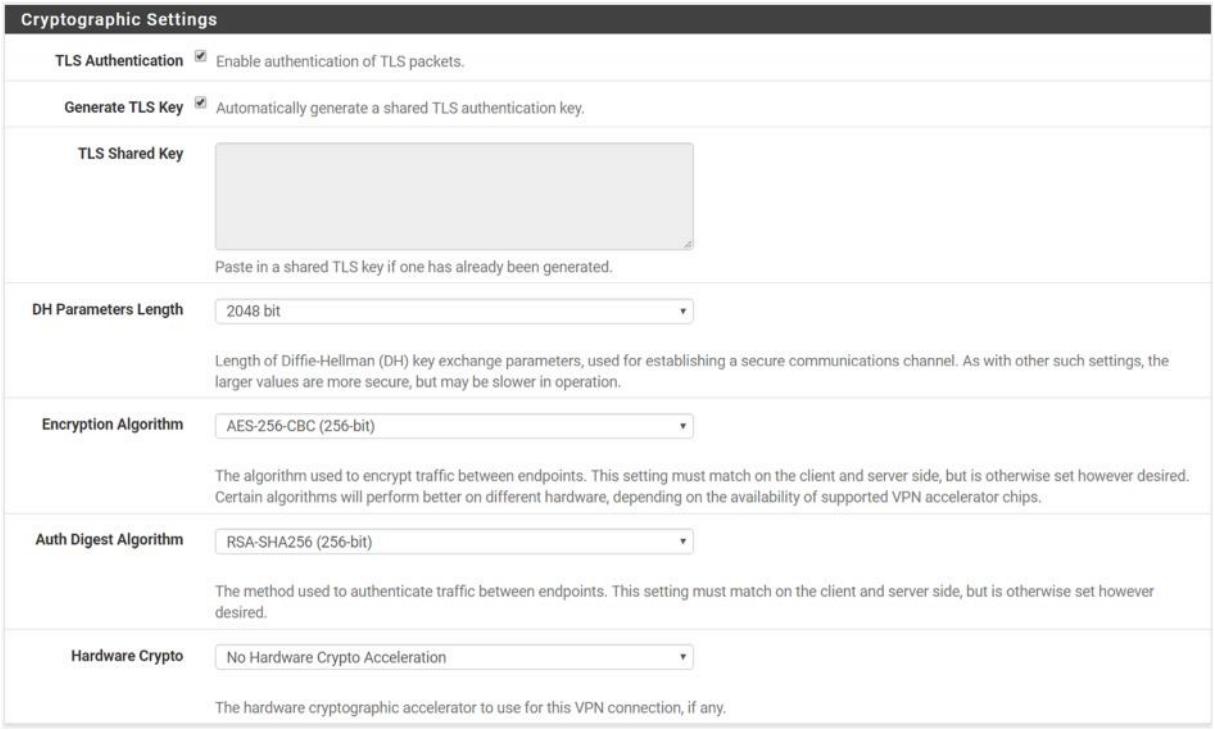


Figure III.22 : La cryptographie

III.4.4. Création et configuration du tunnel VPN

Le champ tunnel network correspond à l'adresse IP privée dans le tunnel VPN qui fera la liaison entre l'utilisateur et le réseau LAN

