REPUBLIQUE **A**LGERIENNE **D**EMOCRATIQUE **E**T **P**OPULAIRE

MINISTERE DE L'**E**NSEIGNEMENT **S**UPERIEUR ET DE LA **R**ECHERCHE

SCIENTIFIQUE

UNIVERSITE **M**OULOUD **M**AMMERI DE **T**IZI-**O**UZOU

FACULTE DU **G**ENIE **E**LECTRIQUE ET D'**I**NFORMATIQUE
DEPARTEMENT D'**E**LECTRONIQUE

Mémoire de Fin d'Etudes
De MASTER ACADEMIQUE

Domaine : **Sciences et Technologies F**ilière : **Génie électrique**

Spécialité : **Télécommunication et réseaux**

Thème

Installation et configuration d'un Firewall Logiciel [Pfsense] « ENIEM »

Présenter par :

Messahel Nouara
Saadi Khadra

Dirigé par :

Mme. LAHDIR

Promotion : 2016/2017

Remerciements

Nous remercions dieu tout puissant qui nous à donner la force et surtout la patience d'arriver au bout de notre travail.

Du fond du cœur nous remercions nos chers parents qui nous ont toujours guidé, encouragé et qui ont fait de leurs mieux pour que nous arrivons là aujourd'hui.

Nous remercions notre promotrice Mme LAHDIR pour son aide tout au long de notre travail .comme nous tenons à le remercie pour ses encouragements, son soutien et ses précieux conseils et orientations.

Nous remercions également tout le personnel d'entreprise ENIEM en particulier Mr TALEB, pour leur contribution et pour la documentation mise à notre disposition.

Nous adressent nos sincères remerciements pour les membres de jury d'avoir accepté d'examiner et d'évaluer notre travail.

Nous remercions tous ceux qui ont contribué à notre formation au niveau de l'université, en particulier les professeurs et tous ceux nous aidé de loin et près à mener à terme ce travail.

Dédicaces

Je dédie ce modeste travail réalisé à dieu à :

Ma très chère mère qui a été toujours à mes coté et qui me donne que le soutien, beaucoup d'amour, le courage pour avoir cette réussite et bien sûr à mon père qui a été la source de ma volonté.

- *A ma sœur : Ouiza ;*
- *A ma grand-mère YammaNouara et ma grand-mère yamma djida qu'elle repose en paix ;*
- *A mon grand frère Ouali et sa femme Djoudjou et à mon petit frère Fateh.*
- *A tous mes amis : Ouiza ; Saadia ; Dihia ; Hayet ; Kenza ; Nassima ; Saliha ; Fatiha; Sofiane ; Cherif ; et à mon binôme Khadra et sa famille ;*
- *A toute la promotion 2017 ;*
- *A toute personne ayant contribué de près ou de loin à la réalisation de ce travail.*

Nouara

Dédicaces

Je dédie cet humble travail :

- *A mes chères parentes*
- *A mes frères et mes sœurs*
- *A toute ma famille*
- *A toute mes amis*

Khadra

Sommaire

Chapitre I : généralité sur les réseaux

Chapitre II : sécurité de réseaux informatique.

Chapitre III : Application.

Bibliographe

GLOSSAIRE

LAN : Local Area Network

MAN : Metropolitain Area Network

WAN : Wide Area Network

P2P : Peer To Peer

CSMA/CD : Carrier Sense Multiple Access/Collision Detection

MAC : Media Access Control

OSI : Open System Interconnexion

TCP/IP : Transmission Control Protocol/Internet Protocol

HTTP : HyperText Transfer Protocol

SMTP : Simple Mail Transport Protocol

POP : Post Office Protocol

Telnet : Terminal **net**work ou Télécommunication network

IMAP : Internet Message Access Protocol

FTP : File Transfer Protocol

NNTP : Network News Transfer Protocol

UDP : User Datagram Protocol

ARP : Adress Resolution Protocol

IGMP : Internet Group Management Protocol

DHCP : Dynamic Host Configuration Protocol

RARP : Reverse Address Resolution Protocol

ICMP : Internet Control Message Protocol

VLAN : Virtual Local Area Network

IEEE : Istitute of Electrical and Electronics Engineers

GLOSSAIRE

DNS : Domain Name System

DOS : Denial Of Service

SSL : Secure Sockets Layer

SSH : Secure Shell

IPSec : Internet Protocol Security

HTTPS : HyperText Transfer Protocol Secure

PKI : Public Key Infrastructure

CA : Certificate Authority

IDS : Intrusion Detection services

IPS : Intrusion Prevention Services

SI : Informatique System

VPN : Virtual Private Network

MPLS : Muli Protocol Label Switching

IP : Internet Protocol

IPX : Internetwork Packet Exchange

ACL : Access Control List

CD/DVD : Compact Disc/Digital Versatile Disc

DMZ : Demilitarized Zone

NAT : Network Address translation

PAT : Port Address Translation

TLS : Transport Layer Security

URL : Uniform Ressource Locator

QOS : Quality Of Service

GLOSSAIRE

BSD : Berkeley Software Distribution

PFSense : Packet Filter Sense

Liste des figures

Liste des figures

Introduction Générale

De nos jours, l'informatique est devenue un outil incontournable de gestion, d'organisation, de production et de communication. Le réseau informatique est devenu un outil indispensable pour chaque entreprise aujourd'hui,elle possède de nombreux postes informatiques qui sont reliés entre eux par un réseau. Ce réseaud'entreprise met en œuvre des données sensible, les stocke, les partages entre les divers collaborateurs internes de l'entreprise.

La possibilité de travail collaboratif entre entreprises fait l'ouverture de leurs systèmes d'information à leur partenaire ou à leur fournisseur, il est donc essentiel de connaitre les ressources de l'entreprise à protéger et de maitriser le contrôle d'accès et les droits des utilisateurs du système d'information.

L'ouverture de l'accès de l'entreprise sur internet provoque plusieurs attaques et pour se protéger contre ces derniers, une architecture de réseau sécurisée est nécessaire, tel qu'un pare-feu. Cet outil a pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les tentatives d'intrusion pour ce protégé le mieux possible. Cela permet de rendre le réseau ouvert sur Internet beaucoup plus sûr. Le firewall propose donc un véritable contrôle sur le trafic réseau de l'entreprise. Il permet d'analyser, de sécuriser et de gérer le trafic réseau, et ainsi d'utiliser le réseau de la façon pour laquelle il a été prévu.

L'objectif principal de notre projet est basé sur la sécurité de l'entreprise ENIEM contre les menaces extérieures avec un cout minimal, en utilisant un pare-feu logiciel «Pfsense ». Donc nous avons fait l'installation et la configuration de notre pare feu sur un réseau composé par un ensemble de machines virtuelles.

Notre mémoire est structuré en trois chapitres :

Le premier chapitre intitulé « les généralités sur les réseaux informatique ».dans lequel, nous allons expliquer en détail les différents éléments d'un réseau tel que : définition d'un réseau, les différents types de réseaux, les catégories des réseaux, les types de supports de transmissions, architecteur des réseaux, les VLANS.

Le deuxième chapitre sera basé sur la sécurité des réseaux informatique. Dans ce chapitre, nous allons définir la sécurité informatique, l'objectif de la sécurité, typologie des

attaques réseau, les types de menaces, les protocoles de sécurité, méthode de défenses, VPN, Firewall.

Le troisième chapitre sera consacré en premier lieu à l'installation de la machine virtuel « virtualbox » par la suite nous allons définir notre solution pare-feu « le pfsense », son fonctionnement son installation et sa configuration.

Et en fin, nous terminons notre mémoire par une conclusion générale ainsi que des perspectives.

I. Préambule :

Toute entreprise possède aujourd'hui un ou plusieurs système de télécommunication qui véhiculant les différentes informations nécessaires à son fonctionnement. Ces systèmes sont organisés sous forme de réseaux locaux, qui utilisent des protocoles simples qu'on peut définir comme des ensembles d'équipements et de supports de transmission dont une des fonctions est le transfert d'informations. [8]

En informatique deux ordinateurs reliés entre eux par un câble forment déjà un réseau. Dans ce chapitre, nous allons expliquer les différents éléments d'un réseau et leurs caractéristiques.

I.1.Définition d'un réseau informatique :

Un réseau informatique est un ensemble d'équipements informatiques (ordinateurs et périphériques) autonomes connectés entre eux grâce à des supports de communication et qui sont situés dans un certain domaine géographique, afin que les utilisateurs et les applications qui fonctionnent sur ces dernières puissent échanger des informations.

Un réseau informatique à plusieurs buts distincts :

- ✓ Décrire la façon dont les machines d'un site sont interconnectées ;
- ✓ Spécifier les protocoles qui sont utilisés pour que les machines communiquent.
- ✓ Le partage de ressources (fichiers, application ou matériel, connexion à internet etc.) ;
- ✓ La communication entre personne (courrier électrique, discussion en direct etc.) ;
- ✓ La communication entre processus (entre les ordinateurs par exemple) ;
- ✓ La garantie de l'unicité et de l'universalité de l'accès à l'information (base de données en réseau). [11]

I.2.Les différents types de réseaux :

On distingue différents types de réseaux selon leurs tailles, leurs vitesses de transfert des données ainsi que leurs étendues. En générale on a trois catégories de réseaux :

- ✓ Les réseaux locaux **LAN (Local Area Netwok) :** Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique.

- ✓ Les réseaux **MAN (Métropolitain Area Network) :** correspond à la réunion de plusieurs réseaux locaux(LAN) à l'intérieur d'un même périmètre pouvant relier des points distants de 10 à 25 Km. En générale le support physique le plus utilisé dans ce type de réseau est le câble coaxial.
- ✓ Les réseaux étendus **WAN (Wide Area Network)** : Il s'agit d'un réseau multiservices couvrant un pays ou un groupe de pays, qui est en fait constitué d'un ensemble de réseaux locaux interconnectés. Un WAN peut être privé ou public. [11]

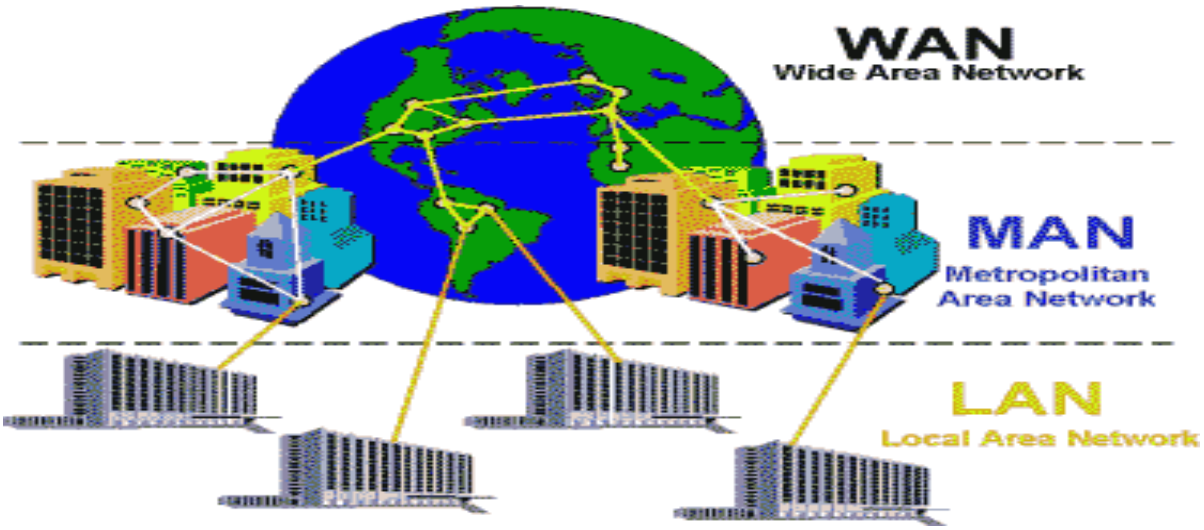


***Figure I.1** : Les différents types de réseaux.*

I.3.Les architectures des réseaux :

On distingue également deux architectures de réseaux :

- ➢ Réseaux poste à poste (peer to peer= P2P).
- ➢ Réseaux avec serveur dédié (Server/client).

I.3.1.Réseaux poste à poste :

Dans cette architecture les données ne sont pas centralisés et tous les ordinateurs connectés ont le même statut et se partagent toute l'information et tous les services sans l'aide d'un serveur.

I.3.2.Les réseaux organisés autour d'un serveur (client/serveur) :

Tous les ordinateurs (clients) sont reliés à un serveur dédié qui centralise les données relatives au bon fonctionnement du réseau et ils ne partagent pas les mêmes informations (par exemple un client a le droit de se connecté à Google mais n'a pas l'accès aux autres sites). [15]

I.4. Les topologies des réseaux :

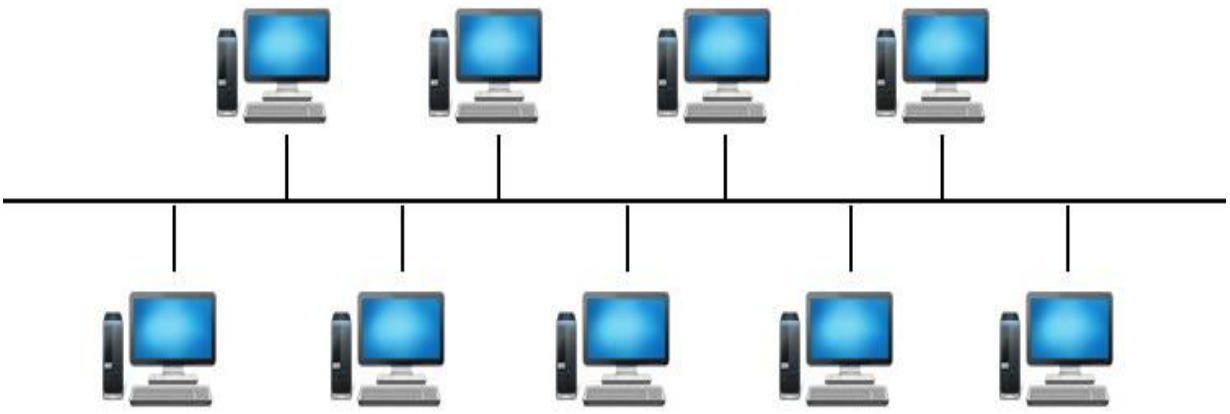
La topologie des réseaux est la façon dont les ordinateurs sont interconnectés entre eux grâce au matériel (câblages, cartes réseaux, autres équipements permettant d'assurer la bonne circulation des données).

Il existe deux topologies :

I.4.1.Topologie physique :

La topologie physique concerne la façon dont les machines sont connectées (Bus, Anneau, Étoile ….).

a – en bus : Dans cette topologie, tous les ordinateurs sont reliés à une même ligne de transmission par l'intermédiaire d'un câble coaxial. Cette topologie a pour avantages d'être facile à mettre en œuvre et de fonctionner facilement, par contre elle est extrêmement vulnérable étant donné que si l'une des connexions est défectueuses, c'est l'ensemble du réseau qui est affecté.[21]



***FigureI.2** : Topologie en bus.*

b- en étoile : Dans cette topologie, les ordinateurs du réseau sont reliés à un périphérique central tel qu'un Hub ou un concentrateur. Les réseaux suivant une topologie en étoile sont

moins vulnérables que la topologie en bus car on peut facilement retirer une des connexions en la débranchant du concentrateur sans paralyser le reste du réseau.

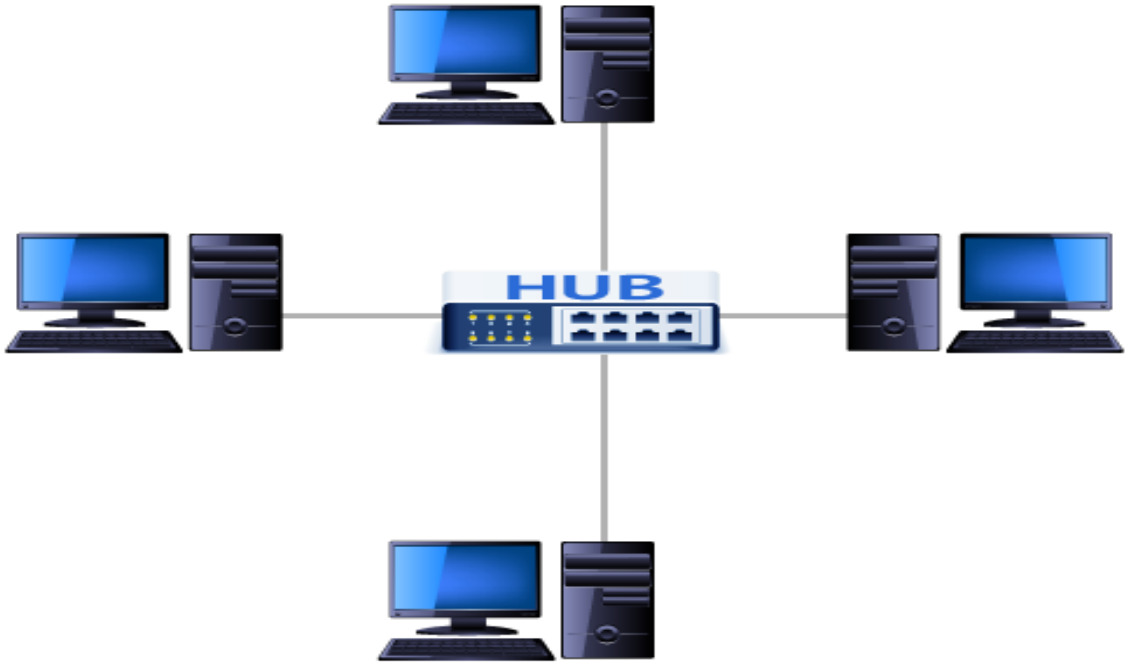


Figure I.3 *: Topologie en étoile.*

c- en anneau :

Dans cette topologie, chaque nœud est relié à deux autre nœuds qui sont poches de lui (cette elle vise le raccordement des ordinateurs), et l'ensemble du réseau forme un cercle les données sont transmises.

Autour de l'anneau dans une seul direction chaque station de travail accepté et répond aux paquets qui lui sont adressés, puis les fait suivre à la prochaine station de l'anneau. Dans ce cas le retrait ou la panne d'une entité active paralyse le trafic du réseau et elle est difficile d'insérer une nouvelle station.

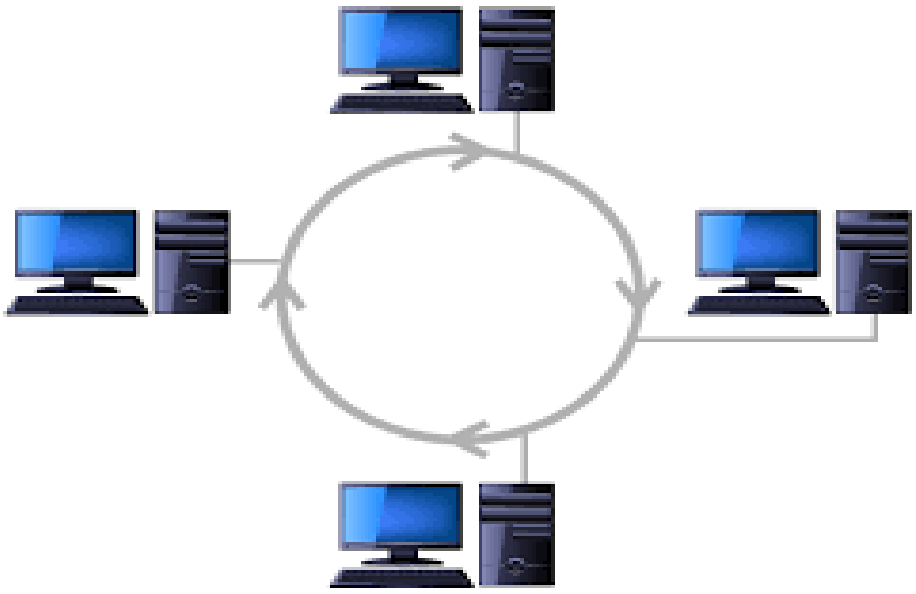


***Figure I.4**: Topologie en anneau.*

I.4.2.Topologie logique :

La topologie logique montre comment les informations circulent sur le réseau (diffusion ou point à point). Cette topologie s'appelle aussi un système de transport réseau. Elle décrit la manière par laquelle les données sont mises en trames et comment les impulsions électrique sont envoyées sur le support physique du réseau et les éléments d'une topologie logique appartiennent à la fois aux couche liaison du modèle OSI.

Donc nous avons deux normes de réseaux a distingué : la norme Ethernet et la norme Token Ring.

- ✓ **La norme Token Ring (accès par jeton):**

Elle fonctionne sur un réseau en anneau, sur un tel réseau, un ordinateur doit capturer une trame spéciale appelée jeton. Le jeton circule et passe de nœud en nœud d'une manière séquentielle, seul le détecteur de jeton qui doit transmettre un message. Avec cette méthode on peut envoyer des données sans avoir de collisions (elle évite les collisions).

- ✓ **La norme Ethernet :**

Elle est basée sur la gestion des collisions. Cette norme va définir la méthode d'accès CSMA/CD (Carrier Sense Multiple Access/Collision Détection)

- ✓ **La méthode d'accès CSMA/CD :**

CSMA/CD (accès multiple avec écoute de porteuse et détection de collision), il s'agit de la technique de contrôle pour l'accès au support physique utilisé par les réseaux Ethernet et 802.3, elle détermine quand et comment un paquet de données est situé dans le câble.
Son principe est celui de la politesse : on parle que quand personne ne parle. [4]

I.5.Les types de supports de transmissions :

Afin que les informations circulent au sien d'un réseau, il est nécessaire de relier les différentes unités de communications à l'aide d'un support de transmission. Le support de transmission est un canal physique permettant de relier des ordinateurs et des périphériques. Les supports les plus utilisés sont : la fibre optique, le câble a paire torsadée et le câble coaxial.

I.5.1. Le câble à paire torsadées :

Le câble a paire torsadée est une ligne symétrique formée de deux fils conducteurs enroulés l'un sur l'autre. La paire torsadées a quatre brins de cuivre entrelacés deux par deux et chaque couple de c'est brins a deux blindages et les tout enroules dans une enveloppe isolante. La paire torsadée permet une meilleure protection du signal électrique car les fils sont torsadés de sorte que le câble était moins sujet à des perturbations électromagnétiques. La paire torsadée est utilisée pour les câbles internet ou de téléphone. Elle se branche à l'aide d'un connecteur Rj-45. [28]

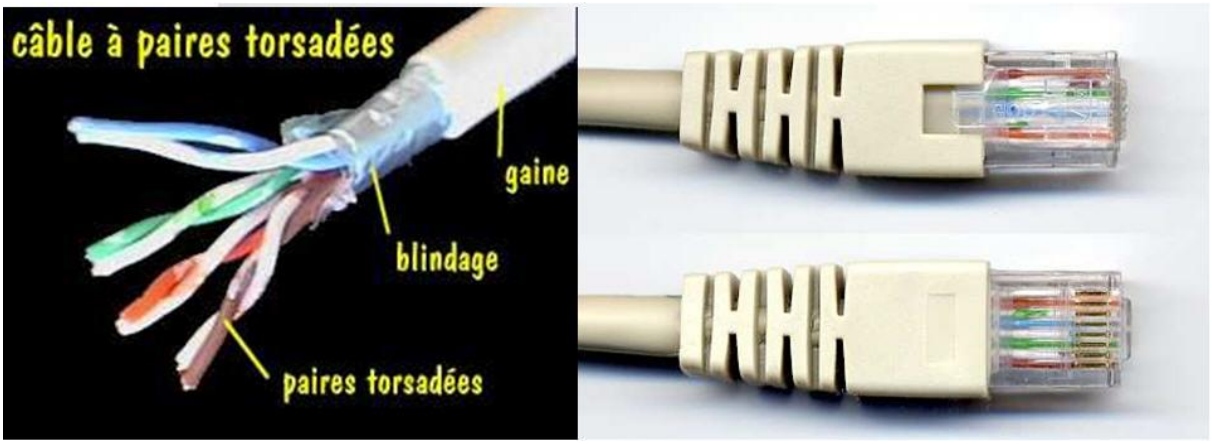


Figure I.5 : câble à paire torsadée

I.5.2.Le câble coaxial :

Pour éviter les perturbations dues aux bruit externes, on utilise souvent deux conducteurs cylindriques de même axe, séparés par un isolant, et qui forment un ensemble appelé câble coaxial ou ligne coaxial. Le câble coaxial présente de meilleur caractéristique que le câble a paire torsadée, et également le support le plus largement employé pour le transport par fil de signaux de radiofréquence élevée, en particulier les signaux de télévision par câble.

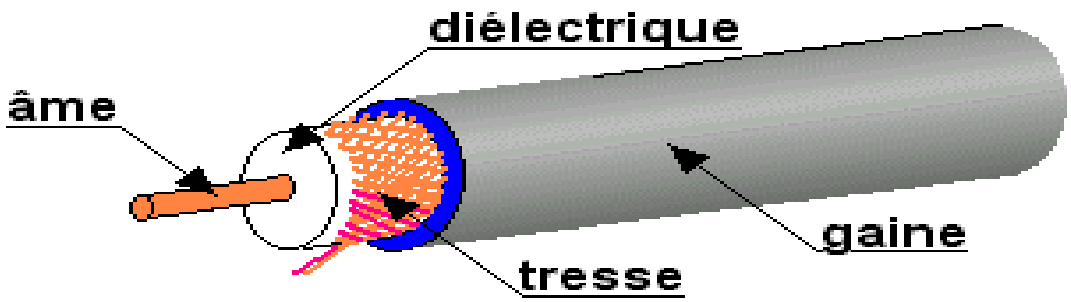


Figure I.6 : ligne ou câble coaxial

I.5.3.La fibre optique :

Depuis quelques années, la fibre optique a été fortement introduite comme support de transmissions terrestres de données, d'images et même de la voix

Une fibre optique est constituée d'un fil de verre très fin à basse de silice. Elle comprend un cœur dans lequel se propage la lumière, une impulsion lumineuse représente l'information binaire 1 tandis que l'absence de lumière représente l'information binaire 0.

La fibre optique elle a deux types : la fibre optique monomode à saut d'indice (elle transport un seul rayon lumineux) et la fibre optique multimode à gradient d'indice (la lumière voyage en modes multiples). [9]

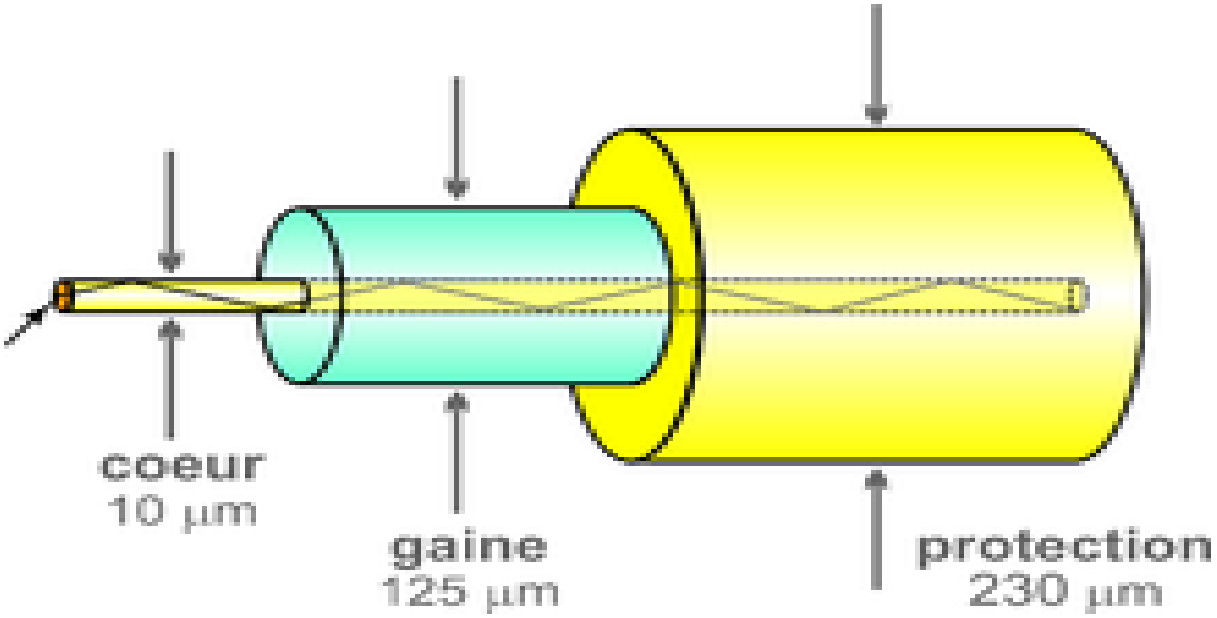


Figure I.7 : la fibre optique

I.6.Les équipements d'interconnexion du réseau :

Les réseaux hétérogènes formant Internet sont reliés entre eux grâce à des dispositifs d'interconnexion (Passerelle, Routeur, Ponts…) qui assurent le transfert des données.

- **Les routeurs :**

  Ce sont des dispositifs matériels ou logiciels, permettant de choisir le chemin qu'un message doit emprunter. De plus, ils permettent de manipuler les données (qui circulent sous forme de datagramme) afin de pouvoir assurer le passage d'un type de réseau à un autre .Ainsi, les réseaux ne peuvent pas faire circuler la même quantité simultanée d'information en termes de taille de paquets de données.

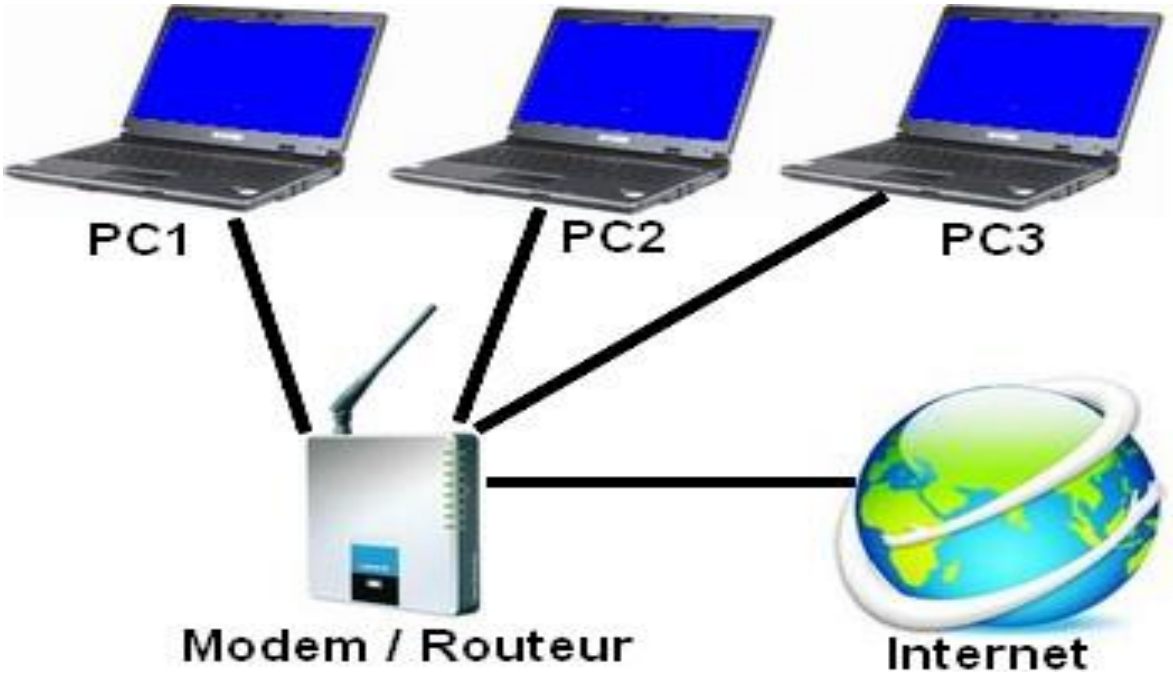


Figure I.8: *Routeur connectés à deux réseaux.*

- **Les Hubs (concentrateur) :**

Le Hub est également appelé concentrateur. C'est un boitier électronique assurant la liaison des postes et des périphériques du réseau. Il contente de transférer les ressources qui lui arrivent vers tous les autres éléments du réseau.

Lorsqu'une information arrive sur un Hub, elle est rediffusée vers toutes les destinations possibles à partir de celui-ci, c'est à dire vers toutes ses prises.

- **Les Switch (commutateur) :**

C'est un boitier électronique assurant la liaison et l'optimisation des échanges entre les éléments du réseau. Contrairement au Hub, le Switch est capable d'orienter les ressources vers leur unique destinataire sur le réseau. Le Switch permet de libérer la bande passante en évitant ainsi le transfert de donnés inutiles sur le réseau.

- **Switch fédérateur :**

Un Switch fédérateur est un Switch qui regroupe plusieurs Switch utilisateurs et Switch serveurs et c'est à lui de gérer ces réseaux et il est connecté par des routeurs qui ont l'accès vers des réseaux externe donc c'est un nœud administratif qui contient plusieurs branches et c'est la partie importante après le routeur dans un réseau. [30]

❖ **Switch de niveau 2 et niveau 3 :**

Un Switch niveau 2 ne fait que de la commutation au niveau des adresses MAC et si on crée un VLAN, chaque VLAN seront isoler par contre un Switch niveau 3, il permet d'assigner une adresse IP par Vlan et de pouvoir faire du routage Inter Vlan. Un Switch niveau 3 a la fonctionnalité d'un routeur.

❖ **Les ponts :**

Ce sont des dispositifs matériels ou logiciels, permettant de relier des réseaux travaillant avec les mêmes protocoles. De plus ils filtrent les informations et ne laissent passer que celles qui doivent effectivement aller d'un réseau vers un autre. Ils peuvent être utilisés pour augmenter les distances de câblage en cas d'affaiblissement prématuré du signal.

Un pont possède deux connexions à deux réseaux distincts. Lorsqu'il reçoit un paquet donné sur l'une de ses interfaces, il analyse l'adresse physique(MAC) du destinataire et de l'émetteur. Si le pont ne connait pas l'émetteur, il stocke son adresse dans une table afin de se souvenir de quel côté du réseau se trouve l'émetteur. [30]

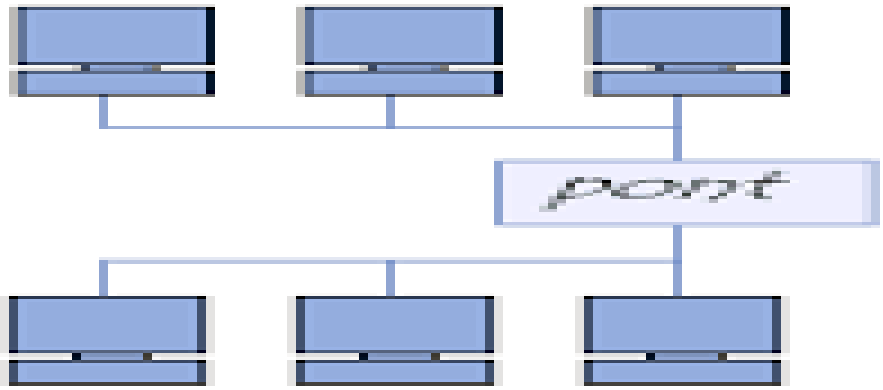


Figure I.9 : deux réseaux relient avec un pont.

❖ **Les passerelles :**

Ce sont des système matériels ou logiciels permettant de faire des liaisons entre plusieurs réseaux de protocoles différents (par exemple un réseau local et le réseau internet), lorsqu'un utilisateur distant contacte un tel dispositif, ce dernier examine sa requête et, si celle-ci correspond aux règles que l'administrateur réseau a définies, la passerelle crée une liaison entre les deux réseaux. [10]

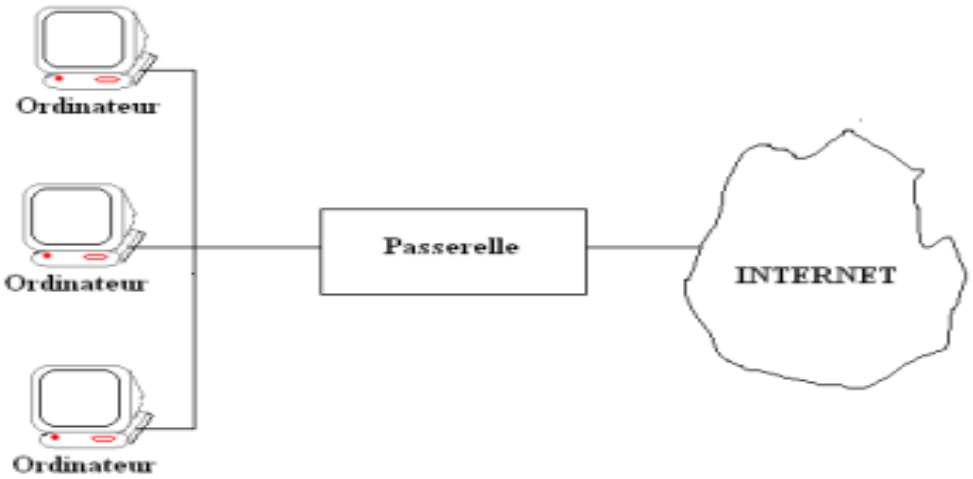


Figure I.10 : deux réseaux reliés avec une passerelle.

I.7.Les modèles des réseaux :

I.7.1. Le modèle OSI :

OSI signifie (**O**pen **S**ystem **I**nterconnexion), Ce modèle a été mise en place par l'**ISO** (**I**nternational **S**tandard **O**rganisation) afin de mettre en place un standard de communication entre les ordinateurs d'un réseau.

Le modèle **ISO** décrit la manière dont deux éléments d'un réseau (station de travail, serveur…) communiquent, en décomposant les différents opérations à
Effectuer en 7 étapes successives, qui sont nommées les 7 couches du modèle OSI.

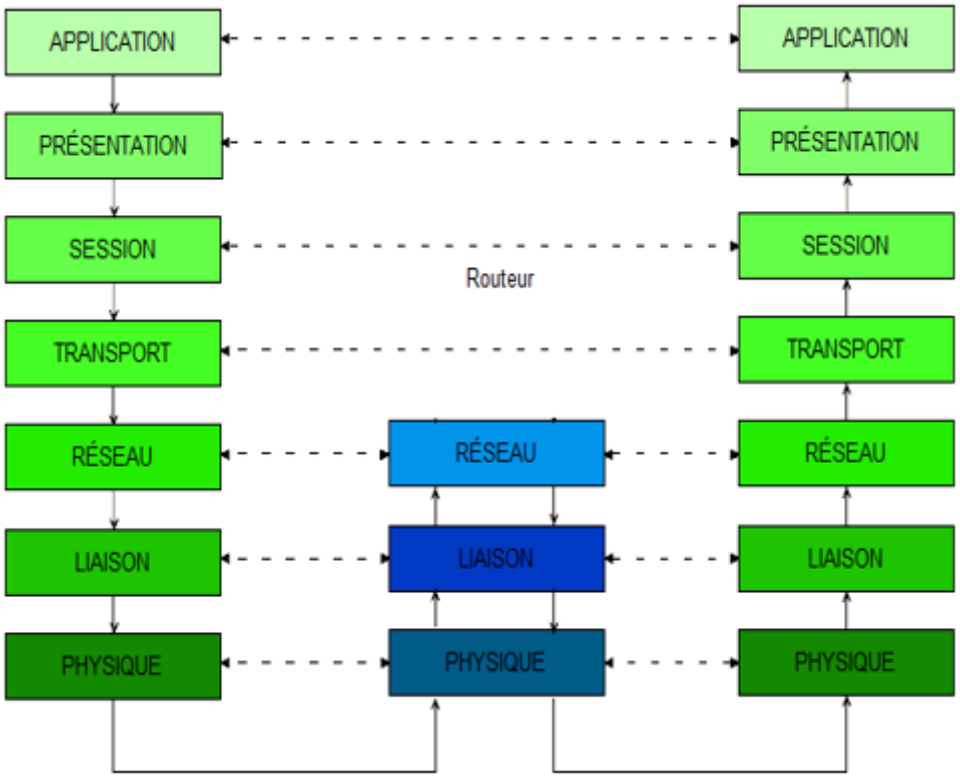


***Figure I.11** : Les 7 couches du modèle OSI.*

Les 7 couches sont :

- ✓ ***Couche 7 « application »:***
  Comprend les programmes qui utilisent le réseau, la messagerie électronique ou le transfert des fichiers.
- ✓ ***Couche 6 « présentation »:***permet le codage et conversion des données de la couche application afin que les données issues du périphérique source puissent être bien interprétées sur le périphérique de destination, elle permet aussi la compression des données de sorte que celles-ci puissent être décompressées par le périphérique de destination.
- ✓ ***Couche 5 « session »:***gère l'établissement, la gestion et coordination des communications.
- ✓ ***Couche 4 « transport »:***s'occupe de la gestion des erreurs, notamment avec les protocoles UDP et TCP/IP. Permet l'acheminement de bout en bout sans se soucier

des relais intermédiaires, elle permet la fragmentation du message en unités plus petites dites segments.

- ✓ ***Couche 3 « réseau »:***sélectionne les routes de transport (routage) et s'occupe du traitement et du transfert des messages: gère par exemple les protocoles IP (adresse et le masque de sous-réseau) et ICMP.
- ✓ ***Couche 2 « liaison de données »:****est un moyen* de communication brut apparaisse à la couche réseau comme étant une liaison. Elle décompose les données en trames de données et envoie ces dernières en séquence, permet aussi de contrôler l'erreur à l'émission et à la réception.

(Elle fiabilise la transmission entre systèmes directement reliés par un support d'interconnexion).

- ✓ ***Couche 1 « physique »:***gère les connexions matérielles et la transmission, définit la façon dont les données sont converties en signaux numériques, elle assure la transmission de bits entre les entités physique. [25]

I.7.2. Le modèle TCP/IP (modèle Internet) :

TCP/IP désigne communément une architecture réseau, mais cet acronyme désigne en fait 2 protocoles étroitement liés : un protocole de transport **TCP** (**T**ransmission **C**ontrol **P**rotocol) et un protocole réseau **IP** (**I**nternet **P**rotocol). Ce qu'on entend par "modèle TCP/IP", c'est en fait une architecture réseau en 4 couches dans laquelle les protocoles **TCP** et **IP** jouent un rôle prédominant car ils en constituent l'implémentation la plus courante. Par abus de langage TCP/IP peut donc désigner deux choses : le modèle TCP/IP et la suite de deux protocoles TCP et IP.

Le modèle TCP/IP s'inspire du modèle OSI auquel il reprend l'approche modulaire mais réduit le nombre à quatre. Les trois couches supérieures du modèle OSI sont souvent utilisées par une même couche d'application.

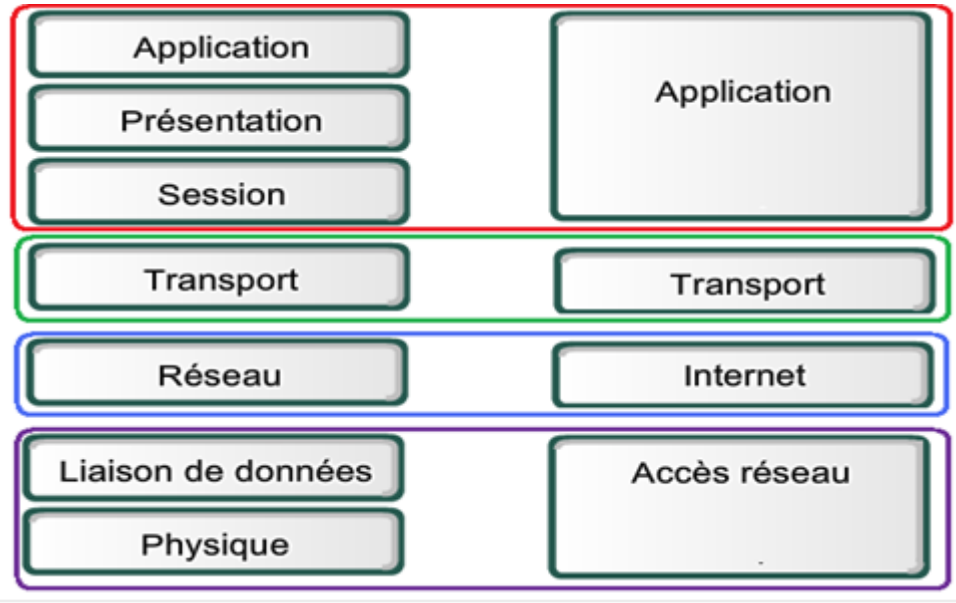


***Figure I.12** : les 4 couches du modèle TCP/IP'e.*

Les couches du modèle TCP/IP sont :

- ✓ **La couche accès réseau :**

La couche Accès réseau spécifie la forme sous laquelle les données doivent être transmises. Elle prend en charge les notions suivantes:

- ❖ Type de réseaux (Ethernet, Token Ring, ...), y compris les cartes réseaux.
- ❖ Transfert des données.
- ❖ Synchronisation de la transmission de données.
- ❖ Mise en forme (format) des données.
- ❖ Conversion analogique/numérique pour les modems téléphoniques.
- ❖ Contrôle des erreurs. [16]

- ✓ ***Couche INTERNET :***

La couche Internet est chargée de fournir les paquets de données. Elle définit les datagrammes et gère la décomposition / recomposition des segments.

