République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la

Recherche Scientifique

**Université Abderrahmane Mira. Bejaïa**

Faculté des Sciences Exactes
Département Informatique

**Mémoire de fin d'études**

**en vue de l'obtention du diplôme de Master Professionnel en Informatique**

## Option : Administration et sécurité des réseaux

## Thème

# *Installation et configuration de pare-feu pfsense au sein de l'entreprise Ramdy*

**Présenté par** :

- Tahtat lahna.
- Bensafia Zakia**.**

**Encadré par :**
Mme Yessad Samira.
**membre de jury**
Mr Amroun Kamel.
Mme Belkhiri Louiza.

**Année Universitaire : 2019/ 2020**

# 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 YESSAD 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 RAMDY en particulier Mr DJOUNNER, 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 mes grandes tantes : Adouda, Chrifa ,Fatiha.
- A mes sœurs : Dalia et Amina ;
- A mon grand frère MOUNIR et a mon petit frère ANIS.
- A tous mes cousins et cousines.
- A tous mes amis : Zouina, Selma ,Zahra , Samra ,Kenza ; Dalila.
- et à ma binôme lahna et sa famille,
- A toute la promotion 2020.
- A toute personne ayant contribué de près ou de loin à la réalisation de ce travail.

**ZAKIA**

# Dédicaces

Je souhaite de tout mon cœur, avec l'aide de dieu tout puissant que ce mémoire soit à la hauteur.

Je dédie ce modeste travail accompagnée d'un profond amour : à mon très cher papa qui avait la soif de connaissance et de savoir, ma source d'amour, d'affection de générosité et de sacrifices.

Tu étais toujours la près de moi pour me soutenir, m'encourager et me guider aves tes précieux conseils et qui m'a permis de mieux comprendre la vie que son âme repose au paradis tu me manque énormément

A mon adorable maman aucune dédicace ne saurait exprimer mon respect, ma source de ma vie l'amour éternel et de tendresse qui n'a pas cessé de m'encourager et de prier pour moi vous m'avez toujours aidé par vos conseils et vos sacrifices. Puise dieu le tout puissant t'accorder meilleure santé et longue vie

A mes cher sœur : Feriel et son mari anis et toute sa famille et mon petite ange ilyes hamou et Notre trésor Sarah et à mon cher frère Saïd leur patience soutien et leur sentiments d'amour aux moments les plus difficiles je vous souhaite une longue pleine de santé et de réussite

A mes oncles et mes adorables cousines et a toute la famille Tahtat ainsi la famille Ouahabrache et Bouzit pour leur encouragements et leur soutien morale.

A mes chers amis Rafik , Tinhinene ,Dihia et ma binôme Zakia.

**Lahna**

# Liste des figures

# Liste des tableaux

# Liste des abréviations

**AAA:** **A**uthentication **A**uthorization **A**ccounting.

**ACL**: **A**ccess **C**ontrol **L**ist.

**ARPANET**: **A**dvanced **R**esearch **P**rojects **A**gency **N**etwork

**BSD**: **B**erkeley **S**oftware **D**istribution

**CD:** **C**ompact **D**isc.

**DARPA:** **D**efense **A**dvanced **R**esearch **P**rojects **A**gency

**DHCP**: **D**ynamic **H**ost **C**onfiguration **P**rotocol

**DMZ**: **D**emilitarized **Z**one

**DNS**: **D**omain **N**ame **S**ystem

**Dos**: **D**enial **O**f **S**ervice

**FTP**: **F**ile **T**ransfer **P**rotocol

**H-IDS**: **H**ost **B**ased **I**ntrusion **D**etection **S**ystem

**HTTP:** **H**yper **T**ext **T**ransfer **P**rotocol

**IDS***:* **I**ntrusion **d**etection **S**ystem

**IP:** **I**nternet **P**rotocol

**IP sec**: **I**nternet **P**rotocol **S**ecurity

**IPV4**: **I**nternet **P**rotocol **V**ersion 4

**IPV6:** **I**nternet **P**rotocol **V**ersion 6

**IRC-DCC:** **I**nternet **R**elay **C**hat **D**irect **C**lient-to-**C**lient

**ISO:** **I**nternational **S**tandard **O**rganization

**LAN**: **L**ocal **A**rea **N**etwork

**MAC**: **M**edia **A**ccess **C**ontrol

**MAN:** **M**etropolitan **A**rea **N**etwork

# Liste des abréviations

**NAT**: **N**etwork **A**ddress **T**ranslation

**N-IDS**: **N**etwork **B**ased **I**ntrusion **D**etection **S**ystem

**OS: O**perating **S**ystem

**OSI: O**pen **S**ystem **I**nterconnect

**PAN: P**ersonal **A**rea **N**etwork

**PF**: **P**acket **F**ilter

**Pfsense** : **P**acket **F**ilter **S**ense

**PIX**: **P**rivate **I**nternet **E**xchange

**RADIUS**: **R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice

**RAN: R**egional **A**rea **N**etwork

**SI** : **S**écurité **I**nformatique

**SMTP**: **S**imple **M**ail **T**ransfer **P**rotocol

**TCP: T**ransmission **C**ontrol **P**rotocol

**Telnet*:* T**elecommunication **N**etwork

**UDP**: **U**ser **D**atagram **P**rotocol

**UFS: U**niversal **F**lash **S**torage

**VLAN: V**irtual **L**ocal **A**rea **N**etwork

**VPN**: **V**irtual **P**rivate **N**etwork

**WAN**: **W**ide **A**rea **N**etwork

# Introduction

De nos jours, la plupart des entreprises possèdent de nombreux postes informatiques qui sont en général reliés entre eux par un réseau local. Ce réseau permet d'échanger les données entre les divers collaborateurs internes à l'entreprise et ainsi de travailler en équipe sur des projets communs. Une entreprise n'est jamais complètement fermée sur elle-même. Il est par exemple nécessaire de pouvoir partager des informations avec les clients de l'entreprise, ce qui signifie laisser une porte ouverte à divers acteurs étrangers. Cette porte peut être utilisée pour des actions qui, si elles ne sont pas contrôlées, peuvent nuire à l'entreprise (piratage et destruction de données).

Pour parer à ces attaques, une architecture de réseau sécurisée est nécessaire. L'architecture devant être mise en place doit comporter un composant essentiel qui est le pare-feu. Cet outil a pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les tentatives d'intrusion et d'y parer au mieux possible. Cela permet de rendre le réseau ouvert sur Internet beaucoup plus sûr. De plus, il peut également permettre de restreindre l'accès interne vers l'extérieur et inversement.

En plaçant un pare-feu limitant ou interdisant l'accès à ses services, l'entreprise peut donc avoir un contrôle sur les activités se déroulant dans son enceinte.

Dans ce cadre s'inscrit notre projet de fin d'études qui consiste à mettre en place un pare-feu pfsense d'entreprise, cas de RAMDY. Pour mener à bien notre travail, nous le répartissons en quatre chapitres.

Nous allons préluder par « organisme d'accueil » où nous allons faire une présentation de l'entreprise RAMDY et dégager la problématique de l'entreprise et proposer une solution.

Dans le deuxième chapitre «« Généralités sur les réseaux et sécurité informatique », nous allons définir les réseaux, leurs rôles ainsi que leurs différents type d'une part et définir la sécurité informatique et retracer quelques attaques d'autre part.

Dans le troisième chapitre nommé « Les pare-feu », nous allons expliquer c'est quoi un pare-feu et ses différents types.

Le dernier chapitre « Réalisation » sera consacré à la réalisation de notre travail qui est une installation et configuration de pare-feu Pfsense sous virtuel box.

## Table des matières

## Chapitre 1 : présentation de l'organisme d'accueil.



## Chapitre 2: Généralité sur la sécurité dans les réseaux informatique

## Chapitre 3:les pare-feu



## Chapitre 4:Réalisations

# Chapitre 1 : Présentation de l’organisme d’accueil

## Introduction

Dans ce chapitre, nous allons présenter l'entreprise dans laquelle nous avons effectué notre stage pour la réalisation de notre projet de fin de cycle, ensuite nous ferons le point sur la problématique posée et la solution proposée.

## 1. Présentation de la SARL Ramdy.

### 1.1. Historique de l'entreprise Ramdy.

La SARL Ramdy (ex Laiterie Djurdjura) est une entreprise privée spécialisées dans la production des produits agroalimentaires, elle a été criée le 01/01/1983. Elle s'est spécialisée dans la production des yaourts, crèmes desserts, et les fromages frais et fondus. Le 15 Octobre 2001, le groupe français Danone s'est associé avec la laiterie Djurdjura pour les activités yaourts, pâtes fraiches et desserts. Depuis, l'activité de la laiterie Djurdjura s'est consacrée à la production des fromages fondus, aux pâtes molles (camembert) et au lait pasteurisé.

Deux années plus tard, elle s'est implantée dans une nouvelle unité située en pleine cœur de la zone d'activités Taharacht (Akbou) triplant ainsi sa capacité de production en fromage fondus. Dans le souci de répondre à une demande croissante du consommateur, la laiterie s'est équipée d'un matériel hautement performant dont une nouvelle conditionneuse de 220

PS/mn, et une ligne complète du fromage barre.

En Juin 2004, la SARL laiterie Djurdjura a changé de raison sociale pour devenir SARL Ramdy.

Aujourd'hui, les produits laitiers Djurdjura s'affichent sous la nouvelle dénomination "Ramdy".

En Octobre 2009, la SARL Ramdy a repris la production des yaourts et crèmes desserts [1].


**Figure 1.1 :** le panneau publicitaire d'entreprise ramdy

### 1.2. Situation géographique

La société Ramdy est implantée comme le montre la Figure 01 :

• Dans une zone industrielle, véritable carrefour économique de la wilaya de Bejaia, de quelques50 unités de production agroalimentaire et en cours d'extension.

• A 2 Km d'une grande agglomération.

• A quelques centaines de mètre de la voie ferrée.

• A 60 Km de Bejaia, chef-lieu de la région et pôle économique important en Algérie dotée d'un port à fort trafic et d'un aéroport international.

• A 170 Km à l'est de la capitale Alger [1].


**Figure 1.2 :** Carte géographique de l'entreprise RAMDY.

Ramdy emploie 365 personnes, 46 d'entre eux sont des cadres, 139 des agents de maîtrise et le reste (173) sont des agents d'exécution. Ce personnel qualifié est reparti dans les différents services de l'entreprise qui sont donnés dans l'organigramme de la figure 1.2 [1].

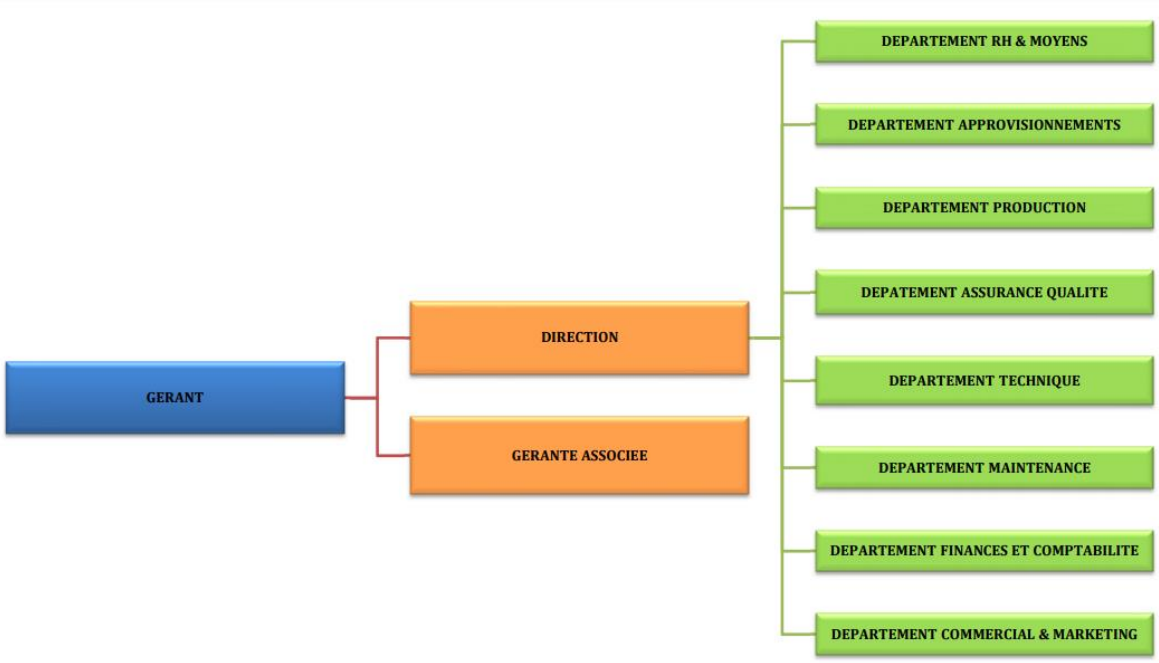



**Figure 1.3** : Organigramme de l'entreprise RAMDY.

### 1.3. Les services de l'entreprise [1].

L'entreprise RAMDY s'organise et se compose de :

- **Direction générale:** Qui assure la bonne gestion de l'entreprise et supervise tout son effectif.
- **Département des ressources humaines et moyens :** Elle regroupe le service personnel, le service hygiène, gestion et paie.
- **Département approvisionnements :** Il s'occupe de l'approvisionnement en matières première, et tous les autres produits nécessaires à l'activité de l'entreprise, ce service est devisé en deux sections : achat et gestion des stocks.
- **Département finance et comptabilité :** Il rassemble trois fonctions complémentaires qui sont : fonction financière, fonction comptabilité générale, et la fonction analytique.
- **Département maintenance:** Il veille à ce que les équipements de production soient en bon état de marche afin de garantir une durée de vie maximale.
- **Département commercial et Marketing :** Ce service est chargé de commercialiser les produits, planifier les ventes, prospecter le marché national. Il se compose de trois sections : section vente ; section recouvrement ; section réception.

- **Département production :** Il est considéré le plus important dans l'entreprise, il s'occupe de la production de fromage et du yaourt.
- **Département assurance et qualité :** elle assure le suivi permanent et continuel de processus de production sous la supervision du laboratoire central qui suit la qualité microbiologique des produits
- **Département technique :** est chargé de manager l'ensemble de l'activité technique de l'entreprise. Sa mission et de partager entre avant-vente, développement et après-vente. Il peut aussi animer, gérer une équipe de consultants techniques et entretenir les relations avec les partenaires.
- **Service informatique**

C'est un service qui appartient au service responsable organisation et TIC. Ses principales fonctions sont :

- Le suivi des applications de gestion.
- La maintenance du parc informatique de l'entreprise.
- Audit et amélioration du système d'information.
- Sauvegarde et contrôle des données de l'entreprise.
- Le développement de nouvelles applications aux différentes structures.

## 1.4. L'objectif de l'entreprise [1].

L'objectif principal de la SARL Ramdy est d'améliorer les ventes sur le temps par rapport à la concurrence et assurer et satisfaire les besoins du consommateur, sa stratégie vise le développement de l'extension du marché afin d'avoir une importante part de ce dernier.

Le rôle de l'entreprise Ramdy ne se limite pas à la production et à la satisfaction des besoins du marché en terme de produits mais elle vise aussi à innover c'est-à-dire proposer de nouveaux produits et participer aux progrès économique et à la concurrence.

Outre que les objectifs principaux l'organisme mit au point les objectifs suivants dans le but de contribuer à la croissance de l'économie du payé : [1]

- Améliorer la qualité de ses produits par rapport à ceux de ses concurrents.
- Atteindre une importante part du marché.

- Satisfaire la demande du marché et fidéliser ses clients.
- Assurer la croissance de l'entreprise.
- Réduire le taux de chômage en recrutant plus de travailleurs.
- Améliorer les conditions de travail.
- Répondre aux attentes des salariés et les former à la nouvelle technologie.
- Lancer de nouveaux produits sur le marché.
- Etablir de nouveaux contrats avec de nouveaux clients.
- Motiver et sensibiliser l'ensemble du personnel.
- Gérer méthodiquement les relations interne (salariés / administration) et externe (fournisseurs / clients).

## 2. Problématique :

De nombreuses difficultés sont rencontrées lors de l'utilisation de la connexion internet au sein de l'entreprise Ramdy parmi lesquelles : Le problème de la gestion de la connexion internet pour des alias (les gérants, les adjoints et les assistants) de réseau local et le problème de sécuriser le LAN de l'extérieur.

## 3. Objectif :

L'objectif de notre travail au sein de l'entreprise Ramdy repose sur :

- Accès illimité de la connexion internet pour les gérants.
- Accès illimité de la connexion pour les adjoints sauf aux réseaux sociaux.
- Accès interdit pour les assistants sauf a des horaires de pose (12 :00-13 :00) et (16 :00-16 :30).
- Sécuriser le réseau local de l'entreprise ouvert sur l'extérieur

## 4. Solution proposée.

Dans l'optique de trouver une solution adéquate à la problématique ainsi posée, nous proposons de faire une installation et une configuration de pare feux.

Ainsi, notre projet consiste à mettre en place une architecture sécurisée pour le réseau LAN de l'entreprise RAMDY.

L'objectif de ce projet dans lequel s'intègre notre travail est de pouvoir gérer la gestion de la connexion internet pour les alias de réseau local.

**Conclusion**

Dans ce chapitre, nous avons présenté les structures de la SARL Ramdy, ainsi que la problématique traitée dans ce mémoire. Le chapitre suivant sera sur les généralités de la

Sécurité informatique et les réseaux informatiques.

# CHAPITRE 2

# Généralités sur la sécurité dans les réseaux informatiques

## Introduction

Les réseaux informatiques de nos jours sont devenus indispensables pratiquement dans tous les domaines de la vie : banques, assurance, santé, administration, transport, …

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

Un système d'information qui néglige la protection de ses données et de ses communications peut avoir des grands risques, ainsi que la société qui l'utilise. C'est la raison pour laquelle la sécurité informatique s'occupe de toute protection

L'objectif de ce chapitre est de présenter les concepts de base liés aux réseaux informatiques et la sécurité informatique. Ces notions formeront la base nécessaire à notre contribution.

## 1. Généralités sur le réseau informatique.

### 1.1. Définition de réseau informatique.

Un réseau informatique est un ensemble d'équipements interconnectés pouvant communiquer (ou échanger des informations). Il a pour but de transmettre des informations d'un équipement ordinateur à un autre [3].