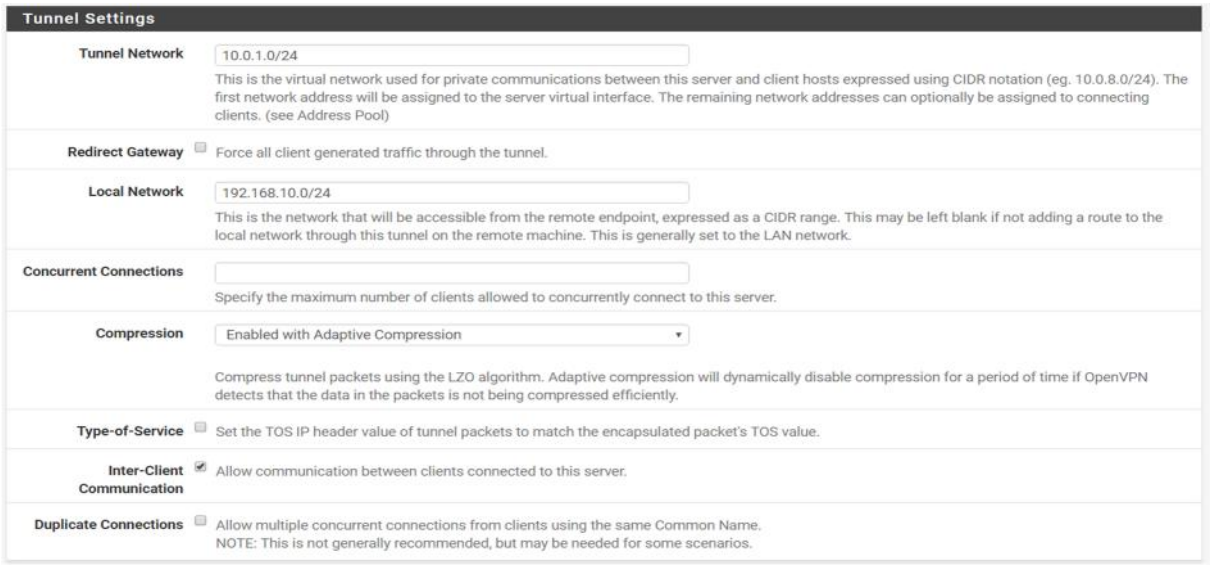


Figure III.23 : création du tunnel

Pour l'activation des pare-feu par défaut, il faut cocher les cases pour Firewall rule et OpenVPN rule