La couche Internet utilise 5 protocoles, seuls les 3 premiers sont importants):

- ❖ **Le protocole IP:** gère les destinations des messages, adresse du destinataire.

- **Le protocole ARP (Adresse Resolution Protocol):** gère les adresses des cartes réseaux et la correspondance avec l'adresse IP. Chaque carte a sa propre adresse MAC d'identification codée sur 48 bits.

- **Le protocole ICMP (Internet Control Message Protocol) :** gère les informations relatives aux erreurs de transmission. ICMP ne les corrige pas, il signale uniquement que le message contient des erreurs.

- **protocole RARP (Reverse Address Résolution Protocol) :** gère l'adresse IP pour les équipements réseaux qui ne peuvent en récupérer une automatiquement par lecture d'information dans un fichier de configuration ou via un serveur DHCP.

- **Le protocole IGMP (Internet Group Management Protocol) :** permet d'envoyer le même message à des ordinateurs qui font partie d'un groupe. Il permet aussi à ces machines de s'abonner et se désabonner d'un groupe. Ce protocole permet de regrouper des stations.

✓ ***Couche transport :***

La Couche transport permet le transfert des données et les contrôles qui permettent de vérifier l'état de la transmission.

Les protocoles de cette couche permettent d'envoyer des données issues de la couche application. La couche transport gère 2 protocoles de transport des informations, indépendamment du type de réseau utilisé:

- **TCP** est orienté connexion (il vérifie la bonne transmission de données par des signaux d'accusés de réception), il assure ainsi le contrôle des données
- **UDP** est non orienté connexion, n'assure aucun contrôle de transmission des données, par exemple utilisé en streaming.

Ces 2 types (orienté connexion et non orienté connexion) sont une notion utilisée pour les firewalls.

✓ ***Couche application :***

La Couche Application reprend les applications standards en réseau informatique et Internet:

- **SMTP (S**imple **M**ail Transport **P**rotocol) : gère le transfert de mails entre serveurs.
- **POP:** gère le transfert des mails entre un serveur de messagerie et un ordinateur client.

- **TELNET:** connexion sur une machine distante (serveur) en tant qu'utilisateur
- **FTP** (**F**ile **T**ransfert **P**rotocol) : transfert des fichiers via Internet. [11]

I.8.LES VLANS :

Un réseau **VLAN** (Virtual Local Area Network ou réseau local virtuel) est un réseau local regroupant un ensemble de machines de façon logique et non physique.

Un réseau local virtuel est un regroupement virtuel d'au moins deux périphériques. Ce regroupement virtuel peut s'étendre au-delà de plusieurs commutateurs. Les périphériques sont regroupés sur la base d'un certain nombre de facteurs suivant la configuration du réseau.
Grâce aux réseaux virtuels (Vlan) il est possible de s'affranchir des limitations
De l'architecture physique (contraintes géographiques, contraintes d'adressage) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.).

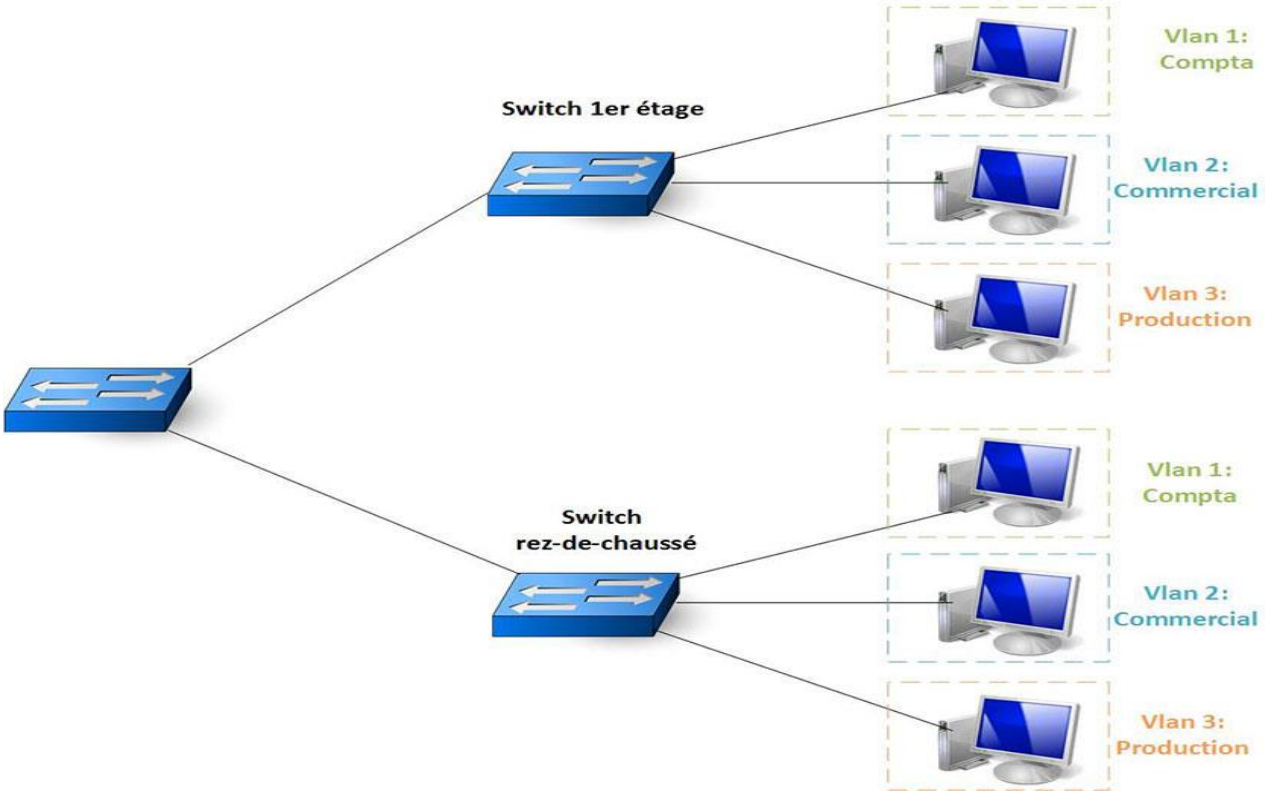


Figure I.13: les vlan étages.

❖ **VLAN niveau 1 :**

Un VLAN de niveau 1(aussi appelés VLAN par port) définit un réseau virtuel en fonction des ports de raccordement sur le Switch ou commutateur. Dans le cadre des réseaux VLAN basés sur les ports, l'appartenance de chaque port du commutateur à tel ou tel réseau VLAN est configurée manuellement.

❖ **VLAN niveau 2 :**

Un VLAN de niveau 2(également appelé VLAN MAC, *VLAN par adresse IEEE)* consiste à définir un réseau virtuel en fonction des adresses MAC des stations. Ce type de VLAN est beaucoup plus souple que le VLAN par port car le réseau est indépendant de la localisation de la station.

❖ **VLAN niveau 3 :**

On distingue plusieurs types de VLAN de niveau 3 :

✓ Le **VLAN par sous-réseau** : associe des sous réseaux selon l'adresse IP source des datagrammes. Ce type de solution apporte une grande souplesse dans la mesure où la configuration des commutateurs se modifie automatiquement en cas de déplacement d'une station.

✓ Le **VLAN par Protocol :** permet de créer un réseau virtuel par type de protocole (par exemple TCP/IP), regroupant ainsi toutes les machines utilisant le même protocole au sein d'un même réseau. Avec les réseaux VLAN basés sur les protocoles, c'est le protocole de couche 3 transporté par la trame qui permet de déterminer l'appartenance aux réseaux VLAN. [30]

I.9. Les serveurs :

I.9.1.Le proxy :

Un proxy est un composant logiciel informatique qui joue le rôle d'intermédiaire en plaçant entre deux hôtes pour facilites ou surveiller leurs échanges. Un proxy est un programme servant d'intermédiaire pour accéder à un autre réseau généralement internet.

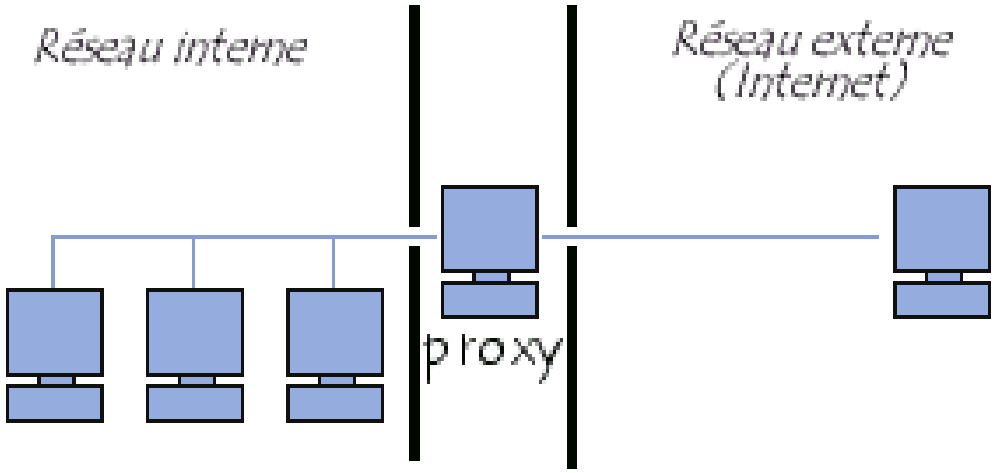


Figure14 : serveur proxy

I.9.2. le DHCP :

Dynamic Host Configuration Protocol (protocole de configuration dynamique des hôtes) est un protocole réseau dont le rôle est d'assuré la configuration automatique des paramètres IP d'une station au d'une machine, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau. DHCP peut aussi configurer l'adresse de la passerelle par défaut, des serveurs de noms DNS. [21]

Conclusion :

Dans ce chapitre nous avons fait une étude générale sur les réseaux informatique. Les réseaux peuvent être divisés en LAN, MAN, WAN et réseaux d'interconnexion et chacun d'eux a ses propres caractéristiques selon les topologies et les supports de transmissions, le modèle OSI, le modèle TCP/IP, et leurs différents protocoles de communication.

Chaque réseau informatique doit être protégé contre les menaces et pour cela dans le chapitre suivant nous allons faire des généralités sur la sécurité réseau.

II. Préambule :

La sécurité informatique de nos jours est devenue un problème majeur dans la gestion des réseaux d'entreprise ainsi que pour les particuliers toujours plus nombreux à se connecter à Internet. La transmission d'informations sensibles et le désir d'assurer la confidentialité de celles-ci est devenue un point primordial dans la mise en place de réseaux informatiques.

Comme le réseau aujourd'hui domine le monde informatique, les grandes entreprises ne peuvent plus survivre sans que leur machines soit connectée à un réseau étendu (WAN ou internet). [28]

Donc dans ce chapitre nous définissons le terme de sécurité des réseaux ainsi que les méthodes des attaques utilisées et comment se protéger contre ces attaques en utilisant le pare-feu « firewall ».

II.1.La sécurité informatique :

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles.

II.1.1.Objectifs de la sécurité :

Les solutions de sécurité doivent contribuer à satisfaire au moins les critères suivant:

- ✓ **Intégrité :**

  L'intégrité signifie que les méthodes de gestion des données garantissent que ces données sont traitées sans erreurs. Les données ne doivent pas être modifiées lors de leur transfert ou de leur stockage. Personne ne peut changer le contenu de l'information ni celui des fichiers. N'est encore moins les supprimer. Afin d'assurer l'intégrité des données, l'expéditeur doit toujours être authentifié [11].

- ✓ **Confidentialité :**

  La confidentialité signifie que l'accès à l'information disponible sur le réseau ou la circulation dans le réseau est réservé à ceux qui en ont reçu l'autorisation. Personne ne peut accéder à l'information s'il n'en a pas le droit. L'identification des utilisateurs requiert une authentification. Maintenir l'information à l'abri des indiscrets requiert un cryptage [12], effectué par des moyens techniques.

- ✓ **Disponibilité :** Permettant de maintenir le bon fonctionnement du système d'information. L'objectif de la disponibilité est de garantir l'accès à un service ou à des ressources, elle nécessite que le système reste à tout moment opérationnel et sans aucune dégradation de son fonctionnement.
- ✓ **Authentification :** Est la procédure qui consiste, pour un système informatique, à vérifier l'identité d'une entité (personne, ordinateur…), afin d'autoriser l'accès de cette entité à des ressources (systèmes, réseaux, applications…). L'authentification permet donc de valider l'authenticité de l'entité en question.
- ✓ **Non-répudiation :** c'est le fait de ne pas pouvoir revenir sur le contenu d'un document électronique ou d'une transaction.

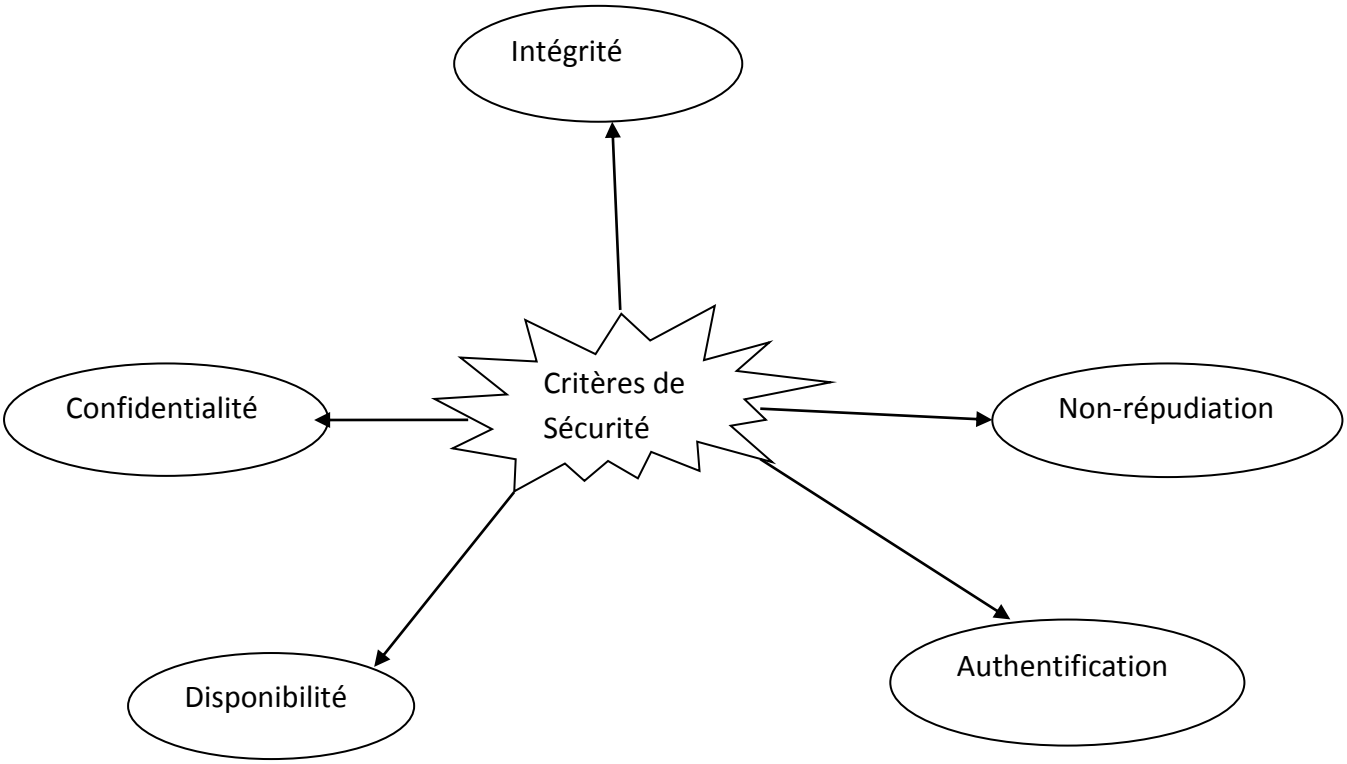


***Figure II.1** : Critères de sécurité.*

II.1.2.Les causes de l'insécurité :

On distingue généralement deux types d'insécurité :

- ★ **L'état actif d'insécurité :** c'est-à-dire la non-connaissance par l'utilisateur des fonctionnalités du système, dont certaines pouvant lui être nuisibles (par exemple la non-désactivation de services réseaux non nécessaires à l'utilisateur)
- ★ **L'état passif d'insécurité :** c'est-à-dire lorsque l'administrateur (ou l'utilisateur) d'un système ne connaît pas les dispositifs de sécurité dont il dispose.

II.2.La politique de sécurité :

Une politique de sécurité ou stratégie de sécurité est une déclaration formelle des règles qui doivent être respectées par les personnes qui ont accès aux ressources et données de l'entreprise en vue de protéger son réseau contre les attaques menés soit de l'intérieur, soit de l'extérieur.

La politique de sécurité a pour rôle :

- ✓ Définir le cadre d'utilisation des ressources du système d'information;
- ✓ Identifier les techniques de sécurisation à mettre en œuvre dans les différents services de l'organisation ;
- ✓ Sensibiliser les utilisateurs à la sécurité informatique.

II.3.Les menaces :

Les menaces sont considérées comme une violation potentielle du système de sécurité, elles viennent d'individus compétents à cause des vulnérabilités de système de sécurité.

II.3.1.Type de menaces :

Toute communication entre les utilisateurs sur un canal peu est sûr soumis à des types d'attaques da la part de pirate.

1. Les menaces accidentelles : Les menaces accidentelles peuvent se manifester ou résulter de l'exposition ou de la modification d'un objet, elles peuvent êtres des erreurs des utilisateurs ou d'administrateur, matériel ou accidents de nature industrielle (un incendie).

2. Les menaces intentionnelles :

L'ensemble des actions malveillantes (qui constituent la plus grosse partie du risque). Qui devraient être l'objet principal des mesures de protection. C'est une action exécutée par une entité pour voiler la sécurité de l'information et l'utilisation non autorisée des ressources. Les menaces intentionnelles peuvent être passives ou actives :

a. Menaces passives : Dans ce cas le pirate se contente d'écouter le message. Son rôle est de collecter les informations. En générale il est très difficile de détecter une attaque passive car elle n'interagit pas dans le fonctionnement de système.

b. Menaces actives : le pirate peut modifier le contenu des messages échangés (des modifications de l'état de fonctionnement du système), ce qui menace l'intégrité de l'information. Ce type de menaces est facile à détecter. [10]

II.4.Les attaques informatique :

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque. Une attaque est l'exploitation d'une faille d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables.

Sur internet des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, vers, etc.), à l'insu de leur propriétaire.

II.4.1.Typologie d'attaques réseau :

Les attaques réseau peuvent être classées comme suit :

- **Les attaques permettant de dévoiler le réseau :**
  - **a. Les attaques par cartographie du réseau :**

    Les attaques visant à établir la cartographie d'un réseau ont pour but de dresser (construire, installer) les artères de communication des futurs systèmes cibles.

Elles ont recours pour cela à des outils de diagnostic tels que le trace route, qui permet de visualiser le chemin suivi par un paquet IP d'un hôte à un autre. Le trace route utilise l'option durée de vie TTL (Time To live) du paquet IP pour émettre un message ICMP time_exceeded (temps dépassé) pour chaque routeur qu'il traverse, sachant que chaque routeur qui manipule un paquet décrémente le champ TTL, ce champ devient un véritable compteur de tronçon et permet de déterminer l'itinéraire précis suivi par les paquets IP vers un système cible.

b. Les Attaques par identification des systèmes réseaux :

Certaines attaques visent à identifier tous les systèmes présents dans le but d'adresser les futurs moyens de pénétration du réseau ou de système qui le compose, il existe pour cela différentes techniques de balayage des systèmes :

- ✓ **Attaque par balayage ICMP :**

C'est l'une des méthodes les plus simple de balayage, elles utilisent le protocole ICMP et sa fonction request plus connue sous le nom de Ping. Elle consiste à envoyer des paquets ICMP écho-request vers le serveur, le serveur répondant par un paquet ICMP echo-replay**.**

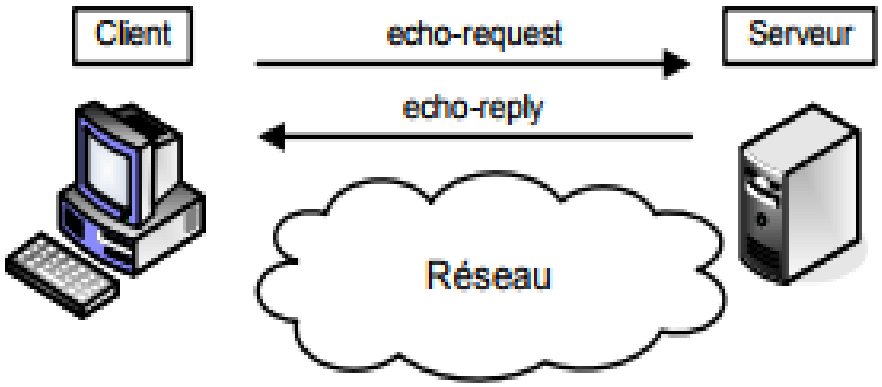


Figure II.2 : *Fonctionnement de la commande Ping.*

✓ **Attaque par balayage TCP :**

c'est en partant du principe que le flux réseau toujours accessible au pirate est celui qui est destiné à être accessible au public que la technique du balayage TCP a été inventée.

Similaire au balayage ICMP, sa spécificité est de s'appuyer sur le protocole TCP. Le client envoie un paquet SYN vers un port réseau particulier de l'adresse IP du serveur. Si le port est en écoute, un paquet SYN/ACK est reçu en retour. Sinon, la réception d'un paquet RST signifie qu'il n'y a pas de service en écoute sur le port. Le client envoie en réponse un paquet RST pour terminer la connexion. Si aucune réponse n'est reçue en retour, c'est qu'il existe un équipement filtrant entre le serveur et le client ou qu'il n'y a aucune machine derrière l'adresse IP visée.

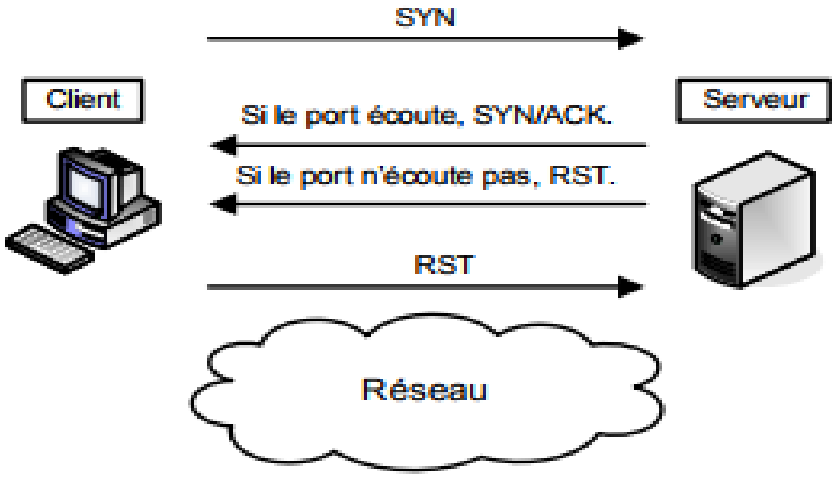


Figure II.3 : *Le balayage TCP.*

✓ ***Attaque par Balayage de port :***

Le balayage de port (*port scanning*) est une technique servant à rechercher les ports ouverts sur un serveur de réseau. Cette technique est utilisée par les administrateurs des systèmes informatiques pour contrôler la sécurité des serveurs de leurs réseaux. La même technique est aussi utilisée par les pirates informatiques pour tenter de trouver des failles dans des systèmes informatiques. Un balayage de port

effectué sur un système tiers est généralement considéré comme une tentative d'intrusion, car un balayage de port sert souvent à préparer une intrusion.

II.4.2.Les types d'attaques :

Les personnes malveillantes utilisent plusieurs techniques d'attaques qui peuvent être regroupées en trois familles déférentes :

a. Les attaques directes :

Les attaques réseau peuvent être lancées directement, le pirate attaquant sa victime et exposant ainsi son identité, comme l'illustre la figure II.4. L'attaque directe est la plus simple à réaliser :

- Le hacker attaque directement sa victime à partir de son ordinateur par des scripts d'attaques faiblement paramétrable ;
- Les programmes de hacking qu'ils utilisent envoient directement les paquets à la victime ;
- Dans ce cas, il est possible en général de remonter à l'origine de l'attaque, identifiant par la même occasion l'identité de l'attaquant.

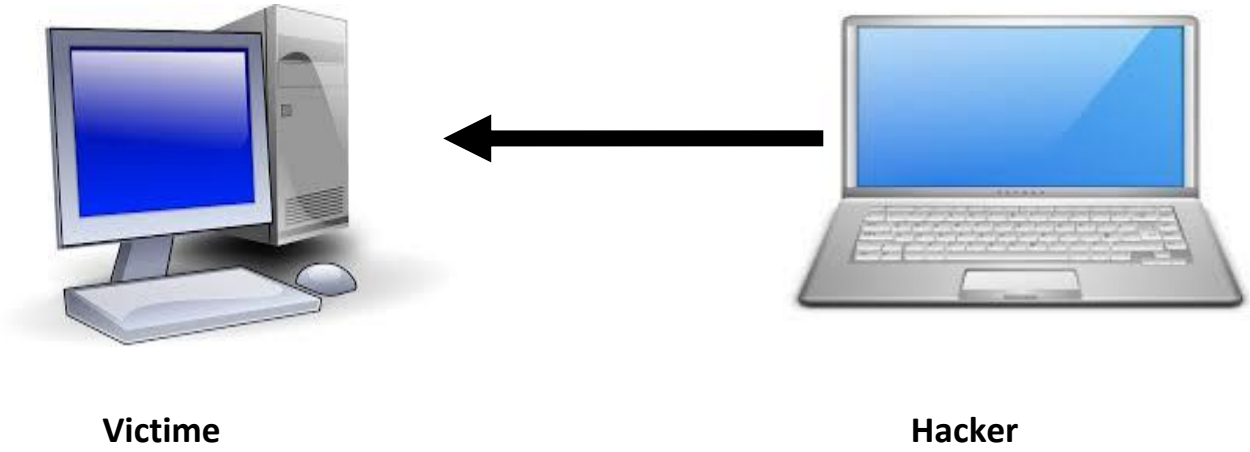


***Figure II.4** : Attaque direct.*

b. Les attaques indirectes par rebond :

Les attaques réseau peuvent aussi être lancées indirectement par l'intermédiaire d'un système rebond afin de masquer l'identité (adresse IP) du pirate et d'utiliser les

ressources du système intermédiaire. Les paquets d'attaque sont dans ce cas envoyés au système intermédiaire, lequel répercute l'attaque vers le système cible, comme l'illustre la figure II.5.

***Figure II.5** : Attaque indirecte par rebond.*

c. Les attaques indirectes par réponse :

Les attaques indirectes par réponse, offrent au pirate les mêmes avantages que les attaques par rebond. Au lieu d'envoyer l'attaque au système intermédiaire pour qu'il la répercute, l'attaquant lui envoie une requête, et c'est la réponse à cette requête qui est envoyée au système cible, comme l'illustre la figure II.6.[1]

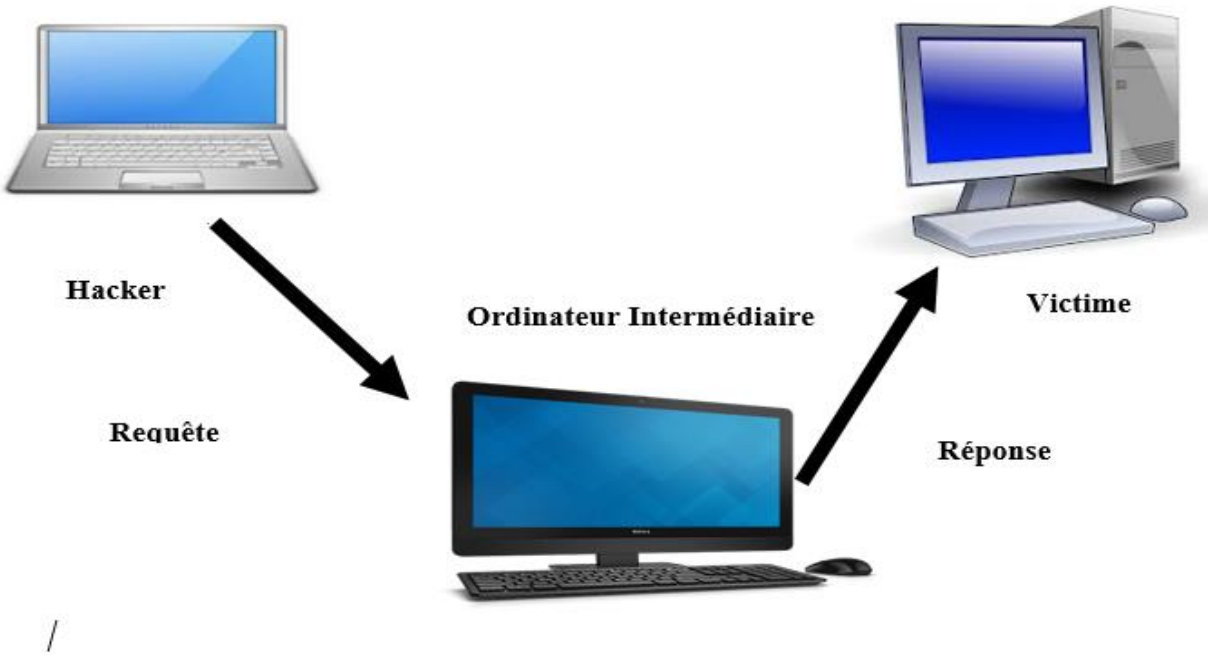


***Figure II.6 :** Attaque direct par réponse.*

II.4.3.Les attaques logicielles :

★ **Les virus :**

Les virus représentent la menace sur la sécurité la plus largement connue. Un virus informatique est un programme conçu pour se propager à d'autres ordinateurs. Les virus infectent principalement les fichiers exécutables, mais peuvent aussi s'infiltrer dans les courriels et dans certains types de fichiers de données.

★ **Les vers(Worm) :**

Un ver est un programme qui peut se reproduire et se déplacer à travers un réseau en utilisant ses mécanismes, sans avoir réellement besoin d'un support physique ou logique pour se propager, donc un ver est un virus réseau. Il a la capacité de se multiplier en recopiant ses instructions, qui à leur tour se recopient. La croissance explosive du ver peut paralyser les réseaux en les congestionnant avec les données de ses propres activités.

★ **Logiciel espion (Spyware) :**

Un spyware est un logiciel qui transmet par le biais d'Internet des informations, généralement à des annonceurs publicitaires, sur l'utilisateur ou sur ses habitudes. Les spywares se transmettent principalement par l'intermédiaire de sites Web et parfois par e-mail. Ce logiciel malveillant s'installe dans un ordinateur ou autre appareil mobile, dans le but de collecter et transférer des informations sur l'environnement dans lequel il s'est installé, très souvent sans que l'utilisateur en ait connaissance.

★ **Le pourriel (Spam):**Le spam, courriel indésirable ou pourrie**l** est une communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires. [3]

★ **Le cheval de Troie :**

En informatique, un cheval de Troie est un programme ou un fichier qui comporte une fonctionnalité cachée connue de l'attaquant seul. Il effectue une fonction illicite (divulguer ou altérer des informations) tout en donnant l'apparence d'effectuer une fonction légitime. Cependant un cheval de Troie doit d'abord être installé et ceci n'est possible que si les mesures de sécurité sont incomplètes, inefficaces ou si l'agresseur bénéficie d'une complicité. La méthode la plus efficace pour se protéger de ces programmes est d'utiliser un bon antivirus. [20]

II.4.3.Les autres attaques :

★ **Le Sniffing (l'écoute du réseau) :**

Cette technique est utilisée par les pirates pour capturer les mots de passe. Lorsqu' on se connecte à un réseau qui utilise le mode broadcaste, toutes les données en transit arrivent à toutes les cartes réseau connectées à ce réseau.

Le Sniffer : est un dispositif permettant d'écouter le trafic d'un réseau, il permet de capturer les infirmations qui y circuler sur ce réseau. Le Sniffer peut ainsi servir à déceler les failles de sécurité, mais il peut aussi être utilisé de façon malveillante pour intercepter les mots de passe du réseau par exemple.

★ **Les attaques par déni de service (DOS : Denial Of Service) :**

Une attaque par déni de service est un type d'attaque visant à rendre indisponible pendant un temps indéterminé les services ou ressources d'une organisation. Ceci peut s'effectuer de plusieurs manières, par le biais d'une surcharge réseau rendant ainsi la machine totalement injoignable, ou bien de manière applicative en crashant l'application à distance. Le but d'une telle attaque n'est pas de récupérer ou d'altérer des données, mais de nuire à la réputation de sociétés ayant une présence sur internet et éventuellement de nuire à leur fonctionnement si leur activité repose sur un système d'information. [7]

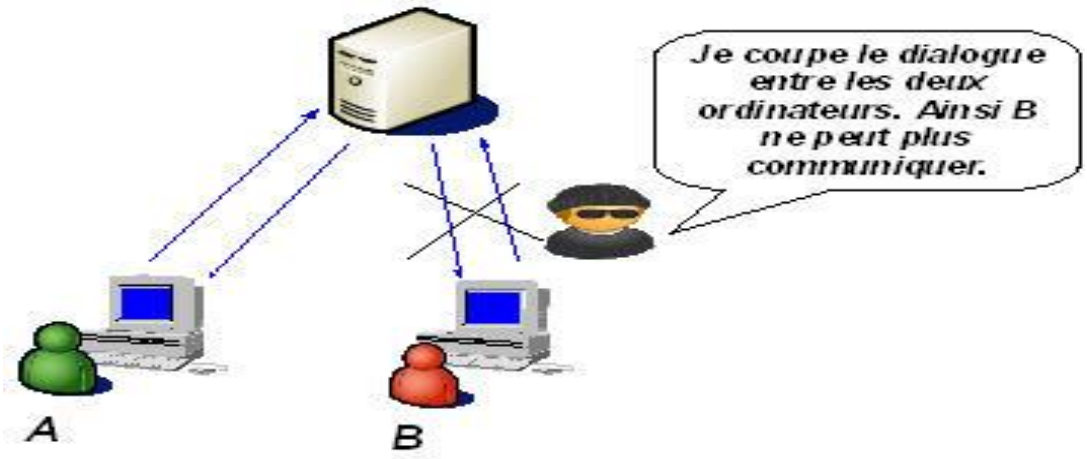


Figure II.7 : Attaque par Déni de service.

★ **Scanning :**

Le scanning consiste à balayer tous les ports sue une machine en utilisant un outil appelé scanner. Le scanner envoie des paquets sur plusieurs ports de la machine. En fonction de leurs réactions, le scanner va en déduire si les ports sont ouverts. C'est un outil très utilisé pour les hackers, cela leur permet de connaitre les points faibles d'une machine et ainsi de savoir par où ils peuvent attaquer.

Figure II.8 : Le scanning.

★ **Intrusion :** Nous appellerons intrusion toute utilisation d'un système informatique à des fins autres que celles prévues. L'intrus est généralement vu comme une personne étrangère au système informatique qui a réussi à en prendre le contrôle, mais les statistiques montrent que les utilisations abusives (du détournement de ressources à l'espionnage industriel) proviennent le plus fréquemment de personnes internes ayant déjà un accès au système.

★ **Attaque de l'homme de milieu (man in the middle) :**

L'attaque man in the middle consiste à faire passer les échanges réseau entre deux systèmes par le biais d'un troisième, sous le contrôle du pirate. Ce dernier peut transformer à sa façon les données à la volée, tout en masquant à chaque acteur de l'échange la réalité de son interlocuteur.

Pour mettre en œuvre l'échange réseau approprier, il faut soit que la machine du pirate se trouve physiquement sur le chemin réseau emprunté par les flux de données, soit que le pirate réussisse à modifier le chemin réseau afin que sa machine deviennent un des point de passage. [30]

Figure II.9 : *Attaque par homme de milieu.*

★ **Usurpation d'adresse IP (IP Spoofing) :**

Le Spoofing (ou bien Mystification), en sécurité informatique, est lorsqu'une personne réussit à obtenir des avantages en envoyant de fausses données, ou encore des données trafiquées. Souvent, le Spoofing peut permettre de cacher son identité en falsifiant son adresse matérielle (MAC) ou son adresse logique (IP).

L'usurpation d'adresse IP (Spoofing IP) est une technique consistant à remplacer l'adresse IP de l'expéditeur IP par l'adresse IP d'une autre machine.

★ Les attaques de mot de passe :

Les attaques sur les mots de passe peuvent consister à faire de nombreux essais jusqu'à trouver le bon mot de passe. Dans ce cadre, notons les deux méthodes suivantes :

- ♣ **L'attaque par dictionnaire :** le mot testé est pris dans une liste prédéfinie contenant les mots de passe les plus courants.
- ♣ **L'attaque par force brute :** toutes les possibilités sont faites dans l'ordre jusqu'à trouver la bonne solution. Cette méthode est en générale considérée comme la plus simple concevable. Elle permet de casser tout mot de passe en un temps fini indépendamment de la protection utilisée. [24]

★ La bombe logique (Fork Bomb) :

Une bombe logique fonctionne en créant un grand nombre de processus très rapidement afin de saturer l'espace disponible dans la liste des processus gardée par le système d'exploitation. Si la table des processus se met se saturer, aucun nouveau programme ne peut démarrer tant qu'aucun autre ne termine. [4]

★ Attaque par inondation :

L'inondation est la méthode la plus classique pour empêcher un réseau d'assurer sa mission. Son principe de fonctionnement est le suivant :

- Une ou plusieurs machines inondent le réseau avec des paquets réseau afin de saturer la bande passante de celui-ci ;
- Une fois que toute la bande est occupée, les autres machines ne peuvent plus travailler, ce qui génère une situation de déni de service. [20]

II.5.Les protocoles de sécurité :

II.5.1.Protocole SSH (Secure Shell) : Permet à un client d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers

de manière sécurisée : les données circulant entre le client et le serveur sont chiffrées dans un flux TCP en mode tunnel dans une session SSH.

II.5.2.Protocole SSL (Secure Sockets Layer) : Le protocole SSL permet de sécurisé tout protocole applicatif s'appuyant sur TCP/IP (http, FTP,…).

Le SSL est un protocole de couche 4(niveau transport) utilisé par une application pour établir un canal de communication sécurisé avec une autre application. Il fournit un accès sécurisé (via un tunnel dédicacé) vers des applications spécifiques de l'entreprise ou de l'administration.

Le SSL comme son nom l'indique est une couche (layer) supplémentaire sécurisée. Ce protocole va créer une sorte de canal sécurisé entre le client et le serveur. (On pourrait comparer cela au VPN, sauf que le VPN créé un canal mais pour l'ensemble de l'ordinateur, d'ailleurs les VPN s'appuient sur SSL/TLS). Grace un échange de clés entre eux, le serveur et le client vont établir une connexion chiffrée dont eux seuls pourront lire le contenu. Car seul le client et le serveur en possession de la clé de décryptage pourront déchiffrer les données reçues.

II.5.3.Protocole IPsec (Internet Protocol Security) : IPSec est un protocole destiné à fournir différents services de sécurité. Son intérêt principal reste sans contexte son mode de tunneling, c'est-à-dire d'encapsulation d'IP qui lui permet de créer des réseaux privés virtuels. Ce protocole est très utilisé lors de la création de réseaux privés virtuels et la sécurisation des accès à un intranet. Les services IPSec sont basés sur des mécanismes cryptographiques qui leur confèrent un niveau de sécurité élevé.

II.5.4.HTTPS (http sécurisé) : Est un procédé de sécurisation des transactions http utilisé pour la navigation sécurisé. Il offre des possibilités d'authentification et de chiffrement pour les sites web nécessitant un certain niveau de sécurité dans leurs échanges avec les navigateurs web.

Pour garantir cette sécurité, il faut usage de méthodes de cryptographie asymétrique pour l'authentification et de méthodes de cryptographie symétrique pour le chiffrement des échanges.

II.5.5.Le protocole PKI (Public Key Infrastructure) :

PKI se base sur le chiffrement asymétrique. Selon cette formule, une organisation ou une personne s'adresse à un tiers de confiance appelé autorité de certification ou CA pour lui demander une paire de clés de chiffrement. L'une de ces clés est privé et l'autre publique. [2]

II.6.Méthodes de défenses :

Le but de la sécurité informatique est de préserver la confidentialité, l'intégrité et la disponibilité des données du réseau. Certaines méthodes de défense permettent de prévenir les attaques, d'autres, moins efficaces, ne font qu'une détection ultérieure.

II.6.1.Authentification :

L'authentification pour un système informatique est un processus permettant au système de s'assurer de la légitimité de la demande d'accès faite par une entité (être humain ou un autre système...) afin d'autoriser l'accès de cette entité à des ressources du système (systèmes, réseaux, application…) conformément au paramétrage du contrôle d'accès. L'authentification permet donc, pour le système, de valider la légitimité de l'accès de l'entité, ensuite le système attribue à cette entité les données d'identité pour cette session (ces attributs sont détenus par le système ou peuvent être fournis par l'entité lors du processus d'authentification). C'est à partir des éléments issus de ces deux processus que l'accès aux ressources du système pourra être paramétré (contrôle d'accès).

Les techniques d'authentification les plus utilisées sont les mots de passe mais aussi, de plus en plus, les certificats de clé publique.

- **Le mot de passe :**

Le moyen le plus simple et la plus classique de s'assurer que seules les personnes autorisées peuvent accéder à une partie de réseau est de protéger certaines zones du réseau par un mot de passe. De nombreux utilisateurs choisissent des chiffres ou des mots facile à retenir pour leurs mots de passe, comme des dates d'anniversaires, des numéros de téléphonons ou des noms d'animaux de compagnie.

- **Certificats numériques :**

En général, un certificat est un document qui certifie que quelqu'un est le détenteur légitime de quelque chose. Les certificats numériques sont utilisés dans des applications de la

cryptographie à clefs publiques pour certifier qu'une entité (une personne, une application,…) possède une clef.

Un certificat contient deux champs importants : la clef publique d'une entité et son identité. Ces deux champs sont certifiés par un tiers de confiance, appelé l'autorité de certification.

Les certificats numériques sont généralement utilisés à fins d'identification, lors de l'établissement de tunnels sécurisés sur Internet, comme c'est le cas dans les réseaux virtuels privée(VPN) et sont émis par une autorité de certification.

- **Système de détection d'intrusion (IDS : Intrusion Detection System) :**

  Un système de détection d'intrusions reposant sur le réseau fournit une surveillance constante de réseau. Ce système analyse les flux de paquets de données du réseau à la recherche d'activités non autorisées, telles que les attaques de pirates et permet aux utilisateurs de répondre aux failles dans la sécurité avant que les systèmes ne soient compromis.

  Un IDS est un capteur informatique qui écoute de manière furtive le trafic sur un système, vérifie, filtre et repère les activités anormales ou suspectes, ce qui permet ultérieurement de décider d'action de prévention. Sur un réseau, l'IDS est souvent réparti dans tous les emplacements stratégiques du réseau.

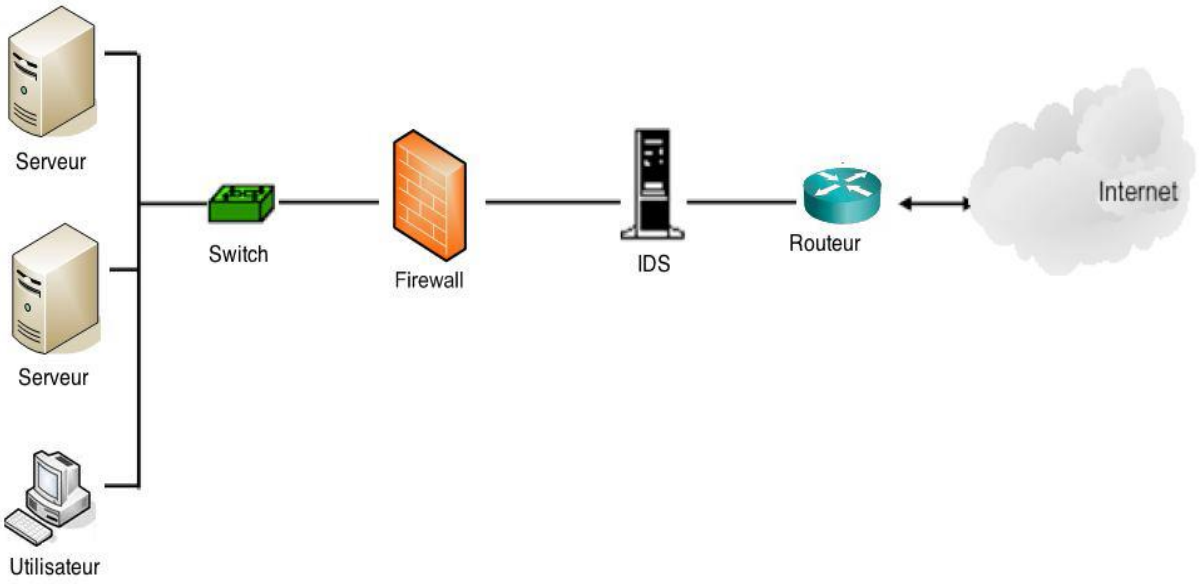


Figure II.10 : *Exemple d'un IDS dans un réseau.*

- **Audit de sécurité :**

Un audit de sécurité consiste à s'appuyer sur un tiers de confiance afin de valider les moyens de protection mis en œuvre, il permet de s'assurer que l'ensemble des dispositions prises par l'entreprise sont réputées sures. L'audit répertorie les points forts, et surtout les points faibles (vulnérabilités) de tout ou partie du système. L'audit informatique a pour objectif d'identifier et d'évaluer les risques associés aux activités informatiques d'une entreprise ou d'une administration. [31]

II.6.2.Cryptographie :

La cryptographie est la science qui utilise les mathématiques pour chiffrer et déchiffrer des données. La cryptographie vous permet de stocker des informations sensibles ou de les transmettre à travers des réseaux non sûrs (comme Internet) de telle sorte qu'elles ne puissent être lues par personne à l'exception du destinataire convenu.