### 1.2. Classification des réseaux.

Les caractéristiques permettant de différencier les familles de réseaux portent sur :

- La distance
- Le mode de transmission de données.

On peut classifier les réseaux en cinq types comme montre la figure 2.1en fonction de la distance [3].

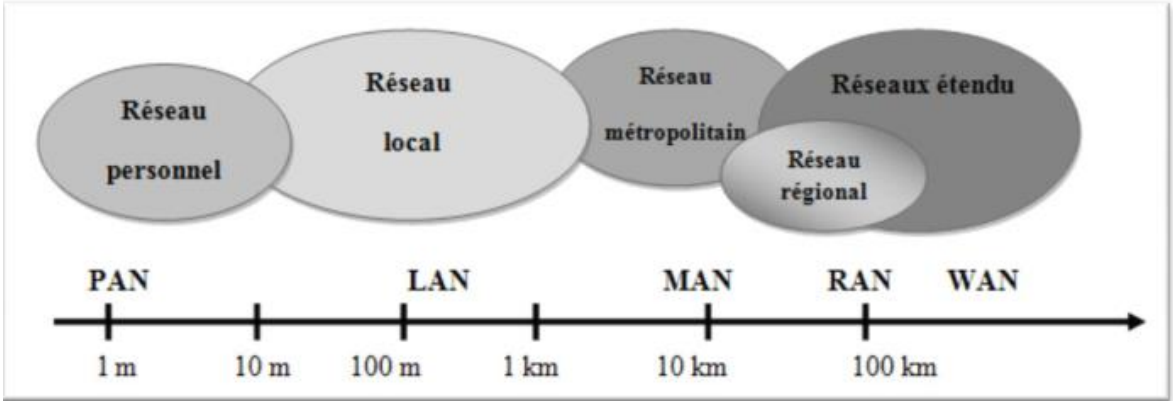



**Figure 2.1 :** Les types de réseaux.

A. **Les réseaux PAN :** Les réseaux personnels, ou PAN (Personale Area Network), interconnectent sur quelques mètres des équipements personnels tels que les portables, d'un même utilisateur

B. **Les réseaux LAN :** Local Area Network ou réseau local, permettent de connecter deux à plusieurs centaines de machines à l'intérieure d'une même enceinte. Il s'agit de la plupart des réseaux informatiques présents dans les entreprises.

C. **Les réseaux MAN :** Métropolitain Area Network, il s'agit d'un réseau dont la couverture s'étale à une ville. Le principe est de relier les différents réseaux locaux mais les normes des transmissions sont différentes. Un MAN est une série de réseaux locaux interconnectés à l'échelle d'une ville.

D. **Les réseaux RAN :** Les réseaux régionaux, ou RAN (Régional Area Network), ont pour objectif de couvrir une large surface géographique. Dans le cas des réseaux sans fil, les RAN peuvent avoir une cinquantaine de kilomètres de rayon, ce qui permet à partir d'une seule antenne, de connecter un très grand nombre d'utilisateurs.

E. **Les réseaux WAN :** Wide Area Network ou réseau de grande taille, interconnecte des réseaux MAN pour assurer une couverture et une interconnexion au niveau d'un pays, voire à travers le monde. Ce type de réseau utilise les satellites pour certaines

interconnexions. Le WAN le plus célèbre est le réseau public Internet, dont le nom provient de cette qualité : Inter Networking, ou interconnexion de réseau.

**1.3. Topologies des réseaux.**

Une topologie caractérise la façon dont les différents équipements réseaux sont positionnelles unes par rapport aux autres. On distingue :

- La topologie physique, relative au plan du réseau.
- La topologie logique précise la façon dont les informations circulent au plus bas niveau [4].

**1.3.1. Topologies physiques :**

A. **En bus :** La topologie en bus (support linéaire) comme le montre la figure suivante repose sur un câblage, sur lequel viennent se connecter des nœuds (postes de travail, équipements d'interconnexion, périphériques). Il s'agit d'un support multipoints. Le câble est l'unique élément matériel constituant le réseau et seuls les nœuds génèrent les signaux. La topologie en bus ne nécessite pas une grande quantité de câbles ni de point centraux, par contre son inconvénient majeur est dû au fait que si le bus est coupé, les stations ne pourront pas s'échanger des informations sur le réseau.

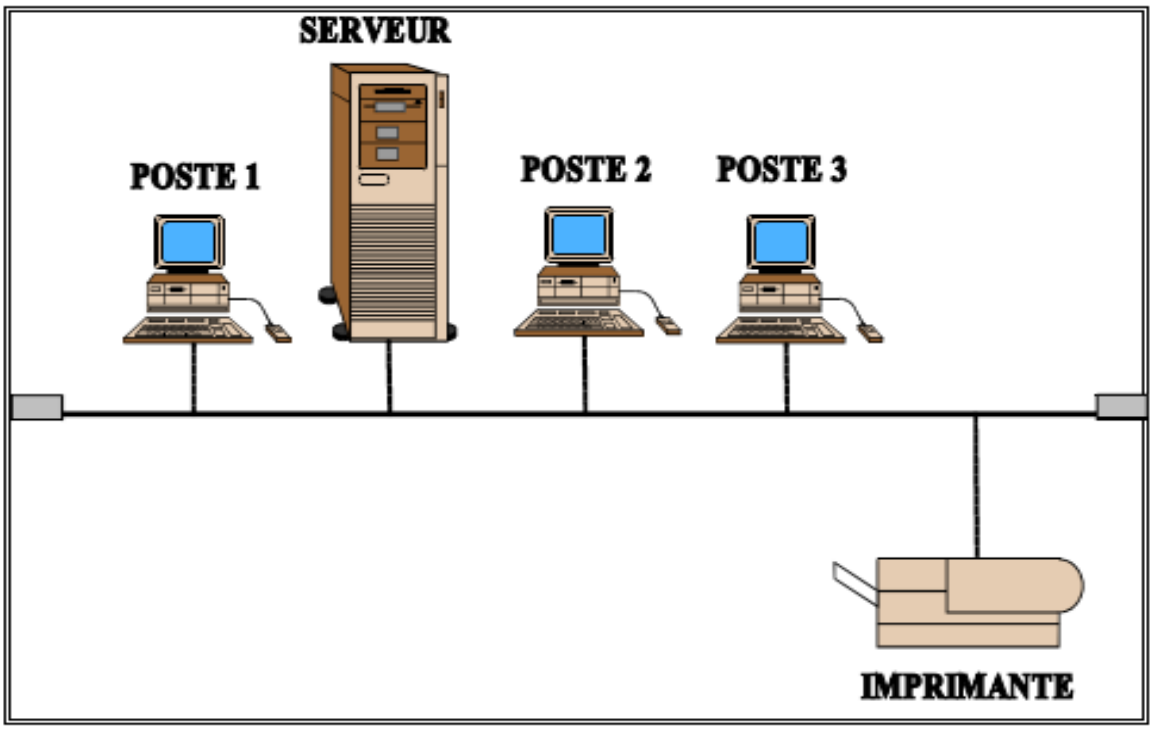



**Figure 2.2** : La topologie en Bus

B. **En étoile :** La topologie en étoile repose, quant à elle, sur des matériels actifs. Un matériel actif remet en forme les signaux et les régénère. Ces points centraux sont

appelés des concentrateurs (hubs). Il est possible de créer une structure hiérarchique en constituant un nombre limité de niveaux. La figure 2.3 illustre une topologie en étoile, dans ce type de topologie une panne ne touche qu'une seule branche (sauf si c'est le point central qui est touché).

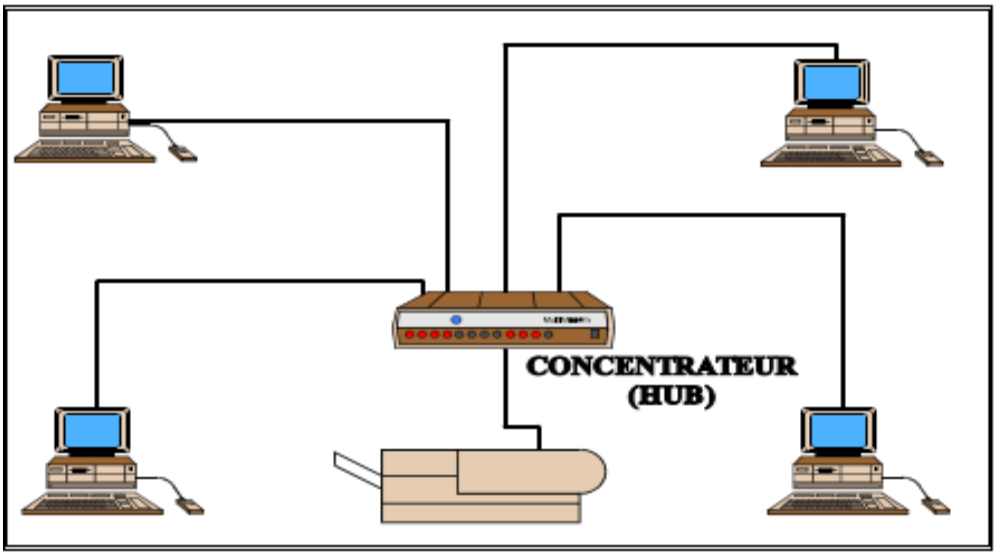



**Figure 2.3 :** La topologie en étoile**.**

C. **La topologie en anneau :** Cette topologie repose sur une boucle fermée, en anneau (ring), constituée de liaisons point à point entre périphériques. Les trames transitent par chaque nœud qui se comporte comme un répéteur (élément actif).

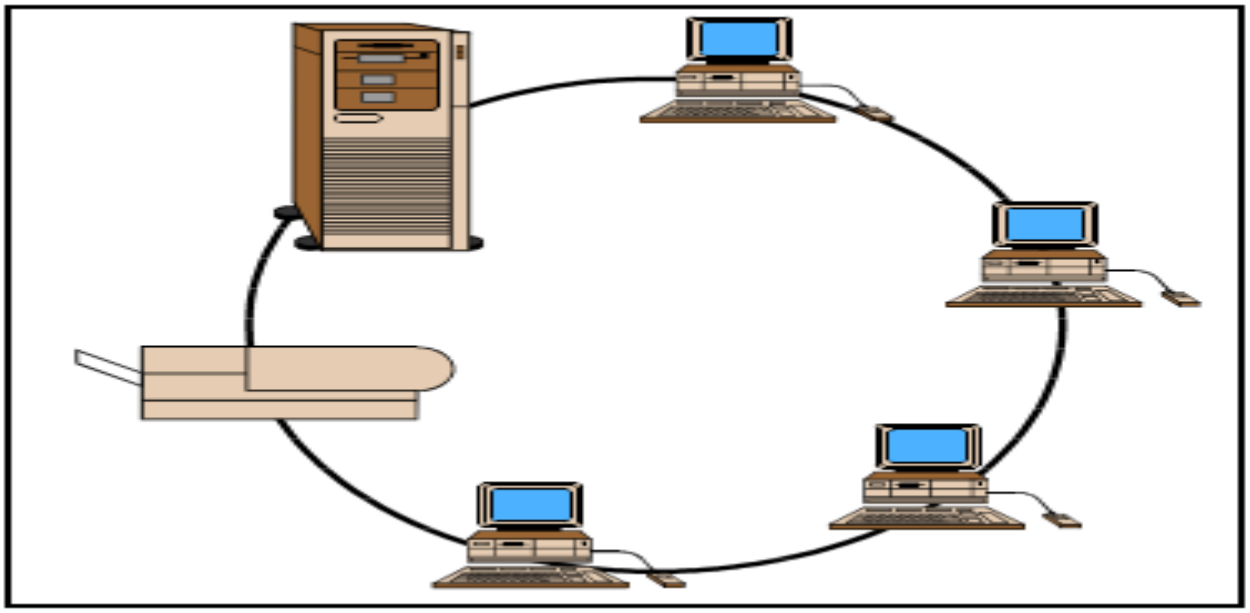


**Figure 2.4:** Architecture en anneau.

## 1.4. Les modèles de communication d'un réseau informatique:

Un réseau informatique permet de partager des données et fichiers ou des périphériques (imprimante, sauvegarde, modem, scanner, ...) entre plusieurs ordinateurs.

La transmission d'information entre deux programmes informatiques sur deux machines différentes passe par deux modèles:

- Le modèle OSI
- Le modèle TCP/IP.

Ces deux normes permettent à chaque partie de la communication de dialoguer suivant différentes couches. Chaque couche doit envoyer un message compréhensible par le reçoit le message.

### 1.4.1. Le modèle OSI (Open System InterConnect)

Le modèle OSI a été utilisé pour concevoir les réseaux ARPANET qui est le premier réseau à transfert de paquets développé aux États-Unis par la DARPA. Normalisé par ISO (International Standard Organisation), le modèle OSI est le standard en matière de normalisation de tous les systèmes ouverts.

Le modèle OSI présente une structure en couche. Chaque couche fournit des services
Directement à la couche supérieure
Les concepts architecturaux utilisés pour décrire le modèle de référence à sept couches,

Proposé par l'ISO, sont décrits dans la norme ISO 7498-1. La figure 2.5 schématise

Le fonctionnement du modèle OSI. [5]

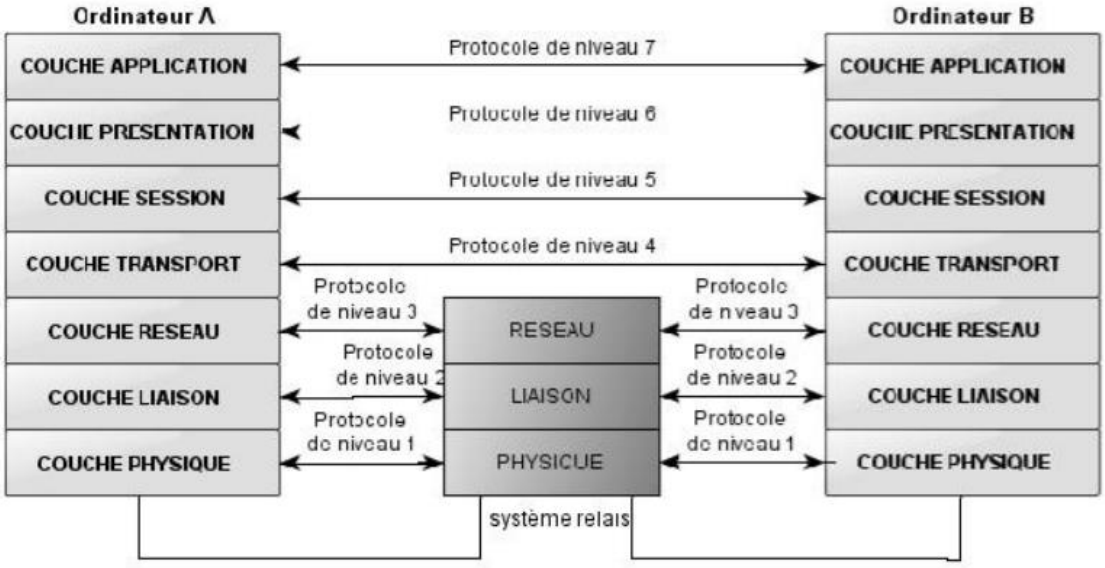



**Figure 2.5 :** Le modèle OSI.

- **La couche Physique :** Elle assure le transfert des bits sur le support de transmission. À cet effet, elle définit les spécifications mécaniques (connecteur), électriques (niveau de tension), et les spécifications fonctionnelles des éléments de raccordement nécessaires à l'établissement, au maintien et à la libération de la ligne.
- **La couche Liaison :** Elle assure un service de transfert de blocs de données (trames) entre deux systèmes adjacents en assurant le contrôle, l'établissement, le maintien et la libération du lien logique entre les entités. Elle permet en outre, de détecter les erreurs incohérentes aux supports physiques

- **La couche Réseau:** La couche réseau doit permettre d'acheminer correctement les paquets d'informations jusqu'à l'utilisateur final. Pour aller de l'émetteur au récepteur, il faut passer par des nœuds de transfert intermédiaire interconnectant deux ou plusieurs réseaux. Cette couche assure trois fonctionnalités principales :
    - Le contrôle de flux,
    - Le routage
    - L'adressage.

- **La couche Transport :** Elle est la couche pivot du modèle OSI. Elle assure le contrôle du transfert de bout en bout lors du transfert des informations (messages) entre les deux extrémités communicantes.

Elle est la dernière couche de contrôle des informations, elle doit assurer aux couches supérieures un transfert fiable quelle que soit la qualité du sous-réseau de transport utilisé.

- **La couche Session :** Elle gère l'échange de données entre les applications distantes. La fonction essentielle de cette couche est la synchronisation des échanges et la définition de points de reprise.
- **La couche Présentation :** Cette couche assure la mise en forme des données pour qu'elles soient accessibles à l'utilisateur. Elle effectue les fonctions de codage, compression, cryptage, décryptage, etc.
- **La couche Application :** Cette couche est le point de contact entre l'utilisateur et le réseau, c'est donc elle qui apporte à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichiers, la messagerie, etc.

### 1.4.2. Le modèle TCP / IP :

L'architecture TCP/IP porte le nom des protocoles principaux qui la constituent, à savoir TCP (Transmission Control Protocol) et IP (Internet Protocol), on l'a définie dans les années1960 pour le réseau ARPANET. Elle s'est développée avec le succès d'Internet. [6]

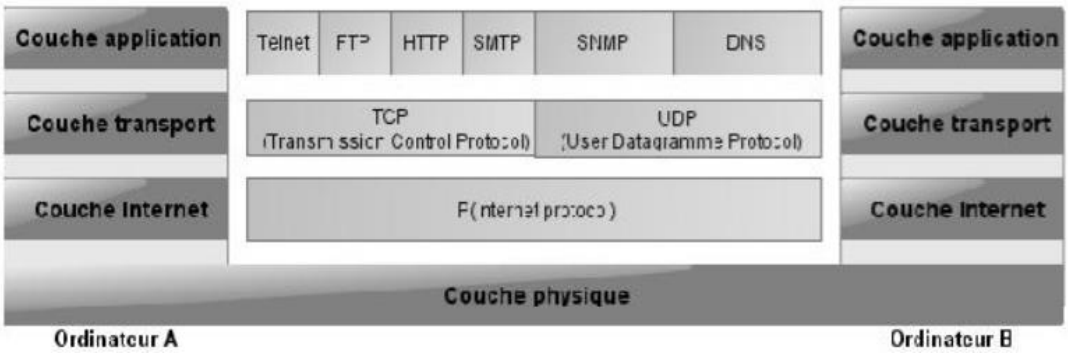



**Figure 2.6 :** Le modèle TCP/IP.

- **La couche Physique :** Aucune caractéristique particulière n'est requise pour l'infrastructure du ou des réseaux physiques traversés. La couche physique est donc quelconque.

