République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

**Université Abderrahmane Mira. Bejaïa**

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

**Faculté des Sciences Exactes**

**Mémoire de fin d'études en vue de l'obtention du diplôme de**

# MASTER

## Informatique option ASR

**Thème :**

# *Installation et configuration de Pfsense*

**Présenté par:**

ARKOUB Yacine Zakari

BOUDRIOUA Nacer- Eddine

**Membre du jury :**

| | |
|---|---|
| Président : | Mr SALHI Nadir |
| Examinatrice : | Mme BELALTA Ramla |
| Encadreur : | Mr TOUAZI Djoudi |

*Année Universitaire : 2015/ 2016.*

## *Remerciements*

J'aimerais exprimer toute ma gratitude à :

- Notre promoteur. Monsieur TOUAZI pour ses conseils et ses connaissances qui m'ont aidé à réaliser ce mémoire.

- A tous nos professeurs du département Informatique ainsi qu'à son personnel.

- A tous ceux qui de près ou de loin ont contribué à notre apprentissage.

# DÉDICACES

*A mes parents sans qui je ne serais l'homme que je suis devenu*

*A tous les membres de ma famille sur qui j'ai pu compter et sur leur soutien indéfectible à mon épanouissement*

*A mes frères et ma sœur.*

*A ma « Clique», ma deuxième famille avec qui j'ai partagé de bons moments (mais aussi, de moins bon)*

*A mes amis pour leurs encouragements*

*A toute personne qui m'ont apporté leurs soutiens et qui ont cru en moi*

***Nacer-eddine***

***BOUDRIOUA***

# DÉDICACES

*A mes parents  sans qui je ne serais devenu  l'homme que je suis*

*A tous les membres de ma famille sur qui j'ai pu compter et sur leur soutien indéfectible à mon épanouissement*

*A mon frère et mes sœurs et mon oncle*

*A ma « Clique», ma deuxième famille avec qui j'ai partagé de bons moments (mais aussi, de moins bon)*

*A mes amis pour leurs encouragements*

*A toute personne qui m'ont apporté leurs soutiens et qui ont cru en moi*

***Zak ARKOUB***

## *Chapitre I :*

## *Chapitre II :*

## *Chapitre III :*

## *Chapitre IV :*

# *Table des figures :*

## *Chapitre II*



## *Chapitre III*

## *Chapitre IV*

# Liste des abréviations

**Admin :** administrateur

**DHCP :** Dynamic Host Configuration Protocol

**DNS :** Domain Name System

**IP :** internet protocol

**LAN :** Local Area Network

**MAC :** Media Access Control

**NAT :** Network Address Translation

**NTPD :** Network Time Protocol Daemon

**RIP :** Routing Information Protocol

**SNMP :** Simple network Management protocol

**TCP :** Transmission Control Protocol

**UDP :** User Datagram Protocol

**VPN :** Virtual Private Network

**WAN :** Wide Area Network

# Introduction générale

Internet est un gigantesque réseau qui relie un nombre sans cesse croissant de réseaux et d'ordinateurs individuels, c'est un moyen de communication idéal pour ceux qui souhaitent apprendre, améliorer leur culture, ou encore découvrir de nouveaux domaines. Bien qu'il ait beaucoup d'avantages, Internet est aussi un monde peuplé de dangers ayant de mauvaises influences sur les jeunes, dans la mesure où il a un pouvoir adductif très fort, et en raison des risques liés notamment aux sites pour adultes.

Cependant Les réseaux domestiques deviennent de plus en plus vulnérables et il est impossible aux parents d'être sans cesse derrière l'écran de leurs enfants, quelle est alors la solution qui permet aux parents de protéger leurs enfants ?

De nombreux outils et logiciels simples et efficaces existes pour la surveillance des enfants.

- Problematique et objectif :

  ce present travail a pour objectif la mise en place d'un systéme de surveillance dans un reseau domestique , afin de permettre aux parents de controller l'acces de leurs enfants a internet.

- Presentation des chapitres :

Le mémoire comporte quatre chapitres

Dans le premier chapitre nous donnons quelques généralités sur les différentes notions liées aux réseaux informatiques .

Dans le second, nous avon fait une etude de l'existance.

Dans le troisième, nous avons presenté l'outil Pfsense .

Le quatrième chapitre montre les etapes d'installation et de configuration de

Pfsense

Et enfin Une conclusion qui termine le mémoire.

## I.1 Introduction

Dans ce chapitre, nous donnerons quelques généralités sur les différentes notions liées aux réseaux informatiques dont la supervision.

## I.2 La supervision réseaux informatiques

En informatique, la supervision est une technique de suivi, qui permet de surveiller, analyser, rapporter et d'alerter les fonctionnements anormaux des systèmes informatiques.

En outre, la supervision informatique consiste à indiquer et/ou commander l'état d'un serveur, d'un équipement réseau ou d'un service software pour anticiper les plantages ou diagnostiquer rapidement une panne. [1]

## I.3 Réseau local

### I.3.1 Définition

Un réseau local, souvent désigné par l'acronyme anglais LAN (Local Area Network), est l'interconnexion d'équipements informatiques situés dans une zone géographique restreinte (appartement, maison, boutique, locaux d'entreprise, etc.), afin qu'ils puissent communiquer entre eux et éventuellement partager une connexion internet par le biais d'un routeur. [2]

### I.3.2 Caractéristiques d'un réseau local

Un réseau local est caractérisé par:[3]

- La courte distance entre les nœuds (< 10 km)
- Haut Débit (Une vitesse de transmission élevée: 10 Mbit/s à 10 Gbit/s)
- Un faible taux d'erreur
- La nature privée du réseau
- Des équipements diversifiés: connectiques, média, ordinateurs
- La Topologie logique de connexion : bus, étoile, …etc

- La méthode de partage des accès : droit de parole
- Format des trames : Plusieurs types d'informations.

## I.4 Réseau WAN

### I.4.1 Définition

Un réseau étendu, souvent désigné par son acronyme anglais WAN (Wide Area Network), est un réseau informatique couvrant une grande zone géographique, typiquement à l'échelle d'un pays, d'un continent, voir de la planète entière. Le plus grand WAN est le réseau Internet. [31]

## I.5 Routeur

Un routeur est un équipement d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter. [5]

## I.6 Firewall

Un firewall (ou pare-feu) est un outil informatique (matériel et/ou logiciel) conçu pour protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet par exemple, ou protection d'un réseau d'entreprise).

Il permet d'assurer la sécurité des informations d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies par son administrateur. [6]

## I.7 Proxy

### I.7.1 Définition

Un serveur proxy est un ordinateur ou un module qui sert d'intermédiaire entre un navigateur Web et Internet, le proxy participe à la sécurité du réseau. [7]

### I.7.2 Principe de fonctionnement

Les serveurs proxy permettent de sécuriser et d'améliorer l'accès à certaines pages Web en les stockant en cache (ou copie), Ainsi, lorsqu'un navigateur envoie une requête sur la demande d'une page Web qui a été précédemment stockée, la réponse et le temps d'affichage en sont améliorés, l'utilisateur accède plus rapidement au site et ne sature pas le proxy pour sortir, les serveurs proxy renforcent également la sécurité en filtrant certains contenus Web et les logiciels malveillants, tout de même il ne faut pas confondre avec un firewall (pare-feu), bien que le couplage des deux matériels en un, soit très courant. [7]

## I.8 Filtrage

Le filtrage est appliqué en fonction de la politique de sécurité en place sur le réseau, ceci permet de bloquer selon une liste noire, les sites considérés comme malveillants et/ou inutiles au contexte de travail de l'entreprise. [7]

## I.9 Authentification

Afin de limiter l'accès au réseau extérieur et de renforcer ainsi la sécurité du réseau local, il peut être nécessaire de mettre en place un système d'authentification pour accéder aux ressources extérieures, ceci est assez dissuasifs pour les utilisateurs souhaitant visiter des sites contraires à la charte de leur système d'information, Ils se sentent suivis et restent "sages" dans leurs recherches. [7]

## I.10 Internet

### I.10.1 Définition

Internet est un nouvel outil d'information et de communication en pleine évolution offrant des perspectives de croissance exceptionnelles.

C'est devenu un formidable moyen de communiquer, d'échanger, de travailler, de rencontrer, d'apprendre et même de commercer.

Internet est en train de modifier nos habitudes et de transformer complètement notre mode de vie. [8]

Il est constitué de bonnes et de mauvaises choses et certaines sont nuisibles notamment pour les plus jeunes.

## I.10.2 Ce qu'on peut trouver sur Internet

### a. Réseaux sociaux

Le terme de réseaux sociaux désigne généralement l'ensemble des sites internet permettant de constituer un réseau d'amis ou de connaissances professionnelles et fournissant à leurs membres des outils et interfaces d'interactions, de présentation et de communication.

Les réseaux sociaux les plus connus sont Facebook, Twitter, Linkedin, Viadeo, Pinterest, etc. Youtube peut également être considéré partiellement comme un réseau social dans la mesure où le service a développé des outils d'interactions entre ses membres. [9]

### b. Chats

Ce terme correspond à la possibilité de discuter en ligne sur internet en temps réel avec une ou plusieurs personnes. Contrairement au logiciel de messagerie, le chat permet à l'interlocuteur de prendre instantanément connaissance du contenu du message. [10]

### c. jeux en ligne

Un jeu en ligne (ou jeu sur internet) est un jeu jouable par le biais d'un réseau informatique.

L'expansion du jeu en ligne a reflété l'expansion des réseaux informatiques et même d'Internet. Les jeux en ligne peuvent incorporer de simples jeux d'écriture aux jeux complets et détaillés, dans lesquels plusieurs joueurs se retrouvent d'une manière simultanée (jeux

multi-joueurs), certains jeux multi-joueurs en ligne sont accessibles grâce à un abonnement payant mensuel, tandis que d'autres, offrent une accessibilité gratuite. [11]

### I.10.3 Les dangers que représente internet pour les enfants

### a. Le risque d'harcèlement en ligne

Les enfants se sont toujours moqués d'autres enfants, ce n'est qu'en grandissant qu'ils apprennent à se conduire de manière civilisée, avec l'avènement des réseaux sociaux, une photo peu avantageuse ou une réponse mal formulée à un poste peuvent déclencher tout un processus de victimisation, avec des conséquences très graves dans la vie quotidienne de l'enfant, impactant lourdement son développement. [12]

### b. Trop d'Internet

Les adolescents peuvent rester éveillés toute la nuit collés à leur écran, à lire des forums, à regarder des vidéos ou scotchés sur un jeu vidéo, et ces nuits de veille laissent des traces le lendemain et la fatigue accumulée nuit à la concentration et impacte directement sur les études.

De plus, rester assis sans bouger pendant des heures devant l'ordinateur n'apporte rien en termes de bonne hygiène de vie. [12]

### c. Sites Internet pour adultes ou illégaux

Entre les paris en ligne, ventes de drogues ou d'armes, sites de torrent proposant du téléchargement illégal, il y a beaucoup d'endroits sur Internet qui ne sont pas faits pour les enfants.

Historiquement, c'est la maturité des technologies de vidéos en ligne qui a permis à l'industrie pornographique de se ruer sur un nouveau marché immense et d'inonder la toile avec des sites

pour adultes. Et de nos jours encore, les sites inappropriés se multiplient comme des petits pains. Les éditeurs essayent à tout prix de faire venir les visiteurs sur leur site, n'hésitant pas à diffuser largement des publicités explicites et volontairement trompeuses dans les promesses. [12]

### d. Des conversations dangereuses

Les e-mails, la messagerie instantanée ou les réseaux sociaux sont des moyens de communications extrêmement pratiques, pour échanger avec ses amis ou sa famille. Mais, c'est aussi une porte ouverte aux personnes aux intentions dangereuses. Un jeune avec un compte Skype renseigné ou un profil Facebook public s'expose à des contacts avec des personnes inconnues, qui ne pourraient pas l'approcher autrement dans la vie courante.

Selon plusieurs études, plus d'un enfant sur deux aurait été abordé par des inconnus en ligne et l'ONU estime à plus de 750 000 le nombre de prédateurs cherchant à entrer en contact avec des enfants sur Internet.

Les méthodes employées par des pédophiles montrent souvent des approches insidieuses, avec de longues périodes de dialogue via les messageries instantanées afin de créer un climat de confiance. Souvent l'objectif final est d'organiser une rencontre physique. [12]

## I.10.4 Comment lutter contre ces dangers

### a. La pédophilie

Les réseaux sociaux du type Facebook permettent de préciser les règles de confidentialité de son profil, Par exemple, on peut empêcher toute personne qui ne fait pas partie de son réseau d'amis de vous envoyer un message. [13]

### b. Le harcèlement

Il ne faut pas hésiter à faire comprendre à son interlocuteur qu'il a dépassé les limites lorsqu'il vous envoie des messages à répétition que l'on n'a pas sollicités. Et s'il n'obtempère pas, il ne faut pas hésiter à l'enlever de sa liste d'amis ("défacebooker"). [13]

### c. Le temps passé sur cette activité

Là, c'est aux parents d'intervenir et de surveiller discrètement ce que font leurs enfants sur Internet. Pour cela, la meilleure solution reste encore d'installer l'ordinateur dans une pièce commune où la famille peut jeter un coup d'œil sur ce qui se passe. [13]

## I.11 Conclusion

Dans ce chapitre, nous avons donné quelques généralités sur le mal que peut causer l'activité des réseaux sociaux notamment sur la frange juvénile, cité la nécessité de la surveillance dans les réseaux locaux et nous nous sommes intéressé a l'impacte que peux avoir internet sur l'éducation de nos enfants.