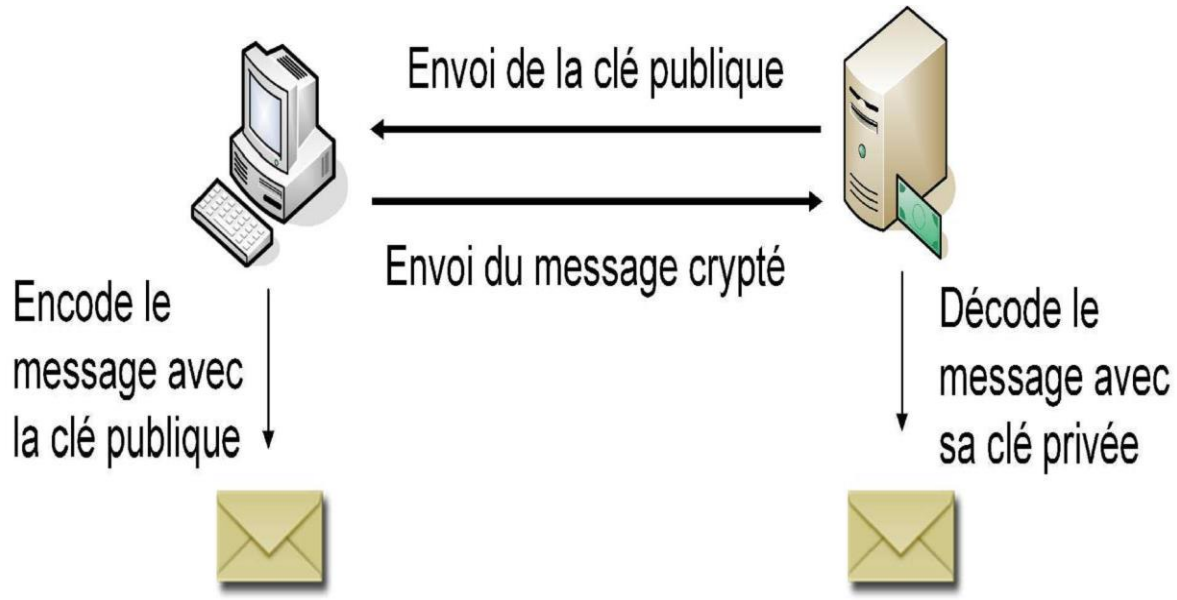


Figure II.11 : *Le cryptographe.*

a. Chiffrement symétrique (à clé privée) :

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

Le cryptage à clé privé ou symétrique est basé sur une clé partagée entre les deux parties communicantes. Cette même clé sert à crypter et décrypter les messages.

b. Chiffrement asymétrique (à clé publique) :

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 calculés l'une en fonction de l'autre. Ce système de cryptage utilise deux clés différentes pour chaque utilisateur :

Une est privée et n'est connue que de l'utilisateur, l'autre est publique et donc accessible par tout le monde. Les clés publique et privée sont mathématiquement liées par l'algorithme de cryptage de telle manière qu'un message crypté avec une clé publique ne puisse être décrypté qu'avec la clé privée correspondante. Une clé est donc utilisée pour le cryptage et l'autre pour le décryptage. [28]

II.6.3.VPN(Le réseau Privé Virtuel) :

L'acronyme **VPN** correspond à **V**irtual **P**rivate **N**etwork (réseau privé virtuel), est une technologie permettant de communiquer à distance de manière privée, comme on le ferait au sein d'un réseau privé de type intranet d'entreprise. Ces réseaux offrent deux avantages majeurs :

- ✓ De hautes performances en termes de bande passante, autrement dit des communications à très haut débit et de très grande qualité.
- ✓ La sécurité et la confidentialité des données.

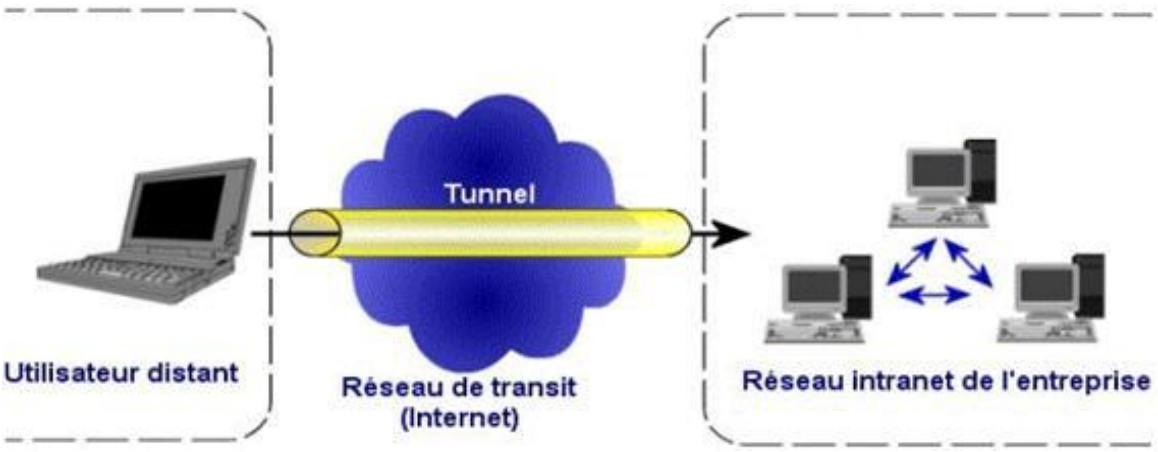


Figure II.12: *Réseau Privé Virtual.*

Un réseau VPN repose sur le protocole de tunneling. Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre 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 machines en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu couteux aux intranets ou aux extranets de l'entreprise, les VPN d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagé, comme internet. [6]

En d'autres termes, il est aujourd'hui possible, grâce à ces technologies, d'étendre son réseau privé d'entreprise à toute la planète. Ainsi, un commercial en déplacement pourra se connecter au réseau de son entreprise indépendamment du lieu où il se trouve. A tout moment il peut envoyer ou recevoir des données confidentielles de manière sécurisée et rapide.

De manière similaire, deux sites d'une même entreprise pourront être virtuellement réunis en un seul site, l'interconnexion entre ces deux sites offrant les mêmes prestations qu'un réseau local.

- **Les avantages de la VPN :**

- ✓ Les connexions VPN offrent un accès au réseau local à distance et de façon sécurisée pour les travailleurs nomades ;
- ✓ Les connexions VPN permettent d'administrer efficacement et de manière sécurisé un réseau local à partir d'une machine distante ;
- ✓ Les connexions VPN permettant aux utilisateurs qui travaillent à domicile ou depuis d'autres sites distants d'accéder à distance à un serveur d'entreprise par l'intermédiaire d'une infrastructure de réseau public telle qu'Internet ;
- ✓ Les connexions VPN permettent aux entreprises de disposer des connexions routées partagées avec d'autres entreprises sur un réseau public ;
- ✓ Les connexions VPN permettent de partager des fichiers et programmes de manière sécurisées entre une machine locale et une machine distante.

II.6.4.Les logiciels antivirus :

Un antivirus est un programme de sécurité que vous installez sur un ordinateur ou sur un appareil mobile pour le protéger contre l'infection de logiciels malveillants. Il est capable de :

- ✓ Détecter et de détruire les virus contenus sur un disque ;

- ✓ Surveiller la présence de virus et éventuellement de nettoyer et supprimer les fichiers infectés ;
- ✓ Ils surveillent tous les espaces dans lesquels un virus peut se loger, c'est à dire la mémoire et les unités de stockage qui peuvent être locales au réseau.

II.6.5.Firewall(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 :

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

Figure II.13 *: Présentation d'un firewall.*

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

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

a. Pourquoi un firewall ?

Sans l'utilisation d'un firewall, les différents systèmes du sous-réseau s'exposent à des attaques venant de l'extérieur.

Dans un environnement, sans firewall, la sécurité du réseau est basée sur la sécurité au niveau des hôtes et tous les hôtes doivent, dans un sens, coopérer pour atteindre un haut niveau uniforme de sécurité. Plus le sous-réseau est grand, moins il est facile de maintenir tous les hôtes au même niveau de sécurité. Lorsque les erreurs et les défaillances en sécurité deviennent courantes, les intrusions n'apparaitront plus comme le résultat d'attaques complexes, mais à cause de simples erreurs de configuration et de choix de mots de passe inadéquats. Il suffirait alors qu'un des systèmes hôtes soit compromis pour que tout le site devienne vulnérable.

b. Fonctionnement d'un système pare-feu :

Un système pare-feu contient un ensemble de règles prédéfinies permettant. Le principe de ces règles permet de mette en œuvre une méthode de filtrage dépendent 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 ;
- ✓ soit d'empêcher les échanges qui ont été explicitement interdits.

Le choix de l'une ou l'autre de ces méthodes dépend de la politique de sécurité adoptée par l'entreprise désirant mettre en œuvre un filtrage des communications.

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

c. Principes du filtrage :

Selon l'équipement, des informations sont extraites des flux réseaux depuis une ou plusieurs des couches 2 à 7 du modèle OSI, éventuellement corrélées entre elles, et comparées à un ensemble de règles de filtrage. Un état peut être mémorisé pour chaque flux identifié, ce qui permet en outre de gérer la dimension temporelle avec un filtrage en fonction de l'historique du flux.

d. Les différents types de filtrages :

- **Le filtrage simple de paquets(Stateless) :**
  C'est une méthode de filtrage la plus simple, elle opère au niveau réseau et transport du modèle OSI. La plupart des routeurs permettent d'effectuer du filtrage simple de paquet et cela consiste à accorder ou refuser le passage de paquet d'un réseau à un autre.

- **Le filtrage dynamique (Stateful) :**
  Cette technique a été proposée pour pallier aux certaines limites de pare-feu utilisant le filtrage simple. L'idée est de conserver les traces de sessions et de connexions dans des tables d'états internes aux pare-feu. Ces traces seront également prises en considération par les pare-feu lors de prise de décisions. Ces informations augmentent considérablement les capacités des pare-feu à détecter des attaques sophistiquées. Il reste, cependant, que les failles applicatives (les failles liées aux logiciels), qui sont à l'origine de la plus grande majorité de problèmes de sécurité, pour ce type de filtrage.
- **Le filtrage applicatif :**

Il a été proposé comme étant une amélioration supplémentaire du filtrage dynamique. Ce mécanisme est attaché au niveau de la couche application, où il peut extraire les données du protocole de niveau 7 pour les étudier. Le filtrage applicatif suppose une connaissance des protocoles utilisés par chaque application. Il permet la destruction des en-têtes précédant le message applicatif, ce qui permet de fournir un niveau de sécurité supplémentaire.

e. Les différents types de firewall :

Firewall matériel : Ils se trouvent souvent sur des routeurs achetés dans le commerce par de grands constructeurs comme Cisco ou Nortel. Intégrés directement dans la machine, ils font office de « boite noire » et ont une intégration parfaite avec le matériel .Ils sont aussi peu vulnérables aux attaques car présent dans la « boite noire » qu'est le routeur.

- **Firewall logiciel :** Les pare feux logiciels sont des programmes qui peuvent être installés sur un ordinateur en les téléchargeant directement à partir d'un site web ou les charger à partir d'un CD ou un DVD. Pare feu logiciels sont inclus dans le cadre d'un package de sécurité Internet. Norton Internet Security et Kaspersky Internet Security, par exemple, les deux sont livrés avec un pare feu.

f. Les avantages d'un firewall :

Les avantages d'un firewall peuvent être résumés dans les points suivants :

- ✓ **La protection contre des services vulnérables :** on peut par exemple définir que seules les connexions extérieures vers les services Web et FTP seront accepté sur un système hôte donné.
- ✓ **Le contrôle d'accès aux systèmes :** Le firewall fournit l'habilité à contrôler les accès aux systèmes du site protégé. Par exemple, on peut rendre accessibles certains des systèmes hôtes à partir de réseaux externes, tout en bloquant les accès vers les autres.
- ✓ **La concentration de la sécurité au niveau d'un seul point :** Le firewall est un outil qui permet de gérer en un seul point les accès vers ou en provenance du réseau local.
- ✓ **Les statistiques sur l'utilisation du réseau :** Si tous les accès passent par le firewall, ce dernier pourra fournir des statistiques sur l'utilisation du réseau. Si de plus, le firewall, possède des alarmes appropriées, il signalera une activité suspecte en donnant des informations sur l'attaque éventuelle.

g. Les problèmes et les limites des firewalls :

Malgré les avantages cités ci-dessus, un firewall présente un certain nombre de désavantages qui sont cités dans ce paragraphe.

- ✓ **Un potentiel pour l'exploitation des backdoors (portes dérobées) : l**es firewalls ne protègent pas contre les problèmes des backdoors. Par exemple, si un accès par modem non restrictif est autorisé à un site protégé par un firewall, les attaquants pourraient contourner ce dernier.

- ✓ **Une protection peu efficace contre les fuites d'information :** il ne peut empêcher, par exemple, un utilisateur interne de copier des données sur une bande et de l'emporter vers l'extérieur du site.
- ✓ **Les firewalls ne protègent pas contre le chargement de programmes infectés de virus à partir d'Internet** : il existe une multitude de méthodes de codage de fichiers binaires pour le transfert, et une variété d'architectures et de virus pour tenter de les détecter tous par le firewall.
- ✓ **Un système firewall est faillible comme tout autre système :** il faut veiller à ce qu'il soit sécurisé au maximum. [11]

II.6.6.DMZ (Zone démilitarisé) :

Une DMZ (Zone Démilitarisée) est une zone intermédiaire, du point de vue de la sécurité informatique, entre le réseau local de l'entreprise et l'Internet. Cette zone protégée et délimitée par un ou plusieurs pare-feu, est habituellement utilisée pour installer les serveurs de l'entreprise qui doivent être accessibles depuis le réseau Internet.

II.6.7. NAT (Network Address Translation) :

Le NAT consiste à établir des relations entre l'adresse privée dans un réseau et l'adresse publique pour se connecter à Internet. Donc, un routeur fait du NAT lorsqu'il fait correspondre les adresses IP internes privées (non uniques et souvent non routables) d'un Intranet à un ensemble d'adresses externes publiques (uniques et routables). Ce mécanisme permet notamment de faire correspondre d'une seule adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé.

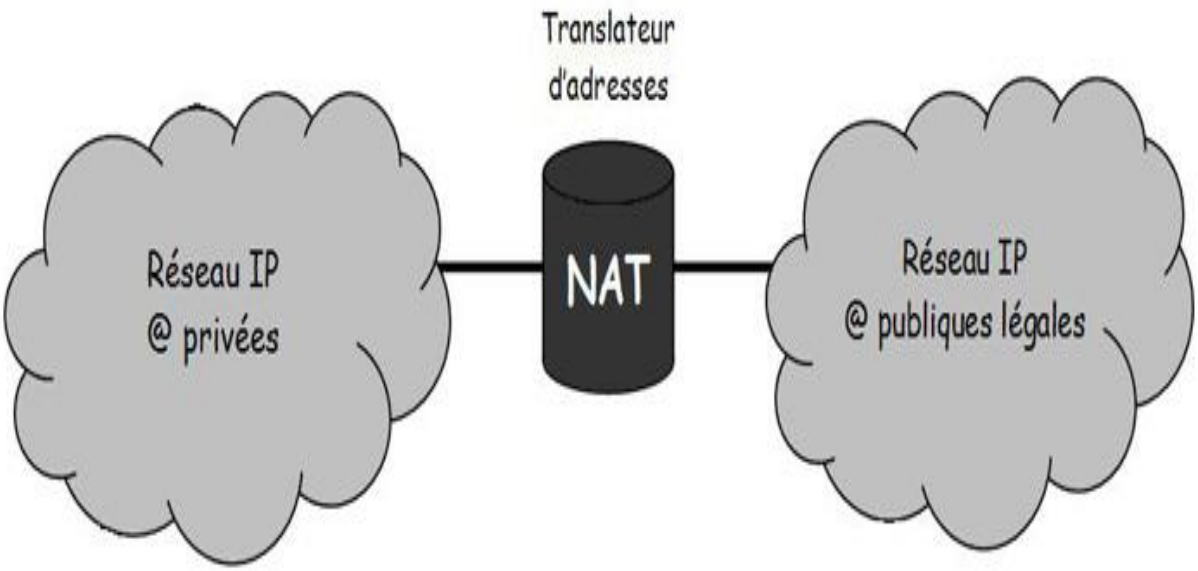


Figure II.14 : *Le réseau NAT.*

On distingue deux types du NAT :

- **NAT statique :** Le principe du NAT statique consiste à associer une adresse IP publique à une adresse IP privée interne au réseau. Le routeur (ou plus exactement la passerelle) permet donc d'associer à une adresse IP privée **(par exemple 192.168.0.1)**à une adresse IP publique routable sur Internet et de faire la traduction, dans un sens comme dans l'autre, en modifiant l'adresse dans le paquet IP.

- **NAT dynamique :** Le NAT dynamique permet de partager une adresse IP routable (ou un nombre réduit d'adresses IP routables) entre plusieurs machines en adressage privé. Le NAT dynamique utilise le mécanisme de translation de port (PAT : Port Address Translation), c'est-à-dire l'affectation d'un port source différent à chaque requête de telle manière à pouvoir maintenir une correspondance entre les requêtes provenant du réseau interne et les réponses des machines sur Internet, toutes adressées à l'adresse IP du routeur. [9]

Conclusion :

La sécurité d'un réseau est extrêmement importante au sien d'une entreprise. C'est pourquoi, la mise en place de solutions de protection, de surveillance tels que pare-feu permet de répondre à ce besoin de sécurisation. La sécurité ne révèle sa valeur qu'en cas de problème.

Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles est les différents types d'attaques et de prévoir la façon de procéder pour se protéger (sécurisation) contre ces menaces. Dans le prochain chapitre, nous présenterons le pare-feu Pfsense qui sécurise l'entreprise ENIEM et leurs différentes étapes d'installation et configuration.

III.1.Introduction :

L'objectif de cette partie est de mettre en œuvre une infrastructure réseau sécurisé par le pfsense (pour voir son emplacement dans l'entreprise ENIEM vous pouvez aller dans les annexes), ce dernier permet aux clients de l'entreprise de partager des informations et des données en tout sécurité afin d'améliorer sa réactivité et sa compétitive.

III.2.pré-requis :

Pour la réalisation de notre travail, nous disposons des paramètres suivant :

- Une machine virtuelle « Virtualbox » ;
- Un pare feu « Pfsense », qui dispose deux cartes réseaux une pour l'interface LAN et l'autre pour l'interface WAN ;
- Trois machines clientes XP, qui dispose une seule carte réseau chaque une.
    - **Installation de VirtualBox :**

Figure III.1 *: installation de virtualbox*

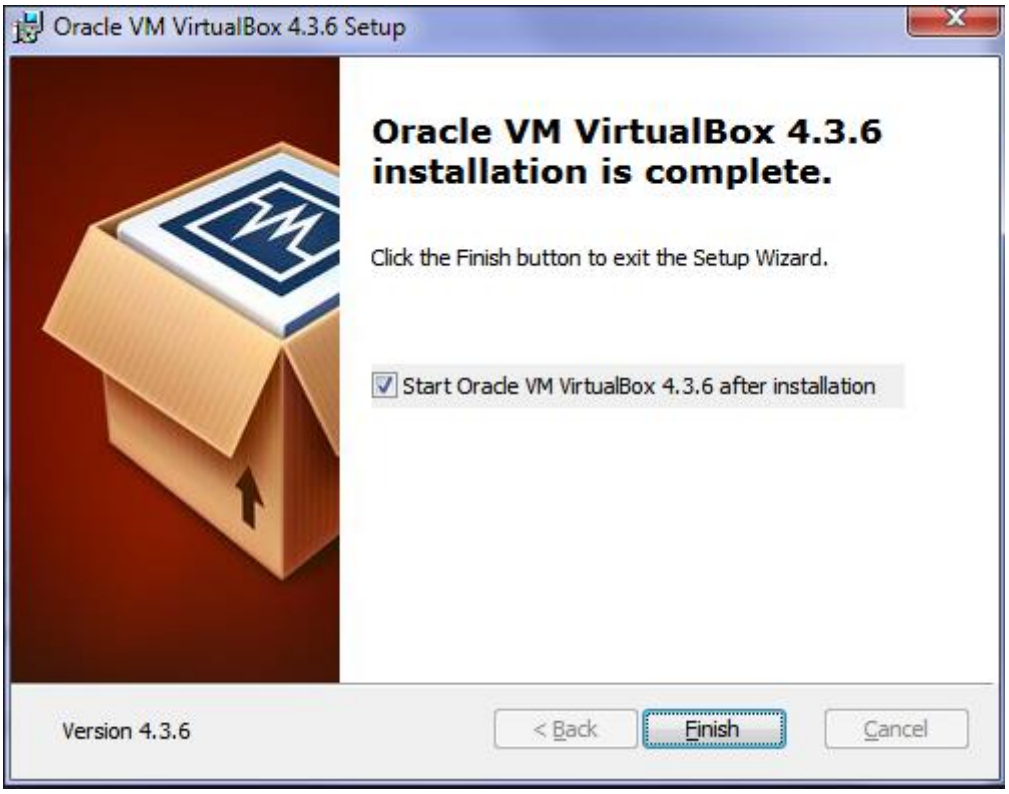
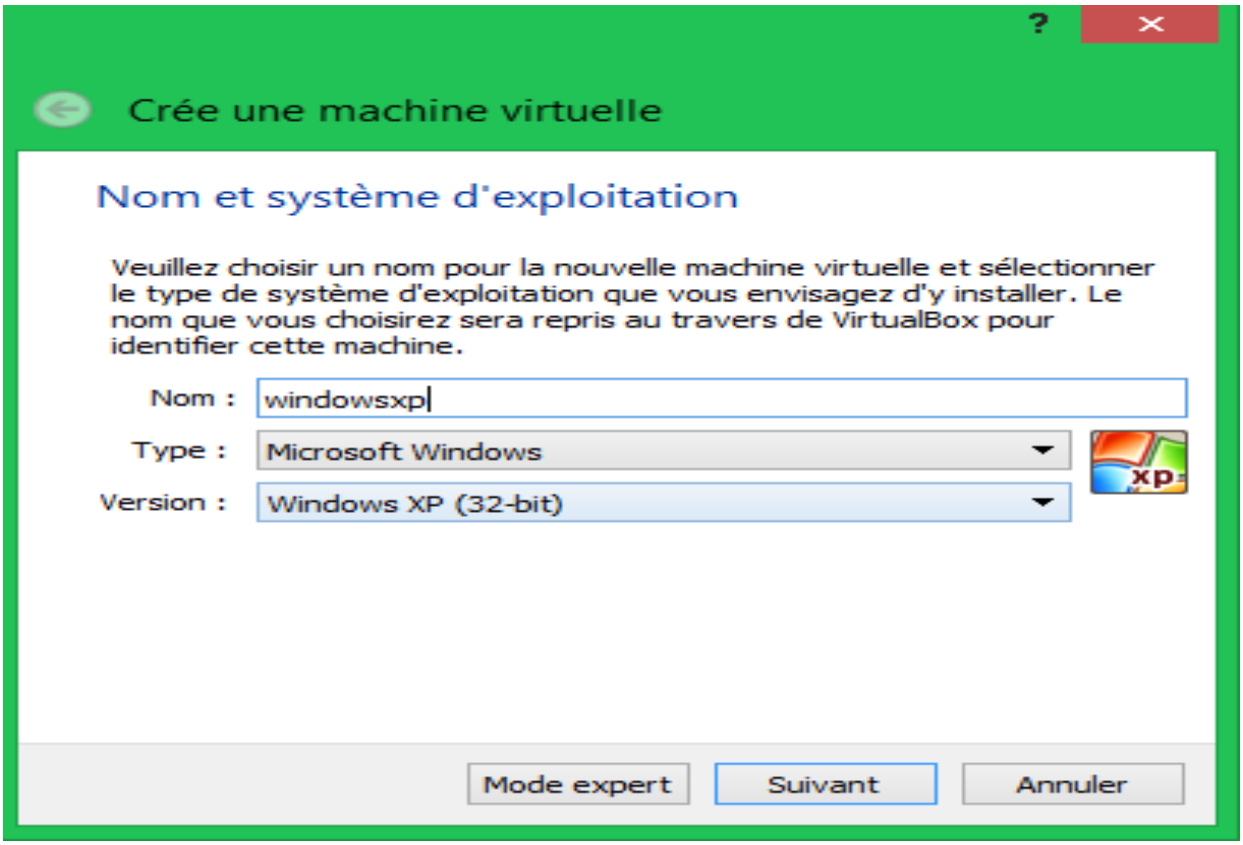


Figure III.2 : fin d'installation de la machine virtuelle.

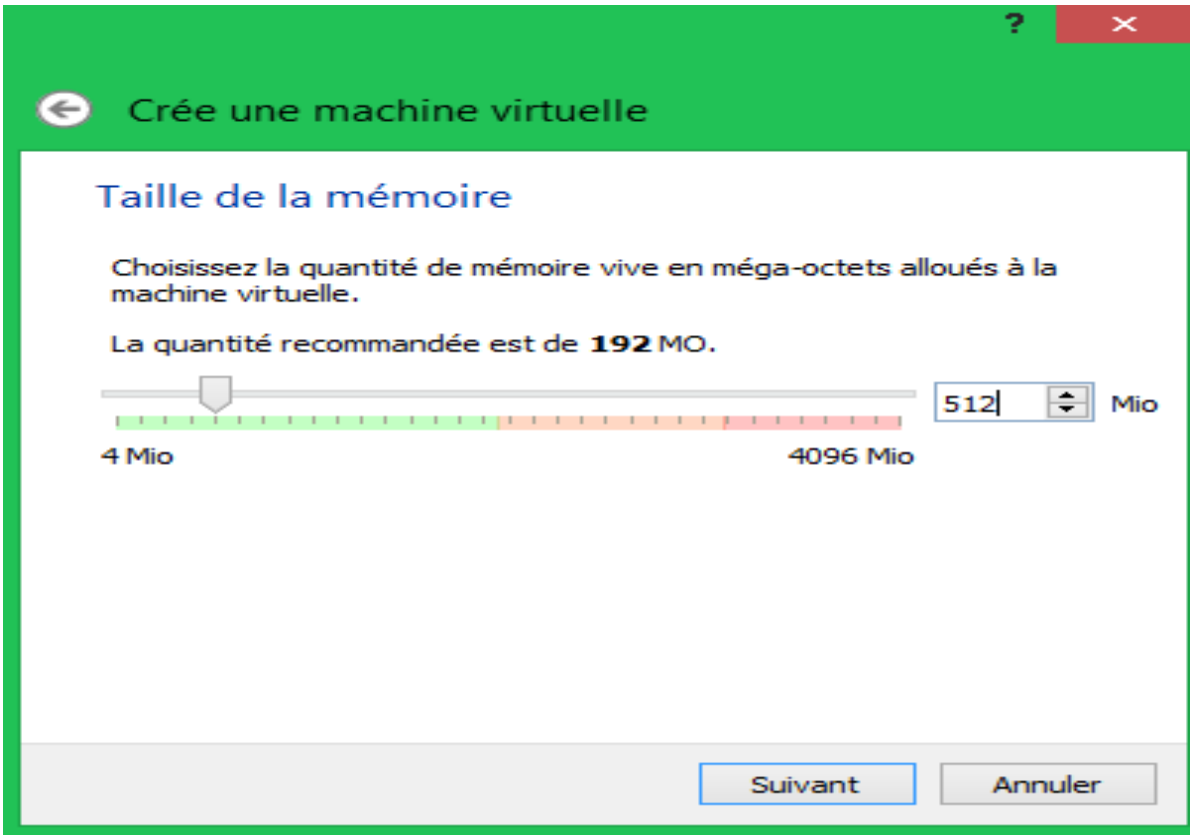
- **Les étapes d'installation et configuration de la machine cliente XP sur le virtualbox :**

Télécharger limage iso de client XP :

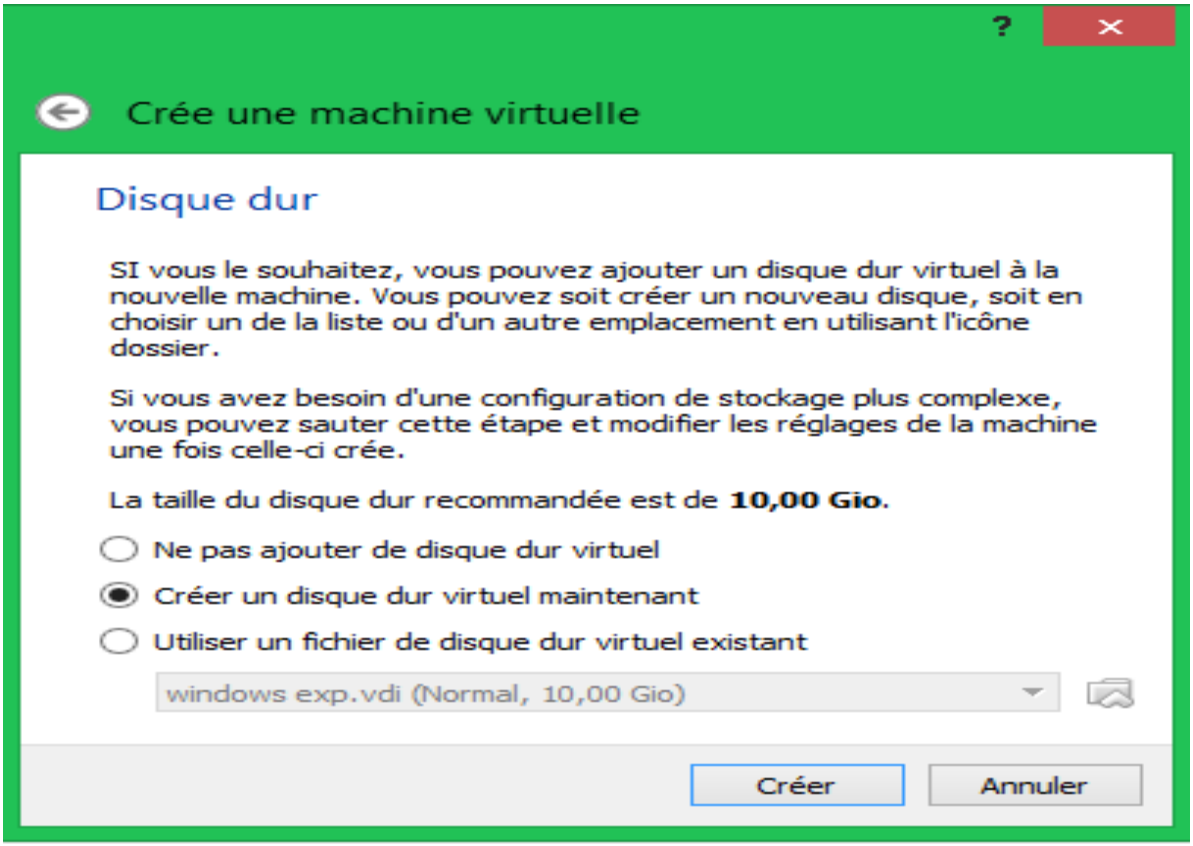


Premièrement, on choisit un nom pour la machine client (Windows XP par exemple), puis nous cliquons sur **« suivant ».**

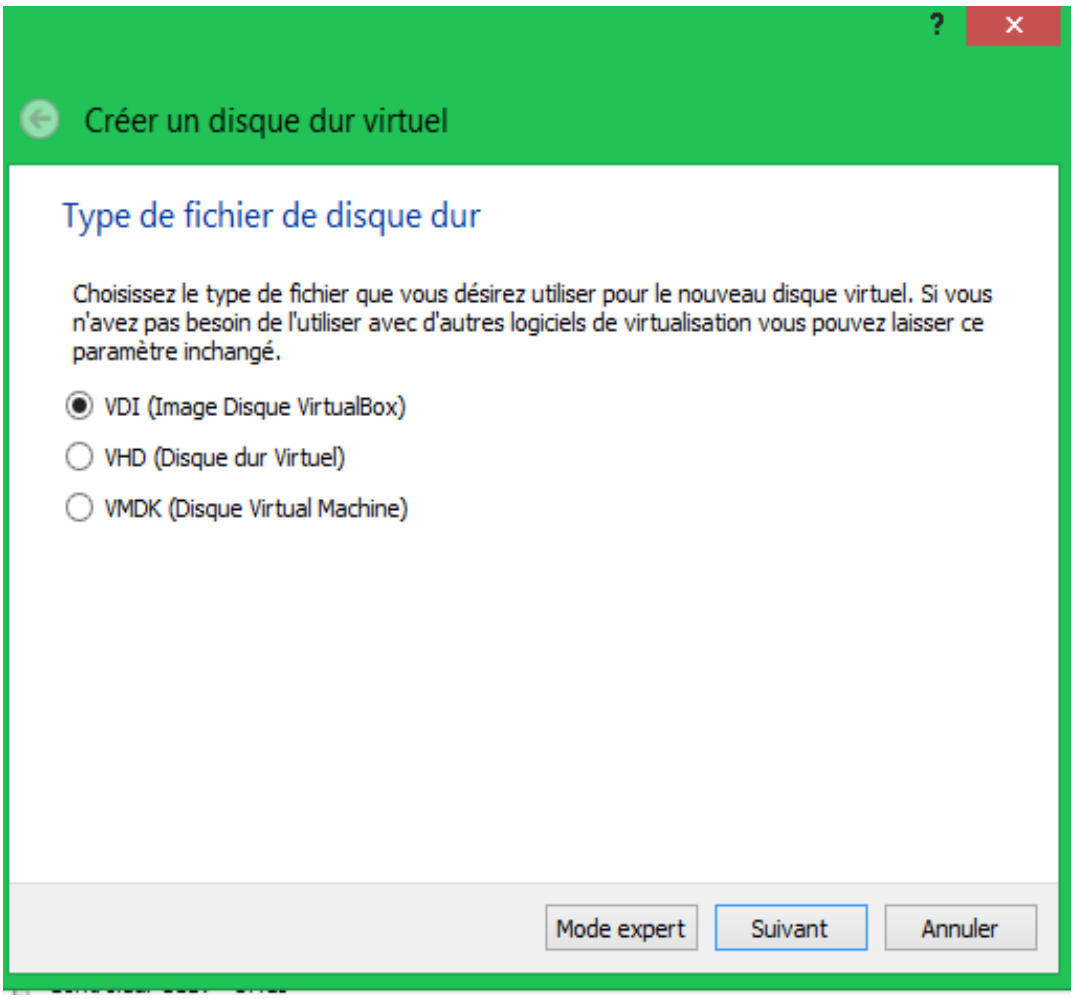
Dans la seconde étape, on donne une taille de la mémoire pour la machine en méga-octets (on a choisi 512 MO).



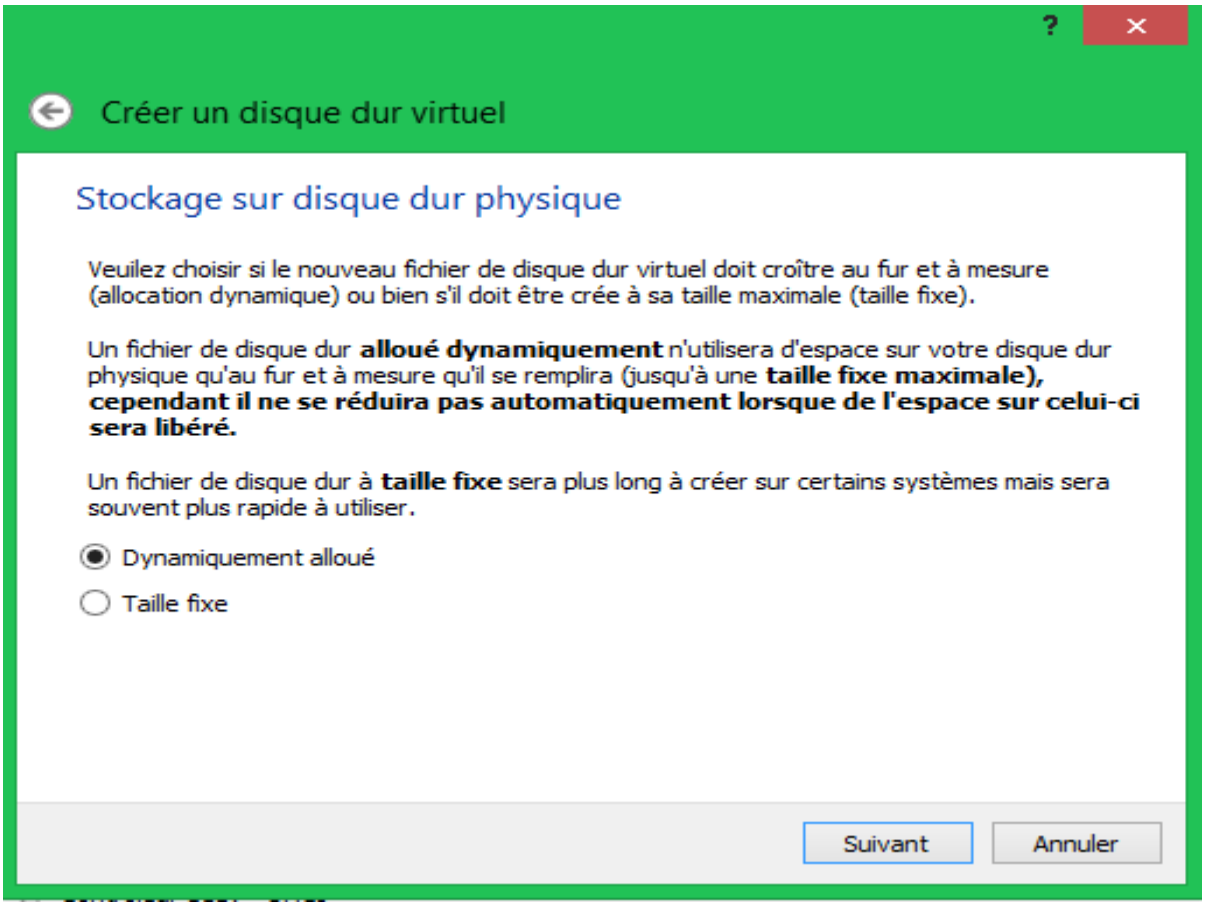
Pour la création du disque dur, nous choisissons **« créer un disque dur virtuel maintenant »,** puis on clique sur **« créer ».** (Nous avons créé un disque dur 10 GO).

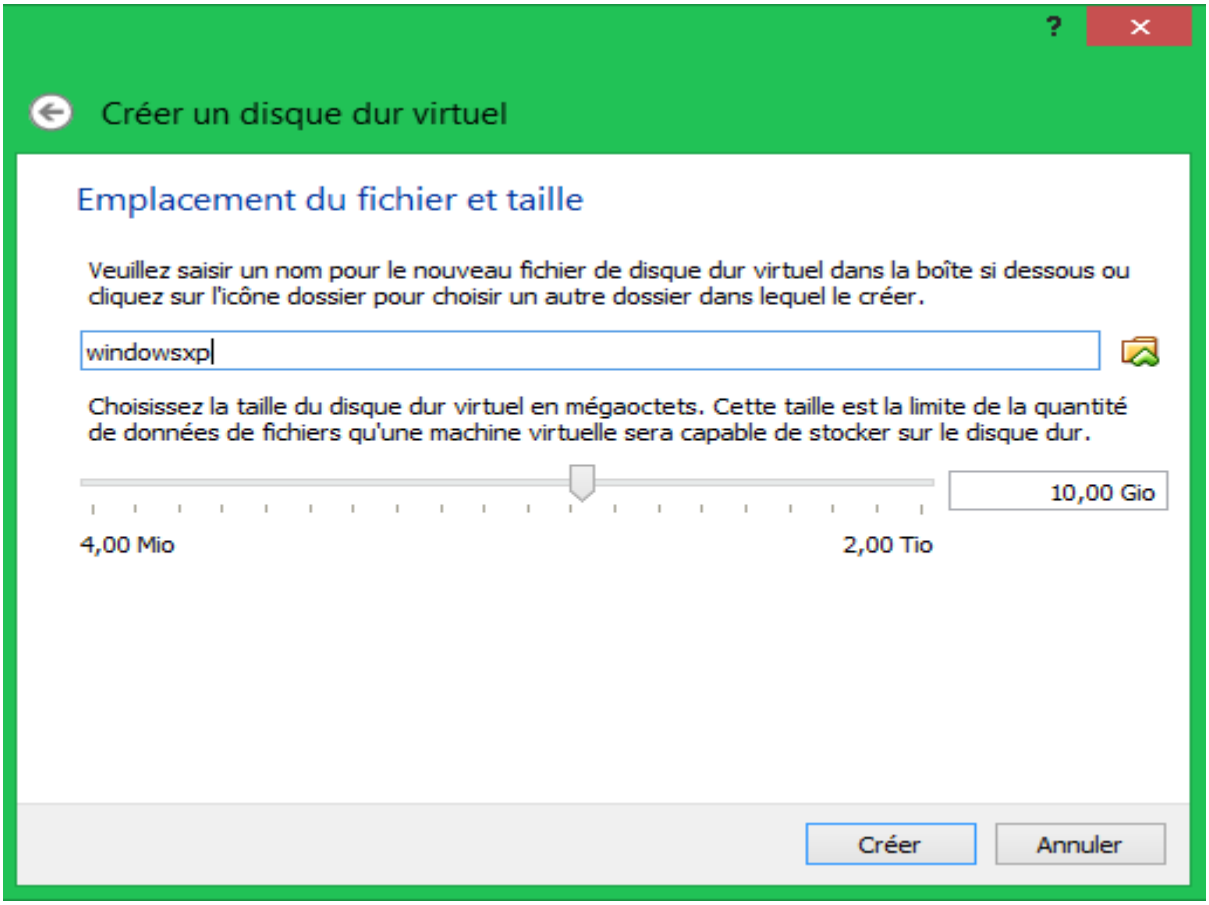


Pour le type de fichier du disque dur, on a choisi **VDI** (image disque VirtualBox) et on clique sur **« suivant »**, parce qu'on fera l'installation de la machine avec l'image ISO Windows XP.