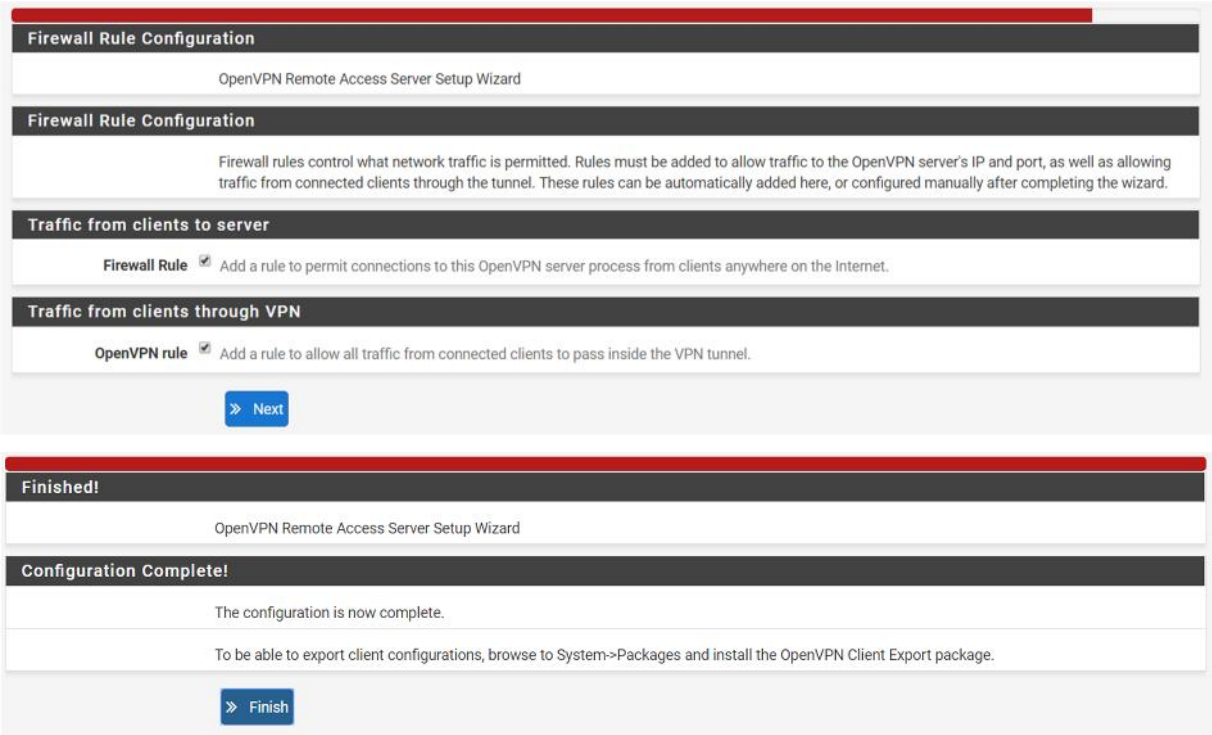
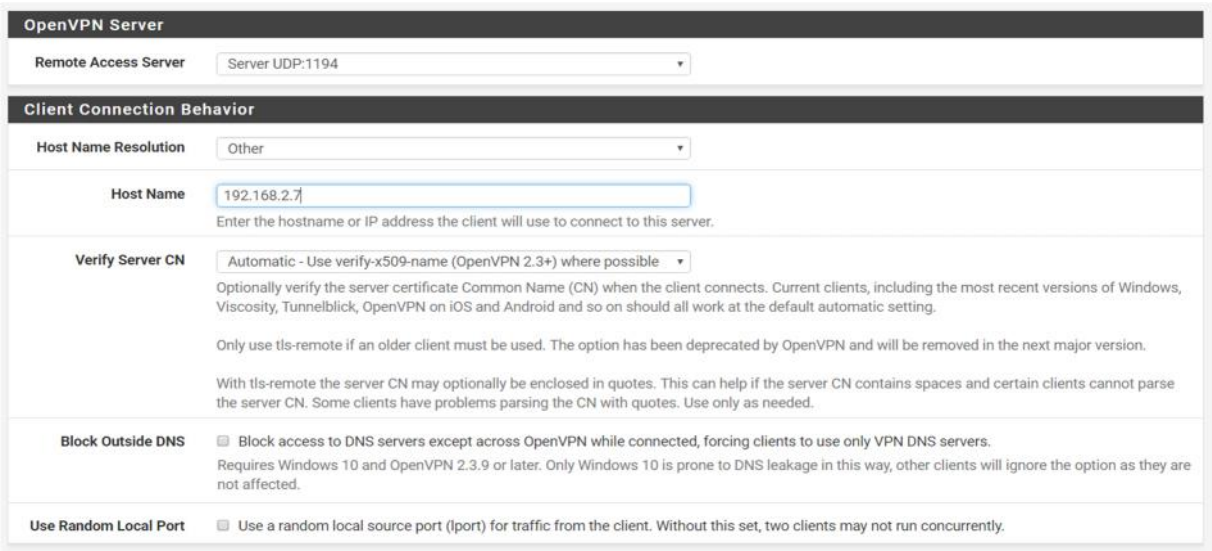


Figure III.24 : Activation du pare-feu

Cliquer sur « next »puis « finish »

A fin d'exporter le protocole Openvpn sur la machine cliente, en clic sur « standard de configuration » =>archive sur la figure III.25.