## II.1 Introduction

Dans ce second chapitre, nous allons définir le thème du contrôle parental, puis nous présenterons quelques logiciels de contrôle parental que nous allons comparer entre eux.

## II.2 Contrôle parental

Le contrôle parental peut être définit comme un moyen et outil système qui assure la protection des enfants qui se trouvent confrontés constamment à des contenus qui ne leur sont pas destinés et qui proposent des outils pour gérer l'utilisation d'Internet par les enfants. [14]

## II.3 Logiciel de contrôle parental

Pour une utilisation efficace et optimale de tout logiciel de contrôle parental, deux sessions minimum doivent être créées, sinon le logiciel ne servirait à rien.

- Une session « parent » qui gèrera l'administration principale du PC et celle du logiciel.
- Une session enfant et/ou une session ado, n'ayant aucun pouvoir. [15]

Il est important de bien paramétrer le logiciel de contrôle parental afin que son utilisation soit adaptée à l'âge et la maturité de l'enfant et au mode d'éducation des parents.

Le logiciel de contrôle parental a la possibilité de :

1. Réglementer les horaires de connexion selon des plages horaires définies par les parents
2. Bloquer l'accès à certains sites web.
3. Consulter l'historique des sites visités. [14]

### II.3.1 Réglementer les horaires de connexion

Le logiciel de contrôle parental permet de réglementer les horaires de connexion selon des plages horaires définies par vos soins. Ainsi, vous allez pouvoir limiter les horaires d'accès à Internet, voir même l'utilisation de l'ordinateur lui-même. [16]

### II.4.1.1 Horaire Pc

### a. Descriptions

Horaire PC est un logiciel qui permettra de se fixer des limites horaires pour l'utilisation du PC, afin de combattre toute forme d'usage abusif de l'ordinateur, Le logiciel s'adresse en grande partie aux parents désirant contrôler l'utilisation du PC par leurs enfants, ainsi, les parents pourront restreindre l'utilisation de certaines applications à certaines heures de la journée et/ou certains jours de la semaine. [17]

### b. Fonctionnalités du logiciel Horaire PC

Le logiciel de contrôle parental horaire pc offre la possibilité a l'utilisateur de :

- fixer des plages horaires d'utilisation de l'ordinateur et/ou de l'écran.
- fixer une durée maximum d'utilisation de l'ordinateur et/ou de l'écran pour chaque jour de la semaine.
- fixer une durée maximum d'utilisation du PC ou de l'écran pour la semaine entière.
- interdire l'utilisation de n'importe quel logiciel (msn messenger, jeux en ligne, internet explorer,...) à certaines heures de la journée et/ou certains jours de la semaine. [18]

### c. Les plus d'Horaire PC

Ce logiciel offre éventuellement des fonctions supplémentaires qui nous permettent de :

- bloquer seulement l'écran sans éteindre le PC, vous pouvez ainsi empêcher vos enfants d'utiliser l'ordinateur sans être obligé d'interrompre d'éventuels téléchargements que vous auriez en cours.
- fixer des limites aux simples utilisateurs mais également aux administrateurs de Windows.
- continuer de fonctionner en mode sans échec
- fixer des limitations différentes pour chaque utilisateur. Ce qui le rend multiutilisateur.
- fixer des règles qui s'appliquent à tous les utilisateurs de l'ordinateur, y compris les comptes administrateurs et le compte du mode sans échec.
- donner à l'administrateur la possibilité de fixer ses propres limites, la fonction d'autocontrôle, permet de fixer des limites horaires qui resteront en vigueur jusqu'à une date de votre choix, et que vous ne pourrez pas modifier avant cette date (même avec le mot passe). [18]

## II.4.2 Possibilité de bloquer l'accès au site

Afin de bloquer l'accès à certains sites, il existe 3 types de listes correspondant à différentes stratégies de protection.

**1)** Liste de mots clés : cette liste bloque l'accès aux sites contenants ces mots dans les URLs ou dans les pages du site.

**2)** Liste noire : c'est une liste de sites interdits, généralement mise à jour à chaque connexion par le logiciel mais qui n'est pas exhaustive.

**3)** Liste blanche : cette liste contient les sites autorisés par le logiciel (il est à tout moment possible d'ajouter et supprimer des sites dans cette liste), tous les sites qui ne figurent pas dans la liste blanche seront bloqués par le logiciel, c'est sans doute la meilleure pour des enfants en bas âge, moins pour des plus grands qui ont besoin de pouvoir naviguer librement pour faire des recherches, que ce soit pour le collège ou pour leurs loisirs. . [14]

### II.4.2.1 Xooloo

### a. Description

Xooloo est un logiciel de protection des enfants et des adolescents sur Internet.
Les technologies de filtrage Xooloo sont brevetées et assurent un haut niveau de sécurité pour chaque membre de la famille. [19]

### c. Ergonomie: des réglages automatiques très pratiques

Vous n'avez pas besoin d'être expert en informatique pour L'installation et l'utilisation de ce logiciel, il est suffisamment facile pour permettre à tous les parents de sécuriser la connexion de leurs enfants.

Les modes et les profils de filtrages sont ajustables en un clic, les réglages ne sont vraiment pas compliqués, le mode Adolescent et le mode Enfant sont pré-paramétrés par défaut, c'est-à-dire que sans paramétrage personnalisé, ces deux modes sont filtrés par défaut. De toute façon, moins vous personnaliserez les modes prédéfinis, plus efficace sera le filtrage. [20]

### d. Fonctionnalités de xooloo

Le contrôle parental Xooloo propose trois profils de protection préconfigurés ajustables en un clic afin de protéger vos enfants :

- Le mode Adolescent : les enfants peuvent naviguer sur la totalité des sites Internet à l'exception des sites identifiés comme inappropriés dans la liste noire, mises à jour par l'équipe de documentalistes.
- Le mode Enfant : les enfants peuvent naviguer en sécurité sur une sélection de plusieurs milliers de sites Internet dont les contenus sont préalablement analysés et vérifiés par notre équipe de documentalistes, qu'on nomme whiteliste.
- Enfin, un mode Parent permet de surfer sans être filtré. [24]

### e. Compatibilité Mac et PC

Le logiciel de contrôle parental Xooloo est le seul à être compatible avec Pc et Macintosh.

La Liste Blanche Xooloo (liste des sites sur lesquels peuvent surfer les enfants en toute sécurité) est la première à allier une technologie de pointe et l'évaluation humaine, d'où sa pertinence et sa qualité. [20]

## II.4.2.2 Optenet Web Filter pc

### a. description

Web Filter PC est un outil de contrôle parental qui permet de filtrer les sites Internet consultés par vos enfants ainsi que les fichiers téléchargés, C'est une solution efficace et facile d'aide aux parents désirant laisser leurs enfants surfer en toute sécurité. [30]

### b. Ergonomie: très simple d'utilisation

Le logiciel Web Filter s'adresse exclusivement aux parents et est conçu pour leur faciliter l'usage, Aucune connaissance spécifique n'est requise pour utiliser le logiciel, pas besoin de le configurer, vous installez le logiciel et pouvez le laisser tourner les yeux fermés, la configuration par défaut protège les enfants des contenus inappropriés. [20]

### c. Fonctionnalités: les outils de dialogue en ligne aussi

Web Filter permet de bloquer et de filtrer les contenus de sites catalogués dans plus de 50 catégories, Il permet aussi de bloquer l'accès aux chats de discussions, forums, messageries instantanées, de limiter les téléchargements et les temps de connexion à Internet. [20]

### d. Les plus: les corrections rapides

Optenet intègre un analyseur sémantique et un analyseur d'URL qui permettent une analyse pointue et détaillée du contenu visité sur Internet en 180 langues et dialectes ! D'éventuelles erreurs de filtrage sont corrigées dans le quart d'heure qui suit. [20]

## II.4. Consulter l'historique des sites visités

### II.4.1 SpyMyKeyboard

### a. Description

SpyMyKeyboard est un enregistreur de frappe de clavier (keylogger), il enregistre tout ce qui est tapé sur l'ordinateur (mots de passe, conversations, etc.) et envoie les données par mail avec une copie de l'écran. [21]

### b. Fonctionnalités

SpyMyKeyboard S'inscrit dans la catégorie des Keyloggers, ces programmes espions qui enregistrent tout ce qui est tapé au clavier, nous citerons ci-dessus quelques fonctionnalités que nous offre ce logiciel :

- Ultra discret car totalement invisible

- Configuration encore plus simple : le logiciel vous guide pour le paramétrer en 5 étapes
- Envoi par e-mail de tout ce qui est tapé sur l'ordinateur
- Envoi de capture d'écran par mail
- Fréquence d'envoi des e-mails paramétrable
- Fonctionne en tâche de fond
- Aucune installation nécessaire
- Lancement automatique au démarrage
- Indétectable par les anti-virus
- Affichage du nom de la fenêtre en cours [22]

## II.5 Pfsense

### II.5.1 Définition

PfSense est libre, une distribution personnalisée de FreeBSD adapté pour être utilisée comme routeur et pare-feu. En plus d'être une plate-forme puissante, flexible de routage et de pare-feu, elle comprend une longue liste de caractéristiques connexes et un système de package permettant en outre l'évolutivité sans ajouter de ballonnement et de failles de sécurité potentielles à la distribution de base. PfSense est un projet populaire éprouvé dans d'innombrables installations allant des petits réseaux domestiques pour protéger un ordinateur unique, pour les grandes entreprises, les universités et d'autres organisations protégeant des milliers de périphériques réseaux. [24]

### II.5.2 les caractéristiques de pfSense

Parmi les composantes de pfsense, nous citerons ci-dessous quelques unes, du moins les plus importants, ainsi que le rôle de chacune d'elle :

## a. Pare-feu

- Filtrage par IP source et destination, le protocole IP, la source et port de destination pour le trafic TCP et UDP
- Permet de limiter les connexions simultanées basées sur une règle
- Politique de routage très flexible pour la sélection de la passerelle basée sur des règles (pour l'équilibrage de charge, basculement, WAN multiple, etc.). [24]

## b. Tables d'états

La table d'état du pare-feu gère les informations sur votre connexion réseau ouvertes, le logiciel PfSense est un firewall qui gère les états par défaut et toutes les règles prennent cela en compte.

La plupart des pare-feux ne sont pas capables de contrôler finement votre table d'état, le logiciel PfSense a de nombreuses fonctionnalités permettant un contrôle détaillé des flux d'utilisateurs avec plusieurs paramètres ou détails de votre table d'état.

## c. Translation d'adresses (NAT)

- Le port forward comprend l'utilisation de plages ainsi que de plusieurs adresses IP publiques.
- le NAT 1:1 pour les IPs individuels ou sous réseaux entiers.
- Outbound NAT
    - Les paramètres par défaut NAT du trafic sortant vers l'IP WAN.

    Dans plusieurs scénarios WAN, les paramètres NAT sorte par défaut vers l'adresse IP de l'interface WAN utilisé.
    - Les fonctions avancées du NAT sortant qui permet ce comportement est désactivé par défaut et permet la création de règles NAT très flexible.
- NAT Reflection est possible si les services sont accessibles par IP publique à partir des réseaux internes. [24]

### d. Equilibrage de charge

L'équilibrage de charge du serveur est utilisé pour répartir la charge entre plusieurs serveurs, ceux qui ne répondent pas aux requêtes ping ou aux connexions de port TCP sont retirés du pool. [23]

### e. Rapport et monitorage

Permet d'avoir des informations sur les points suivants [23]:

- L'utilisation du processeur
- Le débit total
- L'état des pare-feux
- Débit individuelle pour toutes les interfaces
- Taux de paquets par seconde pour toutes les interfaces
- Temps de réponse des interfaces de passerelle WAN
- Files d'attente Traffic Shaper sur les systèmes avec le lissage du trafic activé. [23]

### f. Information temps réel

L'historique d'information est important, mais parfois, il est plus important d'obtenir des informations en temps réel. [23]

### g. DNS dynamique

Un client DNS Dynamique est inclus pour permettre d'enregistrer votre adresse IP publique avec un certain nombre de fournisseurs de services DNS dynamiques. [23]

### h. Portail captif

Le Portail captif a pour rôle de forcer l'authentification, ou la redirection vers une page de clic pour l'accès au réseau. [23]

### i. Serveur et relais DHCP

Le logiciel pfSense comprend à la fois le serveur DHCP et la fonctionnalité de relais. [23]

### II.5. Comparaison entre logiciels

| | **Filtrer les sites web** | **Réglementer les horaires** | **Consulter l'historique des sites visités** |
|---|---|---|---|
| **Horaire pc** | | ✓ | |
| **Xooloo** | ✓ | | |
| **optenet web filter pc** | ✓ | ✓ | |
| **SpyMyKeyboard** | | | ✓ |
| **Pfsense** | ✓ | ✓ | ✓ |

*Table II.1 Comparaison des logiciels*

Nous remarquons à travers le tableau ci-dessus, que Pfsense est bien plus performant que les logiciels cités précédemment.