- **La couche Internet :** Elle assure la communication entre les réseaux grâce au protocole IP. On utilise la commutation de paquets de type datagramme. Le protocole IP gère les datagrammes, il les achemine jusqu'à leur destinataire, IP définit un service sans garantie de délai ou de fiabilité de communication.

- **La couche Transport :** Elle définit deux protocoles de transport, un en mode connecté TCP, et un autre en mode non connecté UDP (User Datagramme Protocol). Le protocole TCP est destiné à fiabiliser les échanges avec le contrôle de flux, le contrôle d'erreur et le contrôle de séquence entre les deux extrémités. Le protocole UDP est non fiable, il sert aux applications dites temps réel qui nécessite des temps de traitement optimisés telle que la vidéo.

- **La couche Application :** Elle contient tous les protocoles de haut niveau qu'un utilisateur souhaite avoir à sa disposition tels que Telnet (utilitaire permettant l'utilisation de programmes sur des machines distantes via un réseau), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol), HTTP (Hyper Txt Transfer Protocol), et autres.

## 2. Généralités sur la sécurité informatique.

### 2.1. Définition

La sécurité informatique (SI) est l'ensemble des moyens (méthodes, techniques et outils) mis en œuvre pour minimiser la vulnérabilité d'un système contre des menaces accidentelles ou intentionnelles [9].

### 2.2. Les objectifs de la sécurité [9].

La sécurité a pour objectif d'assurer les propriétés suivantes :

- **La Confidentialité** : Assurer que l'information ne soit divulguée ou révélée qu'aux personnes autorisées.
- **L'Authentification** : C'est la propriété qui assure que seules les entités autorisées ont accès au système.
- **L'Intégrité** : Assurer que l'information contenue dans les objets ne soit ni altérée, ni détruite de manière non autorisée.
- **La Disponibilité** : L'accès par un sujet autorisé aux ressources et informations du système doit être toujours possible
- **Non répudiation** : C'est la propriété qui assure la preuve de l'authenticité d'un acte c'est-à-dire que l'auteur d'un acte ne peut denier l'avoir effectué.

### 2.3.Terminologie de la sécurité informatique [9].

La sécurité informatique utilise un vocabulaire bien défini. L'objectif est de mieux comprendre les risques possibles des attaques informatiques. Et évidemment, pour pouvoir mieux s'en défendre par la suite, il est nécessaire de définir certains termes :

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

## 2.4. Les Types d'attaques [8].

Les attaques peuvent à première vue être classées en 2 grandes catégories :

- **Les attaques passives** : consistent à écouter sans modifier les données ou le fonctionnement du réseau. Elles sont généralement indétectables mais une prévention est possible.
- **Les attaques actives** : consistent à modifier des données ou des messages, à s'introduire dans des équipements réseau ou à perturber le bon fonctionnement de ce réseau. Noter qu'une attaque active peut être exécutée sans la capacité d'écoute. De plus, il n'y a généralement pas de prévention possible pour ces attaques, bien qu'elles soient détectables (permettant ainsi une réponse adéquate).

### 2.4.1. Les différentes étapes d'une attaque [8].

La plupart des attaques, de la plus simple à la plus complexe fonctionnent suivant le même schéma :

- **Identification de la cible** : Cette étape est indispensable à toute attaque organisée, elle permet de récolter un maximum de renseignements sur la cible en utilisant des informations publiques et sans engager d'actions hostiles. On peut citer par exemple l'utilisation des bases Whois, l'interrogation des serveurs DNS.
- **Le scanning** : L'objectif est de compléter les informations réunies sur une cible visées, il est ainsi possible d'obtenir les adresses IP utilisées, les services accessibles de même qu'un grand nombre d'informations de topologie détaillée (OS, versions des services, subnet, règles de pare-feu. . .). Il faut noter que certaines techniques de scans particulièrement agressives sont susceptibles de mettre à mal un réseau et entrainer la défaillance de certains systèmes.
- **L'exploitation** : Cette étape permet à partir des informations recueillies d'exploiter les failles identifiées sur les éléments de la cible, que ce soit au niveau protocolaire, des services et applications ou des systèmes d'exploitation présents sur le réseau.
- **La progression** : Il est temps pour l'attaquant de réaliser ce pourquoi il a franchi les précédentes étapes. Le but ultime étant d'élever ses droits vers la root

(administrateur) sur un système afin de pouvoir y faire tout ce qu'il souhaite (inspection de la machine, récupération d'informations, nettoyage des traces,. . .).

### 2.4.2. Quelques attaques courantes [9].

Il existe un grand nombre d'attaques permettant à une personne mal intentionnée de désapproprier des ressources, de les bloquer ou de les modifier. Certaines requièrent plus de compétences que d'autres, en voici quelques-unes :

**- IP spoofing**: Cette attaque est difficile à mettre en œuvre et nécessite une bonne connaissance du protocole TCP, elle consiste, le plus souvent, à se faire passer pour une autre machine en falsifiant son adresse IP de manière à accéder à un serveur ayant une "relation de confiance" avec la machine "soiffée". Cette attaque n'est intéressante que dans la mesure où la machine de confiance dont l'attaquant a pris l'identité peut accéder au serveur cible en tant que root.

**- Le sniffing**: Grace à un logiciel appelé "sniffer", il est possible d'intercepter toutes les trames que notre carte reçoit et qui ne nous sont pas destinées. Si quelqu'un se connecte par Telnet par exemple à ce moment-là, son mot de passe transitant en clair sur le net, il sera aisé de le lire. De même, il est facile de savoir à tout moment quelles pages web regardent les personnes connectées au réseau, les sessions ftp en cours, les mails en envoi ou réception. Une restriction de cette technique est de se situer sur le même réseau que la machine ciblée.

**- Le Dos (Denial of Service)** : Le Dos est une attaque visant à générer des arrêts de service et donc à empêcher le bon fonctionnement d'un système. Cette attaque ne permet pas en elle-même d'avoir accès à des données. En général, le déni de service va exploiter les Faiblesses de l'architecture d'un réseau ou d'un protocole.
Il en existe plusieurs types comme le flooding, le smurf ou le débordement de tampon (buffer-overflow) ;

**- Les programmes cachés ou virus** : Il existe une grande variété de virus. On ne classe cependant pas les virus d'après leurs dégâts mais selon leur mode de propagation et de multiplication. On recense donc les vers (capables de se propager dans le réseau), les troyens (créant des failles dans un système), Les bombes logiques (se lançant suite à un évènement du système (appel d'une primitive, date spéciale).

**- Le scanning (appelé analyseur de réseaux)** : L'objectif est de compléter les informations réunies sur une cible visée, il est ainsi possible d'obtenir les adresses IP utilisées, les services accessibles, de même qu'un grand nombre d'informations de topologie détaillée (OS, versions des services, subnet, règles de firewall. . .).Il faut noter que certaines techniques de scans particulièrement agressives sont susceptibles de mettre à mal un réseau et entraine la défaillance de certains systèmes.

**- L'ingénierie sociale (social engineering)** : Ce n'est pas vraiment une attaque informatique en soit, mais plutôt une méthode qui est basée sur l'utilisation de la force de persuasion et l'exploitation de la naïveté des utilisateurs

**- Le craquage de mots de passe (Brute force)** : Cette technique consiste à essayer plusieurs mots de passe afin de trouver le bon. Elle peut s'effectuer à l'aide d'un dictionnaire des mots de passe les plus courants (et de leur variantes), ou par la méthode de brute force (toutes les combinaisons sont essayées jusqu'à trouver la bonne). Cette technique longue et fastidieuse, souvent peu utilisée à moins de bénéficier de l'appui d'un très grand nombre de machines.

**- Le flood** : un flood consiste à envoyer très rapidement de gros paquets d'informations à une personne. Cette dernière visée ne pourra plus répondre aux requêtes et le modem va donc se déconnecter, c'est cette méthode qui a été employée à grande échelle dans l'attaque des grands sites commerciaux.

## 2.5. Les éléments à sécuriser dans un réseau

Les réseaux sont constitués de divers équipements d'une part et de liens filaires ou non filaires, qui, les relient d'autre part. Toute où partie de ces équipements peuvent

être gérés par des programmes adaptés et plusieurs sortes de données y sont stockées. Certains d'entre elles peuvent être l'objet de transferts selon des protocoles appelés protocole de réseaux. Dans ce cadre, la sécurité concerne celle du matériel, celle des programmes, celle des données et celle des protocoles[9].

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

A. **Matériel** : Mis à part les ordinateurs que les réseaux relient, le matériel inclut aussi, les équipements intermédiaires comme les répéteurs, commutateurs (Switch), routeurs, serveur, modems, firewalls, etc. La limitation d'accès à chaque matériel participe à la sécurité de l'ensemble

B. **Programme** : les programmes incluent les systèmes d'exploitation y compris les pilotes de périphériques ainsi que les logiciels et programmes gérant les différents mécanismes de réseaux. Les services permettant une meilleure gestion à distance et plus d'autonomie, on parle dans ce cas-là de services réseau tels que : DHCP, DNS, FTP, etc.

C. **Données** : On distingue deux sortes de données, celles qui servent au fonctionnement du réseau comme les tables de routage, les bases de données de clients, les fichiers relatifs aux droits d'accès, etc. On trouve aussi des données qui ne sont pas en rapport avec le fonctionnement du réseau tels que : les documents et les archives.

## 2.6. Stratégies de sécurité.

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

1) **Un pare-feu :** est un élément du réseau informatique, logiciel et/ou matériel, qui est aujourd'hui incontournable dans la sécurité de tout système informatique car il permet d'appliquer une politique d'accès aux ressources informatiques. Il a pour principale tâche de contrôler le trafic entre les différentes zones de confiance, en filtrant les flux

de données qui y transitent [10]. Le pare-feu est également intéressant dans le sens où il constitue un point unique (goulot d'étranglement) où l'audit et la sécurité peuvent être imposés. Tous les échanges passeront par lui. Il pourra donner des résumés de trafic, des statistiques sources trafic, ou encore toutes les connexions entre les réseaux.

2) **Zone Démilitarisée [11] :** Si une entreprise doit héberger elle-même un site web public complet avec des serveurs tel qu'un serveur de messagerie, elle pourra envisager l'emploi d'un pare-feu avec deux interfaces (interne et externe) et lui laisser la tâche de créer les règles de traduction qui dirigent le trafic en entrée vers les serveurs appropriés au réseau d'entreprise. Cela peut s'avérer désastreux si un pirate a des vues sur ce réseau. D'où l'idée de recourir à une DMZ (De militarized Zone).

Une DMZ est une interface située entre un réseau connu (réseau interne) et un réseau externe (internet). Une série de règles de connexion configurées sur le pare-feu font de cette interface une zone physiquement isolée entre les deux réseaux. Cette séparation physique permet d'autoriser les accès internet à destination des serveurs placés dans la DMZ et non à ceux destinés au réseau privé (interne).
La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :

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

La DMZ possède donc un niveau de sécurité intermédiaire, mais il n'est pas suffisant pour y stocker des données critiques pour l'entreprise. Il est à noter qu'il est possible de mettre en place des DMZ en interne afin de cloisonner le réseau interne selon différents niveaux de protection et ainsi éviter les intrusions venant de l'intérieur.

3) **La technologie AAA :** Nous vivons dans un monde où presque tout doit être protégé contre une utilisation abusive ou impropre et où rien n'est gratuit. Que vous soyez administrateur système, responsable, ingénieur réseau ou étudiant. Lorsque vous accédez à un réseau, vous êtes toujours confronté aux trois aspects suivants : [12]

• **Authentification(Authentification)** : il s'agit de la vérification de l'identité d'un utilisateur, elle est généralement assurée au moyen d'un secret partagé ou d'un logiciel approuvé (protocole RADIUS).

• **Autorisation (Autorisation)** : Elle intervient à l'issue de l'authentification. Une fois l'utilisateur authentifié, il faut s'assurer qu'il est autorisé à accomplir les actions qu'il demande, tels que l'accès à des fichiers, le droit d'écrire, etc. L'autorisation est gérée au moyen de liste ACL ou des stratégies.

• **Comptabilité (Accounting)** : Elle permet de collecter des informations sur les utilisateurs et les actions qu'ils accomplissent lorsqu'ils sont connectés aux équipements du réseau.

4) **Liste de contrôle d'accès(ACL) :** Les administrateurs réseaux doivent trouver le moyen d'interdire l'accès au réseau à certains utilisateurs tout en permettant aux utilisateurs internes d'accéder aux services nécessaires, les routeurs assurent cette fonction à l'aide des listes de contrôle d'accès. Une ACL est un ensemble de conditions qui est appliqué au trafic circulant via une interface du routeur. Elle indique au routeur les types des paquets à accepter ou à rejeter. Les ACLs permettent de gérer le trafic et de sécuriser l'accès d'un réseau en entrée comme en sortie.

5) **Proxys :** Un proxy, parfois appelé mandataire, c'est un composant logiciel qui se place entre deux autres pour faciliter ou surveiller leurs échanges. Dans le cadre plus précis des réseaux informatiques, un proxy est alors un programme servant d'intermédiaire pour accéder à un autre réseau, généralement internet. Par extension, on appelle aussi proxy un matériel (un serveur par exemple) mis en place pour assurer le fonctionnement de tels services [13].
6) **Les réseaux privés virtuel :** Les réseaux privés virtuels permettent à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination. Grace à un

principe de tunnel (tunneling) dont chaque extrémité est identifiée, les données transitent après avoir été éventuellement chiffrées. Un des grands intérêts des VPN est de réaliser des réseaux privés à moindre coût. En chiffrant les données, tout se passe exactement comme si la connexion se faisait en dehors d'Internet. Il faut par contre tenir compte de la toile, dans le sens où aucune qualité de service n'est garantie.

7) **Systèmes de détection d'intrusion :** Divers raison peuvent conduire un attaquant (pirate) à vouloir s'introduire sur un réseau : défi personnel, espionnage, motivation politique, gain financier ou simplement nuisance. Surveiller le réseau pour détecter les attaques éventuelles relève non seulement du bon sens mais constitue également un impératif pour n'importe quelle entreprise, D'où l'utilisation des systèmes de détection d'intrusion, ou IDS (Instruction Détection System). Par définition un IDS est le système d'alarme du réseau. seul l'IDS permet de savoir qu'un intrus tente d'y accéder. Les sondes de détection d'intrusion constituent le complément d'un pare-feu. Elles permettent d'analyser les actions ou les flux pour y détecter une tentative d'intrusion. Les IDS peuvent être déployés en plusieurs endroits du réseau afin d'augmenter la sécurité, ils sont généralement de deux types :
- Les N-IDS (Network Based Intrusion Detection System), ils assurent la sécurité au niveau du réseau.

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

## Conclusion

Dans ce chapitre, nous avons défini les notions fondamentales dans les réseaux informatiques et les stratégies de sécurité à prendre pour remédier aux attaques. Le prochain chapitre sera consacré aux pare-feu.

# Chapitre 3: Les pare-feu

## Introduction

Toutes les entreprises possédant un réseau local possèdent aussi un accès à Internet. Cette ouverture vers l'extérieur est indispensable et dangereuse en même temps. Pour parer à des attaques, une architecture sécurisée est nécessaire. Pour cela, le cœur d'une telle architecture est basée sur un firewall (pare-feu). Cet outil a pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les tentatives d'intrusion et d'y parer au mieux.

Dans ce chapitre nous présenterons les principales caractéristiques des firewalls, quelques définitions et principes de fonctionnement,

### 1. Définition d'un pare-feu.

Un système permettant de protéger un ordinateur ou un réseau d'ordinateurs de l'intrusion provenant d'un réseau tiers.

Le pare-feu est un système permettant de filtrer les paquets échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseaux suivantes : [2]

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

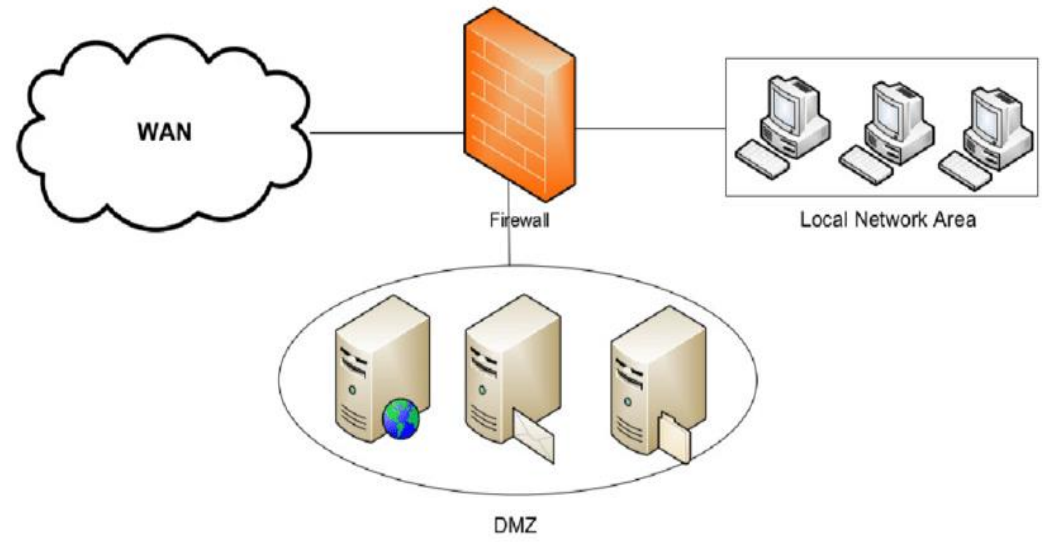



**Figure 3.1 :** Architecture d'un pare-feu

## 2. Principe de fonctionnement d'un pare-feu :

Il existe deux types de pare-feu : [14]

1. **Les filtres de paquets** : Le filtrage du trafic de données se fait au niveau des couches réseau et transport du modèle OSI.
2. **Les passerelles** : Le filtrage est plus fin car il est réalisé au-dessus de la couche réseau.