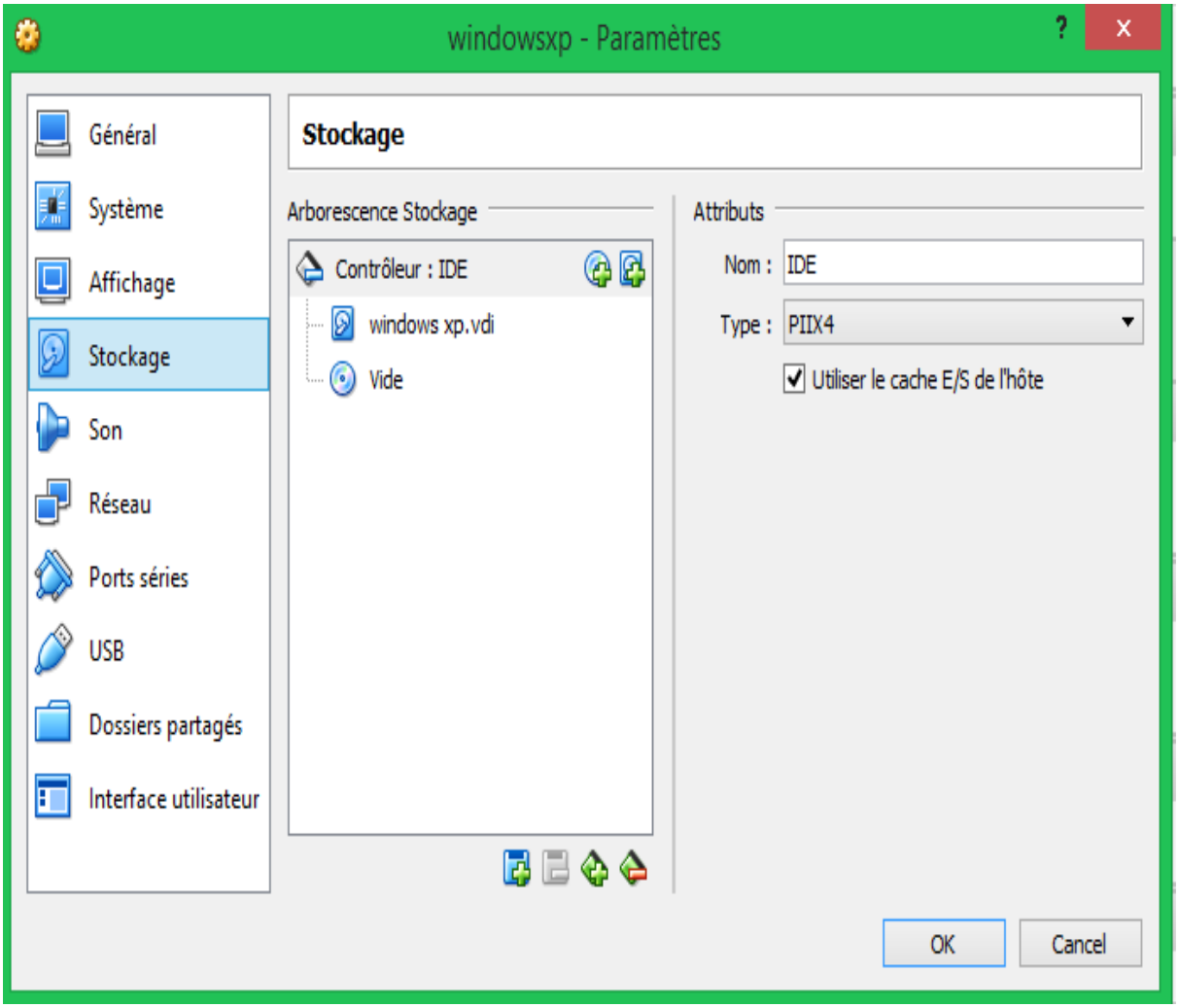


Et pour le stockage de nouveau fichier sur disque dur physique, nous choisissons **« dynamiquement alloué »**, puis on clique sur **« suivant »** comme illustre la figure suivante :

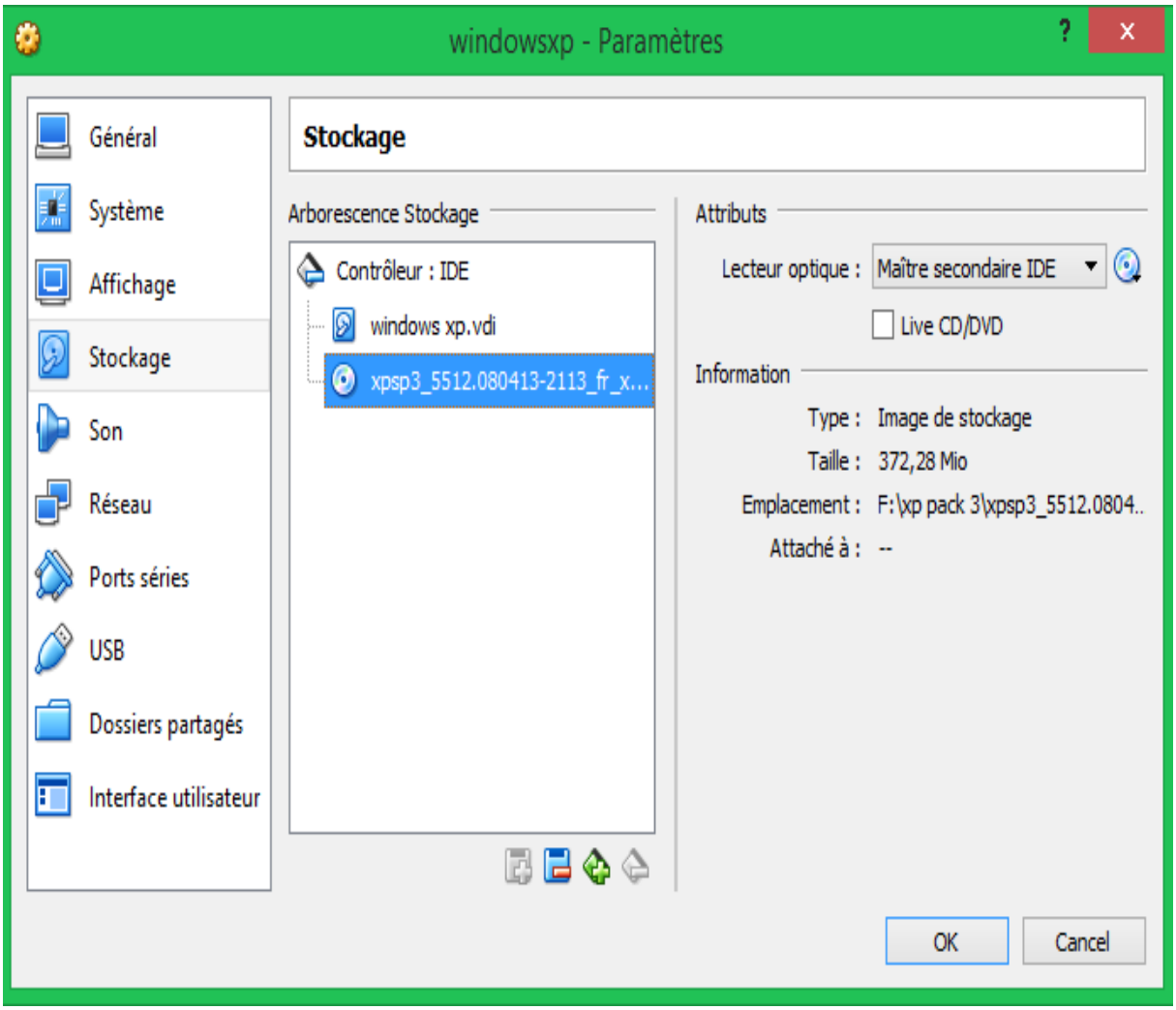

Créer un disque dur virtuel
Stockage sur disque dur physique
Veuilez choisir si le nouveau fichier de disque dur virtuel doit croître au fur et à mesure (allocation dynamique) ou bien s'il doit être crée à sa taille maximale (taille fixe).
Un fichier de disque dur alloué dynamiquement n'utilisera d'espace sur votre disque dur physique qu'au fur et à mesure qu'il se remplira (jusqu'à une taille fixe maximale), cependant il ne se réduira pas automatiquement lorsque de l'espace sur celui-ci sera libéré.
Un fichier de disque dur à taille fixe sera plus long à créer sur certains systèmes mais sera souvent plus rapide à utiliser.
Dynamiquement alloué
Taille fixe
Suivant
Annuler


Créer un disque dur virtuel
Emplacement du fichier et taille
Veuillez saisir un nom pour le nouveau fichier de disque dur virtuel dans la boîte si dessous ou cliquez sur l'icône dossier pour choisir un autre dossier dans lequel le créer.
windowsxp
Choisissez la taille du disque dur virtuel en mégaoctets. Cette taille est la limite de la quantité de données de fichiers qu'une machine virtuelle sera capable de stocker sur le disque dur.
10,00 Gio
4,00 Mio
2,00 Tio
Créer
Annuler

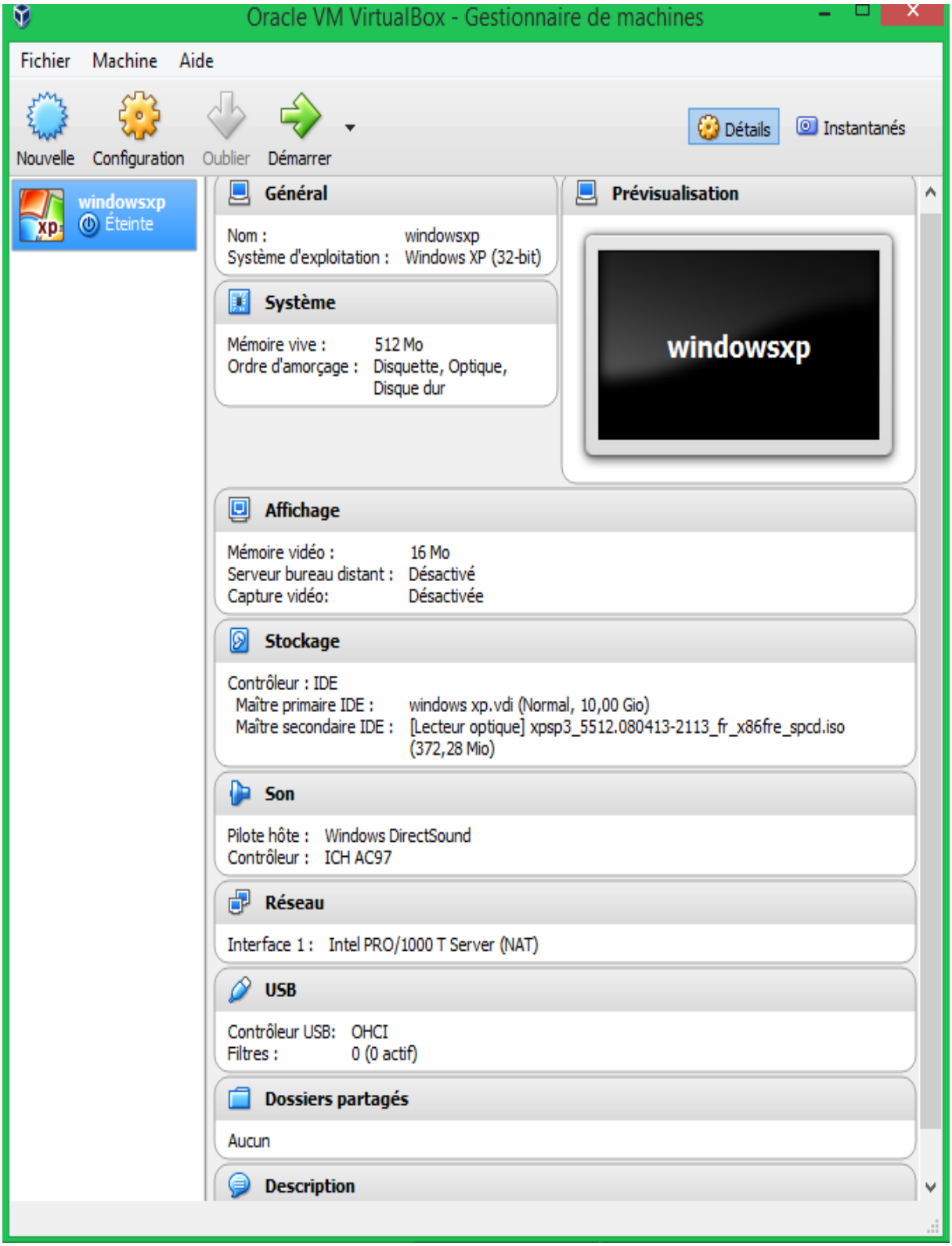
Pour le réglage des paramètres, on clique sur **« stockage »** et dans l'arborescence stockage, nous cliquons sur « **vide »** pour télécharger l'image ISO Windows XP.



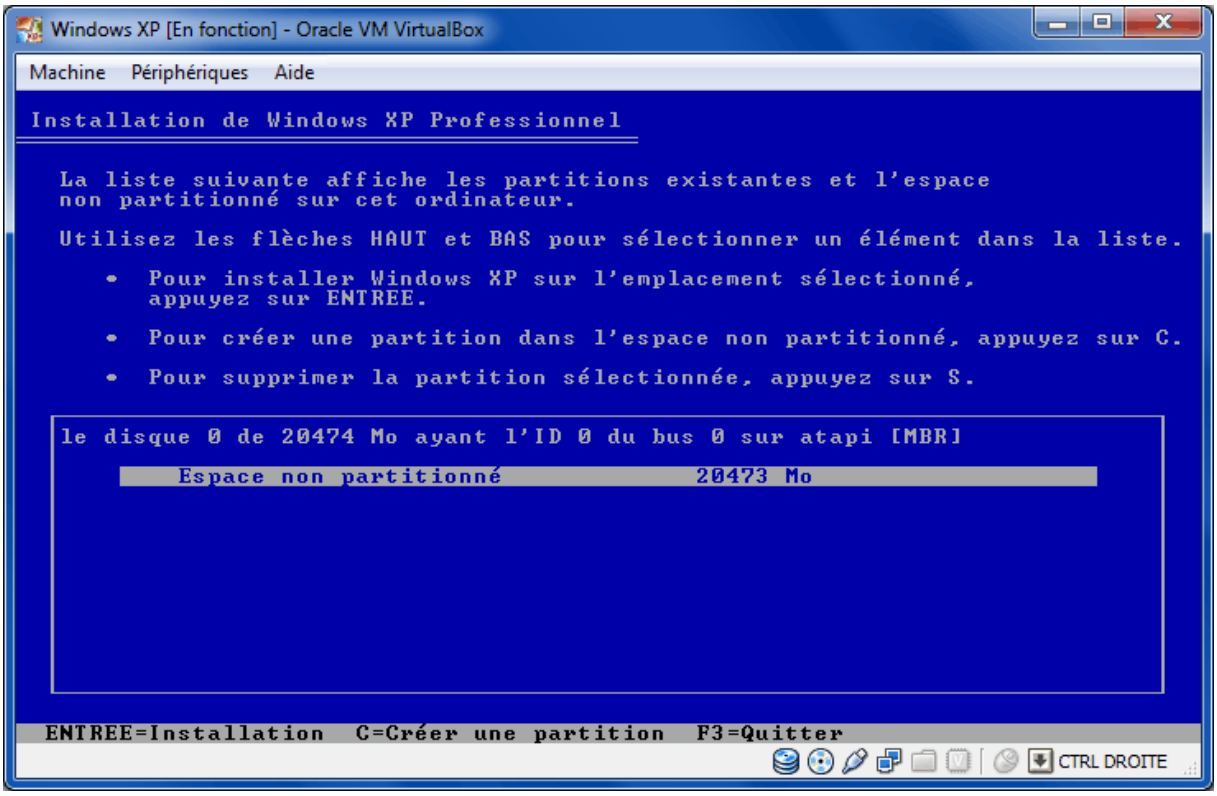
Nous cliquons sur le disque qui se trouve dans la lecture optique, on choisit un fichier du disque optique virtuel : **Windows-XP-Service-Pack-3.iso** puis on clique sur « OK ».



Après avoir vérifié tous les paramètres dans la fenêtre de VirtualBox, on fera lancer notre machine cliente XP et pour cela on clique sur **« démarrer »**.



Après avoir fait démarrer la machine, nous suivons quelque étape pour faire l'installation de cette machine.


Windows XP [En fonction] - Oracle VM VirtualBox
Machine Périphériques Aide
Installation de Windows XP Professionnel
La liste suivante affiche les partitions existantes et l'espace non partitionné sur cet ordinateur.
Utilisez les flèches HAUT et BAS pour sélectionner un élément dans la liste.
• Pour installer Windows XP sur l'emplacement sélectionné, appuyez sur ENTREE.
• Pour créer une partition dans l'espace non partitionné, appuyez sur C.
• Pour supprimer la partition sélectionnée, appuyez sur S.
le disque 0 de 20474 Mo ayant l'ID 0 du bus 0 sur atapi [MBR]
Espace non partitionné 20473 Mo
ENTREE=Installation C=Créer une partition F3=Quitter
CTRL DROITE

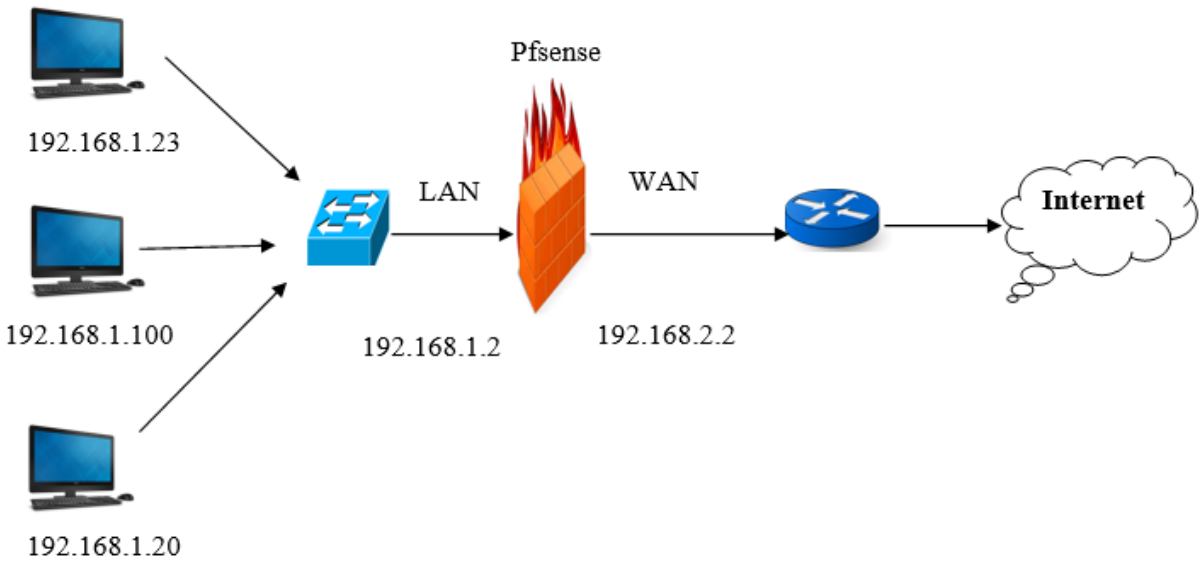

Windows XP [En fonction] - Oracle VM VirtualBox
Machine Périphériques Aide
Microsoft Windows xp
Bienvenue dans ce système d'exploitation de Microsoft
Merci d'avoir acheté Microsoft Windows XP.
Prenons quelques minutes pour préparer votre ordinateur.
Pour continuer, cliquez sur Suivant.
Pour obtenir de l'aide, cliquez ici ou appuyez sur F1.
Suivant
CTRL DROITE

III.3.Les étapes d'installation de Pfsense :

III.3.1. Présentation :

Pfsense est un système d'exploitation transformant n'importe quel ordinateur en routeur/pare-feu. Basé sur Free BSD, connu pour sa fiabilité et surtout sa sécurité, Pfsense est un produit Open Source adapté à tout type d'entreprise.

- **Schéma explicatif :**



III.3.2.Télécharger l'image ISO Pfsense :

Pour faire fonctionner pfsense nous avons besoin d'une image iso de 32 bits « pfsense-CE-2.3.3-RELEASE-amd32.iso », que vous pouvez télécharger sur le lien suivant :

https://www.pfsense.org/download/mirror.php?section=downloads.

III.3.3.Installation :

Nous réalisons l'installation sur une VM (machine virtuelle) depuis Virtualbox, la procédure d'installation est la même si vous êtes sur une machine physique.

Lors du démarrage de l'ordinateur avec le CD ou l'ISO (image iso pfsense) monté, un menu de boot apparaît.

Une fois l'image gravée, on boot sur le CD et on arrive aux menus suivants :

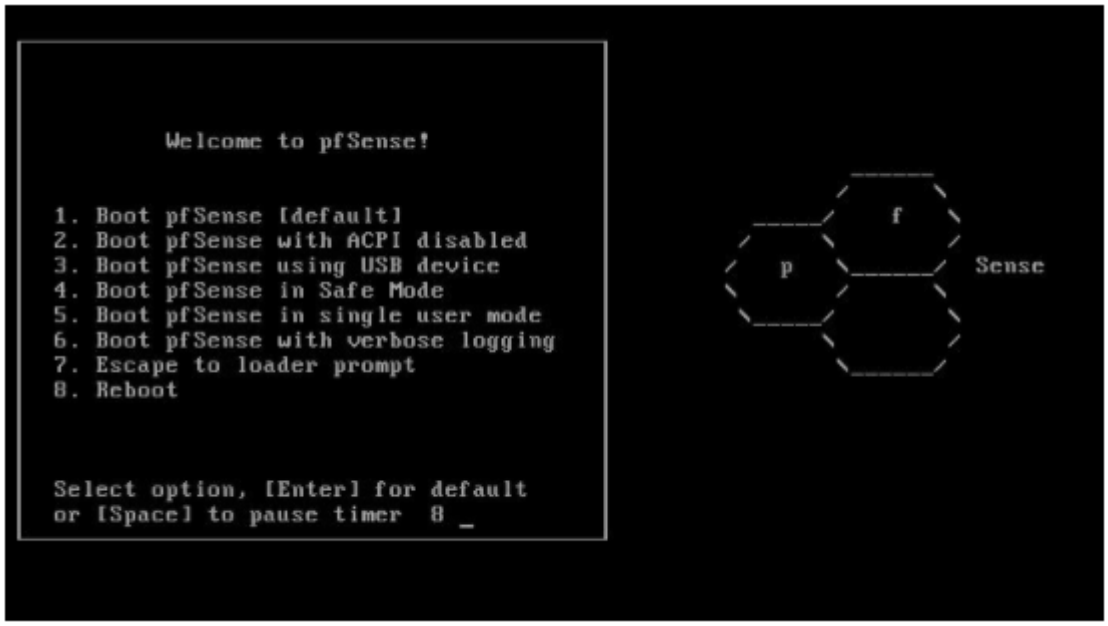


Figure III.3. :*Pfsense sur virtualbox.*

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.

L'installation va se poursuivre un moment, avec un enchainementde commandes, jusqu'à s'arrêter sur l'écran suivant :

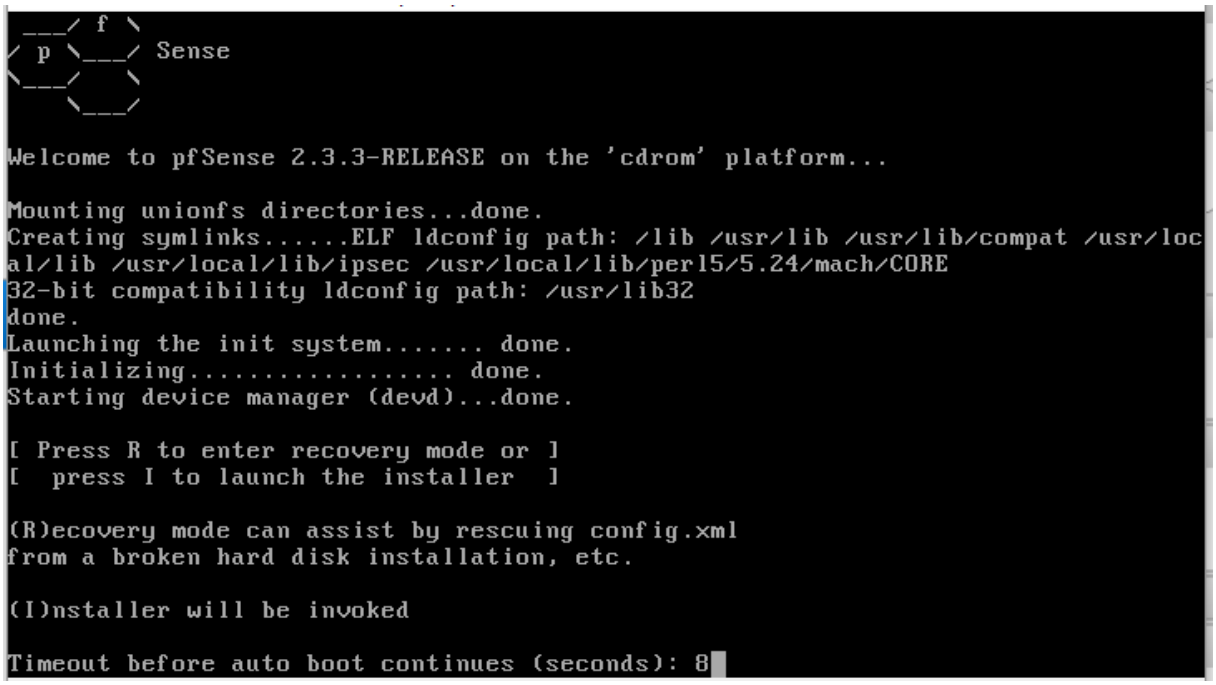
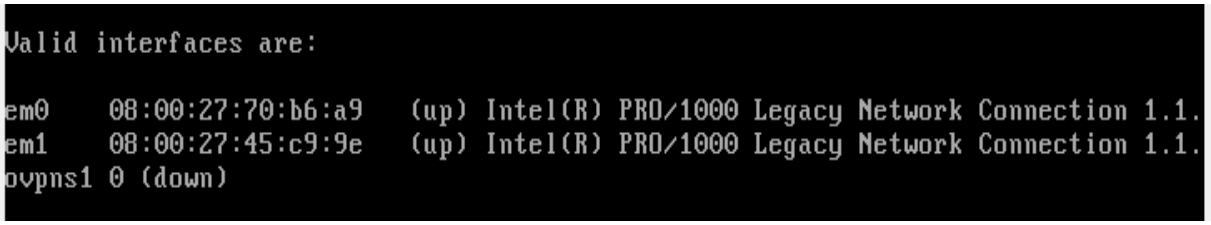


Figure III.4. : *Lancement de l'installation.*

L'assistant d'installation détecte bien les deux cartes réseaux, qui sont nommées « em0 » pour l'interface WAN et « em1 » pour l'interface LAN.



FigureIII.5 : *Détection des cartes réseaux.*

- **Le début d'installation de l'ISO Pfsense :**

Nous laissons tout par défaut, il suffit d'accepter toutes les demandes (formatage si nécessaire et création de la partition), et nous continuons l'installation en cliquant sur « Acceptthese Settings » et nous cliquons sur « Entrée ».

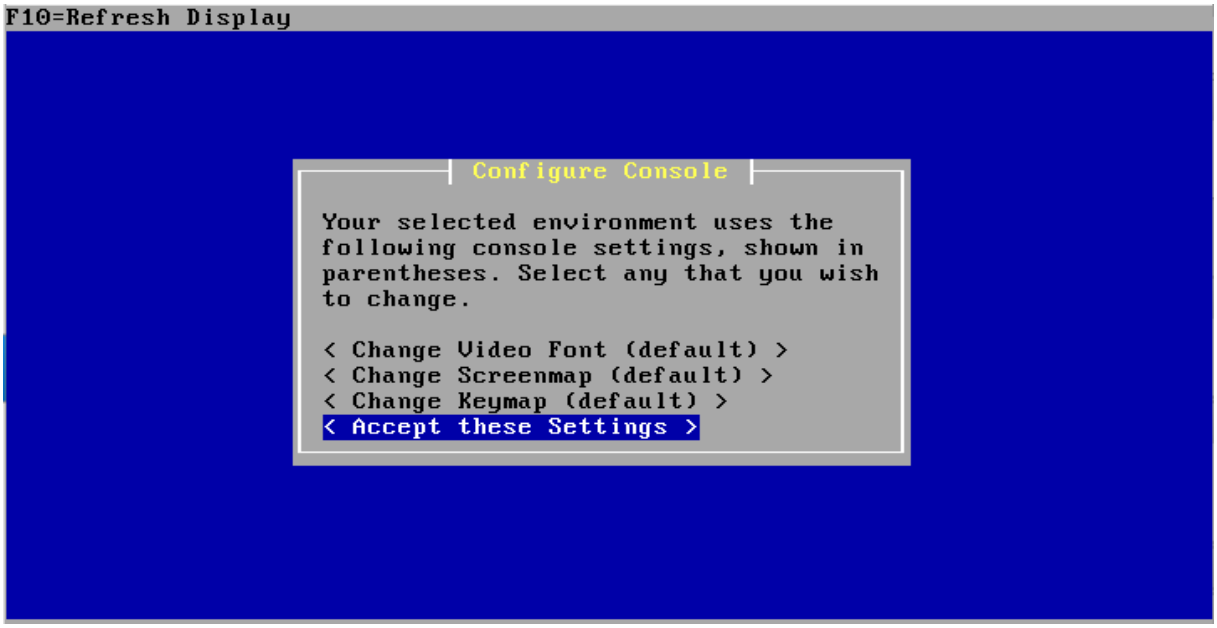


Figure III.6 :*Acceptation de l'installation.*

Dans l'étape suivant pour lancer l'installation nous choisissons**Quick/Easy Install**, pour faire une installation facile.

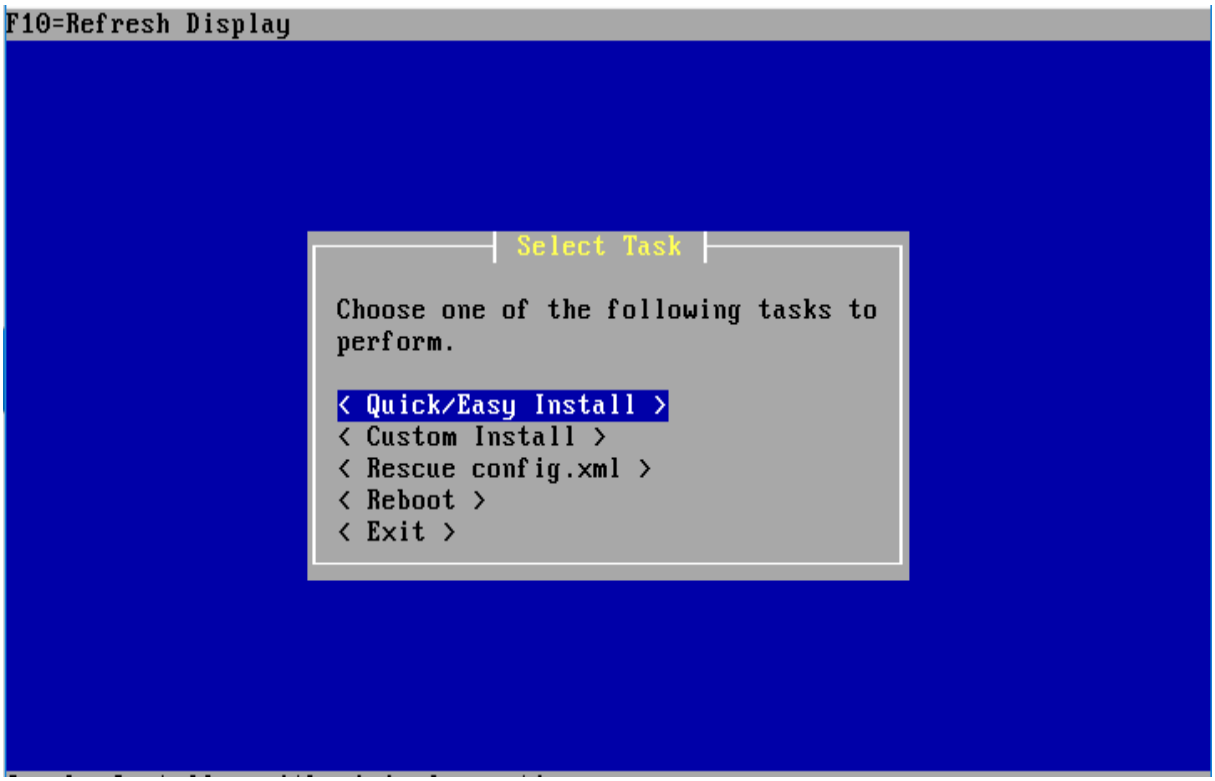


Figure III.7 :*Installation facile.*

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

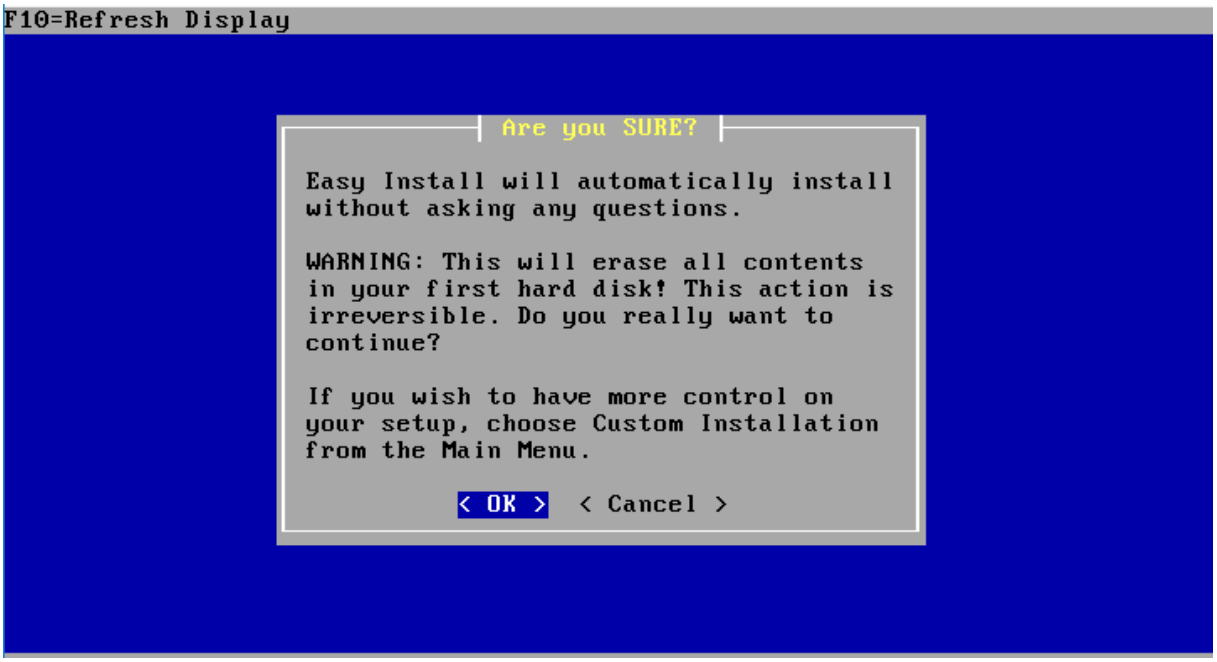


Figure III.8:*Installation et formatage du disque.*

L'installation débute et copie les fichiers nécessaires sur le disque dur et dans quelque seconde, nous obtenons la figure suivante :

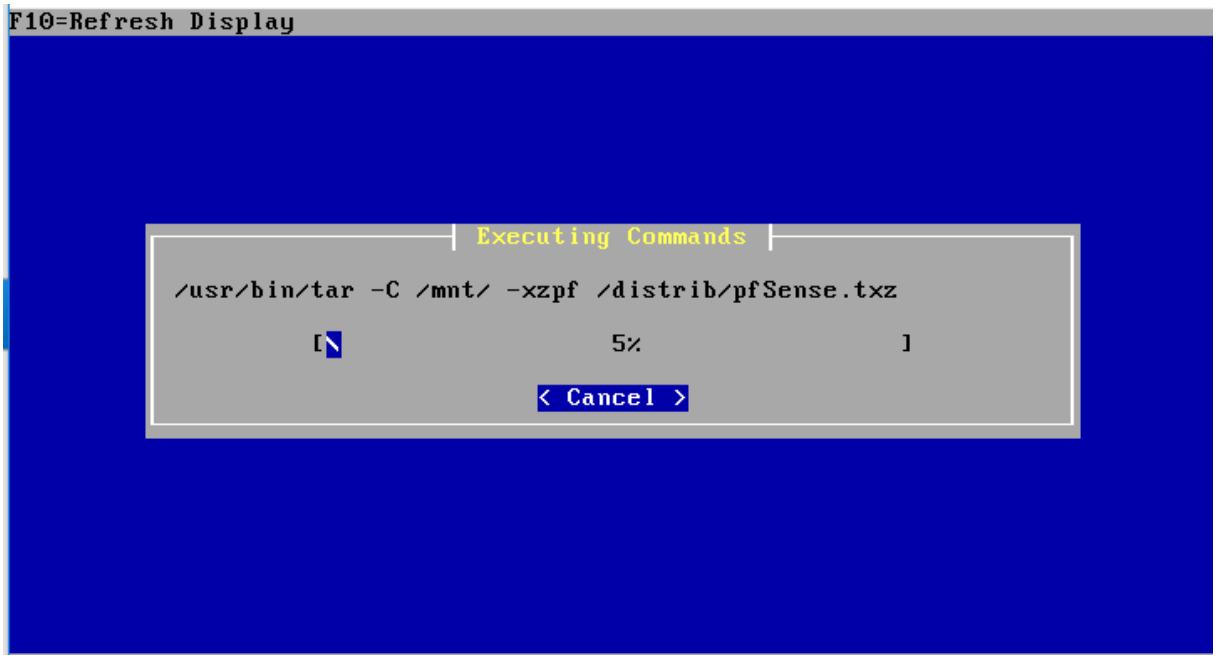


Figure III.9: *Installation et copie des fichiers.*

Dont l'étape suivante nous cliquons sur l'option « Standard kernel »,et celle qui est sélectionné par défaut car c'est le plus simple à utiliser. En effet, le second kernel « Embedded kernel » ne dispose pas d'accès à la console.

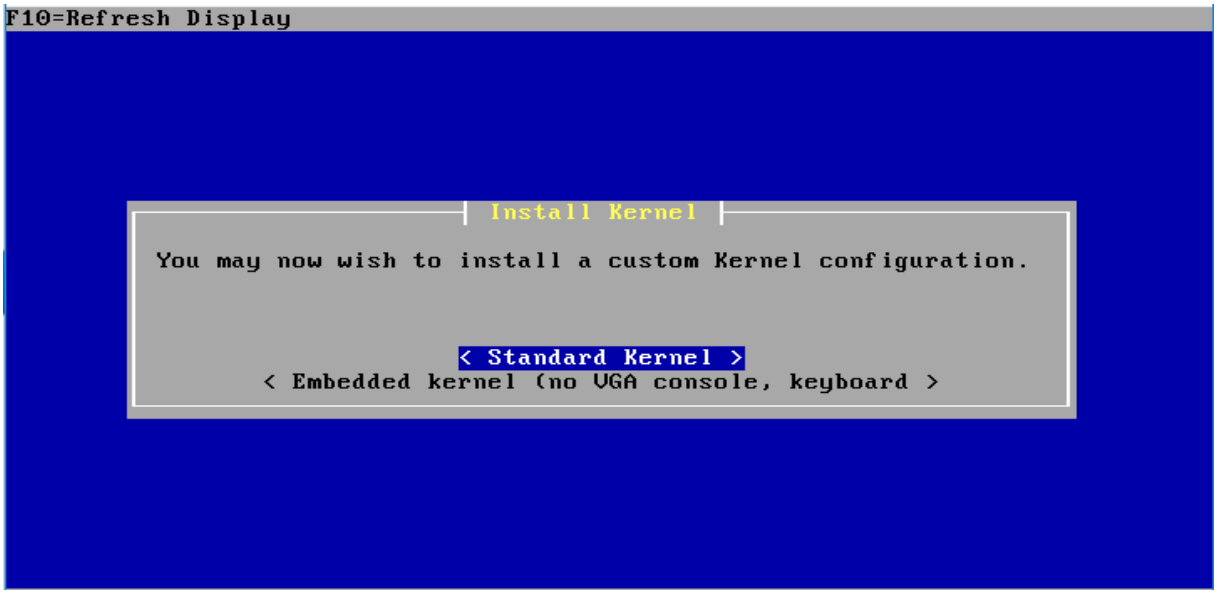


Figure III.10 :*Installation du noyau.*

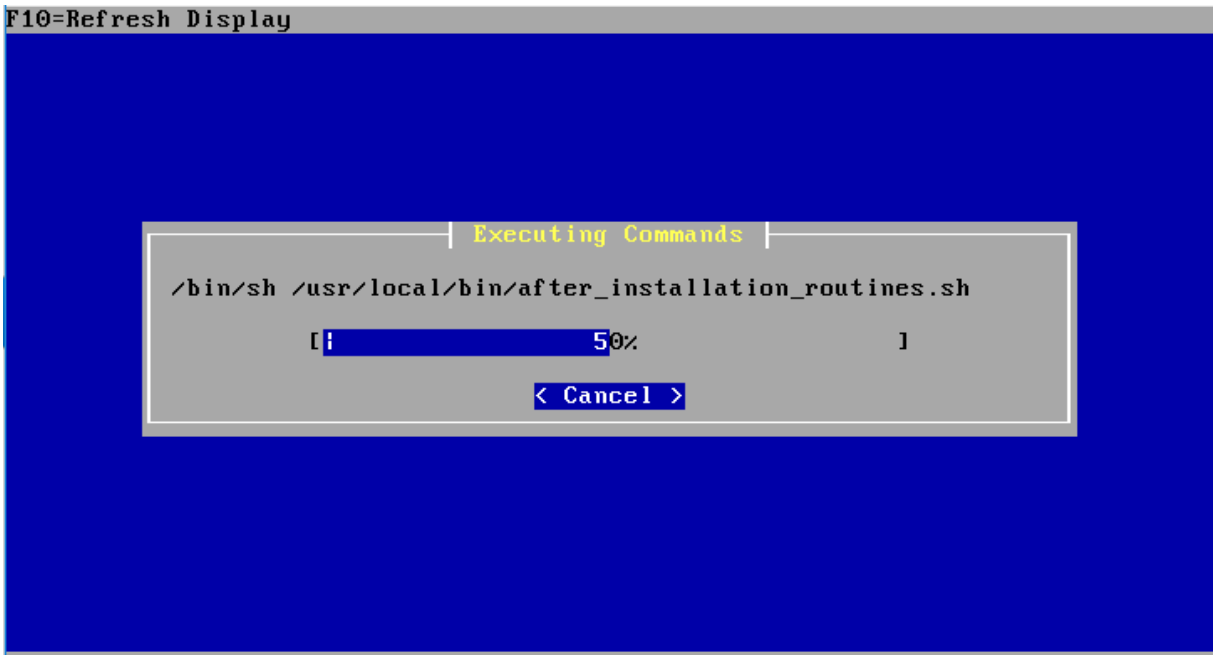


Figure III.11 :*Installation du noyau 2.*

Après quelques secondes nous obtenons la figure suivante :

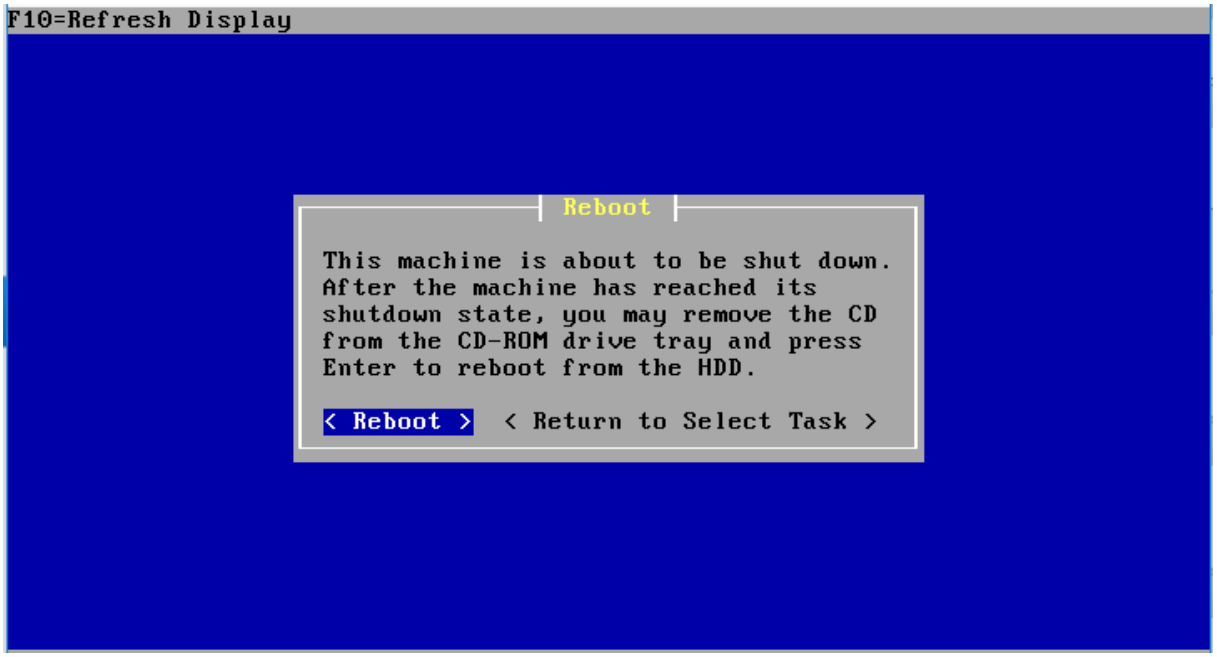


Figure III.12 :*Rebooter.*

Après quelques minutes Pfsense sera intégralement installé.