## II.6 Synthèse

Dans la figure ci-dessous, nous avons regroupé tous les logiciels vus précédemment ainsi leurs fonctionnalités sous forme d'un schéma.

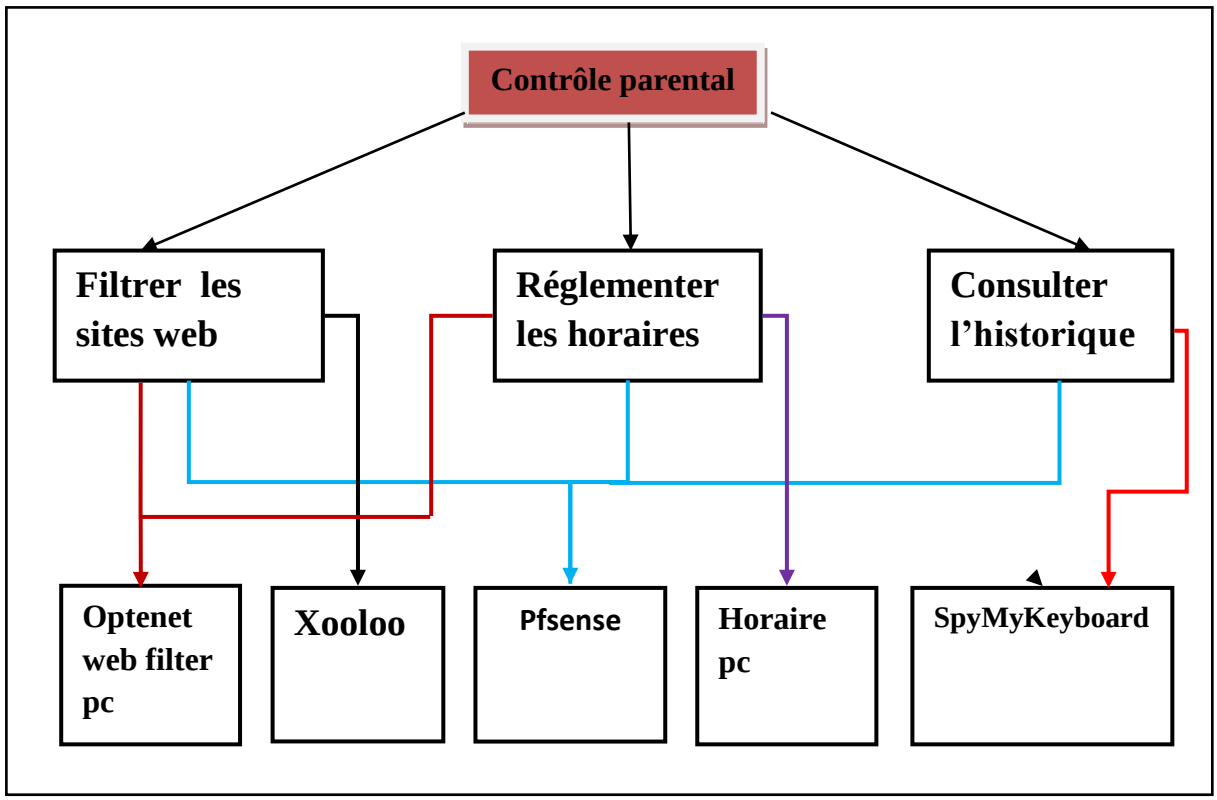



Figure II.1 Catégories du contrôle parental

## II.7 Conclusion

Dans ce chapitre, nous avons effectué des recherches sur les logiciels de contrôle parental, puis nous avons comparé entre eux selon leurs caractéristiques et leurs fonctionnalités et avons donc conclu que Pfsense est le plus performant d'entre eux, c'est pour cela que nous l'avons choisi pour effectuer ce travail.

## III.1 Introduction

Nous allons vous présenter dans ce chapitre, le logiciel que nous avons choisi pour effectuer ce projet, puis nous décrirons notre travail et présenterons quelques fonctionnalités de Pfsense à travers différents diagrammes.

## III.2 Description de notre travail

L'objectif de ce travail consiste à sécuriser et superviser un réseau domestique, afin de permettre aux parents de restreindre automatiquement l'accès de leurs enfants à Internet et pour cella que nous avons choisi Pfsense.

## III.3 Architecture global

La figure ci-dessous représente l'architecture globale de notre réseau domestique, elle comprend :

- un réseau local contenant un ordinateur qu'utilise l'administrateur (parent), ainsi que un ou plusieurs autres qu'utilisent les clients (enfants).
- un système Pfsense qui joue le rôle d'un firewall, protégeant le réseau LAN.
- Un modem relié au réseau WAN (internet).

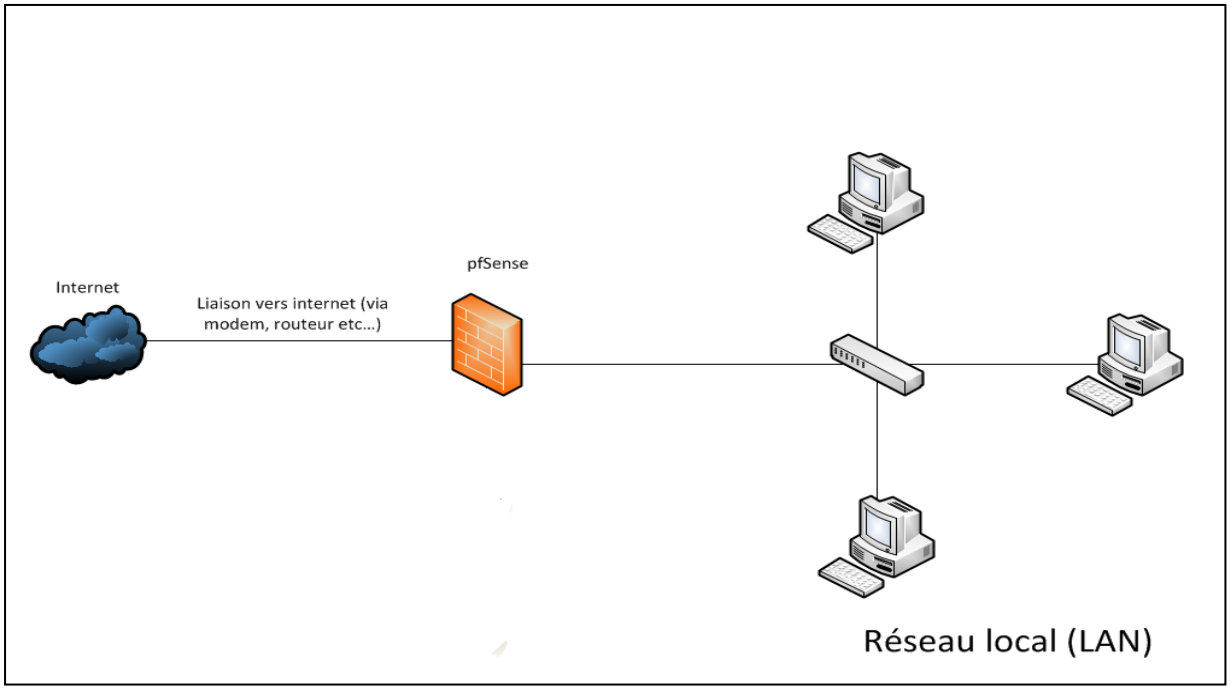



*FIGURE III. 1 Architecture du réseau domestique*

## III.4 Présentation de l'outil PfSennse

PfSense est un outil qui ne joue pas seulement le rôle d'un firewall, il offre toute une panoplie de services réseaux. Nous allons vous en présenter une partie, du moins la plus intéressantes.

- Pare-feu : indispensable pour une distribution "firewall".
- Table d'état: La table d'état contient les informations sur les connexions réseaux.
- Traduction d'adresses réseaux (NAT) : Permet de joindre une machine située sur le LAN à partir de l'extérieur. .
- Serveur DHCP.
- Serveur DNS et DNS dynamiques.

- Portail Captif.
- Redondance et équilibrage de charge.

Les logiciels s'installent grâce à un système de paquet, ils sont configurés pour s'intégrer à l'interface web. [25]

## III.5 Service de PfSense

### III.5.1 System

Cette section regroupe tous les utilitaires system, dont nous citerons [26]:

### a. Advanced

Représente les options avancées de PfSense comme l'accès SSH, les clés SSL, etc.

### b. Firmware

Cela permet de mettre à jour PfSense

### c. General Setup

Représente les configurations de base de PfSense rentrées lors de l'installation.

### d. Package

Il est possible d'installer de nouveaux paquets tels que MRTG (interface graphique à SNMP), Squid (serveur mandataire), etc.

### e. Setup Wizard

Le Setup Wizard est le guide rencontré au début de l'installation de PfSense. Il est possible de le refaire.

### f. Static Route :

Les routes statiques sont importantes lorsqu'une adresse réseau n'est pas « vue » par la passerelle.

### III.5.2 Interfaces

Il est possible de modifier l'attribution d'une interface à une carte réseau à l'aide de l'adresse MAC.

Les VLANs peuvent également y être gérés. [26]

### III.5.3 Pare feu

Parmi les sections qui permettent le paramétrage du firewall nousciterons [26] :

#### a. Aliases

Les alias permettent principalement d'associer un nom à une adresse d'hôte, un port, ou un réseau.

#### b. 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.

#### c. Schedules :

Schedule (planifier) correspond à un intervalle de temps dans le mois ou dans la journéePar exemple, l'accès Internet ne sera autorisé que de 9h à 19h.

#### d. Traffic Shaper :

Le Traffic Shaping permet de contrôler l'utilisation de la bande passante.

### III.5.4 Services

Plusieurs services peuvent être gérés par PfSense. Ils peuvent être arrêtés ou activés depuis cette interface, voici la liste de quelquesservices [26] :

- **Captive Portal** (portail captif)
- **DNS Forwarder** (transporte les DNS)
- **DHCP relay** (agent relais DHCP)
- **DHCP server** (serveur DHCP)
- **Dynamic DNS** (permet de rendre « statique » un DNS dynamique grâce à un nom)
- **Load Balancer** (répartition de charges)
- **RIP** (protocole de routage)
- **SNMP** (gérer des équipements réseaux à distance)
- **OpenNTPD** (gestion de l'horloge)
- **Wake on LAN** (permet à un ordinateur éteint d'être démarré à distance)

### III.5.5 VPN

Plusieurs catégories de VPN sont supportées par PfSense, parmi eux : Le VPN IPSec qui peut être utilisé en mode transport ou en mode tunnel, Il gère le protocole AH (Authentification) et ESP (Cryptage)et les autorités de certification. Le VPN OpenVPN gère les serveurs et les clients VPN. Il gère également les autorités de certification. [26]

### III.5.6 Status

L'onglet Status permet de voir l'état de PfSense. Nous pouvons par exemple vérifier si les interfaces sont actives,leurs adresses,voir l'état des connexions, arrêter ou lancer un service, etc. [26]

### III.5.7 Diagnostics

Cet onglet permet quelques fonctionnalités supplémentaires telles que : arrêter ou redémarrer PfSense, visualiser la table de routage, effectuer un « Ping », modifier des fichiers, revenir à une installation de PfSense neuve, etc.[26]

## III.6 Les diagrammes

Les diagrammes ci-dessous nous montrent les différentes fonctionnalités de Pfsense.

### III.6.1 Diagramme de cas d'utilisation

Les diagrammes de cas d'utilisation décrivent les services les plus importants rendus par un système, Partant des acteurs, participants externes qui interagissent avec le système, Un cas d'utilisation peut être divisé endiagrammes de séquence, qui détaillent les différentes fonctions du cas d'utilisation. [27]

Dans notre cas, nous avons uniquement un acteur qui utilise le système pour accomplir plusieurs taches, comme illustré dans la figure ci-dessous

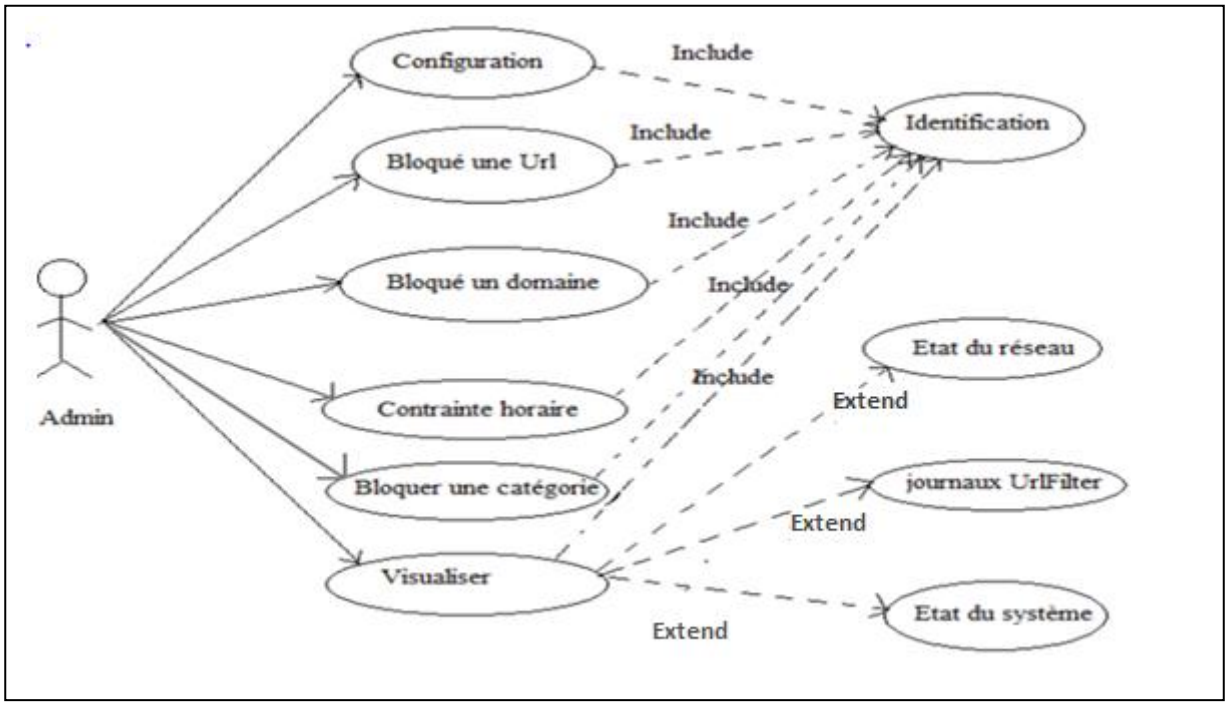



*Figure III.2- Diagramme de cas d'utilisation*

### III.6.2 Diagramme de séquence

Les diagrammes de séquence présentent la coopération entre différents objets. Les objets sont définis et leur coopération est représentée par une séquence de messages entre eux. [28]

Les figurent qui suivent représentent les différents diagrammes de séquence pour le cas d'utilisation.