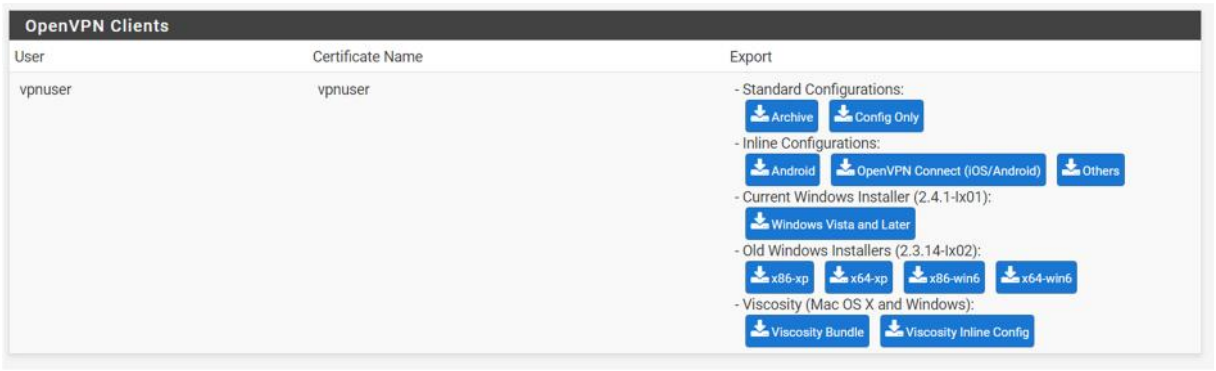


Figure III.25 : Formulaire du serveur OpenVPN

III.5. Reconfiguration du modem :

A fin d'autoriser l'accès à l'utilisateur externe, nous devons apporter une modification dans la configuration des ports du modem.

- Affectation du port pour l'utilisateur externe :

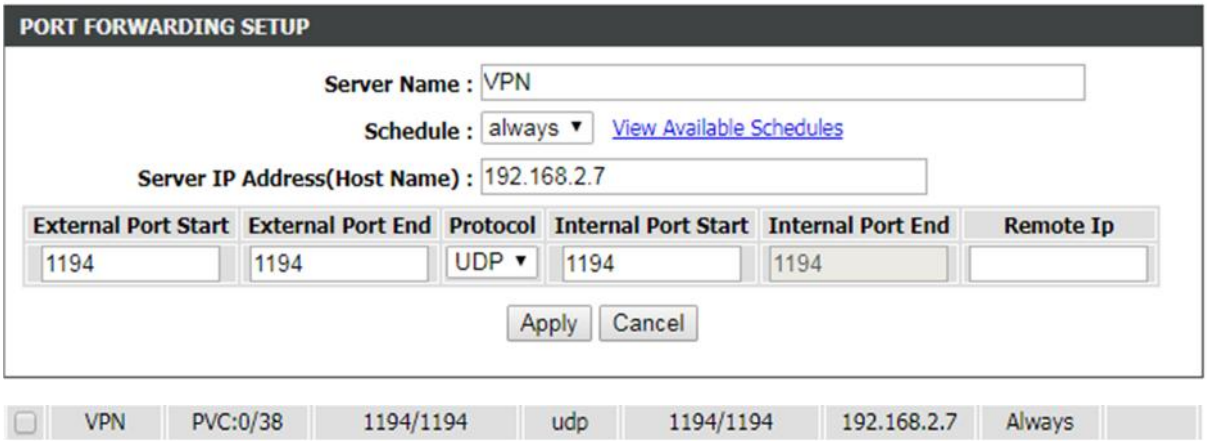


Figure III.26 : Configuration de transfert de port

III.6. Installation d'OpenVPN sur la machine de l'utilisateur :

On lance l'installation d'OpenVPN sur la machine.

Figure III.27 : Istallation de openVPN

Lorsque OpenVPN est en cours d'exécution, nous avons ce petit symbole de verrouillage et d'écran sur notre barre des tâches. On clic droit dessus et on choisit "Connecter" pour se connecter à notre serveur vpn.

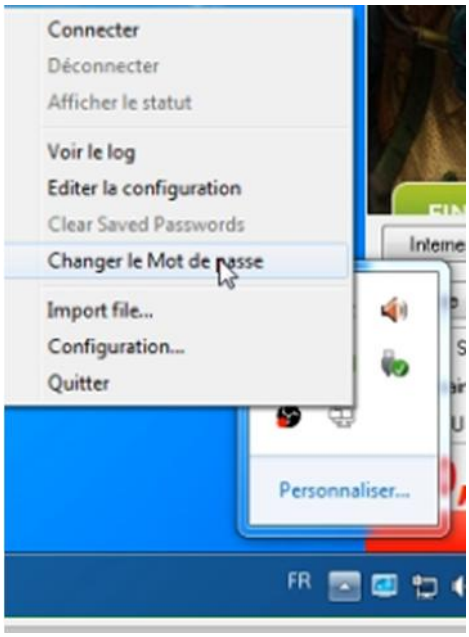


Figure III.28 : choix dans la Barre des taches

Pour accéder au VPN, l'utilisateur doit remplir la table d'authentification en utilisant les mêmes informations configurées dans le certificat.

