Ministère des Enseignements Secondaire et Supérieur
(**MESS**)

---

Secrétariat Général

---

Université Polytechnique de Bobo-Dioulasso (**U.P.B.**)

---

Ecole Supérieure d'Informatique (**E.S.I**)

Cycle des Ingénieurs de Travaux Informatiques (**C.I.T.I**)
Option : Réseaux et Maintenance Informatiques (**RéMI**)

# Rapport de fin de cycle

**THEME** : « Etude et mise en place d'un portail captif sur le réseau de l'Université Polytechnique de Bobo-Dioulasso : Cas du Campus Numérique Francophone Partenaire »

*Période du 06 Aout au 05 Novembre 2013*

**Auteurs** : Salifou KONANE & Zakaria KINDA

**Maître de stage**

M. SANON Dramane Edmond

Responsable du CNFP

**Superviseur**

Dr PODA Pasteur

Enseignant chercheur à l'ESI

Année académique : 2012-2013

# DEDICACE

*Nous dédions ce rapport*

*A nos très chères familles qui ont toujours été là pour nous soutenir tout au long de nos études et qui nous ont donné un magnifique modèle de labeur et de persévérance. Nous espérons qu'elles trouveront dans ce travail toute notre reconnaissance et tout notre amour*

# REMERCIEMENTS

Nous remercions très sincèrement :

- L'École Supérieure d'Informatique pour nous avoir donné cette formation ;
- Dr Pasteur PODA, notre superviseur, pour ses encouragements, sa disponibilité et ses remarques pertinentes et enrichissantes ;
- M. Dramane E. SANON, le responsable du CNFP ; notre maître de stage grâce à qui ce stage a été possible au CNFP et pour ces précieux apports, sa sincérité et sa disponibilité ;
- Mme OUATTARA/OUEDRAOGO Alizèta, intérimaire de l'assistante documentaliste au CNFP pour sa disponibilité et sa sympathie ;
- Nos amis qui nous ont toujours soutenus dans nos différentes tâches ;
- Nos camarades d'école avec qui nous avons passé tout ce temps à l'ESI pour leur collaboration.

Et enfin nous rendons grâce à DIEU TOUT PUISSANT qui nous a permis de tenir jusqu'à ce jour.

# GLOSSAIRE

**AP** : Access Point

**CARP** : Common Address Redundancy Protocol

**CPU** : Central Processing Unit

**DMZ** : Demilitarized Zone

**DHCP** : Dynamic Host Configuration Protocol

**DNS** : Domain Name Service

**FAI** : Fournisseur d'Accès à Internet

**FTP** : Foiled Twisted Pair

**HTTP** : HyperText Transfer Protocol

**HTTPS** : HyperText Transfer Protocol Security

**HTML** : HyperText Markup Language

**IP** : Internet Protocol

**LAN** : Local Area Network

**MAC** : Medium Access Control

**NFS** : Network File System

**NTP** : Network Time Protocol

**NAT** : Network Address Translation

**NAS** : Network Access Server

**PPTP** : Point-to-Point Tunneling Protocol

**PHP** : Hypertext Preprocessor

**RADIUS** : Remote Authentification Dual-In User Service

**RAM** : Random Access Memory

**SSL** : Secure Sockets layers

**SSH** : Secure Shell

**STP** : Shielded Twisted Pair

**TCP** : Transfer Control Protocol

**UDP** : User Datagram Protocol

**UTP** : Unshielded Twisted Pair

**VPN** : Virtual Private Network

**WIFI** : Wireless Fidelity

**WAN** : Wide Area Network

# LISTE DES TABLEAUX

# LISTE DES FIGURES

# AVANT-PROPOS

L'Ecole Supérieure d'Informatique (ESI) est l'une des écoles que compte l'Université Polytechnique de BOBO-DIOULASSO. Créée en 1991 dans le but d'accompagner le Burkina Faso dans son ambition de s'approprier les technologies de l'information et de la communication (TIC), l'ESI est la seule école supérieure d'informatique publique du pays. Elle forme des ingénieurs de travaux informatiques en Analyse et Programmation (AP), et en Réseaux et Maintenance Informatiques (RéMI) ; des ingénieurs de conceptions ainsi que des étudiants en cycle de DEA informatique. Les étudiants en fin de Cycle des Ingénieurs de Travaux Informatiques (CITI) doivent effectuer un stage pratique d'au moins Trois (3) mois dans une entreprise, lequel stage est sanctionné à la fin par une soutenance publique. Le stage de fin de cycle en RéMI met l'accent sur une réalisation concrète pour laquelle l'étudiant met en place un protocole de travail bien déterminé. Les thèmes proposés impliquent une étude approfondie dans les domaines balayés par les réseaux et maintenance informatiques.

C'est ainsi que nous avons effectué, du 06 août au 05 novembre 2013, au Campus Numérique Francophone Partenaire de Bobo-Dioulasso (CNFP), un stage pratique au cours duquel nous avons développé un projet de fin d'étude pour lequel le présent document tient lieu de rapport.

# TABLE DES MATIERES

# INTRODUCTION GENERALE

Selon les statistiques mondiales [1], huit burkinabè sur mille sont utilisateurs d'Internet (en 2008). Ce chiffre a quasiment triplé en 2012. Cet engouement à l'utilisation des TIC impose une augmentation de l'offre des services Internet. En effet, bon nombre de cette population disposent aujourd'hui d'un appareil mobile (portable, PDA, Smartphone, ...) et souhaitent pouvoir accéder à Internet dans la majorité des lieux qu'ils fréquentent. Dans cette optique, l'expansion très rapide des points d'accès sans-fil permet la connexion des appareils nomades. Néanmoins chaque réseau possède sa politique d'accès et ne souhaite pas laisser n'importe qui accéder aux ressources réseaux et plus particulièrement les ressources Internet qui sont très limitées.

Ainsi, il est nécessaire de mettre en place des systèmes d'authentification sur ces réseaux qui doivent cumuler de multiples avantages. Ces avantages sont entre autres : une compatibilité avec la majorité des appareils mobiles du marché, une sécurité des échanges entre les clients et le reste du réseau, une plus grande transparence offerte à l'utilisateur aussi bien lors de la phase d'authentification que lors de l'utilisation du réseau, une réduction de l'impact au niveau des ressources matérielles et de la bande passante, etc.

Face à ces enjeux, le portail captif s'est imposé comme une solution fréquemment utilisée dans les points d'accès payants ou non. Il peut se généraliser à tous les modes d'accès (sans-fil ou filaire) nécessitant un contrôle d'accès.

L'Université Polytechnique de Bobo-Dioulasso (UPB) dispose d'un réseau informatique dont la gestion se complique avec la diversité et le nombre croissant des utilisateurs d'où la nécessité de mettre en place un portail captif. L'étude et la mise en place d'une telle solution sera effectuée dans sa première phase sur le réseau du Campus Numérique Francophone Partenaire (CNFP). Elle sera par la suite généralisée à tout le réseau de l'UPB. Ce document synthétise nos travaux menés dans ce cadre et est organisé en cinq chapitres.

Le premier chapitre de ce document présente la structure d'accueil, le thème d'étude ainsi que le contexte dans lequel s'inscrit le stage. Le deuxième chapitre est consacré à l'analyse du système informatique de la structure d'accueil; ce qui permettra de l'évaluer afin de proposer une solution bien adaptée. L'étude générale des portails captifs fait l'objet du troisième chapitre ; ce qui nous permettra de choisir la solution à implanter. Le quatrième chapitre est consacré à l'étude technique de l'outil PFsense et le cinquième chapitre détaille la mise en œuvre pratique et technique de la fonction captive de PFsense.

# Chapitre I :

## PRESENTATION DU PROJET

Le projet de portail d'accès captif est de créer une passerelle entre un réseau interne et le réseau Internet. La finalité est de pouvoir déployer la solution dans toutes les structures de l'Université Polytechnique de Bobo-Dioulasso.

Le portail sera doté de fonctionnalités d'authentification qui permettent d'identifier les usagers du service à des fins de traçabilité. Il sera équipé d'un système de filtrage d'adresses internet, ce qui permettra ainsi d'éviter l'utilisation des sites indésirables. Un filtrage applicatif sera également mis en place afin de limiter l'utilisation de certains logiciels.

Le dernier aspect important réside dans l'utilisation optimale de la bande passante, la sécurisation des connexions et la centralisation des données d'authentification.

## I.1. Structure d'accueil et contexte

L'Université polytechnique de Bobo-Dioulasso (UPB) est une université publique du Burkina Faso. Son site principal est situé dans le village de Nasso, à une quinzaine de kilomètres de Bobo-Dioulasso, dans la région des Hauts-Bassins. Elle est constituée de six établissements d'enseignement supérieur et de recherche ayant en leur sein plusieurs départements ouvrant sur des spécialités diverses. Ces établissements sont placés chacun sous la responsabilité d'un directeur assisté d'un directeur adjoint. Ce sont :

- l'École Supérieure d'Informatique (ESI) ;
- l'Institut Universitaire de Technologie (IUT) ;
- l'Institut du Développement Rural (IDR) ;
- l'Institut des Sciences de la Santé (INSSA) ;
- l'Unité de Formation et de Recherche en Science et Technique (UFR/ST) ;
- l'Unité de Formation et Recherche en Sciences Juridique, Politique, Économique et de Gestion (UFR/SJPEG).

L'Université dispose aussi de trois écoles doctorales.

L'UPB est une université nationale qui a pour mission l'élaboration et la transmission de la connaissance par la formation des hommes et des femmes afin de répondre aux besoins de la Nation. Cette mission s'entend dans le cadre de la politique de décentralisation de l'enseignement supérieur du gouvernement burkinabè et de la conquête du marché de l'emploi, la formation des cadres dans les filières professionnalisantes pour plus de productivité dans les secteurs socio-économiques et culturels. Pour y parvenir l'UPB s'assigne les objectifs suivants :

- former des cadres dans tous les domaines en général et dans les filières

professionnalisantes en particulier ;

- conduire des activités de recherches scientifiques et en vulgariser les résultats ;
- élever le niveau technique, scientifique et culturel des étudiants pour une ouverture sur le marché de l'emploi et les secteurs de production ;
- délivrer des titres et diplômes ;
- valoriser les compétences dans tous les secteurs d'activité du pays.

Pour l'atteinte de ces objectifs l'utilisation des TIC/TICE est plus que nécessaire et l'UPB, pour mettre à profit ces TIC/TICE, s'est dotée d'une direction pour la promotion des Technologies de l'information et de la communication. En plus de cette direction, l'UPB dispose d'un Campus numérique francophone partenaire (CNFP), fruit d'une convention de partenariat avec l'Agence universitaire de la francophonie (AUF). C'est précisément au CNFP que s'est déroulé notre stage. Le CNFP met à la disposition du public différents services informatiques tels l'accès à Internet, l'accès à la documentation, la commande d'articles scientifiques en ligne, les formations ouvertes et assistées à distance, des formations grand public, etc.

En outre, le CNFP œuvre à la promotion des logiciels libres. Le CNFP désire optimiser l'utilisation des ressources réseaux comme l'accès à Internet, car celles-ci sont généralement limitées si l'on veut assurer une meilleure qualité du service. En effet, vu le nombre et la diversité des utilisateurs leur demande en ressources s'accroît et leur gestion se complique davantage. Ainsi c'est dans un objectif d'amélioration des services réseaux de l'UPB en général, et du contrôle d'accès au réseau du CNFP en particulier que s'inscrit ce projet.

## I.2. Présentation du thème

### I.2.1 Problématique

Le réseau du CNFP, comme n'importe quel autre réseau n'est pas sans faille en termes de sécurité car ses utilisateurs sont de diverses origines.

En effet, bien que moderne, l'accès au réseau sans fil du CNFP se fait par authentification par adresse MAC, et celui au filaire par la détention d'un compte valide (identifiant/mot de passe) sur les poste fixes. Cela reste insuffisant quand on sait qu'il existe de nos jours des logiciels qui arrivent à contourner l'authentification par adresse MAC. L'authentification par adresse MAC a aussi cette particularité de ne pas permettre une gestion efficace des utilisateurs car, hormis l'autorisation d'accès au réseau, on ne saurait qui est réellement connecté, quelle est la

cause de la politique d'authentification déjà existante. En outre, l'authentification par le filaire autorise la connexion des machines externes à la structure ; c'est-à-dire qu'un utilisateur qui venait brancher sa machine personnelle à partir d'un câble du réseau, pouvait se connecter sans qu'il ne lui soit demandé de s'authentifier. Ce qui n'est pas sans risque car un utilisateur mal intentionné pourrait contourner facilement l'authentification d'où une remise en cause de la politique d'accès. Ainsi l'évolution du nombre croissant d'utilisateurs Wi-Fi et le contrôle d'accès de tous les utilisateurs font apparaître l'impératif de mise en place d'un système d'authentification transparent et simple d'utilisation. Voilà autant de problèmes auxquels nous avons apporté une solution grâce à cette étude de portail captif.

### I.2.2 Résultats attendus

Prévu au départ pour être déployé sur toute l'Université, nous avons dû revoir cette proposition initiale en concertation avec nos encadreurs. En effet, nous avons restreint la mise en œuvre pratique de la solution sur le réseau du CNFP pour des contraintes liées à l'architecture globale du réseau de l'UPB. L'objectif principal de ce projet est d'implanter une solution technique permettant d'authentifier les utilisateurs et de partager de façon sécurisée l'accès Internet, d'où le déploiement d'une solution de portail captif.

D'après le cahier de charge qui nous a été soumis, l'achèvement de ce projet doit permettre aussi au campus numérique de rendre effectif ce qui suit:

- se doter d'un outil d'authentification libre issu du monde des logiciels libres ;
- pour se connecter, les clients n'ont besoin que d'un navigateur Web, d'un login et d'un mot de passe ;
- les paramètres du compte sont stockés dans une base de données existante et les comptes déjà existants doivent pouvoir être utilisés ;
- toutes les requêtes web des clients doivent être automatiquement redirigées sur la page d'authentification ;
- l'authentification des clients et des administrateurs doit se faire de façon sécurisée ;
- le point d'accès doit être totalement transparent pour le client ;
- l'accès au portail captif et par ricochet au web doit être indépendant du système d'exploitation du client ;
- de même, les utilisateurs du réseau du CNFP ne doivent pas être pénalisés pendant le déploiement ;

- le système doit permettre à l'administrateur d'optimiser l'utilisation de la bande passante; c'est-à-dire que l'administrateur peut par exemple limiter la bande passante au niveau de chaque utilisateur pour éviter que celle-ci soit surchargée ou il peut même filtrer des sites indésirables (téléchargements torrents, peer to peer, sites pornographiques ...).

Pour atteindre ces objectifs le portail captif est une solution candidate.

### I.2.3 Organisation du projet

Pour bien mener ce projet, l'élaboration d'un plan de travail s'avère nécessaire. Ce plan décrit les différentes tâches à réaliser et le rôle de chaque responsable impliqué au niveau des ressources humaines. En effet un groupe de pilotage constitué du superviseur et du maître de stage assure les activités administratives, le suivi et la fourniture des besoins du projet. Le groupe de projet constitué des stagiaires que nous sommes a pour rôle d'effectuer la partie technique du projet. Il est assisté dans ses tâches par le groupe de pilotage. Ainsi les différentes tâches réalisées au cours de ce projet ainsi que leurs responsabilités sont consignées dans le tableau I.1.

**Tableau I.1 : Organisation des activités**

| Phases | Tâches | Périodes | Responsabilités |
|---|---|---|---|
| Etude de l'existant | Information sur la structure, analyse des solutions actuelles, discussion du thème proposé | Deux semaines | Groupe de projet et groupe de pilotage |
| Recherche de solution | Etude du thème, comparaison de solutions, choix d'une solution et de l'architecture à mettre en place | Quatre semaines et deux jours | Groupe de projet |
| Mise en place de la solution | Acquisition des besoins, implantations de la solution et rédaction du rapport | Cinq semaines | Groupe de projet et groupe de pilotage |

# Chapitre II :

# ETUDE DU SYSTEME INFORMATIQUE EXISTANT

Toute révision, modification ou action visant à apporter des améliorations au système informatique du CNFP doit passer par une connaissance préalable de l'ensemble des différents éléments constituant l'architecture de son système informatique existant. L'analyse de l'existant a pour but à la fois d'évaluer le niveau de performance et de disponibilité de l'infrastructure réseau, et de déterminer quelles améliorations peuvent être apportées afin de la rendre plus performante tout en facilitant sa gestion.

## II.1. État des ressources du système informatique

### II.1.1 Les ressources matérielles

Le matériel qui constitue actuellement le système informatique du CNFP peut se présenter comme suit:

- **des postes de travail :** Ce sont les ordinateurs fixes du réseau à partir desquels les utilisateurs accèdent à leurs sessions. Ils sont listés dans le tableau II.1.

**Tableau II.1 : les postes de travail et leurs caractéristiques**

| Type de poste | Marque | Caractéristiques Matérielles | Nombre | État |
|---|---|---|---|---|
| PC bureau moyen tour | Transtec | HDD: 250GB<br>RAM: 2GB<br>CPU: Intel Core Duo CPU E7400 @2.8GHz*2<br>ECRAN: 17 | 06 | 06 en fonctionnement |
| PC bureau moyen tour | Transtec | HDD: 250GB<br>RAM: 4GB<br>CPU: Pentium(R) Dual-Core CPU E6500 @2.93GHz*2<br>ECRAN: 17 | 14 | 14 en fonctionnement |

- **des serveurs :** Les serveurs matériels sont généralement des ordinateurs de plus grande capacité que les stations de travail ordinaires et disposent de mémoire importante pour traiter simultanément les nombreuses tâches actives ou résidantes en

mémoire. Les serveurs ont également besoin d'espace disque pour stocker les fichiers partagés et pour servir d'extension à la mémoire interne du système. Les cartes système des serveurs nécessitent des connecteurs d'extension pour y connecter des périphériques partagés, tels que des imprimantes et plusieurs interfaces réseau. En résumé ce sont des ordinateurs qui ont une grande puissance de traitement et qui sont très robustes afin d'assurer la disponibilité des services réseau. A titre indicatif, un serveur peut rester en marche pendant toute une année sans être éteint. Le tableau II.2 récapitule les serveurs du CNFP.

**Tableau II.2 : Liste des serveurs matériels et caractéristiques techniques**

| Type de poste | Marque | Caractéristiques Matérielles | Nombre | État |
|---|---|---|---|---|
| Serveur | Transtec CALLEO 121 Server | DD : 500Go<br>RAM : 2Go, DDR2<br>CPU : Intel Xeon Quad-Core<br>Année d'acquisition : 2009 | 01 | En fonctionnement |
| Serveur | transtec CALLEO 121 Server | DD : 500Go<br>RAM : 3Go, DDR2<br>CPU : Intel Xeon Quad-Core<br>Année d'acquisition : 2009 | 01 | En fonctionnement |

- **du matériel de visioconférence :** Le CNFP dispose d'un système de visioconférence constitué d'un moniteur et d'un codec.
- **des imprimantes et scanners :** Outils bureautiques par excellence, les imprimantes peuvent constituées aussi des nœuds d'un réseau. Les imprimantes et scanners sont recensés dans le tableau II.3.
- **les équipements d'interconnexions** : Ce sont les éléments du réseau qui relient plusieurs nœuds. Ils sont répertoriés dans le tableau II.4.
- **le câblage :** Le câblage constitue le support physique de transmission du réseau. Il est essentiellement réalisé avec de la paire torsadée FTP, STP, UTP Fast Ethernet de catégorie 5E et de la fibre optique.

**Tableau II.3 : Liste des imprimantes et quelques caractéristiques techniques**

| Type d'imprimantes | Marque | Caractéristiques matérielles | Nombre | État |
|---|---|---|---|---|
| Imprimante Réseau | HP laserJet 1300 | 500 feuilles | 01 | En fonctionnement |
| Imprimante simple | HP | Imprimante, Scanner, Copieuse, Fax | 01 | En fonctionnement |
| Scanner | HP Scan Jet 5590 | 2400*4800ppp/48-bits | 01 | En fonctionnement |

**Tableau II.4 : Équipements réseau et caractéristiques techniques**

| Type d'équipement | Marque | Caractéristiques matérielles | Nombre | Etat |
|---|---|---|---|---|
| Switchs | D-LINK DES-104R | 10/100 Fast Ethernet, 24 ports | 01 | En fonctionnement |
| | D-LINK DGS1216T | 08 ports | 01 | |
| | D-LINK | 10/100 Fast Ethernet, 08 ports | 02 | |
| Modem LS | NOKIA | - | 01 | En fonctionnement |
| Modem ADSL | D-LINK | DSL-520B | 01 | En fonctionnement |
| Routeur | CISCO 1900 Séries | Gigabits/carte HWIC | 01 | En fonctionnement |
| Router sans fil (firewall intégré) | 3COM | 54 Mbps | 01 | En fonctionnement |

### II.1.2 Les logiciels

Il s'agit ici de faire l'inventaire des logiciels installés ainsi que des différents services installés.

- **Les systèmes d'exploitation et logiciels d'application :** Ils sont représentés dans le tableau II.5.

**Tableau II.5 : Systèmes d'exploitation et logiciels d'application**

| Types | Noms | Supports |
|---|---|---|
| Système d'exploitation serveur | DEBIAN 6.0 | Postes serveurs |
| Système d'exploitation client | Ubuntu 10.04 LTS | Tous les postes clients |
| Bureautique | OpenOffice.org | Postes clients |

- **Les services :** Avant de dresser le tableau (tableau II.6) des services installés, il convient d'expliquer et d'expliciter ce que c'est qu'un service réseau. Les serveurs matériels définis un peu plus haut sont des machines conçues pour recevoir des applications (logiciels) appelées **applications serveur** qui permettent aux autres postes du réseau (machines clientes) d'accéder à des ressources (imprimantes, fichiers partagés...) ou à des applications clientes. C'est donc par le terme de services qu'on désigne les applications installées.

**Tableau II.6 : Services installés**

| Service installé | Description |
|---|---|
| Admincompte | Serveur de gestion de compte d'utilisateur développé par l'AUF pour les CNF |
| Backuppc | Serveur de sauvegarde |
| CUPS | Serveur d'impression réseau |
| Connexion Internet | Partage de la connexion Internet à tous les postes connectés au réseau |
| DHCP | Serveur d'attribution dynamique d'adresses IP |
| DNS | Serveur de nom de domaine |
| FTP | Protocole de transfert de fichiers |
| libnss+mysql | Serveur d'authentification+gestion dynamique des utilisateurs |
| Messagerie+antivirus+antispam | Serveur de messagerie et protection antivirus |
| miroir local | Dépôt local |
| Mrtg | Serveur de monitoring du trafic réseau |
| NFS-kernel-server | Serveur de partage de fichiers sous linux |
| netboot (tfpd-hpa, pxe...) +udpcast | Serveur permettant l'installation de système d'exploitation en réseau local à partir du dépôt local. |
| SQUID | Serveur proxy |
| web (www, phplist, roundcube) | Serveur web |

### II.1.3 Le réseau

- **Plan d'adressage :** Le réseau du CNFP est subdivisé en quatre (04) sous-réseaux. Ce type de répartition est fréquent dans de nombreux réseaux et présente plusieurs avantages. Le plan d'adressage du réseau peut être représenté dans le tableau II.7.

**Tableau II.7 : Aperçu de l'adressage**

| Sous réseau | Hôte | Adresse | Commentaire |
|---|---|---|---|
| 212.52.149. y/x | Routeur "Onatel" | 212.52.149. x | Cisco 1900 Series |
| - | Serveur nfs-bobo | 212.52.149. x | - |
| - | Serveur mail-bobo | 212.52.149. x | - |
| - | Serveur Vz www-bobo et miroirs-bobo | 212.52.149. x | hébergé sur mail-bobo |
| - | Polycom Visio-bobo | 212.52.149. x | - |
| 192.168.0. y/x | - | - | Zone privée machines du CNFP |
| 192.168.1. y/x | - | - | Zone privée pour le Centre de calcul |
| 192.168.2. y/x | - | - | Zone privée pour le wifi |

- **Architecture :** Le réseau du CNFP est un réseau répondant aux normes Ethernet de topologie étoilée. Son architecture peut être représentée la figure II.1.