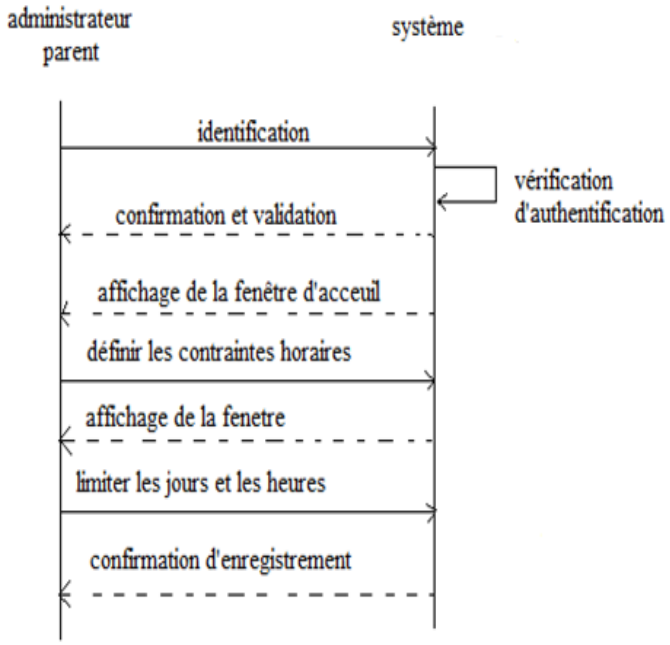



*Figure III.3- Diagramme de séquence « Contraintes horaires»*

La figure ci-dessus nous montre les différentes interactions effectuées entre l'administrateur et le système Pfsense, le parent s'identifie, puis demande de limiter les jours et les heures, et enfin le système confirme l'enregistrement.

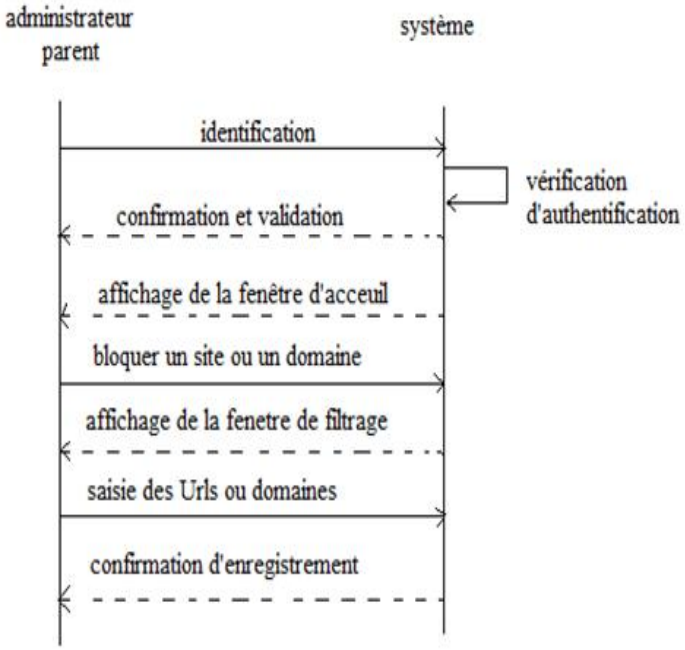
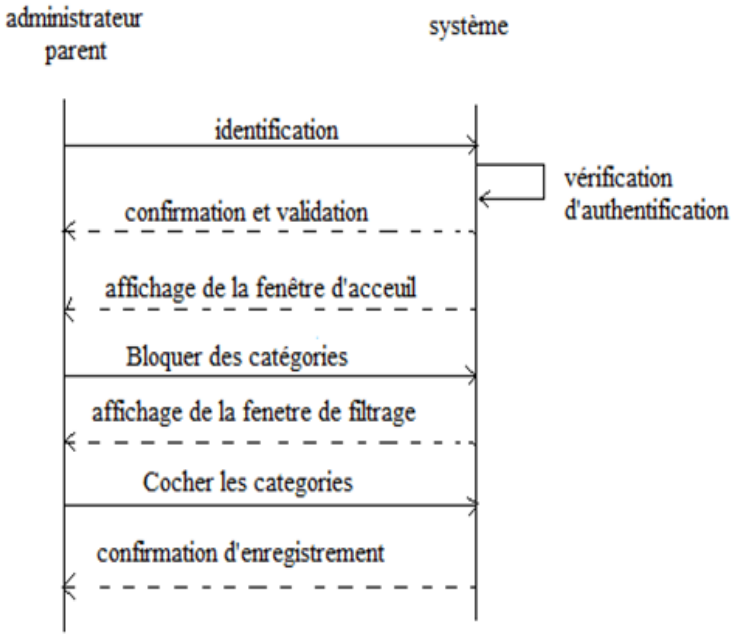



*Figure III.4- Diagramme de séquence « Filtrer un site ou un domaine »*

La figure ci-dessus représente le diagramme de séquence dans le cas de filtrage d'un site ou d'un domaine, elle nous montre les coopérations faites entre l'administrateur et Pfsense, âpres s'être identifié, l'administrateur demande de bloquer un site ou un domaine, le système lui affiche la fenêtre de filtrage, et enfin l'administrateur saisi les Urls ou domaines à bloquer.

.




*FigureIII.5– Diagrammedeséquence «Bloquerunecatégorie »*

Le diagramme ci- dessus nous montre les coopérations faites entre l'administrateur et le système dans le cas de blocage d'une catégorie, âpres s'être identifié, l'administrateur demande de bloquer une ou plusieurs catégorie, le système lui affiche la fenêtre de filtrage, l'administrateur coche une ou plusieurs catégories, enfin le système met à jour, confirme et enregistre.

## III.6.3 Diagramme d'activité

Un diagramme d'activité permet de modéliser le comportement du système, dont la séquence des actions et leurs conditions d'exécution.

Nous allons représenter les différents diagrammes ci-dessous et essayer de les expliquer en quelques mots.[29]

## a. Diagramme d'activité « Identification »

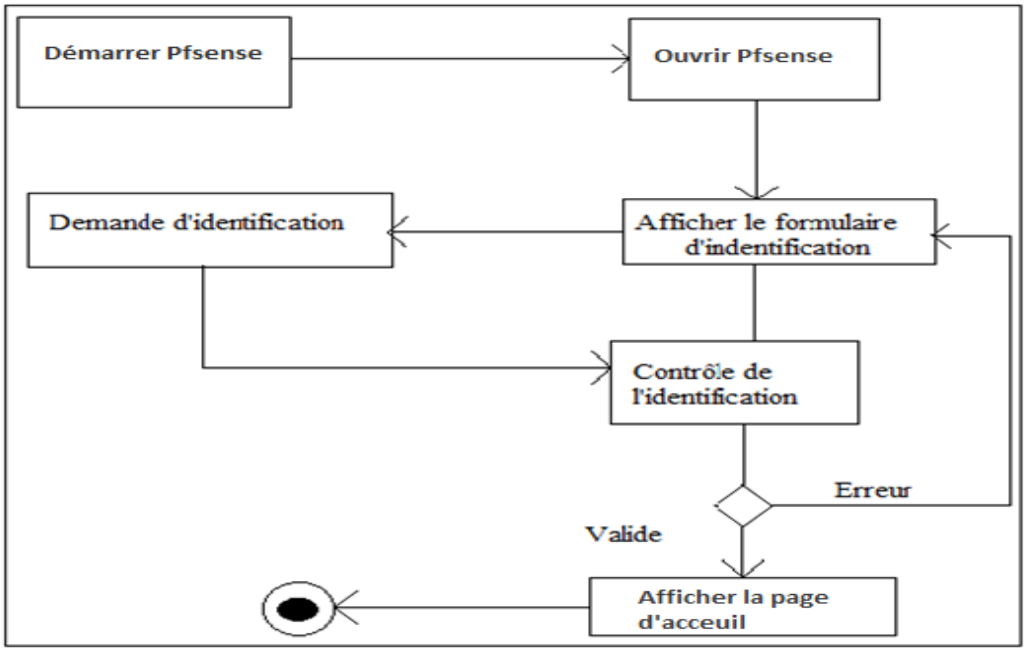



*Figure III.6- Diagramme d'activité « Identification »*

Le diagramme ci-dessus nous décrit les démarches du système lors de l'identification de l'administrateur, âpres avoir démarré Pfsense, le système affiche le formulaire d'identification, l'administrateur saisi ses données, le système vérifie si les informations sont correctes, si c'est le cas, il affiche la page d'accueil sinon il renvoie un message d'erreur et réaffiche le formulaire.

**b. Diagramme d'activité « Filtrer des URLs ou domaines »**

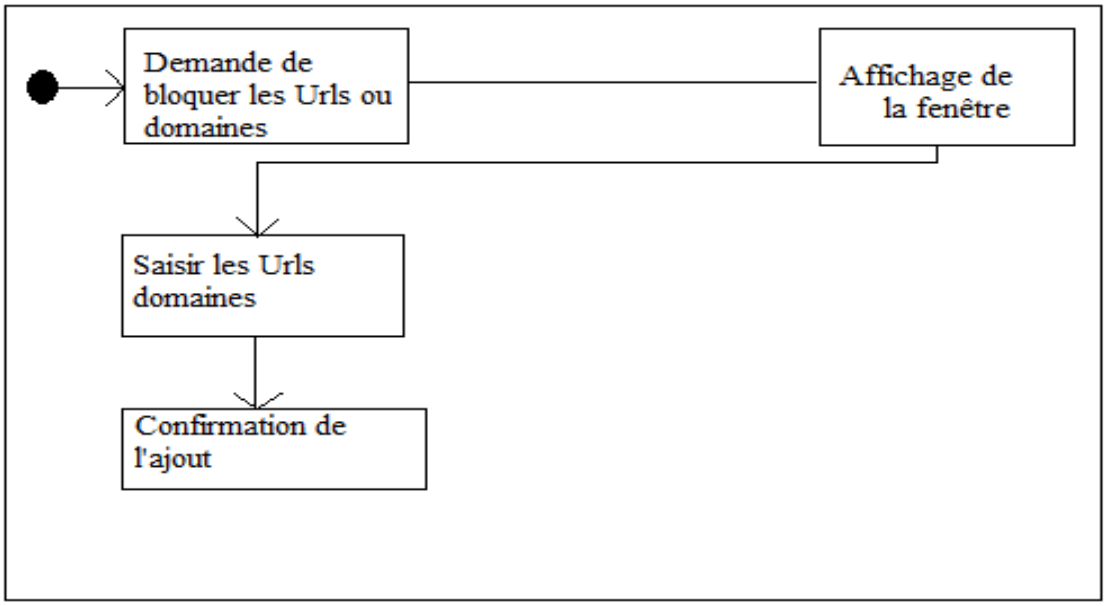



*Figure III.7- Diagramme d'activité « Filtrer des URLs ou domaines »*

**c. Diagramme d'activité « Autoriser ou interdire l'accès a un client »**

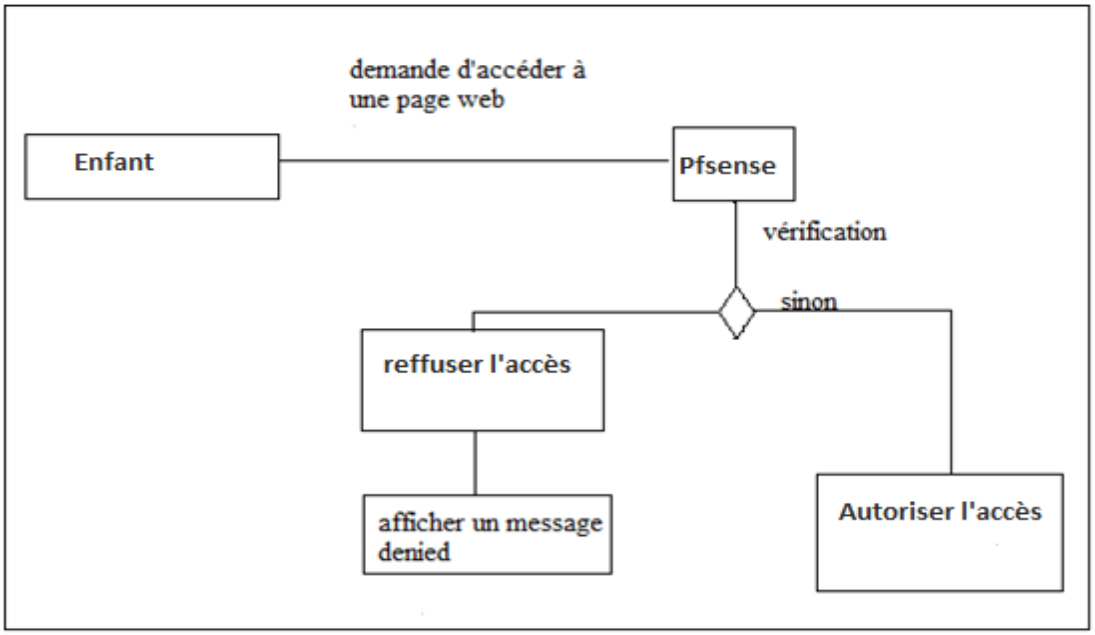



*Figure III.8- Diagramme d'activité « Autoriser ou interdire l'accès a un client »*

La figure ci-dessus nous montre comment procède Pfsense lorsqu'un enfant veut se connecter a une page web, cette requête passe d'abord par Pfsense qui va vérifier si

la page web est bloquée, si c'est le cas le système affiche un message d'erreur, sinon l'enfant accède simplement a la page web.