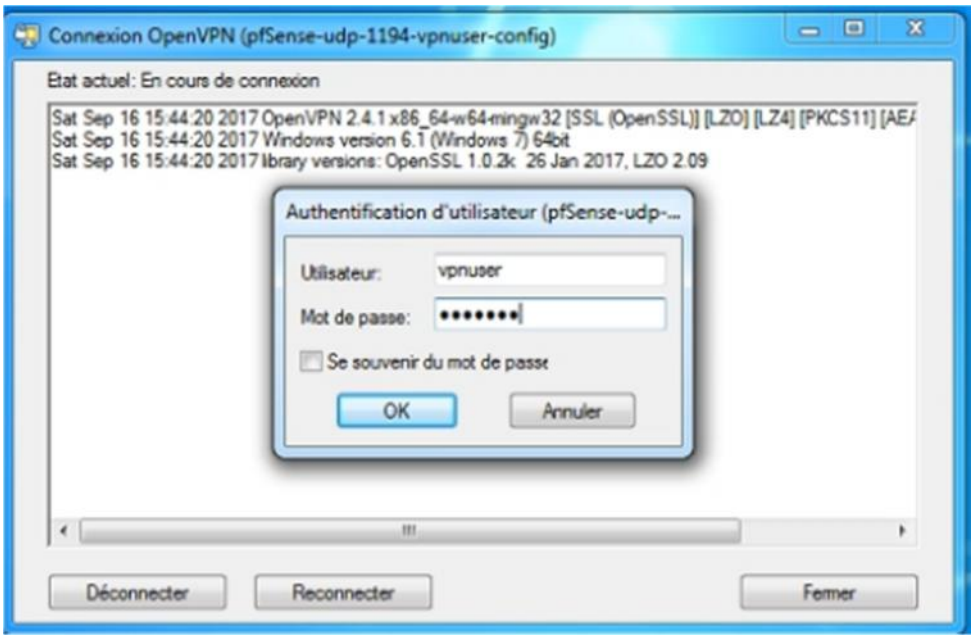


Figure III.29 : Identification du VPN

A fin de s'assurer du fonctionnement du VPN, on effectue les tests de connectivités entre l'utilisateur et le serveur VPN ainsi que le client en utilisant la commande « ping » sous l'invité de commande.