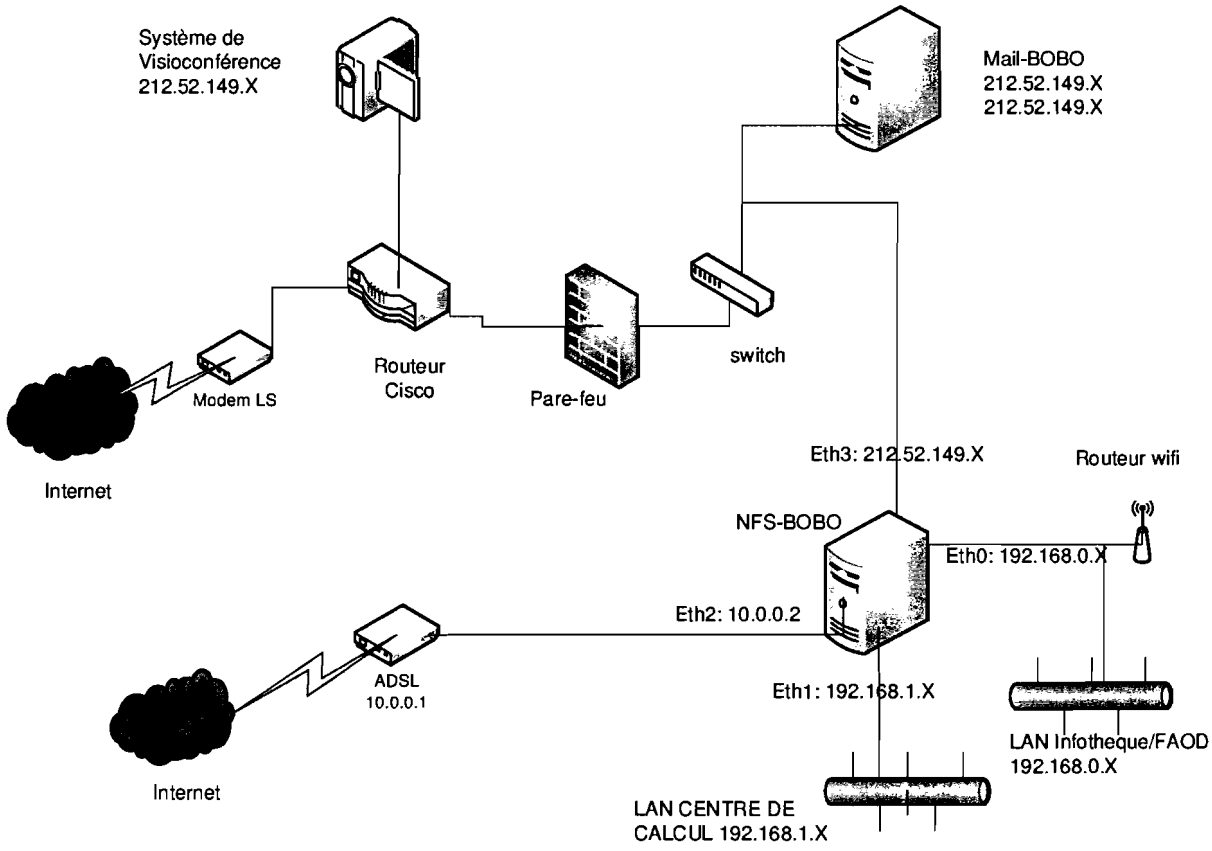


**Figure II.1 : Schéma du réseau actuel**

- **Récapitulatif des serveurs et services installés :** Il s'agit de l'emplacement des différents services sur les serveurs. Ils sont représentés dans le tableau II.8.

**Tableau II.8 : Tableau récapitulatif des services installés**

| serveur | Distribution | Noyau | Backup (*) | Services | Commentaire |
|---|---|---|---|---|---|
| **mail-bobo** | Debian GNU/Linux 6.0 | 2.6.26- 2 openvz-amd64 | Backupc sur dd externe . | DNS principal, messagerie+antivirus+antispam (exim...) + mysql, backuppc | Transtec CALLEO 121 Server, Processeur Intel Xeon Quad-Core, 3GoDDR2, DD 500Go, Année d'acquisition: 2009 |
| **nfs-bobo** | Debian GNU/Linux 6.0 | 2.6.26-2-amd64 | Backuppc sur dd externe à partir de mail-bobo | nfs, libnss-mysql+mysql, dns secondaire, dhcp, SQUID, admincomptes, mrtg, netboot (tfpd-hpa, pxe.)+udpcast | Transtec CALLEO 121 Server, Processeur Intel Xeon Quad-Core, 3GoDDR2, DD 500Go, Année d'acquisition: 2009 |
| **www-bobo** | Debian GNU/Linux 6.0 | 2.6.26-2-amd64 | Backuppc sur dd externe à partir de mail-bobo | Web (www, phplist, roundcube), ftp, mysql, miroir local | Serveur Virtuel OpenVZ VEID 102, installé sur mail-bobo |

## II.2. Analyse critique du système

Afin de mieux appréhender le système, il convient de savoir où résident ses forces pour en déduire ses faiblesses. Ce qui permettra d'apporter des améliorations aux éventuelles failles.

### II.2.1 Aspects positifs du système

Sur le plan physique nous avons apprécié positivement le système informatique du CNFP sur les points suivants :

- **existence d'une charte d'utilisation des outils informatiques** : Cela permet d'informer l'utilisateur sur ses marges de manœuvre, le dissuade de toute tentative d'outrepasser ses droits d'utilisateur et l'observation des règles élémentaires de sécurité car ne dit-on pas que 90% des risques sont le fait des utilisateurs internes ;
- **installation électrique** : des prises de terre et des onduleurs permettent la protection de l'équipement informatique contre les pics de courant, les surtensions et la sauvegarde de données après une interruption électrique. Le réseau électrique interne est protégé par des goulottes et séparé des câbles réseaux: ce qui épargne des risques d'électrocution et évite les interférences électromagnétiques avec les câbles réseau car cela peut être source d'erreurs de transmission ;
- **topologie du réseau** : la topologie étoilée du réseau facilite la gestion du réseau et les interventions physiques sur le réseau. Les câbles utilisés sont des paires torsadées blindées STP et non blindées UTP de catégorie 5E qui sont reconnus pour leur fiabilité et sont protégés par des goulottes ;
- **existence d'un serveur DNS secondaire** (physique) : permet la disponibilité des services de nom de domaine réseau en cas de crash du DNS primaire ;
- **existence d'un second abonnement Internet**: en cas de panne de la liaison ADSL, la liaison spécialisée sert de relais afin d'assurer la continuité du service Internet ;

Sur le plan logique nous avons pu relever :

- **existence d'un outil d'authentification + gestion des comptes par une base de données** : cela permet une gestion centralisée et dynamique des comptes utilisateurs ;
- **politique de droit d'accès** : La connexion à un poste du réseau est conditionnée par la détention d'un compte utilisateur valide ;
- **existence d'un serveur NFS** : permet une centralisation des fichiers d'utilisateurs, et le partage de fichiers en réseau. Un utilisateur accède à ses données depuis n'importe

quel poste du réseau ;

- **configuration logique du réseau en des LANs** : augmente le niveau de sécurité, permet une localisation plus simple de problèmes, diminue l'étendue d'attaque et l'ampleur d'éventuels dégâts et permet une fluidité du trafic réseau ;
- **système de sauvegarde** : les données sont sauvegardées quotidiennement sur disque dur externe, toute chose qui limite la perte de données ;
- **le système** : presque tous les postes tournent sur des plateformes Linux. Notamment les serveurs tournent sur Debian reconnu pour sa fiabilité et sa robustesse. En outre les distributions Linux sont quasiment invulnérables aux virus ;
- **antivirus** : Le serveur mail est doté d'un antivirus+antispam permettant d'éviter la contamination des supports de stockage amovibles des utilisateurs via les e-mails bien que Linux soit très résistant aux virus.

### II.2.2 Failles du système

Partant du fait qu'aucun système informatique n'est parfait, c'est-à-dire que le risque zéro n'existe pas et que tout système est vulnérable en matière de sécurité informatique, alors nous avons pu relever les failles suivantes :

- **les accès non autorisés** : bien qu'il soit mentionné que l'accès à la salle serveur est interdit à toute personne étrangère au service, cela n'est pas suffisant pour la sécuriser. En effet, cette salle se trouve dans un local plafonné et la porte d'entrée est en contreplaqué ; toute chose qui augmente le risque d'incendie et favorise l'aggravation d'un éventuel incendie. Aussi la quasi-totalité des services installés ne se trouve seulement que sur deux serveurs implantés dans le même local, ce qui constitue un potentiel danger pour tout le réseau car le moindre incendie qui surviendrait dans ce local serait susceptible de causer des pertes considérables pour tout le système informatique et par ricochet les données très précieuses ;
- **la restriction de l'accès au WIFI** : le point d'accès utilisé présentement pour l'authentification par adresse MAC déjà en place ne peut prendre en compte que trente-deux adresses MAC maximum, ce qui limite le nombre d'utilisateurs WIFI. De plus lorsqu'un utilisateur change de machine la configuration du point d'accès doit être modifiée pour prendre en compte son adresse MAC ;
- **le manque de traçabilité et de contrôle d'accès** : l'authentification par adresse MAC

ne permet pas la gestion efficace des utilisateurs, hormis l'autorisation d'accès au réseau, on ne peut savoir qui est réellement connecté, et quel est la durée d'abonnement de l'utilisateur d'où une remise en cause même de la politique d'authentification (utilisateur et mot de passe) déjà existant ;

- **la sauvegarde de données** : il n'existe pas de serveur redondant délocalisé pour assurer la continuité des services en cas de panne grave. Dans un éventuel cas, il faudra impérativement (acquérir du matériel nouveau en fonction de la panne) réinstaller et reconfigurer tout le système. Avec tous les services que compte ce serveur il n'en faudra pas moins de 72 heures. Pendant tout ce temps, rien ne fonctionnerait ;
- **la conformité à la réglementation interne et externe** : une charte existe, malheureusement elle n'est pas connue de tous les utilisateurs, car les utilisateurs ne pensent pas souvent à lire les affiches.

Au terme de cette analyse qui vient d'être faite, il ressort que le CNFP est doté d'un réseau informatique autonome. Cependant force est de reconnaître que des failles existent et auxquelles il faut apporter des solutions.

## II.3. Solutions envisageables

Vu les failles décrites plus haut, nous préconisons les améliorations suivantes :

- insistance sur la sensibilisation du personnel au respect des règles de sécurité ;
- renforcement de la sécurité de la salle serveur en remplaçant la porte en contreplaqué par une porte métallique afin de réduire le risque d'incendie ;
- extension du réseau sans fil en particulier à partir de répéteurs sans fil pour permettre une plus grande mobilité des utilisateurs et du réseau global en général par un élargissement du parc informatique ;
- revoir la politique d'accès au réseau d'où la nécessité d'un portail captif ;
- uniformisation de la méthode d'authentification aussi bien pour les clients WI-FI que pour les utilisateurs du réseau filaire ; ici s'impose la nécessité d'un portail captif ;
- mise en place d'une gestion centralisée du matériel et des données par les technologies de virtualisation ou par redondance des sauvegardes pour servir de relais afin d'assurer la continuité du service ;

- gestion efficace des utilisateurs après authentification du point de vue traçabilité, détermination d'une durée de connexion, transparence vis-à-vis de l'utilisateur, compatibilité avec plusieurs plates-formes. Ici aussi s'impose l'impératif d'utiliser un portail captif.

Ainsi il existe une panoplie de solutions mais le portail captif est la mieux indiquée car il permet, en plus d'authentifier les utilisateurs, de gérer ces utilisateurs de manière efficace.

# Chapitre III :

# GENERALITES SUR LES PORTAILS CAPTIFS

## III.1. Définition

Un portail captif est une application qui permet de gérer l'authentification des utilisateurs d'un réseau local qui souhaitent accéder à un réseau externe (généralement Internet) [2]. Il oblige les utilisateurs du réseau local à s'authentifier avant d'accéder au réseau externe. Lorsqu'un utilisateur cherche à accéder à Internet pour la première fois, le portail capte sa demande de connexion grâce à un routage interne et lui propose de s'identifier afin de pouvoir recevoir son accès. Cette demande d'authentification se fait via une page web stockée localement sur le portail captif grâce au serveur HTTP. Ceci permet à tout ordinateur équipé d'un navigateur web et d'un accès Wifi de se voir proposer un accès à Internet. Au-delà de l'authentification, les portails captifs permettent d'offrir différentes classes de services et tarifications associées pour l'accès Internet (Par exemple: Wifi gratuit, filaire payant, 1 heure gratuite,...). Cela est obtenu en interceptant tous les paquets quelles que soient leurs destinations jusqu'à ce que l'utilisateur ouvre son navigateur web et essaie d'accéder à Internet. Lors de l'établissement de la connexion, aucune sécurité n'est activée. Cette sécurité ne sera active que lorsque l'ordinateur connecté tentera d'accéder à Internet avec son navigateur web. Le portail captif va, dès la première requête HTTP, rediriger le navigateur web afin d'authentifier l'utilisateur, sans quoi aucune demande ne passera au-delà du serveur captif. Une fois l'utilisateur authentifié, les règles de firewall le concernant sont modifiées et celui-ci se voit autorisé à utiliser son accès Internet pour une durée fixée par l'administrateur. A la fin de la durée fixée, l'utilisateur se verra redemander ses identifiants de connexions afin d'ouvrir une nouvelle session.

Ce système offre donc une sécurité du réseau mis à disposition, il permet de respecter la politique de filtrage web de l'entreprise grâce à un module proxy et permet aussi grâce à un firewall intégré d'interdire l'accès aux protocoles souhaités.

## III.2. Fonctionnement général des portails captifs

Le fonctionnement type d'un portail captif peut être représenté par la figure III.1 [3].

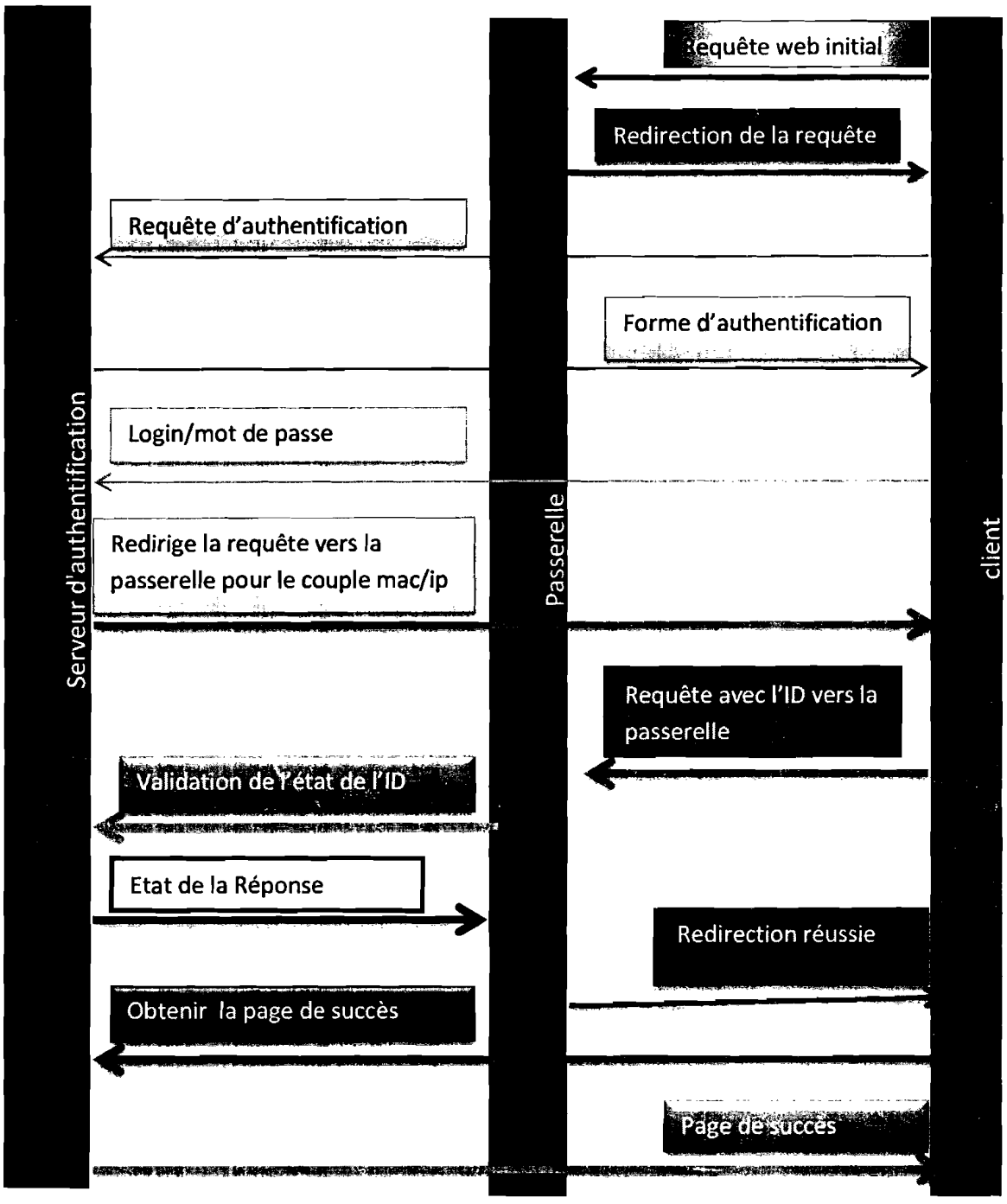


**Figure III.1 : fonctionnement général d'un portail captif**

Le client se connecte au réseau par l'intermédiaire d'une connexion filaire ou au point d'accès sans fil pour du wifi. Ensuite un serveur DHCP lui fournit une adresse IP ainsi que les paramètres de la configuration du réseau. A ce moment-là, le client a juste accès au réseau entre lui et la passerelle, cette dernière lui interdisant, pour l'instant, l'accès au reste du réseau. Lorsque le client va effectuer sa première requête de type web en HTTP ou HTTPS, la passerelle le redirige vers une page web d'authentification qui lui permet de s'authentifier

grâce à un login et un mot de passe. Cette page est cryptée à l'aide du protocole SSL pour sécuriser le transfert du login et du mot de passe. Le système d'authentification va alors contacter une base de données contenant la liste des utilisateurs autorisés à accéder au réseau. Enfin le système d'authentification indique, plus ou moins directement selon les portails captifs, à la passerelle que le couple MAC/IP du client est authentifié sur le réseau. Finalement le client est redirigé vers la page Web qu'il a demandé initialement; le réseau derrière la passerelle lui est dorénavant accessible. Le portail captif, grâce à divers mécanismes comme une fenêtre pop- up sur le client rafraîchie à intervalles réguliers ou des requêtes ping vers le client, est en mesure de savoir si l'utilisateur est toujours connecté au réseau. Au bout d'un délai d'absence sur le réseau, le portail captif va couper l'accès à cet utilisateur.

## III.3. Aperçu des principaux portails captifs

Toutes les solutions que nous avons étudiées sont des solutions libres et gratuites ce qui nous permet de réduire considérablement le coût de leur mise en place.

### III.3.1 PFsense

PFsense est une distribution FreeBSD développée en 2004. L'objectif de départ est d'assurer les fonctions de pare-feu et de routeur mais l'engouement généré par cet applicatif lui a permis d'étendre ses fonctionnalités et présente maintenant les fonctions de portail captif, serveur proxy, DHCP ...

Son installation se fait facilement via une distribution dédiée et toutes les configurations peuvent se faire soit en ligne de commande (SSH) ou via l'interface web (HTTPS). La sauvegarde et la restauration de configuration est disponible à travers l'interface web et permet de générer un simple fichier d'une taille raisonnable. Le portail assure une évolution constante grâce à des mises à jour régulières dont l'installation est gérée automatiquement dans une partie du panneau d'administration.

Cette solution permet une authentification sécurisée via le protocole HTTPS et un couple utilisateur / mot de passe.

Une documentation très complète est disponible sur Internet, un support commercial est désormais présent en cas de gros incident. PFsense dispose aussi d'une communauté très

active.

PFsense assure une compatibilité multi-plates-formes, une personnalisation complète des pages accessibles aux utilisateurs ainsi qu'une simplicité d'utilisation grâce à une page de connexion succincte où on ne retrouve que deux champs (utilisateur / mot de passe).

### III.3.2 ALCASAR

ALCASAR (Application Libre pour le Contrôle d'Accès Sécurisé et Authentifié au Réseau) est un projet français essentiellement dédié aux fonctions de portail captif. Cet applicatif s'installe via un script supporté par la distribution Linux Mandriva, les configurations se font via une interface de gestion sécurisée (HTTPS) ou bien en ligne de commande directement sur le Serveur Mandriva. Une sauvegarde de la configuration est prise en charge via la création d'un ghost système (fichier système) dans le panneau d'administration, ce qui engendre tout de même un fichier d'une certaine taille. Les mises à jour régulières assurent la pérennité de la solution.

L'authentification au portail est sécurisée par HTTPS et un couple utilisateur / mot de passe. Une documentation assez complète est disponible pour l'installation et la configuration et la communauté est active. Tout comme PFsense, ALCASAR est compatible avec de nombreuses plates-formes, la personnalisation des pages utilisateurs et la simplicité d'utilisation sont présentes.

### III.3.3 ZeroShell

ZeroShell est une distribution Linux conçue pour mettre en place une sécurité globale au sein d'un réseau (Pare-Feu, VPN, portail captif...). Son installation est simple via une distribution dédiée. Elle présente une interface de gestion web simple d'utilisation qui permet entre autres de sauvegarder la configuration du portail captif ou encore de personnaliser les pages de connexion et déconnexion dans un éditeur HTML intégré.

Comme les deux autres solutions la page d'authentification est sécurisée et la connexion se fait via un couple utilisateur / mot de passe. On retrouve assez peu de documentation pour la gestion du système mais la communauté à l'air tout de même bien présente. Son utilisation reste identique aux autres solutions présentées.

### III.3.4 ChilliSpot

ChilliSpot est un applicatif dédié à la gestion de l'authentification sur les réseaux, son installation est assez simple via un package applicatif disponible sur les distributions Red Hat et Fedora. La sauvegarde de la configuration est disponible mais elle implique de copier les fichiers de configuration et donc de les connaître. La page de connexion est disponible en HTTPS à condition d'avoir configuré le serveur web (Apache) au préalable en écoute sur le port 443. On retrouve une documentation complète et une communauté assez active, mais le projet est en régression, la dernière version stable date d'octobre 2006 et le projet est mis en suspens depuis le départ du développeur principal. L'utilisation est la même que les autres solutions proposées, page de connexion avec champs utilisateur et mot de passe.

## III.4. Comparaison des portails captifs

Dans l'étude comparative des solutions nous avons mis en évidence plusieurs critères importants que doivent prendre en compte les différentes solutions:

- **Sécurité des échanges lors de l'authentification** : pour éviter la récupération de mot de passe sur le réseau ;
- **Présence d'une documentation complète** : pour assurer la rapidité de mise en place de la solution ;
- **Simplicité d'administration** : pour permettre à différentes personnes d'administrer le logiciel ;
- **Simplicité d'utilisation** : pour permettre à tous les visiteurs (expérimentés ou non) de se connecter au réseau Wi-Fi ou filaire ;
- **Compatibilité multiplate-formes** : pour permettre la connexion depuis les Smartphones, différents navigateurs web et différents système d'exploitation.
- **Présence de sauvegarde et restauration de configuration** : pour permettre un redémarrage du système très rapidement en cas de problèmes ;
- **Pérennité de la solution** : pour pallier les failles de sécurité et augmenter les fonctionnalités de la solution via des mises à jour ;
- **Possibilité de personnaliser la page de connexion** : pour adapter le logiciel à la charte graphique de l'entreprise et ainsi le rendre plus convivial.

Le tableau III.1 fait un récapitulatif des critères de comparaison.

**Tableau III.1 : Comparaisons des différentes solutions de portail captif**

| Critères | Solutions | | | |
|---|---|---|---|---|
| | **PFsense** | **ALCASAR** | **ZeroShell** | **ChilliSpot** |
| Sécurité Authentification | HTTPS | HTTPS | HTTPS | HTTPS |
| Documentation | ● | ● | ○ | ◡ |
| Plates-formes Clientes Supportées | Toutes | Toutes | Toutes | Toutes |
| Personnalisation | ● | ● | ○ | ● |
| Facilité d'administration | Installation via distribution dédiée | Installation via script automatisé | Installation via distribution dédiée | Installation via .rpm sur Red Hat et Fedora |
| Facilité d'Utilisation | ● | ● | ● | ● |
| Sauvegarde/Restauration Configuration | ● | ● | ● | |
| Pérennité de la solution | ● | ● | ○ | ● |

Légende :

● Disponibilité élevée

○ Moyennement disponible

● Moins disponible

## III.5. Choix d'une solution de portail captif

Bien que nous n'ayons pas mis en pratique toutes ces solutions pour les comparer, l'étude théorique permet de retenir les deux premières solutions à savoir PFsense et ALCASAR car elles répondent toutes deux à nos besoins: solutions libres, peuvent s'installer sur un serveur comme sur un poste de travail, authentification des utilisateurs par login et mot de passe, contrôle de la bande passante, facilité d'administration, d'installation et de configuration, facilité d'utilisation, documentation très détaillée et disponible, disponibilité de mises à jour,

etc.