## III.7 Conclusion

Dans ce chapitre, nous avons présenté Pfsense et avons décrit notre travail ainsi que ses différentes fonctionnalités, en donnant l'architecture globale de notre réseau et les différents diagrammes correspondants, c'est une étape qui nous permet de mieux connaitre Pfsense, afin d'entamer sa configuration et son test dans le prochain chapitre.

## IV.1 Introduction

Nous allons présenter dans ce chapitre la phase de réalisation de ce projet, nous présenterons donc les pré-requis utilisés afin de configurer PfSense, ainsi que les étapes de son installation et de sa configuration.

## IV.2 Pré requis

L'installation est réalisée sur une machine virtuelle depuis VirtualBox, la procédure d'installation est la même si vous êtes sur une machine physique.

En termes de configuration requise, nous faisons tourner Pfsense sur une machine virtuelle disposant d'un processeur, 512 Mo de RAM et 8Go de disque, ce qui est empellement suffisant pour Pfsense.

L'architecture se compose d'un serveur ou ordinateur disposant d'au moins deux cartes réseaux, une pour l'interface LAN (du côté du réseau local) et l'autre pour l'interface WAN (du côté du réseau relié à internet),

Le clavier français est en azerty, vous aurez donc besoin de connaître l'emplacement des touches du clavier anglais (qwerty) car lors de l'installation et la configuration via la ligne de commande le clavier est en qwerty. Et malheureusement même en modifiant les options lors de l'installation le clavier azerty n'est pas pris en compte

## IV.3 Obtention de l'outil « PfSense »

Les différentes versions de pfSense sont téléchargeables dans la rubrique «download» du site www.pfSense.org

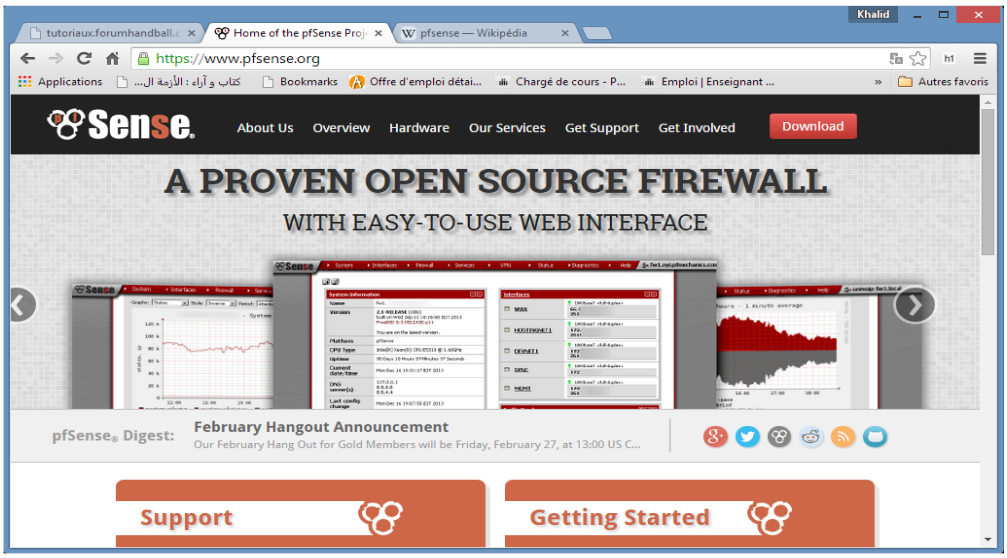



*Figure IV.1 « site de téléchargement »*

Cliquer ensuite sur le lien *here on the mirrors*

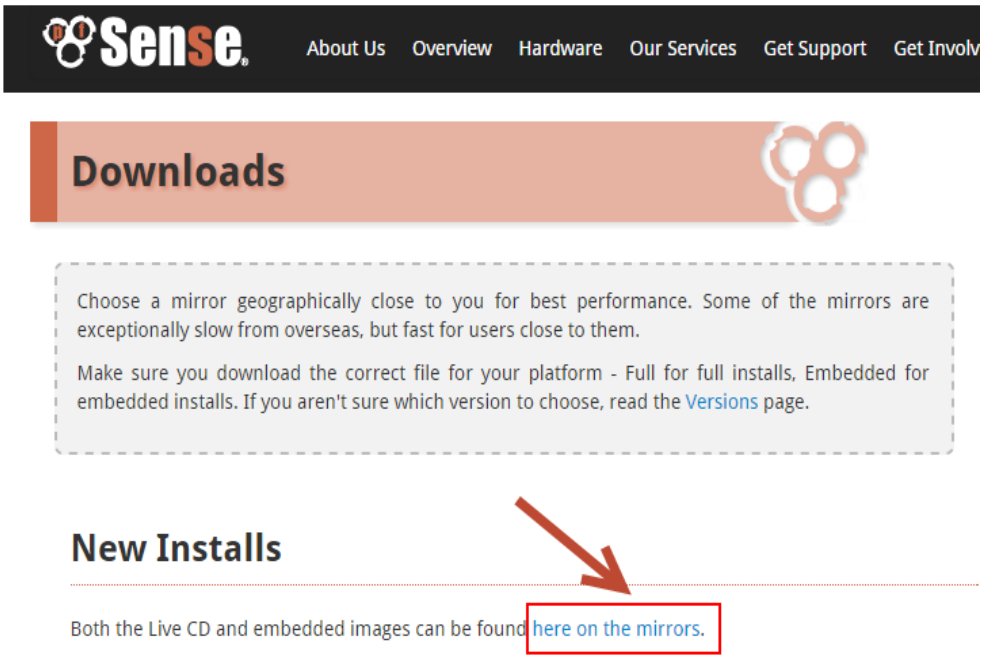



*Figure IV.2 « Lien de téléchargement »*

Choisir l'image dont nous avons besoin selon notre architecture matérielle. Puis choisir l'emplacement du dépôt contenant l'image choisit.

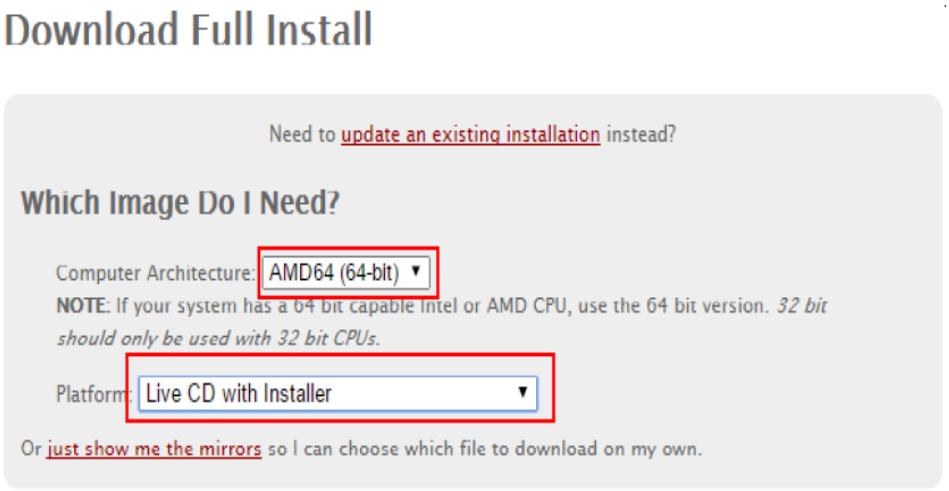



*Figure IV.3 « Choix de l'image»*

## IV.4 Les étapes d'installation de Pfsense

Taper 1 pour choisir le boot pfSense ou laisser démarrer avec l'option par défaut.

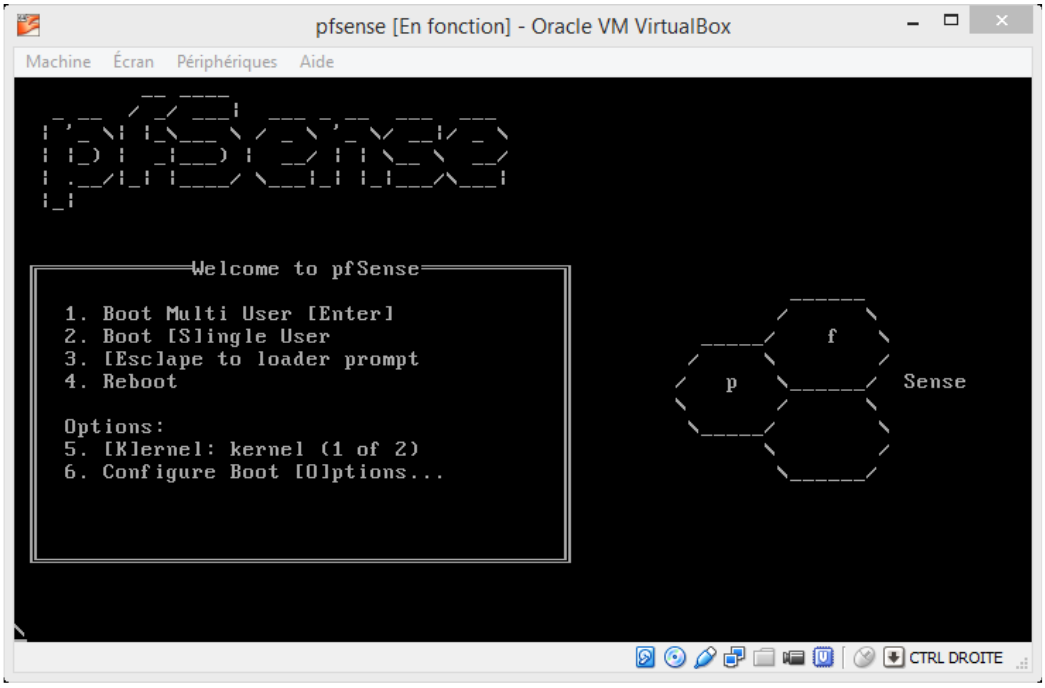



*Figure IV.4 « Pfsense sur virtualbox»*

Pour lancer l'installation, presser « I » à l'invite.

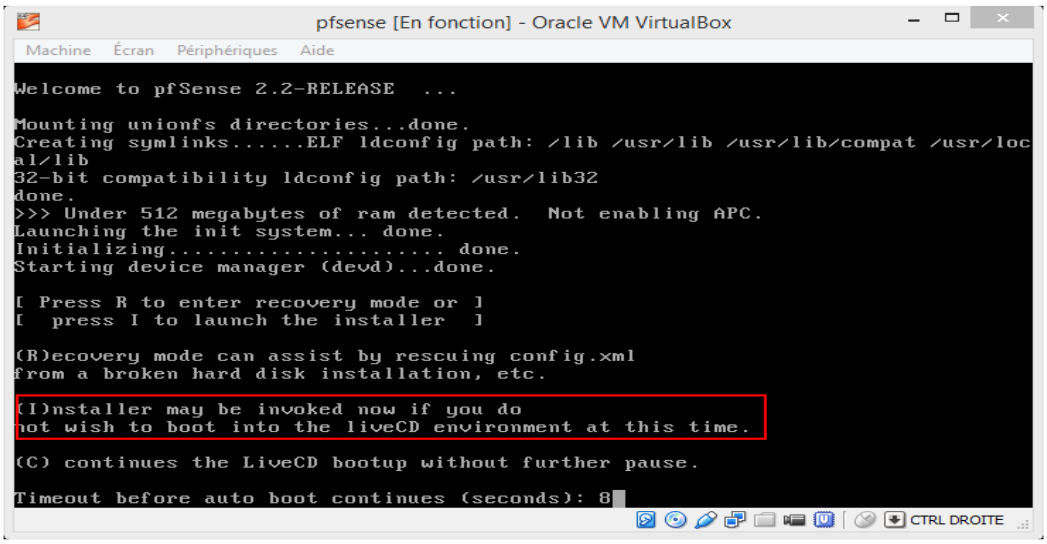



*Figure IV.5 « Lancement de l'installation »*

Choisir l'option « **99** » pour lancer l'installation de pfsense sur le disque.