### 1. Les filtres de paquets. [14]

Certains firewalls sont en fait des routeurs possédant des fonctions de filtrage de paquets. Avec des règles appropriées, l'administrateur réseau peut interdire ou autoriser un certain nombre de services ainsi que bloquer les accès aux équipements de son site, tout en permettant à ses machines l'accès aux services de l'Internet. Le routeur doit être configuré avec une liste d'accès.

Une liste d'accès définit les conditions pour qu'un paquet puisse franchir un routeur. Les informations contenues dans ces listes portent :

- Sur le numéro du protocole de niveau 3, les adresses IP, les numéros de ports...
- D’autres informations dans le paquet comme les drapeaux TCP
- Le type de la règle, c'est-à-dire soit une autorisation soit un refus de faire traverser le paquet.

Quand un paquet arrive sur le routeur, la liste est parcourue et le traitement du paquet est lié à la première condition rencontrée qui correspond au paquet.

Dans ce premier exemple, on suppose qu'une société dispose d'un réseau interne et d'un serveur web. Les machines doivent être inaccessibles de l'extérieur, sauf le serveur web qui peut être consulté par n'importe quel équipement connecté à l'Internet. La liste d'accès n°1 doit servir pour interdire toutes les connexions venant de l'extérieur, sauf vers le port 80 du serveur web.

| Règles | Action | Protocole | Source | | Destination | |
|---|---|---|---|---|---|---|
| | | | Adresse | Port | Adresse | Port |
| 1 | Autorise | TCP | * | * | Serveur | 80 |
| 2 | Autorise | TCP | Serveur | 80 | * | * |
| 3 | Interdit | * | * | * | * | * |

**Tableau 1 :** Liste d'accès n°1.

La règle 1 indique que le routeur laissera passer les paquets destinés à la machine serveur pour le port 80. L'adresse source (notée *) que contient ce paquet est indéterminée puisque n'importe quelle machine connectée au réseau Internet est autorisée à accéder au service web. Le numéro de port source est également indéterminé car celui-ci est choisi dynamiquement par le client au moment de l'ouverture de connexion.

La règle 2 est symétrique de la première. Elle autorise le routeur à laisser passer les réponses du serveur au client distant.

La règle 3 empêche tout autre paquet de traverser le routeur. Elle permet d'appliquer la philosophie : tout ce qui n'est pas explicitement autorisé est interdit.

Maintenant, pour que les utilisateurs du site soient autorisés à consulter les pages web sur Internet, il suffit de rajouter deux règles :

| Règles | Action | Protocole | Source | | Destination | |
|---|---|---|---|---|---|---|
| | | | Adresse | Port | Adresse | Port |
| 1 | Autorise | TCP | * | * | Serveur | 80 |
| 2 | Autorise | TCP | Serveur | 80 | * | * |
| 3 | Autorise | TCP | {site} | * | * | 80 |
| 4 | Autorise | TCP | * | 80 | {site} | * |
| 5 | Interdit | * | * | * | * | * |

**Tableau 2 :** Liste d'accès n°2

Ces deux nouvelles règles (3 et 4) permettent aux équipements internes d'émettre vers l'extérieur des paquets ayant comme port de destination le numéro 80 et de recevoir de l'extérieur des paquets ayant pour source le port 80. L'ensemble des machines du site (représentées par {site}) peuvent être données en listant les numéros de réseaux de site.

### 2. Les passerelles [14].

Il existe deux types de passerelles :

#### A. Passerelles de niveau applicatif (proxy)

Les passerelles applicatives sont des serveurs effectuant un filtrage plus ou moins fin sur les données échangées entre deux réseaux pour un service TCP/IP particulier. Ces passerelles sont situées entre un client du réseau interne et un serveur du réseau externe.

Pour chaque communication, deux connexions sont donc à considérer : client/passerelle et passerelle/serveur.

Les proxies filtrent en fonction du service demandé : Telnet, ftp, smtp, http...

- Le client se connecte au serveur proxy et demande l'accès au serveur distant.
- Le serveur proxy vérifie l'adresse du client, authentifie le client à l'aide d'un serveur d'authentification (type RADIUS) et l'autorise à se connecter sur le serveur.

- Le serveur proxy se connecte sur le serveur distant et relaie les données entre les deux connexions.

#### B. Passerelles de niveau circuit

Les passerelles de niveau circuit filtrent au niveau transport. L'avantage est qu'elles sont communes à toutes les applications TCP/IP.

- Le client établit une connexion TCP avec la passerelle en demandant de communiquer avec le serveur.
- La passerelle peut vérifier l'adresse IP du client et elle va :

  - Autoriser une connexion sur un port pour une durée maximale fixée.
  - N'autoriser la réutilisation d'un même port qu'après un certain délai.
  - Authentifier un terminal.

- La passerelle se connecte au serveur et relaie les données entre les deux connexions TCP.

### 3. Les différentes catégories de pare-feu [14].

Les pare-feu sont le plus vieil équipement de sécurité et comme tel, ils ont été soumis à de nombreuses évolutions. Suivant la génération des pare-feu ou leur rôle précis, on peut les classer en différentes catégories.

#### 3.1. Pare-feu sans état (stateless firewall)

C'est le plus vieux dispositif de filtrage réseau, introduit sur les routeurs. Il regarde chaque paquet indépendamment des autres et le compare à une liste de règles préconfigurées. La configuration de ces dispositifs est souvent complexe et l'absence de prise en compte des machines à états des protocoles réseaux ne permet pas d'obtenir une finesse du filtrage très évoluée. Ces pare-feu ont donc tendance à tomber en désuétude mais restent présents sur certains routeurs ou systèmes d'exploitation

### 3.2. Pare-feu à états (stateful firewall)

Certains protocoles dits « à états » comme TCP introduisent une notion de connexion. Les pare-feu à états vérifient la conformité des paquets à une connexion en cours. C'est à dire qu'ils vérifient que chaque paquet d'une connexion est bien la suite du précédent paquet et la réponse à un paquet dans l'autre sens.

### 3.3.Pare-feu applicatif

Dernière mouture de pare-feu, ils vérifient la complète conformité du paquet à un protocole attendu. Par exemple, ce type de pare-feu permet de vérifier que seul du HTTP passe par le port TCP 80. Ce traitement est très gourmand en temps de calcul dès que le débit devient très important; il est justifié par le fait que de plus en plus de protocoles réseaux utilisent un tunnel TCP pour contourner le filtrage par ports.

Une autre raison de l'inspection applicative est l'ouverture de ports dynamique. Certains protocoles comme le fameux FTP en mode actif échangent entre le client et le serveur des adresses IP ou des ports TCP/UDP. Ces protocoles sont dit "à contenu sale" ou "dirtypayload" car ils échangent au niveau applicatif (FTP) des informations du niveau IP (échange d'adresses) ou du niveau TCP (échange de ports). Ce qui transgresse le principe de la séparation des Couches réseaux. Pour cette raison, les protocoles "à contenu sale" passent difficilement voire pas du tout, les règles de NAT dynamiques, à moins qu'une inspection applicative ne soit faite sur ce protocole. Quelques protocoles "à contenus sale": FTP en mode passif, H323, les protocoles faisant de l'IRC-DCC, les protocoles de gestion de réseau (DNS, certains messages icmp, trace route) Chaque type de pare-feu sait inspecter un nombre limité d'applications. Chaque application est gérée par un module différent pour pouvoir les activer ou les désactiver. La terminologie pour le concept de module est différente pour chaque type pare-feu: Conntrack sur Linux Netfilter, CBACsur Cisco IOS, Fixup puis inspect sur Cisco PIX, ApplicationLayerGateway sur Proventia M, Predefined Services sur JuniperScreenOS...

### 3.4.Pare-feu authentifiant

Un pare-feu authentifiant réalise l'authentification des connexions passant à travers le filtre IP. L'administrateur peut ainsi définir les règles de filtrage par utilisateur et non plus par IP, et suivre l'activité réseau par utilisateur. Plusieurs méthodes différentes existent qui reposent sur des associations entre IP et utilisateurs réalisées par des moyens variés. On peut par exemple

citer  Une méthode est l'authentification connexion par connexion, réalisée par exemple par la suite NuFW, qui permet d'authentifier également sur des machines multiutilisateurs

### 3.5.Pare-feu personnel

Les pare-feu personnels, généralement installés sur une machine de travail, agissent comme un pare-feu à états. Bien souvent, ils vérifient aussi quel programme est à l'origine des données. Le but est de lutter contre les virus informatiques et les logiciels espions.

## Conclusion

Dans ce chapitre, nous avons présenté le firewall et nous avons décrit ses différentes fonctionnalités, et ses déférentes catégories. Le chapitre suivant sera consacré à la mise en œuvre de la solution proposée

# Chapitre 4 : Réalisation

## Introduction

Dans ce chapitre, nous décrirons les outils utilisés, ainsi que les principales étapes de l'installation et configuration de parefeu pfsense.

# 1. Description de l'environnement de travail

### 1.1. Virtual Box.

C'est un logiciel de virtualisation de système d'exploitation qui permet de créer un ou plusieurs ordinateurs virtuels dans lesquels s'installent d'autres systèmes d'exploitation (systèmes invités), et de faire fonctionner plus d'un système d'exploitation en même temps en toute sécurité

La figure 4.1 présente l'interface d'accueil de virtuel box [16] :

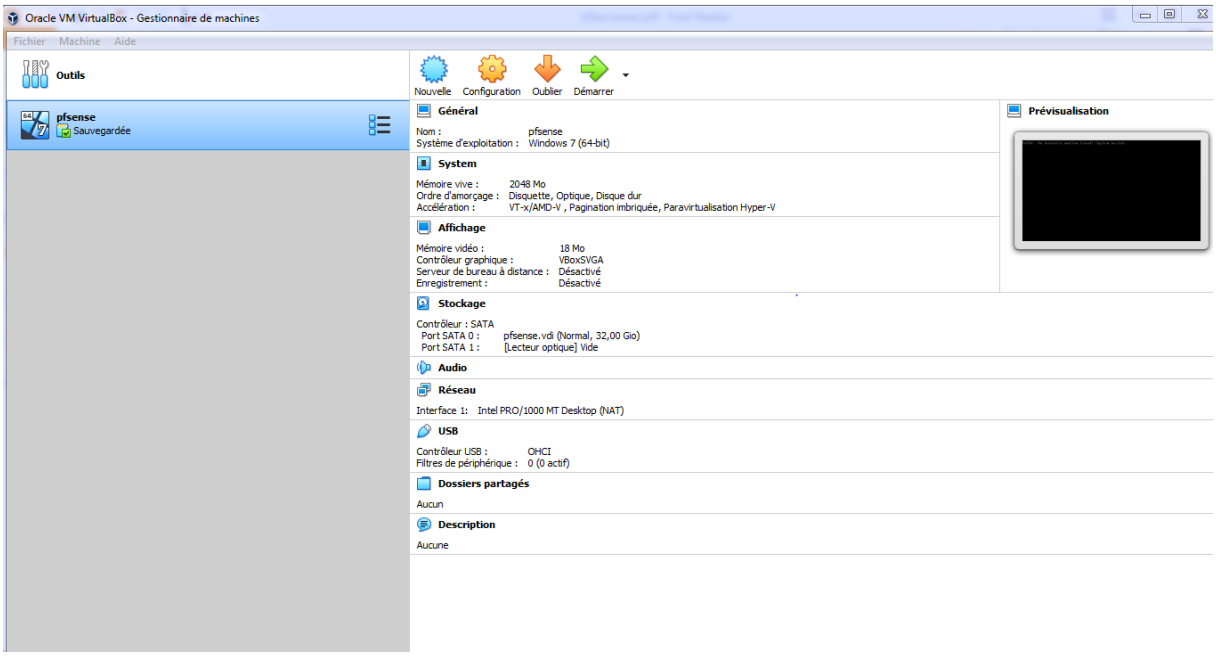



**Figure 4.1** : La page d'accueil de virtuel box.

**1.2. Présentation de PfSense** [15].

PfSense (distribution logicielle), ou ≪PacketFilterSense≫ est un routeur / pare-feu open source basé sur Free BSD. Il date de 2004 à partir d'un fork par Chris Buechler et Scott Ulrich. PfSense peut être installé sur un simple ordinateur personnel comme sur un serveur Basé sur PF (packetfilter), il est réputé pour sa fiabilité. Après une installation en mode console, il s'administre ensuite simplement depuis une interface web.
Les avantages principaux de Pfsense sont les suivants :

- Il est adapté pour une utilisation en tant que pare-feu et routeur.
- Il comprend toutes les fonctionnalités des pare-feu coûteux commercialement.
- Il offre des options de firewalling /routage plus évolué qu'IPCOP.
- Il permet d'intégrer de nouveaux services tels que l'installation d'un portail captif, la mise en place d'un VPN, DHCP et bien d'autres.
- Simplicité de l'activation / désactivation des modules de filtrage,

## 2. Installation et configuration de pfsense.

### 2.1. Instalation de pfsense

- **Création d'une machine virtuelle.**

On crée une Machine Virtuelle sous Virtuel box avec les spécifications suivantes :

- Premièrement, on choisit un nom pour la machine client, puis nous cliquons sur «suivant ». Voir la Figure 4.2

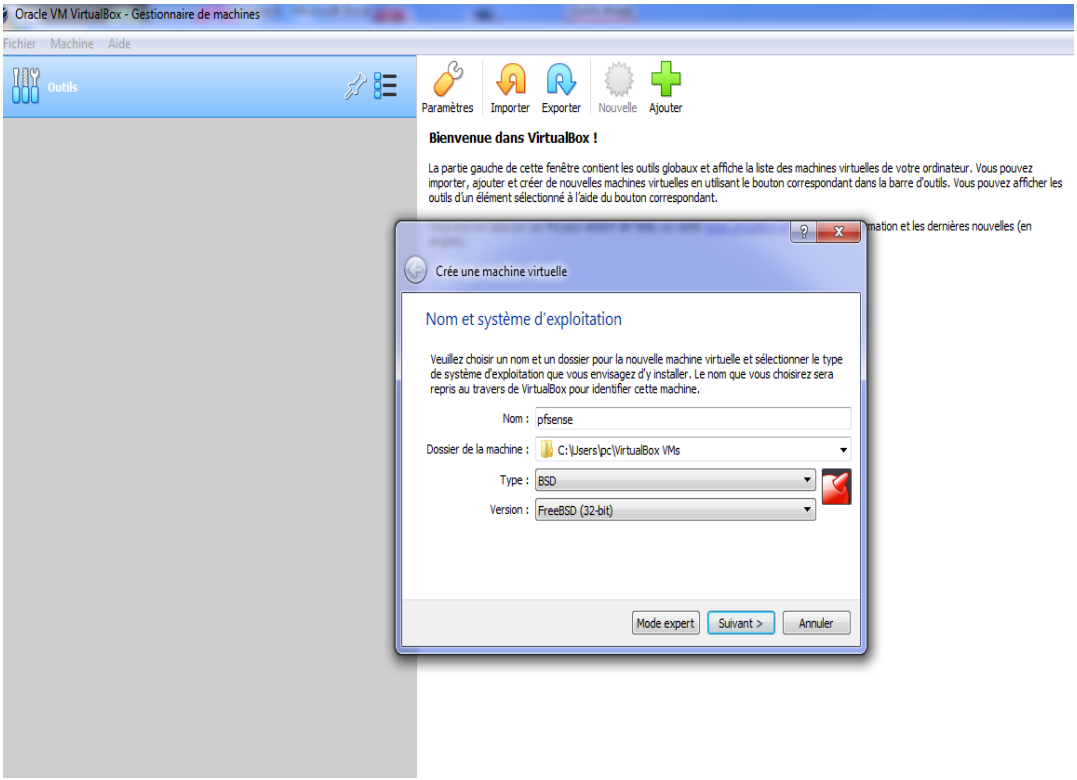



**Figure 4.2** : Création de machine virtuelle.

- Dans la seconde étape, on donne une taille de la mémoire pour la machine en méga-Octets (on a choisi 1024 MO). Voir la figure 4.3

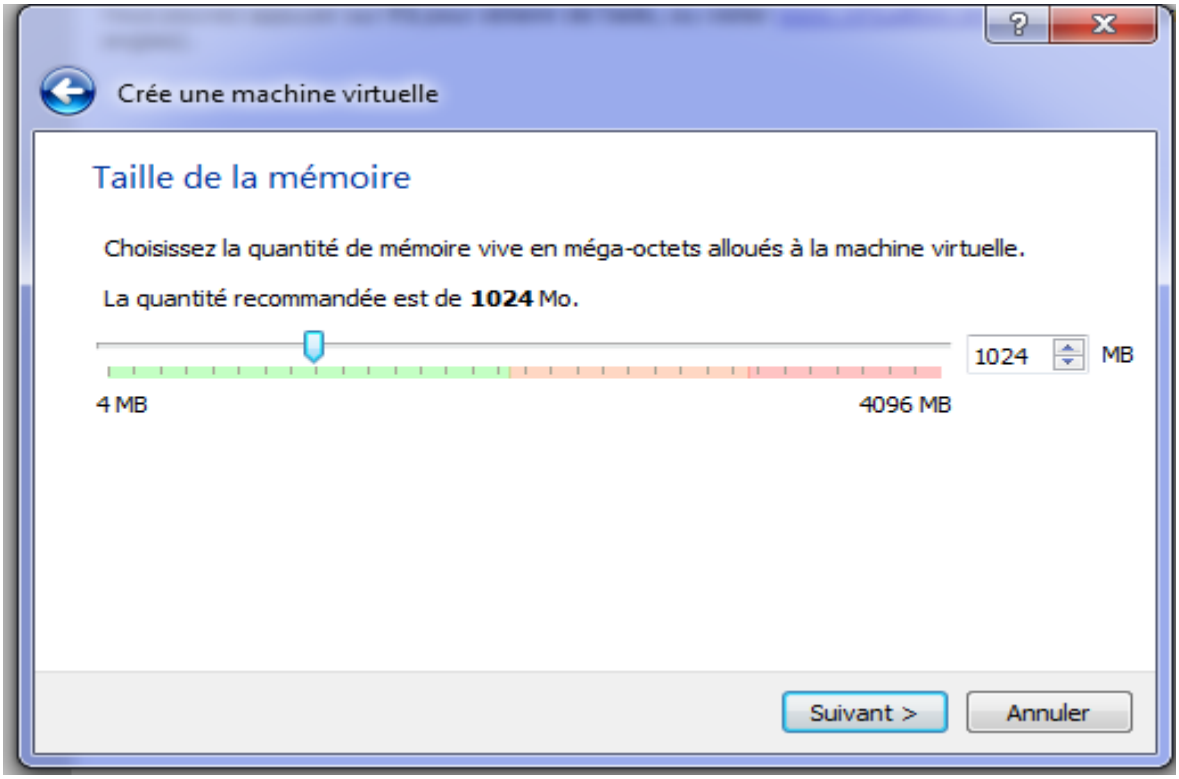



**Figure 4.3** : La taille de la mémoire allouée pour la machine.

- Après avoir vérifié tous les paramètres dans la fenêtre de Virtual Box, on fera lancer notre machine et pour cela on clique sur « démarrer ». Voir la figure 4.4