Les deux solutions répondent tout à fait au cas étudié mais **ALCASAR** s'installe uniquement via une distribution Mandriva. Aussi **ALCASAR** s'installe via un script automatisé, par contre **PFsense** s'installe via une distribution dédiée ; ce qui rend impératif le choix de **PFsense**. De plus **PFsense** présente une interface plus conviviale et une page principale en tableau de bord où l'on retrouve toutes les informations essentielles et que l'on peut modifier en fonction des besoins. Ce produit présente aussi une plus grande assurance car la communauté des utilisateurs est très active.

# Chapitre IV :

## ETUDE TECHNIQUE DE PFSENSE

## IV.1. Qu'est-ce PFsense ?

Développé par **Chris Buechler** et **Scott Ullrich**, PFsense ou « Packet Filter Sense » est un applicatif qui fait office de routeur/firewall open source basé sur le système d'exploitation FreeBSD et Monowall. Il est une reprise du projet Monowall auquel il rajoute ses propres fonctionnalités. PFsense est basé sur PF (*packet filter*), comme iptables sur GNU/Linux et il est réputé pour sa fiabilité [4]. C'est une distribution dédiée qui peut être installée sur un simple poste de travail, un serveur ou même sur un boîtier en version embarquée.

Ce qui séduit chez PFsense est sa facilité d'installation et de configuration des outils d'administration réseau. En effet, après une installation en mode console, il s'administre ensuite simplement depuis une interface web et gère nativement les VLAN (802.1q).

La distribution PFsense met ainsi à la disposition de l'administrateur réseau une multitude d'outils open source et de services permettant d'optimiser ses tâches. Parmi ces services, figure **Captive Portail** (portail captif) qui fait l'objet de ce projet.

## IV.2. Aperçu des fonctionnalités et services de PFsense

En fonction de la version du logiciel, le nombre de services et/ou de fonctionnalités peut varier. Pour ce projet, la version 2.0.3 est utilisée. Ainsi cette version dispose entre autres de:

- Support des VLAN tagués, c'est-à-dire qu'elle permet de créer et gérer nativement les VLAN ;
- Routage IPv4 et (depuis la version 2.1) IPv6 ;
- NAT (Network Address Translation) pour faire correspondre un nombre restreint d'adresses IP publiques à un nombre plus élevé d'adresses privées locales ;
- Filtrage du trafic entrant et sortant pour tout type de trafic (ICMP, UDP, TCP…) pour faire office de pare-feu ;
- Limitation des connexions pour empêcher un utilisateur de se connecter à la fois avec son seul compte ;
- "Load Balancing" pour la transposition de charge en cas de surcharge ;
- "Failover" pour le basculement d'une ligne à l'autre si l'on possède par exemple plusieurs abonnements à Internet ;
- Proxy transparent qui joue le rôle de serveur mandataire ;
- DNS dynamique pour la gestion dynamique des noms de domaines ;

- **Portail captif;**
- Serveur DHCP ;
- Contrôle d'accès par adresses MAC ou authentification RADIUS ;
- Serveur ou relay DHCP / DNS qui est relais du serveur DHCP / DNS ;
- etc.

## IV.3. Les versions du logiciel

Depuis sa mise en route en 2004, le projet PFsense ne cesse d'évoluer et différentes versions du logiciel se sont succédées. Pour chaque version, il en existe pour les architectures i386 (32-bits) et amd64 (64-bits). De même elles sont disponibles en Live CD ou en plate-forme embarquée. Ainsi on a:

- **PFsense 2.1**: disponible depuis le 15/09/2013, elle est la plus récente mais toujours en test ;
- **PFsense 2.0.3** : disponible depuis le 15/04/2013, elle est la plus stable ;
- **PFsense 2.0.2** : disponible depuis le 21/12/2012 ;
- **PFsense 2.0.1**:disponible depuis le 21/12/2011 ;
- **PFsense 2.0**:disponible depuis le 17/09/2011 ;
- **PFsense 1.0** : première version sortie le 14/10/2006.

Il existe aussi des versions intermédiaires non stables (bêta et RC) qui ne sont pas mentionnées ici.

## IV.4. Installation de PFsense

### IV.4.1 Matériel et architecture réseau requis

Pour le matériel sur lequel PFsense doit s'installer, on a besoin d'un minimum qui soit composé d'une machine dotée d'au moins deux cartes réseau et dont les caractéristiques sont :

- au moins 1 Go de disque dur (500 Mo pour les plates-formes embarquées) ;
- au moins 128 Mo de RAM, mais plus de 512 Mo recommandés ;
- un CPU cadencé à au moins 100 MHZ (500 MHZ ou plus recommandé).

Mais dans notre cas nous avons utilisé un poste de travail avec les caractéristiques suivantes :

- disque dur : 40 GB ;
- Processeur : 1350 Mhz ;
- RAM: 768 MB.

L'architecture réseau le plus souvent déployé est représentée par la figure IV.1

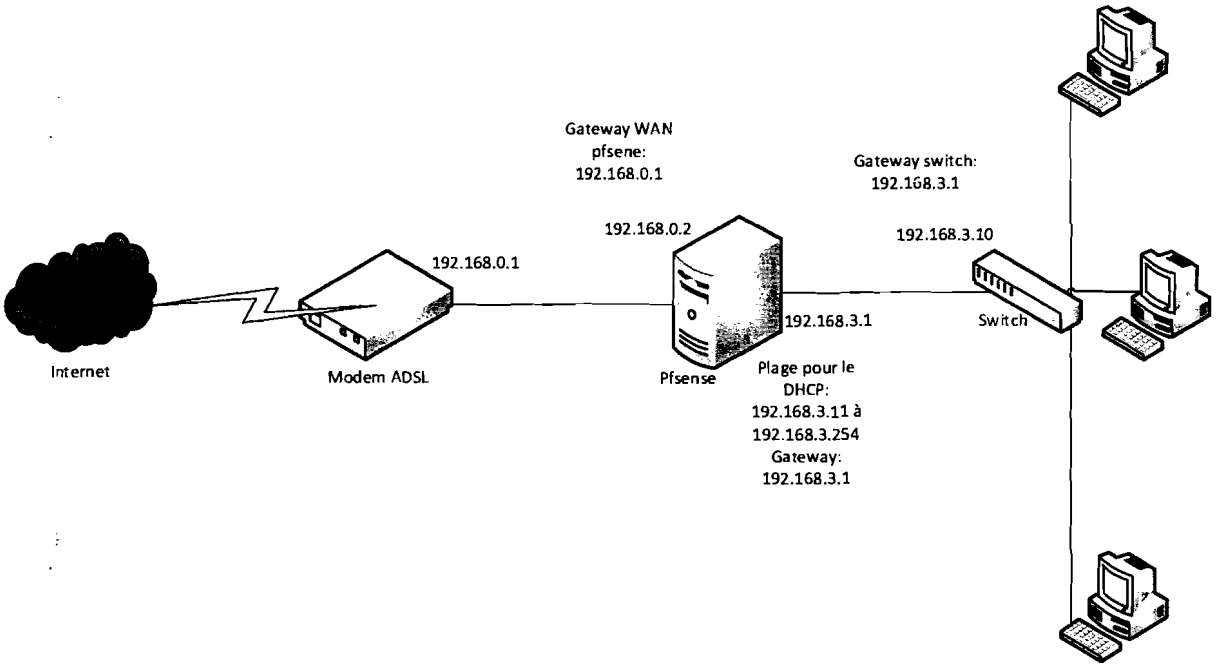


**Figure IV.1 : Architecture réseau standard d'implantation de PFsense**

Rappelons ici qu'à la place du switch il est placé généralement un point d'accès sans fil.

Pour la phase de test de ce projet, nous avons eu besoin d'un point d'accès sans fil, d'un Switch, d'un PC avec carte wifi pour le test et d'un autre PC pour l'administration via le web. L'architecture du réseau existant est représentée par la figure II.1 et celle après implémentation de PFsense est représentée par la figure IV.2.

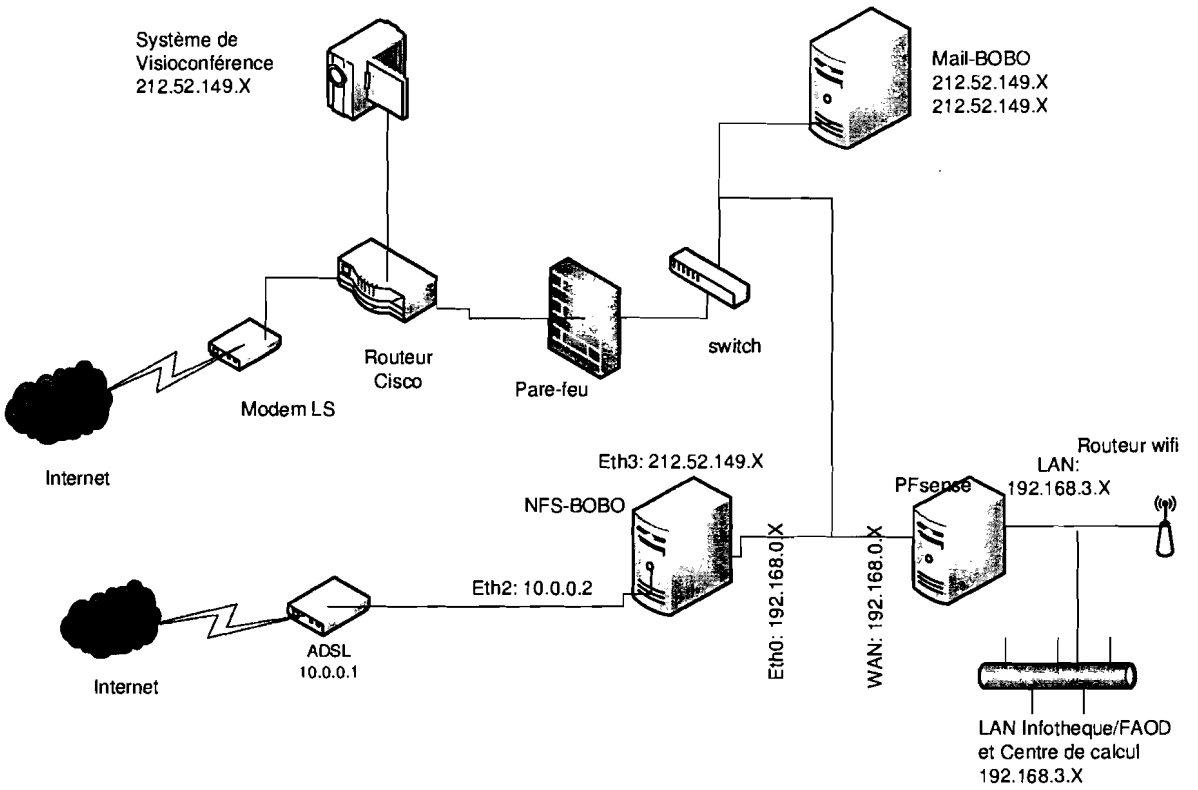


**Figure IV.2 : Architecture réseau du CNFP après implantation de PFsense**

On remarque une légère modification dans cette architecture pour l'utilisation de la fonction captive de PFsense. Nous avons ainsi regroupé les trois sous-réseaux en un seul réseau. Si nous voulons prendre en compte plusieurs sous-réseaux pour l'authentification des utilisateurs, il va falloir augmenter le nombre de cartes réseau sur la machine PFsense.

### IV.4.2 Installation

Pour une mise en œuvre pratique nous avons décrit pas à pas les différentes étapes de l'installation. En effet, on peut utiliser le logiciel de deux façons : installer directement sur le disque dur ou utiliser le logiciel via un live CD sans l'installer.

Cette dernière option est très rapide et efficace. Le chargement se fait automatiquement ainsi que la configuration. Mais elle possède tout de même des inconvénients tels que le chargement long, manque de fiabilité et l'impossibilité d'ajouter des « packages » (logiciels) car on ne peut pas toucher à la structure du CD [5].

Vu les inconvénients du live CD, pour l'implantation dans le réseau, nous allons l'installer sur le disque dur pour plus de sécurité.

Tout d'abord, vérifier que l'ordinateur possède les caractéristiques requises, puis insérer le CD au démarrage de la machine. On accède ensuite à l'écran de démarrage de FreeBSD

Tout d'abord, vérifier que l'ordinateur possède les caractéristiques requises, puis insérer le CD au démarrage de la machine. On accède ensuite à l'écran de démarrage de FreeBSD (figure IV.3) et on choisit l'option 1 (par défaut) ou on attend la fin du compte à rebours.

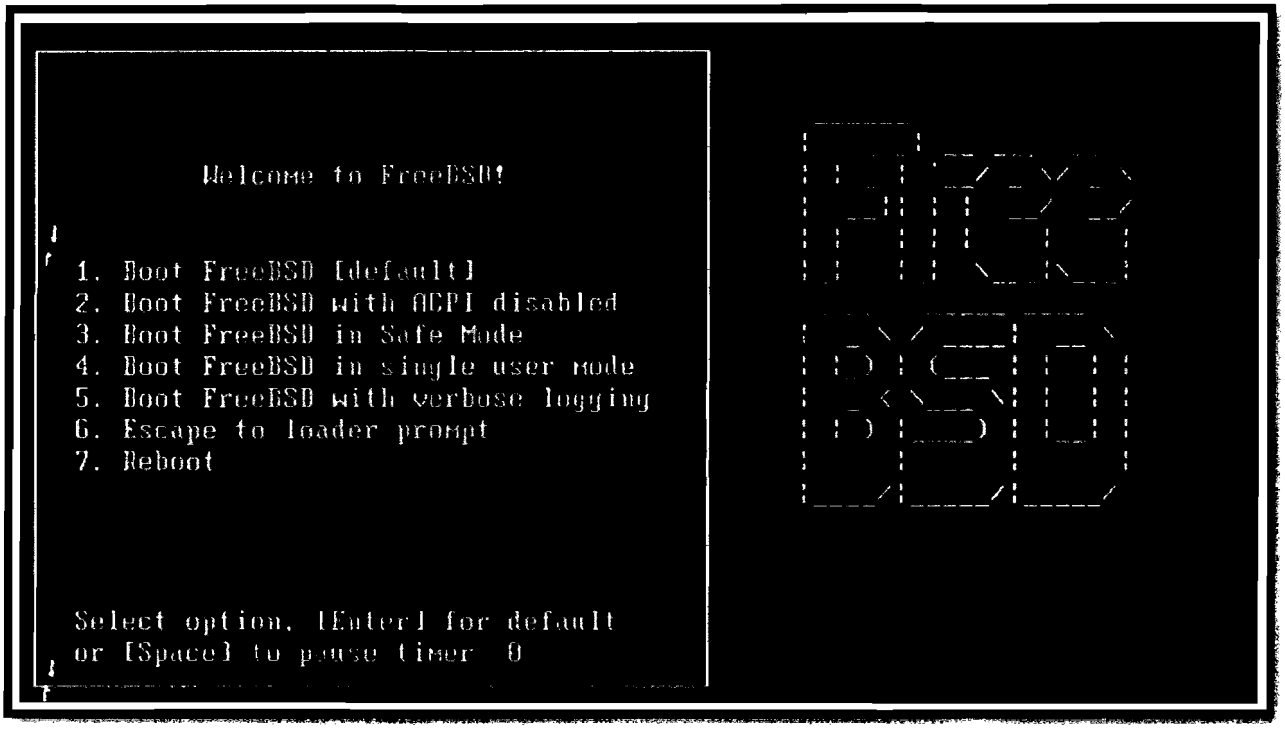


**Figure IV.3 : Écran de démarrage de FreeBSD**

Nous n'allons pas configurer de VLAN pour le moment, la réponse à la question de la figure IV.4 sera donc «n».


**Figure IV.4 : Boite de dialogue pour la configuration de VLAN**

Ensuite vient la configuration des interfaces réseaux. On remarque ici que FreeBSD détecte le nombre de cartes réseau et leur attribue des noms (dans notre cas les interfaces détectés sont : sis0 et xl0). Une fois les interfaces détectées, il est nécessaire de définir l'interface LAN (dans notre cas sis0) et l'interface WAN (xl0) et de valider ces changements en appuyant sur la

touche ENTREE (voir figure IV.5).

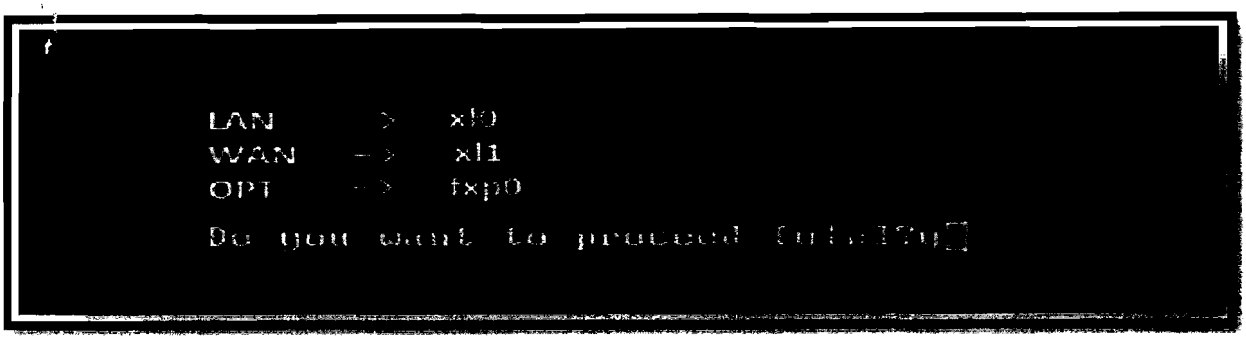


**Figure IV.5 : Validation des noms d'interface**

Si l'on veut ajouter une DMZ, ou configurer d'autres interfaces on les ajoute dans **Optional interface** juste après. Dans notre cas, nous n'avons que deux interfaces et il suffit d'appuyer sur la touche ENTREE (figure IV.6).

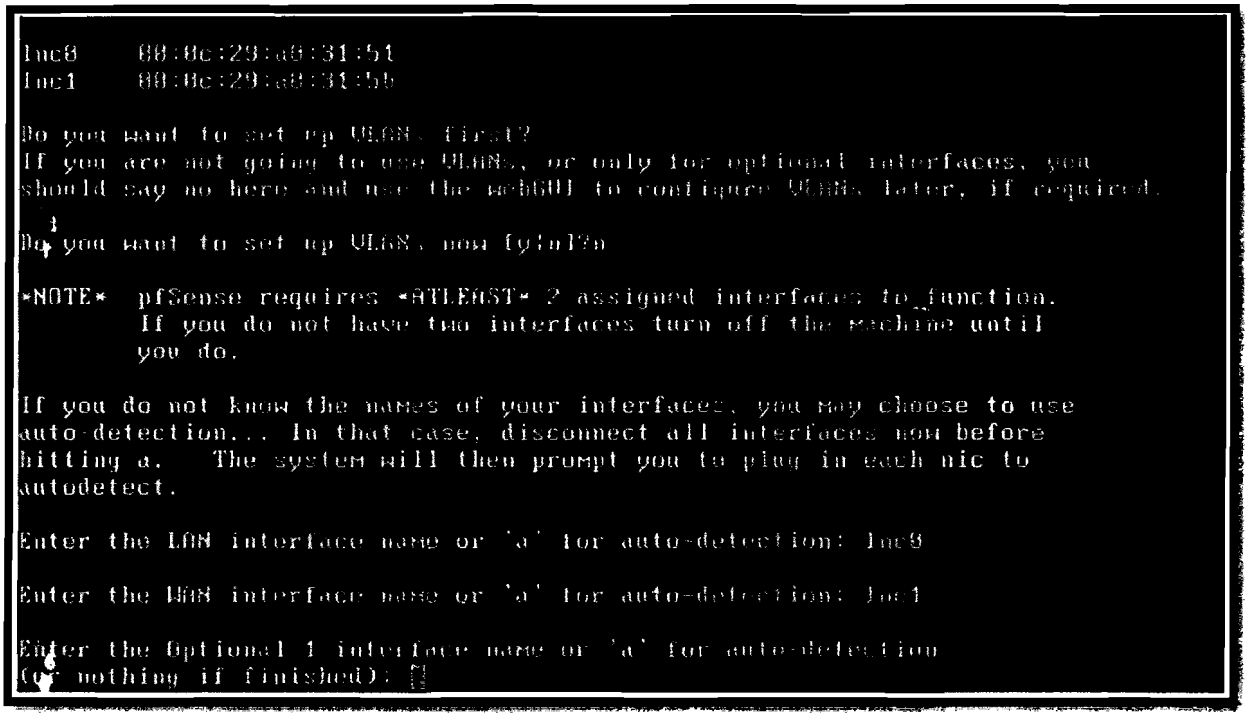


**Figure IV.6 : Ajout ou non de carte optionnelle**

Une fois les interfaces définies, il est nécessaire d'installer PFsense en dur sur le disque dur. L'installation sur le disque se fait en tapant le choix «99» pour les versions antérieures à PFsense2.0 et tapant la lettre «i» depuis la version V2.0. Cette étape est représentée par la figure IV.7.

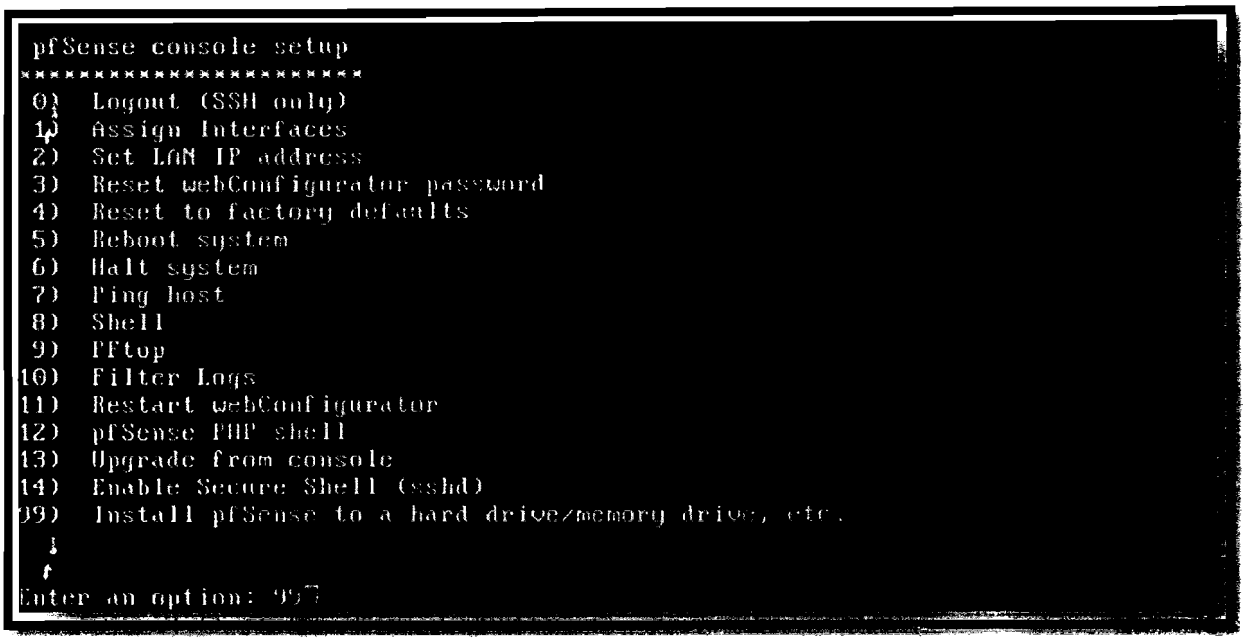


**Figure IV.7 : Option d'installation de PFsense**

Il faut confirmer l'installation sur le disque dur (voir figure IV.8).