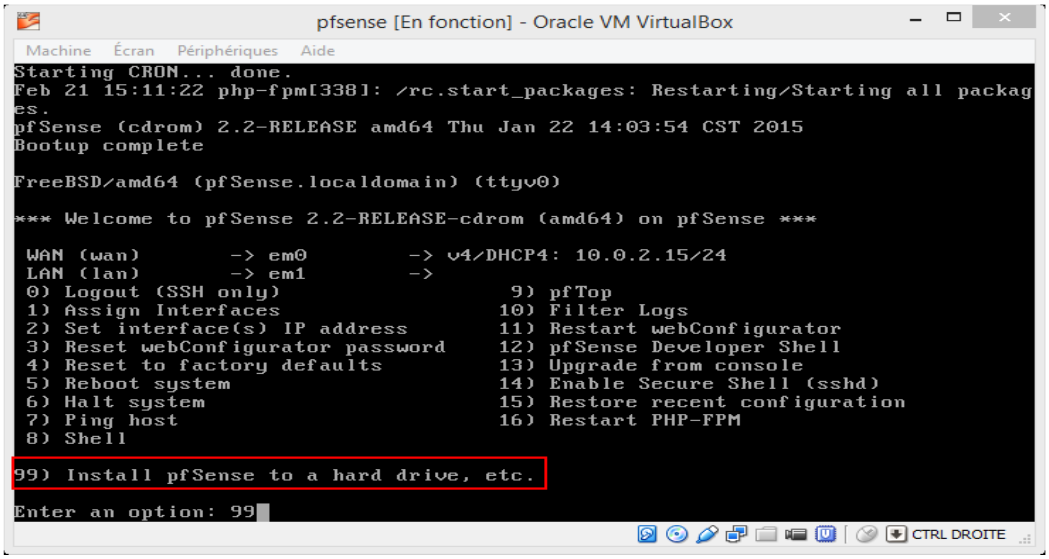



*Figure IV.6 «Choix de l'option »*

Accepter les choix en descendant sur *Accepte these Settings* puis valider

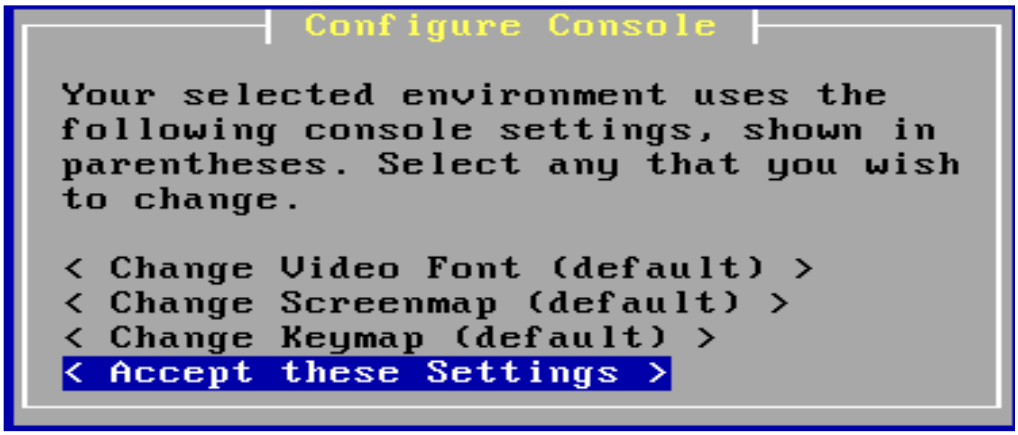



*Figure IV.7 « Acceptation de l'installation »*

Opter pour une installation facile puis confirmer à l'écran suivant.

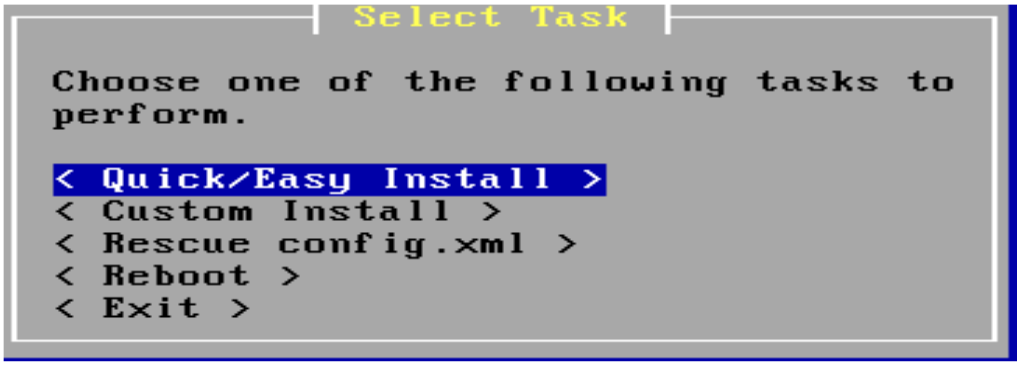



*Figure IV.8 « Installation facile »*

L'installation du noyau: laisser le choix par défaut puis valider.

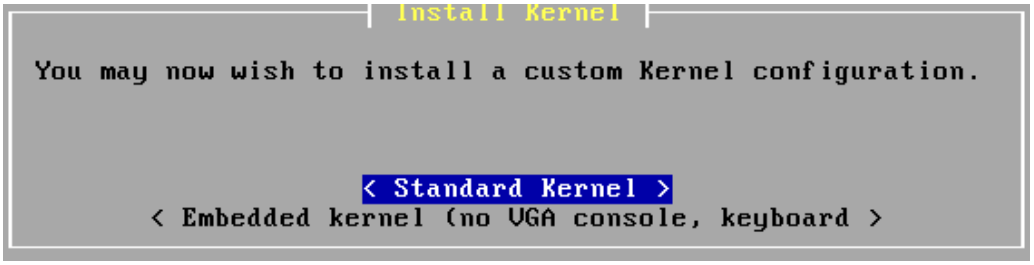



*Figure IV.9 « Installation du noyau »*

« Rebooter » lorsqu'on y est invités.

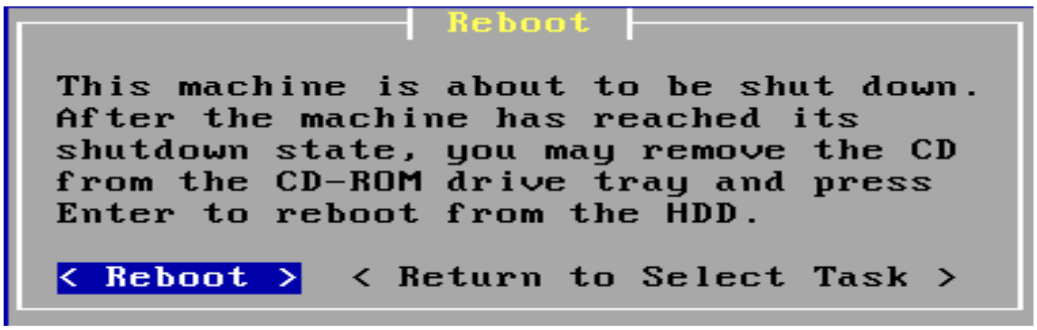



*Figure IV.10 « Rebooter »*

- **Configuration des interfaces réseau**

Dans notre cas « em0 » correspond à l'interface WAN par contre em1 correspond au LAN qu'il faudra configurer. Entrer « **2** » pour lancer la configuration IP d'une interface

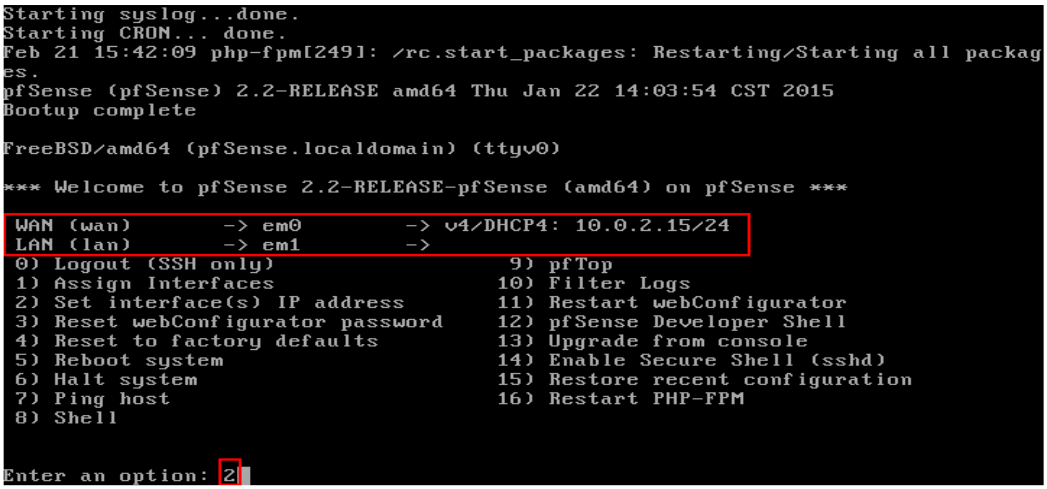



*Figure IV.11 « Configuration des interfaces »*

Puis choisir le numéro de l'interface à configurer

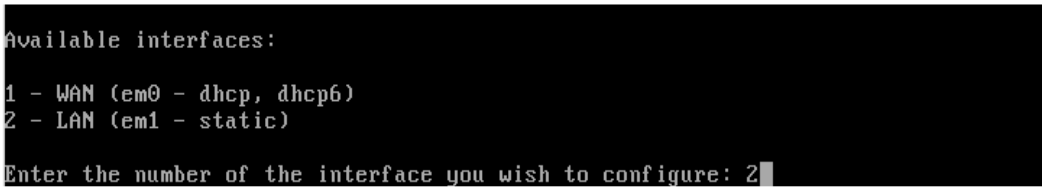



*Figure IV.12 « Choix de l'interface à configurer »*

Répondre aux questions pour configurer l'interface: adresse IP via DHCP ou adresse IP, nombre de bits de sous-réseau etc.

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

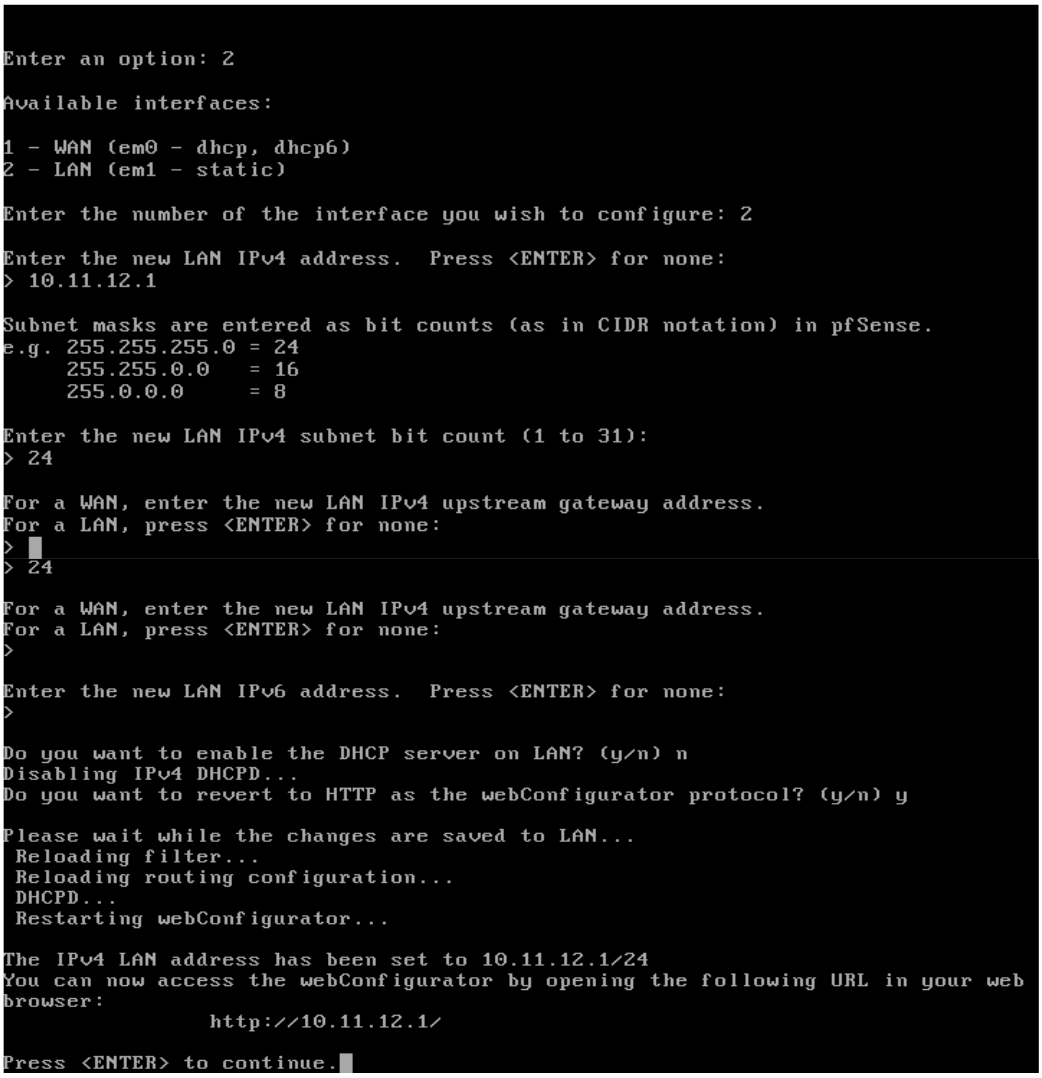



*Figure IV.13 « Choix de configuration »*

Notre interface LAN est maintenant configurée :