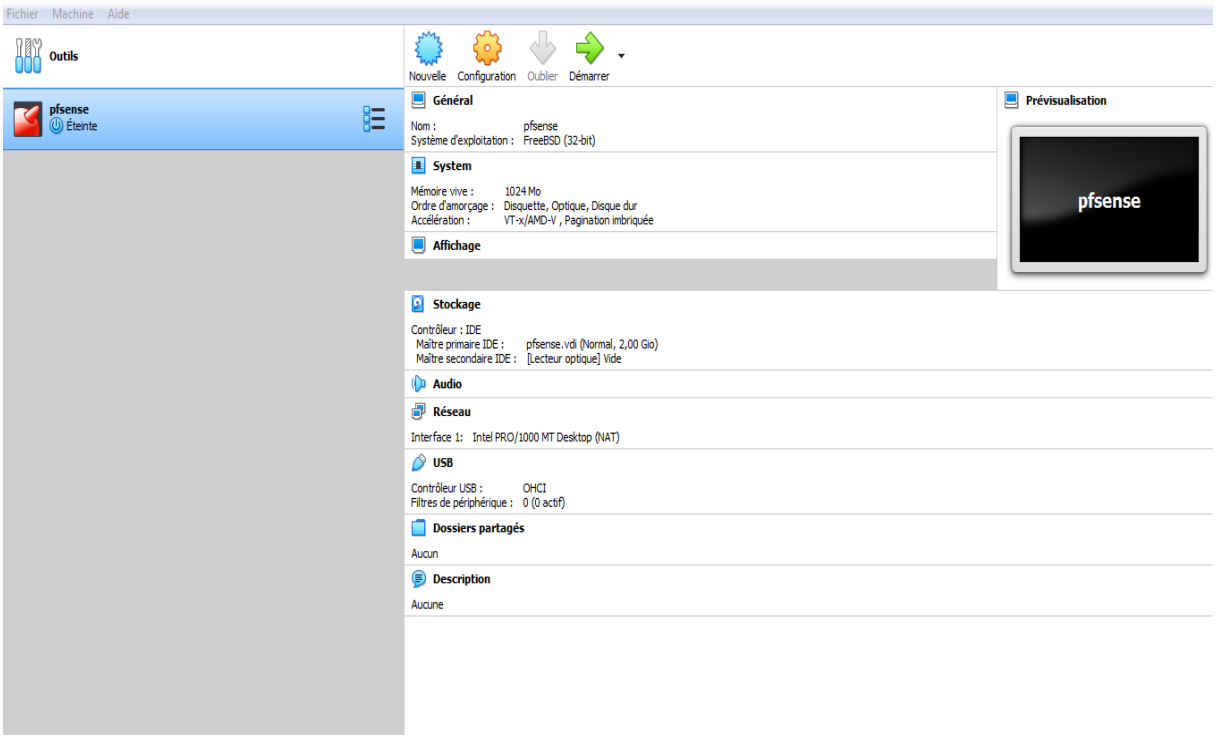



**Figure 4.4:** Démarrage de la machine virtuelle.

- **L'installation de 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.**

Nous réalisons l'installation sur une VM (machine virtuelle) depuis Virtual box, la procédure d'installation est la même que 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.

On boot sur le CD et on arrive aux menus de la figure 4.5 :

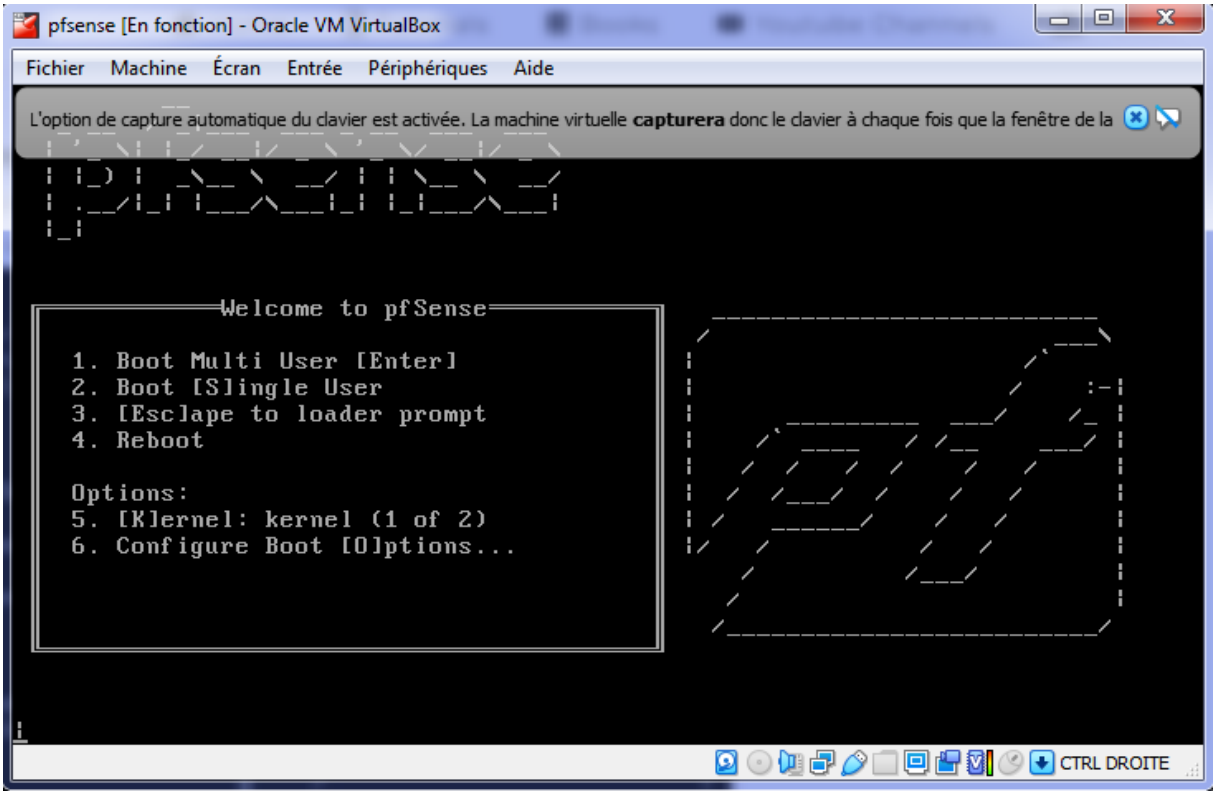



**Figure 4.5** : Pfsense sur Virtual box**.**

- On laisse le système démarrer de lui-même et après quelques secondes, on arrive à l'écran de la figure 4.6 :

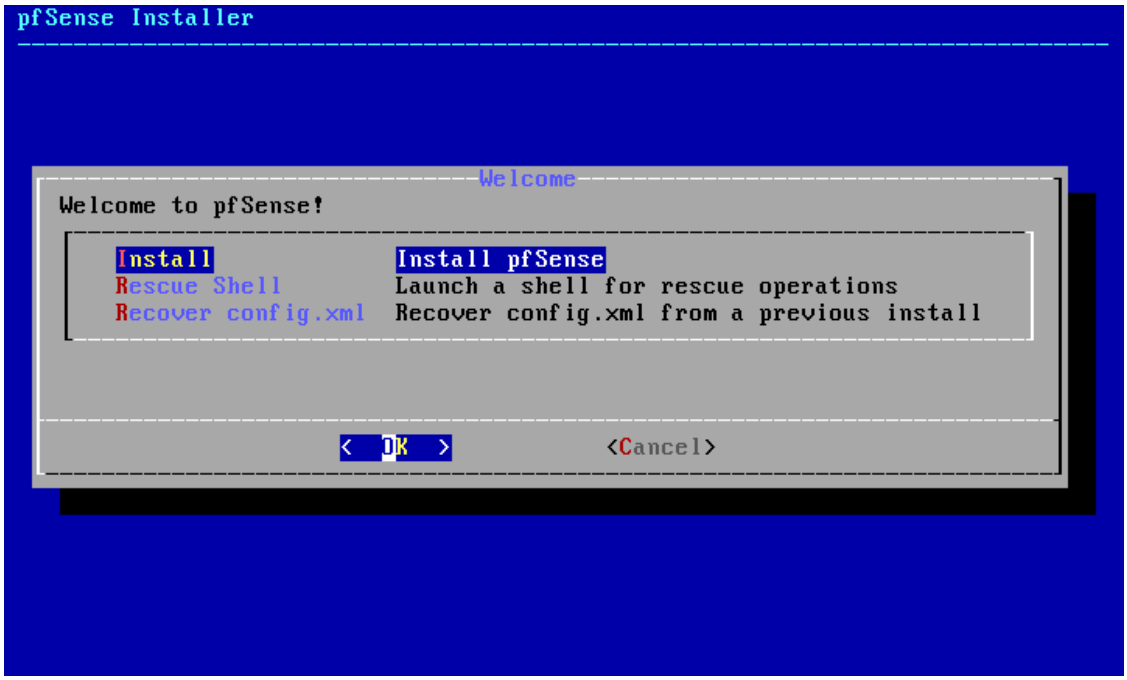



**Figure 4.6** *:* Début de l'installation de Pfsense.

- On accepte le type d'installation puis en validant par la touche « Entrée ».

A présent, il est question de configurer le type de clavier pour le système. On défile le curseur vers le bas pour sélectionner la langue française puis revenir sur « continue with default keyMap » après on valide par la touche « Entrée ». Voir la figure 4.7

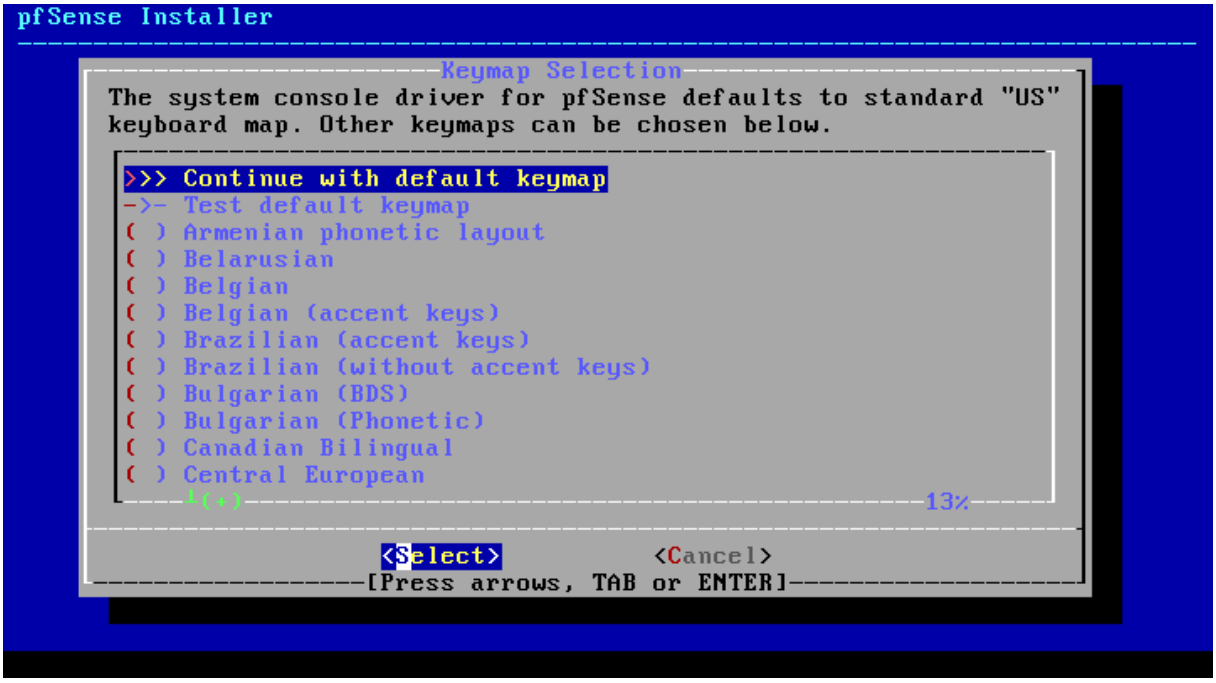



**Figure 4.7** : Configuration du type de clavier de Pfsense.

- Le choix suivant porte sur le type de partitionnement du disque spécifié pour l'installation de Pfsense. On laisse le choix par défaut en validant pour un partitionnement automatique sur « Auto (UFS) ». Comme le montre la figure 4.8


**Figure 4.8** : Partitionnement de l'espace disque de Pfsense.

- Après, toutes ces étapes préliminaires, on procède maintenant au redémarrage du système pour que ça prenne en compte toutes nos manipulations. Voir la figure 4.9


**Figure 4.9**: Fin de l'installation de Pfsense.

- **Configuration de pfsense** :

➢ Durant l'installation, Pfsense détecte automatiquement les cartes réseaux disponibles, et il y attribue respectivement le nom em0 pour le WAN et em1 pour LAN qu'il faudra configurer. Voir la figure 4.10

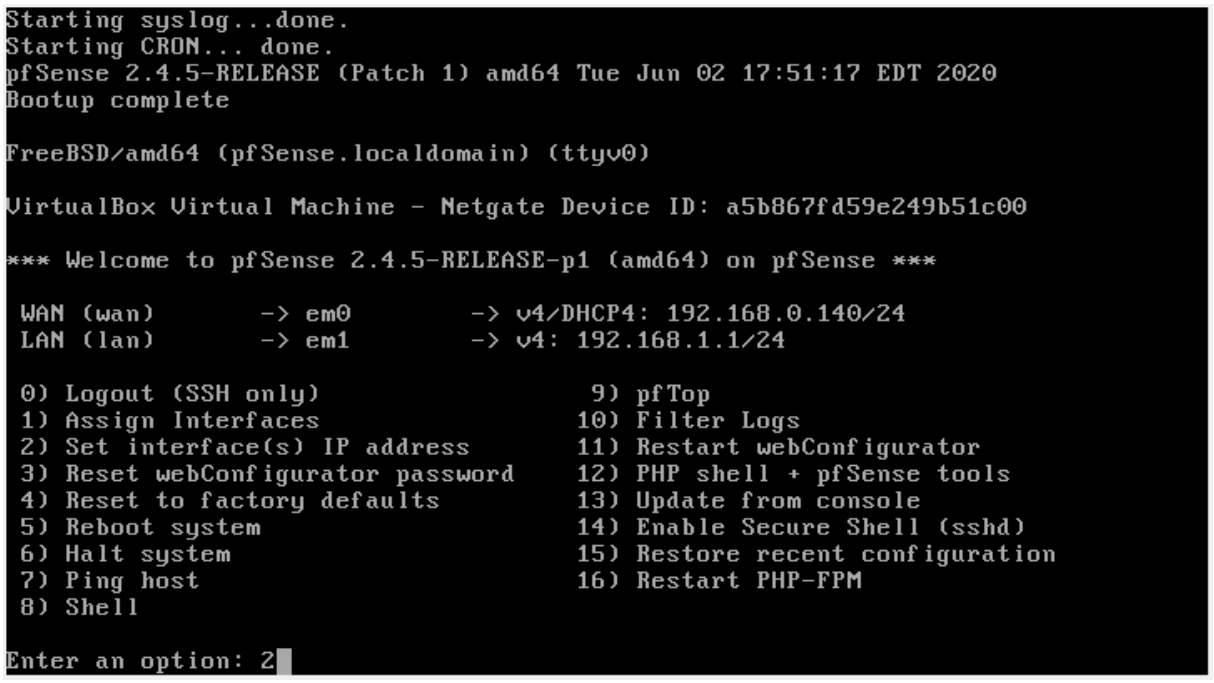



**Figure 4.10** : Configuration des interfaces.

➢ Puis choisir le numéro de l'interface à configurer comme le montre la figure 4.11

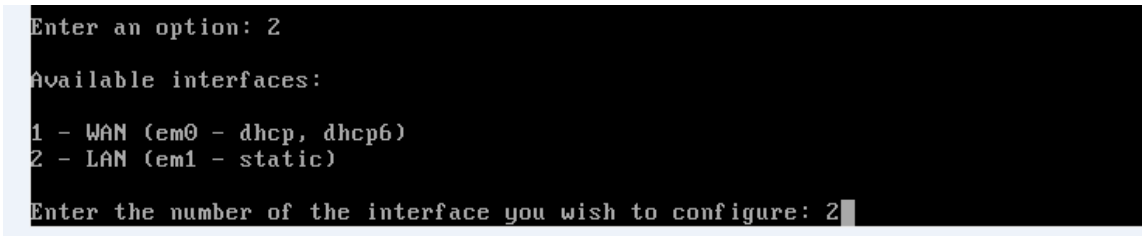



**Figure 4.11** : Choix de l'interface à configurer.

➢ Répondre aux questions pour configurer l'interface: adresse IP via DHCP ou adresse IP, nombre de bits de sous-réseau. Voir la figure 4.12

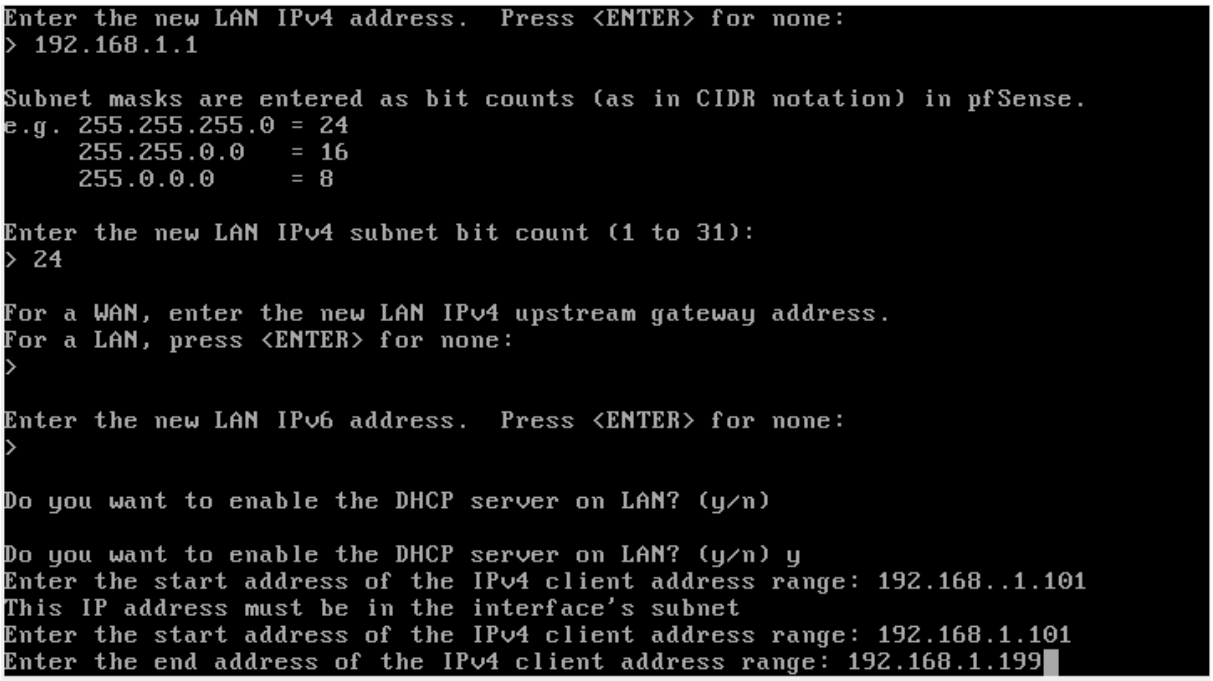



**Figure 4.12** : Les étapes de la configuration

- La configuration IP d'une interface se termine par une question demandant si nous souhaitons autoriser l'accès en http à l'interface web via cette interface.