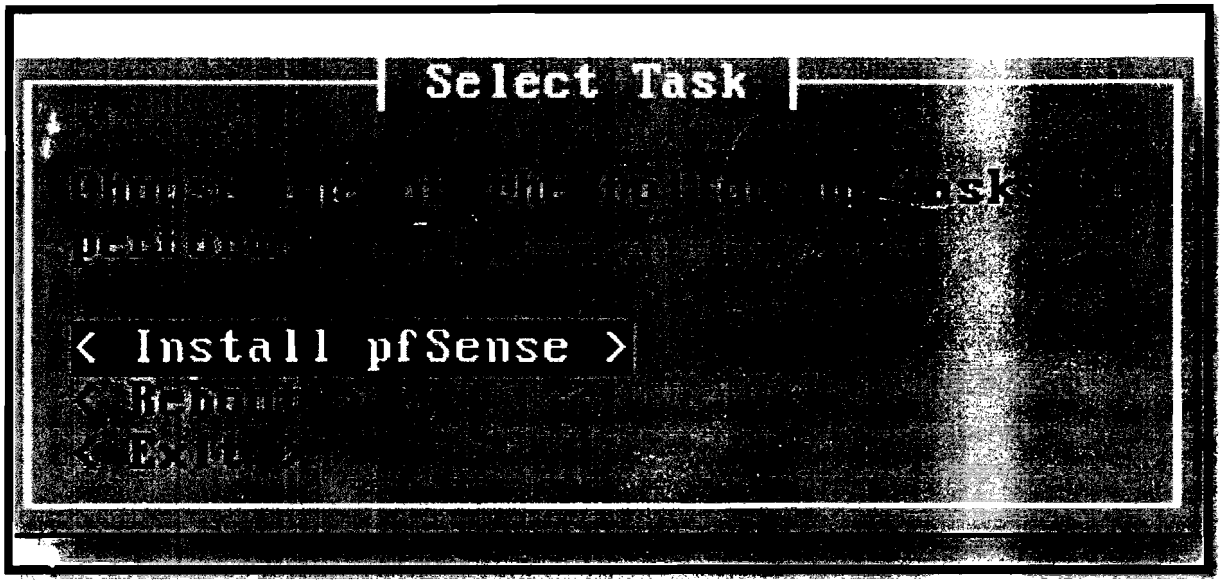


**Figure IV.8 : Confirmation de l'installation**

Une fois l'installation lancée on a différentes procédures d'installation (figure IV.9) et nous optons ici pour l'installation rapide puis confirmons.

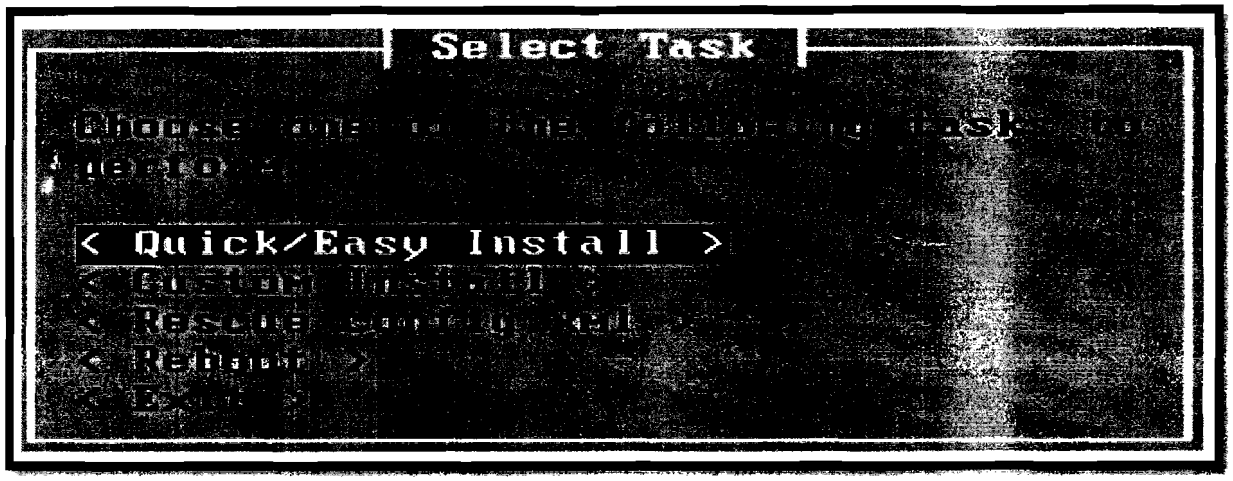


**Figure IV.9 : Type d'installation**

Les étapes suivantes sont obligatoires. Elles permettent la création des partitions accueillant l'installation de PFsense (voir figure IV.10).

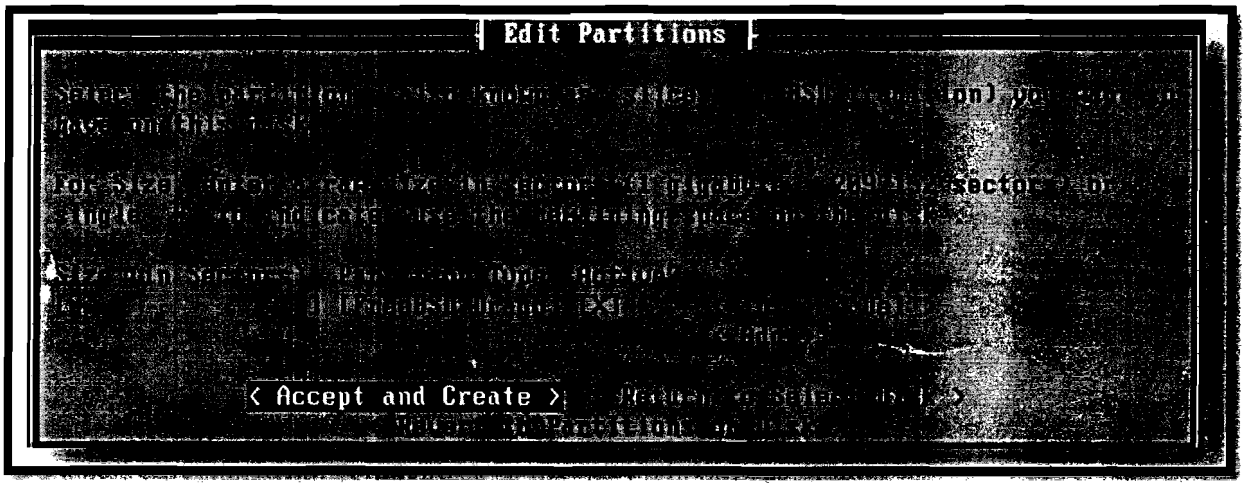


**Figure IV.10 : Création de partition**

Il faut choisir l'option « **Accept and Install Bootblocks** » puis valider en tapant sur la touche ENTREE pour lancer l'installation (figure IV.11).

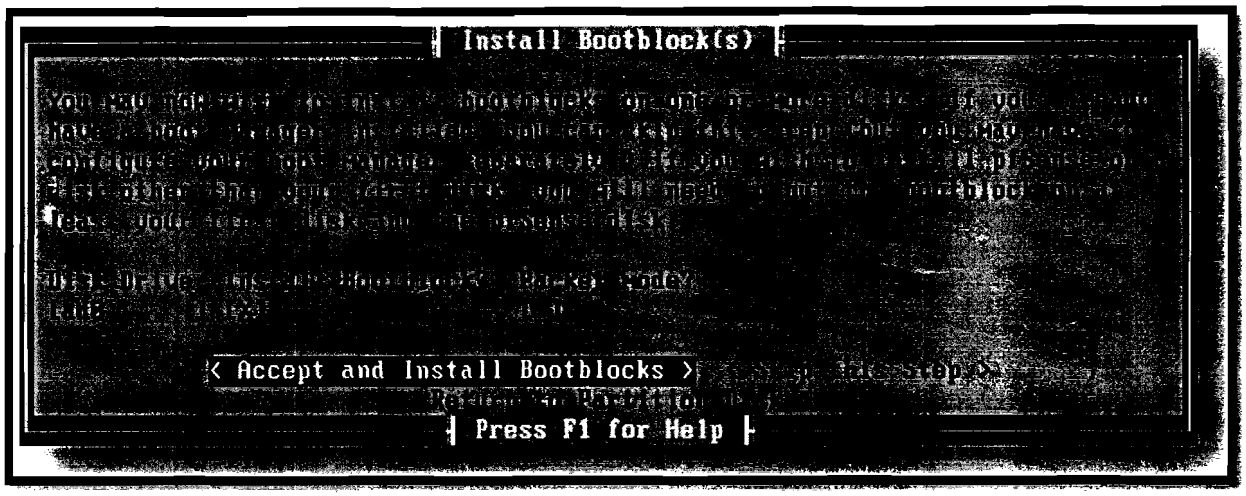


**Figure IV.11 : Lancement de l'installation**

Une fois les partitions créées et paramétrées, il est nécessaire de redémarrer l'ordinateur (figure IV.12) pour que les changements soient effectifs.

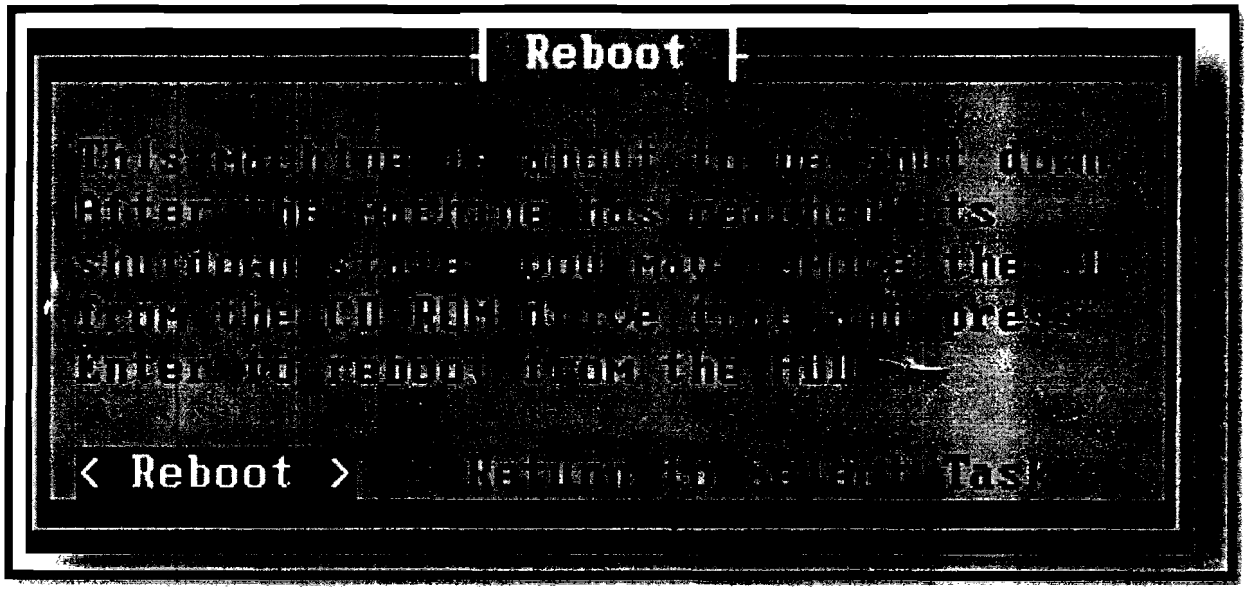


**Figure IV.12 : Fin de l'installation**

Après redémarrage on a le menu de la figure IV.13 qui nous permettra de configurer PFsense.

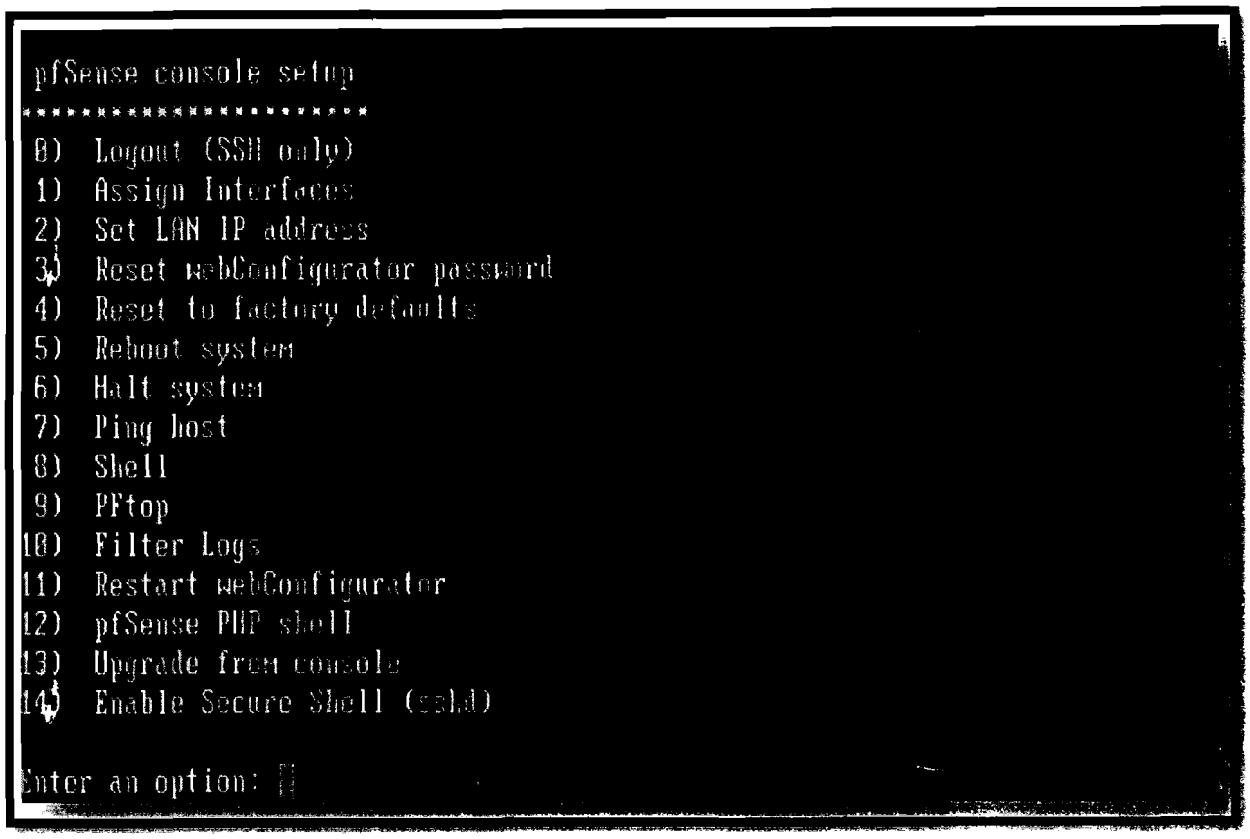


**Figure IV.13 : Menu de configuration**

Avant tout il est conseillé de changer l'adresse IP LAN de PFsense pour plus de simplicité par la suite ; son adresse IP LAN par défaut étant le **192.168.1.1**. Elle sera par la suite modifiée pour être dans notre réseau local. Pour cela, dans le menu de configuration, taper le choix 2: « **Set LAN IP address** » et changer l'adresse IP de PFsense (voir figure IV.14).

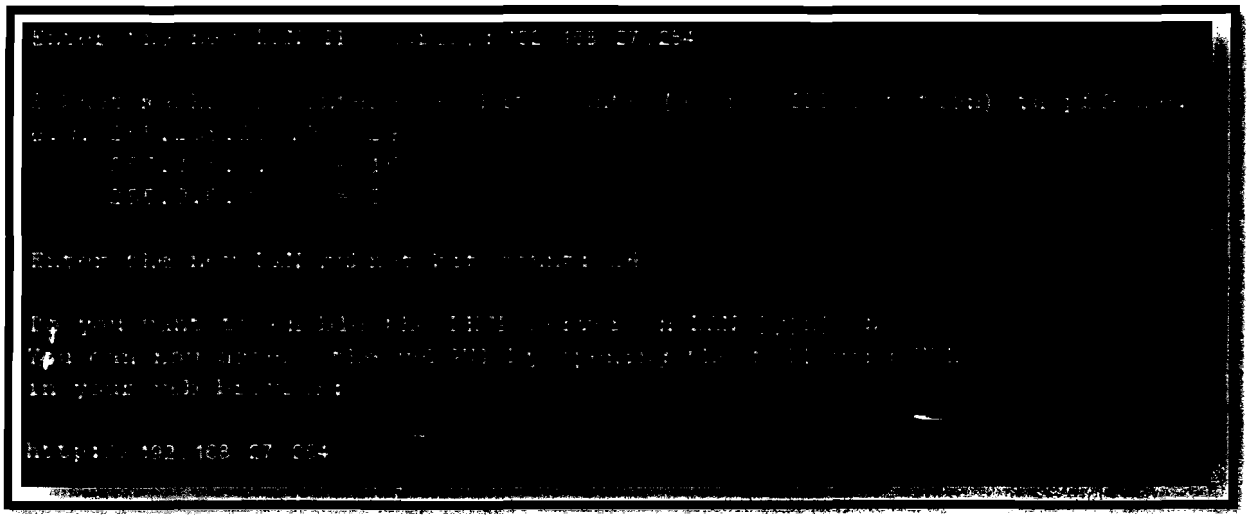

**Figure IV.14 : Configuration de l'adresse IP LAN**

Ainsi prend fin l'installation et on peut dès maintenant commencer à configurer soit en mode console, soit à partir de l'interface web. Nous avons choisi ici la configuration via l'interface web car cela offre plus de convivialité ; les options de la configuration en mode console étant détaillées en annexe A de document.

## IV.5. Configuration de PFsense

### IV.5.1 Configuration générale

Pour la configuration via l'interface web, il faut connecter un PC à l'interface LAN de PFSense. Commencer par ouvrir un navigateur web et entrer l'adresse IP LAN de la machine (PFSense) dans la barre d'adresse : **http://ip_pfsense**. Dans notre cas, nous ferons http://192.168.x.x pour accéder à l'interface de connexion (figure IV.15) où il est demandé d'entrer un nom d'utilisateur et un mot de passe. Entrer ensuite le nom d'utilisateur par défaut **(admin)** et le mot de passe **(pfsense)** pour se connecter en tant que administrateur.

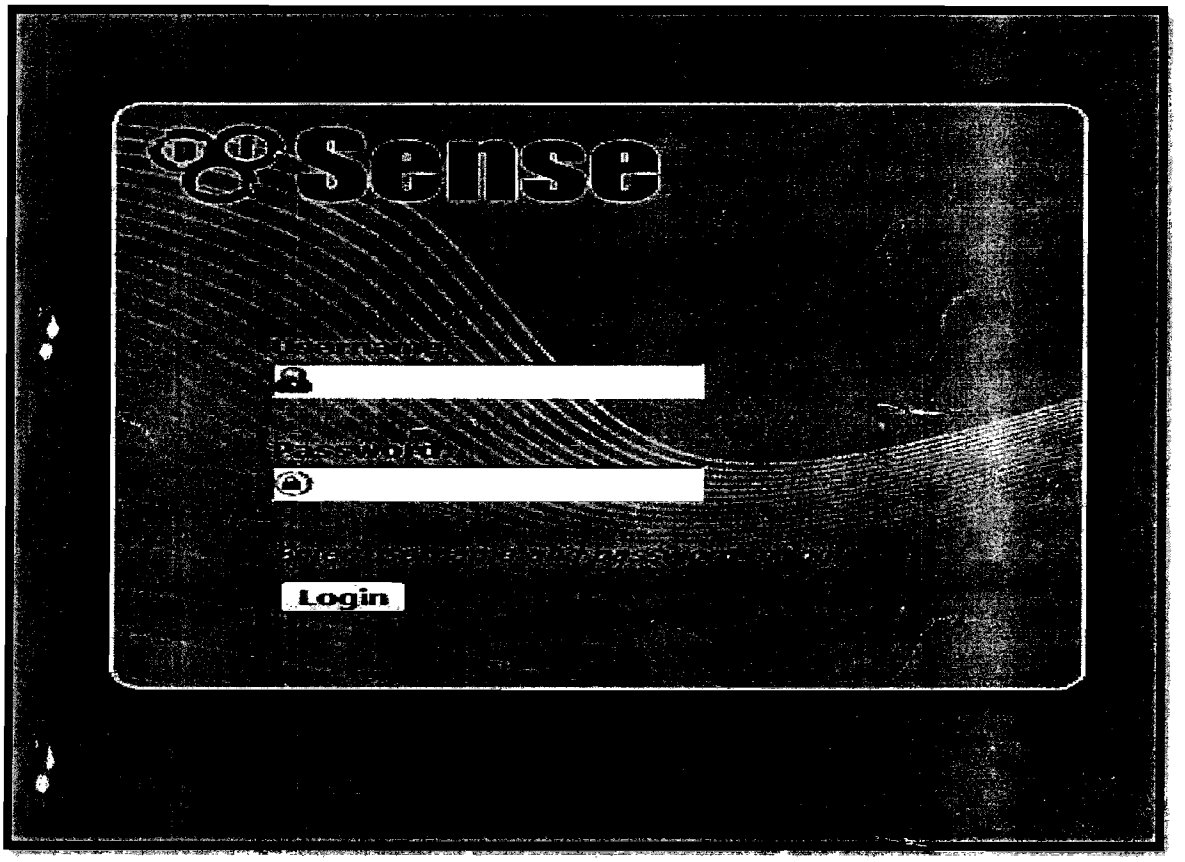


**Figure IV.15 : Portail de connexion à PFsense**

On accède au menu général de PFsense (figure IV.16) qui donne des informations globales sur

le logiciel (version, date de sortie, version du noyau, le nombre d'interfaces connectées etc.).

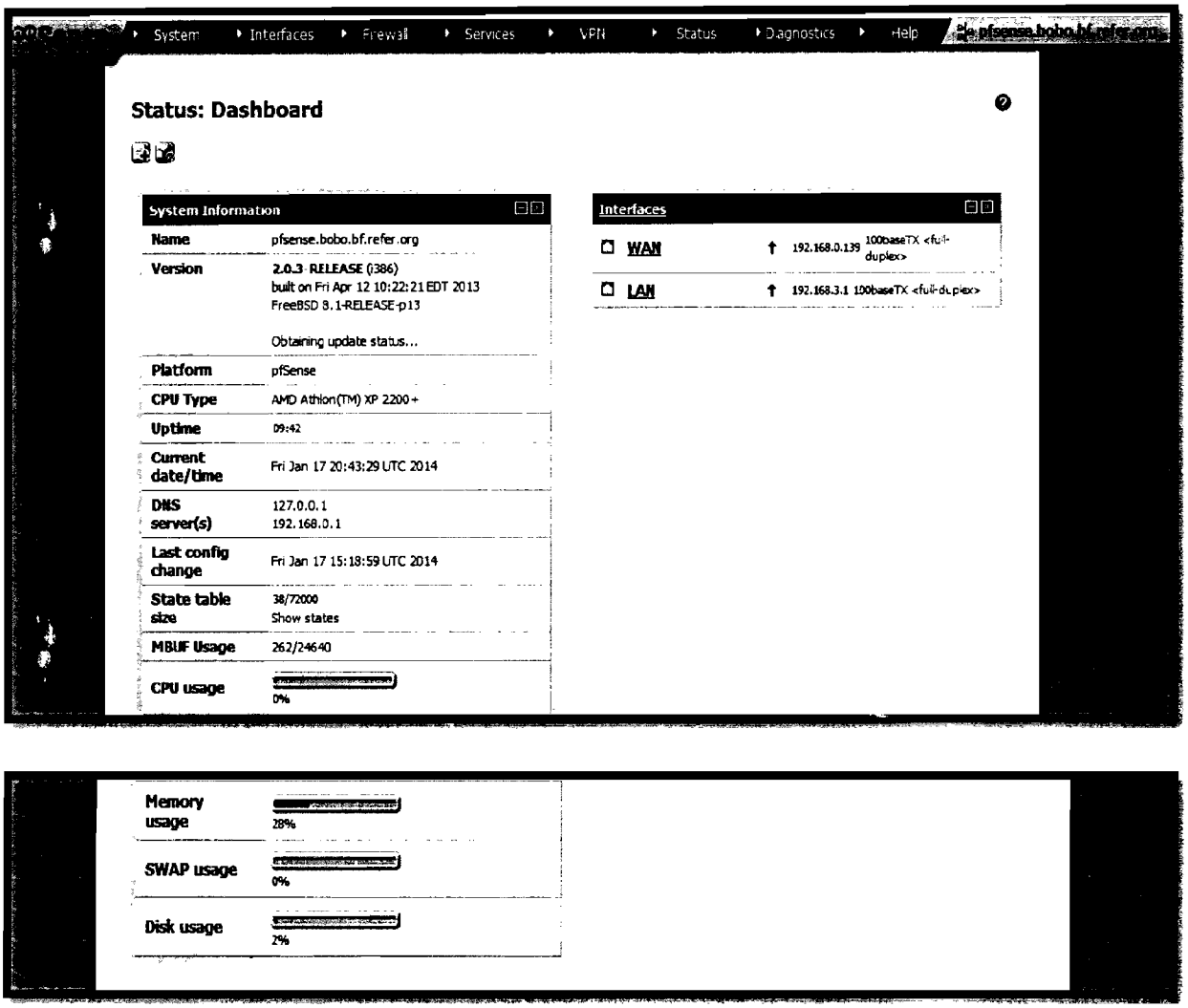


**Figure IV.16 : Paramètres généraux de PFsense**

Pour le paramétrage général, aller dans l'onglet **System**, puis **General Setup** pour voir la configuration générale de PFsense. Entrer ici le nom de la machine, le domaine et l'adresse IP du serveur DNS (dans notre cas le nom : PFsense, domaine : bobo.bf.refer.org, l'IP du DNS : 192.168.0.x). Attention il faut décocher l'option se trouvant en dessous (**Allow DNS server list to be overridden by DHCP/PPP on WAN**). En effet, cette option provoque des conflits puisque le DNS des clients n'est plus PFsense mais un DNS du WAN inaccessible par le LAN.