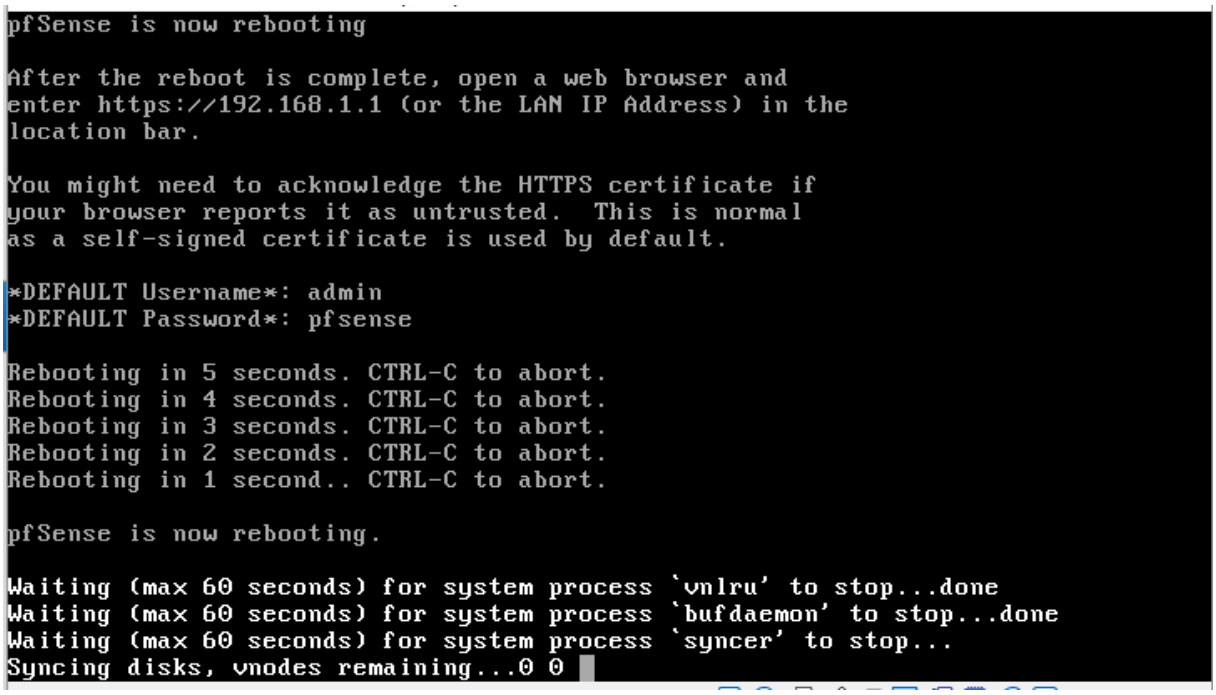
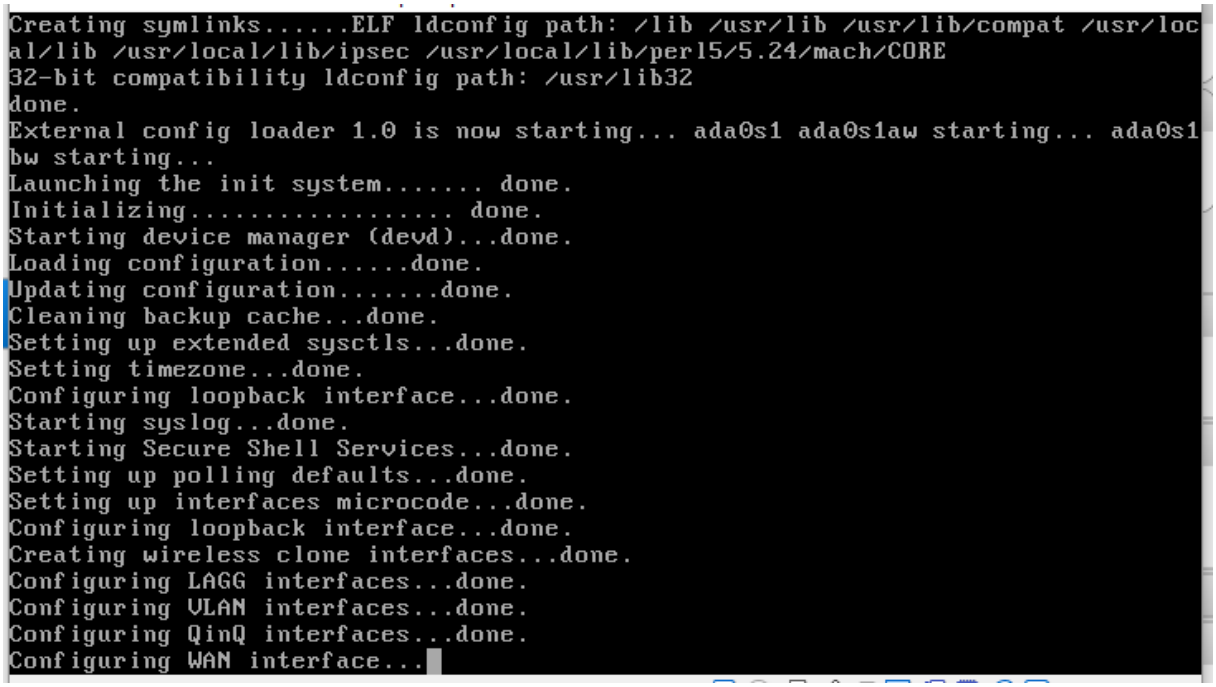


Figure III.13 :*Installation de Pfsense 3.*

Les divers services vont donc pouvoir se lancer.



Il faut obligatoirement redémarrer votre machine et il est nécessaire de retirer l'image ISO de Pfsense avant de le redémarrer.

- **Premiers paramétrages de Pfsense :**

L'installation est terminée, il va désormais falloir effectuer quelques paramétrages afin de pouvoir accéder au pare-feu depuis son interface. La machine démarre sur le nouveau système, et nous devons obtenir cet écran :

Figure III.14 : *Démarrage du système.*

Nous appuyons sur F1 ou bien nous patientons quelques instants.Le temps de chargement des divers paramètres du système d'exploitation peut être long, mais on arrive ensuite à l'écran suivant :

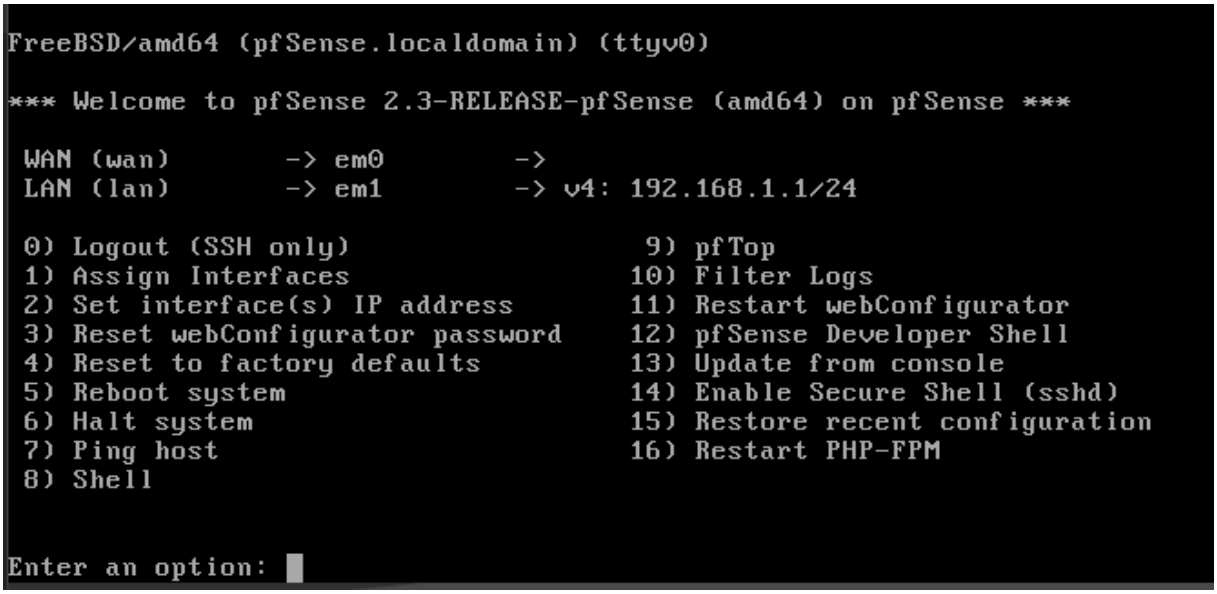


Figure III.15: *Configuration des interfaces.*

Nous sommes maintenant sur la console principale de Pfsense. Il s'agit d'un menu qui nous donnant l'accès à certaines options pour configurer notre pare-feu. A partir de ce point, le Pfsense est installé et fonctionnel.

a. Configuration des cartes réseau :

Dans notre cas « em0 » correspond à l'interface WAN par contre « em1 » correspond à l'interface LAN qu'il faudra configurer.

L'adresse par défaut du LAN est 192.168.1.1 si l'adresse attribue par le serveur automatique DHCP, nous allons la modifier en 192.168.1.2, pour l'intégrer lePfsense à notre réseau.

Nous choisissons l'option « 2 » dans le menu principal de pfsense dans la figure III.15 pour changes les 'interface LAN et WAN. Après nous choisissons l'option 2 dans la figure III.16 pour modifier l'adresse de LAN.

Figure III.16 : *Choix de l'interface à configurer.*

Nous saisissons la valeur **24** correspondant au masque **255.255.255.0.**

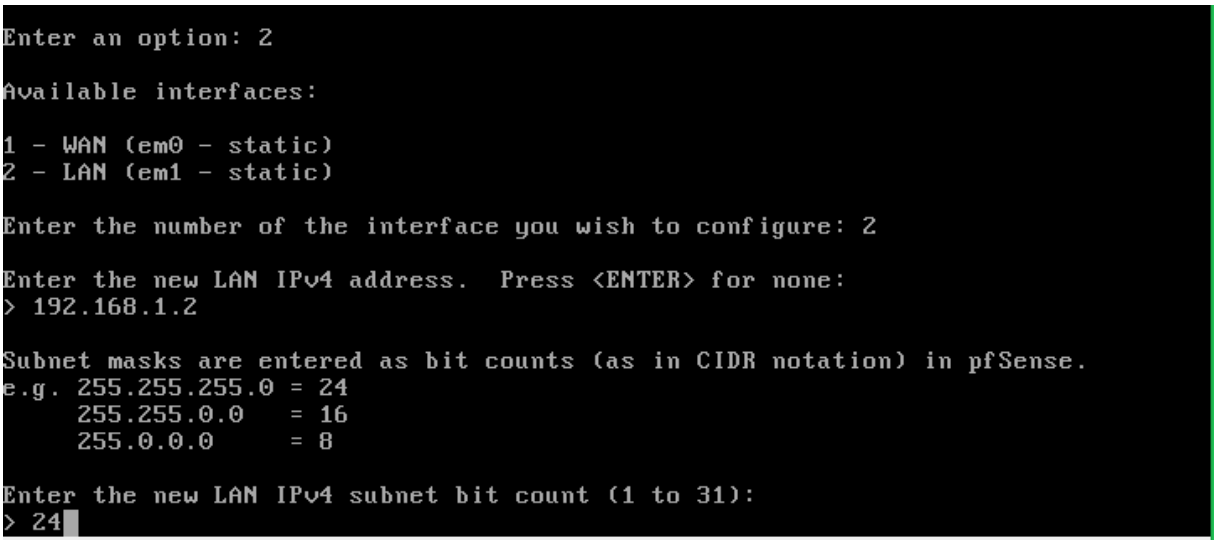


Figure III.17 : *Choix du masque sous-réseau.*

Nous appuyons deux fois sur**Entrée** pour ne pas définir de passerelle puis une troisième fois pour ne pasdéfinir d'adresse IPV6. Entrez **N** pour **NON** afin de ne pas activer le service DHCP.

```
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Enter the new LAN IPv6 address.  Press <ENTER> for none:
> N

Enter the new LAN IPv6 address.  Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) N

Please wait while the changes are saved to LAN...
 Reloading filter...
 Reloading routing configuration...
 DHCPD...

The IPv4 LAN address has been set to 192.168.1.2/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                http://192.168.1.2/

Press <ENTER> to continue.
```

Figure III.18 : *Finde la configuration de LAN.*

Notre interface LAN est maintenant configurée. Donc nous effectuons la même manipulation pour la carte réseau WAN et à la fin nous aurons cette figure :

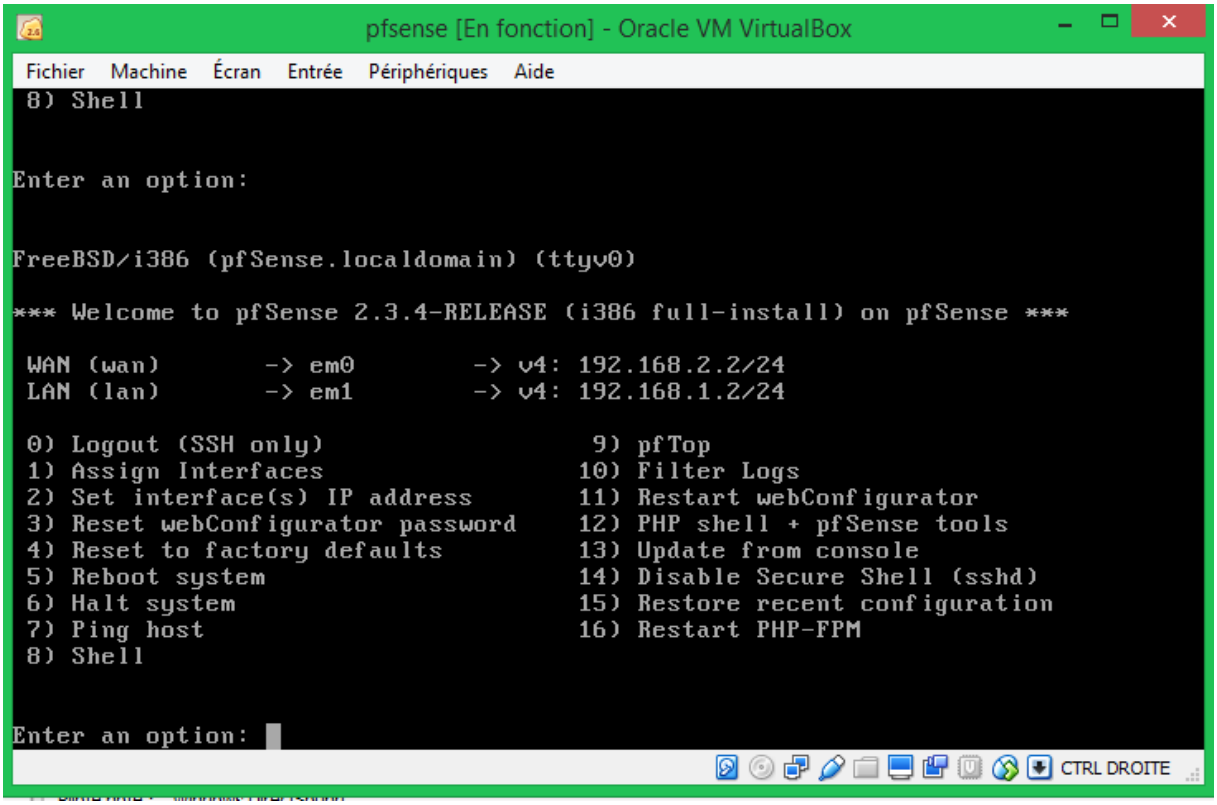


Figure III.19 :*Menu de la console de Pfsense.*

Donc les deux cartes sont configurées.Nous pouvons accéder au*Pfsense*à partir d'une interface Web (Google chrome) qui se trouve dans la machine client XP (l'adresse IP de cette machine est le 192.168.1.100).

III.4.Configuration de Pfsense :

Pfsense est désormais disponible à l'adresse du LAN : 192.168.1.2.C'est à partir de cette adresse que toutes les manipulations vont se dérouler.

URL de serveur web(coté LAN)	http://192.168.1.2/
Identifiant	Admin
Mot de passe	Pfsense

Et voilà la page de connexion à l'interface web.

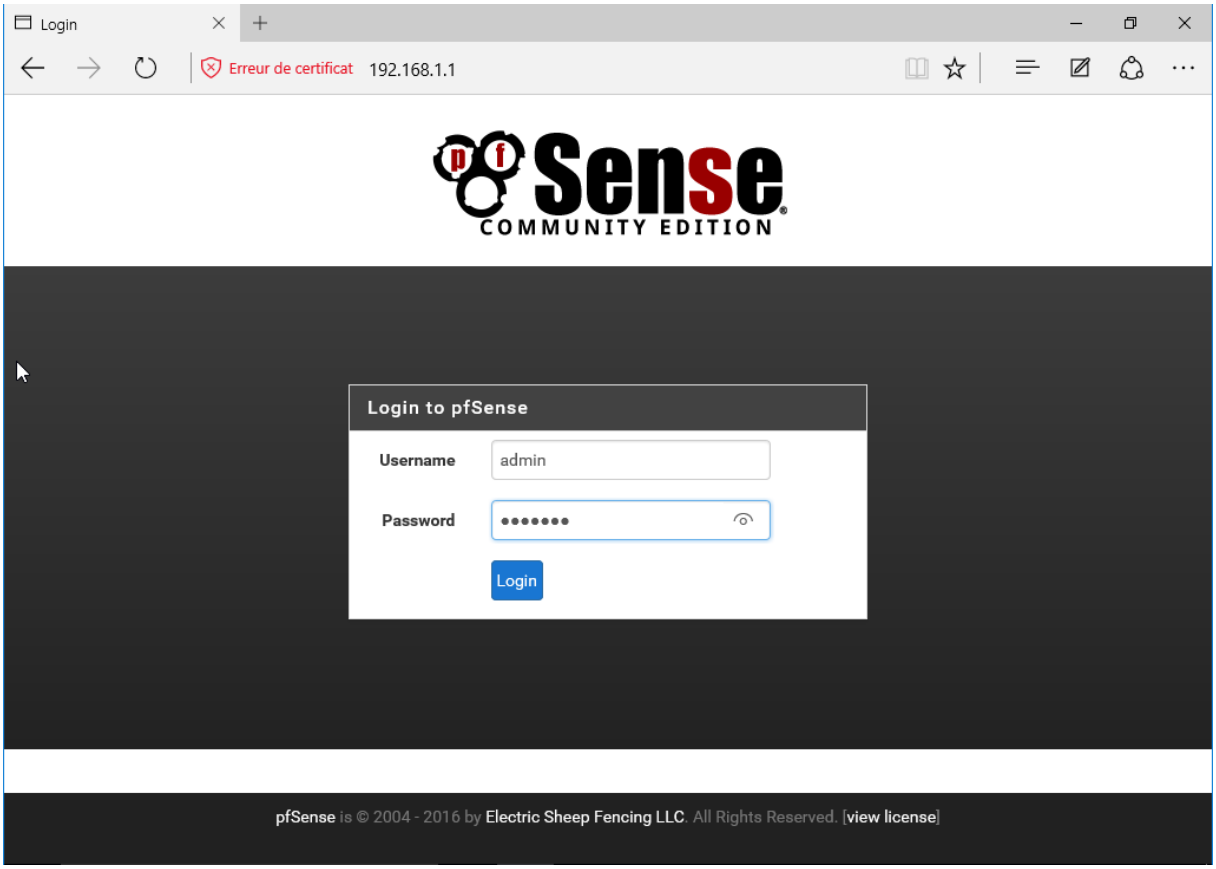


Figure III. 20 : *Page de connexion de l'interface web.*

Une fois connecté avec succès, il est possible d'accéder à l'interface web permettant l'administration de pfsense.Dèsle saisi du nom d'utilisateur et du mot de passe, la page d'accueil de Pfsense s'affiche.

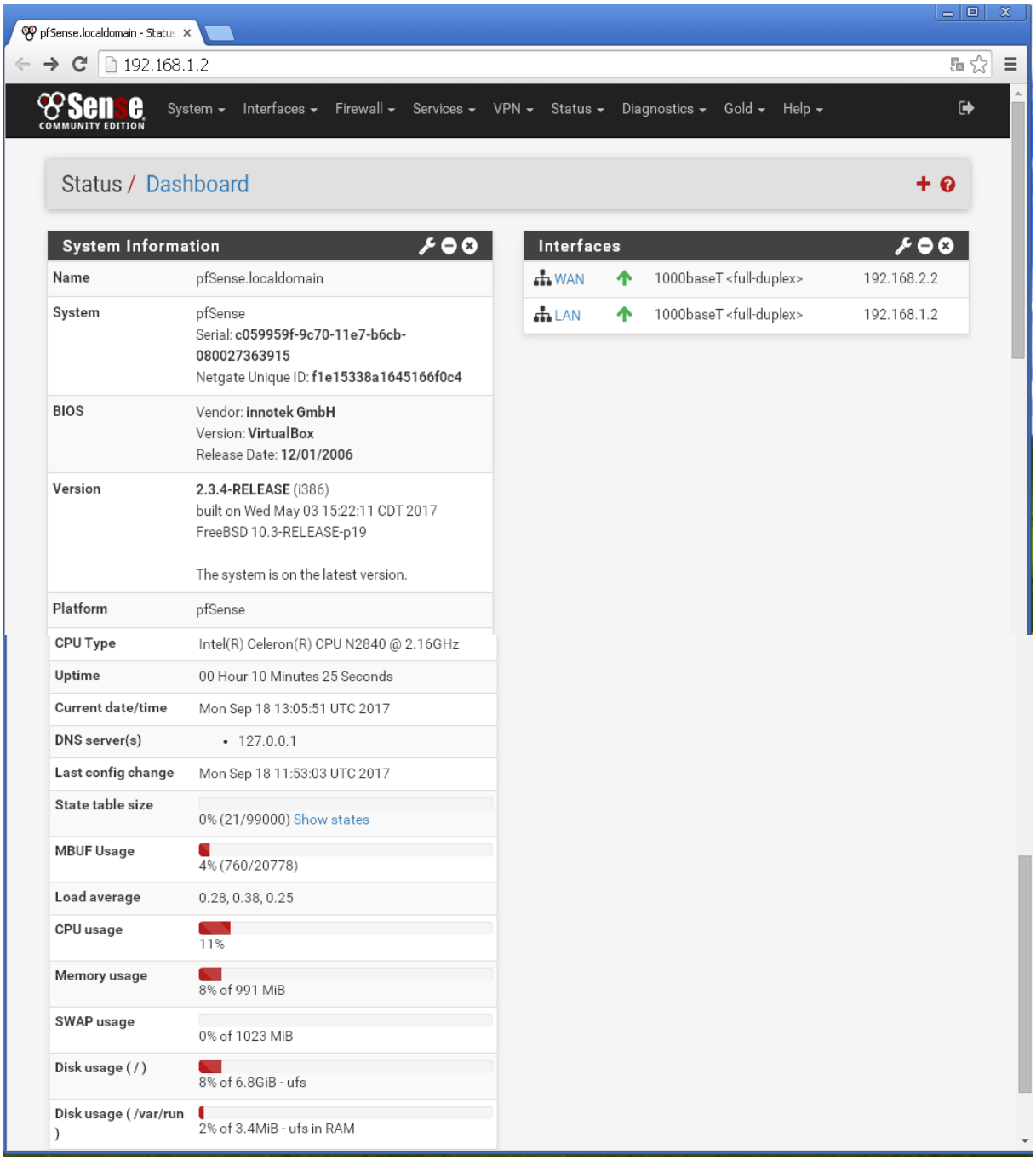


Figure III.21 : *Page d'accueil Pfsense.*

- **Les différents onglets de Pfsense :**

Nous avons des onglets qui fournissent plusieurs services :

- **System :** Permet de faire l'ensemble des réglages concernant le système en lui-même.
- **Interfaces** : Permet la gestion des interfaces réseau (Lan et Wan).
- **Firewall** : Permet de mettre en place toute les règles servant de Firewall.
- **Services** : Permet d'activer de nombreux service faisant de PFSense un firewall multifonction pouvant se transformer en serveur/relai DHCP ou bien encore en portail captif.
- **VPN** : Permet d'activer/désactiver le VPN, de mettre en place une sécurité via IPSec.
- **Status**: Permet de voir le statut de l'ensemble des configurations.
- **Diagnostics** : Permet de donner des outils permettant le diagnostic d'un quelconque bug

- **Activation des protocoles de sécurité de pfsense :**

Pour éviter les intrusions au réseau local LAN, Nous devons effectuer quelque configuration :

- ✓ Activer le HTTPS pour que la connexion entre l'ordinateur et le serveur soit chiffré ;
- ✓ Changer le numéro du port pour accéder à l'interface web ;
- ✓ Cochez la case pour supprimer la redirection automatique vers l'interface web lors de la connexion à l'adresse IP du serveur sur le port 80 ;
- ✓ Activer le SSH pour éviter de passer par la console ;
- ✓ Cochez la case si vous désirez que le mot de passe de l'interface web soit demandé lors de l'accès à la console ;

Pour activé les protocoles HTTPS et SSH nous allons dans l'onglet system de pfsense et nous appuyons sur : system ⟹ Advanced ⟹ Admin Access.

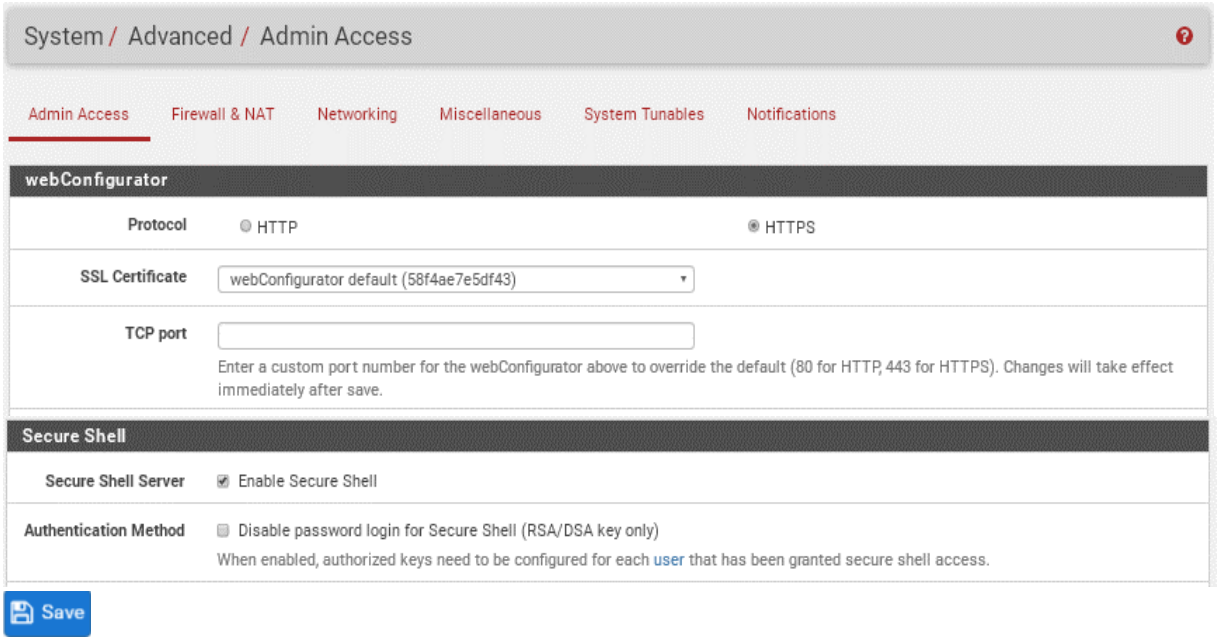


Figure III.22 : *Activation HTTPS et de SSH de pare-feu.*

- **Configuration du serveur DNS :**

Pour activé le serveur DNS nous allons dans : System ⟹ General setup.

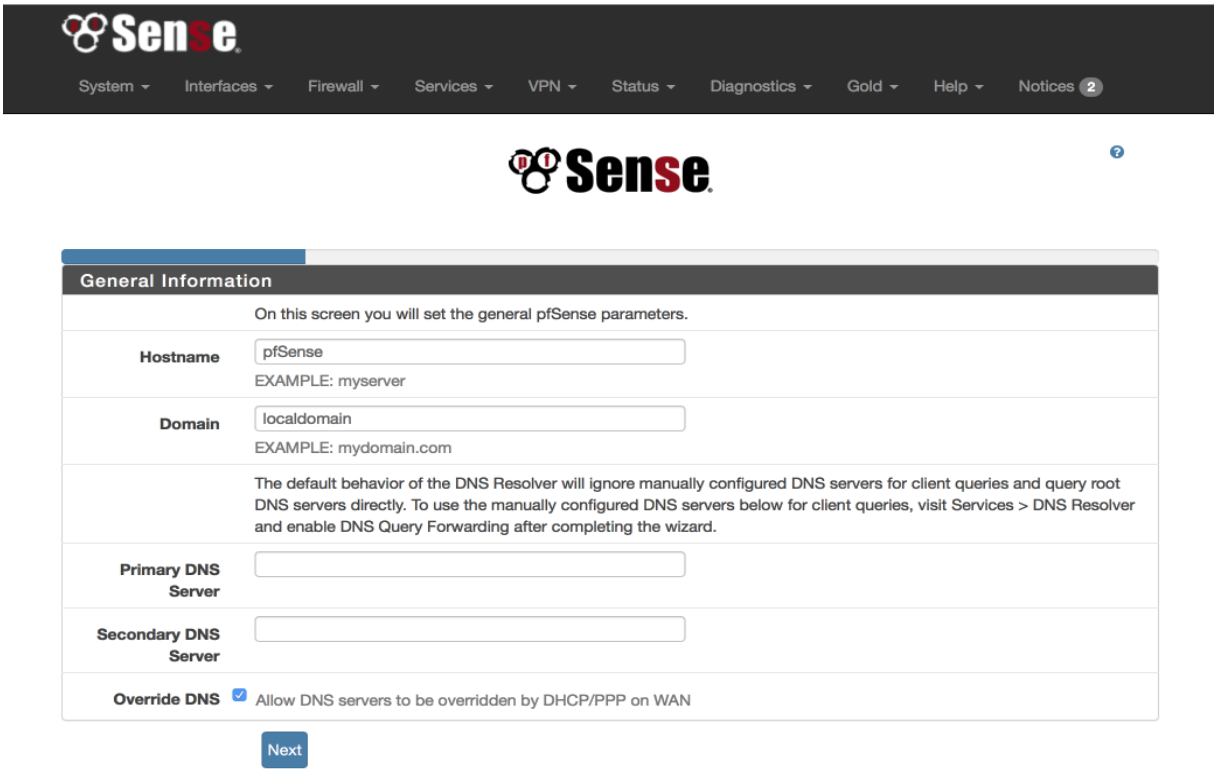


Figure III.23 : *Activationdu Serveur DNS.*

➢ **Configuration des interfaces réseaux :**

La page suivante nous permet de modifier la configuration des cartes réseaux de Pfsense.Nous allons dans l'onglet **Interfaces** et nous choisissons l'interface LAN ou WAN.

♣ **Interface WAN :**

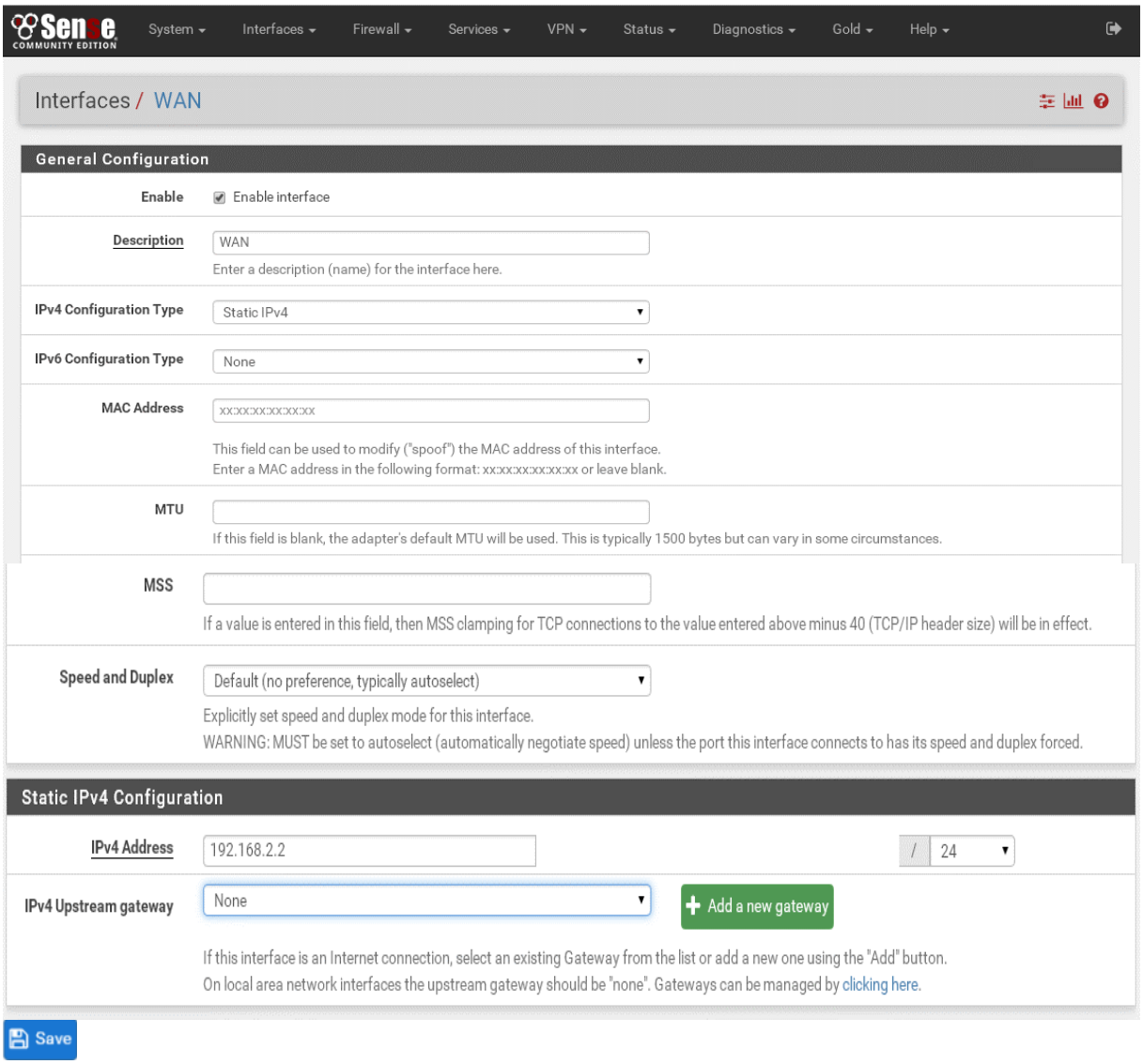
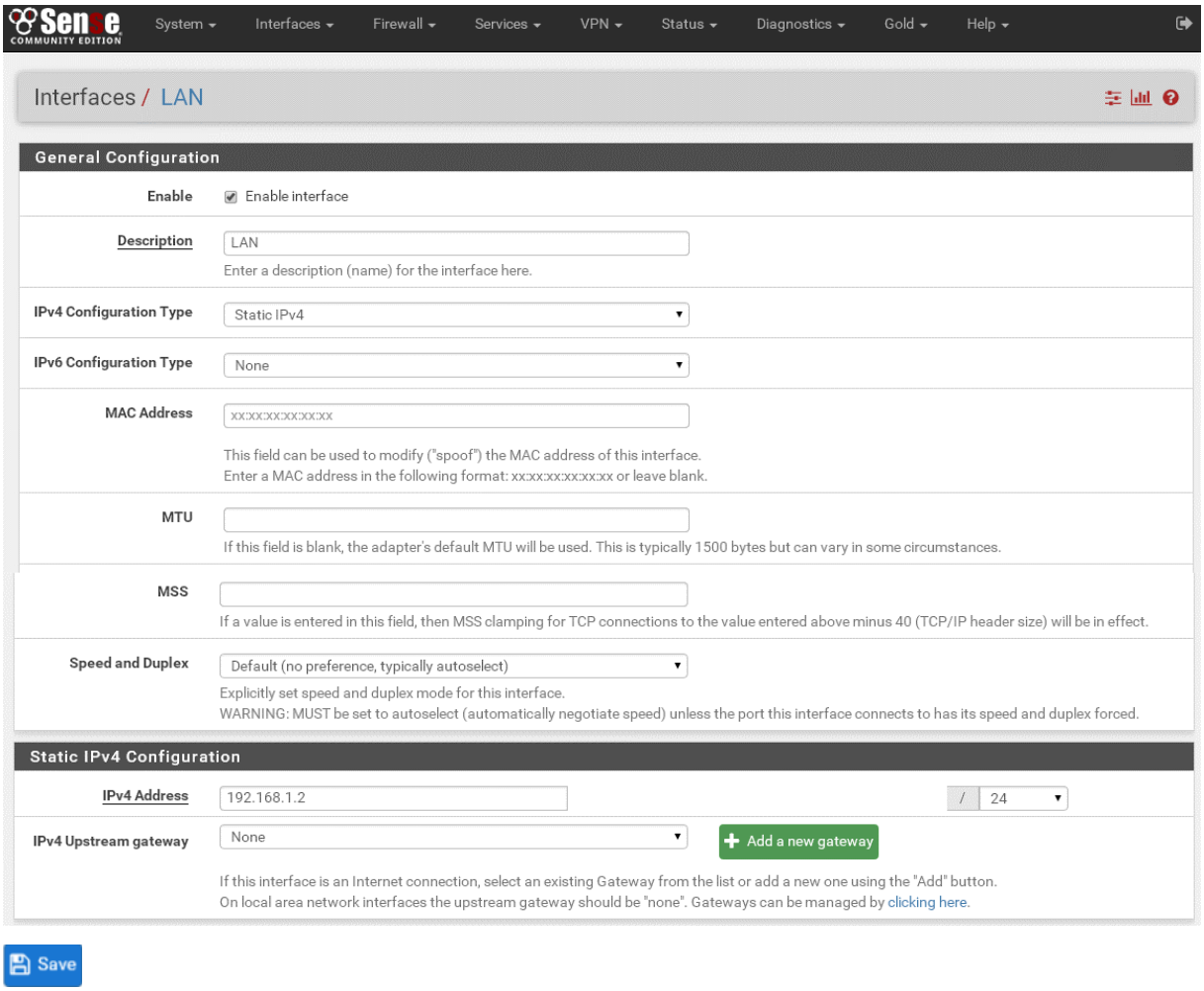


Figure *III.24.* *: Configuration de l'interfaceWAN*

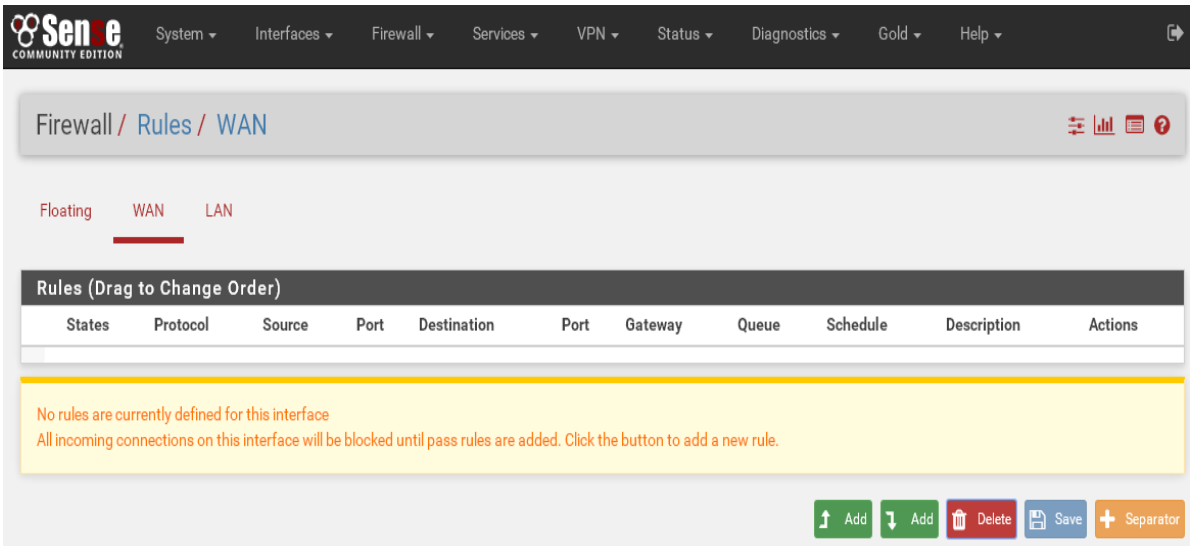
- **Interface LAN :**



- **Les règles d'accès :**

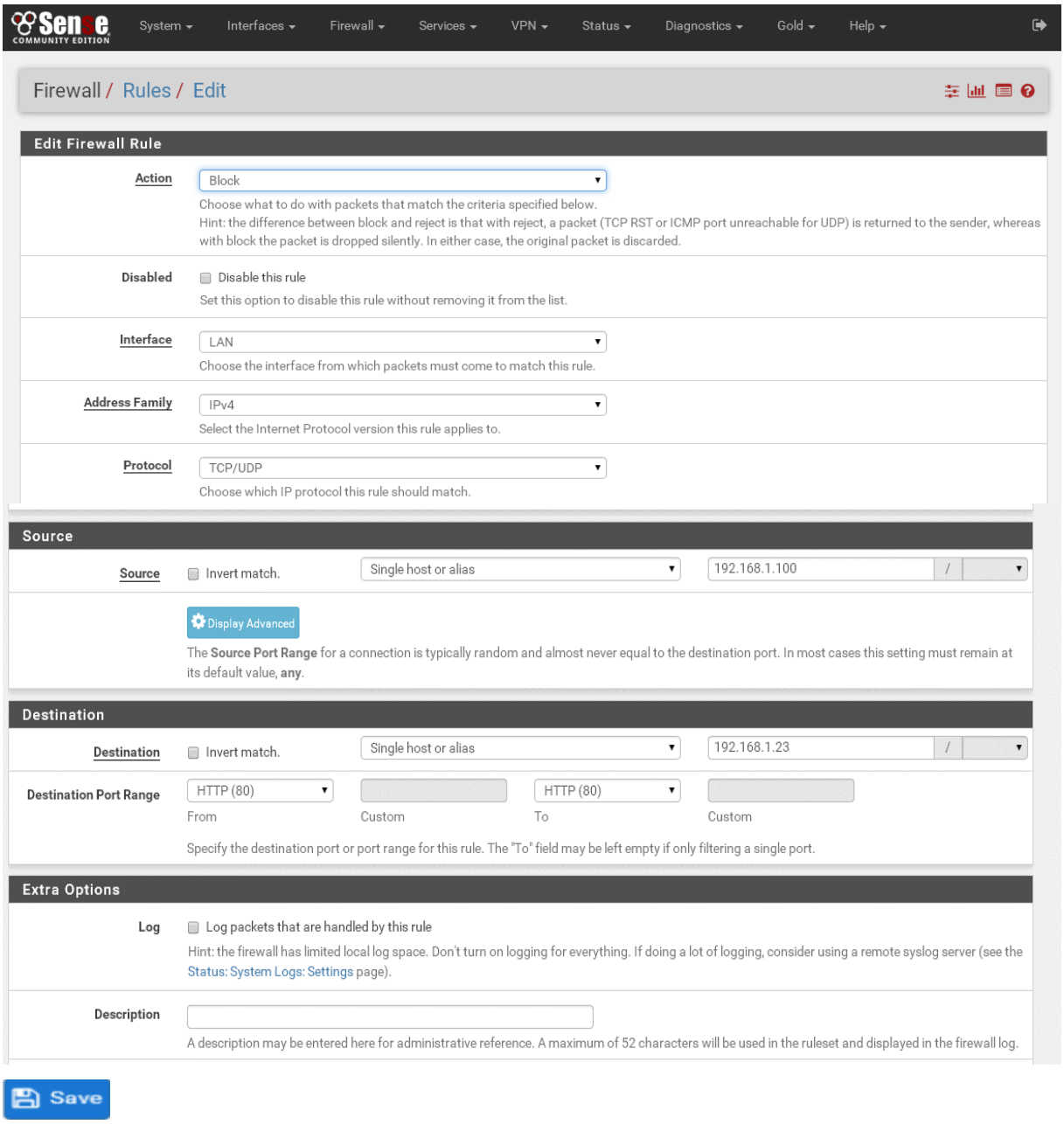
Pfsense permet de réaliser par protocole et par pont sur chaque interface (LAN et WAN), pour cela il faut paramétrer les règles dans l'onglet :

Firewall ⟹ Rules et pour ajouter des règles d'accès, nous cliquons sur LAN ou WAN après sur « **Add »** pour ajouter ces règles**.**



Pour autoriser ou interdire le trafic de certaine adresse dans le LAN nous allons dans :

Firewall ⟹ Rules⟹ Edit.

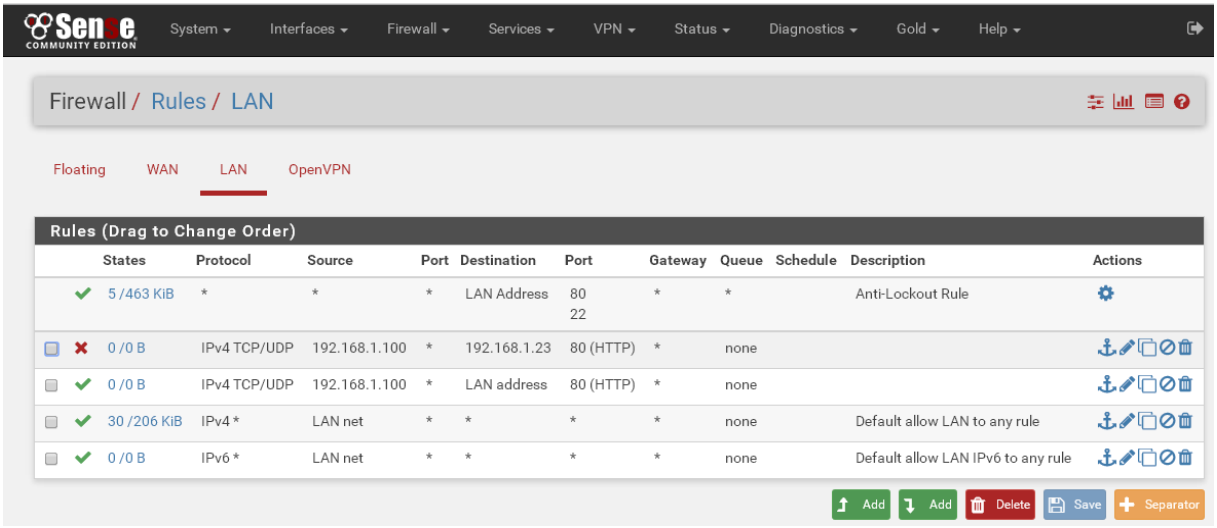


Et pour autoriser ou interdire l'accès l'interface WAN, nous faisons les même étapes que le LAN ,nous changeons l'interface WAN au lieu de LAN.