**Figure 4.13** : Choix de configuration.

- La configuration se termine ici.

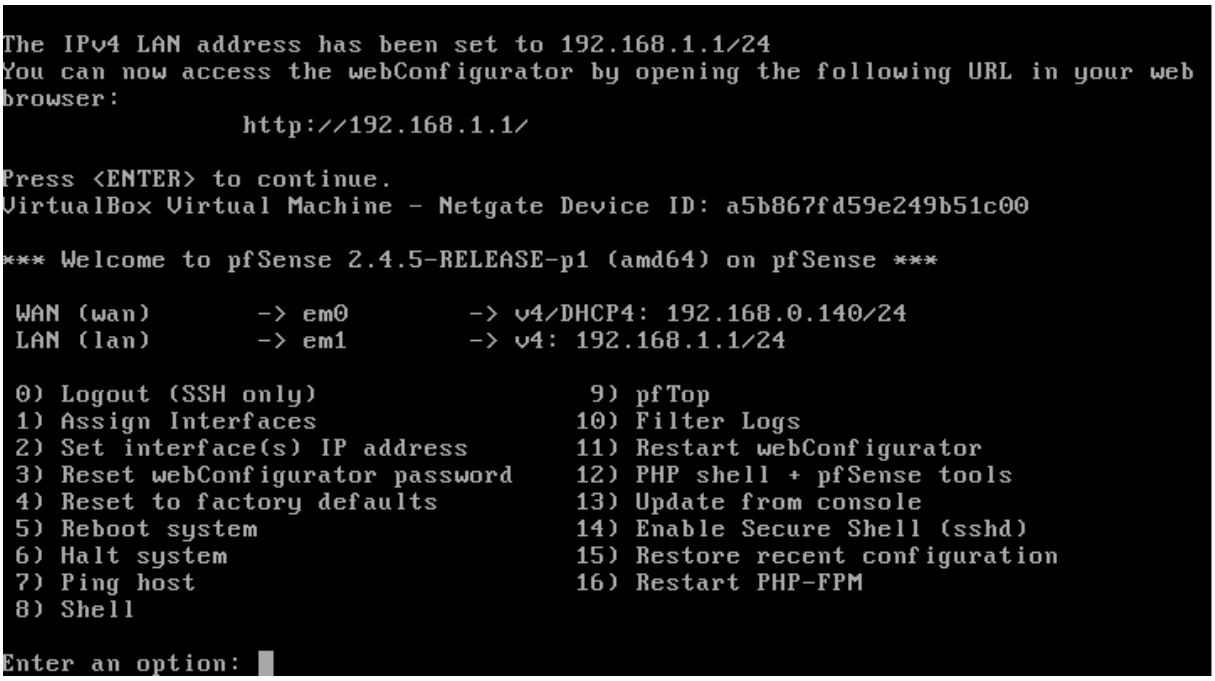



**Figure 4.14 :** Fin de la configuration.

### 3. La configuration des alias.

Pour se connecter à l'interface web de configuration de pfsense on utilise @ IP de l'interface WAN : http //192.168.0.140. La page de la figure 4.15 s'affiche :

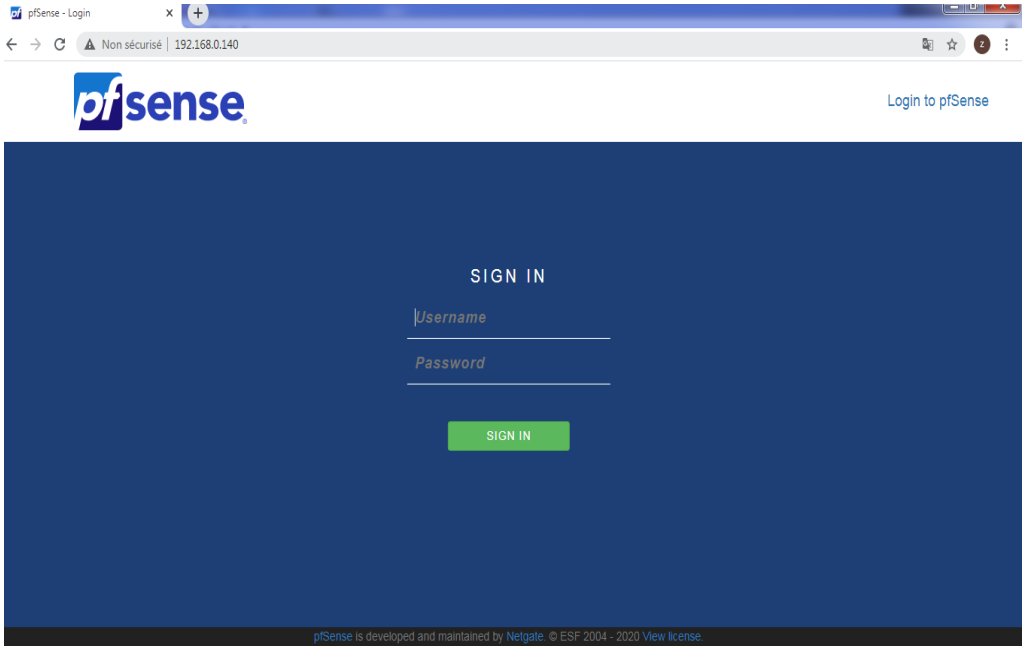
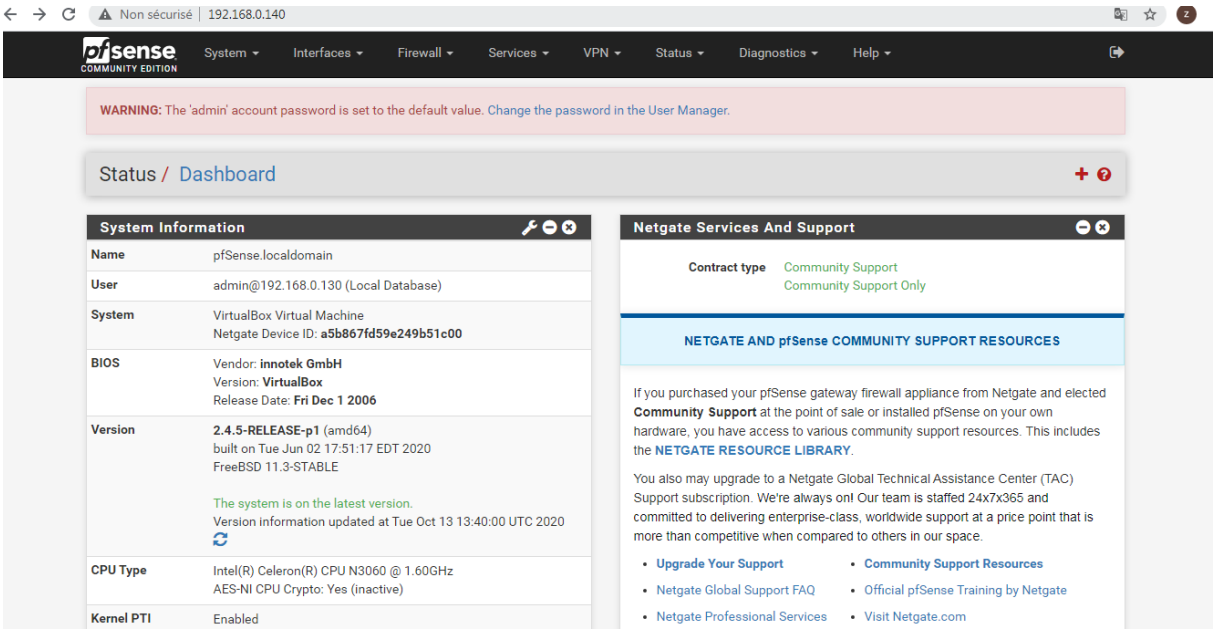



**Figure 4.15**: Page d'identification de PfSense.

Le couple username et password est par défauttel que :

- Username = admin
- Password = pfsense

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



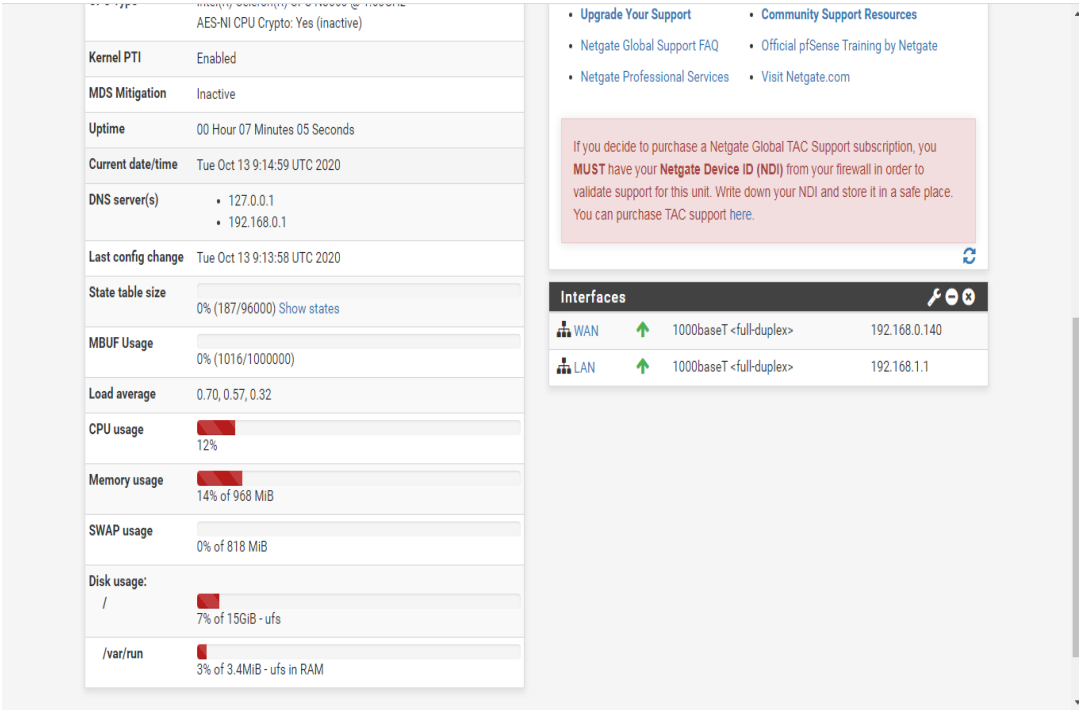




**Figure 4.16**: La page d'accueil de Pfsense.

- **Les services 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.et se compose de plusieurs éléments comme montre la figure 4.17 :

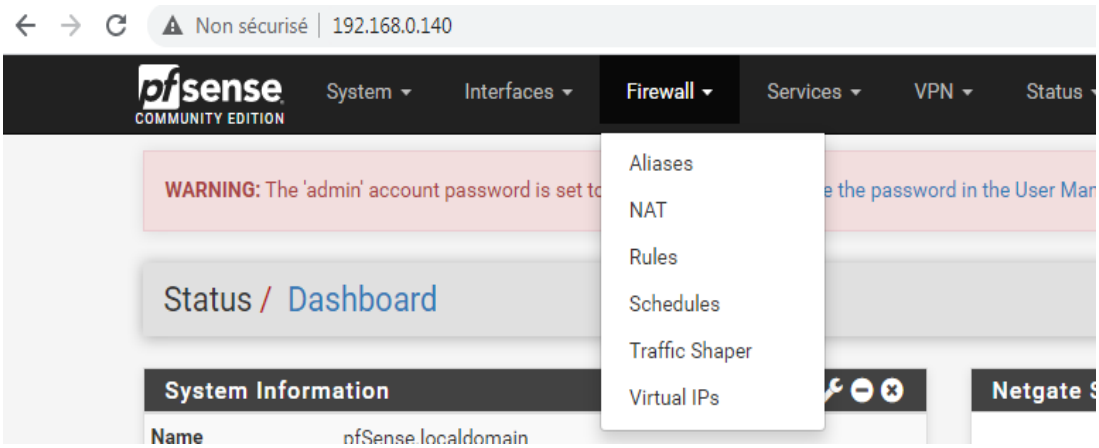



**Figure 4.17** : Les composants de firewall.

- **Aliases** : Les alias permettent principalement d'associer un nom à une adresse d'hôte, un port, ou un réseau.
- **Nat** : Le NAT (Network Address Translation) permet notamment de faire correspondre une seule adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé
- **Rules** : Les règles de filtrages permettent de mettre des restrictions sur des protocoles, Port et adresse IP.
- **Schedule** : Schedule (planifier) correspond à un intervalle de temps dans le mois ou dans la journée par exemple, l'accès Internet ne sera autorisé que de 9h à 19h.
- **Traffic shaper** : Le TrafficShaping permet de contrôler l'utilisation de la bande passante.
- **Virtual IPs**.

- **Services** : Permet d'activer de nombreux services 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, et de mettre en place une sécurité via IP Sec.

- **Status**: Permet de voir le statut de l'ensemble des configurations.

- **Diagnostics** : Permet de donner des outils permettant le diagnostic d'un quelconque bug

### 3.1. Création des alias.

Comme nous avons présenté dans le premier chapitre la problématique posée dans l'entreprise RAMDY était la gestion de la connexion Internet pour des alias (les gérants, les adjoints et les assistants) de réseau local et le problème de sécuriser le LAN de l'extérieur

Pfsense permet de créer des alias sur chaque interface (LAN etWAN), pour cela il faut paramétrer les alias dans l'onglet Firewall ⟹ aliases et pour ajouter des alias, nous cliquons sur LAN ou WAN après sur « **Add »** pour ajouter ces alias.

- **Alias 1** : gérant et responsable.

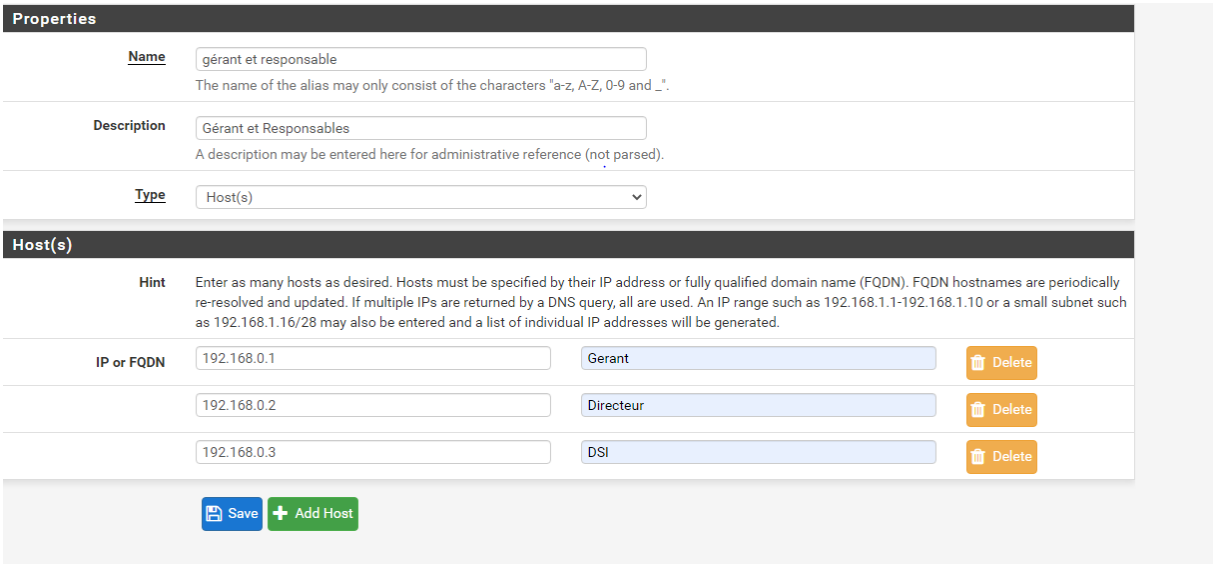



**Figure 4.18**: Interface d'alias ''1e gérant et responsable ''.

- **Alias 02** : adjoins des responsables.