Ensuite, modifier le nom et le mot de passe permettant de se connecter à PFsense. On peut autoriser l'accès à ces pages, via une connexion SSL. Pour cela activer HTTPS en cochant sa case puis entrer le port 443 dans **WebGuid** (port correspondant à SSL). On peut ensuite modifier le serveur de temps NTP et le fuseau horaire pour régler l'horloge (voir figure IV.17).

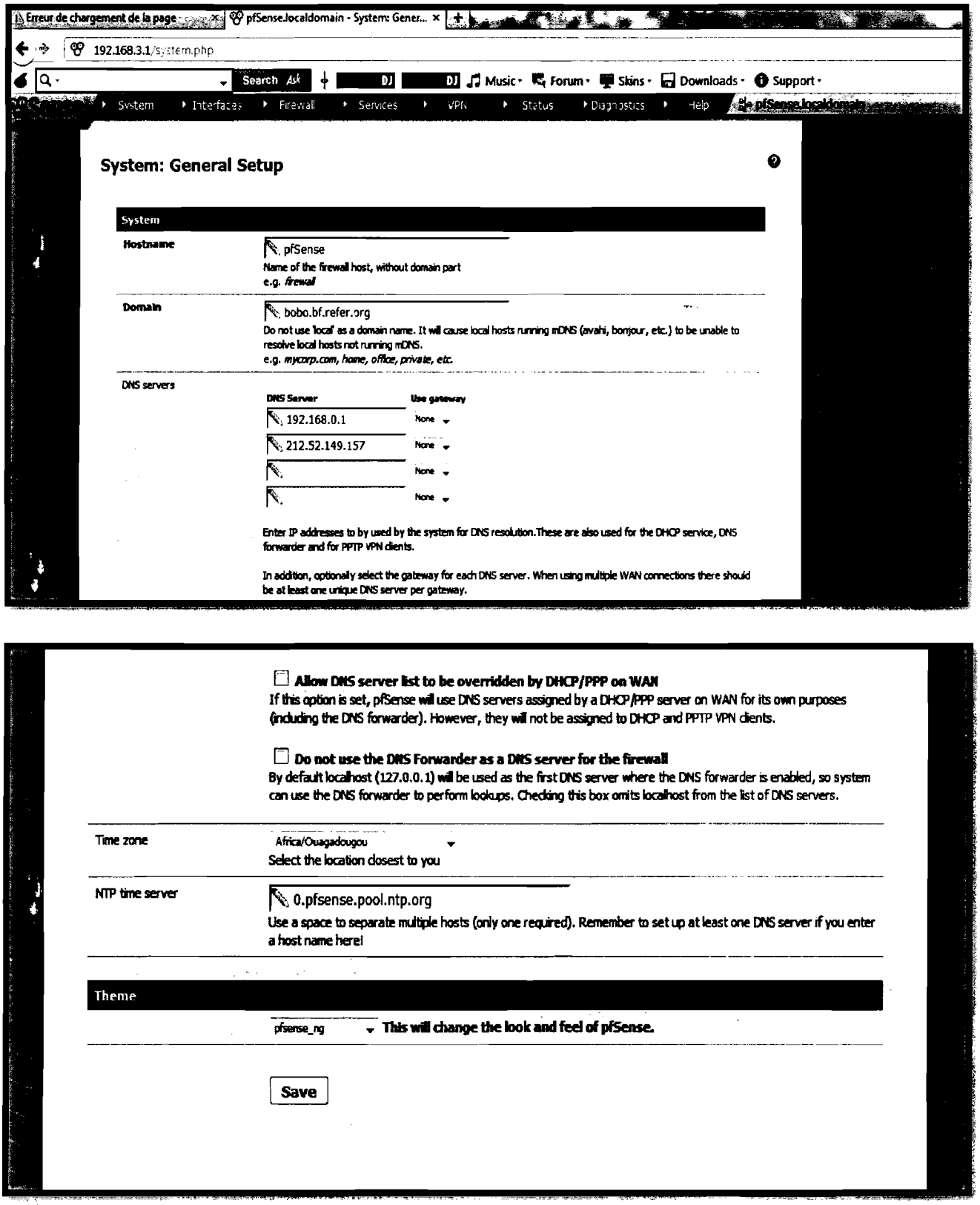


**Figure IV.17 : Configuration générale**

Aller ensuite dans l'onglet **Service** puis dans la section **DNS forwarder**, pour cocher l'option **Enable DNS forwarder**. Cette option va permettre à PFsense de transférer et d'émettre les

requêtes DNS pour les clients.

**Remarque** : Après chaque modification de paramètres il ne faut pas oublier de sauvegarder en cliquant sur **Save** qui se trouve en bas.

### IV.5.2 Configuration des interfaces

#### IV.5.2.1. Interface WAN

Dans l'onglet **Interfaces**, sélectionner **WAN** puis l'activer en cochant **Enable Interface** ; sélectionner ensuite le type d'adressage **Static** ou **DHCP**. Ici nous avons assigné une adresse **Static**. Ensuite préciser son adresse MAC au format indiqué, son adresse IP public (ici 192.168.0.x/24) et sa passerelle (ici 192.168.0.x) dans les cases prévues à cet effet. Puis laisser les autres paramètres par défaut. Cette étape est représentée par la figure IV.18.

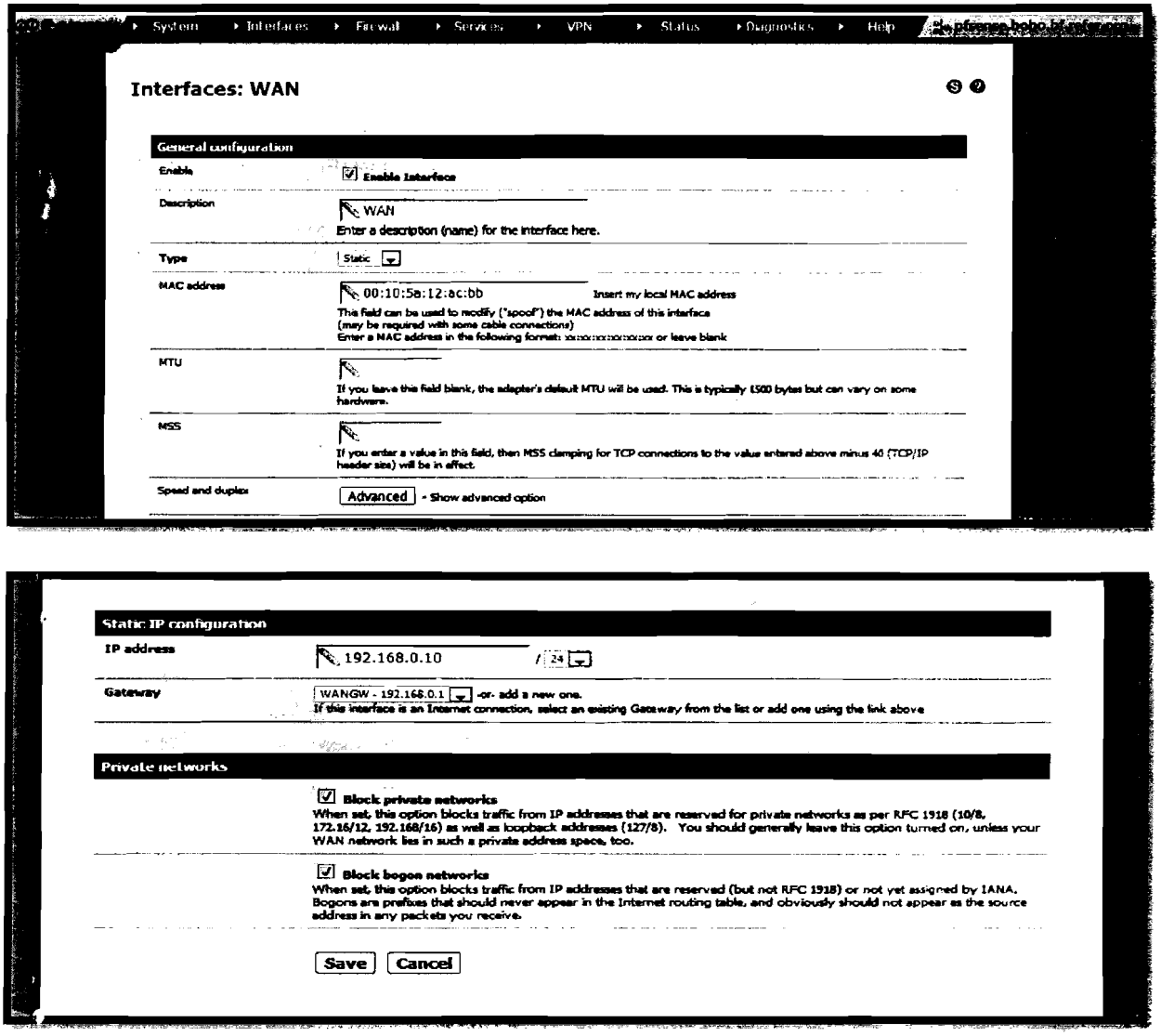


**Figure IV.18 : Configuration de l'interface WAN**

IV.5 2.2. L'interface LAN

Il faut maintenant activer l'interface LAN de la même manière qu'on l'a fait avec le WAN mais cette interface doit être nécessairement en **Static** pour le type d'adressage car, étant celle sur laquelle sera activée le serveur DHCP, il faut que son adresse soit fixée. Puis assigner son adresse MAC au format indiqué, son adresse IP étant déjà définie plus haut, sa passerelle est laissée par défaut, c'est-à-dire sa propre adresse IP car celle-ci constitue la passerelle des clients (voir figure IV.19).

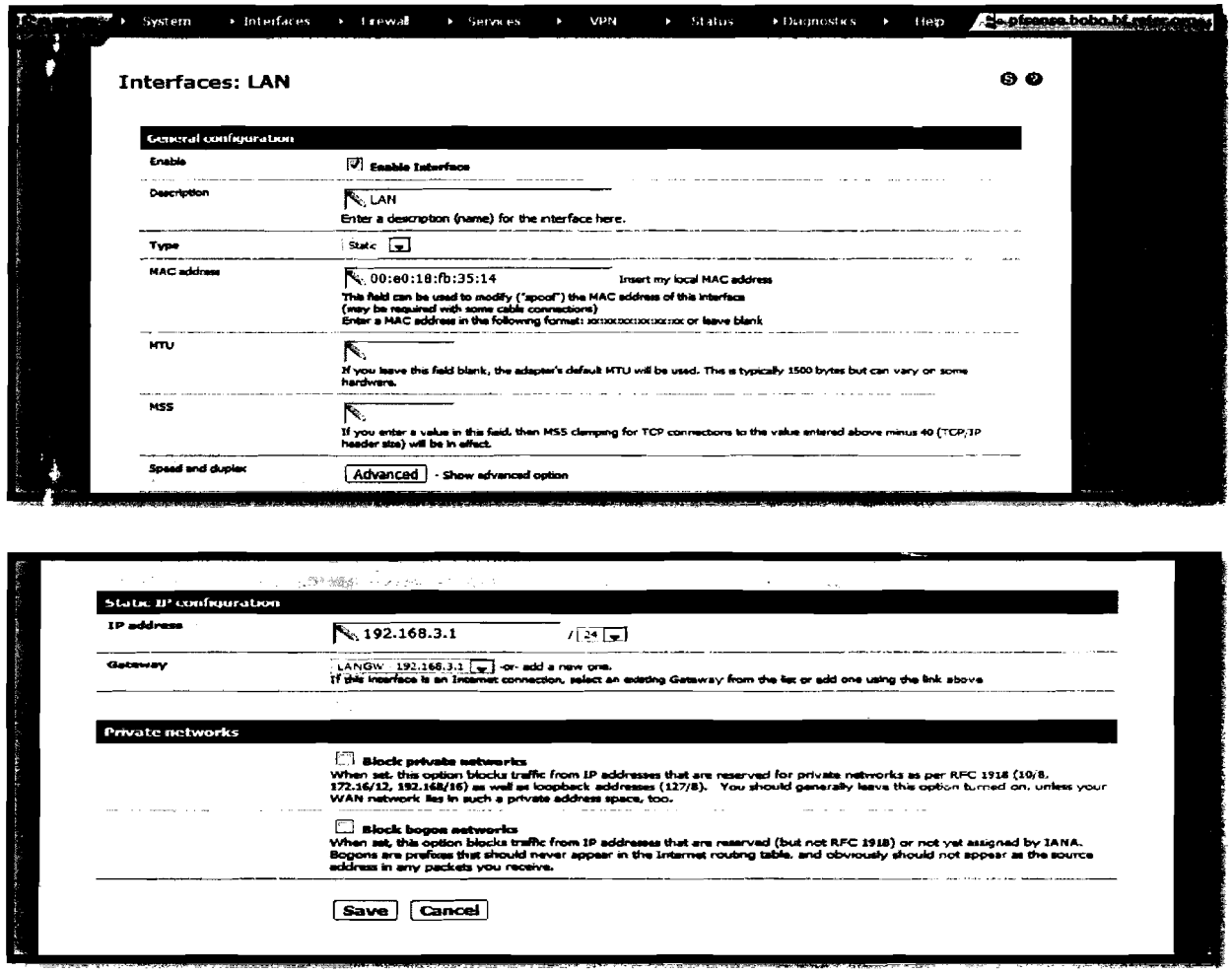


**Figure IV.19 : Configuration de l'interface LAN**

IV.5.2.3. Configuration du serveur DHCP

Il ne reste plus qu'à configurer le serveur DHCP pour le LAN, afin de simplifier la connexion des clients. Pour cela, aller dans l'onglet **Service**, puis dans la section **DHCP serveur**. Cocher la case **Enable DHCP serveur on LAN interface**. Entrer ensuite la plage d'adresses IP qui sera attribuée aux clients. Avant d'activer le service DHCP de PFsense, il faut s'assurer qu'aucun autre serveur DHCP n'est activé sur le réseau afin d'éviter les conflits d'adresse.

Il faut par la suite entrer l'adresse IP du serveur DNS et le nom de domaine qui sera attribué aux clients. Entrer ensuite l'adresse de la passerelle pour les clients. Celle-ci sera l'adresse du portail captif : **192.168.3.x,** puis les autres paramètres peuvent être laissés par défaut (figure IV.20).

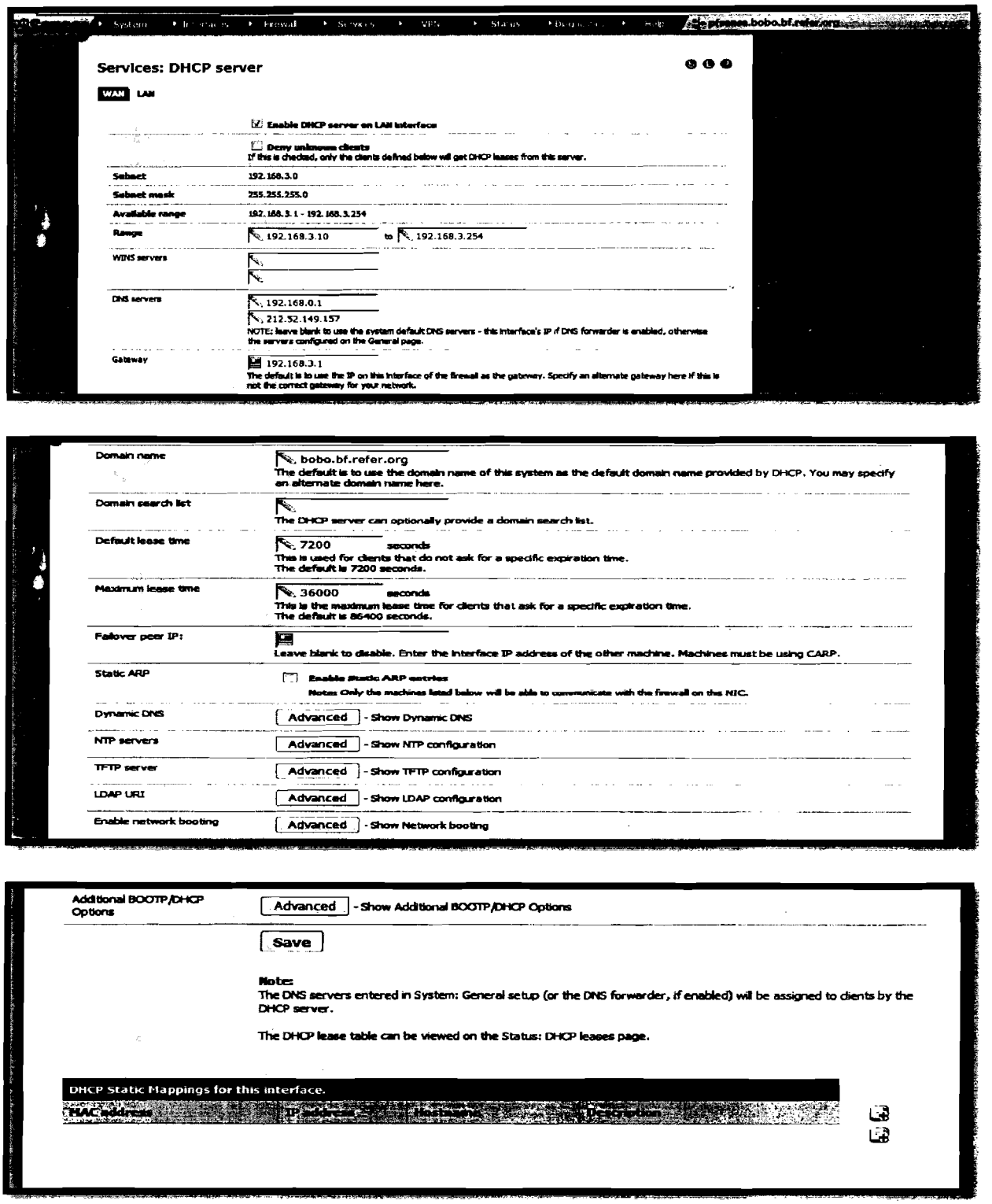


**Figure IV.20 : Configuration du serveur DHCP**

IV.5.2.4. Définition des règles du firewall

PFsense étant aussi un firewall, il faut définir certaines règles élémentaires sur les interfaces pour leur permettre de communiquer entre elles, et avec l'extérieur. Pour cela, aller dans l'onglet **Firewall** puis dans la section **Rules**, puis sélectionner une interface sur laquelle on veut définir des règles [6].

Ainsi sur l'interface LAN, il faut laisser les règles par défaut car elles autorisent tous les paquets IP de source LAN à n'importe quelle destination. Pour le WAN, il faut modifier car tout est bloqué par défaut, ce qui empêche les deux interfaces de se communiquer. Alors cliquer sur le symbole « **e** » pour éditer une règle qui va permettre le passage des paquets du WAN vers le LAN. Pour cela, dans **Action**, choisir l'option **PASS** ; dans **Protocol**, choisir **ANY** ; dans **Interface**, sélectionner **WAN** ; dans **Source**, sélectionner **WAN Subnet** puis dans **Destination** choisir **LAN** (figure IV.21).

Dans certains cas il peut être nécessaire de définir des règles flottantes, c'est-à-dire des règles indépendamment des interfaces. Pour cela, dans l'onglet **Rules,** puis dans le sous-onglet **Floatting**, cliquer sur le symbole « **e** » pour éditer cette règle (le symbole «+» permet d'ajouter une nouvelle règle et le symbole « **x** » permet de supprimer une règle).

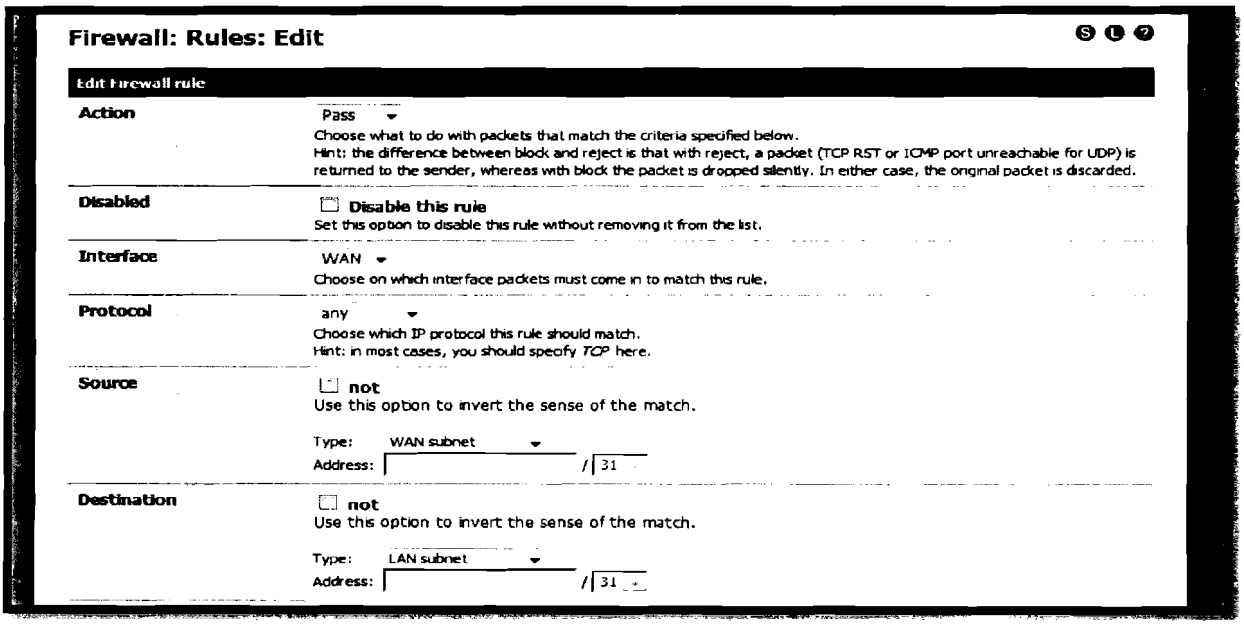


**Figure IV.21 : Règles sur l'interface WAN**

Ainsi PFsense est correctement configuré, mais pour le moment il sert uniquement de firewall et de routeur. Il reste à activer l'écoute des requêtes sur l'interface LAN et contraindre les utilisateurs à s'authentifier pour traverser le firewall.

# Chapitre V :

## Implémentation du portail captif de PFsense

### V.1. Paramètres généraux

Pour activer le portail captif sur l'interface LAN de PFsense, il faut aller dans l'onglet **Service** puis dans la section **Captive portal**. Ensuite il faut cocher la case **Enable Captive portal**, puis choisir l'interface sur laquelle le portail captif va écouter. Ici nous avons choisi LAN puisque nous voulons que les utilisateurs de notre réseau local passent par le portail captif pour aller sur Internet [7].

Dans les options suivantes, il faut d'abord définir le nombre de clients demandant la page d'authentification à la fois, ensuite le temps au bout duquel le client sera automatiquement déconnecté s'il est inactif et le temps au bout duquel il sera déconnecté quel que soit son état puis se voir redemander les paramètres d'authentification. Ainsi **Maximum concurrent connections** défini le nombre de clients demandant la page captive à la fois ; **Idle Timeout** défini le temps au bout duquel un client inactif sera automatiquement déconnecté et **Hard Timeout** défini le temps au bout duquel il sera déconnecté quel que soit son état.

Nous avons choisi de mettre 10 pour le nombre de connexions simultanées, 1 heure pour l'inactivité et 72 heures pour les déconnections brutales.

Ensuite il est possible d'activer ou non une fenêtre popup qui va servir aux clients de se déconnecter. Nous avons préféré ne pas mettre cette option, car de nombreux utilisateurs utilisent des anti-popup et donc ne verront pas ce message. Il est ensuite possible de rediriger un client authentifié vers une URL spécifiée, sinon il est redirigé vers la page demandée initialement. Nous avons choisi de rediriger le client vers l'URL suivante : http : //www.google.com.

Le paramètre suivant **Concurrent user login**, permet d'éviter les redondances de connexions. En effet, l'utilisateur ne pourra se connecter qu'à un seul compte actif à la fois. Cela va donc éviter les usurpations d'identité. En cochant ce paramètre, seule la dernière connexion sera active. Il est aussi possible de filtrer les clients par adresse MAC (figure.V.1, figure V.2).