Dans la figure qui suit nous obtenons les l'adresses que nous avons autorisé et interdit sur le LAN.

L'adresse 192.168.1.100 ont lui interdit le trafic au serveur 192.168.1.23.

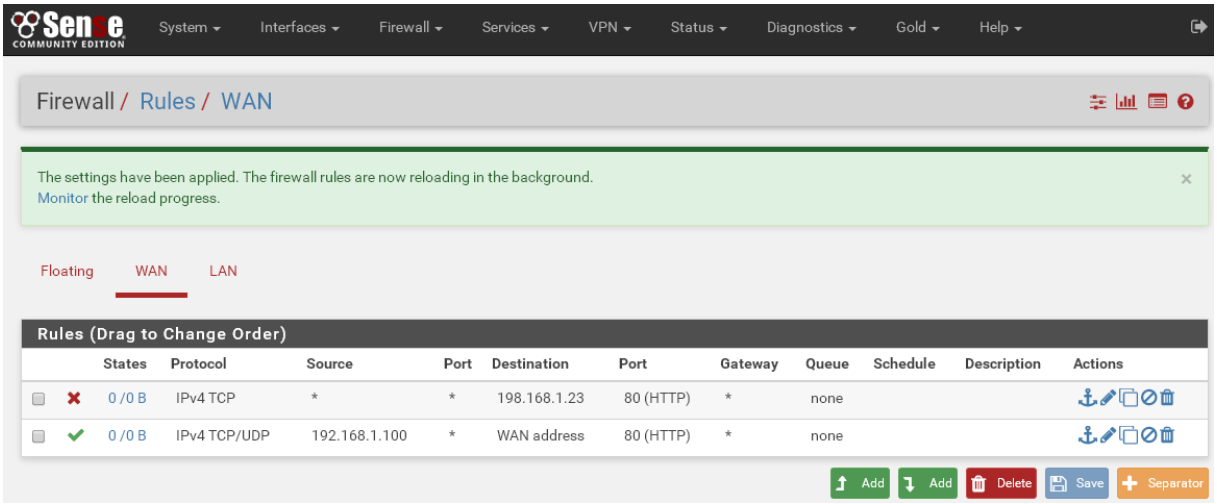
L'adresse 192.168.1.100 à l'accès (nous avons autorisé le trafic) vers le LAN adresse.



Dans la figure qui suit nous obtenons les l'adresses que nous avons autorisé et interdit sur le WAN.

Nous interdire tout le trafic de WAN vers l'adresse 192.168.1.23 (vers le serveur).

Nous allons autoriser le trafic de l'adresse 192.168.1.100 vers le WAN adresse.



- **Activation du serveur proxy :**

Nous allons mettre en place un serveur proxy, avec **Squid**, lui adjoindre des fonctions avancées de filtrage avec **SquidGuard**.

❖ **Squid et SquidGuard :**

Squid est un serveur mandataire, en anglais un proxy, entièrement libre et très performant. Squid est capable de gérer les protocoles FTP, HTTP, HTTPS. Il est généralement utilisé pour des fonctions de filtrage d'URL ou en tant que tampon. Les pages Internet sont stockées localement ce qui évite d'aller les recharger plusieurs fois et permet d'économiser la bande passante.

SquidGuard est un filtre, un redirecteur et un plugin de contrôle d'accès pour Squid. Il va notamment permettre d'appliquer sur un proxy une liste noire de sites ou mots-clés interdits.

Pour installer les deux packages suivants, aller dans : SystemP⇨xage Manag⇨Available ⇨ Packages.

➢ **Installation des packages Squid et SquidGuard :**

Nous allons sur l'onglet **System**de Pfsense puis **Package Manager**puis**Available Packages**et parmi les packages qu'ils s'affichent, nous choisissons Squid et nous cliquons sur **« +install »** pour l'installer et nous faisons la même chose pour SquidGuard.

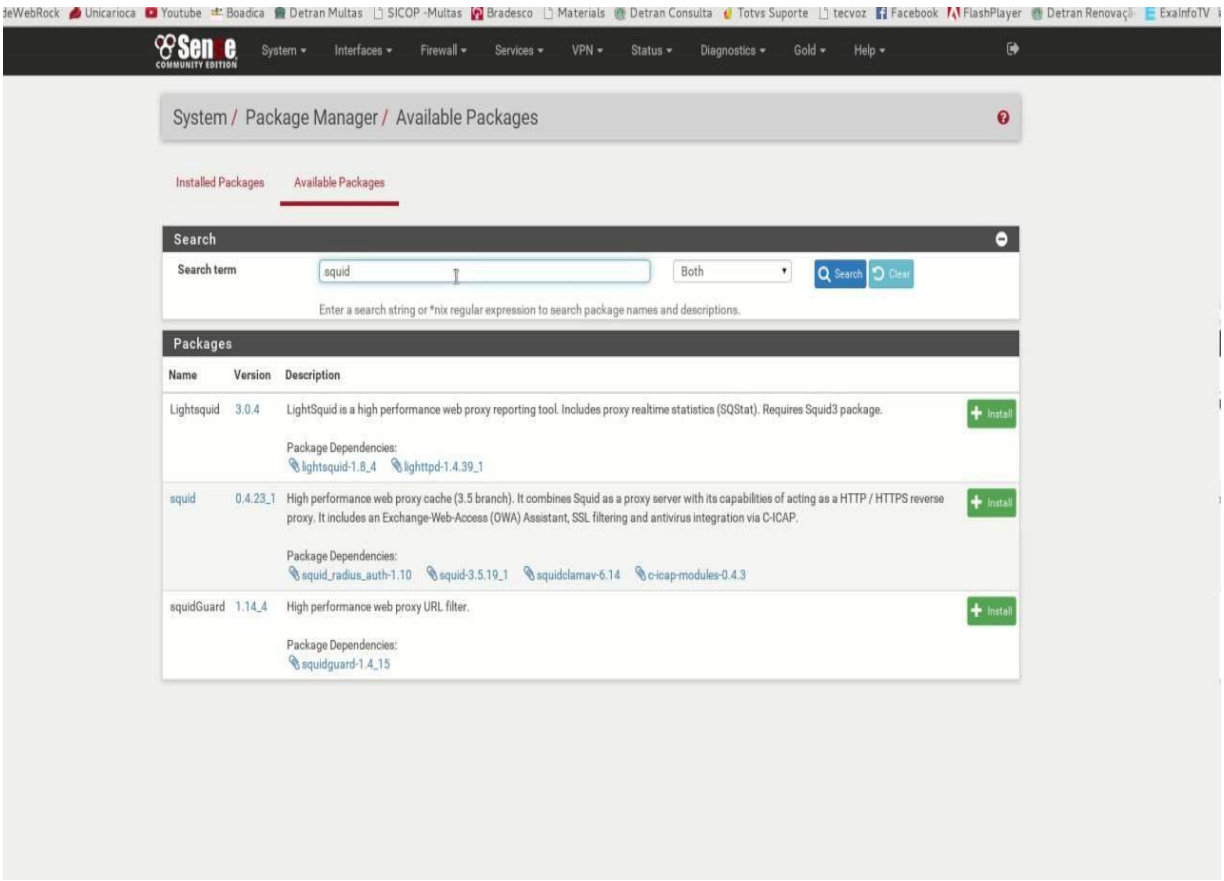


Figure III.25:*Installation de Squid et SquidGuard.*

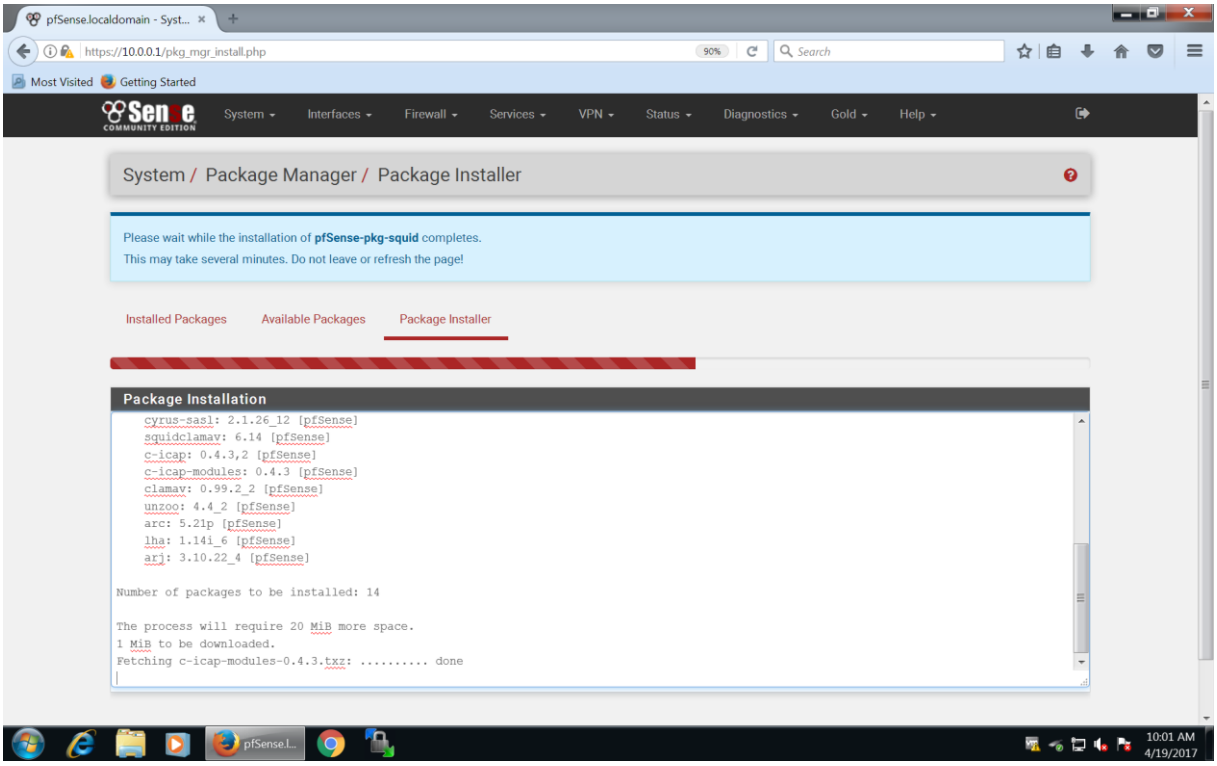


Figure III.26 : *Début d'installation des paquets.*

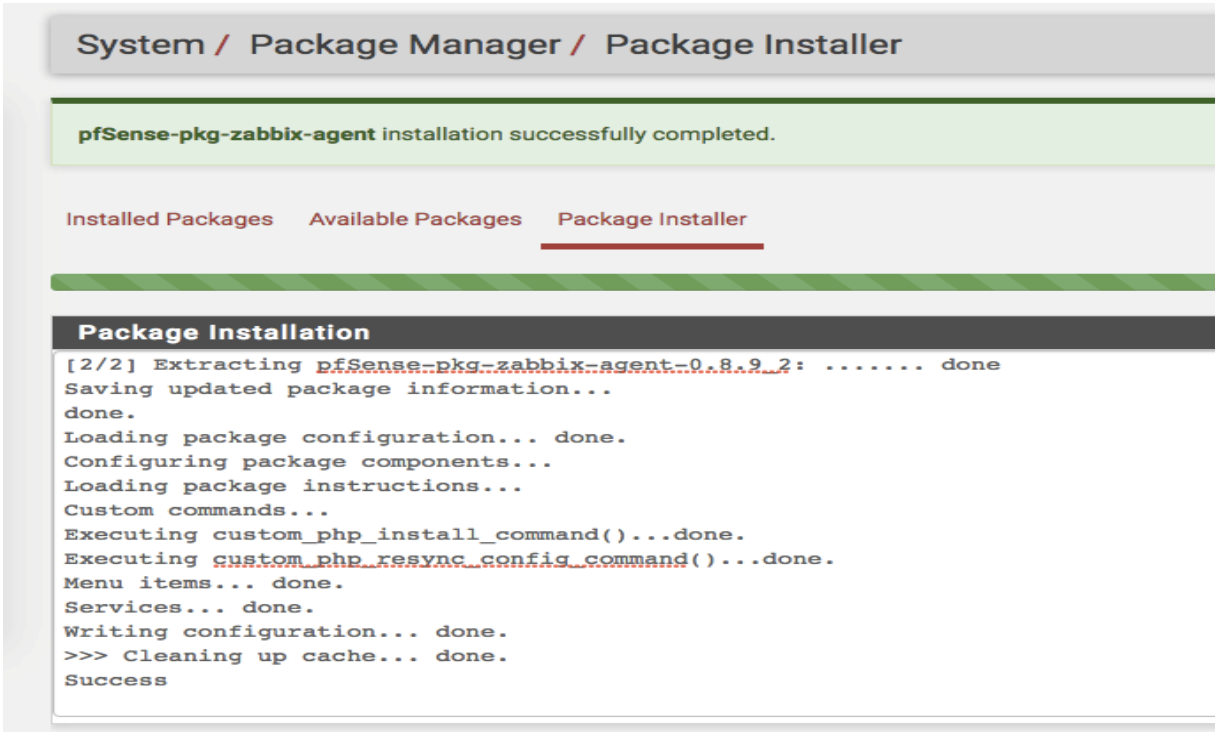


Figure III.27: *Installation des paquets sont terminés.*

L'installation des proxys est terminée avec succès.

Si nous voulonsvérifier que les deux serveurs sont bien installés, on fait :

System→ package manager→ Available packages et nous obtenons cette figure :

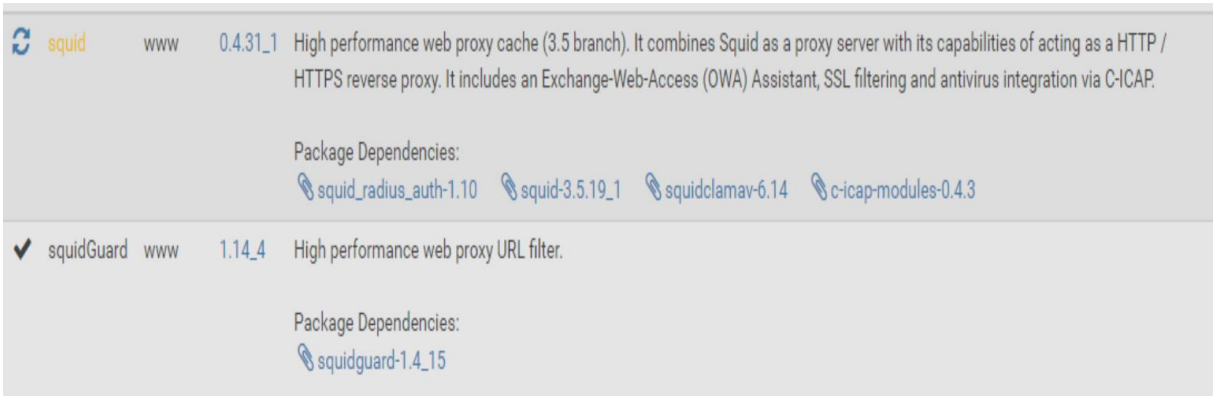


Figure III.28 : *Vérification d'installation des paquets.*

- **Configuration Squid (proxy server) :**

Pour commencer, nous allons dans le menu principal de pfsense puis nous cliquons sur **Services** puis dans **Proxy Server**. Dans la partie "General", nous remplissons les champs comme dans la capture d'écran suivant :

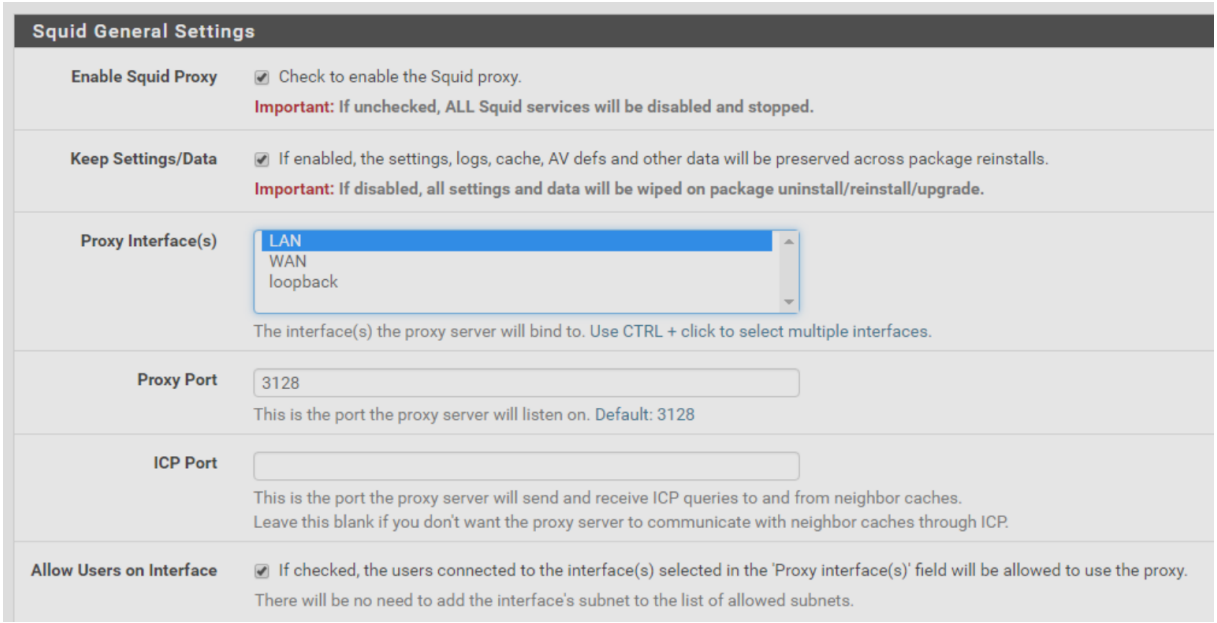


Figure III.29 : *Activation du serveur Proxy.*

Le mode transparent http proxy redirige automatiquement tout le trafic web entrant vers le serveur proxy Squid. Dans la plupart des cas, l'utilisateur ne remarque même pas que son trafic traverse un serveur mandataire.

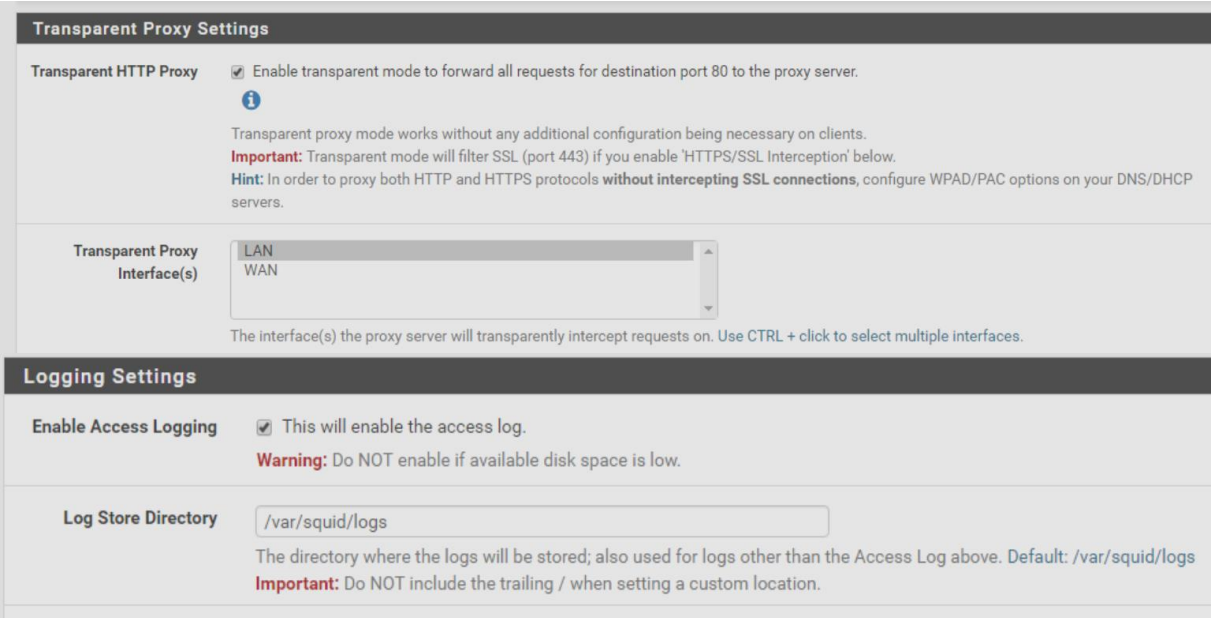


Figure III.30 : Activation du proxy transparent.

- **Configuration SquidGuard (proxy filter http) :**

SquidGuard permet de filtrer et de contrôler les accès. Nous allons utiliser une blacklist complète avec beaucoup de catégories. Cette blacklist Nous pouvons la trouver sur le lien suivant : **http://www.shallalist.de/Downloads/shallalist.tar.gz.**

Nous allons dans le menu **«Services** puis dans **SquidGuard Proxy filter.** Dans la partie **General setting**, nous remplissons les champs comme dans la capture d'écran suivant :

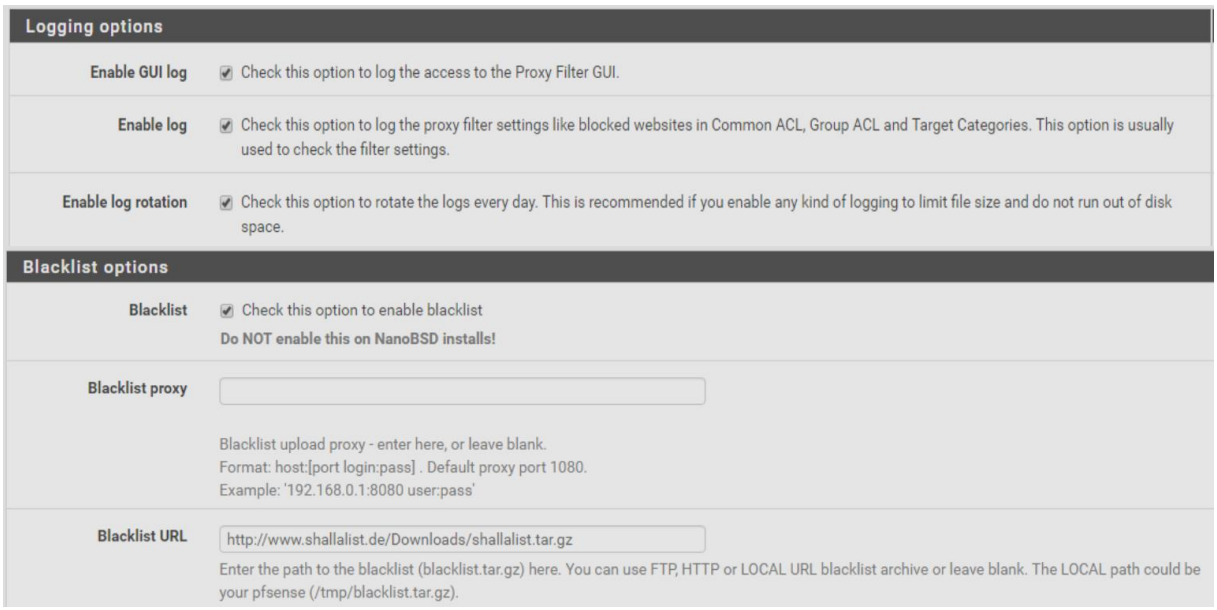


Figure III.31 *: Configuration du SquidGuard.*

Dans l'onglet blacklist, nous collons le lien de la blacklist et nous faisonsdownload pour télécharger la blacklist

Figure III.32 : *Installation de blacklist.*

Après le téléchargement de la blacklist, nous nous rendons dans l'onglet**General Settings**de blacklist, nous cochons la case blacklist et nous enregistrons.

Figure III.33 : *Activation de blacklist.*

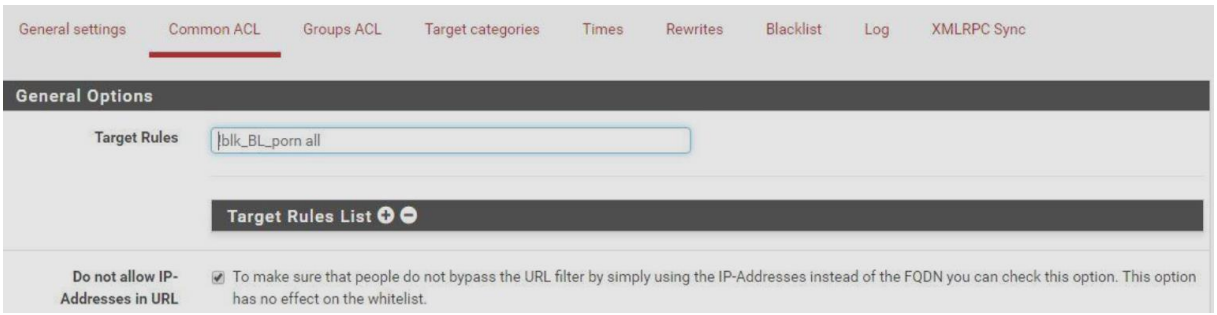
Par défaut le proxy bloque toutes les catégories d'url (adresse de navigateur web), nous allons donc lui spécifier quelles catégories que nous voulons bloquer.

Nous allons donc commencer par autoriser toutes les catégories puis nous interdirons les catégories que nous ne voulons pas.

Pour cela aller dans l'onglet **Common ACL** et cliquez sur **Target Ruleslist.**

Tout en bas de la liste, la catégorie « Default Access [all] » a été « deny », nous allons faire passer au « allow » pour autoriser tous les sites.

Après nous choisissons les catégories de sites à bloquer. Dans**Target Rules List**, nous cliquons sur **« + ».**



Nous obtenons cette figure :

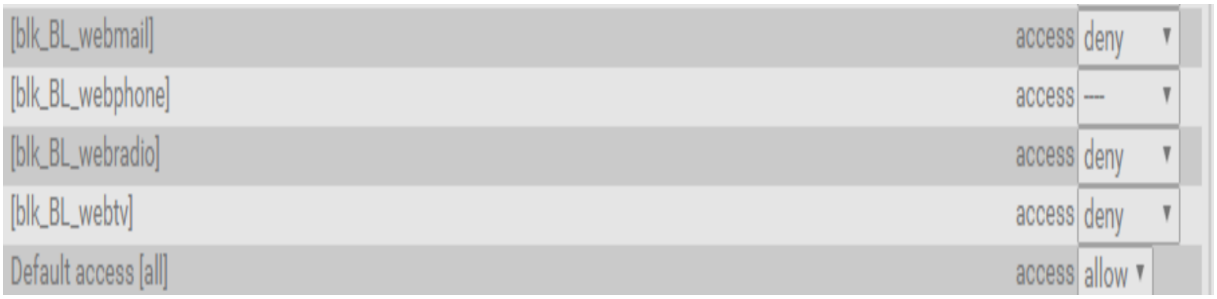


Figure III.34 : *Catégorie de blocage.*

Dans notre exemple, nous avons interdit l'accès à la catégorie Webmail, WebTV, et web radio, puis autorisé toutes les autres catégories.

Ensuite remplir les champs comme dans la capture d'écran ci-contre : (à adapter)

Il y a un menu déroulant pour chaque catégorie :

• **Allow**- Accès au site, sauf si elle estbloquée dans une autre catégorie par'deny'.

• **Deny**- Bloquer l'accès au site.

• **Liste blanche** - Toujours autoriser l'accès au site.

Il est possible de bloquer les téléchargements de fichiers, mais aussi de bloquer l'accès à certains sites par mots clés, ces règles sous PFSense se nomment Target Catégories. Dans l'onglet « Target catégories » cliquer sur ADD. Dans notre exemple ci-dessous nous citons une liste noire pour interdire l'accès à netacad.com.

***Figure III.35** : Interdiction du site netacad.com.*

En fin, nous retournons dans l'onglet General Settings puis nous cochons la case Enable et nous faisons un **apply**pour appliquer la configuration.

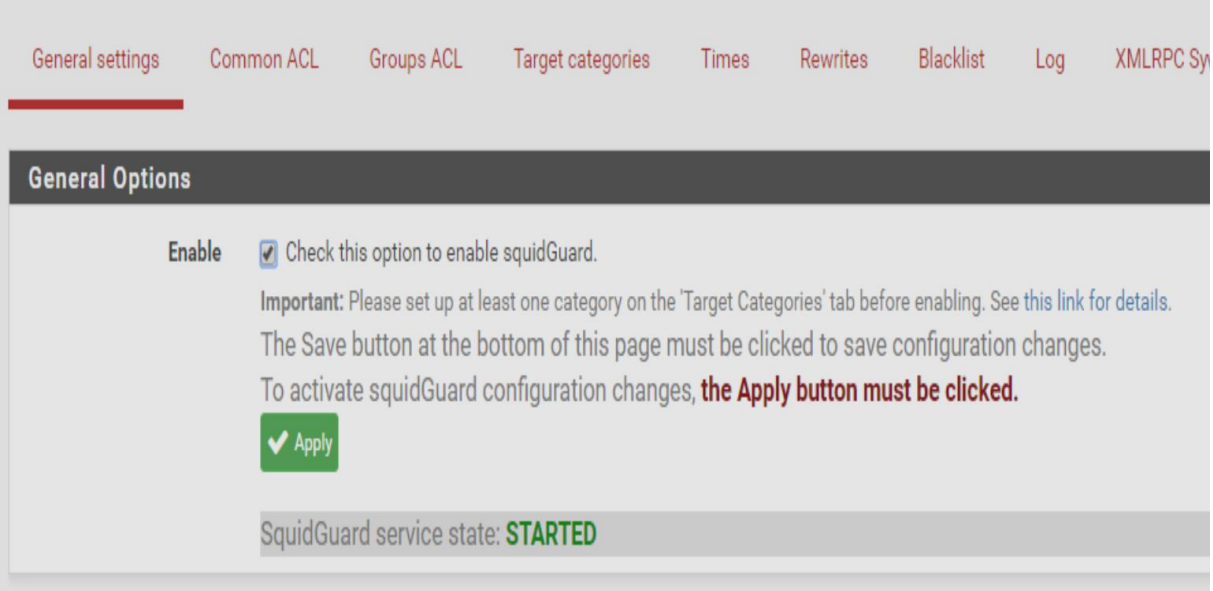


Figure III.36 :*Application des modifications.*

- **Test de l'une des catégories de site bloqué :**

Dans notre liste noire nous avions configuré le site netacad.com, une station du réseau LAN ne peut donc pas accéder à ce site-là !

De même il n'est pas possible d'accéder à des sites web qui sont dans une catégorie « deny »

Dans l'onglet **logs** de SquidGuard nous pouvons voir que l'accès au site netacad.com a été refusé par la liste noire.

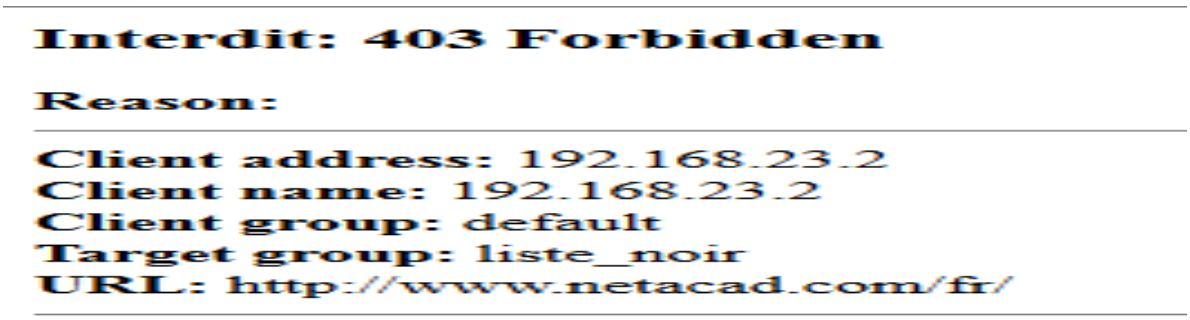
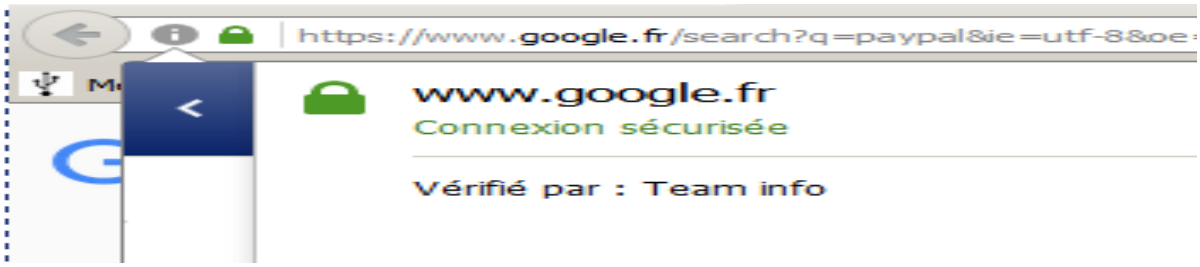


Figure III.37 : Test d'Interdiction du site netacad.

Pour vérifier que le cryptage SSL s'effectue par l'intermédiaire du certificat créé par Pfsense, aller dans le navigateur client et regarder la vérification de la connexion sécurisée :



FigureIII.38: Vérification de la connexion sécurisée.

Les sites web https peuvent être bloqués via la blacklist.

- **Configuration d'OPENVPN sur Pfsense :**

L'OpenVPN est un logiciel libre permettant de créer un réseau privé virtuel VPN. Ce logiciel disponible dans Pfsense, permet à des paires de s'authentifier entre eux à l'aide d'une clé privée partagée à l'avance ou de certificats.

a. Installation du package OpenVPN Client Export Utility :

Il faut commencer par télécharger un package qui va nous permettre de simplifier par la suite l'installation du client OpenVPN ainsi que l'export de la configuration vers les postes mobiles.

Depuis l'interface de gestion du firewall :

System → packages → Available Packages.

Nous Sélectionnons OpenVPN Client Export Utility et nous cliquons sur **« install »** pour l'installer.

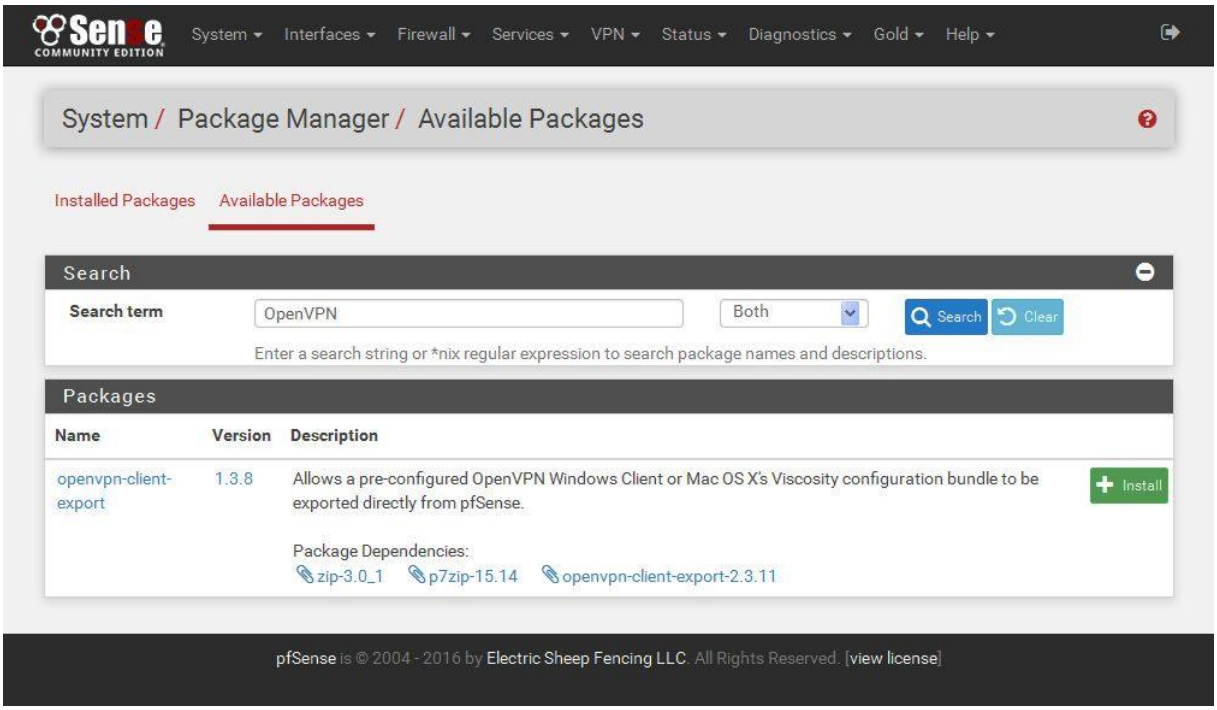


Figure III.39 : *Installation d'OpenVPN-client export.*

L'installation se lance et se termine comme suit :

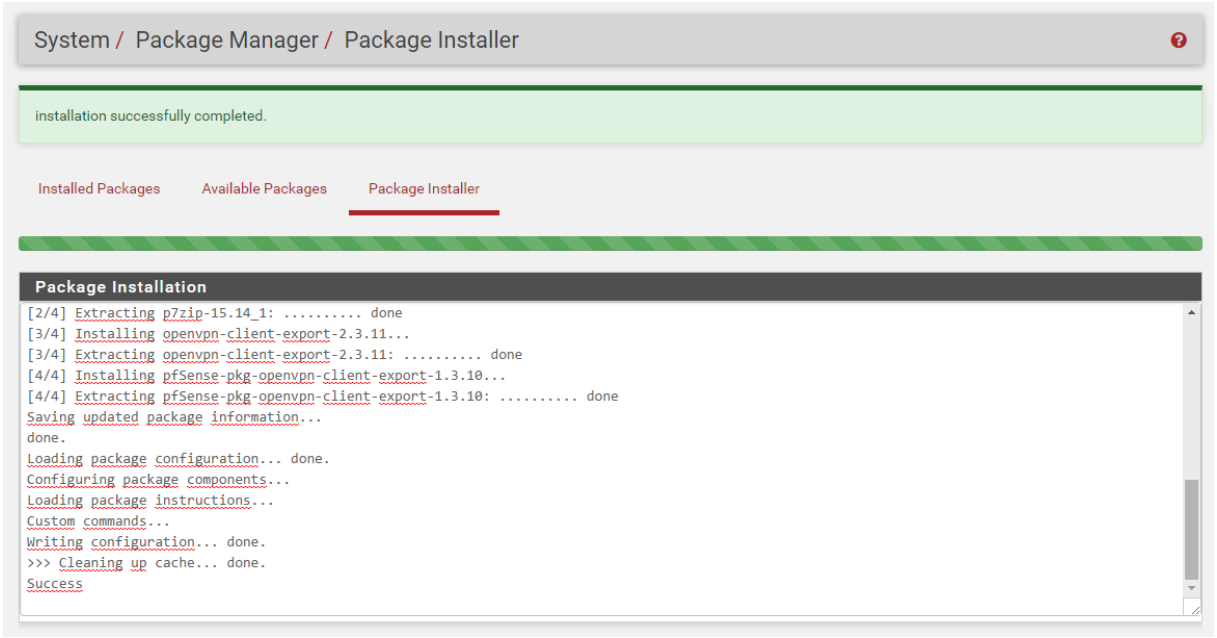


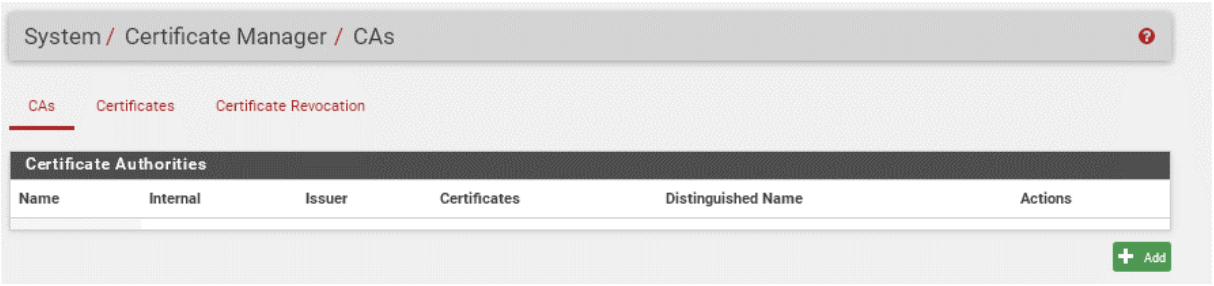
Figure III.40 : *fin d'installation de OpenVPN client/ export avec succès.*

b. Création de l'autorité de certification :

❖ Certificat pour le serveur :

Depuis l'interface de gestion du firewall nous faisons:

System→Cert Manager



Dans l'onglet **« CAs »** cliquer sur **«+add»** pour créer une nouvelle autorité de certification serveur VPN.

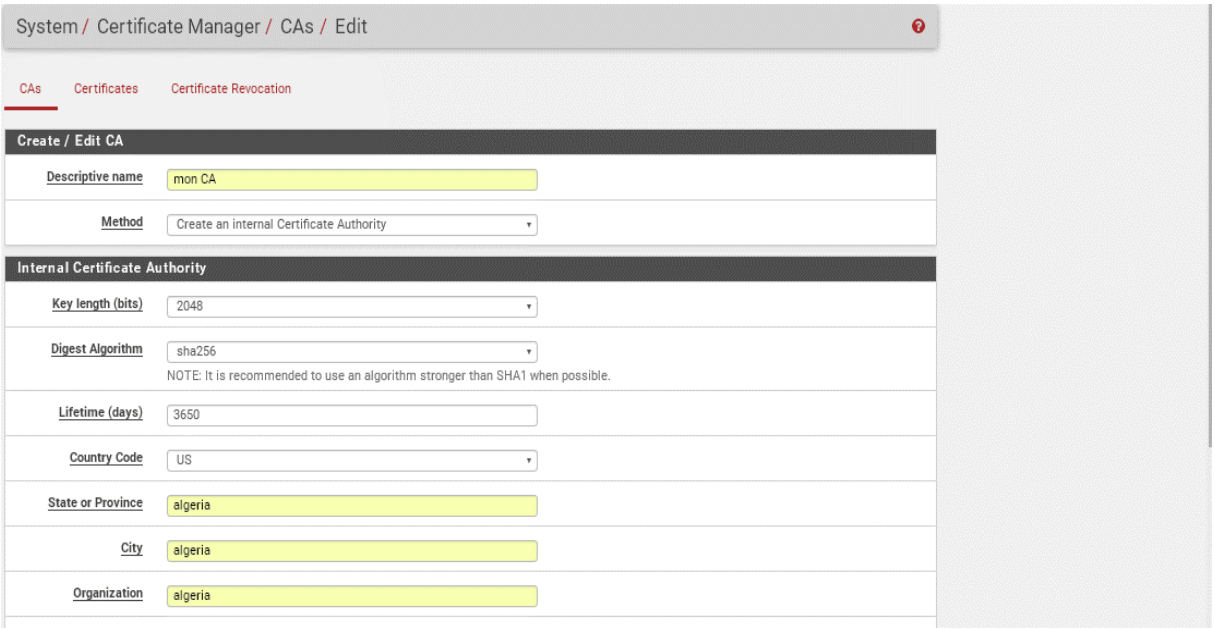


Figure III.41 : Création d'un certificat pour le serveur.

Après avoir enregistré notre certificat, nous revenons sur « CAs » pour l'activer.

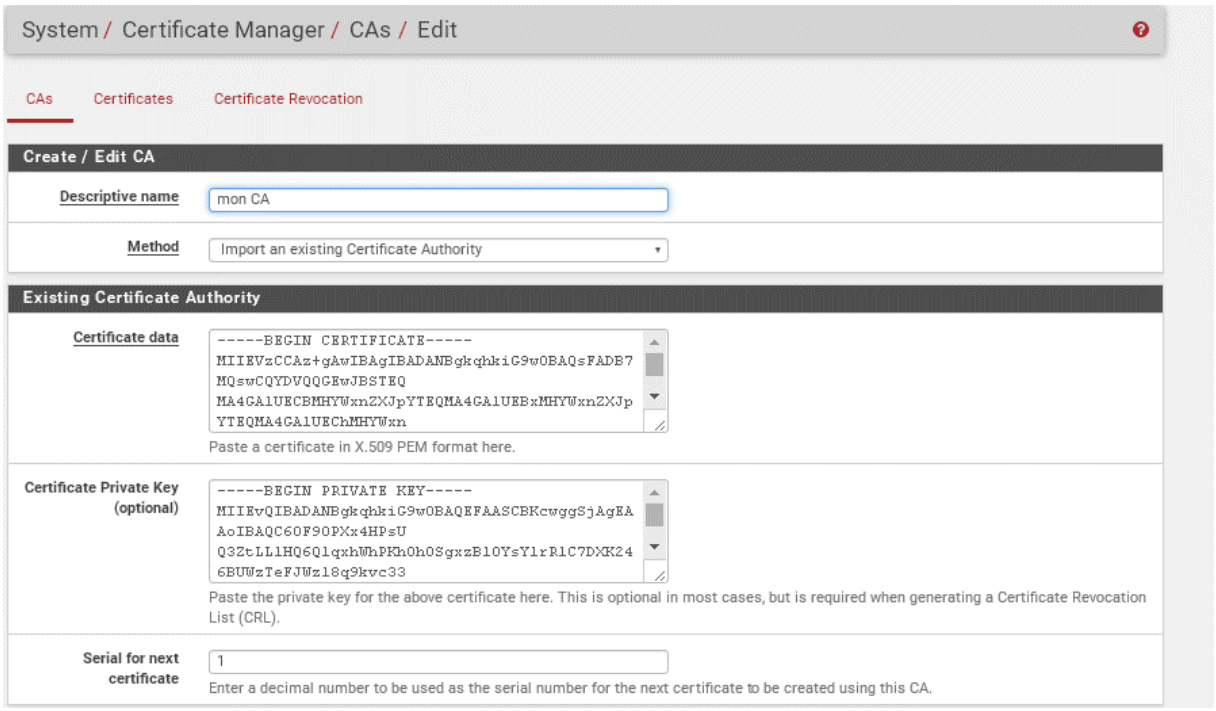


Figure III.42 : Activation du certificat pour le serveur.