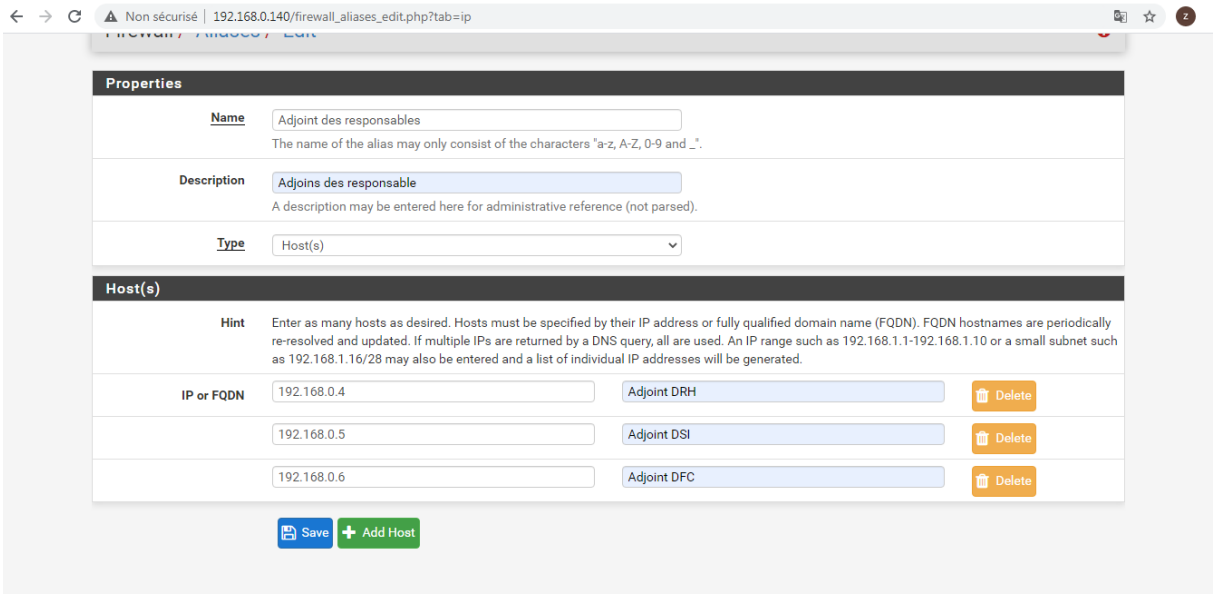



**Figure 4.19** : Interface d'alias 2'' adjoints des responsables''

- **Alias 03** : Assistants.

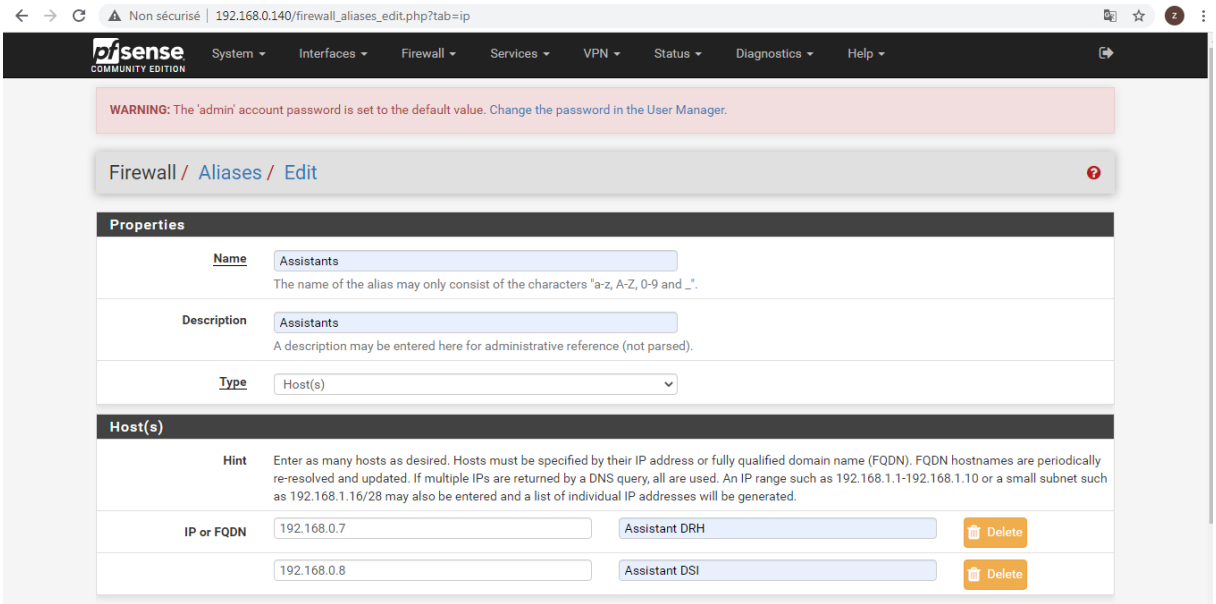



**Figure 4.20** : L'interface d'alias 3 '' assistants »''.

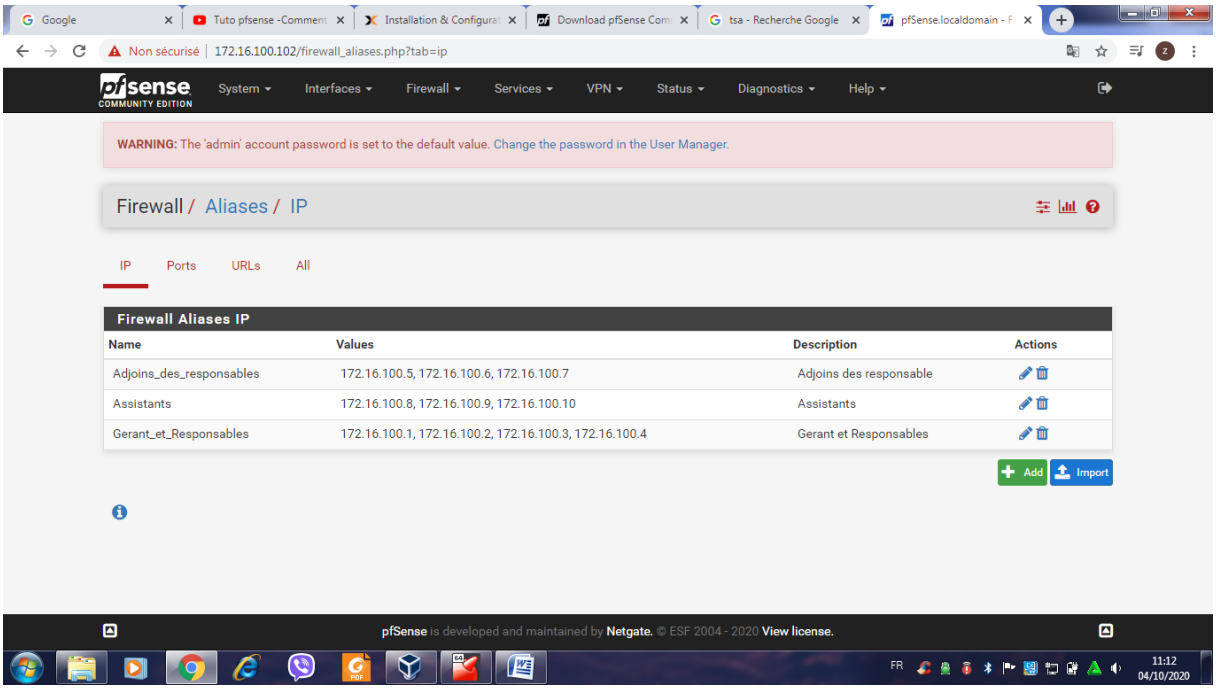



**Figure 4.21** : Interfaces qui montre tous les alias.

### 3.2. Les règles de filtrages.

Elles permettent d'autoriser ou de bloquer des requêtes en provenance de LAN, Pour ajouter une nouvelle règle, Tout d'abord rendez-vous dans Firewall =>Rules puis sur l'interface LAN.

Il y'a plusieurs actions qui peuvent être appliquées sur la règle :

- Block : Détruit le paquet sans retour vers la source.
- Reject : Un retour est effectué vers la source disant qu'il est refusé.
- Pass : Accepte le paquet.

➢ **Règle 1** : autoriser le gérant et les responsables pour un accès illimité à internet.

Nous devons sélectionner notre interface (WAN ou LAN), sur laquelle la règle sera active. On sélectionne si cela concerne IPv4 ou IPv6, ou bien les deux et pour finir on paramètre notre

règle, c'est-à-dire le protocole, la source et la destination et on peut aussi mettre une description afin de savoir rapidement son action.

Dans ce cas-là c'est une règle d'autorisation, mais le principale est le même pour toutes règles.

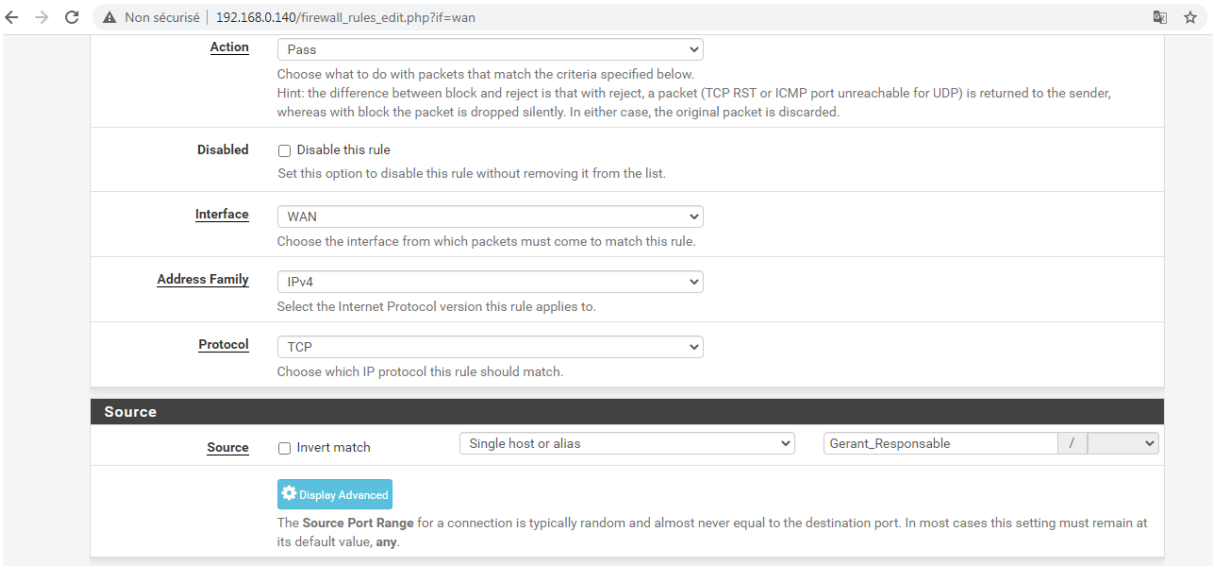
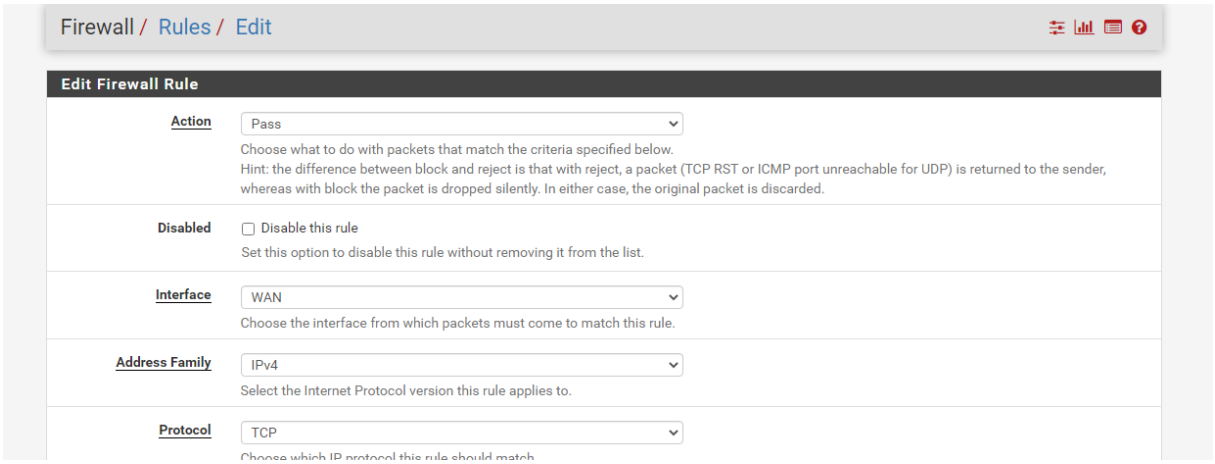



**Figure 4.22** : Interface de la règle d'autorisation.

- **Règle 2** : autoriser les adjoints des responsables pour un accès illimité à l'internet sauf au réseau sociaux exemples Facebook.

  Dans ce cas-là c'est une règle d'autorisation, comme montre la figure 4.23:



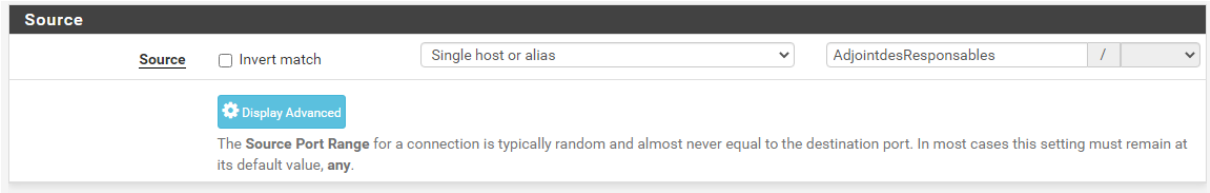



**Figure 4 .23 :** Interface de la règle d'autorisation pour adjoint.

Mais on va bloquer l'accès au Facebook comme montre la figure 4.24 :

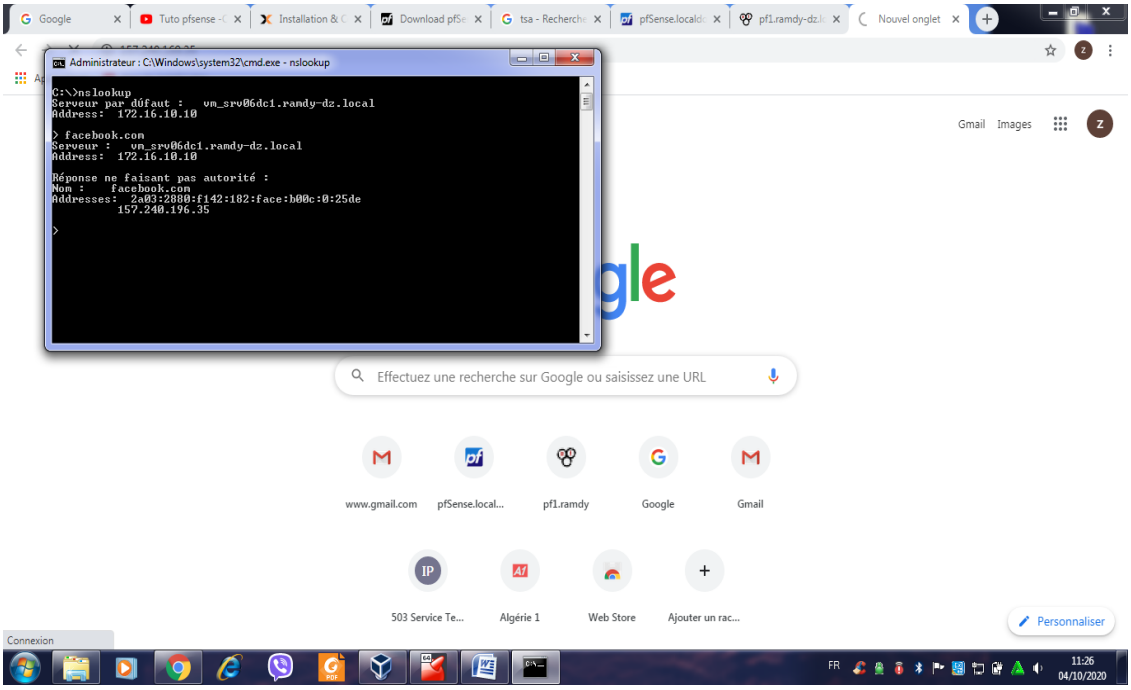



**Figure 4.24** : Adresse IP de Facebook.

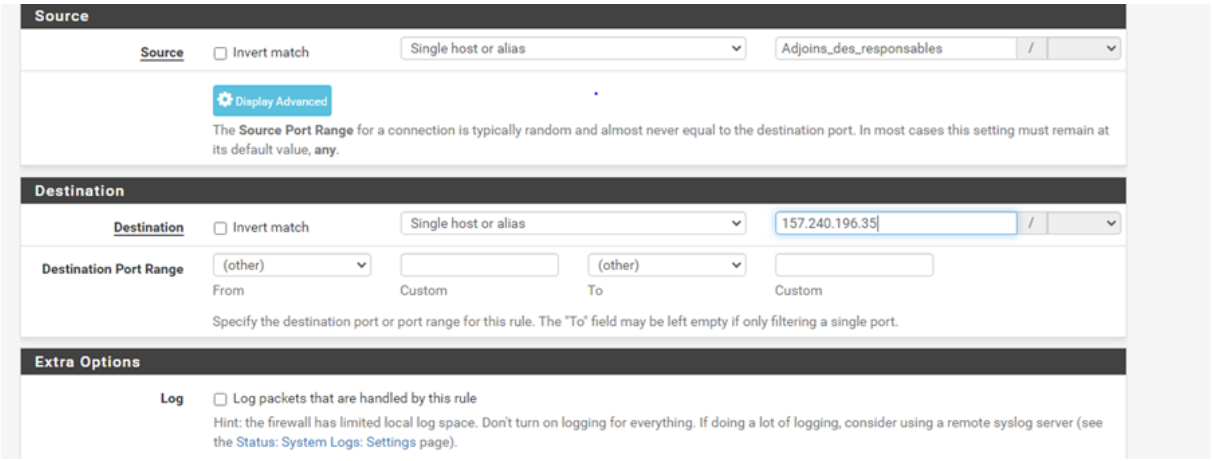



**Figure 4.25**: Interface qui montre le blocage de Facebook.

- **Règle 3** : interdire les assistants pour l'accès à internet sauf dans des horaires limités exemples de (12 :00-13 :00).