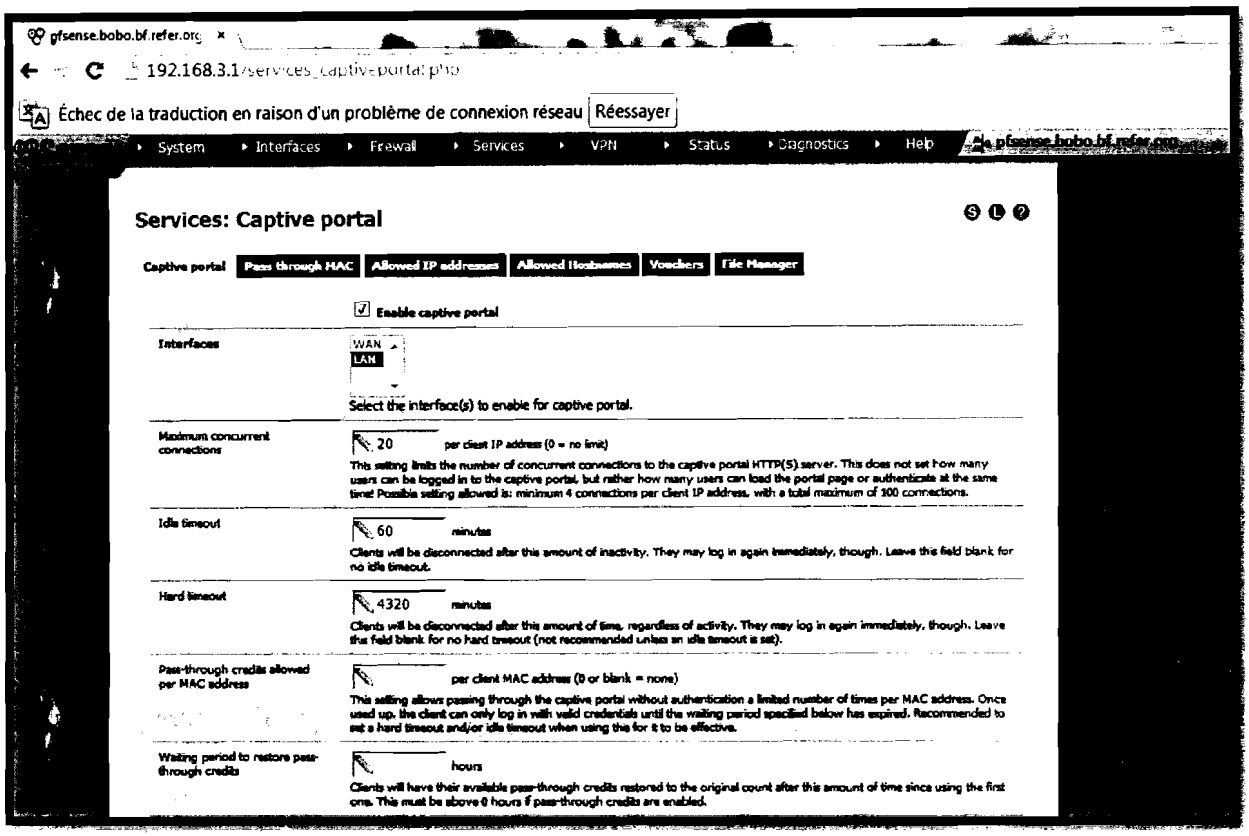


**Figure V.1 : Activation du portail captif**

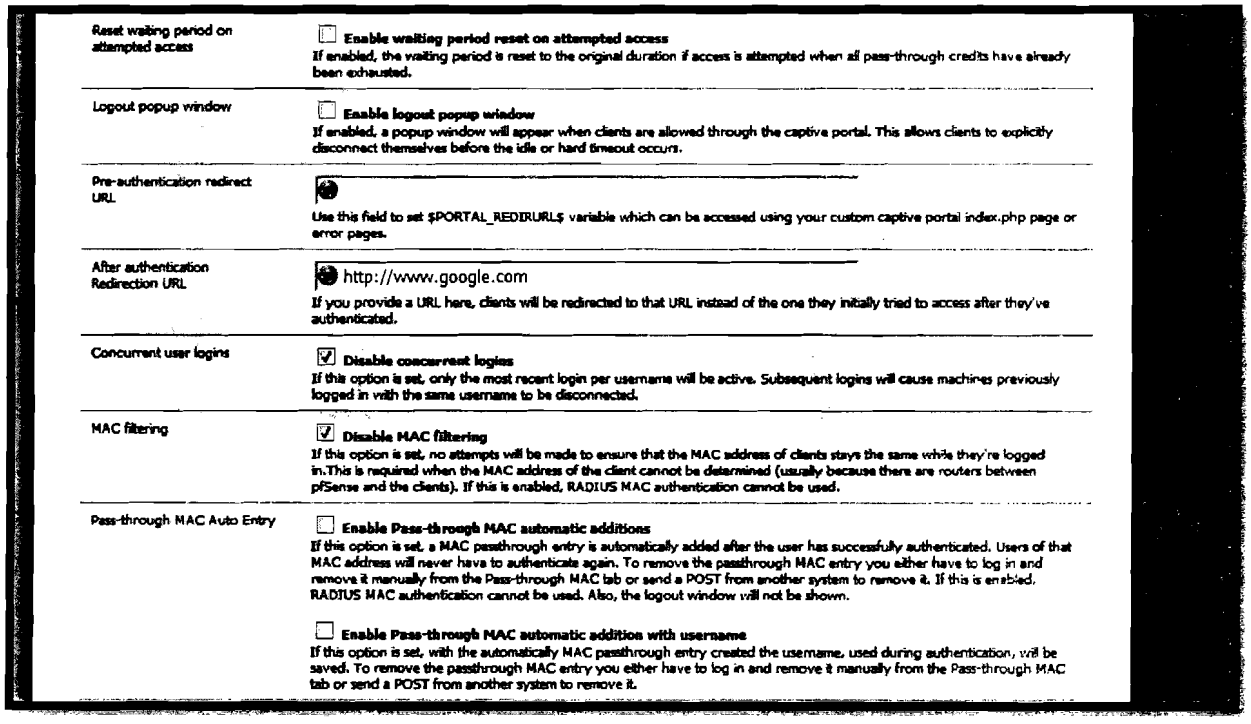


**Figure V.2 : Paramètre de la page de redirection**

Le paramètre de la figure V.3 **Enable per-user bandwidth restriction** permet de fixer un débit maximum montant et descendant de flux Internet par utilisateur afin d'éviter qu'un utilisateur surcharge la bande passante disponible.

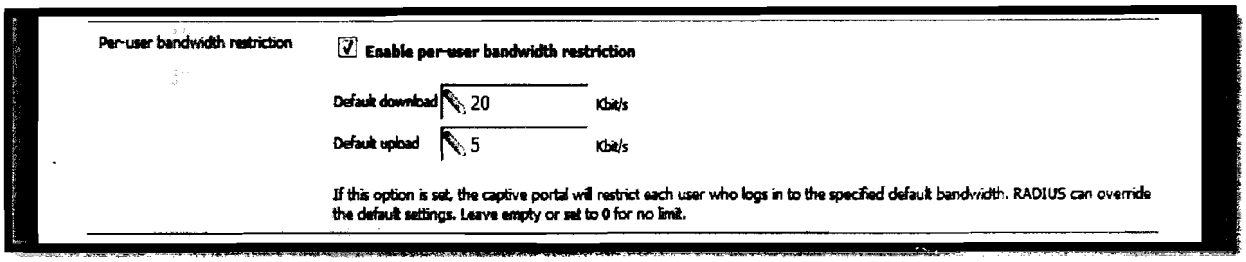


**Figure V.3 : Limitation de la bande passante**

Une fois cette configuration sauvegardée, le portail captif devrait être fonctionnel. On peut aussi modifier la page d'accueil du portail pour l'adapter au besoin de l'entreprise (figure V.6), ainsi que la page de redirection (figure V.7) en cas d'échec d'authentification en important un code HTML ou PHP dans les champs prévus à cet effet (figure V.4). Tout ceci dans un souci de rendre plus conviviale la page captive.

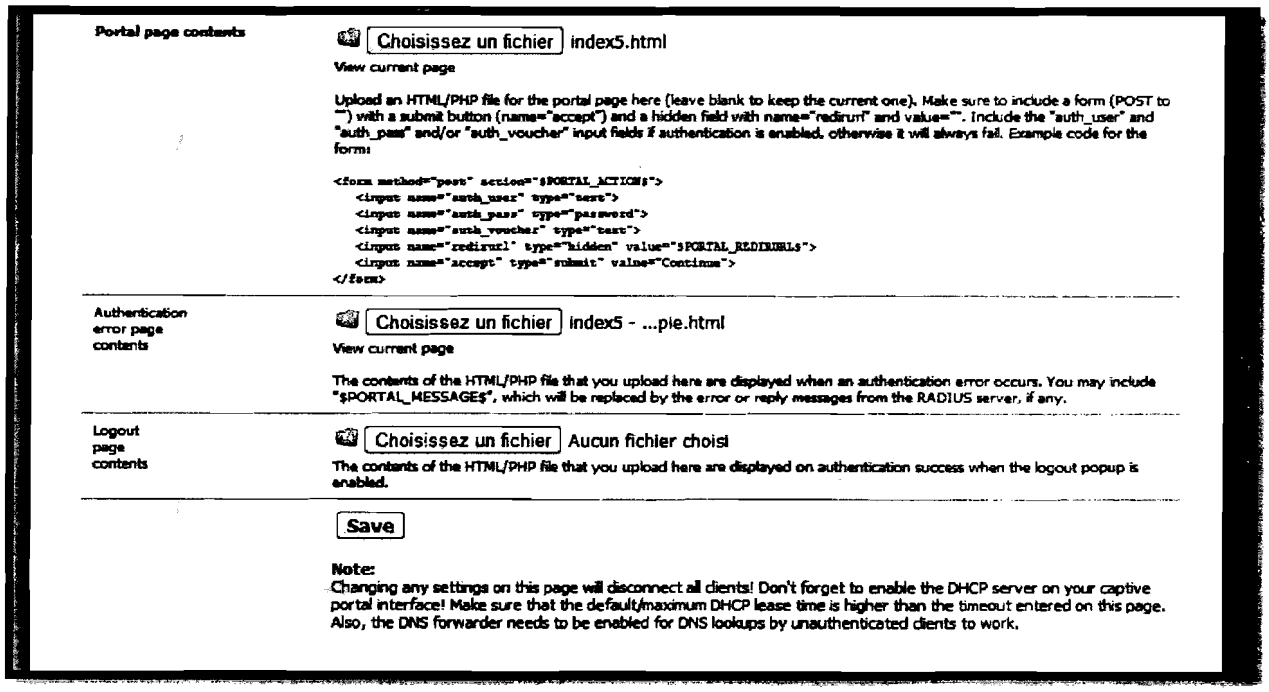


**Figure V.4 : Importation de code HTML**

Il est possible d'insérer des images telles qu'un logo de l'Université dans la page d'accueil. Pour cela, aller dans le sous onglet **File Manager** pour télécharger l'image à afficher. Toutefois la taille de cette image ne doit pas excéder 1MB (voir figure V.5).

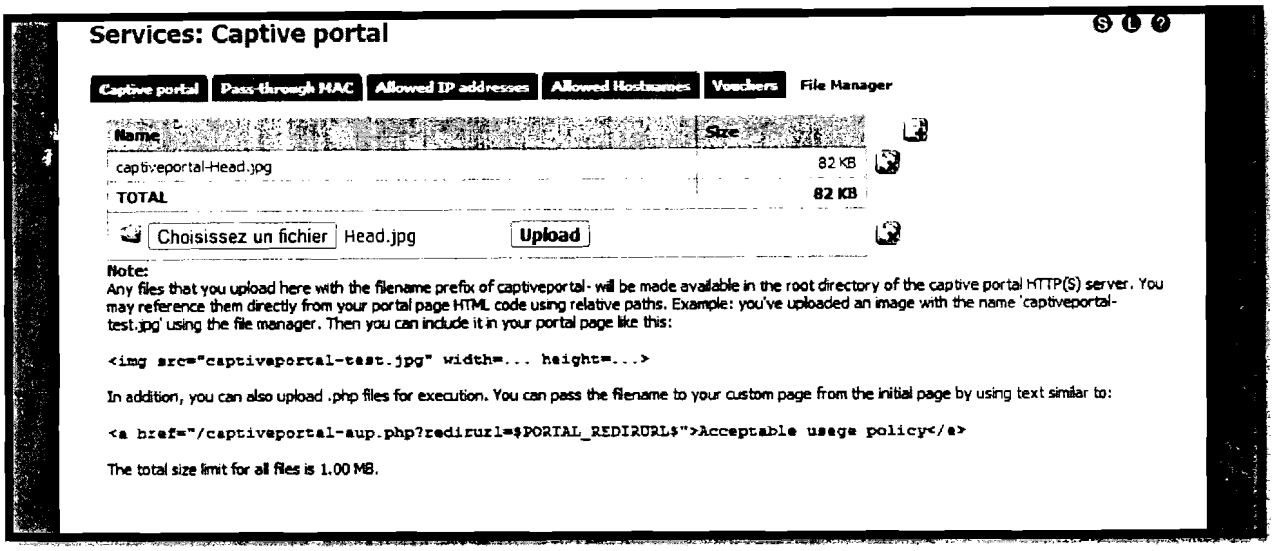


**Figure V.5 : Importation d'image**

Le paramètre **Pass-through MAC** sert à définir les adresses MAC autorisées à traverser PFsense sans authentification. **Allowed IP address** sert à définir les adresses IP autorisées à se connecter sans authentification. **Allowed Hostnames** sert à définir les noms d'hôtes autorisés à traverser PFsense sans authentification et **Vouchers** sert à définir les groupes d'utilisateurs autorisés à se connecter à PFsense. En revanche ces paramètres ne sont pas utilisés à l'étape actuelle de l'étude.

Après importation de nos pages et image d'accueil, voici ce que nous obtenons :

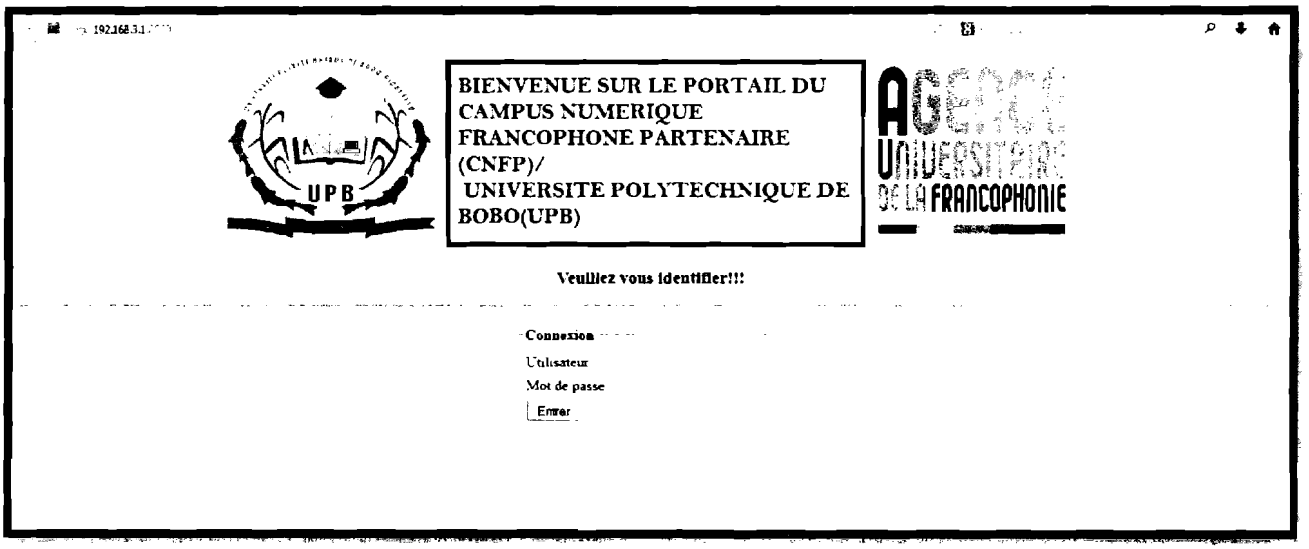


**Figure V.6 : Page d'accueil du portail**

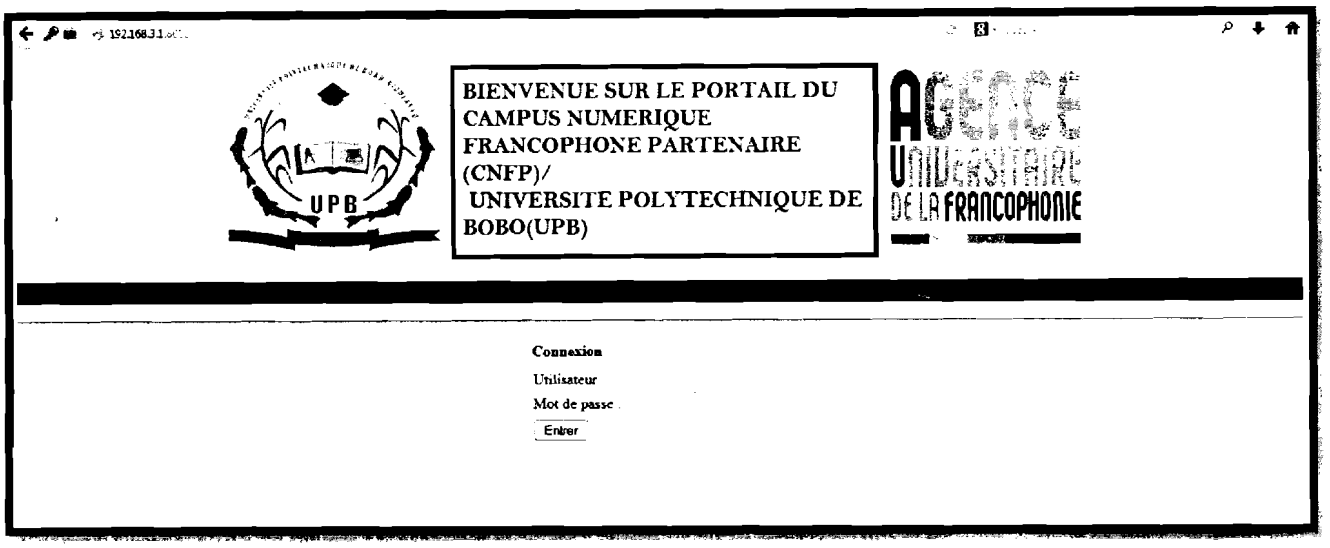


**Figure V.7 : Page d'échec**

## V.2. Authentification et gestion des utilisateurs

L'authentification est un point essentiel de PFsense puisqu'elle définit l'autorisation d'accès vers l'extérieur ; une sorte de portail physique fermé accessible par clé. Ainsi trois méthodes d'authentification sont offertes :

- sans authentification (**No authentification) :** les clients sont libres ; ils verront le portail mais il ne leur sera pas demandé de s'authentifier ;
- authentification via un fichier local **(Local User manager) :** les paramètres des comptes utilisateur sont stockés dans une base de données locale au format XML ;
- authentification via un serveur RADUIS (**RADIUS Authentification**) : à ce niveau, nous avons le choix entre utiliser un serveur embarqué **FreeRADIUS** et utiliser un serveur RADIUS distant du serveur PFsense.

Pour ce projet nous avons testé les trois types d'authentification avec succès et nous avons retenu l'authentification RADIUS embarqué car non seulement cela permet de gérer un grand nombre d'utilisateurs, mais aussi pour des raisons de sécurité. A ce stade, le portail est déjà accessible, c'est-à-dire que pour un utilisateur qui se connecte au réseau local et à partir de son navigateur, demande une page web, il sera redirigé vers la page captive qui lui demandera de s'authentifier avant d'avoir accès à la page demandée initialement.

**NB** : Si le portail apparaît et que l'utilisateur entre correctement ses identifiants mais qu'il n'a pas accès à Internet, il peut être nécessaire de définir une route statique qui permet à

l'interface LAN d'accéder au serveur de nom de domaine. Pour cela, aller dans l'onglet **System >Route > Static Routing.**

### V.2.1 L'authentification par RADIUS

RADUIS (Remote Authentification Dial-In User Service) est un protocole client-serveur permettant de centraliser des données d'authentifications [`8]. Le client RADIUS appelé NAS (Network Access Server) fait office d'intermédiaire entre l'utilisateur final et le serveur. C'est le standard utilisé aujourd'hui surtout par les fournisseurs d'accès à Internet car il est très malléable et très sécurisé.

PFsense intègre un paquet radius libre (FreeRadius) couplé avec une base de données pour stocker les informations des utilisateurs. Mais on peut aussi utiliser une base de données externe pour y stocker ses données d'utilisateurs. De même, on peut utiliser un serveur RADIUS distant pour authentifier les utilisateurs. Ainsi le CNFP utilise une base de données MYSQL sur un autre serveur pour enregistrer ses utilisateurs. Dans ce cas nous pouvons soit installer un serveur RADIUS sur le serveur MySQL pour stocker les données d'identification dans la base MySQL, soit installer le serveur RADIUS sur le serveur PFsense pour y stocker localement les données d'identification. Dans tous les cas le serveur d'authentification (RADIUS) sera l'intermédiaire entre le portail captif et la base de données (locale ou distante). Pour la phase de test, nous avons exploité le second cas c'est-à-dire installer un serveur embarqué FreeRadius sur le serveur PFsense.

Pour installer le paquet FreeRaduis sur PFsense, il faut aller dans l'onglet **System**, puis **Packages**, puis **Available packages**, puis **FreeRadius** ou **FreRadius2**. Après l'installation (ici nous avons installé FreeRadius2), la configuration se fait en trois étapes :

- d'abord configurer l'interface d'écoute (ici LAN) : pour cela aller dans l'onglet **Service**, puis **Freeradius2,** puis dans le sous onglet **Interface.** Le symbole « + » permet d'ajouter une nouvelle interface; puis entrer l'adresse IP de l'interface (LAN), puis cliquer sur **Save** pour enregistrer ;
- ensuite ajouter un client **NAS** : alors dans l'onglet **NAS/Client** entrer l'adresse locale **127.0.0.1** et les autres paramètres.
- enfin créer un compte utilisateur pour tester la configuration: alors dans l'onglet **User**, cliquer sur le symbole « + » pour ajouter un nouveau compte utilisateur puis entrer le nom d'utilisateur et le mot de passe du compte.

Et pour tester la configuration il suffit d'entrer la commande **'radtest** testuser testpassword

127.0.0.1:1812 0 testing123'dans **Diagnostic**, puis **Command prompt** ; **testuser** étant l'identifiant, **testpassword** le mot de passe, **127.0.0.1** l'adresse locale du client NAS, **1812** le numéro de port du service RADIUS et **testing123** la clé sécrète entre le serveur et le client RADIUS.

Ceci est une configuration pour enregistrer les utilisateurs dans la base locale de FreeRadius.

La configuration de la base de données MySQL distante [9] est fournie en annexe B de ce document.

### V.2.2 Gestion de comptes utilisateurs

Pour ajouter un compte avec authentification Radius, il faut aller dans l'onglet **Service**, puis **Freeradius**, puis **User** pour entrer les paramètres du compte. (Figure V.8)

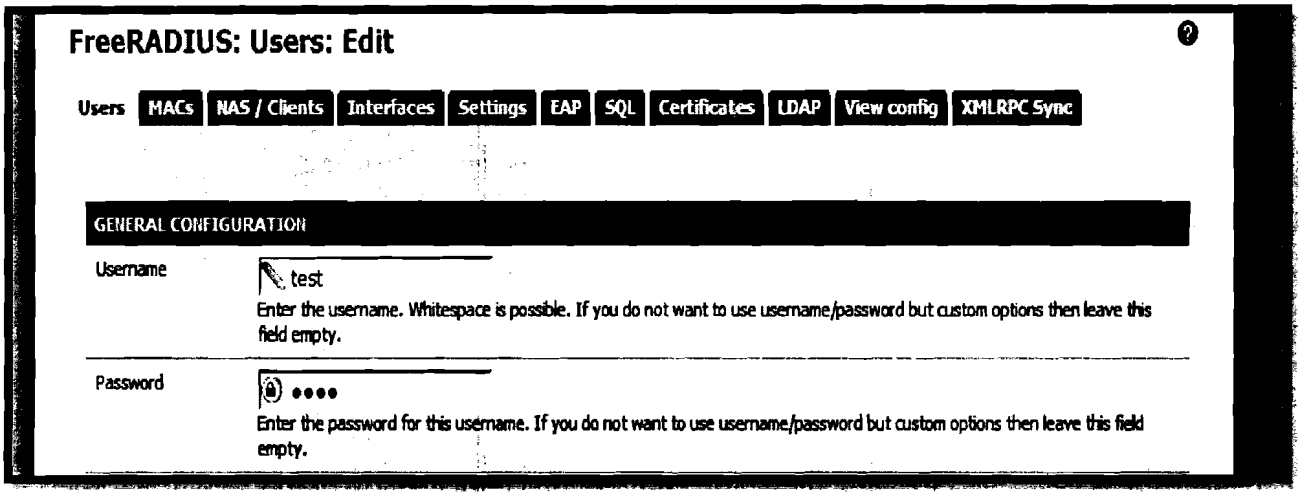


**Figure V.8 : Gestion de comptes avec FreeRadius**

Quant à l'authentification via le fichier local il faut aller dans l'onglet **System** de la figure V.9, puis dans la section **User Manager**. Ici, on a une liste des utilisateurs existants dans la plate-forme. Pour créer un nouvel utilisateur, cliquez sur le symbole « + » et une nouvelle page s'ouvre sur laquelle certains champs sont à compléter :

Il faut en premier lieu activer ou désactiver le compte en décochant ou en cochant la case **Disabled**.