❖ **Création d'utilisateur OpenVPN et certificat privé pour l'utilisateur :**

Depuis l'interface de gestion du firewall faites:

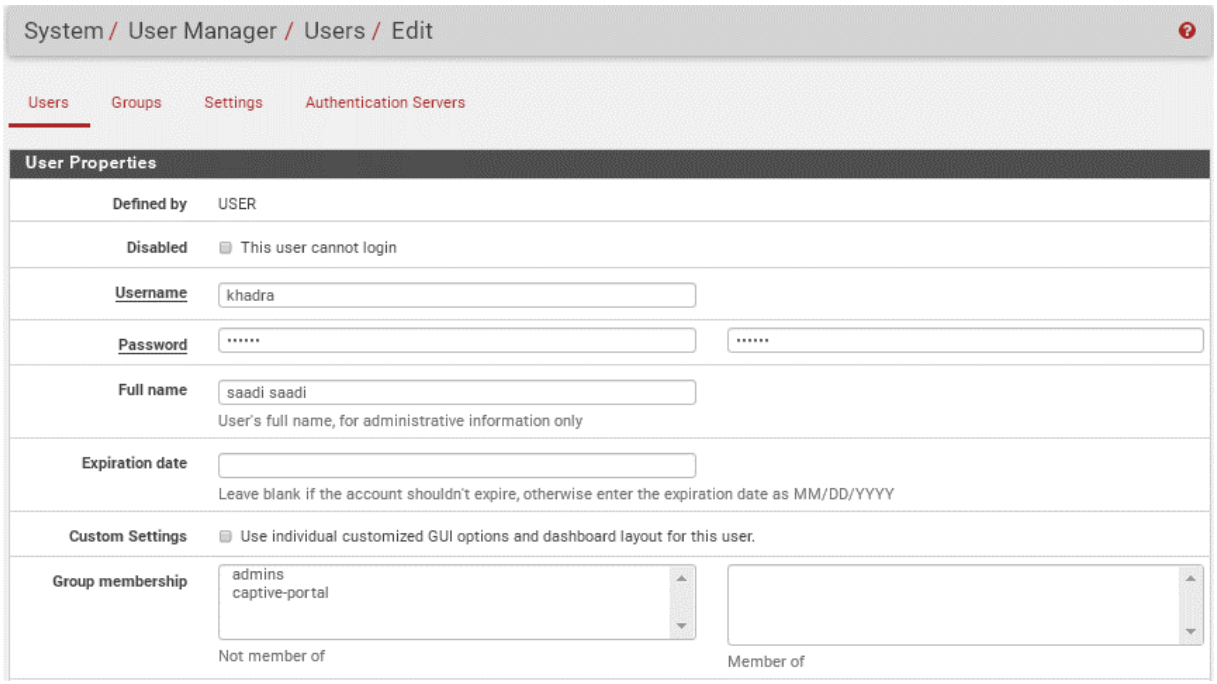
System → User Manager

Dans l'onglet Userscliqué sur « + » pour créer un nouvel utilisateur.

Username : khadra

Password : khadra

Full name : saadisaadi



Nous cochons la case**« *click to Createa user Certificate*»**pour créer notre certificat.

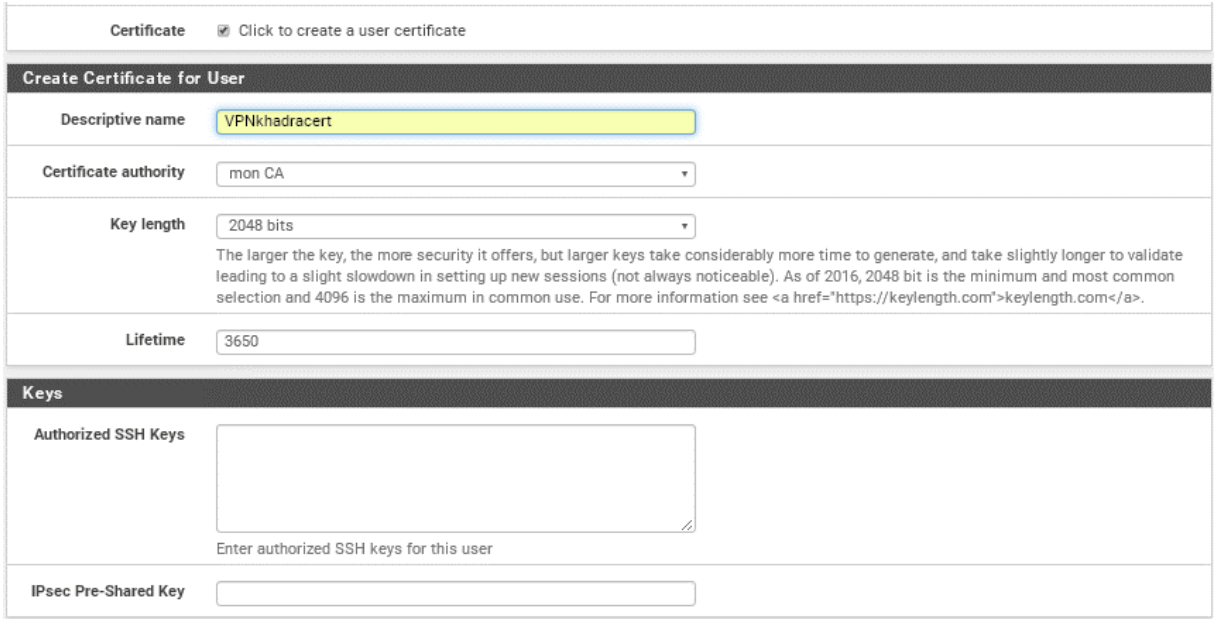


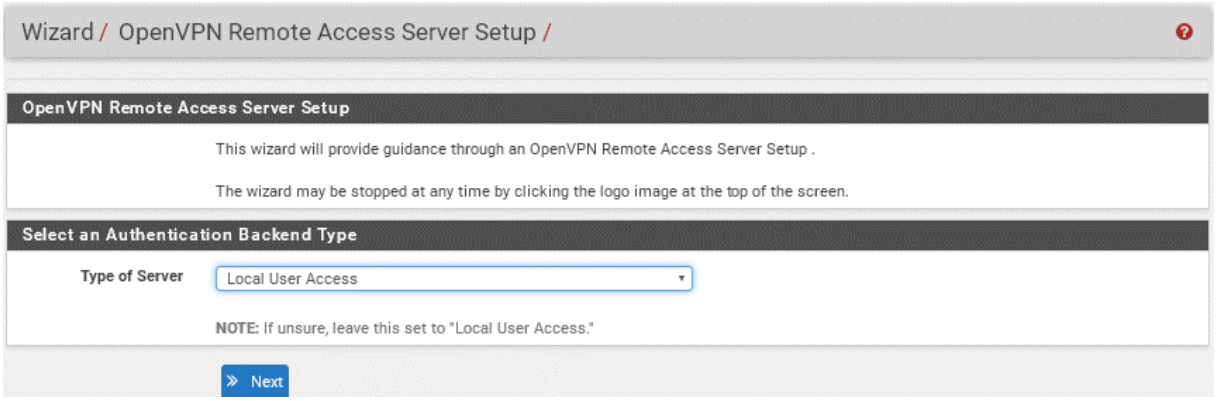
Figure III.43 : *Création d'un certificat pour l'utilisateur*

c. Configuration interface WAN OpenVPN :

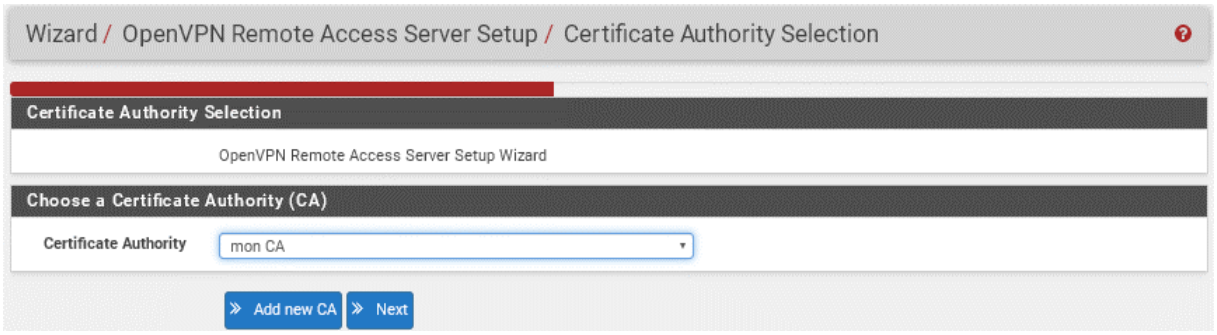
Depuis l'interface de gestion du firewall faites:

VPN→OpenVPN

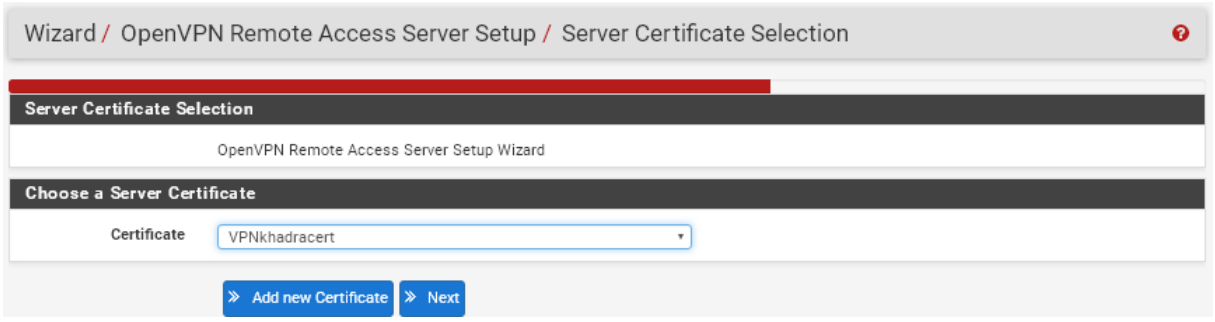
Dans l'onglet **Wizard**,nous définissons le type d'authentification.



A l'étape suivante, on choisit le certificat CA que nous avons crié déjà et qui va valider le certificat donné au PC mobile.



On sélectionne le certificat du serveur.



Nous appuyons sur Next.

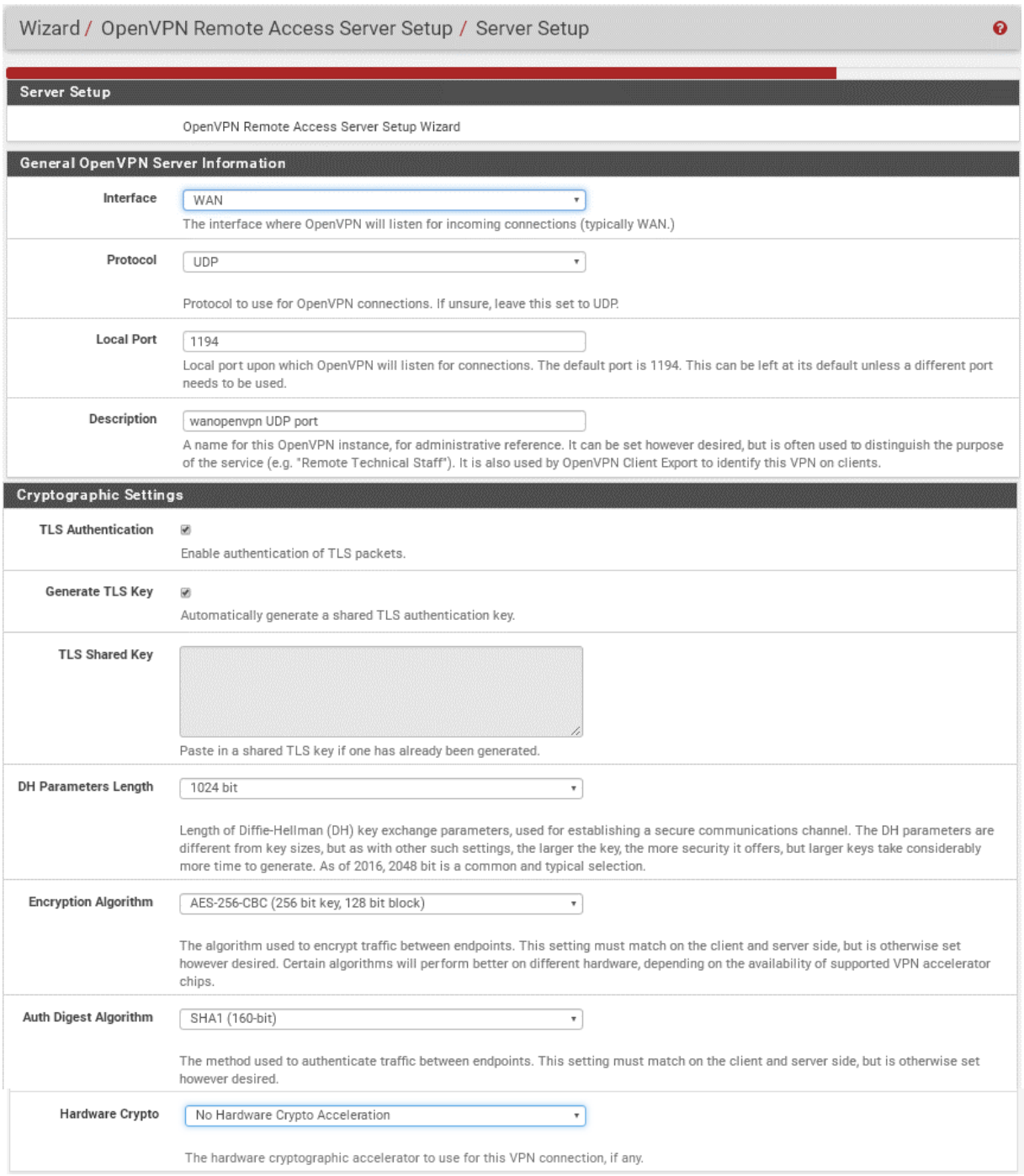


Figure III.44 :*Configuration de VPN coté serveur.*

Tunnel Network : **192.168.1.3/24** (le réseau virtuel au quel le pc distant sera connecté)

Local Network : **192.168.1.2/24**

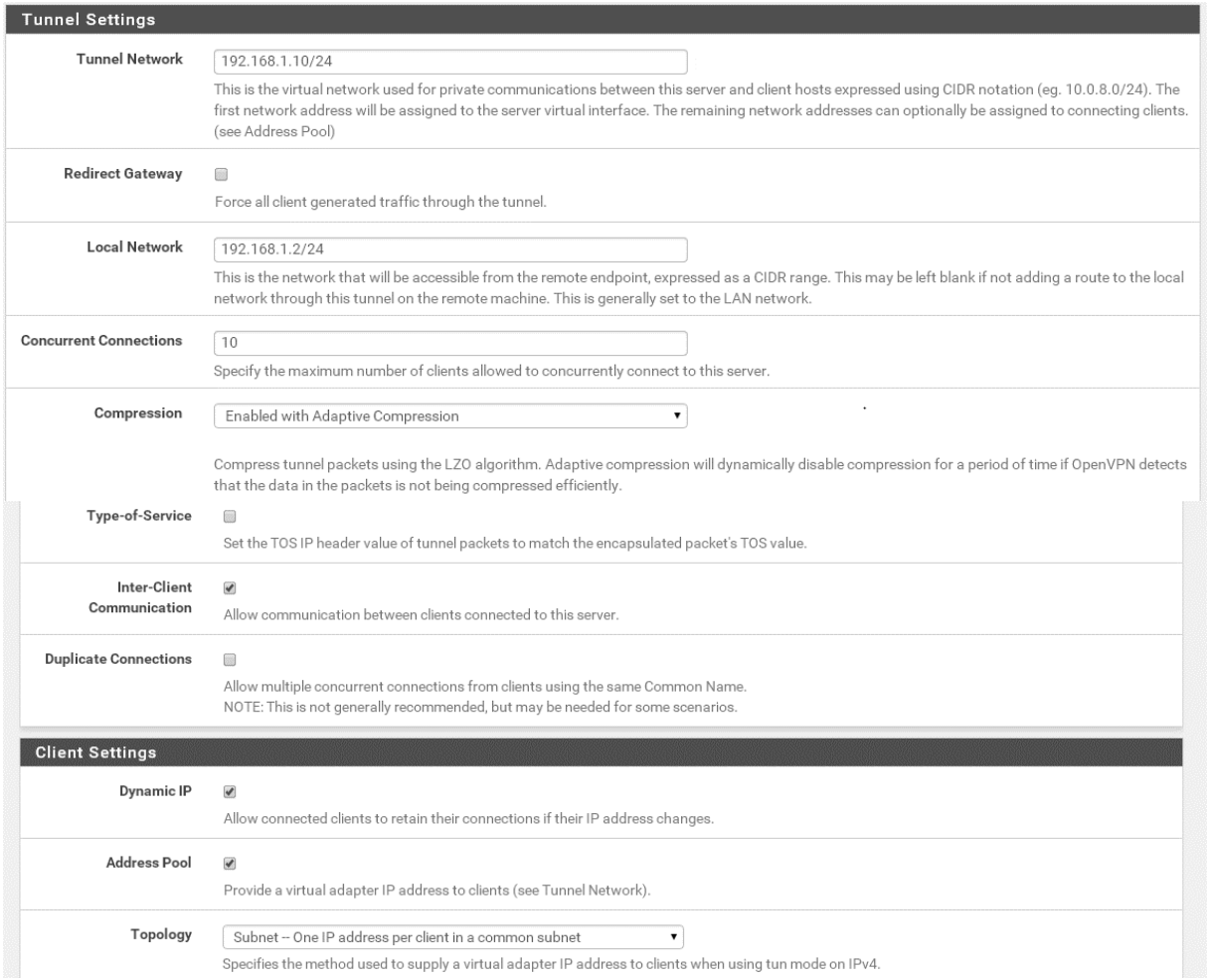
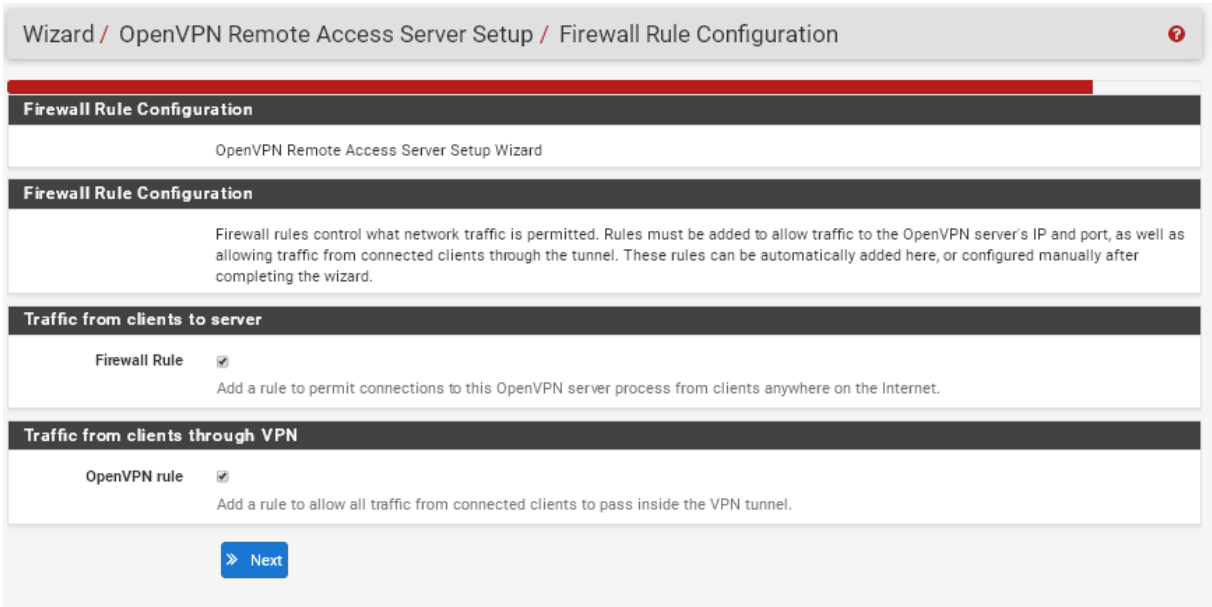
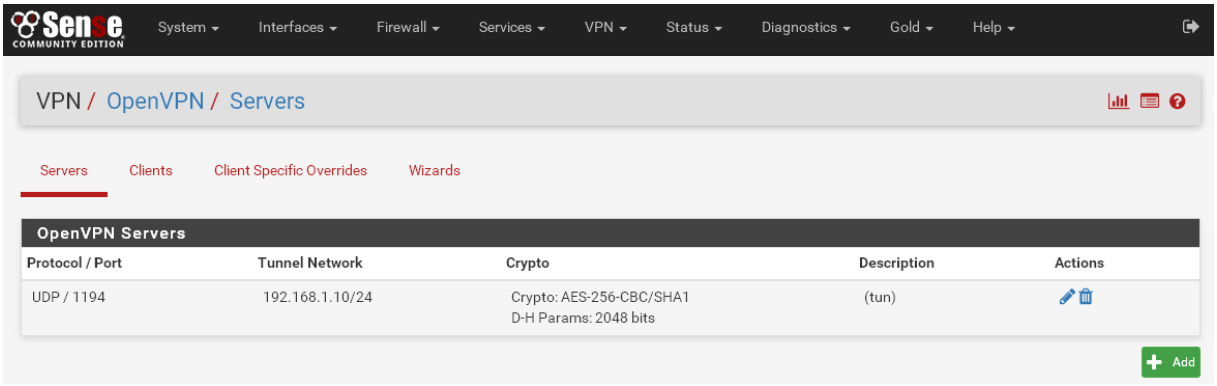


Figure III.45 : *Configuration de serveur 2.*

Le reste on laisse, par défaut, vide et on valide



Donc notre VPN est a été crié maintenant comme nous le voyons dans la figure suivante :



d. Export du client OpenVPN et la configuration :

Depuis l'interface de gestion du firewall faites:

VPN→OpenVPN

Dans l'onglet client Export, nous téléchargeons le client qui correspond à notre Système.

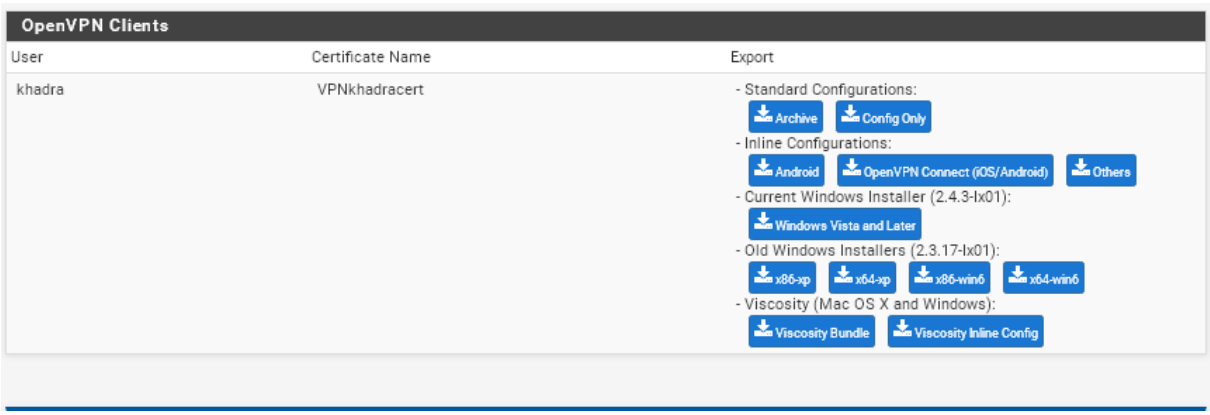


Figure III.46 : *Choix du client export.*

Dans notre cas, nous choisissons x86-xp et nous faisons le téléchargement.

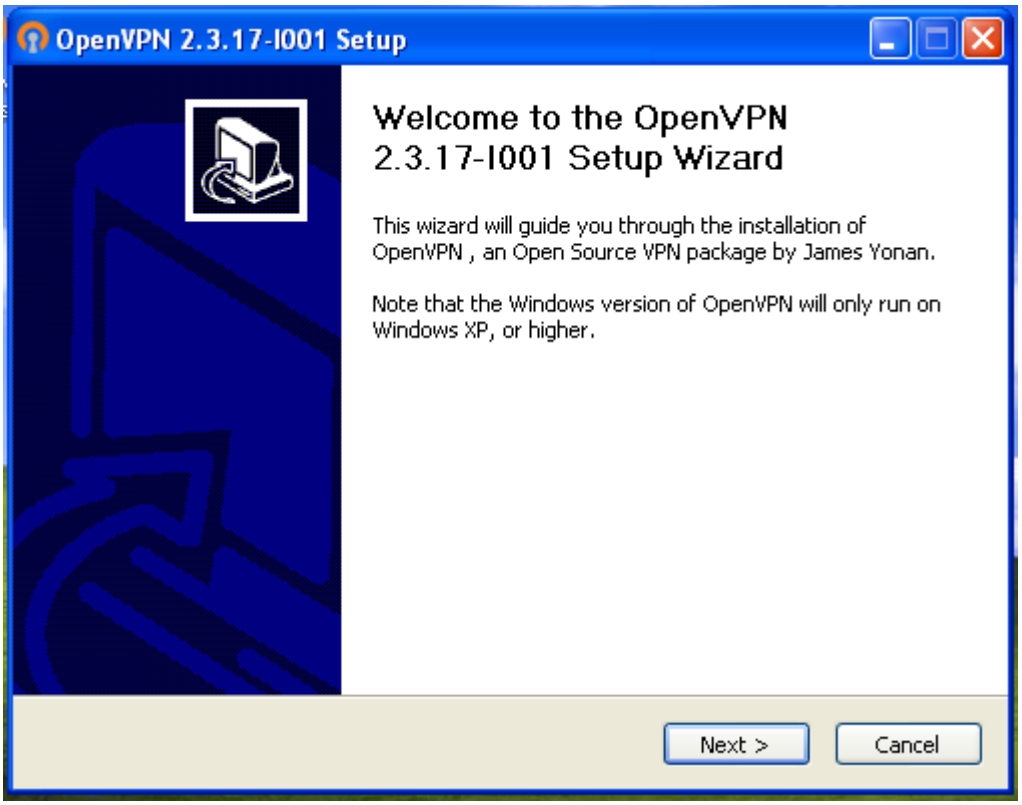


Figure III.47 : *Installation d'un client OpenVPN GUI.*

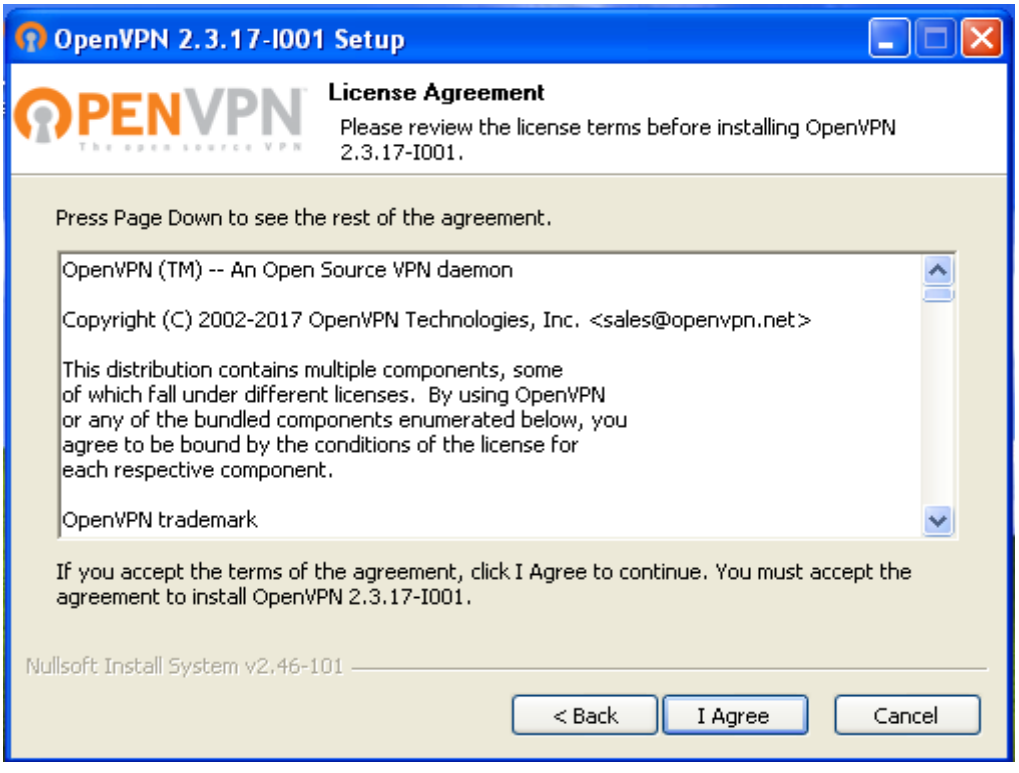


Figure III.48 : *Installation d'un client OpenVPN GUI.*

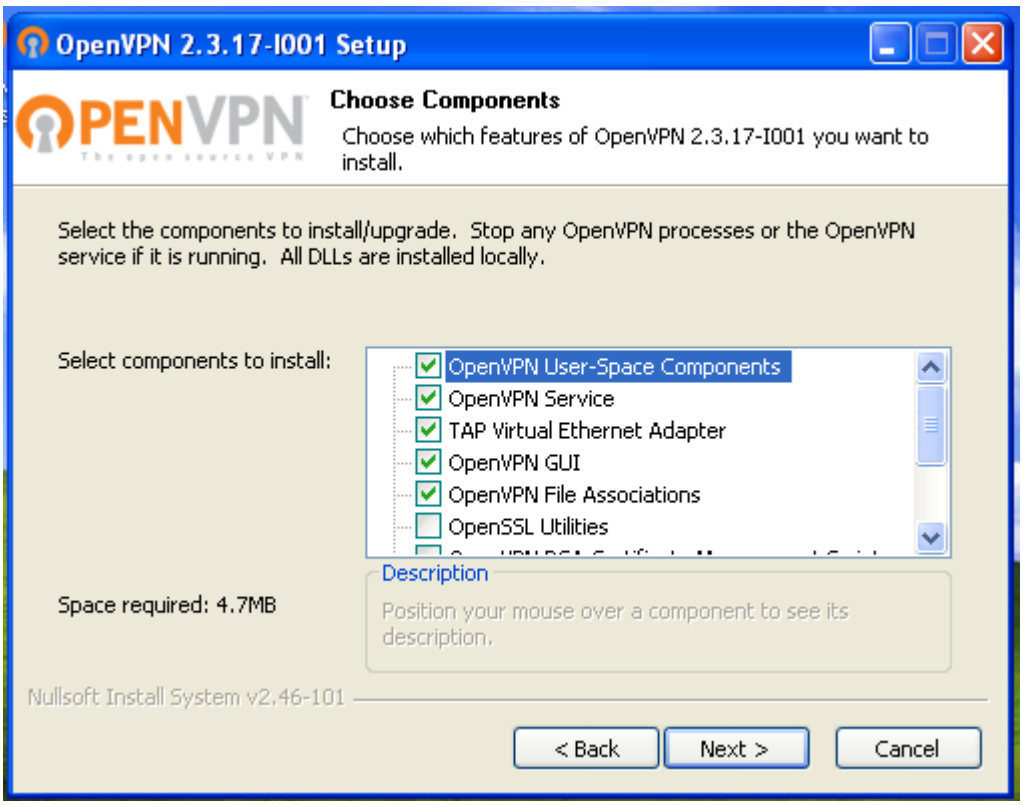


Figure III.49 :*Installationd'OpenVPN GUI.*

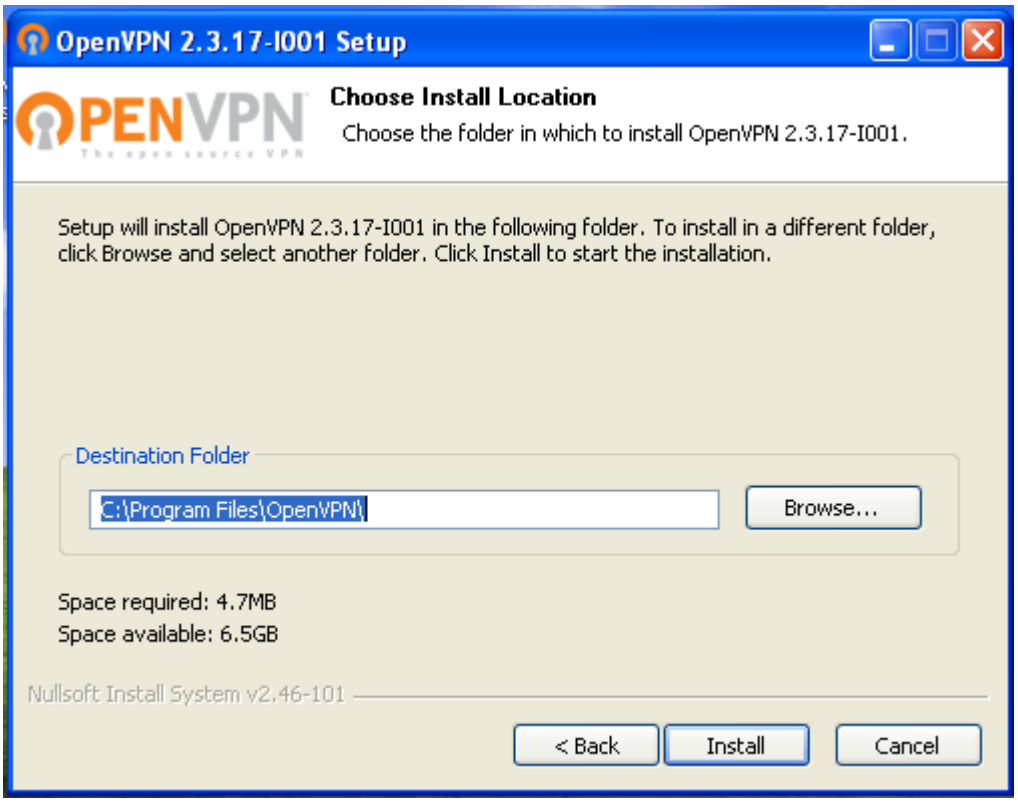


Figure III.50 *: Installation d'OpenVPN GUI.*

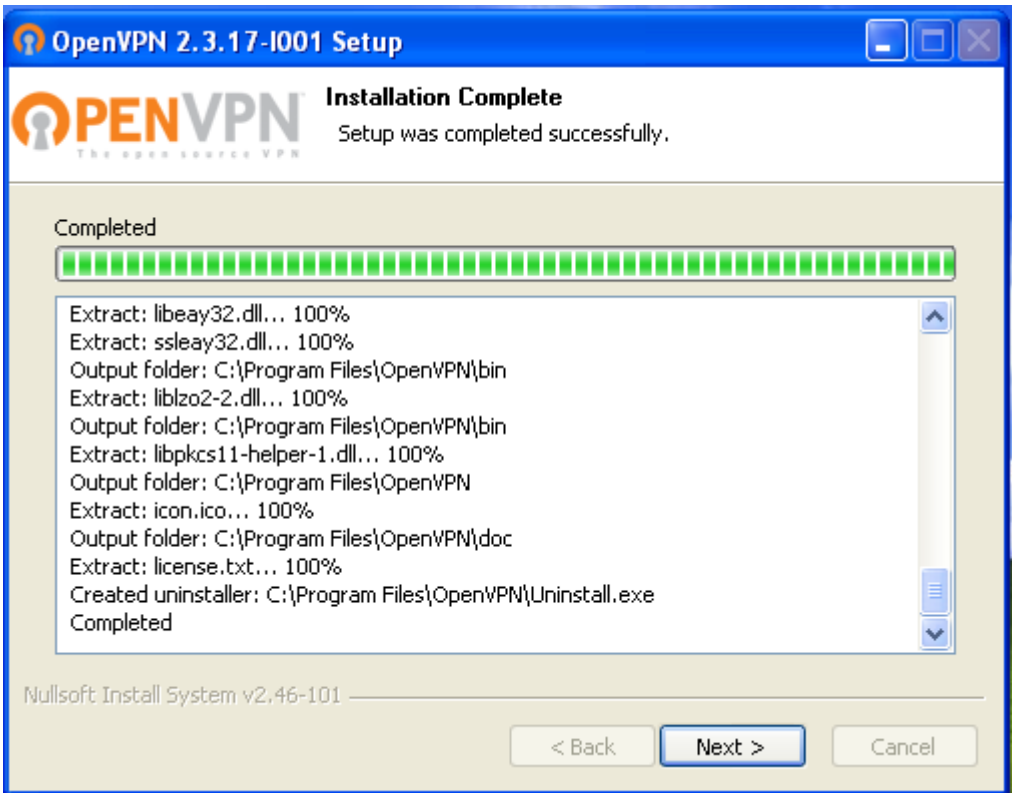


Figure III.51 : *Installation d'OpenVPN GUI.*

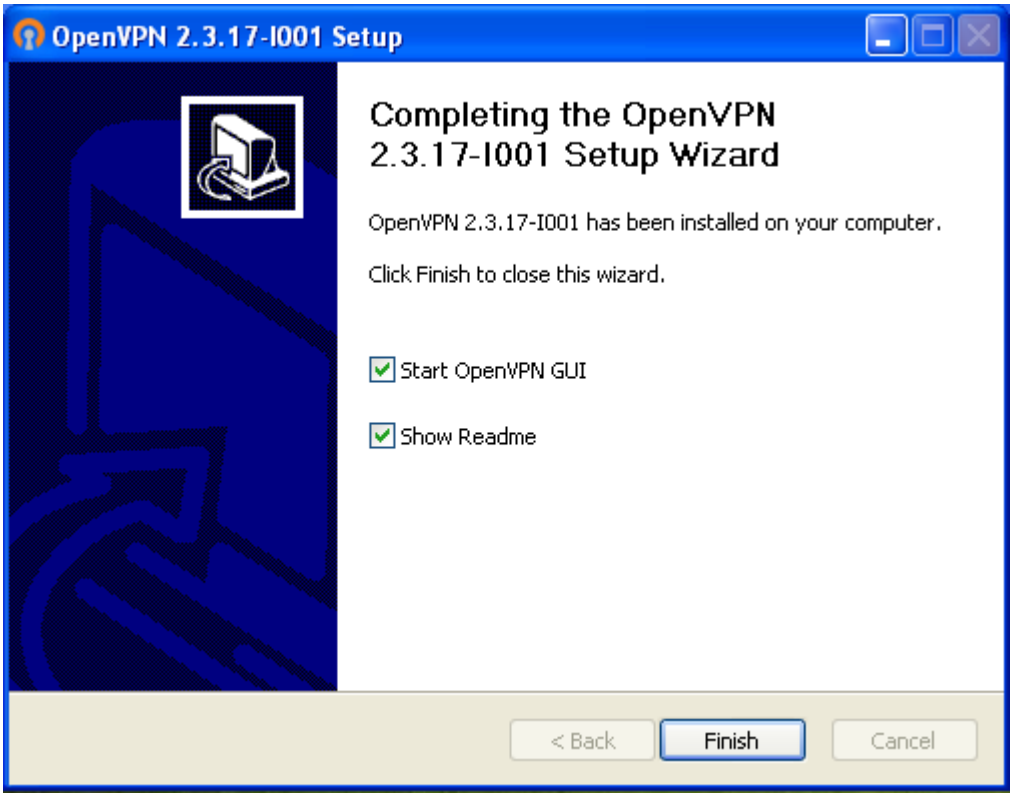


Figure III.52 : *Installation d'OpenVPN GUI.*

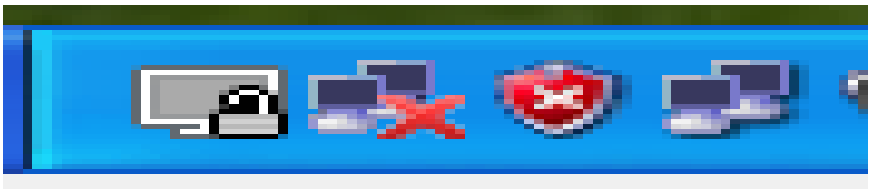


Figure III.53 : *Vérification de l'activation de l'OpenVPN.*

Nous cliquons sur OpenVPN pour obtenir une connexion :

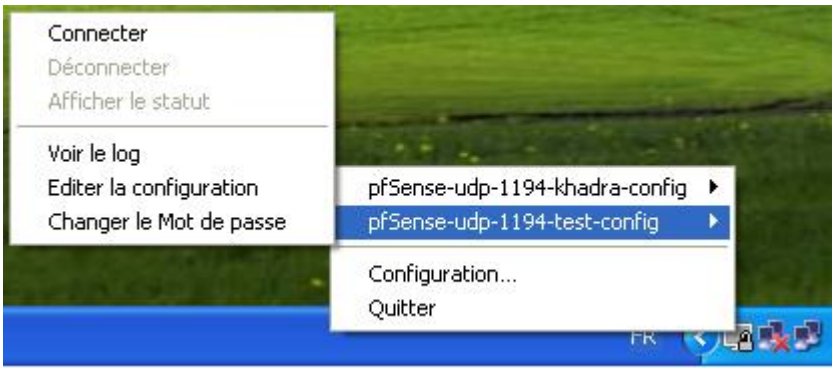


Figure III.54 : *Activation d'OpenVPN GUI.*

Nous cliquons sur connecter et nous obtenons la figure suivante :

Utilisateur : test.

Mot de passe : test.