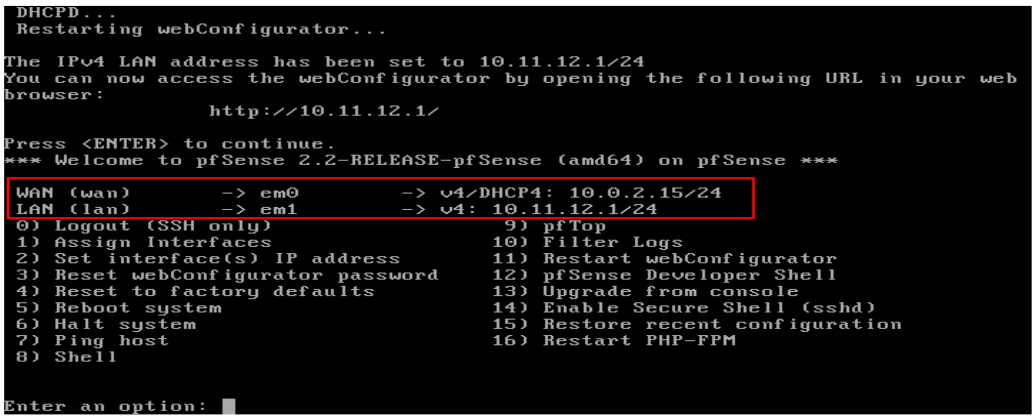



*Figure IV.14 « Fin de la configuration de LAN »*

Nous pouvons accéder à l'interface Web de *pfsense* à partir d'une machine se trouvant sur le réseau natif LAN du *pfsense* (par exemple un poste Windows 7 ayant l'adresse IP 10.11.12.2/24).

## IV.5 Configuration de Pfsense

### IV.5.1 Methodes d'acces a Pfsense


*Figure IV.15 « Accès en mode interface graphique »*

Dés la saisi du nom d'utilisateur et du mot de passe, la page d'accueil de PfSense s'affiche

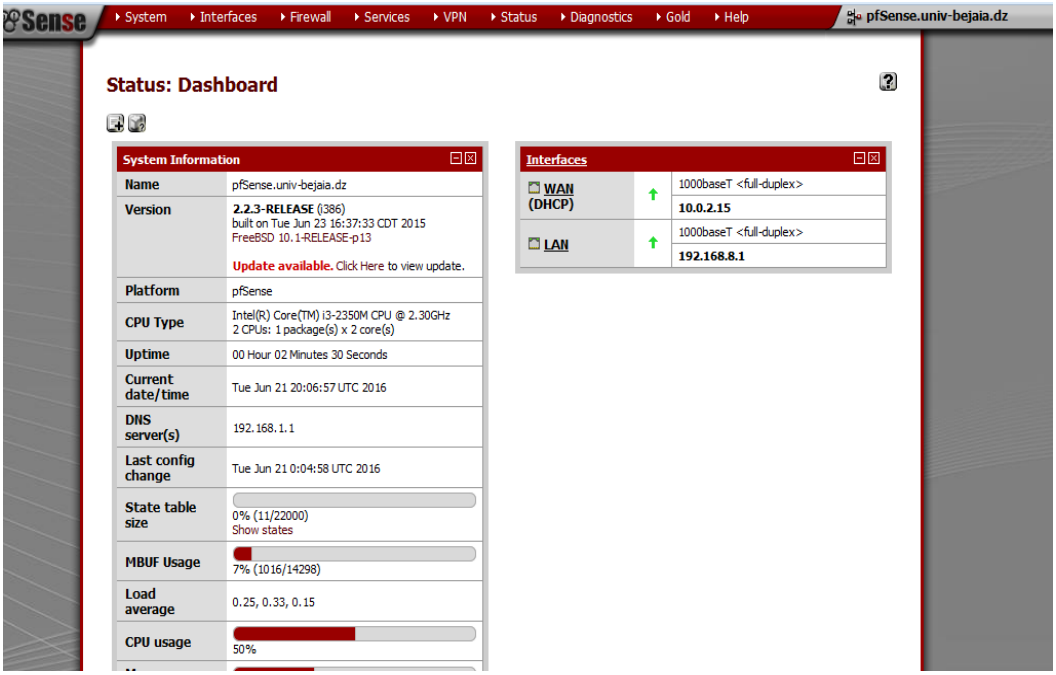



Figure IV.16 « Page d'accueil Pfsense »

## IV.5.2 Configuration du serveur DNS

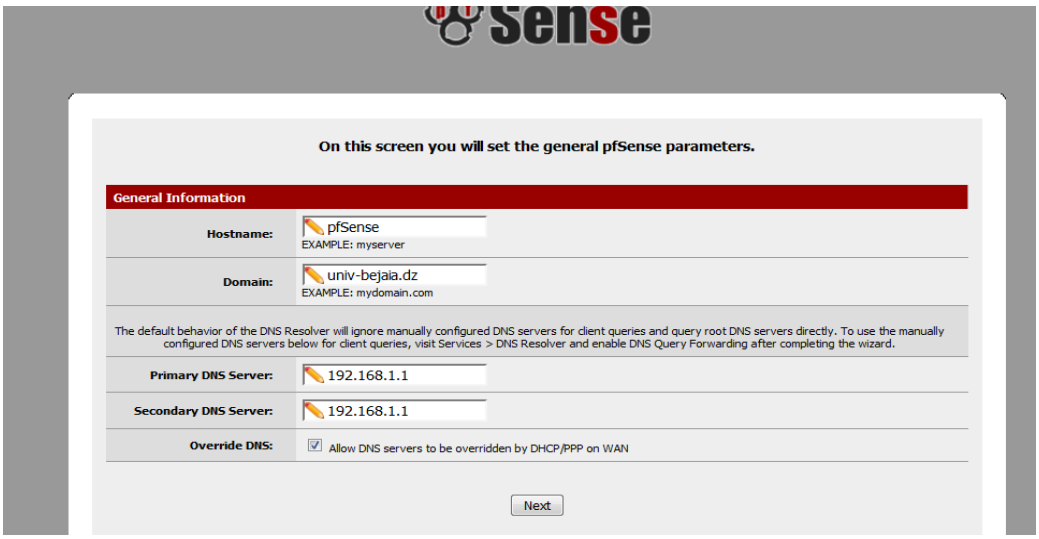



*Figure IV.17 « Serveur DNS »*

## IV.5.3 Activation du serveur proxy

Nous allons mettre en place un serveur proxy, avec Squid, lui adjoindre des fonctions avancées de filtrage avec SquidGuard, et même en faire un proxy transparent avec l'aide d'IPtables.