- entrer le nom d'utilisateur pour le compte utilisateur ;
- entrer le mot de passe à utiliser pour la connexion ;
- entrer le nom complet pour le compte utilisateur ;
- entrer la date d'expiration du compte au format indiqué ;

- sélectionner le groupe dont le compte utilisateur doit faire partir (utilisateur ou administrateur) ;
- cliquer sur «**Save** » pour enregistrer le compte.

La figure V.9 illustre cette partie.

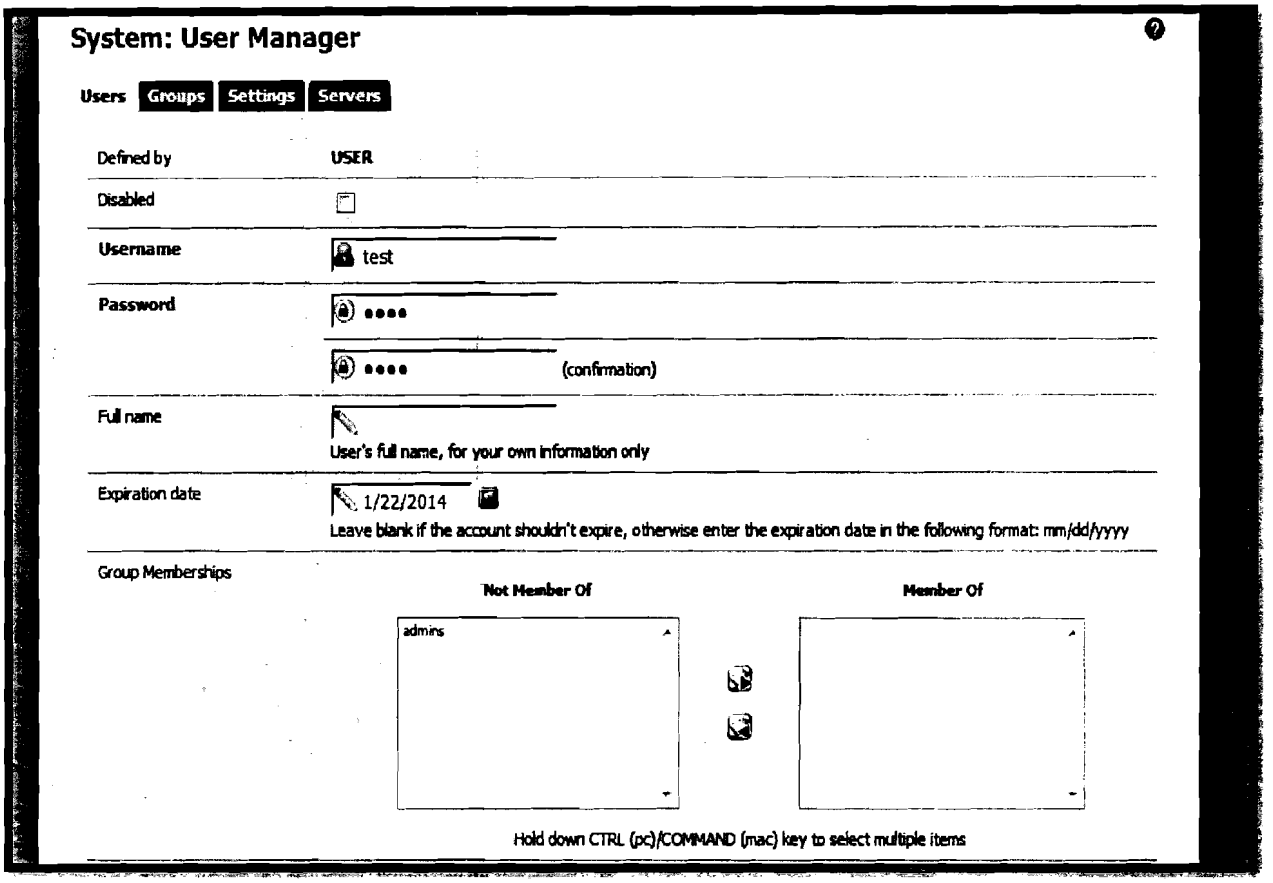


**Figure V.9 : Gestion de compte en local**

## V.3. Sécurité du portail captif

Dans cette partie il est question d'une part de sécuriser l'accès à l'interface web de configuration de PFsense (**webguid**) par le protocole SSL et d'autre part permettre un cryptage des mots de passe des utilisateurs pour assurer une certaine confidentialité des transactions après authentification [10]. Pour se faire l'utilisation d'un certificat est plus que nécessaire. Un **certificat électronique** (aussi appelé **certificat numérique** ou **certificat de clé publique**) étant vu comme une carte d'identité numérique. Il est utilisé principalement pour identifier une entité physique ou morale, mais aussi pour chiffrer des échanges. Il est signé par un tiers de confiance qui atteste du lien entre l'identité physique et l'entité numérique (Virtuel). Le standard le plus utilisé pour la création des certificats numériques est le X.509.

Ainsi le certificat va permettre de crypter les données échangées entre le navigateur et le serveur d'authentification PFsense.

Pour la sécurisation de l'accès au webguig, il faut aller dans l'onglet **System** > **Advanced** de la figure V.10, puis dans la section **Admin Access** pour activez le service **HTTPS** avec son numéro de port **443** (SSL) dans **TCP port.**

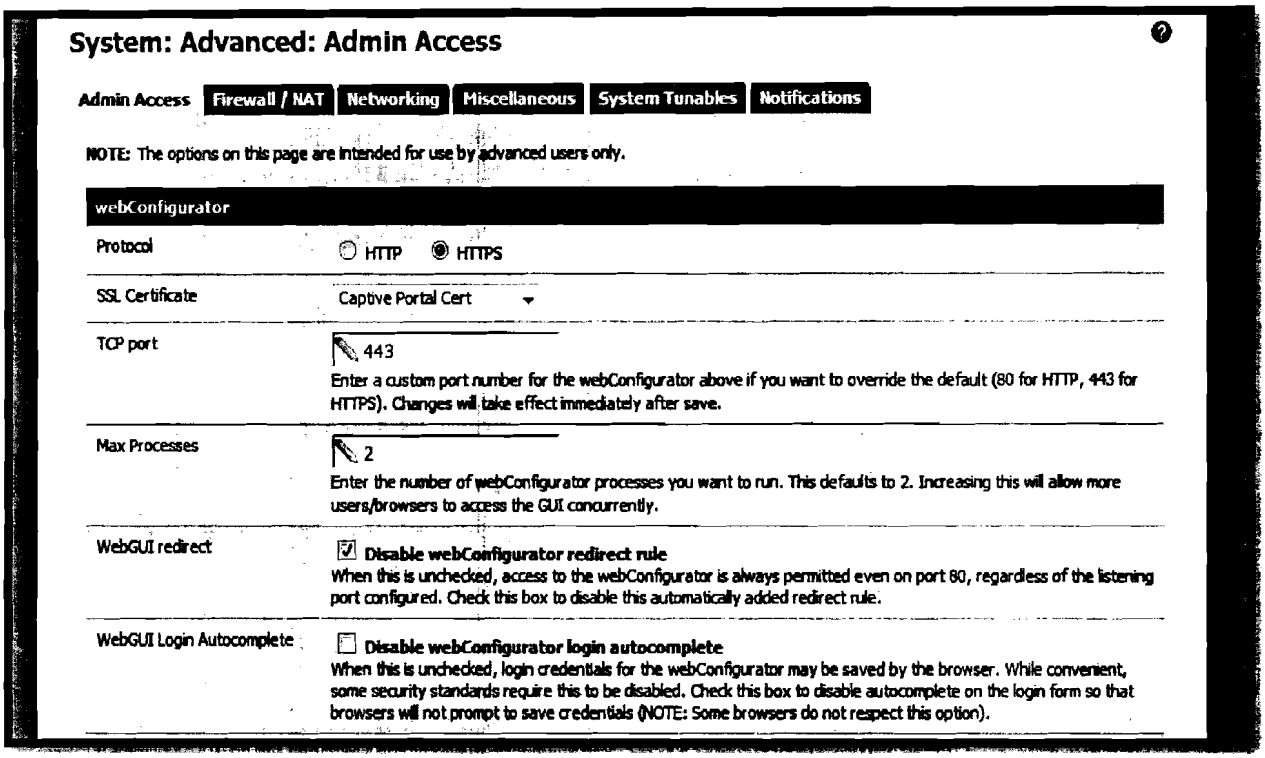


**Figure V.10 : Activation de HTTPS pour l'accès au webguid**

De même pour crypter les mots de passe des utilisateurs et les échanges après leur authentification, il faut créer un certificat pour pouvoir activer HTTPS. Ce qui se fait en trois étapes : choix du type de certificat (autogéré ou proclamé par une autorité de certification), création et téléchargement du certificat puis activation du certificat sur le portail. Pour ce faire aller dans l'onglet **System** puis **Cert Manager** (voir figure V.11 et figure V.12).

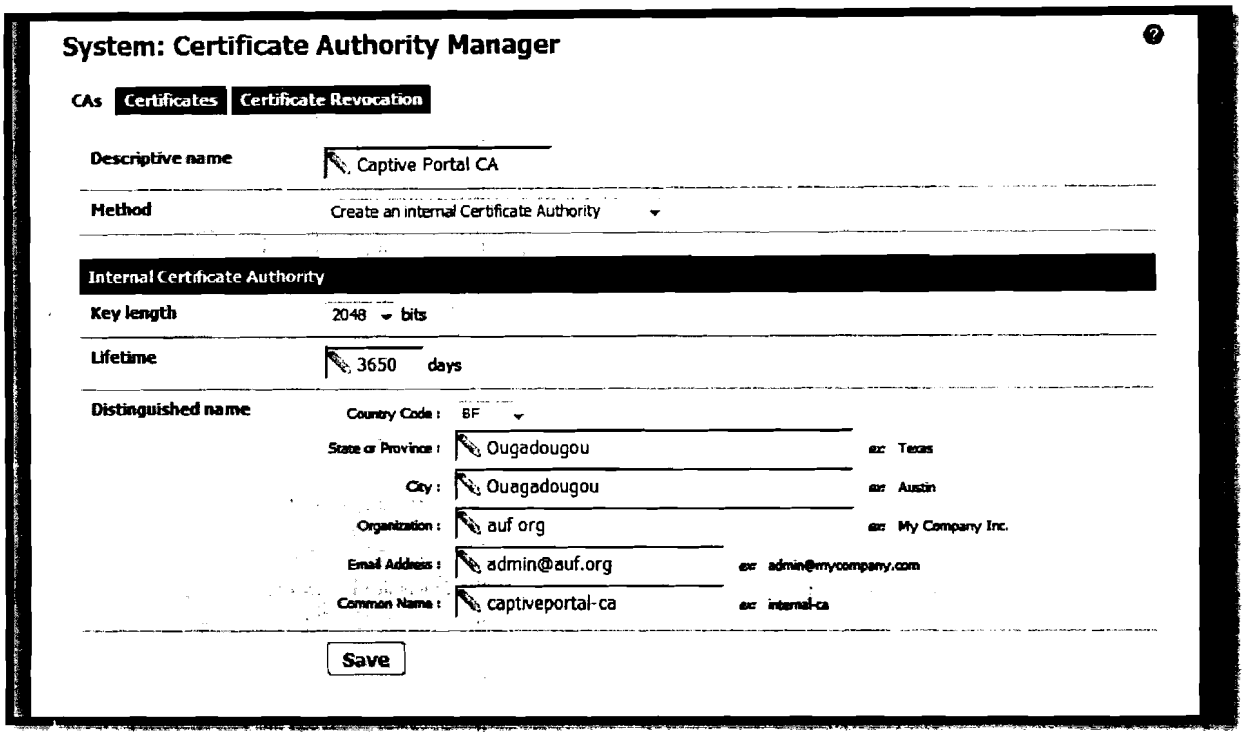


**Figure V.11 : Choix du type de certificat**

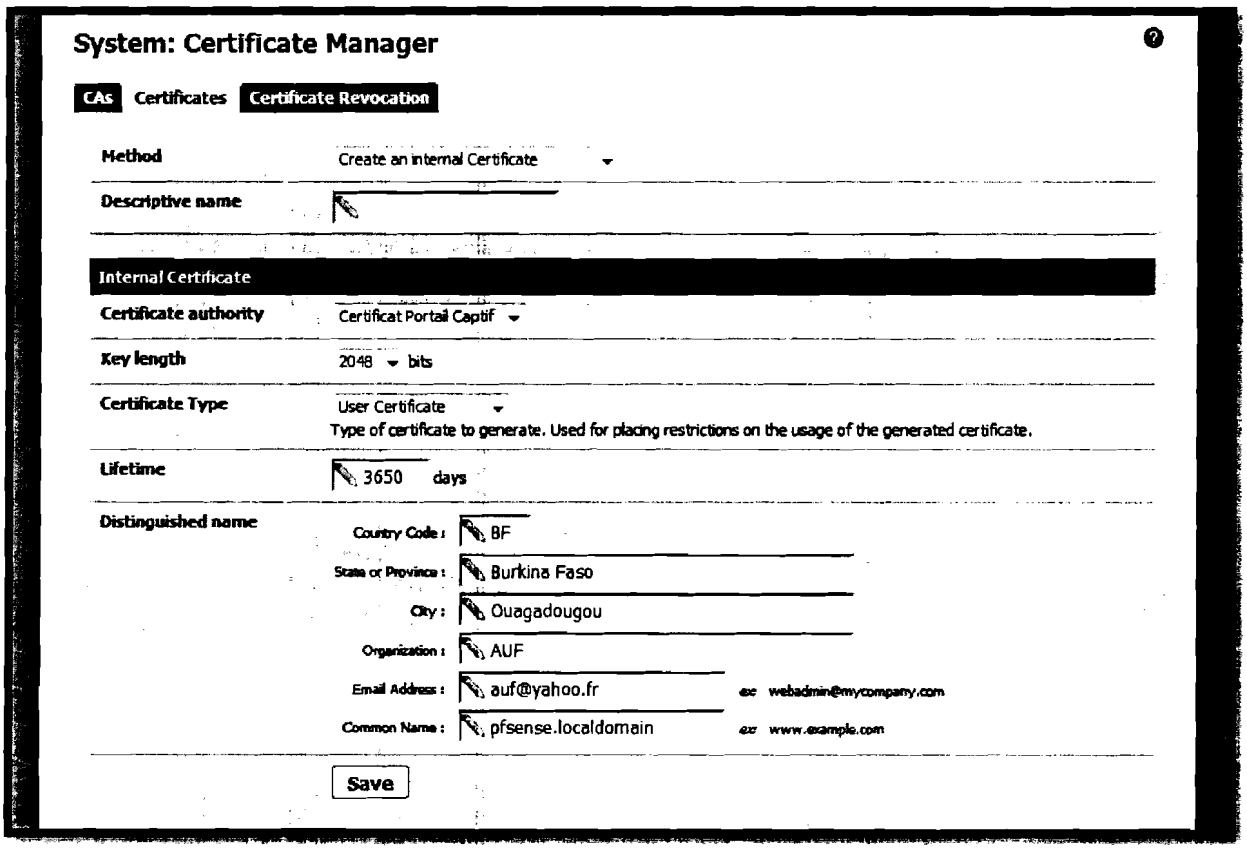


**Figure V.12 : Paramètres du certificat**

Il faut vérifier que le certificat a été bien créé puis il suffit de le télécharger (figure V.13).

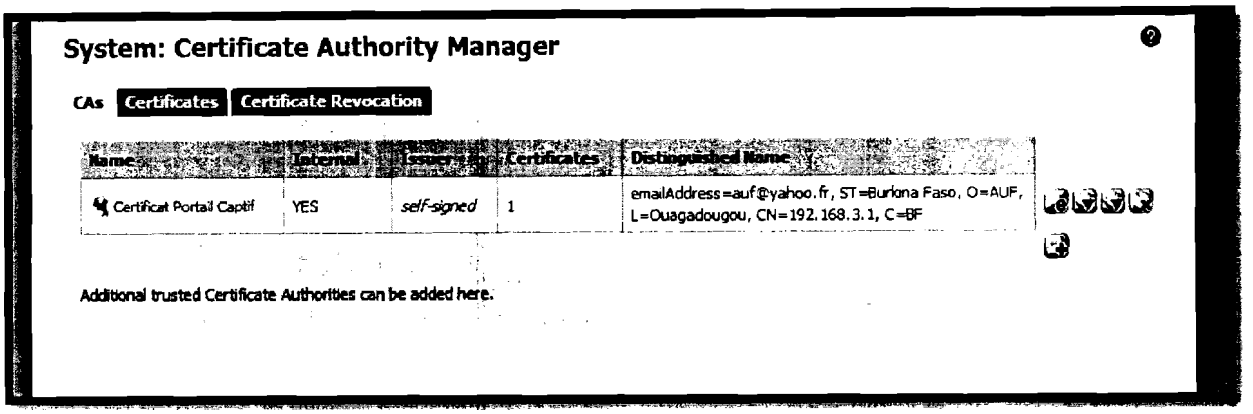


**Figure V.13 : Certificat téléchargé**

Après le téléchargement du certificat aller dans **Service** puis **Captive Portal** pour l'insérer avec sa clé. Cocher ensuite **Enable HTTPS login** en donnant le nom du serveur HTTPS (**HTTPS server Name**). (Figure V.14).

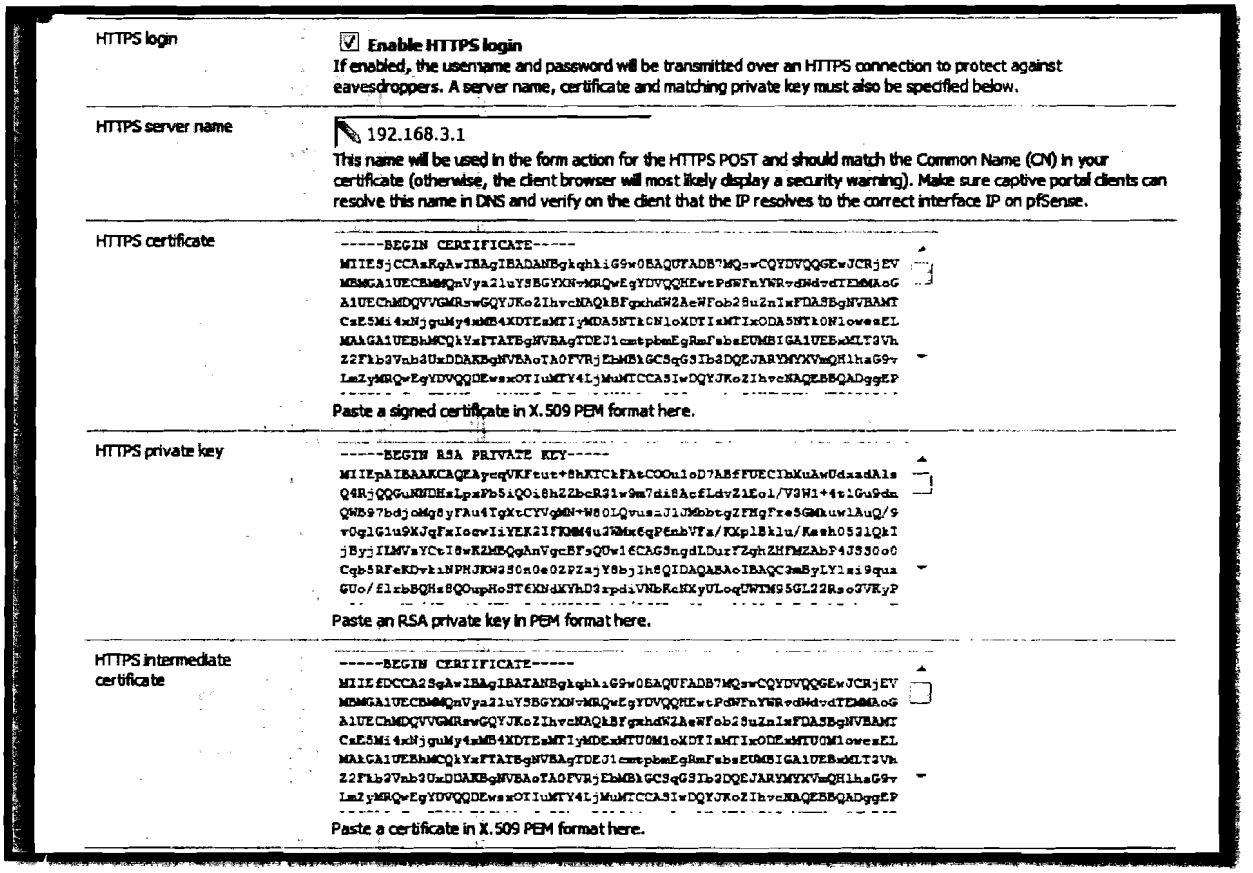


**Figure V.14 : Importation du certificat et de sa clé privée**

A présent le portail autorisera l'accès aux pages web sécurisées et sa sécurité semble renforcée

dans la mesure où la récupération des mots sur le réseau est quasiment impossible.

Cependant pour le test nous n'avons pas utilisé de certificat car la plupart des certificats sont payants mais nous espérons que l'entreprise se dotera de certificat pour le déploiement définitif.

## V.4. Contrôle de la bande passante

### V.4.1 Introduction à la QoS

Le terme **QoS** (acronyme de « Quality of Service », en français « Qualité de Service ») désigne la capacité à fournir un service (notamment un support de communication) conforme à des exigences en matière de temps de réponse et de bande passante [11]. C'est la capacité à véhiculer dans de bonnes conditions un type de trafic donné, en termes de disponibilité, de débit, de délai de transmission, de gigue, de taux de perte de paquet. La mise en place de la QoS peut se faire sur la base de nombreux critères mais dans notre cas elle va se baser sur la consommation de la bande passante. La qualité de service se réalise au niveau de la couche 3 du modèle OSI. Elle doit donc être configurée sur les routeurs ou la passerelle reliée à Internet. Ainsi PFsense étant aussi doté de fonction de routeur, des paquets y sont intégrés pour la gestion de la bande passante. Ce sont entre autres :

- **Traffic Shapper** ou regulateur de flux qui permet de contrôler le volume des échanges sur le réseau ;
- **Bandwitch** qui liste les usages du réseau et construit des fichiers HTML sous forme de graphique et de résumés ;
- **Pftop** qui donne une vue en temps réel des connexions au pare-feu, et la quantité de données qui sont envoyées et reçues. Il peut aider à identifier les adresses IP qui utilisent actuellement de la bande passante ;
- **Ntop** qui permet aussi d'avoir une vue globale sur la consommation de la bande passante. Cet outil sera exploité par la suite pour sa simplicité d'administration ;
- **etc.**

### V.4.2 Contrôle de bande passante avec NTOP

Ntop est un applicatif libre écrit de manière portable afin de pouvoir fonctionner sur toutes les plateformes Unix. Il permet d'avoir une vue globale sur la consommation de la bande passante, il est capable de détecter jusqu'à où les connexions ont été faites par les ordinateurs

locaux et combien de bandes passantes ont été utilisées sur des connexions individuelles. Il fait partie des paquets disponibles sur PFsense et nous l'avons à cet effet exploité.

### V.4.2.1. Installation de Ntop sur PFsense

Comme l'installation de tout autre paquet sur PFsense, se connecter sur l'interface de PFsense à partir du LAN, le WAN étant connecté à Internet, puis dans l'onglet **System** > **Packages** >**Avaible Package** (figure V.15) pour voir les paquets disponibles et sélectionner Ntop pour l'installer.