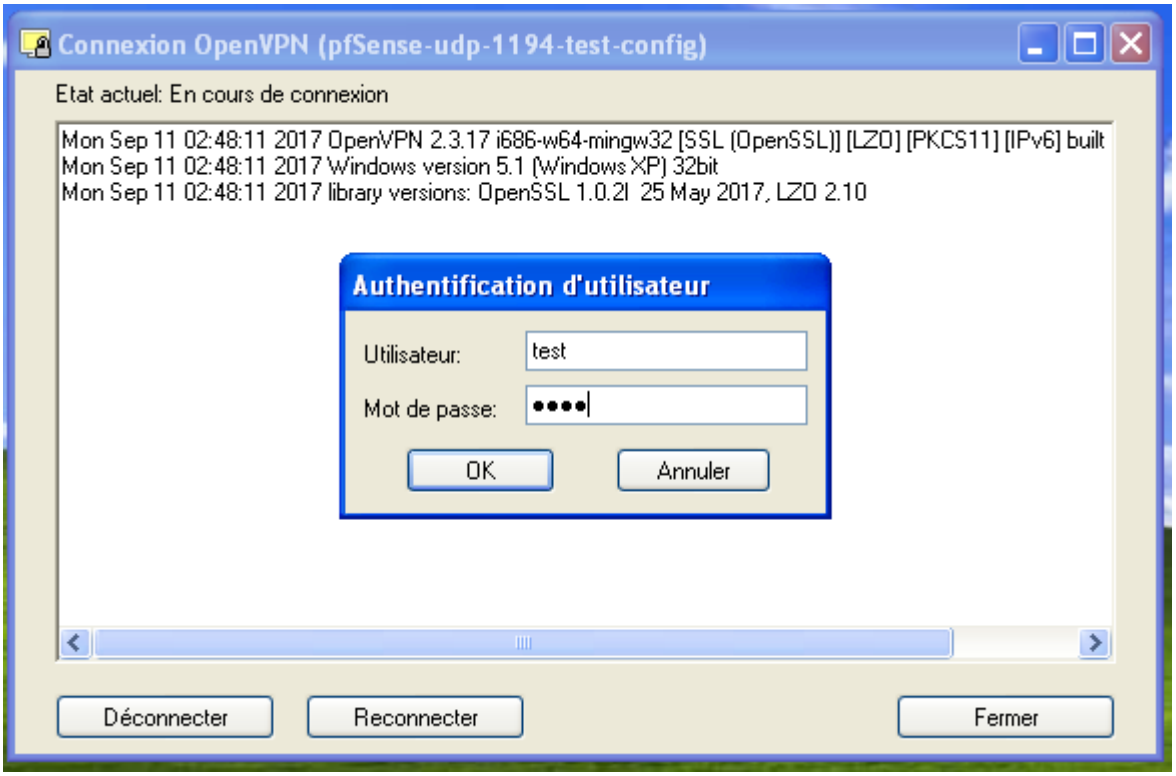


Figure III.55 : *Accès à l'OpenVPN.*

Figure III.56 : *La connexion OpenVPN.*

Donc, pour cela la connexion est établie.

e. Test de Ping vers le serveur distant (client Open VPN) :

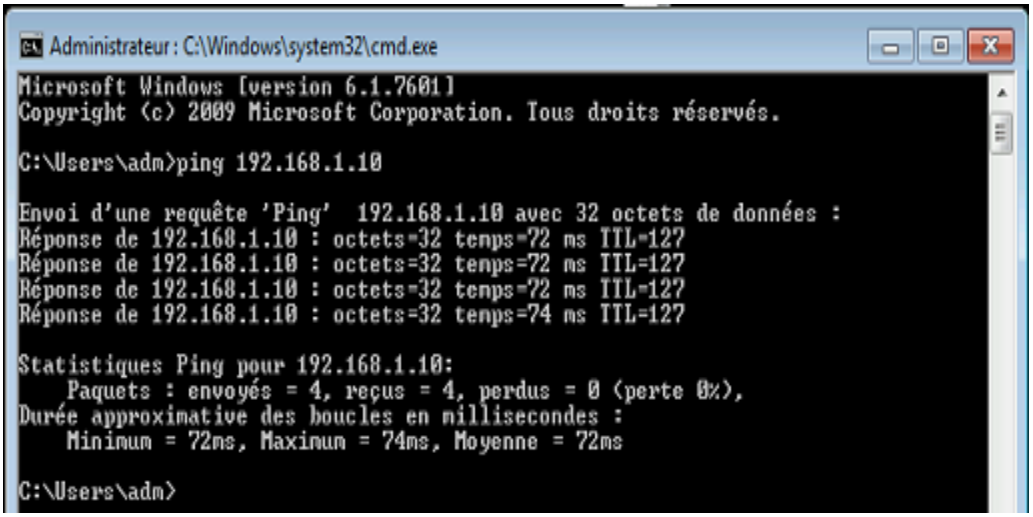
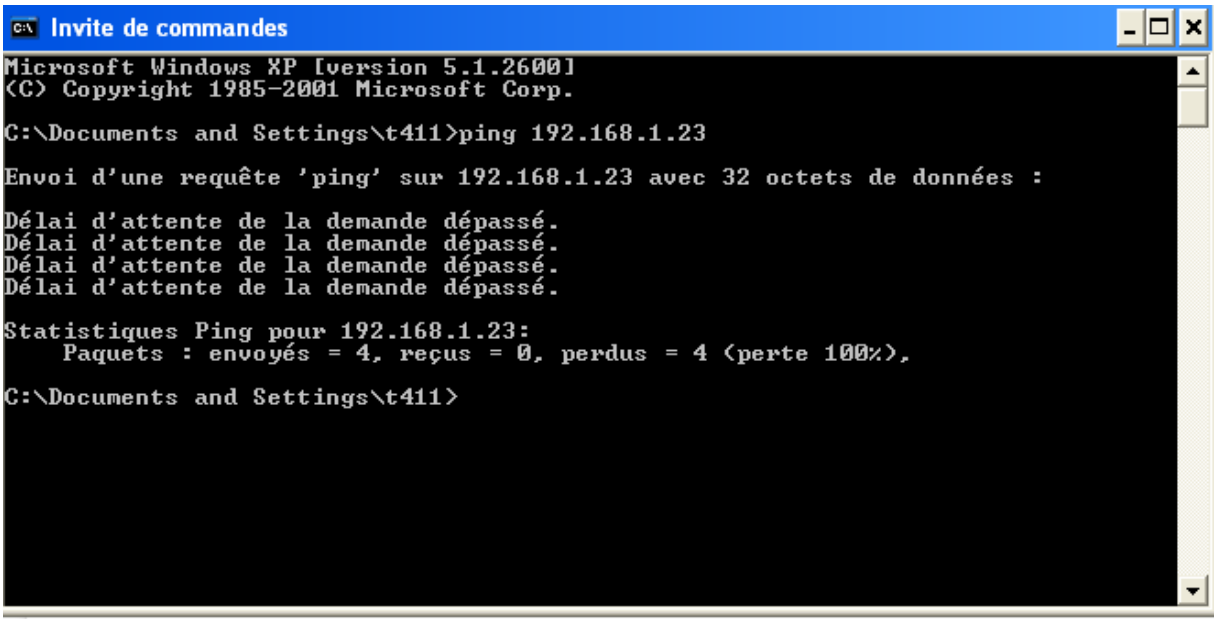
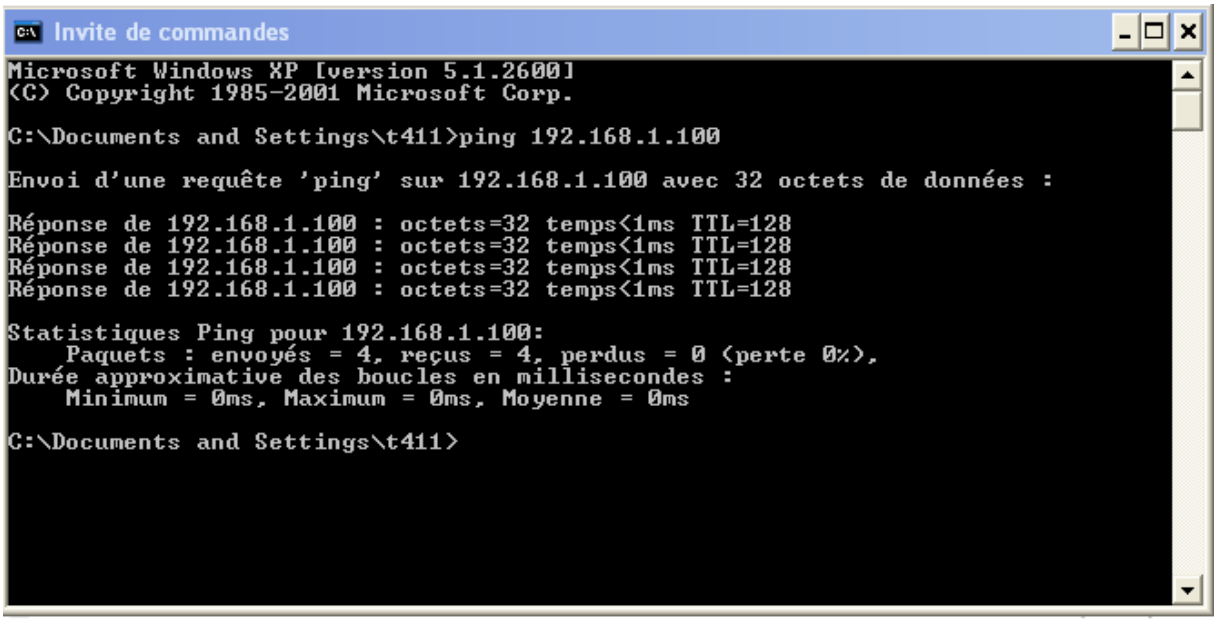


Figure III.57 : *Test de connectivité.*

f. Tester les règles d'accès de pfsense:



Interdire le trafic (l'accès) de Wan vers le serveur 192.168.1.23



Autorisé tout le trafic pour l'adresse 192.168.1.100 vers LAN adresse (vers notre réseau locale)

III.5.Discussion :

Maitriser les outils de sécurisation des réseaux locaux n‘est pas chose aisée, surtout que le nombre de failles ne cesse d‘augmenter et les intrusions nombreuses. Protéger sa vie privée, ses données ou l‘accès à son réseau est une nécessité à notre époque.

Dans ce chapitre, nous avons présenté les prérequis utilisés afin de configurer Pfsense, puis nous avons expliqué à travers diverses captures, les étapes de son installation et de saConfiguration, à travers lesquelles nous définissons quelques fonctionnalités que propose cet outil.

Le réseau informatique et devenu un élément indispensable dans chaque entreprise pour la poursuite de ces activités. Et comme nous l'avons déjà vue dans notre première partie de notre travail pour la réalisation d'un réseau on a besoin de plusieurs éléments tél que les supports de transmission et les équipements d'interconnexion…..etc. chaque réseau existant peut suber des menaces et des attaques à chaque fois qu'il s'ouvre sur internet, et pour cela nous avons opté pour une solution pour la sécurisation de ce réseau contre ces menaces et ces intrusion.

Dans notre mémoire, nous nous sommes intéressés à mettre en place une stratégie de sécurité pour pouvoir sécuriser au maximum le réseau d'une entreprise contre les menaces et les attaques éventuelles qui risquent de l'atteindre.

L'objectif principal assigné notre travail est la mise en place d'un firewall logiciel qui est le pfsense, qui permet de sécurisé le réseau d'entreprise contre les intrusions et les failles de systèmes et des attaques qui vienne par les hackeur, en filtrant tout information et fichier qui rentre et sort du réseau privé vers Internet.

Ce travail nous a permis d'améliorer nos connaissances dans le domaine de la sécurité des réseaux notamment le pare feu « pfsense » ainsi son fonctionnement et son rôle dans la sécurité d'entreprise. Il nous a également permet de découvrir le logiciel de simulation virtualbox.

Nous estimons que la mise en place d'un firewall que nous avons réalisée va répondre aux exigences et besoins des utilisateurs de fait qu'elle permet d'offrir une meilleur sécurité.

Le travail que nous avons réalisé pourrait être complété et poursuivi sous différents aspects notamment :

- Introduction d'IPv6 dans les équipements du service pilotes et avec les sites partenaires.
- Pour amélioration des mécanismes de sécurité en faisant l'installation et la configuration d'un portail captif.
- La mise en place d'une DMZ dans le pfsense.

BIBLIOGRAPHIE

[1] : Tableaux de Bord de la sécurité réseau 3ème édition- Cedric Liorens, Laurnet Levier, Denis Valois et Benjamin Morin, collection blanche, 26 aout 2010.édition PEFC

[2] : Nadia Nouali, les firewalls comme solution aux problèmes de sécurité, 2008.

[3] : Bernard Cousin, Sécurité des réseaux informatiques, Université de Rennes 1.

[4] : Guy pujolle, les réseaux, Eyrolles, 2008.

[5] : Daniel dromard et Dominique Seret, Architecture des réseaux, Pearson Education France, 2009.édition PEARSON.

[6] : Laurent Bloch, Christophe Wolfhugel, Sécurité Informatique, Eyrolles, 2011.

[7] : J.F.Pillou, Tout sur la sécurité informatique, 2ème édition, Paris, Dunod, 2009.édition DUNOD.

[8] : Lagrange Xavier, introduction aux réseaux, en France ,1998.édition HERMES.

[9] : Jeau-Luc Montagrier, pratique des réseaux d'entreprise, paris ,2000. Edition EYRALLES.

[10] : Cisco CCNA1 –Module 9 –Piles des protocoles TCP/IP et adressage IP – V3.1.

[11] : Patrick Ducrot-Sécurité Informatique-2009.

[12] : Jean Babtiste Favre, Firewall : architecture et déploiement, Creative Commons, 2006.

[13] : D.Brent Chapman, Elisabeth D. Wwicky, La sécurité sur internet Firewalls, O'Reilly, 1996.

[14] : Douicher Yacer, Sissouko Seydou, Mise en place d'un pare feu en utilisant le Smoothwall, mémoire fin d'étude, MAST, UMMTO, département électronique, promotion 2012.

[15] : Bendahmane Ahmed, Installation et configuration d'un firewall, Université Abou Berk Belkaid-Tlemcen, 2011.

[16] : Arkoub Yacine Zakari, Boudrioua Nacer-Eddine, Installation et configuration de PFSense, mémoire fin d'étude, MAST, Université de Bejaïa, 2016.

[17] : Benmansour Radjaa, Benmansour Zineb, Netfilter et ipitables appliqué sur un réseau d'une machine virtuelle, mémoire fin d'étude, MAST, Université Abou Bekr Belkaid-Tlemcen, 2013.

[18] : Makraz Hamza, Mise en place d'un pare-feu open source PFSense, mémoire fin d'étude, MAST, Université Cadi Ayyad-Merrakech, 2015.

[19] : Kafi Med Radouane, Etude et simulation d'un réseau de téléphonie sur IP, mémoire fin d'étude, mémoire fin d'étude, ING, Université Kasdi Merbah-Ouargla, 2008.

[20] : Mihoubi Mohamed, Medjani Nacer, Sécurisation d'une infrastructure LAN/WAN à base d'équipement CISCO, mémoire fin d'étude, mémoire fin d'étude, MAST, UMMTO, 2015.

[21] : Belhadj Naima, Etude et conception d'une plate-forme de réseau informatique couplant entre sécurité et supervision pour l'entreprise ENIEM, mémoire fin d'étude, MAST, UMMTO, 2013.

[22] : Belhadj Belaid, Hamadouche Yacine, Etude et sécurisation d'une infrastructure DMZ avec ASA CISCO5510, mémoire fin d'étude, MAST, UMMTO, 2015.

[23] : Aliche Sonia, Haddad Abbas, Implémentation d'une politique de sécurité au réseau informatique de l'entreprise ENIEM de T.O, UMMTO, 2011.

[24] : Abtout Nadjia, Douani Dalila, Sécurisation d'une infrastructure DMZ avec ASA 5510, mémoire fin d'étude, MAST, UMMTO, 2012.

[25] : Aliouine Boussad, La mise en place de la protection d'accès au réseau NAP associe au serveur DHCP, mémoire fin d'étude, MAST, UMMTO, 2012.

[26] : Ouelhadj Mohamed Amine, les techniques de sécurité des réseaux, mémoire fin d'étude, MAST, UMMTO, 2015.

[27] : Yaddadane Farida, Toumi Nedjma, mise en œuvre d'une infrastructure réseau sécurisée par l'ISA server, mémoire fin d'étude, MAST, UMMTO ,2012.

[28] : Allou Saïd, Allouane Kahina, Cryptographie et sécurité des réseaux Implémentation de l'AES sous MATLAB, mémoire fin d'étude, MAST, UMMTO, 2008.

[29] : Loualy Ibrahim Bassirou, Mise en place d'un OpenVPN sous PFSense, mémoire fin d'étude ING,

[30] :http://www.memoireonline.com/recherche3.html.

[31] : http://www.commentçamarche.net.

[32] : https://fr.wikipédia.org.

Annexe A

1-Présentation de l'organisme d'accueil « ENIEM »:

Situation géographique :

L'entreprise ENIEM (Entreprise Nationale des Industries de Electroménagers) se trouve à la zone industrielle AISSAT IDIR-OUED AISSI à 10 Km de TIZI OUZOU, elle s'étale sur une surface totale de 55 hectares, sa direction générale se trouve au chef de lieu de TIZI OUZOU à proximité de la gare ferroviaire.

Activités et objectifs de l'entreprise :

- ✓ **Activités :** Les activités de l'ENIEM sont concentrées sur la production, le montage, la commercialisation, le développement de la recherche dans les différentes branches de l'électroménager. Ces activités sont assurées par cinq unités :
- **Unité froid :** Produit des réfrigérateurs et congélateurs.
- **Unité cuisson :** Assure la production des cuisinières.
- **Unité climatisation :** Produit des climatiseurs, machines à laver et des chauffes eau.
- **Unité commerciale :** Assure la distribution et l'exportation des produits ENIEM, ainsi les services après-vente.
- **Unité prestation technique :** Assure les fonctions de soutien aux autres unités.

- ✓ **Objectifs :**
    - L'amélioration de la qualité et l'augmentation du volume de production.
    - La maitrise des coûts de production.
    - L'augmentation des capacités d'études et de développement.
    - Amélioration de la maintenance de l'outil de production des installations.
    - La valorisation de ressources humaines.

2-Organisation de l'entreprise :

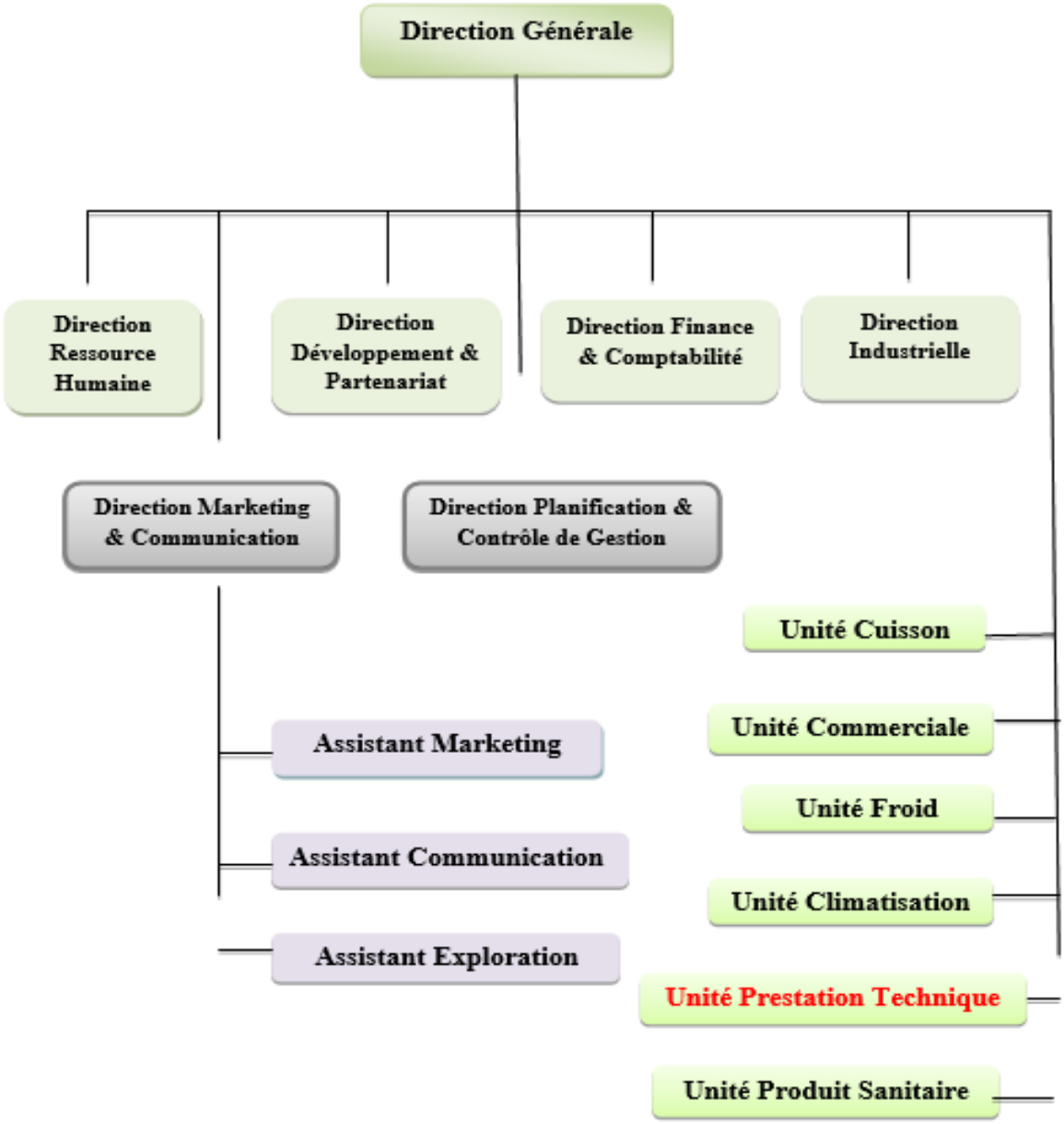


Figure 2 : Organigramme de l'entreprise.

3-Le champ d'étude :

a- L'organigramme de l'unité prestation technique :

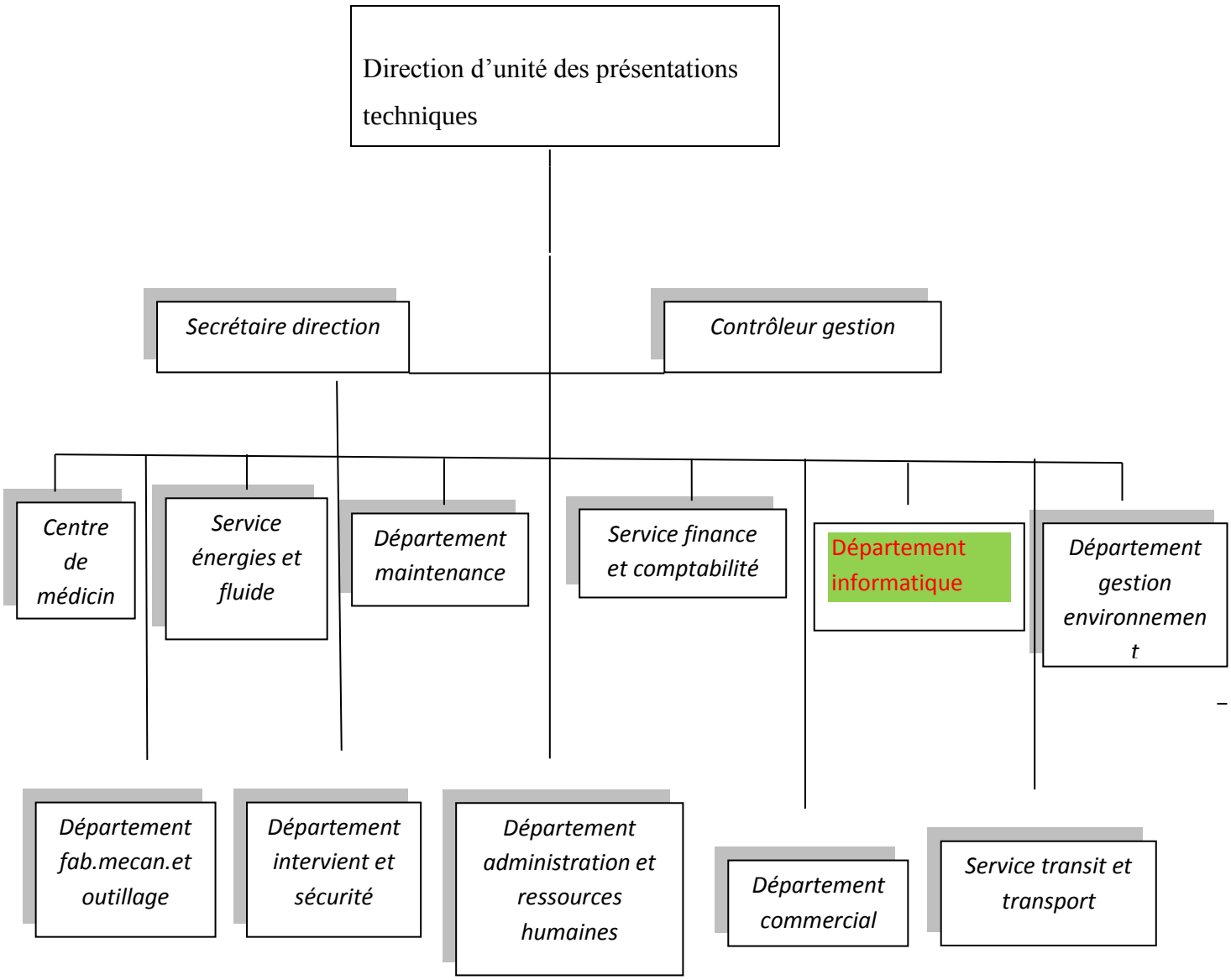


Figure 3 : *Organigramme de l'unité présentation technique.*

Annexe A

b -L'organigramme de département informatique (champ d'étude) :

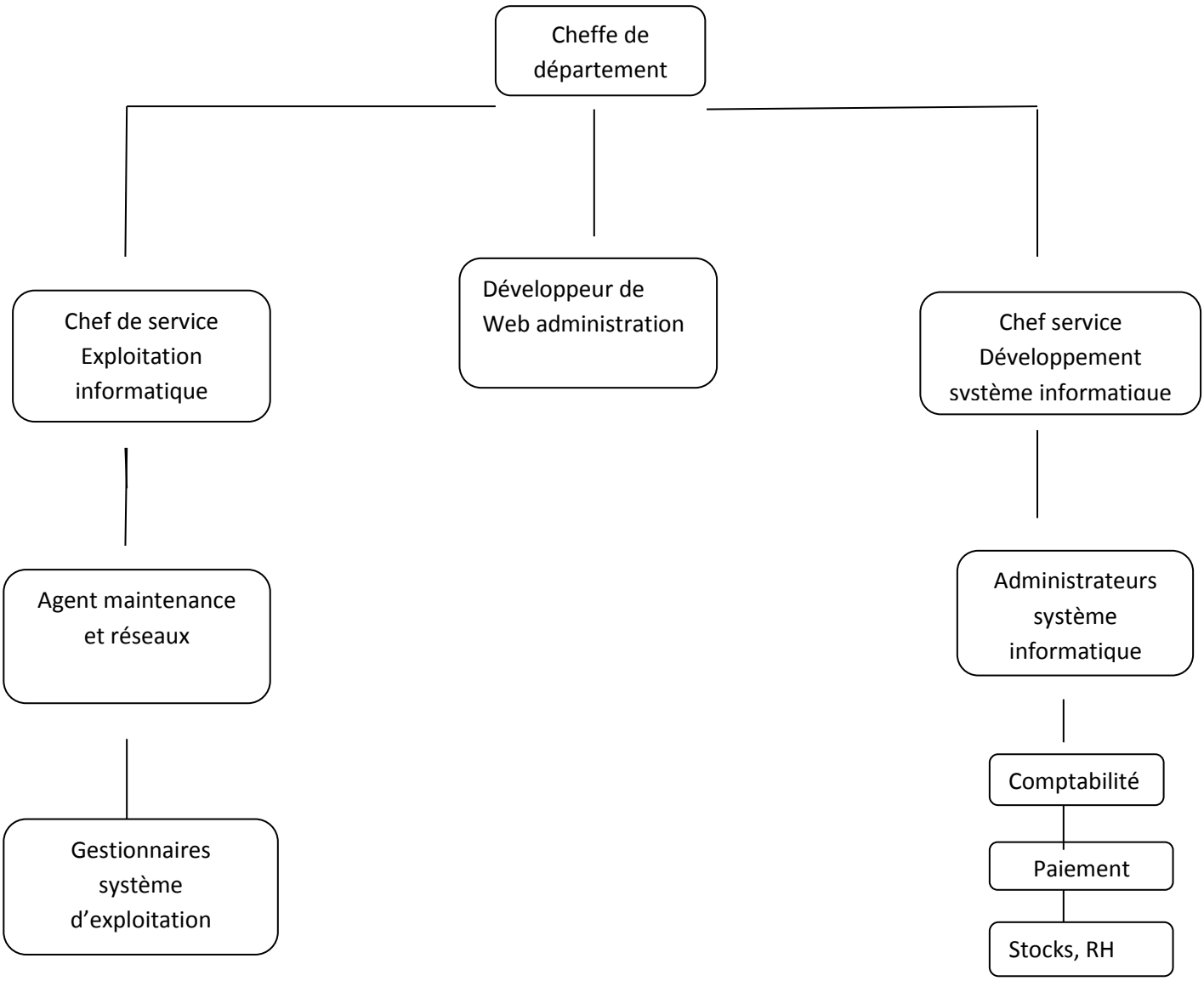


Figure 4 *: Organigramme du champ d'étude.*

Annexe A

Description de département informatique :

Le département informatique assure les prestations qui répondent aux attentes des utilisateurs internes en termes de fiabilités, sécurités et délai. Il dispose de :

- 12 postes ;
- Imprimantes : 4 de type HP petite taille et 4 de grande taille ;
- Grand onduleur.

Le département informatique se départage en deux services :

- ✓ Service développement du système informatique(SDSI).
- ✓ Service exploitation informatique(SEI).

1. Service développement informatique :

Ce service s'occupe du développement des applications et des programmes informatiques. Il est constitué de deux sous services, le premier est chargé de la conception développement informatique et le deuxième s'occupe de l'administration des systèmes informatiques.

2. Service exploitation informatique :

S'occupe de la gestion de l'ensemble des moyens informatiques, de saisie, de traitement de transmission et de restitution de l'information et assistance aux utilisateurs. Ce service est composé de deux sous services, l'un est le chef de la salle machine qui est ma responsable des travaux de l'ordinateur st ces annexes. A son niveau, on trouve des gestionnaires système d'exploitation qui le responsable de système. L'autre est le chef se section gestion des systèmes d'exploitation qui le responsable du système hardware

Software et des réseaux. Il doit assurer le bon fonctionnement des équipements (suive des contrats, de maintenance et procède au planning maintenance préventive), procède à des évolutions techniques, réseau, télétraitement, base de données, logiciel de basse etc. IL doit aussi assure la fonction de conseille et d'interface avec l'utilisateur (attaché au chef de salle machine), à son siège on trouve des « Agents réseau informatique »

3. Missions et activités du département informatique :

Le département informatique s'occupe :

- De traiter des commandes d'achats ;
- De la compatibilité générale ;
- Du lancement des commandes en fabrication ;
- De la gestion des stockes de matière première et composant ;
- De la gestion de paie ;
- De l'établissement des procédures de sauvegarde et de restauration des données ;
- D'informer et de former les utilisateurs à l'exploitation optimale des applications.

Le réseau informatique de l'ENIEM :

L'entreprise est dotée d'un réseau intranet et comme cela est constitué des ateliers et du bloc administratif, elle englobe deux types de réseaux :

- ✓ Réseau point à point des ateliers ;
- ✓ Réseau local Ethernet du bloc administratif.
- ✓ **A-Réseau des ateliers :**

Le réseau utilisé au niveau des ateliers est un réseau point à point. Il est composé de 39 terminaux dont 27 écrans de type HP et 12 imprimantes HP reliés au serveurHP3000/A500 par liaison :

- ➢ Directe pour des distances inférieures ou égales à 1200 mètres ;
- ➢ Modem avec des lignes téléphoniques (4 fils) pour des distances supérieures à 1200 mètres ;
- ➢ Multiplexeur- Modem/Modem-démultiplexeur pour les installations de plusieurs distants.

1-Réseau du bloc administratif :

Le réseau informatique intranet de l'ENIEM est un réseau ouvert basé sur la famille des protocoles TCP/IP. Un réseau Ethernet dont la topologie choisie est en « étoile », à savoir deux bâtiments associés donnant une forme T (bâtiment A et bâtiment B ou se trouve notre champ d'étude).

Le schéma général du câblage et défini selon le nombre de bureaux et le nombre d'utilisateurs par bureau. Tous les bureaux sont dotés d'au moins une prise .Il en excite en tout 170 prises. Toutes les prises d'un même étage sont reliées à un Switch contenu dans une armoire dite « armoire d'étage ». Cette dernière est reliée par un câble Fibre Optique à un Switch dit « Fédérateur » contenu dans une armoire centrale installé au niveau de salle machine au sous-sol du bâtiment B où le Switch du département informatique aussi incluse.

Annexe B

Le réseau est composé au total de 06 armoires départagées dans deux bâtiments, deux à chaque étage. L'emplacement est dicté par la distance maximale entre un Switch et un poste de travail, qui ne doit pas dépasser 100 mètres.

Description du matériel utilisé dans le réseau local :

La salle machine est considérée comme le point centrale du réseau dont elle contient les éléments principaux du réseau de l'entreprise. Ces composants sont : un serveur HP3000/A500 et une armoire de brassage.

- **Description du serveur HP3000/A500 :**

a- La face arrière :

Le serveur est composé de DTC (Data Terminal Circuit) qui gère deux types de panneaux : DDP (Panneau de Distribution Direct) et MDP (Panneau de Distribution Modem).

- Les ports sur DDP sont de type RJ45 (norme RS423) et numérotés de 100à 115, 200à 215 pour les ports écrans et de 300à 315 pour les ports imprimantes.
- Les ports sur MDP sont du type BD25 (norme RS232)et numérotés de 400à 415, de 500 à 515 pour les ports écrans et de 600 à 615 pour les ports imprimantes.

La face arrière des ports DTC est composée des ports AUI et des ports BNC T (Thinlan port) et chacun de ces derniers sont connectés entre eux avec un câble coaxial qui est connecté à son tour au convertisseur Ethernet (10 base 2 à 10 base T).La sortie de convertisseur est un port RJ45 qui est connecté à l'armoire centrale.

Il est aussi équipé d'une unité centrale dont la face arrière est rassemblée de :

- **Console UPS port** qui peut être connecté à 3 consoles sorties DB9 avec des câbles HP24252 :
  - ✓ **UPS :** pour brancher l'onduleur ;
  - ✓ **Remporte :** c'est une console secondaire, elle est mise en marche lorsque la console principale se bloque ;
  - ✓ **Console principale.**
- **Une console LAN** 10base T (console réseau) ;

- **Le dérouleur** : pour lire les cartes de l'ancien système.

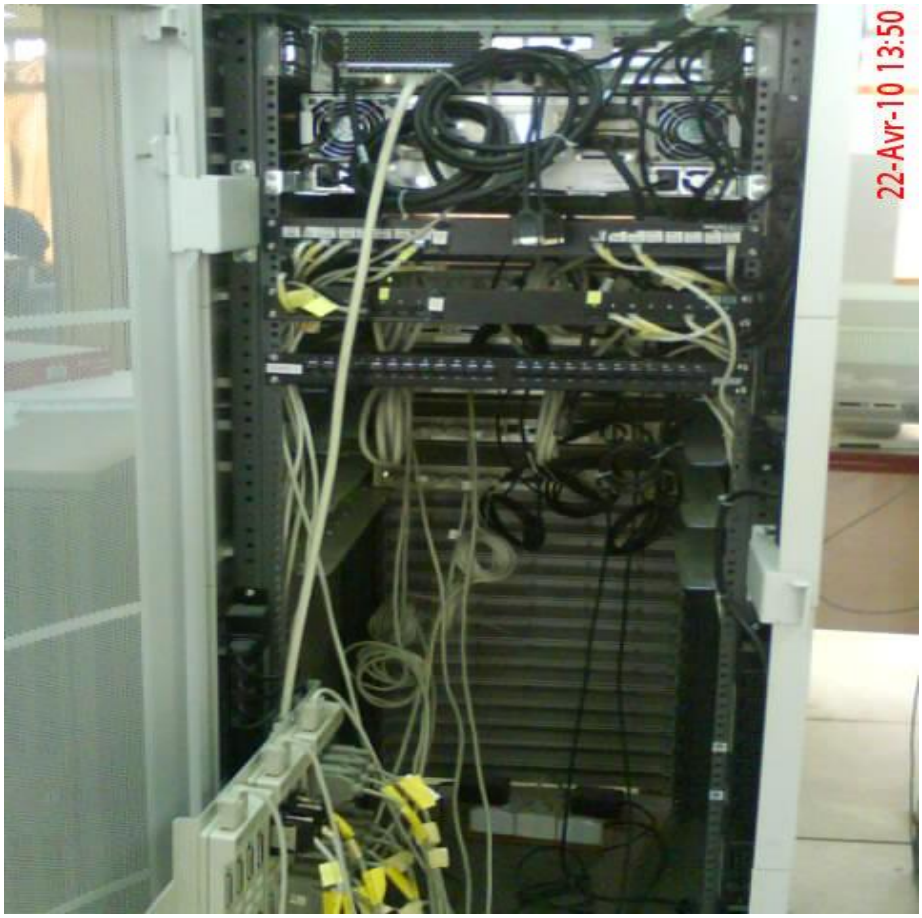


***Figure5** : La face arrière du serveur HP3000/A500.*

b-La face avant :

Elle est composée des éléments suivants :

- ✓ Lecteur cassettes DLT ;
- ✓ Lecteur DVD ;
- ✓ Lecteur DDS.

Figure 6 : la face avant du serveur HP3000/A500.

- **Armoire de brassage centrale :**

C'est l'armoire principale, toutes les armoires d'étages sont reliées à celle-ci, l'interconnexion est assurée grâce au Switch fédérateur, elle est constituée des éléments suivants :

- 02 panneaux de brassage à 16 ports contiennent des connecteurs RJ45 ;
- 01 Switch d'étage CiscoJ45 et des ports GBI ;
- 01Onduleur pour voir le temps à sauvegarder les données ;
- 01 Switch fédérateur contient 7 ports GBIC ;
- 03 tiroirs optiques qui relient les armoires des blocs ;
- 01 Onduleur électrique à 06 prises sous onduleur pour alimenter les périphériques actifs.

Figure 7 : *Armoire de Brassage.*

- **Armoire d'étage :**

Elle est constituée des éléments suivants :

- Switch Cisco de 24 ports;
- Panneau de brassage le grand à 16 ports ;
- 01 tiroir optique ;
- 01 multiprise.

Figure 8: *Armoire d'étage.*

- **Serveur de virtualisation :**

La virtualisation des serveurs peut se définir comme le fait de faire fonctionner plusieurs serveurs virtuels sur un serveur physique, ces derniers étant alors remplacés par leur équivalent virtuel. L'objectif est de mutualiser les capacités de chaque serveur, permettant à l'entreprise de réaliser des économies et de réduire les investissements en infrastructures physique.

Figure 9 : *Serveur de virtualisation.*

6- ***Architecture du réseau informatique existant.***

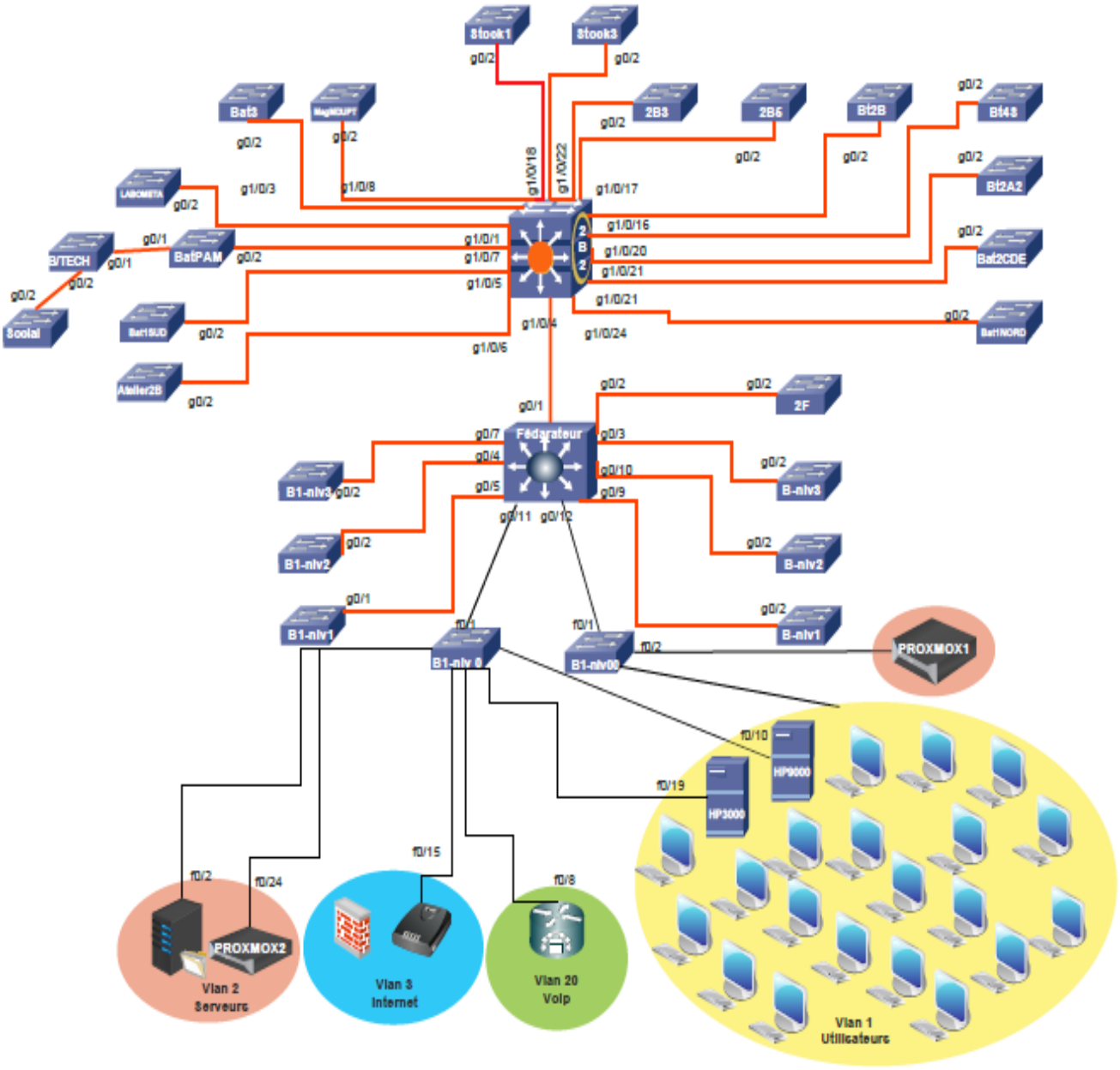


Figure 10 : *Architecture du réseau informatique existant.*

Présentation du réseau existant :

Le réseau existant est principalement composé de :

- ✓ 09 Switch Cisco de niveaux 2 ou de niveau 3 ;
- ✓ 02 Switch Cisco fédérateur ;
- ✓ Un serveur de base de données (HP3000/A500) ;
- ✓ Un serveur de web publié qui peut être vu depuis internet(HP9000) ;
- ✓ Un modem (relie le réseau à internet) ;
- ✓ Des postes de travail de type HP.
- ✓ 02 Switch de virtualisation (proxmox1et 2).

Grace aux visites au niveau du site, nous avons pus avoir une idée sur l'architecture actuelle du réseau informatique de l'entreprise et en dégagée les points suivants :

- ➢ Les différentes structures à savoir les blocs administratifs, les directions d'unités, la structure informatique, et le service commercial des unités, dépendent d'un serveur situé au niveau du département informatique.
- ➢ Le réseau local englobe des Switchs Cisco de niveau deux et trois, dotés d'une configuration par défaut, cela implique que l'utilisation de ces équipements est limitée aux VLAN 1. Ce qui induit que tous les postes se trouvent dans un seul sous-réseau, ceci fait que les communications et les accès sont illimités (aucune politique d'accès).
- ➢ Vulnérabilité au niveau organisation interne : la répartition et la multiplication des systèmes du pôle informatique avec sa solution soit disant moins couteuse, et vu que toutes les unités et leurs foncions appartiennent au même sous-réseau, entraine une complexité voir même une impossibilité à gérer la sécurité de ces systèmes.
- ➢ Les serveurs, de web, de messagerie et de partage de connexion sont assurés par seule machine, celle-ci est directement connectée à internet sachant que le seul moi de sécurisation est un firewall logiciel, cella indique une forme de sécurité minimum et insuffisante.
- ➢ Le réseau local a été conçu aux débuts, dans une logique de réseau ouvert.

Concrètement cette logique ouverte se traduit par un certain nombre de problème :

- Toute prise réseau qu'elle soit accessible en débranchant un poste de travail ou mise a disposition pour des prestataires extérieur par exemple, est une menace potentiel, car l'accès réseau sera, dans tout les cas, donné à la machine connecté.
- un poste mobile, infecté par un ver, pourra en se reconnectant au LAN contaminer le périmètre interne.
- Le serveur de base de donnée contient des données sensibles mais il peut être accessibles par n'importe qui en privilège et en droits (alors qu'il est impératif que l'accès soit interdit de l'extérieur et limité de l'intérieur).
- L'architecture de réseau n'est pas maitriser, car rien n'empêche un employé d'ajouter un équipement réseau non autorisé à la place de son poste de travail (un point d'accès wifi par exemple).

Les besoin interne en termes de sécurité :

Vue l'existant, nous avons peut distinguer les besoins en terme de :

- Confidentialité : assurer que le seuls les tiers autorisés aient accès aux informations de l'entreprise considérées comme étant discrètes, empêcher par cela toute divulgation de celle-ci.
- Disponibilité : toujours garantir la continuité de l'accès aux services offerts par le réseau local, a des informations ou des ressources.
- Intégrité : garantir que les données stockées dans la base de données ou en transit sur le réseau ne soient pas altérées (de manière intentionnelle ou accidentelle).
- Authentification : garantir la justesse d'identité des utilisateurs ou des équipements de réseau informatique de L'ENIEM .
- Contrôle d'accès : contrôler les autorisations de toutes les entités dans le but de limiter les accès aux ressources et aux services protégés (base de données….).

Travail demandé :

Et donc le but de ce projet est de trouver une solution optimale et facile a utiliser spécialement pour la sécurisation de réseau de l'entreprise et a fin de pouvoir réaliser ce travail, on ferra une installation d'un firewall logiciel pour que il nous assure une sécurité minimal de réseau.

Résumé :

L’ouverture de l’accès de l’entreprise sur internet provoque plusieurs attaques et pour se protéger contre ces derniers, une architecture de réseau sécurisée est nécessaire, tel qu’un pare-feu. Cet outil a pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les tentatives d'intrusion pour ce protégé le mieux possible. Cela permet de rendre le réseau ouvert sur Internet beaucoup plus sûr. Le firewall propose donc un véritable contrôle sur le trafic réseau de l'entreprise. Il permet d'analyser, de sécuriser et de gérer le trafic réseau, et ainsi d'utiliser le réseau de la façon pour laquelle il a été prévu.

Dans notre mémoire, nous nous sommes intéressés à mettre en place une stratégie de sécurité qui le firewall pfsense pour pouvoir sécuriser au maximum le réseau d’une entreprise ENIEM contre les menaces et les attaques éventuelles qui risquent de l’atteindre.

Les mots clé :

ENIEM

PFSENSE

Virtualbox

Firewall

Réseaux

Sécurité