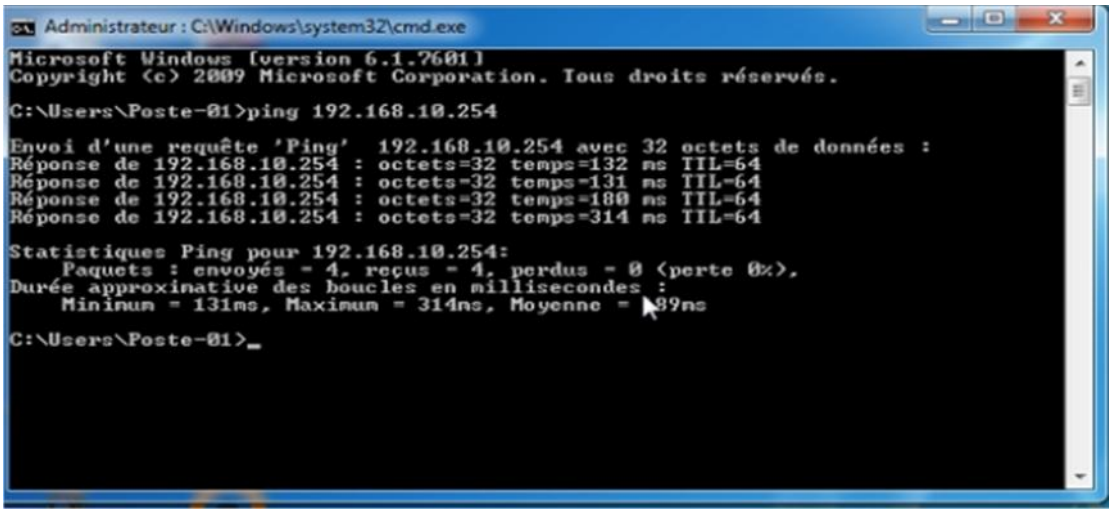


Figure III.30 : Test de connectivité 1

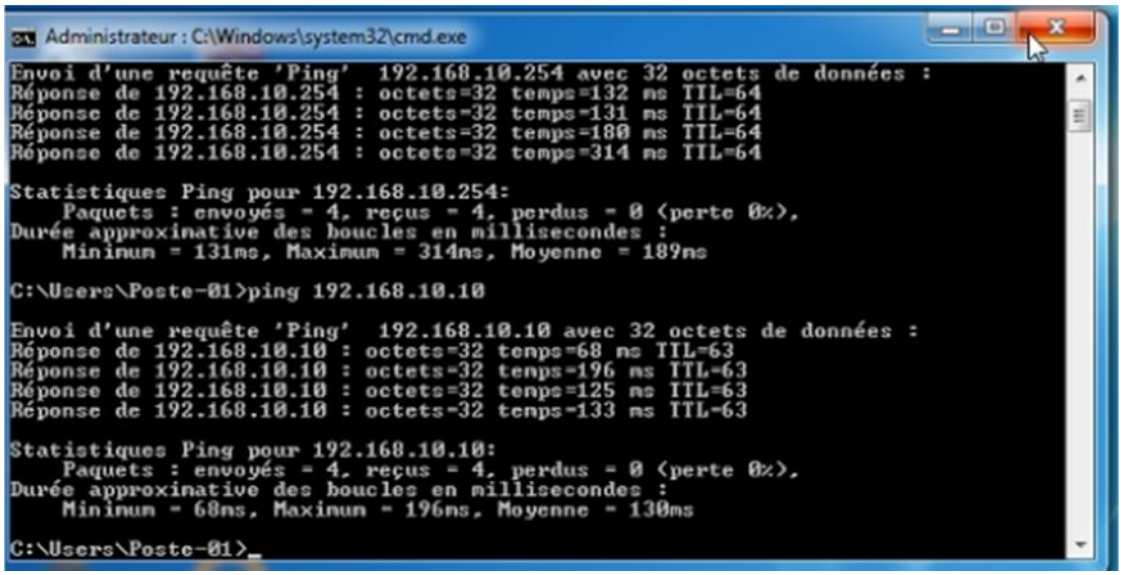


Figure III.31 : Test de connectivité 2

Au cours de ce dernier chapitre nous avons réalisé un réseau VPN nous permettons l'accès a distance vers un réseau LAN.

Nous avons commencé par installer le logiciel de vitalisation « Vmware » afin de pouvoir créer et configurer notre réseau LAN qui sera constitué d'un par-feu pfsense implémenté sur un serveur et un client. Ensuite nous somme passé à la configuration du client utilisateur qui pourra se connecter à distance vers notre réseau.

Nous constatons selon les résultats des « Ping », que l'utilisateur est bien connecté à notre réseau.

Conclusion générale

Le besoin croissant des entreprises de communiquer entre des sites distants a donné naissance aux VPN. En effet, la raison d'être des VPN est d'offrir aux utilisateurs et aux administrateurs d'un système d'informations, les mêmes conditions d'utilisation, d'exploitation et de sécurité à travers un réseau public que celles disponibles sur un réseau privé.

Le VPN est une technologie révolutionnaire et complexe qui repose sur l'utilisation de divers protocoles de « tunneling »assurant un niveau de sécurité plus ou moins élevé.

Le secteur des technologies de l'information étant en constante mutation, le présent travail fait état des résultats obtenus lors de la mise en place d'un réseau VPN d'accès. Nous avons en effet grâce à cette nouvelle technologie permis à un utilisateur l'accès à distance vers un réseau privé à fin de partager de façon protégés leurs données via les protocoles de sécurité qui sont les principaux outils permettant d'implémenter le VPN, ce partage était possible en interne pour les utilisateurs du réseau local de l'entreprise, mais aussi en externe pour les utilisateurs dit « distants » situés en dehors du réseau local.