### a. Installation des packages

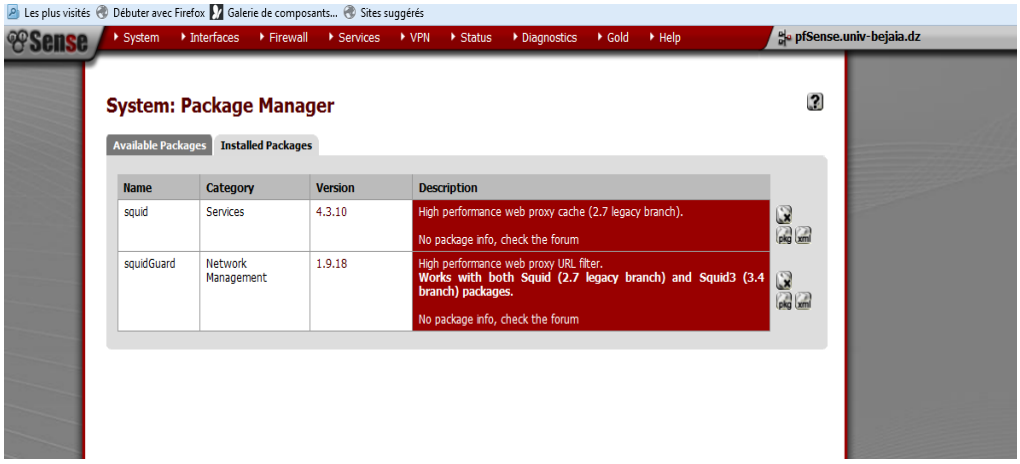



*Figure IV.18 « Installation de squid et squidguard »*

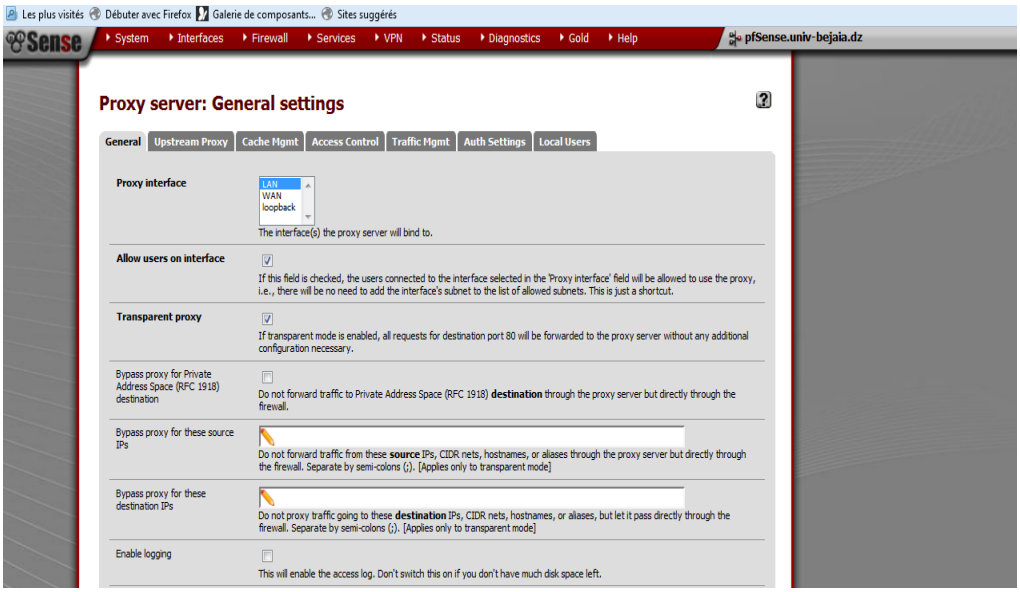



*Figure IV.19 «Activation du serveur proxy »*

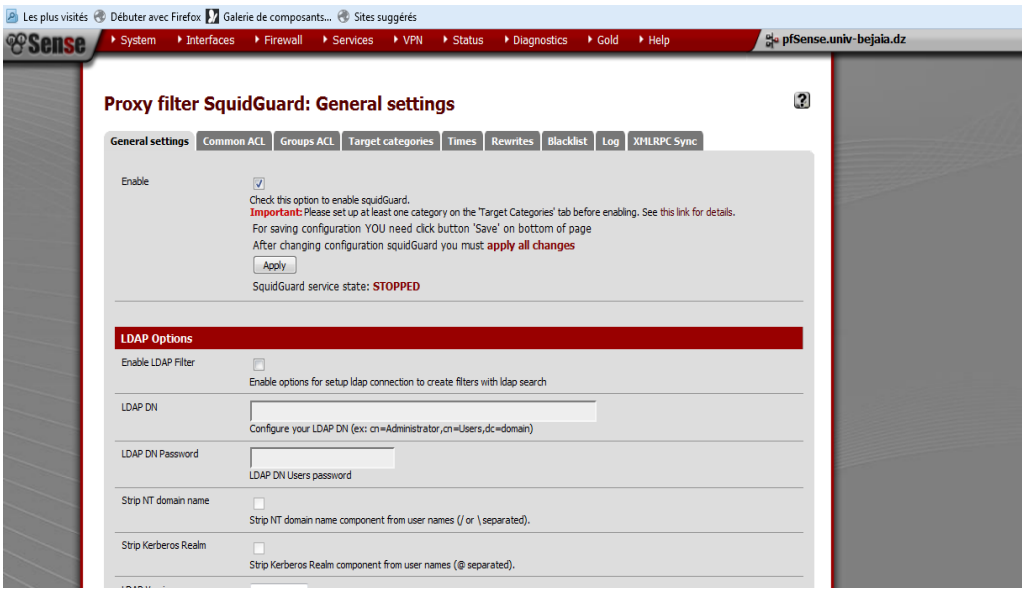



*Figure IV.20 «Activation de squidguard »*

## b. Activation des logs

Les logs nous permettent de voir tous ce qui passe par Pfsense

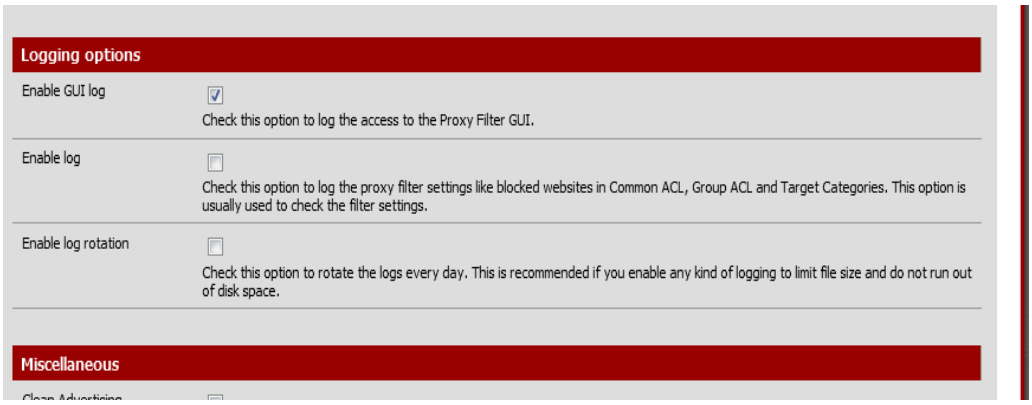



*Figure IV.21 « Activation des logs »*

## IV.5.4 Configuration de l'UrlFilter

### a. Catégorie de blocage

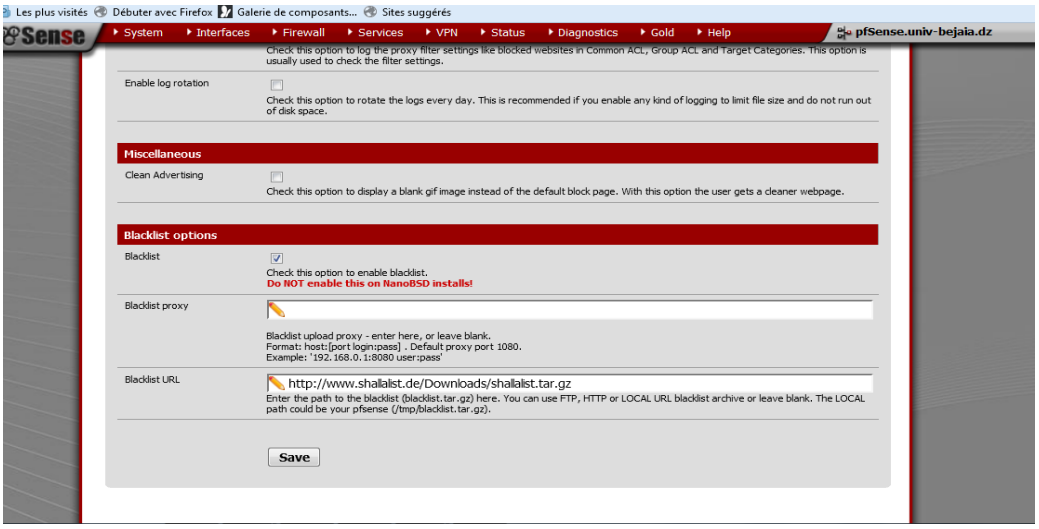



*Figure IV.22 « maintenance des blacklists »*

- **Installation de blacklist shalla :**


*Figure IV.23 « Catégorie de blocage »*

Les catégories peuvent être bloquées en liberant l'acces à toutes les categories puis en choisissant ALLOW dans DEFAUL ACCESS[ALL] et enfin bloquer les catégories souhaitées en mettant DENY, comme nous pouvant faire le contraire.

## b. Blacklist personnalisée

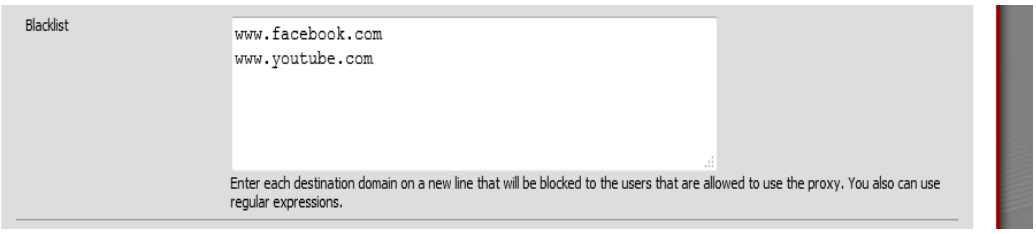
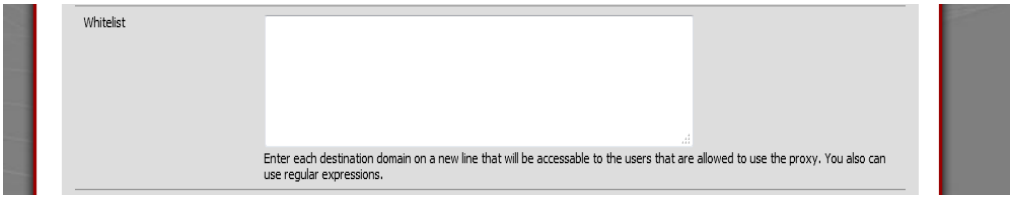


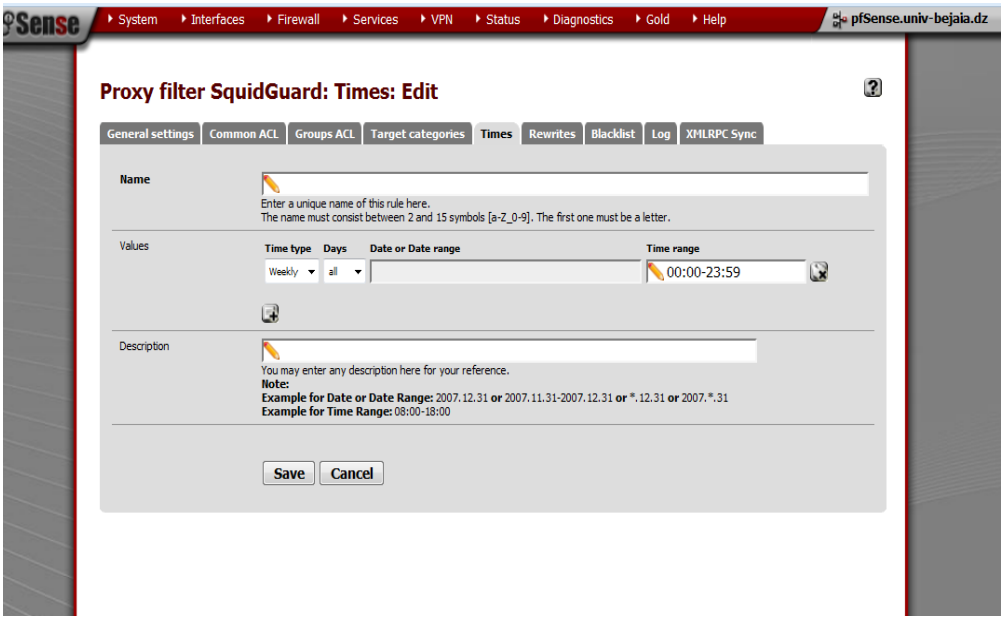
*Figure IV.24 « Blacklists personnalisées »*

### c. Whitelist personalisée




*FigureIV.25 « whitelists personnalisées »*

## IV.5.6 Contrôle d'acces basé sur le temps




*FigureIV.26 « Restriction de temps »*

## IV. Conclusion

Dans ce chapitre, nous avons présenté les pré-requis utilisés afin de configurer Pfsense, puis nous avons expliqué a travers diverses captures, les étapes de son installation et de sa configuration, a travers les quelles nous définissons quelques fonctionnalités que propose cet outil.

# *Conclusion Générale*

Ce projet concerne la supervision des mineurs dans un réseau domestique, en clair c'est la mise en place d'un système permettant aux parents de Controller l'accès de leurs enfants à internet.

Au terme de cette réalisation nous avons rencontré quelques problèmes liés notamment à la non disponibilité de la machine qui héberge PfSense, dotée justement de deux cartes réseaux dont nous aurons besoin, ce qui nous a mené à utiliser des cartes réseaux virtuelles.

Nous avons mis en œuvre une architecture ayant différentes fonctionnalités et qui répond aux besoins de l'utilisateur tout en gérant les différentes sécurités exigées

Des options peuvent être envisagées afin de rendre notre travail plus complet, notamment au niveau de la sécurité informatique des ordinateurs, nous espérons que ce travail fera preuve d'inspiration afin d'être complété.

[1][ http://www.memoireonline.com/04/12/5604/m_Monitoring-dune-infrastructure-informatique-sur-base-doutils-libres14.html] [29/06/2016]

[2][ https://www.hadopi.fr/sites/default/files/page/pdf/ReseauLocal.pdf ] [29/06/2016]

[3] [ http://www.technologuepro.com/reseaux/Chapitre1-reseaux-locaux.htm ] [29/06/2016]

[5][http://www.commentcamarche.net/contents/612-routeur-equipement-reseau] [29/06/2016]

[6][http://www.futura-sciences.com/magazines/high-tech/infos/dico/d/internet-firewall-474/][29/06/2016]

[7][ http://www.commentcamarche.net/faq/17453-qu-est-ce-qu-un-proxy ] [29/06/2016]

[8][http://www.blog.saeeed.com/2010/05/internet-definition-historique-applications-de-l-internet/ [29/06/2016]

[9][http://www.definitions-marketing.com/definition/reseaux-sociaux/][29/06/2016]

[10][http://www.anthonyharmant.com/111-glossaire-definition-chat.html] [29/06/2016]

[11][https://fr.wikipedia.org/wiki/Jeu_en_ligne] [29/06/2016]

[12]http://www.witigo.eu/controle-parental/les-dangers-d-internet[29/06/2016]

[13]http://www.lemonde.fr/technologies/chat/2009/02/09/reseaux-sociaux-de-nouveaux-dangers-pour-nos-enfants_1151995_651865.html [29/06/2016]

[14][http://www.internetsanscrainte.fr/s-informer/qu-est-ce-que-le-controle-parental-comment-ca-marche]. [29/06/2016]

[15][http://www.commentcamarche.net/faq/24542-test-comparatif-de-logiciels-de-controle-parental ] [29/06/2016]

[16][ http://www.peo60.fr/ordi60/les-precedentes-saisons-ordi60/saison-5-ordi60-2012-2013/le-controle-parental/ ] [29/06/2016]

[17][ http://www.lelogicielgratuit.com/logiciel/horaire_pc/ ] [29/06/2016]

[18][http://www.horaire-pc.com/[29/06/2016]

[19][https://www.xooloo.com/fr/controle-parental/] [29/06/2016]

[20][http://www.commentcamarche.net/faq/24542-test-comparatif-de-logiciels-de-controle-parental[29/06/2016]

[21][http://www.toucharger.com/fiches/windows/spymykeyboard-keylogger/62839.htm [29/06/2016]

[22][http://www.easycommander.com/telecharger/spymykeyboard ] [29/06/2016]

[23][http://www.calexium.com/fr/pfsense-le-logiciel.html ] [29/06/2016]

[24][ http://www.jetelecharge.com/Internet/5330.php ] [29/06/2016]

[25][ http://www.generation-linux.fr/index.php?post/2009/11/30/Presentation-de-pfSense ] [29/06/2016]

[26] [LAGARDE yannick Manuel d'installation et d'utilisation du logiciel pfsense ] [29/06/2016]

[27][http://support.objecteering.com/objecteering6.1/help/fr/objecteering_uml_modeler/diagrams/use_case_diagrams.htm ] [29/06/2016]

[28][http://support.objecteering.com/objecteering6.1/help/fr/objecteering_uml_modeler/diagrams/sequence_diagrams.htm ] [29/06/2016]

[29][http://docwiki.embarcadero.com/RADStudio/Berlin/fr/D%C3%A9finition_des_diagrammes_d'activit%C3%A9s_UML_2.0 ] [29/06/2016]

[30] [http://www.01net.com/telecharger/windows/Securite/controle-parental/fiches/43602.html ] **[29/06/2016]**

[31][ https://fr.wikipedia.org/wiki/R%C3%A9seau_%C3%A9tendu ] [29/06/2016]

# Résumé :

Ce présent travail porte  sur le contrôle d'accès des mineurs à internet dans un réseau domestique, il a pour objectif de permettre  aux parents de mener à bien le contrôle du contenu web de leurs enfants, en particulier ceux inappropriés

Il s'agit de mettre une configuration sur le réseau domestique grâce à l'outil « Pfsense » qui joue le rôle d'un pare feu afin de bien mener la surveillance et la sécurité de leur réseau.

« VirtualBox »  a été utilisé pour mener l'installation de Pfsense virtuellement.



**Mots clés :** réseaux domestique, contrôle parental, PfSense, VirtualBox.



# Abstract:

This present work deals with the access control of minors to Internet in a home network, it aims to enable parents to carry out the web content control their children, especially those inappropriate

This is putting a setup on the home network through the " Pfsense " tool that acts as a firewall to properly conduct surveillance and security of their street-network .

« VirtuelBox » was used to conduct the PfSense installation virtually.



**Keywords:** domestic networks, parental control, PfSense, VirtualBox.