  Dans ce cas-là c'est une règle de blocage, comme montre la figure 4.26 :

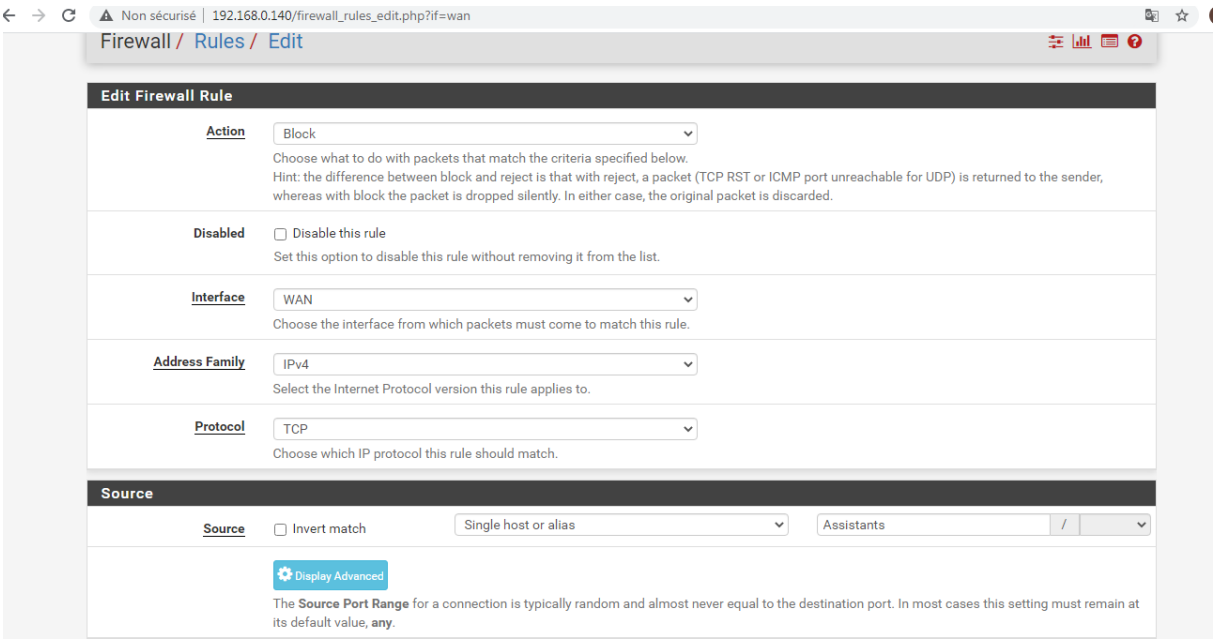



**Figure 4.26:** Interface de la règle de blocage pour assistant.

### 3.3. Création des règles basées sur des conditions d'horaire.

Une fonctionnalité pratique de pfSense, mais très méconnue, est la possibilité de définir des règles de filtrage qui seront appliquées en fonction de la date, du jour ou de l'heure.

On peut imaginer l'utilité pour ouvrir des accès temporaires le temps de mises à jour planifiées, pour différencier les horaires d'accès à Internet pour un usage professionnel / personnel ou encore pour un événement éphémère.

Ces règles de filtrage sont présentes avec les autres règles, mais elles seront actives uniquement sur les créneaux horaires définis. Le reste du temps, elles seront simplement ignorées par pfSense.

- **Configurer un calendrier**

La première étape consiste à configurer un calendrier. Cela se passe dans le menu Firewall > Schedule :

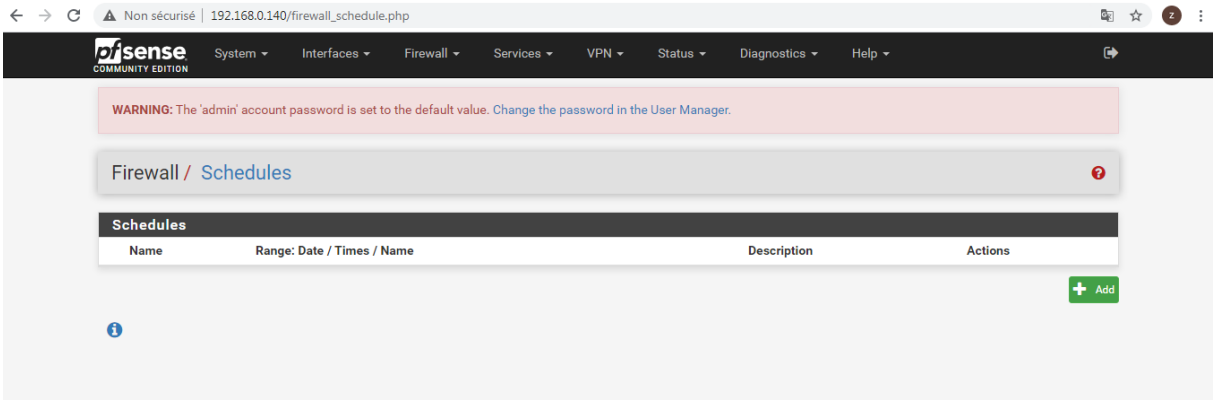



**Figure 4.27**: Interface qui permet d'accéder au Schedule.

➢ On cliquer sur le bouton "Add", Les champs à compléter sont les suivants :

- **Schedule Name** : le nom de votre "calendrier", sans espace ni caractères spéciaux.
- **Description** : champ purement informatif.
- **Month** : le mois et l'année applicable ; on ne peut sélectionner qu'un seul mois à la fois.
- **Date** : les jours où la condition horaire sera appliquée. Pour sélectionner chaque jour individuellement, il suffit de cliquer sur la case correspondante. Un jour sélectionné

sera sur fond vert. Il est également possible de sélectionner toutes les occurrences d'un jour donné (par exemple tous les samedi) ; pour cela, on peut cliquer directement sur l'entête de colonne correspondant (**Fri**dans notre exemple du vendredi). Les jours sélectionnés seront sur fond bleu.

- **Time** : l'horaire de début et de fin (se configure par tranche de quinze minutes)

Donc, si nous souhaitons sélectionner tous les vendredis du mois d'octobre 2020 sur le créneau 12h - 13h, le résultat ressemblera à ce qui est présenté sur la figure 4.28

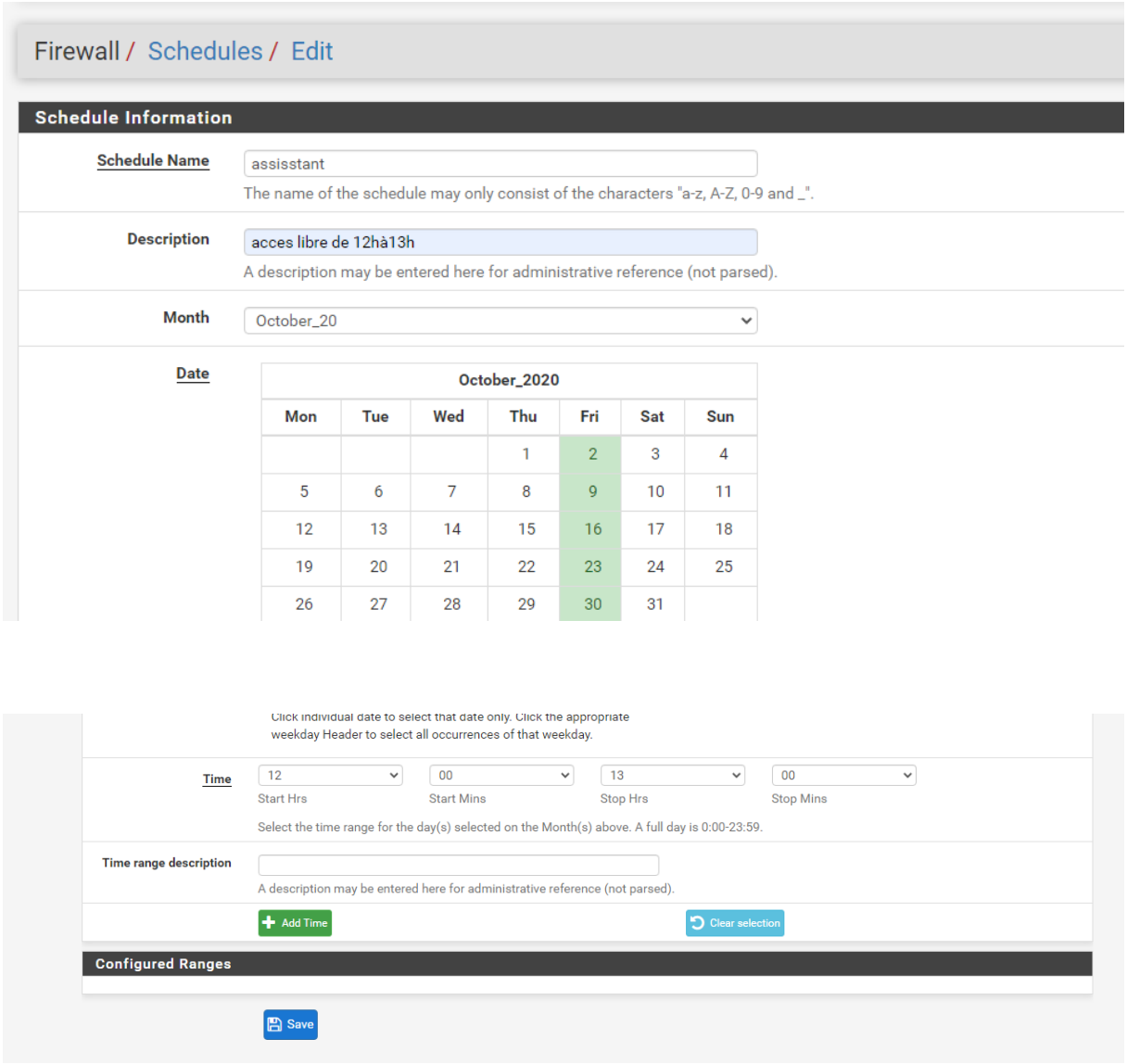



**Figure 4.28** : Configuration de calendrier.

Une fois notre configuration réalisée, il faut la valider en cliquant sur le bouton "+Add Time". Cela permet également d'ajouter d'autres dates et d'autres créneaux horaires à notre calendrier.

Enfin, il reste à cliquer sur le bouton "**Save**" pour sauvegarder notre calendrier.

- **Appliquer le calendrier à une règle de filtrage**

La création, ou la modification, d'une règle de filtrage s'effectue depuis le menu Firewall >Rules

Une fois sur votre règle de filtrage, il faut se rendre dans les options avancées (Section "Extra Options", cliquer sur le bouton "Display Advanced" :

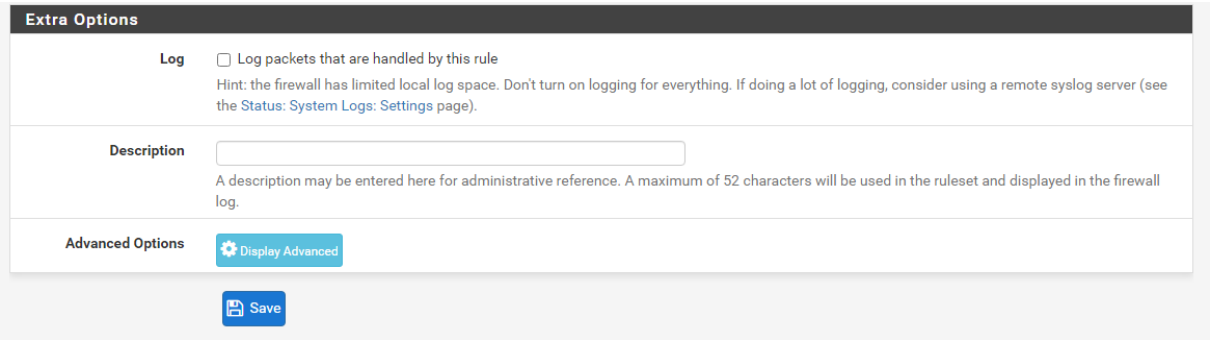



**Figure 4.29 :** Appliquer le calendrier à une règle.

Puis pour le champ **Schedule**, choisir le calendrier créé précédemment :

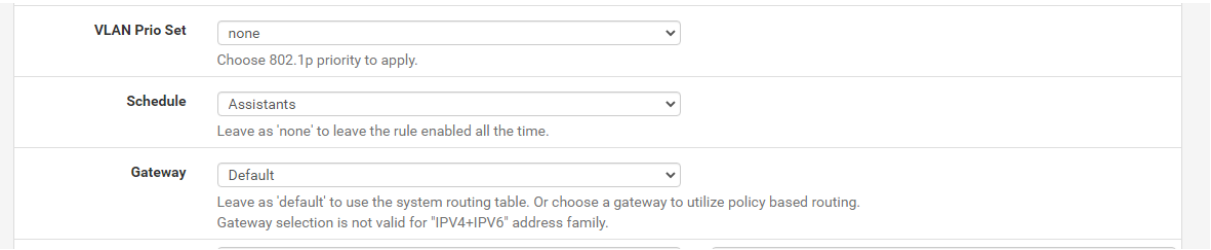



**Figure 4.30 :** Configurer le Schedule**.**

Le résultat obtenu comme est montrée sur la figure 4.31 :

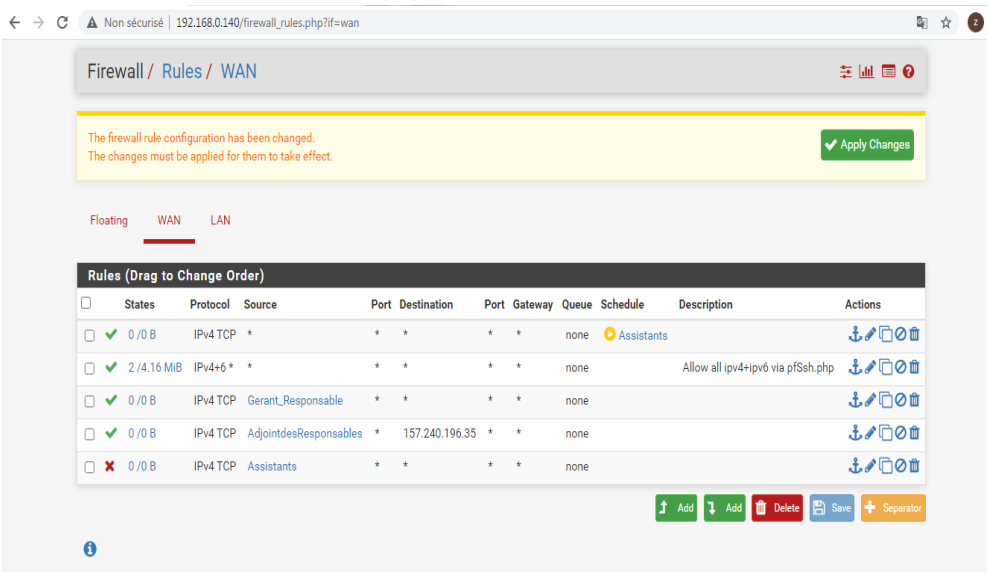



**Figure 4.31**: La configuration est terminée.

Le pictogramme jaune indique que la règle n'est actuellement pas active, c'est le cas de la première règle avec le calendrier "assistant".

## Conclusion

Dans ce chapitre, nous avons présenté les outils que nous avons utilisé, Ensuite, nous avons présenté les différentes étapes de l'installation et la configuration de notre solution qui est le pare feu pfsense, et les différentes règles de filtrages.

# Conclusion Générale

# Conclusion Générale

Un pare-feu est un composant réseau qui permet non seulement de concentrer l'administration de la sécurité en des points d'accès limités au réseau d'entreprise mais aussi de créer un périmètre de sécurité, par exemple entre le réseau intranet de l'entreprise et le réseau Internet. Une architecture à base de pare-feu offre l'avantage de concentrer les efforts de sécurité sur un unique point d'entrée.

Les pare-feu sont en outre des éléments cruciaux pour les investigations de sécurité grâce à des fonctions de journalisation des événements.

Durant le présent projet de fin de cycle, il nous a été confié la mission, au sein de l'Entreprise RAMDY pour mettre en place le pare-feu pfSense. Pour cela, notre travail a été décomposé en quatre chapitres majeurs. Dans Le premier chapitre on a présenté l'entreprise et la problématique ainsi une solution qui est le pare feu pfsense. Le second a porté sur les généralités sur les réseaux informatiques et la sécurité informatique. Le troisième a porté sur les pare feu ou nous avons brossé de façon claire les notions, le fonctionnement ainsi que les différentes catégories d'un pare feu. Le dernier chapitre qui était beaucoup plus pratique a porté sur la présentation de l'environnement du travail et enfin, la réalisation du projet qui était l'installation et la configuration de pare-feu pfsense sous virtuel box.

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 permis de découvrir le logiciel de simulation Virtual box.

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.

# Références Bibliographiques

# *Références Bibliographiques*


[1] : Présentation de l'Entreprise RAMDY, Documents internes de RAMDY.

[2] :Jean-François Pillou et Jean-Philippe Bay. Sécurité informatique.3ième édition, Dunod, Paris 2013

[3] : PatrickDucrot, Sécurité Informatique ,2009.

[4] : 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.

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

[6] :Arkoub Yacine Zakari, BoudriouaNacer-Eddine, Installation et configuration de PFSense, mémoire fin d'étude, MAST, Université de Bejaïa, 2016

[7] : JeanBabtiste Favre, Firewall : architecture et déploiement, Créative Commons, 2006

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

[9] : Lourent Bloch-Christophe Wolfhugel. EYROLLES, 2éme édition. 2005.

[10] :M.Righidel. Pour l'émergence d'une nouvelle sécurité dans les réseaux de communications et les systèmes d'information futurs, OFTA, Arago Vol.23, paris, 2000.

[11] : Encyclopédie informatique comment ça marche : introduction à la cryptographie introduction à la sécurité, http : //www.commentcamarche.com

[12] : TOM Thomas. La sécurité des réseaux, 2005.

[13] :S.Ikhalef. sécurité informatique Proxy, mémoire de fin d'études Ingéniorat, université de Bejaia 2003.

[14] :http : //www.tele.ucl.ac.be/EDU/ELEC/1997/firewall/Firewalls.html.

[15] : COSTANZO A., GRILLAT D., LEFRANCOIS L., Étude des principaux services fournis par pfSense, PfSense, 2009

[16] :http://www.formations-virtualisation.fr/vmware-definition-vmware.php: Définition de VMware

## ***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 RAMDY contre les menaces et les attaques éventuelles qui risquent de l’atteindre.



## Abstract

Opening up corporate access to the internet causes several attacks and to protect against them, secure network architecture is needed, such as a firewall. The purpose of this tool is to make the company's local network as secure as possible, to detect intrusion attempts to protect it as well as possible. This makes the open network on the Internet much more secure. The firewall therefore offers real control over the company's network traffic. It allows you to analyze, secure and manage network traffic,and thus use the network in the way it was intended.

In our brief, we were interested in putting in place a security strategy that the firewall considers to be able to secure as much as possible the network of a RAMDY company against the threats and possible attacks that may reach it.