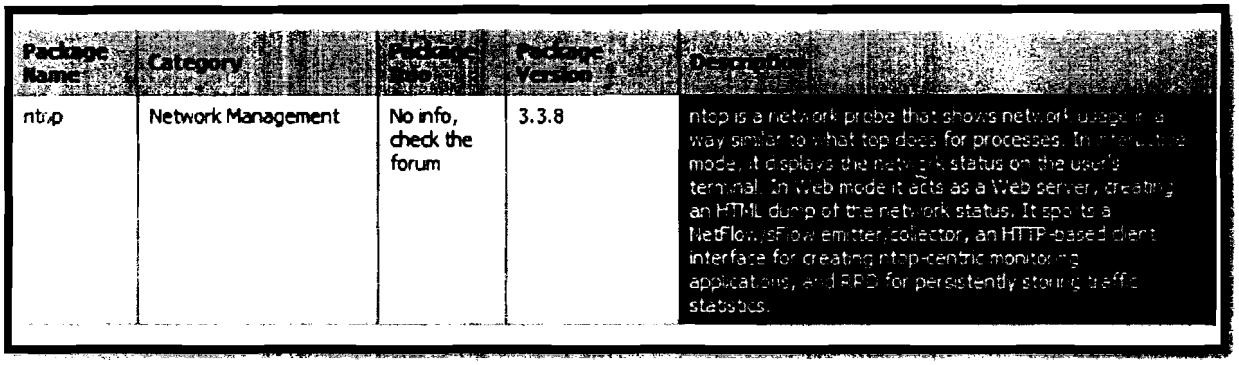


**Figure V.15 : Installation du paquet Ntop**

### V.4.2.2. Configuration du service Ntop

Une fois l'installation terminée, il faut se rendre dans l'onglet **Diagnostics** > **Ntop Settings** de la figure V.16 pour initialiser Ntop et lancer le service correspondant. Les paramètres disponibles ici sont moindres, et permettent seulement de configurer le mot de passe administrateur pour accéder à la configuration avancée de Ntop, ainsi qu'à l'interface d'écoute.

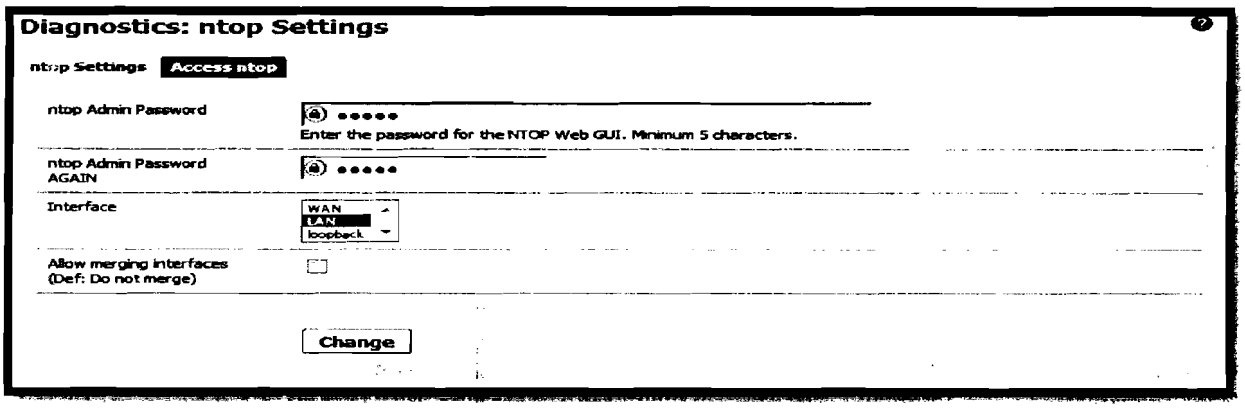


**Figure V.16 : Configuration de mot de passe Ntop**

Désormais Ntop est accessible via le navigateur à l'adresse suivante : **http://<@pfsense>:3000** (mais aussi en cliquant directement sur le bouton « **Access ntop** » ci-dessus, ou encore via le menu PFsense « **Diagnostics** > **ntop** »). En se connectant à cette adresse, on accéde aux statistiques générales de notre réseau comme le montre la figure V.17, la figure V.18 et la figure V.19 :

- Des informations concernant Ntop (interface d'écoute, le nom du domaine…)

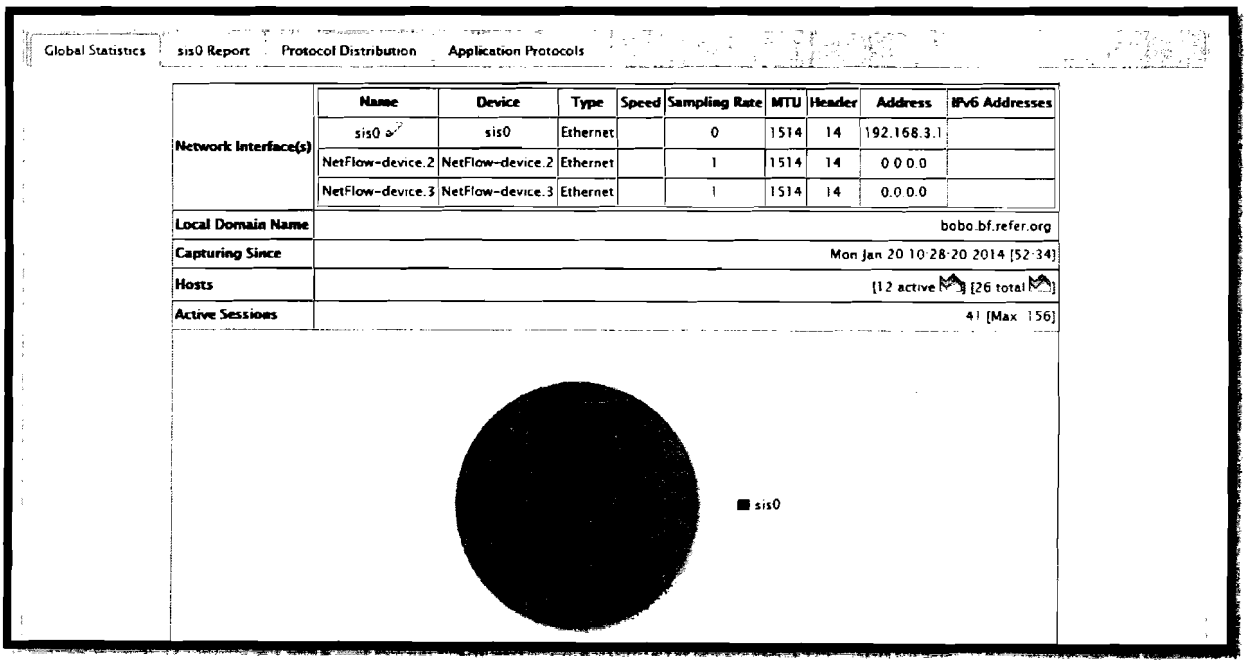


**Figure V.17 : Statistiques globales**

- Un rapport concernant le trafic sur l'interface d'écoute (paquet, trafic ou la charge)

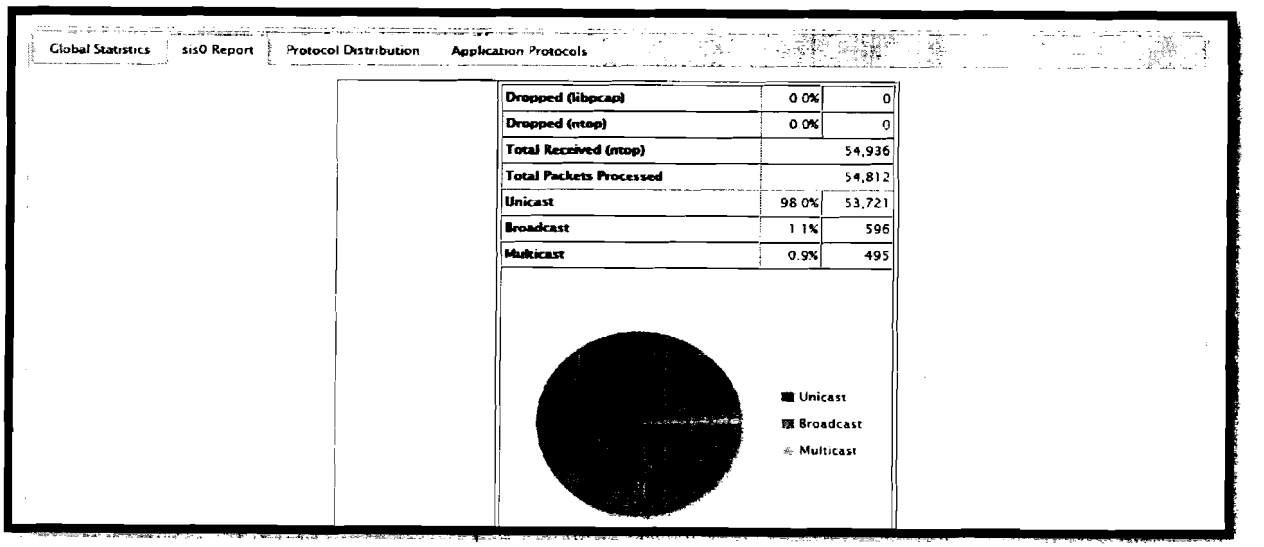


**Figure V.18 : Rapport du trafic sur l'interface d'écoute**

- La répartition totale des protocoles

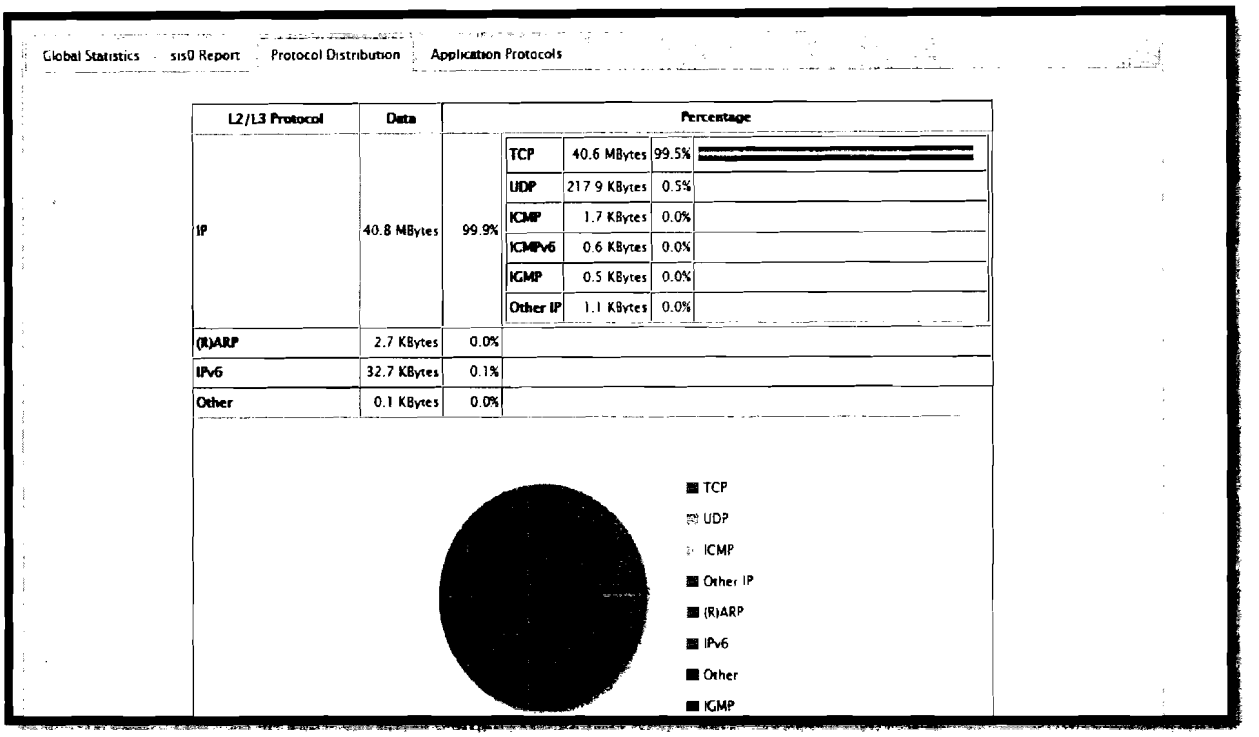


**Figure V.19 : Vue des protocoles**

Sur l'interface de Ntop se trouvent beaucoup d'autres options qui ne sont pas détaillées ici.

Et pour finir, la configuration proprement dite de Ntop ne sera pas détaillée, mais reste relativement simple et est fonction des besoins personnels tant l'outil tel qu'installé est déjà entièrement exploitable. Dans tous les cas, le menu « **admin** » offre toutes les options nécessaires pour personnaliser Ntop.

## V.5. Coûts d'implantation

La solution qui vient d'être mise en place peut être déployée en deux semaines par deux ingénieurs de travaux informatiques. Ainsi le coût de mise en œuvre de ce projet, compte tenu de sa durée, de la main d'œuvre et des équipements nécessaires à sa réalisation ; est estimé à 1 900 000 FCFA ; les détails étant consignés dans le tableau V.1.

**Tableau V.1 : Coûts d'implantation**

| Désignations | Coûts en F CFA |
|---|---|
| Coût du matériel | 600 000 |
| Apport technique | 1 000 000 |
| Formation de l'administrateur | 300 000 |
| Total | 1 900 000 |

# CONCLUSION GENERALE

Pour authentifier les utilisateurs de son réseau afin de partager la connexion Internet de façon sécurisée, l'UPB à travers le CNFP s'est orientée vers une solution de portail captif. Après une présentation de la structure d'accueil, la démarche suivie pour cette étude a permis d'analyser d'abord son système informatique pour connaître ses forces et faiblesses. Ensuite une étude comparative de portail captif a permis de choisir une solution à implanter. C'est ainsi que la solution PFsense a été retenue. Cet applicatif libre a été ensuite étudié de façon technique et sa fonction captive a été implantée de façon effective. Enfin le paquet Ntop intégré à PFsense a été installé et configuré pour avoir une vue globale sur la consommation de la bande passante.

Nous pensons que le but de ce projet est atteint car, il nous aura permis de savoir d'abord l'existence de solutions libres de portail captif, ensuite de mener une étude comparative et de faire enfin l'implémentation concrète de la solution libre PFsense.

Pour finir, l'outil PFsense tel que conçu, propose d'autres services réseau qui peuvent être mis à profit en fonction des besoins.

# REFERENCES BIBLIOGRAPHIE

[1] http://www.statistique-mondiale.com :

Visiter le 03/09/2013

[2] http://wifihotspot888.com/?page_id=181. wifi Hostspot 888 :

Visiter le 16/08/2013

[3] http://fr.wikipedia.org/wiki/Pfsense principe :

Etude faite le 12/08/2013

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

Visiter le 25/09/2013

[5]http://www.memoireonline.com/02/10/3156/m_Implementation-dune-infrastructure-securisee-dacces-internet-portail-captif0.html :

Visiter le 08/10/2013

[6] https://forum.pfsense.org/index.php?topic=43451.0 pfSense Forum :

Visiter le 17/10/2013

[7] https://www.totorux.info/weblog/?p=164. totorus & linux :

Etude faite le 21/10/2013/

[8] http://blog.stefcho.eu/?p=854 blog pfsense authentification :

Visiter le 29/10/2013

[9] http://blog.stefcho.eu/?p=814 blog pfsense HTTPS :

Visiter le 04/11/2013

[10] http://www.osnet.eu/fr/content/qos-avec-pfsense-20-hfsc-dans-le-d%C3%A9tail :

Visiter le 11/111/2013

[11] http://pfsensesolution.blogspot.com/2013/01/bandwidth-usage-probe.html :

Visiter le 10/08/2013

# ANNEXES

# Annexe A : Les options de la configuration en mode console

### A.1 Assign Interfaces

Cela va redémarrer la tâche d'affectation des interfaces, qui a été couvert précédemment dans l'installation. Vous pouvez créer des interfaces VLAN, réaffecter les interfaces existantes, ou en créer de nouvelles.

### A.2 Set interface(s) IP adress

Cette option peut être utilisée de manière évidente pour définir l'adresse IP des interfaces mais il y a aussi d'autres tâches utiles qui surviennent lors de l'utilisation de cette option. Par exemple, quand ce paramètre est choisi, vous obtenez également la possibilité d'activer ou de désactiver le DHCP sur l'interface, et de régler la plage d'adresses IP DHCP.

### A.3 Reset web Configurator password

Cette option permet de réinitialiser le nom d'utilisateur et mot de passe WebGUI, respectivement à admin et PFsense.

### A.4 Reset to factory default

Cela permet de restaurer la configuration du système aux paramètres d'usine. Cela n'apporte cependant pas de modifications au système de fichiers ou aux paquets installés sur le système d'exploitation. Si vous soupçonnez que les fichiers système ont été endommagés ou modifiés, le meilleur moyen consiste à faire une sauvegarde, et réinstaller à partir du CD ou autre support d'installation.(Également possible dans le WebGUI, onglet **Diagnostic** puis **Factory de faults**).

### A.5 Reboot system

Arrête proprement pfSense et redémarre le système d'exploitation.(Également possible dans le Web GUI, onglet **Diagnostic** puis **Reboot**).

### A.6 Halt system

Arrête proprement pfSense et met la machine hors tension (Également possible dans le WebGUI, onglet **Diagnostic** puis **Halt system**).

### A.7 Ping host

Joint une adresse IP, à qui seront envoyées trois demandes d'écho ICMP. Le résultat du ping sera montré, y compris le nombre de paquets reçus, les numéros de séquence, les temps de réponse et le pourcentage de perte de paquets.

### A.8 Shell

Démarre une ligne de commande shell. Très utile, et très puissant, mais a aussi le

potentiel d'être très dangereux. Certaines tâches de configuration complexes peuvent nécessiter de travailler dans le shell, et certaines tâches de dépannage sont plus faciles à accomplir du shell, mais il y a toujours une chance de provoquer des préjudices irréparables au système s'il n'est pas manipulé avec soin. La majorité des utilisateurs pfSense ne toucheront peut-être jamais au shell, ou même ignoreront qu'il existe. Les utilisateurs de FreeBSD pourront se sentir à l'aise, mais il y a beaucoup de commandes qui ne sont pas présentes sur le système pfSense, puisque les parties inutiles de l'OS ont été supprimées pour des contraintes de sécurité ou de taille.

**A.9 pfTop**

Pftop vous donne une vue en temps réel des connexions du pare-feu, et la quantité de données qu'ils ont envoyées et reçues. Il peut aider à identifier les adresses IP qui utilisent actuellement de la bande passante et peut aussi aider à diagnostiquer d'autres problèmes de connexion réseau.

**A.10 Filter Logs**

En utilisant cette option vous verrez toutes les entrées du journal de filtrage apparaissant en temps réel, dans leur sous forme brute. Il est possible de voir ces informations dans le WebGUI (onglet **Status** puis **System Logs** et enfin onglet **Firewall**), avec cependant moins de renseignement par lignes.

**A.11 Restart webConfigurator**

Redémarre le processus du système qui exécute le WebGUI. Dans de rares occasions, un changement sur ce dernier pourrait avoir besoin de cela pour prendre effet, ou dans des conditions extrêmement rares, le processus peut avoir été arrêté pour une raison quelconque, et le redémarrer permettrait d'y rétablir l'accès.

**A.12 PFsense Développer Shell**

Le shell du développeur est un utilitaire très puissant qui permet d'exécuter du code PHP dans le contexte du système en cours d'exécution. Comme avec le shell normal, il peut aussi être très dangereux à utiliser, et les choses peuvent rapidement mal tourner. Ce shell est principalement utilisé par les développeurs et les utilisateurs expérimentés qui sont familiers avec à la fois le code PHP et le code de base de PFsense.

**A.13 Upgrade from console**

En utilisant cette option, il est possible de mettre à niveau le firmware de PFsense, et ce en entrant l'URL de l'image PFsense à mettre à niveau, ou grâce à un chemin d'accès local vers une image téléchargée d'une autre manière.

**A.14 Enable Secure Shell (sshd)**

Cette option vous permettra de changer le statut du démon Secure Shell, sshd. Son activation par le WebGUI est détaillée dans la suite de ce document. Il est maintenant possible de se connecter à l'interface web en prenant comme URL l'adresse LAN de la machine.

# Annexe B : L'authentification RADIUS à partir d'une base de données MySQL

## Installation du paquet RADIUS

Nous allons à présent installer les paquets "freeradius" "freeradius-utils" et "freeradius-mysql".

- aptitude install freeradius
- aptitude install freeradius-utils
- aptitude install freeradius-mysql

## Installation du client/serveur MySQL.

Installons le paquet "mysql-server" et "mysql-client". Lors de l'installation de la partie Server, vous allez devoir spécifier le mot de passe "administrateur". Retenez-bien ce mot de passe afin de pouvoir vous connecter ensuite au serveur.

- aptitude install mysql-server
- aptitude install mysql-client

## Création d'une base "radius" et d'un compte d'administration "admin_radius".

### Connexion au serveur MySQL :

Mysql –u root –p

### Création de la base de données "radius

Create database radius

### Création de l'utilisateur d'administration :

rant all on radius.* to admin_radius@'%' identified by 'adminadmin'

### Application des droits sur la base :

Flush privileges

Injection SQL pour la création des tables.

### Injection de la table "schema" :

mysql -u admin_radius -p radius < /etc/freeradius/sql/mysql/schema.sql

**Injection de la base "nas" :**

mysql -u admin_radius -p radius < /etc/freeradius/sql/mysql/nas.sql

**Création des NAS (Network Access Server).**

**Création du NAS local pour les tests**

INSERT INTO nas (nasname, shortname, secret) VALUES ('127.0.0.1','localhost','testing123'); **Création du NAS distant (correspond à notre routeur dans notre exemple).**

INSERT INTO nas(nasname,shortname,secret) VALUES ('192.168.10.254','cyberoam','zXv73gm24');

**Création des utilisateurs d'accès.**

**Creation de l'utilisateur toto avec un password en clair.**

INSERT INTO radcheck (Username, Attribute, op,Value) VALUES ('toto','Cleartext-Password',':=','toto123');

**Création de l'utilisateur tata avec un password crypté.**

INSERT INTO radcheck (Username, Attribute, op,Value) VALUES ('tata','Crypt-Password',':=',ENCRYPT('tata123'));

**Configuration RADIUS sur la partie MySQL.**

Pour ce faire nous allons modifier le fichier de configuration /etc/freeradius/sql.conf. Dans votre fichier spécifiez le login et password de connexion au serveur MySQL ainsi que le nom de la base de données (dans notre exemple "radius"). Attention l'option "ReadClient" qui permet d'utiliser la table NAS de notre MySQL est lu seulement au démarrage du service. De ce fait, si vous ajoutez un nouveau périphérique, pensez à relancer votre service RADIUS. Pour la table radcheck (les comptes utilisateurs) vous n'avez pas besoin de redémarrer le service.

**Reboot du service:**

/etc/init.d/freeradius restart

login = admin_radius

password = adminadmin

radius_db = radius

ReadClients = yes

**Configuration RADIUS.**

Nous allons procéder à quelques modifications au niveau du fichier de configuration du RADIUS /etc/freeradius/radius.conf

**Décommentez les lignes suivantes :**

$INCLUDE sql.conf

$INCLUDE sql/mysql/counter.conf

**Commentez la ligne suivante pour gérer vos utilisateurs sur la base :**

$INCLUDE clients.conf

**Reboot du service RADIUS.**

Une fois toutes les modifications apportées, nous procédons au redémarrage du service RADIUS. Afin de visualiser ce qui se passe sur le serveur nous allons utiliser une commande particulière. Le but est de démarrer le service en mode "Debug". Saisissez la commande suivante:

**Arrêt du service :**

/etc/init.d/radius stop

**Execution du service en mode "Debug"**

freeradius -X

**Test de connexion en local.**

On se rappelle que, lors de l'intégration des NAS sur notre base MySQL, il a été ajouté un Routeur et le serveur lui-même "localhost". Nous allons donc tester la connexion au serveur depuis lui-même. Pour ce faire, depuis un autre "tty" exécutez la commande suivante :

user@debian-lab01:~$ radtest toto toto123 127.0.0.1 0 testing123
Sending Access-Request of id 94 to 127.0.0.1 port 1812
User-Name = "toto"
User-Password = "toto123"

user@debian-lab01:~$ radtest toto toto123 127.0.0.1 0 testing123

NAS-IP-Address = 192.168.10.1

id=94, length=20

Si tout est OK on doit avoir ce type de retour. Access-Accept.

**Gestion de la base de données.**

Voici quelques commandes à retenir afin de gérer les utilisateurs.

**Lister les utilisateurs :**

select * from radcheck;

**Supprimer un compte utilisateur :**

delete from radcheck where id='3';

**Ajouter un compte utilisateur avec password clair :**

INSERT INTO radcheck(Username,Attribute,op,Value) VALUES ('nomutilisateur','Cleartext-Password',':=','votremotdepasse');

**Ajouter un compte utilisateur avec password crypté :**

INSERT INTO radcheck (Username, Attribute, op, Value) VALUES ('nomutilisateur','Crypt-Password',':=',ENCRYPT ('votremotdepasse'))

**Ajouter un NAS :**

INSERT INTO nas (nasname, shortname, secret) VALUES ('IPDeVotreNAS,'NomDuNAS','MotDePasse');

Voilà si tout est OK, alors le serveur RADIUS est opérationnel. On peut à présent configurer l'équipement réseau (ici PFsense) pour faire ses requêtes sur le serveur RADIUS.