En effet, la mise en place de VPN permet aux réseaux privés de s'étendre et de se relier entre eux au travers d'internet. Cette solution mise en place est une politique de réduction des coûts liés à l'infrastructure réseau des entreprises. Il en ressort que la technologie VPN basée sur le protocole de sécurité comme IPsec et OpenVPN est l'un des facteurs clés du succès qui évolue et ne doit pas aller en marge des infrastructures réseaux sécurisés et du système d'information qui progressent de façon exponentielle.

Bien que nous n'ayons pas mis en pratique notre proposition pour des raisons matérielles évidentes la suite logique de ce travail consisterait à :

- Mettre en place notre réseau VPN.
- Étudier de façon approfondie les failles de ce système à fin de développer l'aspect de sécurité et de confidentialité de ce dernier.

Ce travail nous a permis d'acquérir et d'enrichir nos connaissances et nos compétences dans de nombreux domaines, il nous a initié au monde de la recherche sur les réseaux surtout ce qui concerne leur sécurisation. Nous nous somme initiées à la ritualisation ainsi que la mise en place des réseaux VPN et la configuration de ses protocoles.

CONCLUSION

M^elle Sadoud lila, M^elle Saddedine Malika, Mémoire de fin d'études en master 2 réseaux et télécommunications, implémentation d'une solution d'interconnexion entre deux forets différents avec une relation d'approbation et VPN site à site.

M^elle Tinhinane Tebani, mémoire de fin d'études en master 2 réseaux et télécommunications, simulation d'un tunnel VPN-SSL pour la sécurisation de deux réseaux LANs.

Share VB Sécurité GNU/Linux Virtual Private Network à partir du site

www.bestcours.com/reseaux/vpn/

Eric BAHATI – shabani , Mise-en-place-dun-reseau-VPN- à partir du site

www.memoireonline.com

M^elle Ait dahmane Nouara,M^elle Chekkal Saida, Mémoire de fin d'études en master 2 réseaux et télécommunications ,Mise en place d'un tunnel VPN imlémenté sur ASA Cisco.

Mr Touradj Ebrahimi ,Mr Franck Leprévost,Mr Bertrand Warusfel, ouvrage en cryptografie et sécurité des systèmes et réseaux.

Mr Donald Sottin, mémoire en ligne, Implimentation de VPN sous Linux Ubuntu.

https://openclassrooms.com/courses/creer-son-propre-serveur-vpn-avec-open-vpn

CONCLUSION

LISTE DES FIGURES

LISTE DES FIGURES

M^elle L.Sadoud , M^elle M.Saddedine, Mémoire de fin d'études en master 2 réseaux et télécommunications, implémentation d'une solution d'interconnexion entre deux forets différents avec une relation d'approbation et VPN site à site.

M^elle T. Tebani, mémoire de fin d'études en master 2 réseaux et télécommunications, simulation d'un tunnel VPN-SSL pour la sécurisation de deux réseaux LANs.

Share VB Sécurité GNU/Linux Virtual Private Network à partir du site

Eric BAHATI – shabani , Mise-en-place-dun-reseau-VPN- à partir du site

M^elle N.Ait dahmane ,M^elle S.Chekkal, Mémoire de fin d'études en master 2 réseaux et télécommunications ,Mise en place d'un tunnel VPN imlémenté sur ASA Cisco.

Mr T. Ebrahimi ,Mr F.Leprévost,Mr B. Warusfel, ouvrage en cryptografie et sécurité des systèmes et réseaux.

Mr D.Sottin, mémoire en ligne, Implimentation de VPN sous Linux Ubuntu.

https://openclassrooms.com/courses/creer-son-propre-serveur-vpn-avec-open-vpn

www.bestcours.com/reseaux/vpn/

www.memoireonline.com